

# AVG BUSINESS MANAGED WORKPLACE<sup>®</sup> 10 SP2 MR1

User Guide



# TABLE OF CONTENTS

---

<b>Chapter 1: Welcome</b> .....	<b>17</b>
<i>About this Document</i> .....	18
<i>Where to Get More Help</i> .....	18
<i>Contact Us</i> .....	18
Documentation .....	18
Technical Support .....	19
AVG Partner Portal .....	19
<b>Chapter 2: What's New in Managed Workplace</b> .....	<b>21</b>
<i>What's New in This Release</i> .....	22
<b>Chapter 3: Introducing Managed Workplace</b> .....	<b>31</b>
<i>Managed Workplace</i> .....	32
About Managed Workplace .....	32
Logging In and Out.....	33
Changing Your Login Password .....	33
<i>Learning the Essentials</i> .....	34
Using the Central Dashboard .....	34
Viewing Assets .....	35
Service Plans .....	36
Grouping .....	36
Monitoring.....	37
Monitoring Network Services .....	37
Monitoring Cloud Services and Websites .....	38
Alerting .....	42
Reporting .....	46
<i>Viewing Managed Workplace Contract Information</i> .....	47
Viewing Your Managed Workplace Account Summary .....	47
<b>Chapter 4: Working with Service Plans</b> .....	<b>49</b>
<i>What is a Service Plan?</i> .....	50
About Service Plans .....	50
<i>Working with Policies and Services</i> .....	51
Understanding Policies and Services .....	51
Getting Started with Policies .....	53
Understanding Services .....	53
Creating Services.....	54
Adding Service Modules to Services .....	56
Copying Services .....	57
Modifying Services.....	57
Run the Policy Application Rules in a Service .....	58
<i>About the Built-in Service Plans in Managed Workplace</i> .....	58
Reactive Service Plan .....	59

---

Proactive Service Plan.....	59
Fixed Fee Service Plan.....	60
Comparing the Built-In Service Plans.....	60
<i>Creating Service Plans</i> .....	61
Creating a Service Plan .....	61
<i>Determining a Service Delivery Model</i> .....	62
Understanding Site versus Group Service Delivery Model .....	62
<i>Applying Service Plans to Existing Sites</i> .....	63
Viewing the Service Plan Application for a Site .....	63
Applying a Service Plan to a Site .....	63
<i>Applying Service Plans to Site Groups</i> .....	64
Applying Service Plans to a Site Group .....	64
<i>Setting Up Execution Schedules</i> .....	65
Understanding Execution Schedules .....	66
Execution Schedule Best Practices .....	66
Creating an Execution Schedule .....	67
Setting the Automation Schedule .....	67
Setting the AVG AntiVirus Schedule .....	69
Setting the Patching Schedule .....	71
Suppressing Alerts During an Execution Schedule.....	72
Adding Sites, Groups, or Devices to an Execution Schedule.....	73
Setting an Execution Schedule as the Default .....	73
Copying an Execution Schedule .....	74
Deleting an Execution Schedule .....	74
<i>Setting Up Maintenance Schedules</i> .....	75
Understanding Maintenance Schedules .....	75
Creating a Maintenance Schedule .....	76
Setting the Maintenance Schedule.....	77
Editing a Maintenance Schedule .....	80
Terminating a Maintenance Schedule .....	80
Deleting a Maintenance Schedule .....	82
Setting Up Ad Hoc Maintenance Schedules.....	82
Extending the Duration of Ad Hoc Maintenance Schedules.....	84
<i>Viewing, Modifying, and Organizing Service Plans</i> .....	85
Comparing Service Plans with the Comparison View .....	85
Viewing a List of Service Plans with the Table View .....	86
Viewing Descriptive Information about Service Plans with the Panel View .....	87
Managing Service Plan Precedence .....	87
Copying Service Plans .....	87
<i>Viewing Service Plan Activity on the Services Dashboard</i> .....	88
Viewing and Filtering Data on the Services Dashboard .....	89
Viewing Alerts from the Services Dashboard .....	90
Viewing AVG AntiVirus Results on the Services Dashboard .....	90
Viewing Automation Results on the Services Dashboard .....	91
Viewing Patch Management Results on the Services Dashboard .....	92

---

Viewing Reporting Results on the Services Dashboard .....	94
Viewing Trouble Ticket Results on the Services Dashboard .....	94
<b>Chapter 5: Setting Up and Maintaining Sites .....</b>	<b>97</b>
<i>About Sites</i> .....	98
<i>Setting Up a Site Managed By Onsite Manager</i> .....	100
Creating a Site in Service Center .....	100
Installing Premium Remote Control Automatically on Devices Added to Sites.....	103
Setting Default Premium Remote Control Options for Creating New Sites .....	104
Deploying Onsite Manager within a Domain .....	105
About Scan Configuration .....	108
Configuring the Scan Range .....	110
Discovering and Onboarding Devices .....	113
Configuring Device Discovery .....	115
Running a Scan Manually .....	121
Running an MBSA Scan Manually .....	121
Enabling or Disabling Power Management for a Site .....	122
Upgrading and Rebooting Onsite Managers.....	122
<i>Adding Device Managers to a Site</i> .....	123
Installing Device Managers .....	123
Searching for a Device Manager .....	125
Updating Device Managers.....	125
Rebooting Device Managers .....	126
Uninstalling Device Managers .....	126
<i>Working with Sites</i> .....	127
Viewing an Overview about a Site .....	127
Viewing Alerts for a Site.....	128
Viewing Devices at a Site .....	128
Viewing and Changing the Service Plans and Services Applied to a Site .....	128
Changing the Service Delivery Model for a Site.....	130
Viewing and Changing the Execution Schedules Applied to a Site .....	132
Putting a Site on Hold .....	132
Approving a Site After It's Been On Hold.....	133
Deleting a Site .....	133
Adding Consent to a Site.....	133
Viewing Information about a Site .....	134
Changing Contact Information for a Site .....	135
Viewing the Physical Location of a Site on a Map .....	135
Adding Notes about a Site .....	135
<i>Setting Site Options</i> .....	136
Setting Premium Remote Control Options .....	136
Setting When to Run an MBSA Scan .....	137
Setting When to Delete Down Devices.....	138
Setting the Website Addresses to Use to Determine Internet Availability .....	139
Setting the Polling Interval for Printer Monitoring.....	140
Setting Site-Specific Options for Power Management .....	140

---

---

Setting Alerting Actions for Site Communication Failures.....	140
Setting Alerting Actions for New Devices for a Site.....	143
Setting Alert Actions for Loss of Monitoring Protocol at a Site.....	144
Modifying the Alert Configurations.....	145
Setting the Device Discovery Defaults.....	146
<i>Managing Site Credentials.....</i>	<i>146</i>
<i>About Updating Service Center.....</i>	<i>151</i>
About Using Update Center.....	151
Viewing Notifications for Product Updates.....	152
Updating Managed Workplace Products.....	153
Updating Service Center.....	154
Updating and Installing Service Center Components.....	155
Viewing a List of Available Components.....	155
<b>Chapter 6: Setting Up User Accounts and Roles .....</b>	<b>159</b>
<i>Setting Up User Accounts .....</i>	<i>160</i>
About User Accounts.....	160
Creating a User Account.....	161
Adding a Role to a User Account.....	162
Deleting a Role from a User Account.....	162
Setting the Objects a User Account Can Access.....	163
Removing the Objects a User Account Can Access.....	164
Deleting a User Account.....	164
Setting Global Account Options.....	164
Setting User Account Options.....	166
<i>Setting Up Roles.....</i>	<i>169</i>
About Roles.....	169
Creating a Role.....	170
Adding a User Account to a Role.....	171
Deleting a User Account from a Role.....	171
Setting Permissions for a Role.....	172
Renaming a Role.....	173
Deleting a Role.....	173
<b>Chapter 7: Grouping.....</b>	<b>175</b>
<i>About Grouping.....</i>	<i>176</i>
<i>Creating Service and Site Groups.....</i>	<i>178</i>
Creating a Group.....	178
Creating Rules to Automatically Add Devices to a Group.....	179
Defining Scope for a Service Group.....	187
Excluding Sites, Groups, and Devices from the Scope.....	189
Previewing a Group.....	191
Running the Automatic Inclusion Rules for a Group.....	191
Manually Adding Devices to Groups.....	191
Applying Policies to Groups.....	194
Viewing the Policies Applied to a Group.....	195

---

Applying MDM Configuration Profiles to a Group.....	195
<i>Creating Shared Site Groups</i> .....	196
<i>Managing Groups</i> .....	198
Replicating Site Groups.....	198
Viewing the Devices Included in a Group .....	199
Renaming Groups and Service Group Folders .....	199
Moving a Service Group to a Different Group Folder .....	200
Deleting a Service or Site Group .....	200
<b>Chapter 8: Working with Assets and Devices.....</b>	<b>201</b>
<i>Assets</i> .....	202
About Asset Management .....	202
Viewing Windows Inventory .....	203
Viewing SNMP Inventory .....	204
Viewing Mobile Device Inventory.....	204
<i>Devices</i> .....	204
About Devices .....	204
Viewing a List of Devices.....	206
Viewing Summary Details about a Device .....	208
Viewing Details about a Printer .....	215
Viewing Details about a Virtual Machine.....	215
Customizing Devices .....	217
Viewing and Changing the Service Plans, Services, and Policies Applied to a Device ..	222
Viewing and Changing the Execution Schedules Applied to a Device .....	225
Working with a Device .....	226
Purging an IP Address from a Device .....	228
Searching for a Device .....	230
<i>Waking Managed Devices Remotely</i> .....	233
About Wake-on-LAN .....	233
Creating a User Account for End Users to Wake Computers at a Site.....	234
Waking a Computer on the Device Overview Page .....	234
Waking a Computer Remotely.....	234
Communicating Steps to End Users for Waking Computers.....	234
<i>Working with Intel® vPro™ Devices</i> .....	236
About Intel® vPro™ Devices.....	236
Setting the Host Name for an Intel® vPro™ Device .....	237
Configuring the Network Settings for an Intel® vPro™ Device .....	237
Enabling or Disabling IDE Redirection (IDE-R) for an Intel® vPro™ Device .....	238
Enabling or Disabling Serial-over-LAN (SOL) .....	238
Enabling or Disabling User Consent for Intel® KVM .....	238
Configuring the Intel® AMT Administrator Account Credentials.....	239
Viewing the Configuration History of Intel® AMT-Enabled Devices .....	239
Determining the Power Status of Intel® AMT Devices .....	239
Powering-on, Powering-off, or Resetting an Intel® AMT Device Remotely.....	240
Viewing the Status of Intel® AMT-Enabled Devices.....	240

---

---

Viewing Intel® AMT Device Events .....	241
Viewing Intel® AMT Device Hardware .....	241
<b>Chapter 9: Managing Mobile Devices .....</b>	<b>243</b>
<i>About Mobile Device Management (MDM) .....</i>	<i>244</i>
<i>Setting Up iOS Mobile Devices for Monitoring .....</i>	<i>246</i>
About Setting Up iOS Mobile Devices .....	246
Setting Up an MDM Signing Certificate for iOS (MSP) .....	247
Setting Up an Apple-Approved APNs Certificate for iOS (Customer) .....	249
Working with iOS Certificates .....	250
<i>Setting up Android Mobile Devices for Monitoring .....</i>	<i>253</i>
About Setting up Android Mobile Devices .....	253
<i>Enrolling Mobile Devices .....</i>	<i>255</i>
About Provisioning Mobile Devices .....	255
Generating a Provisioning Code for Mobile Devices at a Site .....	256
<i>Viewing Mobile Devices .....</i>	<i>257</i>
Viewing a List of Mobile Devices at a Site .....	257
Viewing Details about a Mobile Device .....	258
Viewing Hardware Installed on a Mobile Device .....	258
Viewing Software Installed on a Mobile Device .....	258
Getting the Latest Assets on a Mobile Device .....	258
Locating a Mobile Device .....	259
<i>Securing Mobile Devices .....</i>	<i>259</i>
About Securing Mobile Devices .....	259
Locking a Mobile Device .....	260
Setting the Passcode for a Mobile Device .....	260
Removing the Passcode for a Mobile Device .....	261
Wiping Data from a Mobile Device .....	261
Configuring Lost Device Actions for Mobile Devices .....	261
Mark a Mobile Device as Lost .....	264
Mark a Lost Mobile Device as Found .....	265
<i>Adding a Monitor for Mobile Devices .....</i>	<i>265</i>
<i>About Configuration Profiles .....</i>	<i>267</i>
<i>Setting Up iOS and OS X Configuration Profiles .....</i>	<i>269</i>
Configuring Passcode Settings for iOS Mobile Devices and OS X Devices .....	269
Configuring Network Settings for iOS and OS X Devices .....	270
Configuring Security and Privacy Settings for iOS and OS X Devices .....	272
Configuring VPN Settings for iOS and OS X Devices .....	272
Configuring Restrictions for iOS Mobile Devices .....	274
Configuring Energy Saver Settings for OS X Devices .....	275
Configuring Parental Controls for OS X Devices .....	277
Configuring Restrictions for OS X Devices .....	279
Configure the OS X Software Update Server .....	280
<i>Setting up Android Mobile Device Configuration Profiles .....</i>	<i>280</i>
Configuring Passcode Settings for Android mobile devices .....	280
Configuring Restrictions for Android Mobile Devices .....	282

---



---

<i>Configuring Email for Mobile Devices</i> .....	282
Configuring Email Policies for iOS Mobile Devices .....	282
Configuring Email Policies for Android Mobile Devices.....	286
<i>Deleting a Configuration Policy</i> .....	287
<i>Removing a Mobile Device from Monitoring</i> .....	287
Removing a Mobile Device from Monitoring in Service Center .....	287
Uninstalling the Mobile Manager Agent from a Mobile Device .....	288
<b>Chapter 10: Monitoring</b> .....	<b>289</b>
<i>Monitoring in Managed Workplace</i> .....	290
About Monitoring .....	290
<i>Monitoring Policies</i> .....	291
About Monitoring Policies .....	291
<i>Installing and Importing Monitoring Policies</i> .....	293
Installing vs. Importing .....	293
Installing a Monitoring Policy .....	293
Importing a Monitoring Policy.....	294
<i>Using Monitoring Policies</i> .....	294
About Using Monitoring Policies .....	294
Creating Automatic Inclusion Rules for a Monitoring Policy .....	294
Modifying an Automatic Inclusion Rule.....	299
Deleting an Automatic Inclusion Rule.....	299
Previewing an Automatic Inclusion Rule .....	300
Automatic Inclusion Rule Examples.....	300
Modifying Monitoring Policy Details .....	302
Exporting a Monitoring Policy .....	303
Copying a Monitoring Policy .....	303
Deleting a Monitoring Policy .....	304
Upgrading to a New or Changed Monitoring Policy .....	304
Applying a Monitoring Policy to a Group or Device.....	305
Removing a Monitoring Policy from a Group or Device .....	305
Excluding Devices from a Monitoring Policy.....	306
<i>Optimizing Monitoring Policies</i> .....	306
Adding a New Monitor to a Monitoring Policy .....	306
Turning a Monitor in a Monitoring Policy On or Off.....	307
Deleting a Monitor from a Monitoring Policy.....	308
Setting How Often a Monitor Runs.....	308
Overriding an Alert in a Monitoring Policy .....	309
<i>Creating a Custom Monitoring Policy</i> .....	310
<i>Adding Your Own Monitors</i> .....	311
About Adding Your Own Monitors .....	311
Adding a Monitor for AMT (Active Management Technology) Events.....	312
Adding a Monitor for AVG AntiVirus.....	313
Adding a Monitor for Bandwidth.....	314
Adding a Monitor for Custom Log Files .....	316
Setting Options for Device Availability Monitors.....	318

---

---

Adding a Monitor for Device Warranty .....	319
Adding a Monitor for Microsoft Baseline Security Analyzer (MBSA) Reports .....	321
Adding a Monitor for Mobile Devices.....	323
Adding a Monitor for Network Services .....	325
Adding a Monitor for Patch Status .....	327
Adding a Monitor for Performance Counters.....	328
Adding a Monitor for Print Services.....	330
Adding a Monitor for Microsoft System Center Essentials (SCE).....	331
Adding a Monitor for SNMP Object Identifiers (OIDs).....	332
Adding a Monitor for SNMP OIDs from MIB.....	335
Adding a Monitor for SNMP Traps.....	337
Adding a Monitor for Syslog Messages.....	338
Adding a Monitor for Windows Events.....	340
Adding a Monitor for Windows Services .....	346
Adding a Monitor for Basic Websites or Cloud Services.....	347
Using iReasoning to Add SNMP OID Information to Service Center.....	354
<i>System Log Viewer</i> .....	355
Viewing System Log Information .....	355
<b>Chapter 11: Alerting.....</b>	<b>357</b>
<i>Alerting</i> .....	358
About Alerting.....	358
<i>Setting Alert Actions</i> .....	359
Locating Monitors.....	359
Setting an Alert to Send an Email .....	360
Adding Remediation Information to an Alert Email .....	361
Setting Alert Severity .....	361
Setting an Alert to Create a Trouble Ticket .....	361
Setting an Alert to Self-heal.....	361
Setting an Alert to Run a Script.....	363
Escalating an Alert .....	364
<i>Suppressing Alerts</i> .....	364
Suppressing an Alert .....	365
Suppressing an Alert from an Alert Email.....	365
Viewing Suppressed Alerts .....	365
Reactivating a Suppressed Alert .....	365
<i>Clearing Alerts</i> .....	366
<i>Viewing Cleared Alerts for a Device</i> .....	366
<i>Creating Alert Categories</i> .....	366
About Alert Categories .....	366
Creating an Alert Category .....	367
Editing an Alert Category.....	368
Renaming an Alert Category .....	368
Categorizing an Alert .....	368
Filtering Alerts by Alert Category.....	369
Deleting an Alert Category.....	369

---

<i>Scheduling When Alerts are Delivered</i> .....	370
About Alerts.....	370
Creating an Alert Schedule.....	371
Disabling and Enabling an Alert Schedule.....	371
Deleting an Alert Schedule.....	372
<i>Best Practices for Alerting</i> .....	372
Analyze Alerts.....	372
Analyze Results.....	373
Alert on Success.....	374
<b>Chapter 12: Automating Tasks</b> .....	<b>375</b>
<i>About Automation in Managed Workplace</i> .....	376
About Automating Tasks.....	376
About the Automation Dashboards.....	377
Automation Requirements.....	377
<i>Scripts, Automation Packages, and Tasks</i> .....	379
Scripts.....	379
Automation Packages.....	379
Tasks and Quick Tasks.....	380
<i>Creating Automation Packages</i> .....	380
Create a Script Package.....	380
Adding Scripts and Child Scripts to a Package.....	381
Change the Order of Scripts in a Package.....	382
<i>Preparing Scripts and Packages for Use in a Policy or Task</i> .....	382
Viewing Script Details.....	383
Set Up Alert Conditions for Scripts in a Package.....	383
Set Up Package Termination Conditions.....	384
Adding a Quick Task.....	385
<i>Creating Automation Policies</i> .....	386
Creating Automation Policies.....	386
Applying Automation Policies.....	390
<i>Adding, Importing, and Exporting Scripts and Packages</i> .....	393
About Adding Scripts.....	393
Adding a Script to Managed Workplace.....	397
Importing a Script.....	403
Exporting a Script.....	403
Using Script Templates.....	404
<i>Managing Scripts, Automation Packages, and Quick Tasks</i> .....	405
Viewing Scripts, Automation Packages, and Quick Tasks.....	405
Copying Scripts, Automation Packages, and Quick Tasks.....	405
Designate a Script, Automation Package, or Quick Task as a Favorite.....	406
Viewing Your Favorite Scripts, Packages, and Quick Tasks.....	407
Installing a Script or Automation Package.....	407
Updating a Script or Automation Package.....	407
Deleting a Script.....	408
<i>Scheduling Tasks</i> .....	409

---

---

Adding a Task.....	409
<i>Working with Tasks</i> .....	415
Viewing Tasks.....	415
Following Up on Executed Tasks.....	416
Changing a Task .....	418
Deleting a Task.....	419
<b>Chapter 13: Managing AVG AntiVirus .....</b>	<b>421</b>
<i>About AVG AntiVirus in Managed Workplace</i> .....	422
Using AVG AntiVirus in Managed Workplace .....	422
<i>Setting Up AntiVirus Policies</i> .....	423
About the Default AntiVirus Policies .....	424
Creating a New AntiVirus Policy .....	425
Installing AntiVirus on Devices.....	426
Copying an AntiVirus Policy .....	427
Creating Rules to Automatically Apply an AntiVirus Policy .....	427
Manually Applying an AntiVirus Policy to Devices and Groups .....	428
Configuring the Settings for an AntiVirus Policy .....	428
Removing an AntiVirus Policy .....	451
<i>Setting up AVG AntiVirus Monitoring</i> .....	452
<i>Managing AVG AntiVirus in Managed Workplace</i> .....	452
AVG AntiVirus Overview Dashboard.....	453
AVG AntiVirus Site Dashboard .....	453
AVG AntiVirus Device Dashboard .....	454
Managing AVG AntiVirus Deployment.....	454
Managing AntiVirus Alerts .....	458
Keeping Devices Secure .....	460
<b>Chapter 14: Reporting.....</b>	<b>463</b>
<i>Reports</i> .....	464
About Reports.....	464
<i>Creating a Report</i> .....	466
About Creating a Report .....	466
Creating a Report.....	469
Exporting Managed Workplace Screens to a File .....	470
Copying a Report .....	471
<i>Previewing a Report</i> .....	471
Previewing a Report.....	471
Viewing a Report that Shows Information from More than One Onsite Manager or Site .....	473
<i>Creating Report Policies</i> .....	473
Applying Report Policies .....	476
Viewing Report Policy Execution Results.....	478
<i>Managing Reports</i> .....	478
Viewing a List of the Predefined Reports .....	478
Changing the Report Category for a Report .....	478

---

Installing a Report.....	479
Importing a Report .....	479
Updating a Report.....	480
Deleting a Report.....	480
<i>Organizing Reports into Categories.....</i>	<i>481</i>
About Report Categories .....	481
Creating a Report Category .....	481
Renaming a Report Category.....	481
Assigning a Report to a Report Category.....	481
Deleting a Report Category .....	482
<i>Scheduling a Report.....</i>	<i>482</i>
Creating a Delivery Schedule for a Report.....	482
Viewing the List of Scheduled Reports .....	485
Running a Scheduled Report Immediately .....	485
Deleting a Scheduled Report .....	485
<i>Working with Archived Reports.....</i>	<i>486</i>
About Archiving .....	486
Viewing the Historical Information for a Report .....	486
Exporting an Archived Report to a ZIP File .....	486
Deleting an Archived Report.....	486
<b>Chapter 15: Using Service Modules.....</b>	<b>489</b>
<i>About Service Modules .....</i>	<i>490</i>
<i>Setting Up a Service Module.....</i>	<i>490</i>
Installing a Service Module.....	490
Importing a Service Module .....	490
Updating a Service Module.....	491
Viewing an Overview of All Service Modules.....	491
Viewing Monitoring Information about a Service Module .....	491
Deleting a Service Module .....	492
<b>Chapter 16: Working Remotely .....</b>	<b>493</b>
<i>Remote Control.....</i>	<i>494</i>
About Remote Control.....	494
<i>Initiating a Remote Control Session.....</i>	<i>498</i>
Using the Shortcut Icon .....	498
Initiating a Remote Control Session Using AVG Business Premium Remote Control... 498	
Initiating a Remote Control Session Using AVG Business Premium Remote Control - On Demand.....	499
Initiating a Remote Control Session Using Remote Desktop .....	501
Initiating a Remote Control Session Using Remote Assistance .....	502
Initiating a Remote Control Session Using VNC, Telnet, or PuTTY.....	503
Initiating a Remote Control Session Using UltraVNC.....	504
Initiating a Remote Control Session Using Onsite Manager Utilities.....	505
Initiating a Remote Session to Access the Web Console of Managed Devices .....	506

---

Initiating a Remote Session to Access Intel® AMT-Enabled Devices .....	507
Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM . 509	
Initiating a Remote Control Session by Launching TeamViewer .....	510
Initiating a Remote Control Session by Launching LogMeIn Pro .....	511
Initiating a Remote Control Session by Launching ScreenConnect .....	512
Initiating a Remote Control Session by Launching a Third-Party Remote Control Tool 512	
Saving Remote Control Session Settings.....	516
<i>Working with the Remote Tools</i> .....	516
About Remote Tools .....	516
Using Remote Tools .....	518
<i>Viewing the Remote History</i> .....	524
<i>Adding a Note to a Remote Session</i> .....	524
<i>Edit a Remote Session Note</i> .....	525
<i>Troubleshooting Remote Connections</i> .....	525
<i>Using Onsite Manager Utilities</i> .....	525
<b>Chapter 17: Managing Patches</b> .....	<b>529</b>
<i>About Patch Management</i> .....	530
<i>Understanding the Default Patch Management Settings</i> .....	532
Understanding the Pre-Built Patch Policies .....	533
<i>Setting Up Patch Management in Managed Workplace</i> .....	535
Creating a Patch Policy .....	535
Applying Patch Policies .....	539
Setting Up Approval Groups .....	542
Setting Synchronization Options .....	545
<i>Reviewing Updates</i> .....	547
Viewing an Overview of Patch Management .....	547
Viewing Patches.....	549
Viewing Patch Status .....	551
Run Patches on Devices Immediately .....	552
<i>Approving Updates</i> .....	553
Approving Updates for Installation.....	553
Declining Patches.....	555
Approving Updates for Removal.....	555
Automatically Approving Updates for an Approval Group.....	556
<i>Stopping Patch Management</i> .....	557
Stopping Patch Management for a Device .....	557
<b>Chapter 18: Setting Up Power Management</b> .....	<b>559</b>
<i>About Power Management</i> .....	560
<i>Getting Ready to Use Power Management</i> .....	563
About Power Cost and Usage .....	563
Setting Defaults for Power Management .....	563
Site-Specific Options for Power Management.....	564

---

Marking a Machine as a Virtual Machine .....	567
<i>Viewing Summary Information about Power Management</i> .....	568
<i>Working with Power Plans</i> .....	569
Adding a Managed Workplace Power Plan .....	569
Removing a Device or Group from a Power Plan .....	570
Renaming a Power Plan .....	570
Copying a Power Plan .....	570
Deleting a Power Plan.....	570
Enabling or Disabling Power Management for a Device .....	571
Overriding Power Plan Settings for a Device .....	571
<i>Setting and Overriding Power Plan Precedence</i> .....	572
Setting Power Plan Precedence for Groups.....	572
Overriding Power Plan Precedence for a Device .....	572
<i>Power Plan Settings and Options</i> .....	573
Power Plan Settings .....	573
Vista + Settings .....	573
<b>Chapter 19: Working with Trouble Tickets .....</b>	<b>577</b>
<i>Working with Trouble Tickets</i> .....	578
About Trouble Tickets.....	578
Viewing Trouble Tickets.....	578
Adding a Trouble Ticket .....	579
Changing a Trouble Ticket .....	580
Printing a Trouble Ticket.....	580
Closing Trouble Tickets .....	580
<b>Chapter 20: Customizing Support Assistant .....</b>	<b>583</b>
<i>Customizing Support Assistants</i> .....	584
About Customizing Support Assistant .....	584
Creating a Support Assistant Policy .....	585
Editing a Support Assistant Policy.....	594
Copying a Support Assistant Policy.....	594
Deleting a Support Assistant Policy .....	594
Updating Support Assistant at a Site .....	595
Uninstalling a Support Assistant from a Site or Device .....	596
<i>Keeping Track of Support Assistant Deployment</i> .....	597
<i>Using Support Assistant from a Device</i> .....	598
<b>Chapter 21: Customizing Service Center.....</b>	<b>599</b>
<i>Branding Service Center</i> .....	600
Branding Service Center .....	600
Applying Themes to Service Center .....	601
<i>Customizing Service Center</i> .....	602
Setting Refresh Options for the Central Dashboard and Alert Lists .....	602
Enabling or Disabling Website Usage Tracking.....	602
Setting Regional Preferences .....	602
Setting Onsite Manager Installer Preferences .....	604

---

---

Adding or Deleting Performance Counters.....	605
Adding or Deleting SNMP OIDs.....	606
Adding or Deleting a Custom Network Service.....	607
Setting How Long to Keep the Data.....	608
Viewing or Changing the Communication Settings .....	609
Setting Default Email Options.....	611
Turning Log Monitoring On or Off .....	612
Setting System-Wide Alerting Actions for Site Communication Failures.....	612
Setting System-Wide Alerting Actions for New Devices.....	615
Setting System-Wide Alerting Actions for Loss of Monitoring Protocol.....	616
Modifying the Alert Configurations .....	616
Creating Custom Ticket Statuses .....	617
Working with Printer Transforms .....	618
Setting Remote Control Options.....	620
Configuring Secure Sign On .....	626
Collecting Diagnostics for Support Purposes .....	629
Configuring Modems .....	630
<b>Chapter 22: Working with Mobile Service Manager.....</b>	<b>633</b>
<i>Working with Mobile Service Manager .....</i>	<i>634</i>
About Mobile Service Manager .....	634
Logging In and Out on a Mobile Device .....	634
Viewing an Alert on a Mobile Device .....	634
Suppressing an Alert on a Mobile Device .....	635
Clearing an Alert on a Mobile Device .....	635
<b>Glossary .....</b>	<b>637</b>



## CHAPTER

# 1

## WELCOME

---

*Managed Workplace is a web-based, single pane of glass dashboard providing access to a simplified and centrally planned service delivery platform. The service delivery model aligns with best practices to standardize services that save time, drives efficiencies to new heights and helps MSPs accelerate their sales.*

---

---

## About this Document

This document provides detailed information about Managed Workplace. It's designed to be used as a reference in your everyday work.

Before using this document, you need to install and configure Managed Workplace by following the instructions in the *Setup Guide*.

## Where to Get More Help

**Setup Guide** Contains instructions about how to install and configure Managed Workplace.

**Online Help** Contains all the information from the *User Guide* optimized for use online.

**Integration Guide: Service Desks** Contains the procedures required to integrate Professional Services Automation (PSA) tools or service desks with Managed Workplace.

**Release Notes** Provides last-minute information about the product and documentation.

**Domain Configuration Document** Contains an overview of domain configuration.

**AVG Support Center** The AVG Support Center website contains hundreds of articles to help you use Managed Workplace, including self-guided troubleshooting tools, advanced topics, and answers to frequently asked questions. The Support Center also includes links to connect you by email to an AVG support agent for more specialized help. To access Support Center, in Service Center, click **Help > Support Center**.

**Training** AVG offers a series of live and on-demand technical training courses for all registered Partners. For more information, click [here](#). (You must log into the Partner Portal to access the Training.)

## Contact Us

### Documentation

We are committed to making your experience with our product the best it can be. If you find any errors or omissions in our documentation, or have suggestions for improving it, write to us:

[mwdocumentation@avg.com](mailto:mwdocumentation@avg.com)

---

## Technical Support

Support hours and contact information can be found on the AVG Partner Portal:

[AVG Managed Workplace Technical Support](#)

## AVG Partner Portal

Click this link to access the [AVG Partner Portal](#), click and then log in with your Username and Password.

**Technical Information** To find technical information such as product downloads, performance guidelines, libraries of policy modules, resource library, scripts and predefined reports, log into the AVG Partner Portal and in the main menu, click Download.

**Partner Services** To find training information, including live and 'on demand' training, a list of courses, course descriptions and a course calendar, log into the AVG Partner Portal and in the main menu, click Learn.

To access Knowledgebase articles and frequently asked questions (FAQ), click Knowledgebase located under the Learn menu.

To view or participate in discussions about Managed Workplace, select Forums under the Connect menu.



CHAPTER

# 2

## WHAT'S NEW IN MANAGED WORKPLACE

---

*This chapter provides an overview of the new and enhanced features in the current release of Managed Workplace.*

---

---

## What's New in This Release

### What's New in Managed Workplace 10 SP2 MR1

#### Reboot Control

We have simplified and clarified the user interface for controlling reboots after patches have been applied to devices. When patches require a device reboot, you can choose to have devices reboot immediately, or wait to reboot until after a logged on user finishes their work.

See [To set up a patch schedule that overrides any applicable execution schedules](#).

#### Improvements to Autotask Integration

You can now map Autotask asset types in Managed Workplace.

See Completing the Service Desk Configuration in the Autotask chapter of the PSA Guide.

### What's New in Managed Workplace 10.0 SP2

#### Maintenance Schedules

During maintenance activities, certain sites or devices may become unavailable, resulting in alerts. The new Maintenance Schedule feature lets you suppress alerts on your sites, groups, and devices for the duration of a maintenance activity. For example, if you're performing maintenance that takes a group of devices offline, it would be useful to suppress Device Availability alerts.

While you use Maintenance Schedules, monitoring continues, keeping your system safe. Suppressing alerts frees up the time and effort of having to clear alerts that aren't useful, and prevents unnecessary alerts from pulling a technician's focus from issues that have real-world consequences.

With Maintenance Schedules, you have the option to exclude maintenance downtime from other downtime when generating a report. If you take a site down for maintenance purposes, because the downtime is expected, it won't be reported as downtime on reports and won't affect your statistics.

Use Maintenance Schedules on an ad hoc, one-time basis, or repeat them when you perform maintenance every day, week, or month. You can also add Maintenance to Execution Schedules.

See [Creating a Maintenance Schedule](#).

---

## VAR Admin Maintenance Mode

From VAR Admin, you can now put sites into Maintenance mode, which suppresses Site Not Communicating alerts while you perform maintenance on the site. For details, see the VAR Administration Guide.

## Reporting on Windows Events

You can now create a report of Windows Events, making it easier to troubleshoot application and driver software. Using the Windows Event Details report, you can create up to ten filters that will either include or exclude certain Windows Events, giving you the data you need quickly, letting you easily find and resolve issues.

Windows Event Detail reports also include a pie chart that will display the events that you highlight. For example, if you filter on log on events, you can customize the chart to see if a large proportion of log on events are failing—identifying a potential attack in seconds. See [About Creating a Report](#).

## Reporting on Networks

Managed Workplace can now assess your network and deliver the results as an easy-to-read report that gives you a complete picture of your network landscape. This report helps you better estimate workloads, track devices, and identify vulnerabilities such as unprotected assets. The Aggregate Site Device List report delivers accurate counts of:

- Devices
- Servers
- Workstations
- Printers
- Mobile Devices
- Network Devices
- Devices with AVG Antivirus installed

See [About Creating a Report](#).

## Email Alert Enhancements

Alert emails now have clear, scannable subject lines that let technicians prioritize issues at a single glance. Critical issues, and which systems they impact, can be identified by their subject line even when buried among dozens of other emails. This reduces the time spent searching for issues and gives technicians more time to solve them.

---

Alert emails help technicians solve issues right from their inboxes. Most alert emails now include an actionable description of the alert, links to knowledge base articles for more information, and buttons that let technicians initiate actions right from the body of the email itself.

### **More Accurate Alerting**

Managed Workplace has made alerts even more useful and accurate. This upgrade introduces a new alert type, Invalid Credential. The new type of alert identifies when sites, groups, and devices experience a loss of monitoring due to invalid credentials. Receiving this type of alert will help technicians diagnose and solve monitoring issues faster and more accurately.

### **Mac Support for Premium Remote Control On-Demand**

Premium Remote Control On-Demand sessions can now be initiated from Apple computers, giving more users access to this powerful tool. See [Launching an On-Demand Session - Mac OS](#).

## **What's New in Managed Workplace 10.0 SP1**

### **Premium Remote Control Enhancements**

Previously, unmanaged devices could not be remotely assisted by AVG Managed Workplace. Premium Remote Control On Demand is now available allowing you to connect to your customer's unmanaged devices.

An option to add consent within Premium Remote Control is available for sites where sensitive information could potentially be accessible. This is a configurable item on a per-Site basis.

### **AVG Antivirus**

Integrated Managed Workplace Antivirus now deploys AVG Antivirus 2016. All of your customers now have access to the latest and greatest Antivirus for the most up-to-date protection.

With AVG Antivirus 2016, you can now configure proxy settings for your Antivirus via a policy – these can be defined manually or by a Proxy Auto Configuration. In addition, you can now enable/disable Online Shield's TLS/SSL inspection.

### **Reporting Enhancements**

With the release of Managed Workplace 10.0 SP1 custom reporting has been enhanced. Site Asset Baseline has been updated to display a list of devices in a site based on user specified criteria. Additional data populates textbox filters



---

with suggested values (based on actual values present in the database) as the user types. For Windows and OSX devices only.

Device Asset Inventory displays asset information for a single device. A section for Microsoft Product Keys is now available, which can be selected to be included or excluded from the report. Improvement to the reporting also includes a breakdown of the Hardware sections into subcategories. Each category can be selected to be included or excluded from report.

### **Alerting Enhancements**

Several enhancements have been made to the Alerting functionality. Managed Workplace 10.0 SP1 includes enhancements that help to limit the number of false alerts generated. For example: Device Down alerts for printers and servers has been improved. They will now be checked with TCP/SNMP regardless if they respond to a ping – this will help you determine the status more accurately.

SNMP Trap monitors and Syslog Monitor now have the option to set an alert threshold. These are done by occurrences and time periods similar to Windows Events. Alert emails no longer contain all the information about each trap, but instead link into Managed Workplace so you can view them on the device's page.

Loss of Monitoring protocol now has a detailed description of how the protocol was lost to help you understand what corrective action to take.

Event detail searching is more detailed for better filtering. A new addition is the “does not contain” option. This is now available for Windows Events, SNMP traps, Syslog, and Website Monitors.

## **What's New in Managed Workplace 10.0**

### **Revolutionary Service Delivery Changes**

Managed Workplace 10.0 introduces an entirely new way to standardize and maintain your service offerings. Now, you can set up service plans that represent the different levels of service that you offer your customers. At the core of the service plan model is the new concept of policies. A policy is a collection of configuration settings that determine how a device is monitored. There are six types of policies that you can create: monitoring, automation, reporting, patching, Support Assistant, and AVG AntiVirus. See [Working with Policies and Services](#).

Policies are grouped into services, which are then added to service plans. You can apply service plans to a site, or to groups. Managed Workplace 10.0 includes 3 services plans - Reactive, Proactive, and Fixed Fee - that have been carefully designed by AVG experts to represent baseline, enhanced, and top-

---

tier services. You can use these service plans as-is, or you can customize as needed. You can also create your own service plans. See [About the Built-in Service Plans in Managed Workplace](#) and [Creating Service Plans](#).

To minimize disruption at your customer networks, you can set up execution schedules that determine when patch, automation, and AVG AntiVirus activity occurs at your customer sites. You can create a default execution schedule that is applied to all new sites that you create, and you can override the applicable execution schedule right within the policy, if required. See [Setting Up Execution Schedules](#).

To keep track of service plan activity, Managed Workplace 10.0 includes a new Services Dashboard. You can choose whether to make this dashboard or the Central Dashboard the default that displays when you log into Service Center. The Services Dashboard displays active alerts for each service plan, and provides a jumping-off point to drill to details about automation, reporting, patching, AVG AntiVirus, and trouble ticket activity for each of your service plans. A new Service Infobar flyout displays a condensed version of the Services Dashboard, and is accessible from within any screen in Service Center.


See [Viewing Service Plan Activity on the Services Dashboard](#).

## What's New in Managed Workplace 9.2

### AVG Business Premium Remote Control

New in Managed Workplace 9.2 is the fully-integrated AVG Business Premium Remote Control, which uses ISL Light technology to connect remotely to managed devices, allowing you to file transfer, chat, and perform various administrative functions as you resolve issues remotely. AVG Premium Remote Control requires minimum configuration; the account credentials are automatically created when you enable it in System Settings, and the agent is automatically deployed to all managed devices. For information on enabling AVG Premium Remote Control, see [Configuring AVG Business Premium Remote Control Access](#).

**Note:** If you are upgrading to Managed Workplace 9.2, AVG Premium Remote Control is not enabled by default. However, if you are installing Managed Workplace 9.2 for the first time, AVG Premium Remote Control is enabled by default and the agent will be automatically deployed to managed devices.

When AVG Premium Remote Control is enabled, it is available as an option when remoting to a device, either from the shortcut icon  or from the Device page, by clicking Remote Control on the sidebar. For information on connecting to a device using AVG Premium Remote Control, see [Initiating a Remote Control Session Using AVG Business Premium Remote Control](#).

---

## AVG Device Manager for MAC OS X

You can now monitor and manage off-network MAC OS X devices with AVG Device Manager for MAC OS X. Now you can identify and monitor Mac devices that are not connected to the corporate network, and perform common functions such as automated tasks and remote control.

AVG Device Managers for MAC OS X are deployed and upgraded in the same manner as AVG Device Managers for Windows. For example, when you create a site in Service Center, you can choose to automatically deploy Device Managers to laptops. Onsite Manager will detect the laptop's operating system and deploy an AVG Device Manager for Windows to laptops with Windows operating systems, and an AVG Device Manager for MAC OS X for laptops with Mac OS X operating systems. Similarly, when you upgrade Device Managers in Update Center, both types of Device Managers will be upgraded. For more information, see [Adding Device Managers to a Site](#).

## Integrated AVG AntiVirus Enhancements

Integrated AVG AntiVirus has been enhanced to allow you to password-protect the AVG AntiVirus client on end user devices to prevent unauthorized modification or removal of the client. For more information, see [Configure Password Protection Settings](#).

You can now specify legitimate files, folders, and websites that you do not want scanned by AVG AntiVirus, by creating exception settings. For more information, see [Configure Exception Settings](#).

## What's New in Managed Workplace 9.1 MR2

Managed Workplace 9.1 Maintenance Release 1 (MR 1) contains over 20 customer-driven fixes to improve performance and your overall Managed Workplace experience. To view or search the fixed issues, visit the [AVG Partner Portal](#) and select 9.1.3 from the Version list.

## What's New in Managed Workplace 9.1 MR1

Managed Workplace 9.1 Maintenance Release 1 (MR1) contains over 30 customer-driven fixes to improve performance and your overall Managed Workplace experience. To view or search the fixed issues, visit the [AVG Partner Portal](#) and select 9.1.2 from the Version list.

## What's New in Managed Workplace 9.1

### New Look and Feel

Managed Workplace has been redesigned for a completely new look and feel. Although the physical layout and workflows remain the same, the Service

---

Center interface has been updated for a fresher, more intuitive user experience.

The Site Management page is now accessed through the new Sites menu in the left navigation pane, which you can also use to create a new site, and view Windows, SNMP, and Mobile inventory.

### **AVG Business SSO (Secure Sign On)**

New in Managed Workplace 9.1 is AVG Business SSO, a stand-alone application that allows secure sign on into thousands of popular SaaS and mobile applications, including Managed Workplace. With Business SSO, users can log in using their Active Directory account to access the SSO User Portal, where they can then launch their most frequently used applications without having to re-enter user names and passwords. With AVG Business SSO, you can:

- Use Active Directory to easily add users to Business SSO;
- Easily manage onboarding and offboarding of your employees by simply revoking Active Directory access, without having to go through several different consoles;
- Use multifactor authentication for an added layer of security. With multifactor authentication, you can send a passcode to users that they must enter to access Business SSO;
- Additionally, you can resell Business SSO IDaaS (Identity as a Service) licenses to your customers, allowing you to provide a more robust managed service offering.

Now, you can log in to Managed Workplace directly from the Business SSO User Portal, or you can click the AVG Business SSO logo on the Managed Workplace log in page to access Service Center without entering credentials. For more information, see [Logging In and Out](#).

As the SSO administrator, there are some initial configuration steps you must perform to set up the SSO integration with Managed Workplace. For more information on setting up the SSO integration, see [Configuring Secure Sign On](#).

### **Simplified Deployment**

Creating sites and deploying Onsite Manager and Device Manager is now easier than ever with the new simplified deployment process in Managed Workplace 9.1. An intuitive new user interface guides you through the process of creating a site and choosing a deployment method. If this is your first time logging in to Managed Workplace, the Create Site page appears automatically to help you get started.

Now you can deploy Onsite Manager non intrusively to a site, without the need to make any GPO changes beforehand. Within 30 minutes of deploying

---

Onsite Manager you will start receiving information in Service Center, allowing you to start understanding the site environment faster than ever before. There is no need to troubleshoot WMI, as the Windows Prep utility runs automatically to configure Windows devices when you deploy Onsite Manager.

For more information, see [Creating a Site in Service Center](#).

### **Remote Control Improvements**

Managed Workplace now provides tighter integration with TeamViewer, LogMeIn Pro, and ScreenConnect, through an optional custom third party integration that you configure in System Settings. By providing system-wide access credentials, you can experience a faster, more seamless integration between Managed Workplace and your remote control application of choice. For more information, see [Configuring a Custom Third Party Integration](#).

Additionally, you can now choose to install the UltraVNC agent automatically if it is not installed on all devices at a site. You can set global UltraVNC settings, including the application path and credentials. Optionally, you can choose to automatically uninstall the UltraVNC agent from the device after the remote session ends. For more information, see [Configuring Ultra VNC Access](#).

### **Alerting Improvements**

Several improvements have been made to alerting in Managed Workplace 9.1 to allow for faster remediation action from alert emails, and more precise Windows Event alerting:

- Alert emails now include links to common device management screens in Service Center to allow you to take immediate remediation action. For Windows Events alerts, the alert email contains a link to the device's Windows Event page in Service Center. Alert emails also contain links to the Remote Control page, the Remote Tools page, and the Run Automation page in Service Center. For example, you receive an alert email that a server is low on disk. You can click the Run Automation link in the email to run an automated script against the device to clean up temporary files.
- Windows Event alert rule configuration has been enhanced to allow you to define the number of Windows Events that must occur within a specified period of time for the alert to trigger. Previously, alerts would trigger on the first occurrence of the Windows Event. This new functionality prevents unnecessary alerts if you do not want to be notified on the first occurrence. For example, for logon failure events, you can configure the alert to trigger if there are a large number of logon failures in a short period of time, which could indicate malicious activity on the customer's

---

network. For more information, see [To set the alert configuration for a Windows Events monitor](#).

### **PSA Service Desk Improvements**

Ticketing options for Salesforce, ConnectWise and Autotask service desk modules have been improved to synchronize tickets from Managed Workplace to the PSA by device-based tickets, site-based tickets, website-based tickets, and by synchronizing based on policy sets. For more information, see *Integration Guide: Service Desks* in the Partner portal.

### **Support for Multiple Languages**

Managed Workplace is now available in German.

## INTRODUCING MANAGED WORKPLACE

---

*This section provides detailed information about the following topics:*

- *Managed Workplace*
  - *Learning the Essentials*
-

---

## Managed Workplace

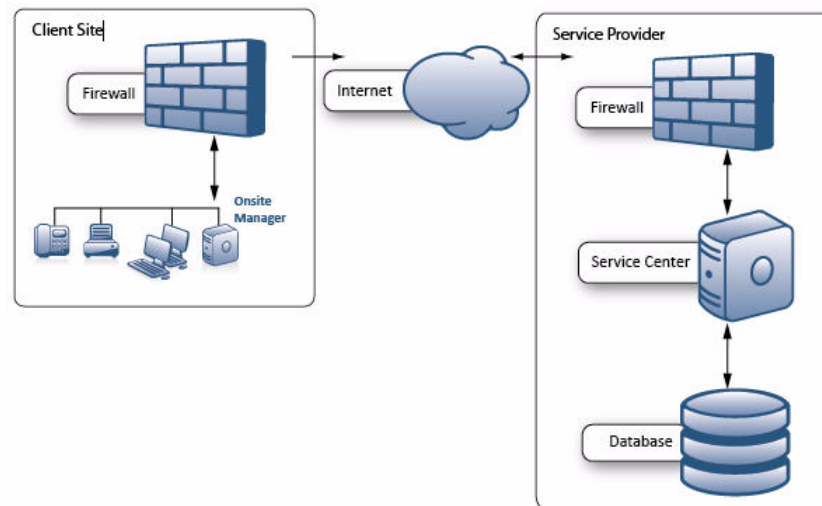
### About Managed Workplace

Managed Workplace provides remote monitoring and management of the entire IT environment of your SMB customers, including virtualized, cloud and software-as-a-service (SaaS) resources, through a single web-based dashboard.

**Service Center** Service Center is a powerful, web-based, centralized dashboard that allows you to view the asset health and performance data sent by Onsite Manager and Device Manager, drill down to details as required, perform rapid remote remediation, configure advanced services and produce a range of useful reports to manage clients' networks.

**Onsite Manager** Onsite Manager is installed on a shared server or dedicated server or appliance at your customer's site and used to probe network devices. Onsite Manager discovers all network devices, proactively discovers new devices introduced on the network, monitors the health, availability and performance of the IT assets and manages the environment. This includes patch management, remote control to virtually any device and automated tasks for routine maintenance and remediation of faults or errors. Onsite Manager also receives information sent to it, including SNMP traps, syslog messages, and so on.

Onsite Manager has both a database and an application and both reside on the same physical server. Onsite Manager monitors devices agentlessly, applications and websites and communicates directly with Service Center.



**Device Manager** Device Manager is a monitoring agent that is installed on a device and communicates directly with Service Center. Device Manager can be



---

installed on a Windows or a MAC OS X device that is out of reach of Onsite Manager, on a roaming laptop, in an environment that doesn't have a server or peer-to-peer network, at kiosks, and so on.

When setting up a site, you can automatically deploy Device Managers to laptops. Managed Workplace will detect the operating system and deploy a Device Manager for Windows or a Device Manager for OS X. If you are installing Device Manager onto a device, or sending an email link to the device user to download Device Manager, you must select either a Device Manager for Windows or a Device Manager for MAC OS X.

For more information, see [Adding Device Managers to a Site](#).

## Logging In and Out

When you access the Service Center web console, you are asked to log in. The method for logging in depends on whether you have set up Business SSO (Secure Sign On). For more information on Business SSO, see or [Configuring Secure Sign On](#).

### To log in using SSO

- 1 On the Service Center log in page, click **AVG Business SSO**.
- 2 If you are accessing a hosted environment, enter your VAR domain and click **Continue with SSO**.

### To log in with your Service Center credentials

- 1 Type your user name, password and VAR domain, if required.
- 2 Click **Log In**.

**Note:** The first time you log in to Service Center, an End User License Agreement appears. You must accept the license agreement before proceeding with the login.

### To log out of Service Center

- Click **Log Out** on the left sidebar.

## Changing Your Login Password

- 1 Click **Edit Profile** on the left sidebar.
- 2 Click **Reset Password**.
- 3 Type your current password, new password and confirm the new password.

- 
- 4 Click **Save**.
  - 5 Click **Save**.

## Learning the Essentials

### Using the Central Dashboard

The Central Dashboard provides status information about the alerts in your customer's environment. Alerts are displayed in two tables: one for service groups, and one for sites.

The service groups and sites with the highest number of alerts appear at the top of the list. Managed Workplace prioritizes alert delivery. Alerts may appear on the Central Dashboard up to a minute before supplementary information displays on the Device Information window.

#### To view the Central Dashboard

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the Central Dashboard icon.

**Tip:** You can also click the logo in the top left to quickly display the Central Dashboard.

#### See Also

[Viewing Status about a Site](#)

[Sorting Columns](#)

[Hiding and Showing the Left Sidebar](#)

#### Viewing Status about a Site

A status icon appears beside the site name.



Site is communicating successfully with Service Center.



Site has one or more Device Managers installed.



Site is experiencing issues communicating with Service Center.

---

### To display information about the last successful check-in time for the site

- Hover the mouse pointer over the status icon.

### Sorting Columns

You can sort on many columns in Managed Workplace. When you hover over a column header and the hand cursor appears, you can sort on that column.

By default, on the Central Dashboard, the alerts are sorted by Total Alerts.

### To sort information in ascending or descending order

- Click a column header.

### Hiding and Showing the Left Sidebar

The left sidebar contains the main navigation commands you need to work with Managed Workplace. If you need more space on the screen, you can hide it.

### To hide or show the left sidebar

- In the upper left corner, hover the cursor until the **Toggle Sidebar** tooltip appears, and click.

## Viewing Assets

One of the first things you can do after installing and configuring Managed Workplace is look at a summary of the assets that Onsite Manager discovered. You can view Windows assets, SNMP-enabled assets, and mobile devices.

**Note:** If the devices aren't showing as WMI- or SNMP-enabled, data may not be there. It also takes some time to appear depending on the number of devices. You can request assets for a specific device. This information will refresh within two minutes.

**Managed Windows Inventory** Provides a summary of assets collected for a given site from devices with a Microsoft Windows operating system installed. The summary contains both hardware and software-related information that Onsite Manager has discovered.

**Managed SNMP Inventory** Provides a summary of all SNMP-enabled devices for a given site, such as printers, routers and firewalls.

**Enrolled Mobile Device Inventory** Provides a summary of the enrolled mobile inventory at a site, including Android and iOS devices.

---

### See Also

[Viewing Windows Inventory](#)

[Viewing SNMP Inventory](#)

[Viewing Mobile Device Inventory](#)

## Service Plans

Managed Workplace includes a built-in framework that allows you to set up and maintain service plans for the managed services you provide. A service plan allows you to centrally plan and standardize your service offerings, and determines the level of involvement that you will have with your customer's technology.

Service plans are made up of services, which in turn are made up of policies. You can create monitoring, automation, AVG AntiVirus, patch, Support Assistant, and reporting policies.

Managed Workplace includes 3 pre-built service plans that you can use out of the box to get new client sites up and running. These service plans are designed to help you upsell your clients to more comprehensive service plans.

### See Also

[About Service Plans](#)

[Creating Services](#)

[About the Built-in Service Plans in Managed Workplace](#)

## Grouping

You can organize devices and applications in two ways:

- Service groups
- Site groups

**Service Groups** A service group is an organizational container for devices with similar characteristics, which may contain devices from multiple sites, and is used for asset management purposes. The advantage of service groups is the ease of administration when managing similar devices or applications.

**Site Groups** A site group is an organizational container for devices related to a single customer site. The advantage of site groups is the ease of identifying alerts occurring on a per-site basis.

---

### To hide service groups

- Click **Hide Groups**.

### To show service groups

- Click **Show Groups**.

### To hide site groups

- Click **Hide Sites**.

### To show site groups

- Click **Show Sites**.

### See Also

[Creating Service and Site Groups](#)

## Monitoring

Managing a site includes monitoring devices, applications, security, and other tasks. You're only as good as the available information that you can manage and act on. You need to know what's happening at your sites at all times.

Monitors sample a status and compare it to an alert rule. When the status matches the threshold defined in the rule, Managed Workplace generates an alert and the configured action takes place. For example, Managed Workplace can send an email, create a trouble ticket, escalate, self-heal, or run a script.

A monitoring policy is a collection of monitors and associated alert rules for a specific application, hardware device or operating system. Monitoring policies can include both automatic application rules, which define the criteria a device must match to be monitored, and manually applied devices and groups.

[Monitoring](#)

## Monitoring Network Services

The **Network Services** dashboard provides a summary of all monitored network services running on each device in a given site or service group.

---

### To view the Network Services dashboard

- In Service Center, click **Status > Network Services**.



The network service is running.



The network service is not running or is experiencing communications issues.



The network service is running but no data has been collected yet. This can also mean there is historical data about this having been monitored in the past even though it is no longer being monitored.

**Tip:** Hover your mouse over the status symbols to see a timestamp of the last sample. Also, if you see two chevrons (>>) in the upper right corner, then click to see more network services.

### To filter the list of network services in the Network Services dashboard

- 1 In Service Center, click **Status > Network Services**.
- 2 Select either the **Site** or **Service Group** button.
- 3 Do one of the following:
  - If you selected the **Site** button, select a site and site group from the list.
  - If you selected the **Service Group** button, select a service group from the list.
- 4 Use the drop-down lists at the top to filter as required.

### To view details about a network service

- 1 In Service Center, click **Status > Network Services**.
- 2 Click a device name.
- 3 Click **Network Services** on the right sidebar.

## Monitoring Cloud Services and Websites

The Cloud Services dashboard provides a summary of the health of cloud services and basic websites that you're monitoring. Along with monitoring basic websites, you can monitor cloud services that involve JavaScript

---

redirection or require persistent sessions. For example, you can monitor cloud services like Microsoft Office 365 or Google Docs.

Managed Workplace monitors the health of the cloud service and provides both the response time to access the service and the transaction duration, which shows how long it takes to complete the login and browsing to the actual page under scrutiny. A stable response time with a climbing transaction duration indicates that there may be bottleneck occurring on the web server.



The cloud service is responsive.



The cloud service is not responsive.

The Search Result column provides more information about the cloud service monitoring:

**Not Executed** A search string has not been defined in the monitor.

**Unhealthy** The search string defined in the monitor was not found. Click for more information.

**Healthy** The search string defined in the monitor was found.

For example, the Google site should have the words “maps” and “images” as part of its search links. If these words are not found, then the website has changed, which could be intentional or unintentional.

### To view the Cloud Services dashboard

- In Service Center, click **Status > Cloud Services**.

### To filter the list of sites in the Cloud Services dashboard

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Select a site from the list.

### To view details about a cloud service

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Click the name of the cloud service.

### To view the availability trend of a cloud service

On the **Availability** tab, you can click **Search Result** to get more information about the monitor, including when the sample was taken, whether it is up or

---

down, response time, and more. If there was an error, you will see the rendered HTML.

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Select the site associated with the cloud service from the **Site** list or select **All Sites** to display all cloud service monitors.
- 3 Click a monitor title under the **Cloud Service** column.
- 4 Click the **Availability** tab.
- 5 Click **Details** to view more information about the data point you want to look at.

**Note:** The errors you see are not Managed Workplace errors but standard error response codes for HTTP and HTTPS (such as the 403 forbidden error code).

### To view response times and transaction durations for a cloud service

The **Response Times** tab graphs information collected by Onsite Manager about how long it took to receive a response from a cloud service (Response Time) as well as how long it takes to log into the cloud service and complete a transaction (Transaction Duration).

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Select the site associated with the cloud service from the **Site** list or select **All Sites** to display all cloud service monitors.
- 3 Click a monitor title under the **Cloud Service** column.
- 4 Click the **Response Times** tab.
- 5 Do one of the following:
  - To specify how much information is to be displayed on the graphs, select a range from the list and click **Go** to refresh the graph.
  - To specify a custom interval, select **Other** from the list and then click a date link. Specify the interval and click **OK**.

**Tip:** To see the values for a point on the graph, hover the mouse pointer over the data line in the graph.

### To clear alerts for a cloud service monitor

The **Active Alerts** tab displays all current alerts triggered by the cloud service monitor.

- 1 In Service Center, click **Status > Cloud Services**.



- 
- 2 Select the site associated with the cloud service from the **Site** list or select **All Sites** to display all cloud service monitors.
  - 3 Click a monitor title under the **Cloud Service** column.
  - 4 Click the **Active Alerts** tab.
  - 5 Do one of the following:
    - To clear a single alert, select the check box for the alert and click **Clear**.
    - To clear all alerts, click **Clear All Alerts**.
  - 6 Type any relevant notes in the **Alert Resolution Notes** box.
  - 7 Click **OK**.

#### **To create a trouble ticket for a cloud service alert**

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Select the site associated with the website from the **Site** list or select **All Sites** to display all cloud service monitors.
- 3 Click a monitor title under the **Cloud Service** column.
- 4 Click the **Active Alerts** tab.
- 5 In the **Ticket** column, click **Create**.
- 6 Add any relevant information to the remaining boxes.
- 7 To generate an email for this trouble ticket, select the **Email Ticket to Assignee** check box.
- 8 To generate an OnForce work order for this trouble ticket, select the **Create OnForce Work Order** check box.
- 9 Click **Submit**.

#### **To view alert history for a website**

The **Alerts History** tab displays a listing of all alerts that have occurred for the cloud service.

- 1 In Service Center, click **Status > Cloud Services**.
- 2 Select the site associated with the cloud service from the **Site** list or select **All Sites** to display all cloud service monitors.
- 3 Click a monitor title under the **Cloud Services** column.
- 4 Click the **Alerts History** tab.

---

## See Also

[Adding a Monitor for Basic Websites or Cloud Services](#)

## Alerting

Managed Workplace has a robust notification engine to keep technicians informed when problems are identified in an environment. The alerting engine is closely tied to the monitoring engine. Based on the monitoring being performed, you can define search strings, thresholds, events or many other parameters and have alerts sent to any user or external individual.

Alert actions can take many forms, including trouble ticket creation, email messages, and can be scheduled via alert schedules to ensure that the appropriate people are being notified. Additionally, with automatic alert escalation capabilities you can ensure that no alerts are missed and that the appropriate action is taking place.

## See Also

[Alerting](#)

## Alerts Viewer

The **Alerts Viewer** is designed for network operation centers' wallboards and displays. It shows alerts, based on time received, in descending order. Audible cues can be configured to notify operators that new alerts have arrived. The Alerts Viewer is a reference tool, not an investigative tool, that provides read-only information.

You can display between 10 and 1,000 alerts in the **Alerts Viewer**.

Operators using the **Alerts Viewer** must belong to a role that grants them access to **Alerts Viewer**. See [Adding a Role to a User Account](#).

## Notes:

- Users that have access to the **Alerts Viewer** see all sites regardless of permissions.

- The **Alerts Viewer** uses Ajax technologies so that new alerts automatically stream into the window without needing to refresh.

**Alerts Viewer** Last Update: Mon Nov 29 15:13:02 EST 2010

13 Active Alerts      0 Site Alerts

Set Alert Tone Option: All sounds

Set Number Of Alerts Displayed: 50  Sorted By: Time Of Alert

Time Of Alert	Site Name	Device / Website	Category	Title
10:43 AM	TAM Industrial Industries	AKHALIFE-DT	Asset	Software Installed
8:18 AM	TAM Industrial Industries	TSHERWOOD-DT	Asset	Software Uninstalled
6:33 AM	TAM Industrial Industries	AKHALIFE-DT	OS	A Service or Driver Failed To Start Alert
11/26/2010 11:51:33 AM	TAM Industrial Industries	STORAGE	OS	Service Terminated Unexpectedly Alert
11/25/2010 7:46:08 PM	The Market on Legget	JZEEMAN-7DT	OS	Account Failed To Log On
11/25/2010 10:30:29 AM	TAM Industrial Industries	SSARAZIN-DT	OS	Program or Feature Incompatible With 64-bit Version of Windows
11/24/2010 11:42:40 AM	TAM Industrial Industries	PJ2K8EE	OS	Windows license validated
11/24/2010 11:02:23 AM	TAM Industrial Industries	PJ2K8EE	OS	Automatic Updates is now paused.
11/24/2010 10:26:46 AM	TAM Industrial Industries	PJ2K8EE	Device Down	Microsoft Windows 2008 Server is down
11/24/2010 8:42:41 AM	TAM Industrial Industries	PJ2K8EE	OS	Windows is unable to connect to the Automatic Updates
11/23/2010 9:45:30 AM	TAM Industrial Industries	LENOVO-M90P	OS	Account Locked Out
11/23/2010 5:57:09 AM	TAM Industrial Industries	KMACINNES-DT	OS	Unable to renew IP Address Alert
11/22/2010 1:09:20 PM	TAM Industrial Industries	TSHERWOOD-DT	OS	Unable to renew IP Address Alert

### To view a summary list of alerts

- In Service Center, click **Status > Alerts Viewer**.

### To view the Alerts Viewer window in full screen view

- Press **F11**.  
Press **F11** again to return it to normal view.

### To rename the Alerts Viewer window

- 1 Click the **Alerts Viewer** banner at the top of the window.
- 2 Type a new name.  
You can format the name using HTML.
- 3 Click **OK**.

### To set the sounds for different alerts in the Alerts Viewer window

**Note:** Replacing the alert sounds is an option for self-hosted environments only.

- From the **Set Alert Tone Option** list, select one of the options.  
**No sound** No sound is played for any alert.

---

**All sounds** All sounds are played for all alerts.

**Site not communicating** A sound is played only when a site is not communicating.

**Device down** A sound is played only when a device is down.

**Website down** A sound is played only when a website is down.

**Tip:** To customize the sounds, overwrite the .mp3 files with those of your choosing. The .mp3 files are located on the device where Service Center is installed. By default, the **Alerts Viewer** sounds are located in C:\Program Files (x86)\Level Platforms\SC\AlertsViewer. Replace any of the following files with a new sound file using these file names:

- alerttone\_devisedown.mp3
- alerttone\_general.mp3
- alerttone\_sitedown.mp3
- alerttone\_websitedown.mp3

### **To set the number of alerts you want displayed in the Alerts Viewer window**

- 1 In the **Set Number of Alerts Displayed** box, type a number.
- 2 Click **Set Count**.

### **To sort the alerts in the Alerts Viewer window in ascending or descending order**

- Click a column header.

### **To go back to the default sort order in the Alerts Viewer window**

- Click **Prioritize Alerts**.

## **Alerts**

The **Alerts** page enables you to view all active alerts for all sites, groups, alert categories, and devices at once. Alerts also appear on the Central Dashboard and the **Alerts Viewer**. You can also view alerts for a device on the **Device Overview** page. See [Viewing Summary Details about a Device](#).


The **Alerts** page refreshes on a default 5 minute interval. To customize the auto-refresh, see [Setting Refresh Options for the Central Dashboard and Alert Lists](#).

- In Service Center, click **Status > Alerts**.

---

**Tip:** To see details about an alert, click the triangle.

#### **To filter the list of alerts**

- 1 In Service Center, click **Status > Alerts**.
- 2 To filter the list to display the alerts you want to see, click the **Advanced Filtering** icon .
- 3 Use the drop-down lists at the top to filter as required.
- 4 Click **Filter**.

#### **To view details about a device with an active alert**

- 1 In Service Center, click **Status > Alerts**.
- 2 Click a device name.

For information about what you can do on the **Device Overview** page, see [Viewing Summary Details about a Device](#).

#### **To view the active and cleared alerts for a device with an active alert**

- 1 In Service Center, click **Status > Alerts**.
- 2 Click a device name.
- 3 Click **Device Alerts** on the right sidebar.
- 4 Do one of the following:
  - To view active alerts on the device, click the **Active** button. This view opens by default.
  - To view a list a of cleared alerts for the device, click the **Cleared** button.

#### **To view the Alert Configuration details**

- Click the name of the alert configuration.

#### **To view the associated trouble ticket for the alert**

- 1 In Service Center, click **Status > Alerts**.
- 2 Click the ticket ID number.

#### **See Also**

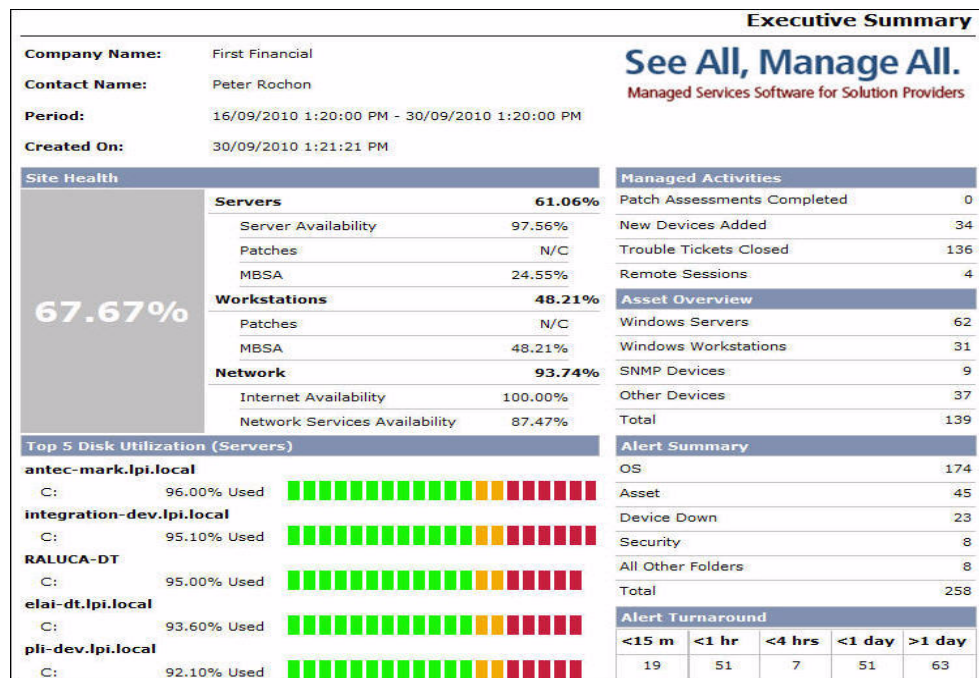
[Alerting](#)

## Reporting

Managed Workplace leverages the power of SQL Server Reporting Services to offer a comprehensive set of customizable reports that enable the following:

- Business management can identify customer opportunities and productivity concerns.
- Technicians can quickly analyze detailed device information to drive high performance.
- Sales staff can identify sales opportunities for improved customer productivity.
- End customers can have tangible proof to appreciate the value of your services.

There are two types of reports: on demand and scheduled reports. You can brand reports and schedule them for email delivery and select from multiple output formats including PDF, CSV, Excel, XML, TIFF, HTML and Word.



See Also

[Reporting](#)

---

## Viewing Managed Workplace Contract Information




### Viewing Your Managed Workplace Account Summary

The **Account Summary** page provides an overall view of your Managed Workplace billing status, allowing you to view what you are entitled to versus your actual usage.

Managed Workplace license models are device-based, in which you purchase the number of devices that you are entitled to manage. Devices are categorized as either servers or other devices, which includes desktops, mobile devices, virtual machines, printers, etc. You can use the Account Summary page to quickly see if you are approaching your contract limit in terms of how many devices you are still entitled to manage, how many you are currently managing, and also the number of seats of AVG services you have purchased and are currently using. AVG services include CloudCare AntiVirus, CloudCare Online Backup, and CloudCare Content Filtering.

The Account Summary page also indicates if Managed Workplace or a CloudCare service is a trial version, and displays the trial expiry dates to help you transition to full versions in a timely manner.

The following symbols indicate the status of your entitlement for each service:

-  The service usage is within the agreed contract limits.
-  The service usage is over the agreed contract limits.
-  The service is in a trial period.

To update your contract, or upgrade a trial version to a full version, contact your AVG sales representative.

#### To view contract usage and entitlement

- 1 In Service Center, click **Configuration > Account Summary**.
- 2 In the **Billing Details** section, view your contract renewal date.
- 3 In the **Entitlement** section, view your usage of the following services:
  - Managed Workplace** Displays number of devices in use and number of devices purchased, for both servers and other devices. Also displays your Service Center license key.

---

**Cloudcare AntiVirus** Displays number of seats in use and number of seats purchased.

**CloudCare Content Filtering** Displays number of seats in use and number of seats purchased.

**CloudCare Online Backup** Displays number of seats in use and number of seats purchased.

**Note:** If you have multiple contracts, some of which are the legacy site based model, the **Account Summary** page might show that your usage is over your entitlement for Managed Workplace. This imbalance will be corrected when you update to the new device-based licensing model.



## WORKING WITH SERVICE PLANS

---

*This section provides detailed information about the following topics:*

- *What is a Service Plan?*
  - *Working with Policies and Services*
  - *About the Built-in Service Plans in Managed Workplace*
  - *Creating Service Plans*
  - *Applying Service Plans to Existing Sites*
  - *Applying Service Plans to Site Groups*
  - *Setting Up Execution Schedules*
  - *Setting Up Maintenance Schedules*
  - *Viewing, Modifying, and Organizing Service Plans*
  - *Viewing Service Plan Activity on the Services Dashboard*
-

---

## What is a Service Plan?

### About Service Plans

Managed Workplace includes a built-in framework that allows you to set up and maintain service plans for the managed services you provide. A service plan allows you to centrally plan and standardize your service offerings, and determines the level of involvement that you will have with your customer's technology. So what is a service plan?

In short, a service plan is the group of *services* that you have agreed to provide to your customer. It can include any of the following:

- basic support, including Support Assistant and remote control capabilities.
- baseline or advanced monitoring and alerting.
- security services, such as patch management, AVG AntiVirus, and backup and disaster recovery.
- ongoing IT maintenance through the use of automated scripts.
- reporting on work completed.

### What You Can Do

You can:

- apply the pre-built service plans in Managed Workplace to new sites, and replace your existing monitoring configuration (if you upgraded to Managed Workplace 10.0 from a previous version) with service plans.
- modify the pre-built service plans by renaming them and adding or removing services.
- create your own service plans.
- monitor service plan activity, including active alerts, in the Services Dashboard.
- create executions to determine when patching, automated tasks, and AVG AntiVirus scans will occur at your customer sites.

The built-in service plans in Managed Workplace are designed to provide your customers with increasing levels of service, from the reactive service plan, which includes support and remote control services, to the fixed fee service plan, which provides complete monitoring and security services to your customer. For more about the built-in service plans, see [About the Built-in Service Plans in Managed Workplace](#).

You can also create your own service plans, or choose not to use them entirely.

---

## Working with Policies and Services

In Managed Workplace, service plans are made up of a collection of *services*, which are in turn made up of a collection of *policies*. Service plans and services are simply containers for policies, which include all of the settings and application rules for the services you want to provide. You can create a number of services containing the policies you require, and then group those services into a service plan.

### Understanding Policies and Services

Services and policies can be defined as:

**Policy** A collection of settings and automatic application rules that perform an action, such as baseline monitoring for Windows workstations, or critical and security patching for servers. There are six policy types: monitoring, automation, patching, reporting, Support Assistant, and AVG AntiVirus. Managed Workplace includes default policies for each policy type.

**Service** A collection of policies that together provide a specific service for your customer. For example, you may have a *Windows Server* service that provides patch management, monitoring, reporting, and maintenance tasks for Windows Servers.

If you choose to create a service plan, or modify an existing one, you should first understand each policy type in Managed Workplace. The following table lists the six types of policies available, with a description and example of each.

Policy Type	Description	Example
Automation	A script or script package that runs an automated task.	The <i>Microsoft Exchange Server Maintenance</i> policy reports on server database stats and health, determines if any messages are stuck queueing, and provides a warning if an SSL is due to expire or has expired.

---

Policy Type	Description	Example
AVG AntiVirus	A group of settings that determine which aspects of AVG AntiVirus are enabled.	The <i>Server AV Policy</i> prevents automatic updates and reboots on servers, and includes automatic application rules to deploy the policy to both member and standalone servers.
Monitoring	A collection of monitors and associated alert rules for a specific application, operating system, or hardware device.	The <i>Microsoft Windows Servers (Enhanced)</i> policy provides core Windows server monitoring on Windows Update, service failures, disk failures, file system failures, network failures, and event log issues.
Patching	A group of patch management settings, including detection frequency, automatic update options, and the approval groups to which the patching policy will be assigned.	The <i>Microsoft Windows Server Patching</i> policy downloads and installs all Windows Server critical and security patches.
Reporting	A collection of reports (both default and custom), the schedule on which the reports will run, and email and formatting options.	The <i>Monthly Report</i> policy includes a list of common reports, such as Executive Summary and Work Completed Summary, as well as a report execution schedule and recipient information.
Support Assistant	A collection of Support Assistant customizations, including the context menu items, branded messages, notification area icons.	The <i>Microsoft Windows Workstation Tray Profile</i> policy deploys and configures the Support Assistant Tray Profile to each Windows desktop and laptop.

---

---

**Note:** Previous to Managed Workplace 10.0, *monitoring policies* were called *policy modules*.

## Getting Started with Policies

You can browse the policies available in Managed Workplace to gain an understanding as to what is currently available. You can modify these policies by copying them and modifying the copy, and you can create your own policies to reflect your unique service offerings.

Click the following links for more help on creating each policy type:

- For more information about viewing, modifying, and creating automation policies, go to **Configuration > Policies > Automation**, or see [Creating Automation Policies](#).
- For more information about viewing, modifying, and creating AVG AntiVirus policies, go to **Configuration > Policies > AVG AntiVirus**, or see [Setting Up AntiVirus Policies](#).
- For more information about viewing, modifying, and creating monitoring policies, go to **Configuration > Policies > Monitoring**, or see [About Monitoring Policies](#).
- For more information about viewing, modifying, and creating patching policies, go to **Configuration > Policies > Patching**, or see [Setting Up Patch Management in Managed Workplace](#).
- For more information about reporting policies, go to **Configuration > Policies > Reporting**, or see [Creating Report Policies](#).
- For more information about viewing, modifying, and creating Support Assistant policies, go to **Configuration > Policies > Support Assistant**, or see [Creating a Support Assistant Policy](#).

## Understanding Services

When you create services, you provide a name and description, and then add policies. You can add multiple policy types to a service; for example, you can add a monitoring policy that provides baseline monitoring and an associated report policy that reports on the alerts that are generated by the monitoring policy.

You can also copy a service. Copied services have the same name as the original, with the word “Copy” appended.

---

## Best Practices for Creating Services

The easiest way to use services is to add them to a service plan. This way, you are standardizing how the service is used across your sites. For example, you can apply the service plan to a site, if you want to use a site-based delivery model. You could also use a group-based delivery model, in which you apply the service plan to a group. For more information about service delivery models, see [Determining a Service Delivery Model](#).

**Avoid relying on specific inclusions or exclusions as a maintenance strategy** Although you can force the inclusion and exclusion of specific sites, groups, and devices in a service, relying too heavily on this method can result in a complicated set-up that is difficult to maintain. As a best practice, you should

- rely on your policies to determine the *type* of devices to which the service will apply, as policies include automatic inclusion rules to determine how the services are applied
- rely on service plans to determine to which sites or groups the service will be applied.

Relying on policies and service plans to determine how services are applied allows you to centrally update your service offerings, by either updating the automatic inclusion rules in the policies, or by applying or removing the entire service plan as needed.

**Ensure that you add Report policies to the same service as their associated policies** For example, if you are providing AVG AntiVirus to a customer, and by extension you are offering the AVG AntiVirus Summary report, you should create a service that includes both the AV policy and the Report policy with the AVG AntiVirus Summary report. Do not put these policies in separate services, as you could end up with an empty AVG AntiVirus Summary report if you happen to remove the service with the AV policy but you do not remove the service with the Report policy.

## Creating Services

When you create a service, you provide a name and description, and add policies.

Optionally, you can select specific sites, groups, and devices to include in the service, or to exclude from the service. Although this practice is not recommended, it may be necessary for fringe cases. The specific inclusions or exclusions that you configure for a service override your service delivery model. For example, if you include the service in a service plan, and that service plan is not applied to a site, but you've included that site at the service level, then the service will be applied to the site.

---

### To create a service

- 1 In Service Center, click **Configuration > Services**.
- 2 Click **New**.
- 3 Provide a name and description for the service.  
Now you will add policies to the service.
- 4 In the **Policies** area, click **Add**.
- 5 From the list, select the type of policy you want to add, and then click **Add**.  
A list of policies appears, filtered by the type of policy you selected in the previous step.
- 6 Select the check box beside each policy you want to add to the service.
- 7 Repeat steps 5 and 6 for each policy type that you want to add until you have finished adding policies to the service.
- 8 Click **OK**.

**Tip:** You can also create a service from the **Configuration > Service Plans** page. Creating services this way is helpful when you are building service plans and you see a need for a new service, and you do not want to leave the **Service Plans** page.

### To include or specific sites, groups, or devices in a service

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 If the Advanced Configuration section is not expanded, click **Show Advanced Configuration**.
- 4 In the **Inclusions** area, do one of the following:
  - To include a site, in the **Sites** area, click **Add**. Select the check box beside each site you want to include, and click **Save**.
  - To include a group, in the **Groups** area, click **Add**. From the **Group Type** list, select **Service Groups**, **Site Groups**, or **All**. Select the check box beside each group you want to include, and click **Save**.
  - To include a device, in the **Devices** area, click **Add**. Use the filters to narrow down your search, and click **Filter**. Select the check box beside each device you want to include, and click **OK**.
- 5 Click **Save**.

---

### To exclude specific sites, groups, or devices from a service

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 If the Advanced Configuration section is not expanded, click **Show Advanced Configuration**.
- 4 In the **Exclusions** area, do one of the following:
  - To exclude a site, in the **Sites** area, click **Add**. Select the check box beside each site you want to exclude, and click **Save**.
  - To exclude a group, in the **Groups** area, click **Add**. From the **Group Type** list, select **Service Groups**, **Site Groups**, or **All**. Select the check box beside each group you want to exclude, and click **OK**.
  - To exclude a device, in the **Devices** area, click **Add**. Use the filters to narrow down your search, and click **Filter**. Select the check box beside each device you want to exclude, and click **OK**.
- 5 Click **Save**.

## Adding Service Modules to Services

In addition to adding policies to services, you can also add service modules to a service. AVG has partnered with many third-party applications, including VMware, Office 365, and Hyper-V to create service modules that allow you to manage these applications from within Service Center.

When service modules are added to a service, and the service is applied either using a service plan, or by applying it directly to a site, the service module is also applied. Note that you must have installed the service module by going to **Update Center > Components**, clicking **Get More**, and then selecting **Service Modules** from the **Type** list.

For more information on service modules, see [About Service Modules](#).

**Note:** The Fixed Fee service plan includes the Infracore service module to provide backup and disaster recovery services to your customers. You do not need to add this service module to any policies, however you must purchase Infracore licenses to activate this capability. See your AVG representative for details.

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 In the **Policies** area, click **Add**.
- 4 From the list, select **Service Modules > Add**.



- 
- 5 All of the installed service modules are listed. Select the check box beside the service module you want to add, and then click **OK**.

## Copying Services

When you copy a service, the copied service is given the same name as the original, with **-Copy** appended to the name. The policy modules in the service, as well as specific inclusions and exclusions are not copied.

- 1 In Service Center, click **Configuration > Services**.
- 2 Select the check box beside the service you want to copy.
- 3 Click **Copy**.
- 4 The copied service appears in the list of services. Click the copied service to provide a new name.

**Tip:** You can also copy a service from the **Configuration > Service Plans** page. Copying services from this page is helpful when you are building service plans and you need to copy a service, and you do not want to leave the **Service Plans** page.

## Modifying Services

You can modify an existing service by changing the name or description, and adding and removing policies.

### To change the name or description of a service

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 Type a new name or description.
- 4 Click **Save**.

### To add policies to a service

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 In the **Policies** area, click **Add**.
- 4 From the list, select the type of policy you want to add, and then click **Add**.  
A list of policies appears, filtered by the type of policy you selected in the previous step.
- 5 Select the check box beside each policy you want to add to the service.

- 
- 6 Repeat steps 5 and 6 for each policy type that you want to add until you have finished adding policies to the service.
  - 7 Click **OK**.

#### **To remove policies from a service**

- 1 In Service Center, click **Configuration > Services**.
- 2 Click the name of a service.
- 3 Select the check box beside each policy you want to remove.
- 4 Click **Remove**.

## **Run the Policy Application Rules in a Service**

If you add or remove policies from a service, you can apply those changes immediately to all devices currently monitored by the service. For instance, if you have a service currently applied to several sites using a service plan, and you add a policy to the service, you can apply the policy in the updated service immediately. The automatic inclusion rules in the newly added policy will be run and all devices that meet the inclusion criteria are added.

- 1 In Service Center, click **Configuration > Services**.
- 2 Select the check box beside a service you want to synchronize.
- 3 Click **Run Rules**.

## **About the Built-in Service Plans in Managed Workplace**

Managed Workplace includes four service plans that have been carefully created by AVG experts to provide out-of-the-box monitoring for your customers, with minimal configuration required. Using these service plans, you can determine whether a customer requires simple monitoring and troubleshooting, or monitoring with ongoing maintenance and preventative actions, and then select and deploy the appropriate service plan to meet their needs.

#### **Notes:**

- *Reactive, Proactive, and Fixed Fee* are simply suggested service plan names, and can be modified to better reflect your service structure as needed.
- The MWNOC service plan has been designed for use by the AVG NOC team.

---

The **Reactive Service Plan** is a baseline solution that provides monitoring, Support Assistant deployment, and reporting. The **Proactive Service Plan** offers more enhanced monitoring, device maintenance, patching, and reporting. The **Fixed Fee Service Plan** is a complete solution that also provides AVG AntiVirus and backup and disaster recovery.

## Reactive Service Plan

The objective of this entry-level service plan is to monitor and report on every device within the customer's network that has an IP address, and on applications as needed. The monitoring policies in this service plan are configured to alert when a device, application, or service fails. Note that this service plan does not reduce or prevent network failure; it's designed to reduce technical troubleshooting, diagnoses and remediation to get the customer back up and running.

### Reactive Service Plan Positioning

The **Reactive Service Plan** is typically positioned as a starter or entry-level solution that provides your customers with increased network up-time, staff productivity, and cost savings. Because you are reacting to issues, this service plan is typically sold with an expiring monthly block of troubleshooting time.

### Target Customer Profile

This service plan is tailored for customers whose network is not critical to the way they deliver their business services. You can also use the **Reactive Service Plan** to gain customers who are hesitant to purchase MSP services, with the possibility of upselling to a more comprehensive service plan at a later time.

## Proactive Service Plan

This mid-level service plan is designed to proactively monitor and report on every device in the customer's network that has an IP address, and applications as needed, with an increased focus on reducing downtime. Monitoring in this service plan is threshold-based, which means that monitoring policies are configured to alert you when devices, applications, and services are *trending* toward failure.

### Proactive Service Plan Positioning

The **Proactive Service Plan** is typically positioned to combine d routine maintenance with proactive network monitoring. The result for your customer is a reduction of costly downtime, increased network up-time, staff productivity and cost savings.

---

### Target Customer Profile

The Proactive Service Plan is designed for customers whose network is critical in terms of how they deliver their business services.

## Fixed Fee Service Plan

This elite service plan is designed to replace the requirement for an in-house IT manager. The **Fixed Fee Service Plan** covers all elements of a customer's network environment, and is designed to meet all of the customer's business needs as it relates to technology. The monitoring policies in this service plan are configured on defined thresholds to alert you in advance of failure on devices, applications, and services.

### Fixed Fee Service Plan Positioning

The **Fixed Fee Service Plan** is a top-tier, fully managed services solution that is based on a fixed monthly price. This service plan aims to reduce negative business impact from IT failure, and deals with any remaining IT failures as a top priority.

### Target Customer Profile

The **Fixed Fee Service Plan** is designed for customers whose network is absolutely critical in how they operate their business. This customer typically has a strong understanding of the relationship between their network and the revenue they generate.

## Comparing the Built-In Service Plans

The following table provides a quick reference for comparing the services included in each of the built-in service plans:

Service	Reactive	Proactive	Fixed Fee
Baseline Monitoring	✓		
Enhanced Monitoring		✓	✓
Server Maintenance		✓	✓
Server Diagnostics		✓	✓
Desktop Maintenance		✓	✓

---

Service	Reactive	Proactive	Fixed Fee
AVG AntiVirus			✓*
Microsoft Windows Patch Management		✓	✓
Support Assistant	✓	✓	✓
Reporting	✓	✓	✓
Backup and Disaster Recovery			✓*

---

\* these services require activation and additional configuration. See [Adding Service Modules to Services](#).

## Creating Service Plans

You can modify the built-in service plans in Managed Workplace to reflect your service offerings, and you can create a custom service plan for the unique services you provide.

When creating a service plan, you provide it with a name and description, and then add the services to complete the service plan. For this reason, you should first create the services that you want to include. For information on creating services, see [Creating Services](#).

### Creating a Service Plan

When you create a service plan, you provide it with a name and description.

**Tip:** The description you provide should describe the services and policies contained therein, as well as whether it is a baseline or a complete solution. This kind of information is helpful when viewing the service plans by clicking **Configuration > Service Plans**, and then clicking the **Panel View** icon.

After creating the name and description, you can add services to the service plan.





#### To create a service plan

- 1 Click **Configuration > Service Plans**.
- 2 Click **New Service Plan**.

- 
- 3 Provide a service plan name and description.
  - 4 Optionally, select a color for the service plan icon by clicking in the **Icon Color** box and then selecting a color from the palette. This icon will appear in the **Services Dashboard** and will be used to differentiate this service plan from other service plans you are using.
  - 5 Click **OK**.
  - 6 Click the **Comparison View** icon, if you are not already in this view.

A new column for the service plan has been added to the table, with all existing services turned off by default. Now you will add services to the service plan. Note that this can only be done if you are in the **Comparison View**.

### To add services to a service plan

- 1 To add services, do one of the following:
  - To add an existing service, click the grey circle  in the row for the service you want to add. The grey circle changes to a checkmark  to indicate that the service has been added. Click **Apply**.
  - To create a service to add, click **New Service**. Provide a name and description, and then add the policies you want included in the service. Click **Save** when you are done. The new service will be added to the list of available services. Click the grey circle  in the row for the service you just created. The grey circle changes to a checkmark  to indicate that the service has been added. Click **Apply**.

## Determining a Service Delivery Model

### Understanding Site versus Group Service Delivery Model

Service plans in Managed Workplace have been set up to provide you with complete granularity over how you want to apply policies and services. For example, you can bypass service plans and apply a single service directly to a site, and you can apply a policy directly to a group. However, Managed Workplace 10.0 has been designed with two service delivery models in mind: site-based delivery and group-based delivery.

**Site-Based Delivery** Service plans are applied to an entire site. This service delivery method requires the least amount of configuration and maintenance, and is best used when you are providing very similar services to multiple customers.

---

**Group-Based Delivery** Service plans are applied to site groups. Use this delivery method if you have structured your service offerings on a more granular level, i.e. you categorize your service offerings by device type, such as various services for servers, and various services for workstations. You can create shared site groups, which are site groups managed with a single group definition, to easily create and manage groups across your customer sites.

## Applying Service Plans to Existing Sites

Once a service plan has been created, you can apply it to existing sites. The service plan can also be applied to new sites during site creation. For more information, see [Creating a Site in Service Center](#).

## Viewing the Service Plan Application for a Site

The **Site** page includes information on how service plans have been applied to the site.

The **Service Plan Application** area indicates whether a service plan has been applied to the entire site, to groups at the site, or whether there is no service plan applied.

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.
- 3 In the **Service Plan Application** area, view the service plan application details:
  - If one service plan has been applied to the entire site, the site name is displayed and the service plan is listed below it.
  - If service plans have been assigned to shared site groups for this site, each shared site group is listed indicating which service plan is applied to it, and the number of devices under the plan
  - If no service plans have been applied to this site, then **No service plan** is displayed.

## Applying a Service Plan to a Site

When you select a new service plan delivery model for a site, note that the current service plan configuration will be lost for the site and cannot be restored. For example, if you have a site with service plans applied to shared site groups at the site, and you choose to instead apply a single service plan to this site, any services in the current service plan model that are not in the new service plan will cease to function for the site.

- 
- 1 In Service Center, click **Dashboards**.
  - 2 If the Services Dashboard is your default dashboard, click the Central Dashboard icon.
  - 3 Click the name of a site.
  - 4 In the **Service Plan Application** area, click the gear icon.
  - 5 In the **Manage Service Plan Application** area, click the gear icon to convert the site to a different service plan delivery model.
  - 6 Select the **Apply a single Service Plan to all devices in this Site** button. Then, click the pencil icon to activate a list of all available service plans. Select a service plan from the list and click **OK**.
  - 7 Click **Convert**.
  - 8 A pop-up appears warning you that the current service plan configuration will be lost and cannot be restored. Click **Remove Configuration and Convert**.

## Applying Service Plans to Site Groups

After creating a service plan, you can apply it to site groups.

If you plan on using a group-based service delivery model for your service plans, you can create a *shared site groups*, which rely on a common site group definition that automatically creates a site group at all new sites using the automatic inclusion rules you define. By allowing you to configure site group automatic inclusion rules in one central location, and then applying these rules across multiple sites, shared site groups allow you to standardize the creation

**Tip:** You create and manage shared site group definitions in Service Center, by going to **Configuration > Groups**, and clicking the **Configure Shared Site Groups** tab. For more information on creating and managing shared site groups, see [Creating Shared Site Groups](#).

## Applying Service Plans to a Site Group

As a best practice, it is recommended that if you choose to apply service plans using a group-based service delivery model, that you apply to site groups that have been created using a shared site group definition. However, if you have already created site groups for the site, you might find it easier to use your existing groups.

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.



- 
- 3 In the **Service Plan Application** area, click the gear icon.
  - 4 If site is not set up to use shared site groups by default, click the gear icon again, and select the **Apply Service Plans directly to groups** button. If the site is already set up to use shared site groups, skip this step.
  - 5 In the **Manage Service Plan Application** area, click the **Apply Service Plan to a new Group** link.
  - 6 From the **Choose an unassigned site group** list, select the shared site group to which you want to apply a service plan.
  - 7 In the **Service Plan Applications** area, from the list select the service plan you want to apply to this site group.  
**Tip:** The **Service Components** area provides a quick visual indication of the types of policies included in the selected service plan. For example, if the service plan contains a monitoring policy, the Monitoring icon is shaded black.
  - 8 Click **Save**.
  - 9 Repeat steps 5 to 8 to apply service plans to other groups, as needed.

## Setting Up Execution Schedules

An execution schedule determines when you want to run automated tasks, AVG AntiVirus scans, and patching at your customer sites. Execution schedules can help ensure that you do not interfere with your customer's business when performing these important maintenance and security actions.

Execution schedules can be applied at the site or group level. When you create an Automation, AV, or Patch policy, you can indicate that it automatically uses the execution schedule that you've applied for a site or group of devices.

For example, for ABC Medical, you may decide to run AV scans, patching, and Windows maintenance tasks on Fridays at 8pm. You can set up an execution schedule that defines these settings, and apply the execution schedule to that site. Then, when you set up your policies that will be used at that site, you can indicate that the policies use an execution schedule. When the policies are run at that site, whether through service plans, or by applying the policies directly to devices at the site, the policies will automatically use the execution schedule you've applied to that site. If you change the execution schedule for that site, either by modifying the existing one or applying a new execution schedule altogether, the policies will automatically begin using the new execution schedule.

Now let's say you create another site for another customer, XYZ Medical. This customer has asked that you run any patching, AV scans, and automated tasks

---

on Monday afternoons, as they are closed on Mondays. You can set up an execution schedule that runs on Mondays at 2pm. You can apply the very same policies to XYZ Medical that you did to ABC Medical, however the policies will run on the execution schedule you applied for this site.

If you do not want the policy to use an execution schedule, you can override the execution schedule entirely and set up a custom schedule for that policy.

**Note:** Execution schedules do not apply to reporting policies, which run on a schedule you define within the policy. For information on creating a schedule to deliver reports, see [Creating Report Policies](#).

## Understanding Execution Schedules

The following table provide an overview of what can be included in an execution schedule:

Policy Type	Settings
Automation	Determines when daily, weekly, and monthly automated tasks are run. See <a href="#">Setting the Automation Schedule</a> .
AVG AntiVirus	Determines when AV scans are performed, when and how often virus definitions are updated, and the program update schedule. See <a href="#">Setting the AVG AntiVirus Schedule</a> .
Patching	Determines frequency and recurrence of patch installations, and reboot behavior. See <a href="#">Setting the Patching Schedule</a> .

## Execution Schedule Best Practices

**Consider your service delivery model when adding sites or groups to an execution schedule** If you are using a site-based delivery model (i.e., you are applying service plans to entire sites), then you should also apply your execution schedules at the site level. Similarly, if you are using a group-based service delivery model, you should apply your execution schedules to groups. When you match up your execution schedules to your service delivery model, it becomes much easier to maintain your execution schedules and to keep track of which execution schedule is being used by the devices in a service plan.

---

**Create a default execution schedule that can be used by most sites or groups** When you create an execution schedule, you select one to use as a default. This is the execution schedule that is applied by default to new sites. For ease of maintenance, the default schedule should be set up so that it can be used by most sites or groups, to minimize the need to override the execution schedule or create a new execution schedule.

**Suppress alerts during your execution schedule** If you know that running the execution schedule will result in alerts that will not require corrective action, consider suppressing alerts during the execution period. You can suppress the kinds of alerts associated with the activities of the execution schedule, which will save you the time and effort of clearing the alerts later. For more information, see [Suppressing Alerts During an Execution Schedule](#).

## Creating an Execution Schedule

When you create an execution schedule, you provide it with a name and a description, and then you set the different schedules for **Automation**, **AV**, and **Patching**.

### To create an execution schedule

- 1 In Service Center, click **Configuration > Schedules > Execution**.
- 2 Click **New**.
- 3 In the **New Schedule** area, provide a schedule name and description.

Now you will set the **Automation**, **AV**, and **Patching** schedules for this execution schedule.

## Setting the Automation Schedule

When you set the Automation schedule, you indicate when the daily, weekly, and monthly automated tasks will occur. Then, when you create an Automation policy, you indicate whether the policy will use the daily, weekly, or monthly automation schedule in the applicable execution schedule.

For example, in the execution schedule, you set the daily automation schedule to occur every day at 3am. Then, when you go to **Configuration > Policies > Automation** to create an Automation policy, on the **Settings** tab, you can indicate that the automated task in the policy will run on the daily automated schedule.

### Setting the Daily Automation

Daily automation schedules can be set to run once a day, or by indicating the frequency, in hours, the schedule should run.

---

When you select a recurrence pattern that occurs more than once a day (i.e. every 2 hours) you can also indicate when the last run time will be. For example, you may want to run tasks every 2 hours starting at 1am, but have the last run time begin at 5am, to help ensure that the automated tasks have completed before the start of the work day.

- 1 In the **Automation Details** area, click the link for the daily automated schedule.  
By default, daily automated tasks are set to run once a day at 7am.
- 2 In the **Start Time** box, enter the time when the daily automation will begin running. You can also click the clock icon to select from a list of start times.
- 3 From the **Run Daily** list, select the frequency in which the automated task will run on a daily basis.
- 4 If you selected something other than **Once a day** from the **Run daily** list, select when the last run time will be for the day. In the **Last run time** box, enter the time when the last occurrence of the daily automation will begin. You can also click the clock icon to select from a list of last run times.
- 5 Click **Save**.

### Setting the Weekly Automation Schedule

Using a weekly automation schedule, you can indicate on which days of the week an automated task will run. You can have the schedule run more than once a week. For example, you can choose to have the schedule run twice a week, by indicating that it will run on Tuesdays and Fridays.

- 1 In the **Automation Schedules** area, click the link for the weekly automated schedule.
- 2 In the **Start Time** box, enter the time when the weekly automation will begin running. You can also click the clock icon to select from a list of start times.
- 3 Select the check box beside each day of the week that you want the weekly automation schedule to run.
- 4 Click **Save**.

### Setting the Monthly Automation Schedule

Monthly automation schedules allow you to determine a day of the month that the automated task will run, i.e. the first, 5th, or last day of the month. Or, you can select a day and week for the task to run, i.e. the second Tuesday of the month.

- 
- 1 In the **Automation Schedules** area, click the link for the monthly automated schedule.
  - 2 In the **Start Time** box, enter the time when the monthly automation will begin running. You can also click the clock icon to select from a list of start times.
  - 3 To select a day of the month when the automated task will run, in the **Run every month on** area, select the top button, and then select a day of the month from the list.
  - 4 To select a day and week for the task to run, in the **Run every month on** area, select the bottom button, and then select a week (first, second, third, etc) and day.
  - 5 Click **Save**.

## Setting the AVG AntiVirus Schedule

The AVG AntiVirus schedule determines when AntiVirus scans, virus definition updates, and program updates will occur.

### Setting the AVG AntiVirus Scan

The AV scan schedule determines when and how often AntiVirus scans are performed on a device.

For more information on AVG AntiVirus scan settings, see [Configure Scan Settings](#).

- 1 In the **AV Schedules** area, click the link for the AV scans schedule.
- 2 To run the AV scan every few hours, select the **Run every** button, and then enter the number of hours in the box, or use the arrows to increase or decrease the number displayed. You can enter from 1 to 24 hours.
- 3 To run the AV scan at a more defined schedule, select the **Run at specific times** button, and then do one of the following:
  - To run the AV scan every day, select **Every day** from the list, and then enter the time when the scan will begin in the corresponding box. You can also click the clock icon and select a time from the list.
  - To run the scan on one or more days of the week, select **Selected days** from the list, and then select the check box beside each day you want the scan to run. Enter the time when the scan will begin in the corresponding box. You can also click the clock icon and select a time from the list.
  - To run the scan on a specific day of the month, select **Every selected day in month** from the list. Enter the time when the scan will begin in

---

the corresponding box. You can also click the clock icon and select a time from the list. Then, in the **Day** box, enter the day of the month when the AV scan will run. Selecting 1 runs on the first day of the month, 2 on the second day, and so on.

- 4 To run the scan when the computer starts up, select the **Run on computer startup** button, and then specify a delay, in minutes, when the AV scan will start running after startup.
- 5 Click **Save**.

### Setting the AntiVirus Definition Update Schedule

The AntiVirus definition update schedule determines when and how often virus definitions are updated.

- 1 In the **AV Schedules** area, click the link for the AV definitions update schedule.
- 2 To update definitions every few hours, select the **Run every** button, and then enter the number of hours in the box, or use the arrows to increase or decrease the number displayed. You can enter from 1 to 24 hours.
- 3 To update definitions every day at a specific time, select the **Run at specific times** button. Enter a time in the box provided, or click the clock icon to select from a list of times.
- 4 Click **Save**.

### Setting the AntiVirus Program Update Schedule

- 1 In the **AV Schedules** area, click the link for the AV program update schedule.
- 2 To update programs every few hours, select the **Run every** button, and then enter the number of hours in the box, or use the arrows to increase or decrease the number displayed. You can enter from 1 to 24 hours.
- 3 To update programs at a more defined schedule, select the **Run at specific times** button, and then do one of the following:
  - To update programs every day, select **Every day** from the list, and then enter the time when the scan will begin in the corresponding box. You can also click the clock icon and select a time from the list.
  - To update programs on one or more days of the week, select **Selected days** from the list, and then select the check box beside each day you want the scan to run. Enter the time when the update will begin in the corresponding box. You can also click the clock icon and select a time from the list.

- 
- To update programs on a specific day of the month, select **Every selected day in month** from the list. Enter the time when the update will begin in the corresponding box. You can also click the clock icon and select a time from the list. Then, in the **Day** box, enter the day of the month when the update will run. Selecting 1 runs on the first day of the month, 2 on the second day, and so on.
- 4 To update programs when the computer starts up, select the **Run on computer startup** button, and then specify a delay, in minutes, when the update will start running after startup.
  - 5 Click **Save**.

## Setting the Patching Schedule

The Patching Schedule determines options such as patching frequency and recurrence, and reboot behavior.

- 1 In the **Patching Schedules** area, click the link for the patching schedule.
- 2 In the **Start Time** box, type a start time for when patching will begin. Alternatively, you can click the clock icon to select a time from the list.
- 3 In the **Recurrence Pattern** area, select whether you want patches to run daily, weekly, or monthly.
- 4 By default, devices will not reboot after patching. To control how devices are rebooted, in the **Reboot Options** area, select one of the following options:
  - To force a reboot, select the **Force a reboot when an update requires one** button. Use this option when you do not want to allow the device user to postpone the reboot. Devices will reboot regardless of whether a user is logged on or not.
  - If you do not want the device to automatically reboot when a user is logged on, select the **Consider logged on users** button, and then select **Do not reboot** to prevent the device from rebooting when a user is logged on, or select **Auto reboot after installation** to prompt the user that the device requires rebooting.

**Important:** Some Microsoft updates will cause a server to reboot if you choose the **Do not reboot** button. This behavior does not come from Managed Workplace, but is native to Windows. AVG recommends reading all details of a patch before applying it to a server.

- 5 If you selected the **Auto reboot after installation** option, set the following reboot prompt settings:

- 
- a In the **Prompt to reboot after** list, specify a time after which a prompt will appear on the device.
    - b In the **Repeat prompt to reboot every** list, specify in minutes how often to repeat the prompt.
  - 6 In the **Missed Installation Options** area, select the **wait X minutes after the next system startup to install** button and enter a value for X in minutes between 1 and 60, or select the **wait until next scheduled time to install** option to define how missed installations are handled.

## Suppressing Alerts During an Execution Schedule

When you know that the activities of an execution schedule will cause alerts that you won't need to take action on, you can use maintenance to suppress alerts, saving you the time and effort of clearing them later.

When maintenance is set to **Planned**, it indicates that downtime is expected during the time period. As a result, during Planned maintenance, the downtime of the affected devices, sites, and network services does not appear as downtime on reports.

Maintenance cannot be associated with tasks that recur more often than once a day or are triggered by computer startup.

The minimum duration is .5 hours. In the **Duration** box, any fraction of an hour less than .5 hours is rounded up to .5 hours. Over .5 hours, numbers are rounded to one decimal place.

**Note:** Maintenance does not suppress the following alerts:

- Cloud monitors
  - Service Center receive alert configuration
  - Onsite Manager processing alert configuration
- 1 In Service Center, click **Configuration > Schedules > Execution**.
  - 2 Click the name of an execution schedule.
  - 3 In the **Schedule** column, click the link to a task schedule.
  - 4 Select the **Apply Maintenance to Schedule** check box.
  - 5 In the **Alert Suppression** area, select the check boxes of the alerts to suppress.
  - 6 In the **Duration** box, type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
  - 7 Click **Save**.



---

## Adding Sites, Groups, or Devices to an Execution Schedule

You can add sites, groups, and devices to execution schedules. Devices can only have one execution schedule applied; if you add a device to an execution schedule that had another execution schedule applied, the newly added execution schedule will immediately replace the previous one.

For best practices on selecting whether to add an execution schedule to a site or a group, see [Execution Schedule Best Practices](#). It is not recommended that you apply an execution schedule to a device, as this can become difficult to keep track of and requires more overhead. However, it may be needed if you have one or two devices with very specific schedule requirements.

- 1 In Service Center, click **Configuration > Schedules > Execution**.
- 2 Click the name of an execution schedule.
- 3 If the advanced configuration is hidden, click **Show Advanced Configuration**.
- 4 To apply the execution schedule to sites, do the following:
  - a In the **Sites** area, click **Add**.
  - b Select the check box beside each site you want to add.
  - c Click **Save**.
- 5 To apply the execution schedule to groups, do the following:
  - a In the **Groups** area, click **Add**.
  - b From the **Group Type** list, select **Service Groups** or **Site Groups**.
  - c Select the check box beside each group you want to add.
  - d Click **OK**.
- 6 To apply the execution schedule to devices, do the following:
  - a In the **Devices** area, click **Add**.
  - b Use the filters to narrow the list of devices, and click **Filter**.
  - c Select the check box beside each device you would like to add.
  - d Click **OK**.
- 7 Click **Save**.

## Setting an Execution Schedule as the Default

A default execution schedule is applied by default to all new sites you create that have a service plan applied. When you create a site, you choose the

---

service delivery model, i.e. applying a service plan to the site, applying a service plan to groups, or opting not to use service plans. When a service plan is applied, via sites or groups, the default execution schedule is automatically applied.

- 1 In Service Center, click **Configuration > Schedules > Execution**.
- 2 Select the check box beside the schedule you want to set as the default.
- 3 Click **Set as Default**.

## Copying an Execution Schedule

When you copy an execution schedule, all of the settings for automation, AV, and patching schedules are also copied. The sites, groups, and devices to which the original schedule were applied are not copied.

Copied execution schedules are automatically provided with the same name as the original, with “-Copy” appended to the name.

- 1 In Service Center, click **Configuration > Schedules > Execution**.
- 2 Select the check box beside the schedule you want to copy.
- 3 The copied schedule is added to the list of execution schedules. To modify the schedule, either by giving it a new name, changing the schedule settings, or applying it to sites, groups, and devices, click the schedule name.

## Deleting an Execution Schedule

You can delete an execution schedule that is no longer required. If the execution schedule is currently applied to any sites, groups, or devices, it will be removed. As a best practice, you should create and apply a replacement execution schedule before deleting any execution schedule that is currently in use.

- 1 In Service Center, click **Configuration > Schedules > Execution**.
- 2 Select the check box beside the schedule you want to delete.
- 3 Click **Delete**.
- 4 A warning message pops up indicating that the schedule will be permanently deleted. Click **OK**.

---

## Setting Up Maintenance Schedules

### Understanding Maintenance Schedules

Maintenance schedules let you selectively suppress alerts at times when you know that the alerts don't represent critical warnings. For example, if you know that taking a group of devices offline for a scheduled maintenance activity will result in multiple Device Availability alerts, you can set up a maintenance schedule to suppress alerts to save time clearing them after the maintenance is complete. When you set up a maintenance schedule, you set the length of time alerts are suppressed. Alerts restart automatically after the maintenance schedule is over.

Maintenance schedules can be used during expected, recurring scheduled maintenance periods as well as when the maintenance period is unexpected. You can set up a recurring maintenance schedule to correspond with regular maintenance that happens at the same time each week or month. When you set up a recurring maintenance schedule, you can have the schedule repeat continuously, or you can set a date for the recurrence to end. After that date, the maintenance schedule no longer appears in the list of schedules.

Maintenance schedules give you full control over the different types of alerts you can suppress. You can suppress all alerts, or select alert types that relate to the type of maintenance you are currently performing. At the same time, you can choose which sites, groups, and devices are included, so that you can continue receiving alerts for the rest of the system.

When they are created, maintenance schedules appear on the list found by clicking Configuration > Schedules > Maintenance. This list includes details such as which sites, groups, or devices the schedule is assigned to, and the start and end time of the current maintenance if maintenance is currently in progress, or the next scheduled maintenance window.

Schedules stay on the list until they are not scheduled to run in the future. For example, if you set a schedule to start immediately and continue for one hour, the schedule remains on the list for an hour. After the hour is over, the schedule no longer appears on the list. If you set the maintenance schedule to run every month on the second day of the month, but you set the end date of the recurrence to February 1, the schedule is removed from the list on January 2 because it has run for the final time.

### Using Maintenance with Execution Schedules

You can use maintenance periods to suppress alerts associated with execution schedules. Maintenance created this way repeats automatically when the execution schedule does. For more information, see [Suppressing Alerts During an Execution Schedule](#).

---

## Creating Ad Hoc Maintenance Schedules

Ad hoc maintenance schedules create a window of time to suppress alerts for individual sites or devices. Use an ad hoc maintenance schedule when you want to suppress alerts on a single site or device immediately, for a certain period of time or until you terminate the maintenance schedule manually. For more information, see [Setting Up Ad Hoc Maintenance Schedules](#).

**Note:** Maintenance schedules replace alert schedules. Alert schedules will be deprecated in a future release of Managed Workplace.

### Adding Devices while a Maintenance Schedule is Running

If you onboard a new device or reinclude a previously excluded device while a maintenance period is running, the device will not be under maintenance during the current period. If the maintenance period recurs, they are included the next time it runs.

## Creating a Maintenance Schedule

When you create a maintenance schedule, you name it and provide a description.

The default duration for maintenance schedules is one hour and the default start time is immediately. Since maintenance schedules cannot be edited while running, if you want to change the default start time, date, or duration, change those options before you click the Save button.

When you create a schedule, you mark it as Planned or Unplanned. If you select **Planned**, the downtime of the affected devices, sites, and network services does not appear as downtime on reports.

If maintenance schedules overlap and one of them has the status of Planned, while the other is Unplanned, the overlapping time is set as Unplanned and the downtime of the affected devices, sites, and network services appears as downtime on reports.

The minimum duration is .5 hours. In the **Duration** box, any fraction of an hour less than .5 hours is rounded up to .5 hours. Over .5 hours, numbers are rounded to one decimal place.

### Notes:

- Maintenance schedules replace alert schedules. Alert schedules will be deprecated in a future release of Managed Workplace.
- Maintenance schedules do not suppress the following alerts:
  - Cloud monitors

- 
- Service Center receive alert configuration
  - Onsite Manager processing alert configuration

### To create a maintenance schedule

- 1 In Service Center, click **Configuration > Schedules > Maintenance**.
- 2 Click **New**.
- 3 Provide a schedule name and description.
- 4 In the **Start Date** box, enter the time when the maintenance schedule runs. You can click the calendar icon to select the date and/or the clock icon to select from a list of start times.
- 5 In the **Duration** box, type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
- 6 In the **Schedule Type** area, select one of the following options:
  - If you do not want device, site, or network services downtime to appear as downtime on reports, select the **Planned** check box.
  - If you want device, site, or network services downtime to appear as downtime on reports, select the **Unplanned** check box.

Now you will set the recurrence, select the alerts to suppress, and select the sites, groups, and devices to include in the maintenance schedule.

## Setting the Maintenance Schedule

There are several options you can set for the maintenance schedule, such as:

- how often the schedule repeats
- the types of alerts that are suppressed
- what sites, groups, and devices are included

### Setting a Maintenance Schedule to Run Once

Maintenance schedules can repeat on a recurring basis, but you can also create a maintenance period that only occurs once.

If a maintenance schedule is not set to repeat, it is removed from the list of schedules when it finishes running.

- 1 In the **Schedule** area, select the **Run Once** check box.

---

## Setting a Maintenance Schedule to Run Daily

Maintenance schedules can be set to run once a day. If you set the maintenance schedule to run daily, the schedule runs once every 24 hours, beginning at the time in the **Start Date** box and continuing for the length of time set in the **Duration** box.

Schedules stay on the list until they are not scheduled to run in the future, when they are removed automatically. If you do not set an end date, the maintenance schedule remains in the list on **Configuration > Schedules > Maintenance** indefinitely. If you establish an end date, then the schedule is removed from the list on that end date.

For example, if you set the schedule to run every day at 9 A.M., and you set the end date of the recurrence to January 1, the schedule is removed from the list after it runs on January 1.

- 1 In the **Schedule** area, select the **Recurring** check box.
- 2 Select the **Daily** check box.
- 3 Do one of the following:
  - Select the **No End Date** check box.
  - Select the **End Date** check box, then type a date or click the calendar icon to select the date.
- 4 Click **Save**.

## Setting a Maintenance Schedule to Run Weekly

Using a weekly maintenance schedule, you can define a time period during which alerts are suppressed, and you can repeat that time period on specific days of the week. For example, you can choose to have the schedule run twice a week by indicating that it runs on Tuesdays and Fridays.

Schedules stay on the list until they run for the final time, when they are removed. If you do not set an end date, the maintenance schedule remains in the list on **Configuration > Schedules > Maintenance** indefinitely. If you establish an end date, then the schedule is removed from the list after it runs for the final time. For example, if the schedule runs on Mondays and Tuesdays and the end date falls on a Thursday, the schedule is removed after it runs for the final time on Tuesday.

- 1 In the **Schedule** area, select the **Recurring** check box.
- 2 Select the **Weekly** check box.
- 3 Select the check boxes of the days of the week you want to run the maintenance schedule.

- 
- 4 Do one of the following:
    - Select the **No End Date** check box.
    - Select the **End Date** check box, then type a date or click the calendar icon to select the date.
  - 5 Click **Save**.

### Setting a Maintenance Schedule to Run Monthly

Monthly maintenance schedules allow you to determine a time period on one day a month when alerts are suppressed, for example, the first, fifth, or last day of the month. Or, you can select a day and week, for example, the second Tuesday of the month.

Maintenance schedules stay on the list until they are not scheduled to run in the future, when they are removed. If you do not set an end date, the maintenance schedule remains in the list on Configuration > Schedules > Maintenance indefinitely. If you set an end date, the maintenance schedule is removed from the list after it runs for the final time.

For example, you might set the schedule to run on the first Monday of every month and set the end date of January 31. The schedule is removed from the list after it has run for the last time, so if the first Monday of the month is January 1, the schedule is removed after it runs on January 1 because it is not scheduled to run again.

- 1 In the **Schedule** area, select the **Recurring** check box.
- 2 Select the **Monthly** check box.
- 3 Do one of the following:
  - Select the **Every month on the date** check box, then select a date from the drop-down list.
  - Select the **Every month on** check box, then select a week, then select a day of the week.
- 4 Do one of the following:
  - Select the **No End Date** check box.
  - Select the **End Date** check box, then type a date or click the calendar icon to select the date.
- 5 Click **Save**.

---

## Selecting the Alerts to Include in a Maintenance Schedule

Maintenance schedules suppress alerts for a specific time period. You can choose the alert types to suppress, selecting to suppress all alerts or one or more specific types.

**Note:** Maintenance schedules do not suppress the following alerts:

- Cloud monitors
  - Service Center receive alert configuration
  - Onsite Manager processing alert configuration
- 1 In the **Alert Suppression** area, select the check boxes of the alerts to suppress.
  - 2 Click **Save**.

## Editing a Maintenance Schedule

You can edit a maintenance schedule that is set to run in the future, however, schedules that are currently running cannot be edited. If you want to edit a schedule that is currently running, you must first terminate it. For more information, see [Terminating a Maintenance Schedule](#).

- 1 In Service Center, click **Configuration > Schedules > Maintenance**.
- 2 Click the name of a maintenance schedule.
- 3 Make your changes.
- 4 Click **Save**.

## Terminating a Maintenance Schedule

Terminating a maintenance schedule stops it from running. If you terminate a maintenance schedule and it is not scheduled to run in the future, the schedule is removed from the list.

- 1 In Service Center, click **Configuration > Schedules > Maintenance**.
- 2 Click the red icon in the **Actions** column of the maintenance schedule you want to terminate.

### Terminating a Maintenance Schedule on a Site

If you terminate a maintenance schedule on a site, alerts are restored for that individual site and the site's devices. Sites, groups, and devices belonging to other sites that have the maintenance schedule applied to them are not



---

affected. If the maintenance schedule recurs, other repetitions of the maintenance schedule are not affected.

Terminating a maintenance schedule on a site terminates all maintenance on any devices on the site, even if a maintenance schedule has been set or extended on an individual device.

The Site Overview page displays all the maintenance schedules running on a site. You can terminate any of the maintenance schedules currently running on the site. Terminated maintenance schedules are removed from the Site Overview page until they run again.

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Actions** column of the maintenance schedule table, click the red icon for the schedule you want to terminate.

### **Terminating a Maintenance Schedule on a Device**

If you terminate a maintenance schedule on a device, alerts are restored for that individual device only. Other sites, groups, and devices that have the maintenance schedule applied to them are not affected. If the maintenance schedule recurs, other repetitions of the maintenance schedule are not affected.

The Device Overview page displays all the maintenance schedules running on a device. You can terminate any of the maintenance schedules currently running on the device. Terminated maintenance schedules are removed from the Device Overview page until they run again.

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Summary** area, click **Devices**.
- 5 Click a device name.
- 6 In the **Actions** column of the maintenance schedule table, click the red icon for the schedule you want to terminate.

---

## Deleting a Maintenance Schedule

Deleting a maintenance schedule removes it from the list found at Configuration > Schedules > Maintenance. Deleted maintenance schedules are deleted permanently and cannot be restored.

You cannot delete a maintenance schedule that is currently running. If you want to delete a schedule that is currently running, you must first terminate it. For more information, see [Terminating a Maintenance Schedule](#).

- 1 In Service Center, click **Configuration > Schedules > Maintenance**.
- 2 Select the check box next to the name of a maintenance schedule.
- 3 Click **Delete**.

## Setting Up Ad Hoc Maintenance Schedules

Ad hoc maintenance schedules let you manually suppress alerts on a single site or device, starting immediately.

When you create an ad hoc maintenance schedule, you mark it as Planned or Unplanned. If you select **Planned**, device, site, and network services downtime does not appear as downtime on reports.

Manual maintenance begins immediately, and can be set to a defined duration of time, or can run until you terminate the schedule manually. Unlike other types of maintenance schedules, you can extend the duration of ad hoc maintenance schedules. For more information, see [Extending the Duration of Ad Hoc Maintenance Schedules](#).

### To Create an Ad Hoc Maintenance Schedule on a Site

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 Click the **Set Maintenance** button.
- 5 In the **Schedule** area, do one of the following:
  - Select the **Until Terminated Manually** check box.
  - Select the **Duration** check box, then type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
- 6 In the **Alert Suppression** area, do one of the following:

- 
- Select the **All** check box.
  - Select the **Configure Alert Suppression** check box, then select the check boxes of the alerts to suppress.
- 7 In the **Maintenance Type** area, select one of the following options:
    - Select the **Planned** check box to keep device, site, and network services downtime from appearing as downtime on reports.
    - Select the **Unplanned** check box to have device, site, and network services downtime appear as downtime on reports.
  - 8 Optionally, in the **Reason** box, type the reason for suppressing the alerts.
  - 9 Click **OK**.

### To Create an Ad Hoc Maintenance Schedule on a Device

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Summary** area, click **Devices**.
- 5 Click a device name.
- 6 Click the **Set Maintenance** button.
- 7 In the **Schedule** area, do one of the following:
  - Select the **Until Terminated Manually** check box.
  - Select the **Duration** check box, then type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
- 8 In the **Alert Suppression** area, do one of the following:
  - Select the **All** check box.
  - Select the **Configure Alert Suppression** check box, then select the check boxes of the alerts to suppress.
- 9 In the **Maintenance Type** area, select one of the following options:
  - Select the **Planned** check box to keep device, site, and network services downtime from appearing as downtime on reports.
  - Select the **Unplanned** check box to have device, site, and network services downtime appear as downtime on reports.
- 10 Optionally, in the **Reason** box, type the reason for suppressing the alerts.

- 
- 11 Click **OK**.

## Extending the Duration of Ad Hoc Maintenance Schedules

Unlike other kinds of maintenance schedules, which cannot be edited while they are running, you can extend the duration of an ad hoc maintenance schedule while it is in progress.

If the green Extend Maintenance Schedule icon is not available in the Actions column of the Maintenance Schedule table of a site or device that has a running maintenance schedule, the maintenance schedule that is in progress is set to run until it is manually terminated.

The minimum you can extend duration for is .5 hours. In the **Hours** box, any fraction of an hour less than .5 hours is rounded up to .5 hours. Over .5 hours, numbers are rounded to one decimal place.

### Extending the Duration of an Ad Hoc Maintenance Schedule on a Site

If you have extended the duration of a maintenance schedule on a device in the site, extending the duration of the maintenance schedule on the site does not apply to that device.

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Actions** column of the maintenance schedule table, click the green icon for the schedule you want to extend.
- 5 In the **Hours** box, type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
- 6 Click **OK**.

### Extending the Duration of an Ad Hoc Maintenance Schedule on a Device

If a device has an ad hoc maintenance schedule applied to it, or a device is part of a site that has an ad hoc maintenance schedule applied to it, you can extend the duration of the maintenance on that device. If you extend the duration of the schedule on the device, the device is treated as if it has an individual schedule; extending the duration of the schedule on the device will not extend the schedule on the site and extending the duration of the schedule on the site does not affect the schedule on the device.

---

For example, if you apply a one hour long ad hoc maintenance schedule to a site called "Innovation Drive," and then extend the ad hoc maintenance on a computer called "Innovation Drive Mac 12" for one hour, the ad hoc maintenance schedule on Innovation Drive will still only be one hour. However, Innovation Drive Mac 12 will have alerts suppressed for one hour longer than the Innovation Drive site.

Alternatively, if you extend the duration of the ad hoc maintenance schedule on the Innovation Drive site for two hours, Innovation Drive Mac 12's maintenance schedule is not extended.

- 1 In Service Center, click **Dashboards**.
- 2 If the Central Dashboard is not your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Summary** area, click **Devices**.
- 5 Click a device name.
- 6 In the **Actions** column of the maintenance schedule table, click the green icon for the schedule you want to extend.
- 7 In the **Hours** check box, type a number or use the up and down arrow buttons to raise or lower the duration in half hour increments.
- 8 Click **OK**.

## Viewing, Modifying, and Organizing Service Plans



You can view, compare, and organize your service plans on the **Service Plans** page in Service Center. The **Service Plans** page offers three views of your service plans, each with a different benefit; a comparison view for comparing services in service plans, a table view that lists the number of services in each service plan, along with the number of sites, groups, and devices to which it is applied and the associated service plan precedence, and finally a panel view that displays the description of each service plan and a list of the services included.

From the **Service Plans** page, you can also create new service plans, copy existing service plans, and manage service plan precedence.

### Comparing Service Plans with the Comparison View

Use the **Comparison View** matrix to see a list of every service in Managed Workplace, and see to which service plan each service belongs. Services are listed in rows, and service plans are listed in columns. If the service belongs to

---

a service plan, a green checkmark  appears in that service plan column. If the service does not belong to a service plan, a grey circle  appears in that service plan column.

**Tip:** You can add and remove services from a service plan by clicking these icons right in the **Comparison View** matrix. To add a service, click the grey circle, and the circle changes to a checkmark. Similarly, to remove a service from a service plan, click the checkmark.

### To access the Comparison View

- 1 In Service Center, click **Configuration > Service Plans**.
- 2 Click the **Comparison View** icon in the upper right corner.
- 3 Optionally, add and remove services from service plans by doing the following:
  - To add a service to a service plan, click the grey circle where the service row and the service plan column intersect. The grey circle changes to a green checkmark to indicate that the service is now included in the service plan. Click **Apply**.
  - To remove a service from a service plan, click the green checkmark where the service row and the service plan column intersect. The green checkmark changes to a grey circle to indicate that the service has been removed from the service plan. Click **Apply**.

## Viewing a List of Service Plans with the Table View

The **Table View** lists the service plans in a table format, and displays the number of sites, groups, and devices included in that service plan. You can click these numbers to view more information about the sites, groups, or devices, and for devices you can then click a device name to go to that device's page in Service Center.

### To access the Table View

- 1 In Service Center, click **Configuration > Service Plans**.
- 2 Click the **Table View** icon in the upper right corner.
- 3 Optionally, click a service plan name to modify the service plan name, description, and icon color. The icon color is displayed in the Services Dashboard, where you keep track of service plan activity. For more information, see [Viewing Service Plan Activity on the Services Dashboard](#).

---

## Viewing Descriptive Information about Service Plans with the Panel View

The **Panel View** displays descriptive information about each service plan, including the description that was provided when the service plan was created, and a bulleted list of the included services.

- 1 In Service Center, click **Configuration > Service Plans**.
- 2 Click the **Panel View** icon in the upper right corner.
- 3 Optionally, click a service plan name to modify the name, description, or icon color.

## Managing Service Plan Precedence

Service plan precedence determines which service plan to use when more than one service plan is applied to a device. For example, you apply Service Plan A to an entire site, and then you apply Service Plan B to a group of devices at the site. In some cases, devices will be added to both service plans, if they meet the automatic inclusion rules for policies in both plans. When you set precedence, you indicate which service plan to apply.

- 1 In Service Center, click **Configuration > Service Plans**.
- 2 Click **Manage Precedence**.
- 3 In the **Manage Service Plan Precedence** pop-up window, drag and drop the service plans to reorder them.
- 4 Click **OK**.

## Copying Service Plans

When you copy a service plan, all of the services in the service plan are also copied. The copied service plan is provided with the same name as the original, with “-Copy” appended to the name, and is placed one level below the original in precedence. For example, if you copy a service plan that has precedence over all other service plans, the copy will be placed at number 2 in the precedence list. For more information on service plan precedence, see [Managing Service Plan Precedence](#).

**Note:** Service plans can only be copied from the **Table View** and **Panel View**

- 1 In Service Center, click **Configuration > Service Plans**.
- 2 Do one of the following:

- 
- To copy a service plan from the **Table View**, click the **Table View** icon. Select the check box beside the service plan you want to copy, and click **Copy Service Plan**.
  - To copy a service plan from the **Panel View**, click the **Panel View** icon. Click anywhere in the service plan column, except for the service plan name. The service plan column becomes grey when selected. Click **Copy Service Plan**.

The new service plan is added to the list of service plans. To add or remove services from the service plan, click the **Comparison View** icon, and then use the table to add and remove services. For more information, see [Comparing Service Plans with the Comparison View](#).


## Viewing Service Plan Activity on the Services Dashboard

When you have service plans set up and running, you can use the **Services Dashboard** to keep track of issues. The **Services Dashboard** displays information about the alerts for each service plan. You can filter the results by service plan and by site to view more granular information.

**Note:** If you have devices that are not monitored by a service plan, you can still track them on the Services Dashboard. These devices will be marked as **Unassigned**, and can be viewed by selecting **Unassigned** from the service plan filter.

The **Services Dashboard** also includes widgets that provide at-a-glance information about the following activities:

- AVG AntiVirus
- Automation
- Patch Management
- Reporting
- Trouble Tickets

**Tip:** The **Services InfoBar** is a condensed view of the Services Dashboard, and can be accessed as a flyout from anywhere in Service Center. To access the **Services InfoBar**, click the **Toggle Services InfoBar** icon  in the top right corner of Service Center.

### What You Can Do

- Filter what is displayed on the dashboard by specifying which service plan or site you want to view.




- 
- Keep track of and address the active alerts for each service plan. The **Services Dashboard** includes an alerting overview at the top of the page. A widget is displayed for each service plan, with the number of active alerts. You can click the alert number to open the **Alerts** page for more details.
  - For AVG AntiVirus, keep track of unprotected devices for each service plan and click to access the AVG AntiVirus Status page to view details and take action.
  - Easily find failed automated tasks, and click to open the **Automation Calendar** to diagnose the issue and run the task again.
  - See a list of failed patches, and click to access the **Device Report** page to run the **Patch Now** command.
  - Ensure that reports were delivered successfully, if they were not click to access the **Report Policy Execution History** to rerun the failed reports.
  - Determine whether there are open tickets and service requests, and click to access ticket management.

## Viewing and Filtering Data on the Services Dashboard



The Services Dashboard provides filters to narrow down the results displayed. You can filter by service plan and site.

You can also make the Services Dashboard the default dashboard that displays when you click **Dashboards** in the navigation menu.

### To access the Services Dashboard

- 1 In Service Center, click **Dashboards**.
- 2 Click the **Services Dashboard** icon .

### To make the Services Dashboard the default

- 1 In Service Center, click **Dashboards**.
- 2 Click the **Services Dashboard** icon .
- 3 Click the grey checkmark  beside **Services** in the top left corner.

### To filter results by service plan

- 1 In the Services Dashboard, from the service plan list in the top right corner, select one of the following
  - To display data from all service plans, select **All**.

- 
- To display data from a single service plan, select the service plan from the list.

**Tip:** To view results for devices that are not monitored by a service plan, select **Unassigned** from the list.

#### To filter results by site

- 1 In the Services Dashboard, from the site list in the top right corner, select one of the following
  - To display data from all sites, select **All**.
  - To display data from a site, select the service plan from the list.

## Viewing Alerts from the Services Dashboard

The Services Dashboard displays the alerts at each service plan you have set up. At the top of the dashboard, each service plan is represented by a widget. The number of active alerts for each service plan is displayed, and you can click the service plan widget to open the Alerts page.

**Tip:** Each service plan widget is color-coded. You can specify the color of each widget by going to **Configuration > Service Plans**, clicking the name of the service plan, and then clicking in the **Icon Color** box to open a color palette.

#### To view the alerts for a service plan

- 1 In Service Center, click **Dashboards**.
- 2 Click a service plan widget at the top of the Services Dashboard.

## Viewing AVG AntiVirus Results on the Services Dashboard

The **AVG AntiVirus** section of the Services Dashboard displays a current snapshot of AVG AntiVirus activity for the sites and service plans that you have filtered for the dashboard. Two dials in this section indicate the following success measures:

- The **Install Succeeded** dial indicates the percentage of successful installations of the AVG AntiVirus client.
- The **Update Succeeded** dial indicates the percentage of successful AVG AntiVirus client updates.

You can take action on threats detected and on unprotected devices from the Services Dashboard. Unprotected devices includes devices that do not have the AVG AntiVirus client installed, and devices that have the client installed but

---

do not have an AVG AntiVirus policy applied. For information about creating and configuring AVG AntiVirus policies, see [Setting Up AntiVirus Policies](#).

### To view detected threats

- 1 In Service Center, click **Dashboards**.
- 2 In the **AVG AntiVirus** section, click the number above **Threats Detected**.
- 3 In the **Alerts** page, view and take action on the alert, if required. For more information about the **Alerts** page, see [Alerts](#).

### To view unprotected devices

- 1 In Service Center, click **Dashboards**.
- 2 In the **AVG AntiVirus** section, click the number above **Unprotected Devices**.
- 3 On the **AVG AntiVirus Status** page, do any of the following:
  - In the **Devices Needing AntiVirus Installation** column, click the number to open the **Devices Needing AntiVirus Installation** page. From here, you can select the check box beside each device on which you want to install AVG AntiVirus, and then click **Install**.
  - If there is a site with devices missing an AntiVirus policy, consider updating the automatic inclusion rules of the AntiVirus policy applied to the site to include all devices.

## Viewing Automation Results on the Services Dashboard

You can view the results of automated tasks run so far today, in the current calendar week, and the current calendar month. The **Automation** section includes two dials that indicate the following success measures:

- The **Tasks Succeeded** dial indicates the percentage of successful tasks for the time period you have selected.
- The **Tasks Completed** dial indicates the percentage of completed tasks for the time period you have selected. For example, if there are tasks that have not yet begun, or are currently running, the **Tasks Completed** dial will indicate the percentage that have not yet run.

You can use the **Automation** section to view details about failed tasks, and tasks that have not yet completed for the time period you specified.

### To filter Automation results by time period

- 1 In Service Center, click **Dashboards**.

- 
- 2 In the **Automation** section, click one of the following:
    - To view results for the current day, click **Today**. Results will be filtered by automation activity beginning at 12:00am the current day.
    - To view results for the current week, click **Week**. Results will be filtered by automation activity beginning on Sunday of the current week.
    - To view results for the current month, click **Month**. Results will be filtered by automation activity beginning on the first day of the current month.

#### To view failed tasks

- 1 In Service Center, click **Dashboards**.
- 2 In the **Automation** section, click the number below **Tasks Failed**.
- 3 The **Automation Calendar** opens displaying the same time period you had filtered on the Services Dashboard. From here, you can click the failed task to take action. For more information, see [Following Up on Executed Tasks](#).

#### To view remaining tasks

- 1 In Service Center, click **Dashboards**.
- 2 In the **Automation** section, click the number below **Remaining Tasks**.
- 3 The **Automation Calendar** opens displaying the same time period you had filtered on the Services Dashboard. From here, you can view the tasks that have not yet completed.

## Viewing Patch Management Results on the Services Dashboard

The **Patch Management** section helps you keep track of devices needing patches, and patch installations that have failed. The **Patch Success** dial indicates the success rate of installed patches for the time frame you have chosen - either for the current calendar month, or since patching was initiated.

You can drill down to the **Device Report** and the **Patch Report** pages to view details about devices needing patches, and failed patch installations. From these pages, you can then click **Patch Now** to remediate the issue.

#### Patch Now

If you try to use Patch Now and the Onsite Manager doesn't receive the command for thirty minutes, for example, if the Onsite Manager is not communicating, Patch Now is cancelled.

---

When using Patch Now, if the Onsite Manager can't communicate with the device being patched on the first try, the Onsite Manager will make two more attempts over twenty minutes. If the third attempt fails, Patch Now is cancelled.

### To filter Patch results by time period

- 1 In Service Center, click **Dashboards**.
- 2 In the **Patch Management** section, click one of the following:
  - To filter results for the current calendar month, click **Month**. Results will be filtered by patch management activity beginning on the first day of the current month.
  - To filter results since patch management was initiated, click **All**. Results will be filtered since patch management was initiated (i.e. a patch policy was applied) for the service plan(s) and site(s) that you are viewing in the dashboard.

### To view a list of devices needing patches

- 1 In Service Center, click **Dashboards**.
- 2 In the **Patch Management** section, click the number above **Devices Needing Patches**.
- 3 In the **Device Report** page, select the check box beside each device you want to patch, and click **Patch Now**.

### To view a list of devices with failed patches

- 1 In Service Center, click **Dashboards**.
- 2 In the **Patch Management** section, click the number above **Devices with Failed Patches**.
- 3 In the **Device Report** page, select the check box beside each device you want to patch, and click **Patch Now**.

### To view a list of failed patches

- 1 In Service Center, click **Dashboards**.
- 2 In the **Patch Management** section, click the number above **Failed Patches**.
- 3 In the **Patch Report** page, select the check box beside each patch you want to install, and click **Patch Now**.

---

## Viewing Reporting Results on the Services Dashboard

The **Reporting** section of the Services Dashboard provides a snapshot of report deliveries for the current day, week, or month.

The **Report Delivery** dial indicates the percentage of successful deliveries for the time period that you are viewing. You can also drill down to the **Report Policy Execution History** page to view and run failed deliveries.

### To filter Reporting results by time period

- 1 In Service Center, click **Dashboards**.
- 2 In the **Reporting** section, click one of the following:
  - To view results for the current day, click **Today**. Results will be filtered by report delivery activity beginning at 12:00am the current day.
  - To view results for the current week, click **Week**. Results will be filtered by report delivery activity beginning on Sunday of the current week.
  - To view results for the current month, click **Month**. Results will be filtered by report delivery activity beginning on the first day of the current month.

### To view a summary of Report deliveries

- 1 In Service Center, click **Dashboards**.
- 2 In the **Reporting** section, click one of the following:
  - To view a list of failed report deliveries, click the number above **Failed Deliveries**.
  - To view a list of successful report deliveries, click the number above **Successful Deliveries**.

Clicking either of these options opens the **Report Policy Execution History** page, with a list of the failed or successful report deliveries.

## Viewing Trouble Ticket Results on the Services Dashboard

The **Trouble Tickets** section of the Services Dashboard provides a quick glance of the open tickets, service requests, high priority tickets, and number of tickets closed today. The results are filtered according to the service plan(s) and site(s) you are viewing on the dashboard.

---

### To view open tickets

- 1 In Service Center, click **Dashboards**.
- 2 In the **Trouble Ticket** section, click the number above **Open Tickets**.  
The **Ticket Management** page opens displaying a list of open tickets for the sites and service plans you were viewing in the Services Dashboard.

### To view service requests

- 1 In Service Center, click **Dashboards**.
- 2 In the **Trouble Ticket** section, click the number above **Service Requests**.  
The **Ticket Management** page opens displaying a list of service requests for the sites and service plans you were viewing in the Services Dashboard.

### To view service requests

- 1 In Service Center, click **Dashboards**.
- 2 In the **Trouble Ticket** section, click the number above **Service Requests**.  
The **Ticket Management** page opens displaying a list of service requests for the sites and service plans you were viewing in the Services Dashboard.

### To view open high-priority tickets

- 1 In Service Center, click **Dashboards**.
- 2 In the **Trouble Ticket** section, click the number above **High Priority**.  
The **Ticket Management** page opens displaying a list of high priority tickets for the sites and service plans you were viewing in the Services Dashboard.

### To view a list of tickets closed today

- 1 In Service Center, click **Dashboards**.
- 2 In the **Trouble Ticket** section, click the number above **Tickets Closed Today**.  
The **Ticket Management** page opens displaying a list of tickets closed today for the sites and service plans you were viewing in the Services Dashboard.





## SETTING UP AND MAINTAINING SITES

---

*This section provides detailed information about the following topics:*

- *About Sites*
  - *Setting Up a Site Managed By Onsite Manager*
  - *Adding Device Managers to a Site*
  - *Adding Support Assistants to a Site*
  - *Working with Sites*
  - *Setting Site Options*
  - *About Updating Service Center*
  - *Updating and Installing Service Center Components*
-

---

## About Sites

A Managed Workplace site is a logical container in Service Center that helps you manage and identify devices by physical location or customer.

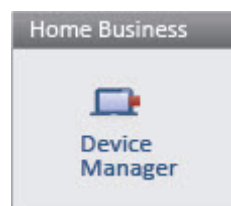
### What Are the Options for Setting Up a Site?

A site can be monitored by Onsite Manager, by Device Managers only or by both Onsite Managers and Device Managers in a mixed environment.

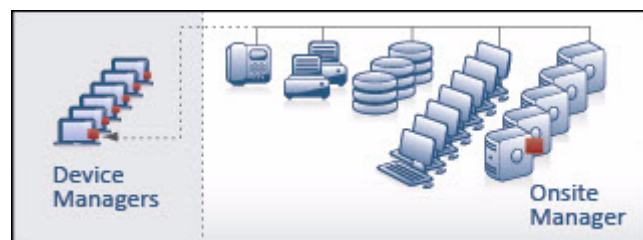
- Onsite Manager site



- Device Manager only site



- Mixed site






### How Do You Set Up a Site?

You create sites in Service Center by performing a series of steps in a guided setup process. See [Creating a Site in Service Center](#).

---







## How Do You See Whether a Site is Monitored by Onsite Manager or Device Manager?

The Central Dashboard indicates whether a site is monitored by Onsite Manager or Device Manager, and provides a warning if Onsite Manager is not communicating.


Icon	Site Deployment Method
	Site is monitored by Onsite Manager.
	Site is monitored by Device Managers only.
	Onsite Manager is not communicating.

## How Do You Know Which Service Modules Have Been Applied to a Site?

If a site has a service module applied to it, you'll see an icon beside the site name:

Icon	Service Module
	The AVG CloudCare service module has been applied to this site.
	The VMware ESXi service module has been applied to this site.
	The Microsoft Hyper-V service module has been applied to this site.
	The BDR Infracore service module has been applied to this site.
	The Symantec Endpoint Protection service module has been applied to this site.
	The Symantec Backup Exec service module has been applied to this site.

---

Icon	Service Module
	The Axcient service module has been applied to this site.

---

### What You Can Do

For each site managed by either Onsite Manager or Device Manager, you can

- change the status of the site from approved to on hold or rejected
- view information about a site
- change contact information for a site
- add notes about a site
- change the website addresses to use to determine internet availability for a site
- set the polling interval for printer monitoring
- set the Microsoft Baseline Security Analyzer (MBSA) schedule for a site
- configure how frequently you want to perform a network scan
- upgrade Device Managers at a site

For each site managed by Onsite Manager, you can also

- set the alerting action for a site not communicating
- set how many days before a down device is automatically deleted from a site
- upgrade Onsite Managers at a site

## Setting Up a Site Managed By Onsite Manager

### Creating a Site in Service Center

You create sites from within Service Center. The **Create Site** page guides you through the process of providing site details, selecting the service delivery model, whether or not to deploy Device Managers, and downloading the Onsite Manager installation package, if required.

A site's service delivery model determines whether you will apply a single service plan to the entire site, apply service plans to groups, or bypass service plans altogether. For more information on selecting a service delivery model, see [Determining a Service Delivery Model](#).

---

When setting up a site, you can automatically deploy Device Managers to laptops. Managed Workplace detects the laptop's operating system and deploys either a Device Manager for Windows devices or a Device Manager for Mac OS X devices.

**Notes:**

- When deploying Device Manager to OS X laptops, you must ensure that the site's SSH account is on the sudoer's list. If it is not, the deployment will fail. To set up the site's SSH credentials in Service Center, see [Managing Site Credentials](#).
- You cannot deploy a Device Manager to an OS X device that has a web proxy configured.

**To create a site in Service Center**

- 1 Do one of the following:
  - If you have not yet set up a site in Service Center, the **Create Site** page displays automatically as your home page when you log in to Managed Workplace.
  - If you have already set up a site in Service Center, and you want to create another, click **Site Management > Create Site**.
- 2 Type the name of the site in the **Site Name** box.
- 3 Select one of the following service delivery models for the site:

**Apply a single service plan to all devices in this site** A single service plan will be applied to the site. Select this option if the entire site can be monitored using a single service plan.

**Apply service plans to any of the following groups** Service plans will be applied to groups at the site.

**Do not use a service plan for this site, I'll configure the site manually** This option is not recommended, however you may need to select this for sites that do not fit any of your current service levels or service delivery models.
- 4 Click **Next**.

**To apply a single service plan to a site**

If you selected the **Apply a single service plan to all devices in this site** option, follow the steps below to select a service plan to apply.

- 1 From the list, select a service plan to apply.
- 2 Click **Next**.

---

**Tip:** When you select a service plan, the icons representing the types of policies that will be applied to devices is highlighted in blue. You can use the **Service Components** matrix to quickly confirm the types of policies that will be applied with the service plan. For more information on the types of policies you can create in Service Center, see [Working with Policies and Services](#).

### To apply service plans to groups

- 1 For each group listed, select the service plan you want to apply.
- 2 Click **Next**.

### To specify how Onsite Manager and Device Manager are deployed

- 1 Choose one of the following deployment methods:
  - Typical Deployment** Downloads a site-specific Onsite Manager. Device Managers will be automatically installed on Windows and OS X laptops.
  - Configure Advanced Options** Allows you to choose whether to download Onsite Manager, Device Manager, and to specify whether or not to automatically deploy Device Managers on Windows and OS X laptops.
- 2 If you selected **Configure Advanced Options** in the previous step, select one of the following options:
  - To download Onsite Manager only, select the **Download Onsite Manager** option button, and then clear the **Automatically deploy Device Managers on Mac and Windows laptops** check box.
  - To download Device Manager for Windows only, select the **Download Device Manager for Windows Device** option button.
  - To download the Device Manager for Mac OS X only, select the **Download Device Manager for Mac Device** option button.
- 3 Click **Next**.
- 4 Click **Create**.

The site is created in Service Center, and the Onsite Manager installation package for this site automatically starts downloading.
- 5 Click **Finish** to complete the process. The **Site Management** page opens with the new site listed.

---

## Installing Premium Remote Control Automatically on Devices Added to Sites

Using Premium Remote Control, you can access Windows and Mac computers remotely, allowing you to install software, troubleshoot issues, and perform other tasks. For more information, see [AVG Business Premium Remote Control](#).

To use Premium Remote Control, the Premium Remote Control agent must be installed on the client device. If you select the Automatically install Premium Remote Control option, Managed Workplace will try to install the Premium Remote Control agent on devices on the site and on any new devices added to the site as long as this option is enabled. The Premium Remote Control agent will not be installed if:

- the Premium Remote Control agent is already installed on the device.
- a failed install of the Premium Remote Control agent is detected on the device.

If you decide you don't want the Premium Remote Control agent installed on devices added to sites, you can turn off the automatic install. This will not uninstall the Premium Remote Control from devices it is already installed on.

### To Enable Automatic Installation of Premium Remote Control on Devices Added to Sites

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the check boxes next to any sites you want to install Premium Remote Control on.
- 3 Click **Premium Remote Control**, then click **Automatically install Premium Remote Control**.

### To Disable Automatic Installation of Premium Remote Control on Devices Added to Sites

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the check boxes next to any sites you want to install Premium Remote Control on.
- 3 Click **Premium Remote Control**, then click **Do not automatically install Premium Remote Control**.

---

## Setting Default Premium Remote Control Options for Creating New Sites

Using Premium Remote Control, you can access Windows and Mac computers remotely, allowing you to install software, troubleshoot issues, and perform other tasks. For more information, see [AVG Business Premium Remote Control](#).

To use Premium Remote Control, the Premium Remote Control agent must be installed on the client computer.

You can select the default Premium Remote Control options for new sites, so that when you create sites, the options you choose will be applied by default.

The options include:

- Installing Premium Remote Control automatically when creating new sites.
- Requiring consent for Premium Remote Control access to client computers.
- Setting the default consent response.
- Setting the timeout for the consent response.

You can enable consent, which requires the end user to give consent for remote access. If you enable consent, when a technician starts a Premium Remote Control session, your customer is presented with a window to allow or reject the access. The Notification Timeout is the number of seconds that the customer has to respond before the request times out. If the request times out, the session will either allow or reject the connection, depending on the default option you choose.

**Best Practice:** For sites where your customers may be working on critical tasks that cannot be interrupted or sensitive information that cannot be shared, enable the require consent option and set the default to Reject.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click **Premium Remote Control**, then click **Set default for new sites**.
- 3 Select the **Automatically install Premium Remote Control** check box.
- 4 Optionally, select the **Require Consent** check box, then in the **Notification Timeout** box, type a number. In the **Default** area, enable one of the following option buttons:
  - **Allow**—Allows Premium Remote Control access if the user does not respond before notification timeout.
  - **Reject**—Rejects Premium Remote Control access if the user does not respond before notification timeout.



- 
- 5 Click **OK**.

## Deploying Onsite Manager within a Domain

The **Resources (Site Management)** page enables you to perform the following actions:

- Download a site-specific **Windows Prep Utility** to configure Windows devices for management. This utility is deployed to Windows devices automatically, however if that deployment fails you can download and run this utility manually from the Resources tab.
- Download a site-specific **OS X Prep Utility** to prepare Mac devices for network management.

### To run the Windows Prep Utility

**Note:** Target devices must have .NET 3.5 SP1, at a minimum .NET 3.5 or higher is delivered with Windows 7 and higher, and is bundled with service packs for Windows XP, Windows Vista SP2, and Windows 2003.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site with which you want to work.
- 3 Click the **Resources** tab.
- 4 In the **Windows Prep Utility** section, click **Download Prep Utility**.
- 5 Click **Save** and select the location to which you want to save the Windows Prep Utility.

**Note:** The .ZIP file contains the omsiteprep.exe in the root folder, and the following files in the SiteSetting folder: lpi.cr1 and MDPrepDotNet.exe.

- 6 From the extracted location, double click the omsiteprep.exe file.

**Note:** For Vista, Windows 7, Server 2008 and Server 2008 R2, right-click the utility and click Run As Administrator. Otherwise, the utility makes no changes in the operating system.

When complete, a dialog box appears stating if the site preparation was successful.

- 7 Click **OK**.

The utility generates the following two log files in C:\Program Files\Level Platforms\LPISetupLogs:

- MWSiteprep.log, which contains information about configurations for the user account, required services, RDP, WMI over DCOM, firewall, UAC, and file and print sharing

- 
- LpiSetups.log, which contains the WMI over WS-MAN log file.

The Windows preparation process does the following:

- Checks if Managed Workplace Windows preparation has been run before.
- Checks the type of platform (Windows operating system) since some preparation tasks are dependent on the operating system version.
- Creates a local MW Service account and adds it to the Local Administrators group. Updates the password if the account already exists.
- Starts and configures dependent system services, if required.
- Configures and enables WS-Management (WS-MAN) for WMI, if required. This includes installing WinRM 2.0 or WinRM 3.0, depending on the device's operating system, if it is not already installed. This also includes the installation of .Net and PowerShell, which are prerequisites for WinRM, if they are not already installed on the device.
- Configures UAC options on Vista and newer versions of Windows operating systems.
- Configures all firewall profiles, regardless of whether the firewall is enabled. This includes allowing ICMP echo; remote administration, file and print sharing, and remote desktop services; and ports required for WMI and Managed Workplace applications.
- Logs all changes to file and updates the registry with a record of execution.

**Note:**

- A reboot is required for some of the changes to take effect. If a reboot is required, a notification message appears indicating which changes are pending the reboot.
- If you are running the Windows prep utility on a Windows XP, Vista, or Server 2003 device using an account that does not have a password, the WS-MAN configuration will fail. You must either log into the system using an administrator account with a password, or you must give the current user a password, log out, and then log back in before running the workgroup prep utility again.

**To run the OS X Prep Utility**

You must configure the following site credentials before downloading the OS X Prep Utility:

- 
- SSH
  - SNMP
  - VNC

If these credentials are not set in Service Center, the Download OS X Prep Utility link is not available. The OS X Prep Utility will set these credentials on the device. For more information, see [Managing Site Credentials](#).

When you run the OS X Prep Utility, you can specify that it also installs a Management Profile on the device. This allows the device to be managed off-network using the Apple Mobile Device Management protocol. You must set up a valid customer APNs (Apple Push Notification service) certificate for this check box to be enabled. See [Setting Up an Apple-Approved APNs Certificate for iOS \(Customer\)](#).

When the Management Profile check box is selected, you can deploy configuration profiles to the device to enforce passcode, email, and network policies, among others. When the device is added to a group that has OS X configuration profiles created, the profiles are automatically applied to the device. See [About Configuration Profiles](#).

**Note:** The OS X Prep Utility is only available for sites with an Onsite Manager.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site with which you want to work.
- 3 Click the **Resources** tab.
- 4 In the **OS X Resources** section, click the **Install Management Profile** check box to allow configuration profiles to be deployed to the device.
- 5 In the **OS X Resources** section, click **Download OS X Prep Utility**.
- 6 Click **Save** and select the location to which you want to save the OS X Prep Utility.
- 7 Unzip the file if it does not unzip automatically, and then run the following file:

```
OS X Prep Util
```

The OS X Prep Utility performs the following actions on the Mac device:

- Configures and enables SNMP. Any existing SNMP settings are overridden.
- Turns on VNC.
- Enables SSH on the device and creates an administrator account, if one does not already exist. If an account already exists, the password will not change.

---

## About Scan Configuration

After you install Onsite Manager, the first scan runs automatically, without the need to manually configure the settings. However, you may want to change the scan range and frequency values set for device and asset discovery. See [Setting the Device Discovery Defaults](#).

**Note:** Onsite Manager is installed from Service Center. For information on setting Onsite Manager installation defaults, see [Setting Onsite Manager Installer Preferences](#). For information on installing Onsite Manager, see the *Setup Guide*.

### What You Can Do

You can configure the scan by

- adding individual IP addresses, ranges of IP addresses, IP subnets or any combination of these
- skipping individual IP addresses or ranges of IP addresses
- excluding devices from the scan
- deleting individual IP addresses, ranges of IP addresses, IP subnets or any combination of these that have been previously configured

### Notes:

- When configuring the Onsite Manager scan, add only the addresses for the devices that should be monitored. Having extra devices can lead to unwanted database growth and licensing issues.
- Do not include addresses that end in .255 or .0, as these are not valid IP addresses.
- The scan automatically attempts to scan up to 65540 IPs based on the subnet mask information collected from Onsite Manager, if the network is configured as Class B. The purpose of this is to isolate any devices that could be present in the network and bring that information back into the Service Center so you can gain insight to what is within the network and what should be managed. In some Class B networks, the scan interval can take up to 15 minutes to complete this configuration. If this is a concern and you wish to decrease the interval, it is recommended that you either alter the scan settings after the automatic scan has occurred, or not use automatic scan in these networks and instead manually configure the scan range.

---

## Process for Network Discovery

Onsite Manager queries each IP address defined in the network scan using an ICMP ECHO request. An ARP cache retrieval is also performed to detect IP addresses on the local subnet that may not respond to the ICMP ECHO request. Each IP address that responds will be further scanned to determine its identity.

To identify...	Onsite Manager...
A-name	Queries the reverse lookup zone in DNS and then validates with the forward lookup zone
Machine name	Uses WMI calls
sysName	Uses SNMP calls
MAC addresses	Uses WMI or SNMP calls.

Onsite Manager uses a combination of device protocols, including SSH, Zeroconf, and NetBIOS, to identify devices. All the collected identifying factors are used to create discovery variables, which are then compared against each known device to see if a match can be found. If a match is found, the IP address is associated with the known device. If no match is found, a new device is created.

### Notes:

- Onsite Manager always discovers itself regardless of whether it is in the scan range.
- Device Managers do not have scan settings for device discovery because it is only responsible for discovering the device on which it is installed.

## Avoiding Issues with Network Discovery

Any or all the following actions will help Onsite Manager intelligently classify unique devices and avoid issues with network discovery:

- Enable a management protocol (such as WMI, SNMP, or SSH) on each device.
- Assign static IP addresses to devices that do not have a management protocol enabled.
- Assign unambiguous DNS names to the device so that it is uniquely reverse resolvable.

---

## Configuring the Scan Range

You can configure the scan range of IP addresses:

- add a new IP address or range
- skip an IP address in a range or skip a range
- delete an IP address, range or subnet

**Skip** Does not query the IP address. Use when you know IP addresses that you do not want to scan. For example,

- if an auditor is at the customer site and has been given a static IP address, you can skip it because the auditor is not your customer.
- if a range of IP addresses is used for visitors to a company, then this range should be skipped as the devices that use this range are not your customers.

See [Skipping IP Addresses During the Scan](#).

**Delete IP address** Removes the IP address from the scan. Use when you know you will never be interested in collecting data at that IP address.

### Adding IP Addresses or a Subnet to the Scan

Add IP addresses one at a time if you know a specific IP address that needs to be added to the scan.

Add one or more ranges to add many IP addresses at once or if you are adding only some in the subnet.

Add a subnet mask to get everything on the network.

**Note:** To add a subnet mask, use a table to look up the notation.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to edit the scan settings.
- 3 Click the **Network Discovery** tab.
- 4 In the **Network Scan (Local Network)** section, click **Modify**.
- 5 In the **Scan Settings** section, click **Add**.
- 6 Do one of the following:
  - To add a single IP address to the scan, select the **Single** option button and type the device IP address in the **IP Address** box.

- 
- To add a range of IP addresses to the scan, select the **Range** option button and type the Start IP Address and End IP Address in the boxes.
  - To add a subnet to the scan, select the **Subnet Mask** option button. Type the network address in the box, and specify the prefix size in the numbered list. Optionally, type a description in the **Description** box.

7 Click **Save**.

### See Also

[Skipping IP Addresses During the Scan](#)

[Deleting an Item from the Scan](#)

[Deleting a Range or a Subnet from the Scan](#)

### Skipping IP Addresses During the Scan

You can skip an individual IP address or a range of IP addresses.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to edit the scan settings.
- 3 Click the **Network Discovery** tab.
- 4 In the **Network Scan (Local Network)** section, click **Modify**.
- 5 In the **Scan Settings** section, click **Add**.
- 6 Do one of the following:
  - To skip a single IP address, select the **Single** option button and type the device **IP address in the IP Address** box.
  - To skip a range of IP addresses, select the **Range** option button and type the Start IP Address and End IP Address in the boxes. Type a description, if desired.
- 7 Select the **Skip** check box.
- 8 Click **Save**.

**Tip:** To return the skipped item to the scan, delete the skipped item.

### See Also

[Adding IP Addresses or a Subnet to the Scan](#)

[Deleting an Item from the Scan](#)

[Deleting a Range or a Subnet from the Scan](#)

---

## Deleting an Item from the Scan

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to edit the scan settings.
- 3 Click the **Network Discovery** tab.
- 4 In the **Network Scan (Local Network)** section, click **Modify**.
- 5 In the **Scan Settings** section, select the check box for the item you want to remove.

**Note:** Ensure that you select an item that is not currently skipped. Selecting a skipped item and clicking **Delete** returns the item to the scan (essentially deletes the skip rule).

- 6 Click **Delete**.

**Tip:** If you want to delete an individual IP address from the scan, and it is part of a scan range, add two scan ranges. Or, use one range and skip the individual IP address.

### See Also

[Adding IP Addresses or a Subnet to the Scan](#)

[Skipping IP Addresses During the Scan](#)

[Deleting a Range or a Subnet from the Scan](#)

## Deleting a Range or a Subnet from the Scan

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to edit the scan settings.
- 3 Click the **Network Discovery** tab.
- 4 In the **Network Scan (Local Network)** section, click **Modify**.
- 5 In the **Scan Settings** section, select the check box for the range or subnet you want to remove.
- 6 Click **Delete**.
- 7 Click **Save**.

### See Also

[Adding IP Addresses or a Subnet to the Scan](#)

[Skipping IP Addresses During the Scan](#)

[Deleting an Item from the Scan](#)



---

## Discovering and Onboarding Devices

When onboarding devices at a site, issues may arise that prevent devices from being monitored. The Onboarding Overview dashboard helps you identify and correct some common discovery issues, including:

- Windows devices that do not have WMI enabled
- SNMP devices that do not have SNMP enabled
- Windows devices that do not have RDP enabled
- Windows devices that do not have the Admin share enabled
- No ICMP for devices that are responding to ARP only
- MAC or Linux devices that do not have SSH enabled
- Devices that are not monitored by a monitoring policy
- VMware devices that do not have vSphere credentials
- Mobile devices that do not have an agent installed.

After correcting the issue, you can trigger the device discovery scan to verify that the device is being monitored as expected.

### Viewing Onboarding Details

The Onboarding Overview dashboard gives you a quick glimpse into the status of recent device discovery scans.

From here, you can view the number of fully deployed sites, which are sites with no device issues. By default, this screen displays a list of all sites, but you can toggle the view to display only sites with device issues.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the **Sites with Issues** button.
- 3 Click a site name to view a list of the devices with onboarding issues.


### Viewing and Solving Device Issues

There are several ways you can sort devices to easily locate the issues you want to view:


- You can sort devices by status, device name, IP address, and detected issue, by clicking a column header.
- You can group issues by device classification and by issue type. Clicking the Classification or Issue Type buttons divides the devices into separate groups, which you can then further sort by clicking a column heading.

---

You can expand a device to view details about its onboarding issues. A device can have more than one issue.

Some issue descriptions include an arrow  that links to a page in Service Center that may provide you with some assistance in resolving the problem. For example, for devices in which WMI access is denied, clicking the arrow takes you to the **Credentials** tab where you can provide the WMI credentials. See [Managing Site Credentials](#).

If the issue cannot be corrected in Service Center, the issue description provides tips on solving the issue. For example, for a Device Unknown issue, the issue description suggests that you enable supported protocols, such as WMI, SNMP, or SSH, if they are available on the device.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click a site name.
- 3 To group the devices, click one of the following buttons:
  - Classification** Groups devices by type, for example Windows or Unix devices.
  - Issue Type** Groups devices by issue category, for example No Admin Share.
- 4 Click the triangle beside a device to view the issue type and description.
- 5 Optionally, do any of the following:
  - Click the device name to open the **Device Overview** page.
  - Some issue descriptions include an arrow that links to a page in Service Center that may provide you with some assistance in solving the problem. Click the green arrow  to solve the device issue.

### Suppressing Device Issues

You can suppress, or hide, device issues that do not require correction or that you deem unimportant. Suppressed device issues are removed from the Devices with Onboarding Issues list, but still available for you to view on the Suppressed Issues page.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click a site name.
- 3 Click the triangle beside a device to view the issue type and description.
- 4 Click **Suppress**.

---

## Viewing and Clearing Suppressed Device Issues

You can view a list of suppressed issues and, optionally, clear suppressed issues. When you clear a suppressed issue, you are in effect returning it to the Devices with Onboarding Issues list, with the probable intent of correcting the issue.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click a site name.
- 3 Click **More Actions** and select **View Suppressed Issues**.
- 4 To clear suppressed issues, do one of the following:
  - to clear all suppressed issues for a device, select the check box beside the device and then click **Clear All Device Issues**.
  - to clear a specific suppressed issue, click the triangle beside a device, and then click **Clear** beside the issue description.
  - to clear all suppressed device issues, select the check box in the header row and then click **Clear All Device Issues**.

## Configuring Device Discovery

You can configure how discovered devices are handled:

- exclude or ignore data from a device, so that the device is unmanaged
- delete data from a device
- delete data from a device and exclude the device from the scan

### About Excluding Devices from Management

Managed Workplace allows you to control which devices you want to exclude from management, so that you do not get billed for devices you do not want to manage. For example, if you do not provide Mobile Device Management (MDM) services at a site, you can exclude all mobile devices from management.

You can choose to automatically exclude all newly discovered devices at a site, which is helpful when

- the site periodically has temporary devices checking in, for example a doctor's office with WiFi
- your technician checks in to the local network to perform some troubleshooting

- 
- you are charging your customers on a per-device basis, and you want to upsell your services by showing them that new devices are not currently under management.

When you exclude a device, it is removed from the scan, and all monitors, alerts, and historical information is purged. Excluded devices are not deleted.

There are three ways you can exclude a device from management:

**Exclude by Device** You can exclude a device from the following locations:

- **Onboarding Overview** dashboard
- the **Device** page

When you exclude a device, the device is hidden in Service Center, but it is not deleted. All monitors, alerts, and historical information are purged. When you reinclude a device, the device comes back immediately.

**Exclusion by Rule** Deletes the device right away from Service Center and Onsite Manager, and does not include the device in the network scan. Use for devices you do not want to monitor where using its name (DNS name, SNMP name or MAC address) makes sense. For example, for a device that uses DHCP, in which case its IP address may change. When an exclusion rule is deleted, the device comes back after it is redetected during a network scan.

**Exclude All Newly Discovered Devices at a Site** All newly discovered devices are excluded from management until you reinclude them. You can view all excluded devices in the Onboarding Overview dashboard. See [Viewing Excluded Devices and Returning them to Management](#).

**Note:** Devices with Onsite Manager or Device Manager installed cannot be excluded from monitoring.

### See Also

[Running a Scan Manually](#)

[Adding IP Addresses or a Subnet to the Scan](#)

[Skipping IP Addresses During the Scan](#)

[Deleting a Range or a Subnet from the Scan](#)

### Excluding Devices Directly

There are two locations in Service Center where you can exclude on a per-device basis; from the Onboarding Overview dashboard, and from the Device Overview page.

---

### To exclude a device when onboarding a site

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the device for which you want to turn monitoring off.
- 3 Select the check box beside the device you want to exclude.
- 4 Click **Exclude Device**.

### To exclude a device when viewing device details

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Exclude Device** on the right sidebar.

### Automatically Excluding Discovered Devices

You can choose to automatically exclude all newly discovered devices at a site.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site for which you want to exclude all newly discovered devices.
- 3 From the **More Actions** list, select **Auto-exclude newly discovered devices**.

### Creating Device Exclusion Rules to Exclude Devices

You can create exclusion rules that specify which device to exclude by identifying the DNS name, SNMP name, or MAC address. You can also exclude a device directly. See [Excluding Devices Directly](#).

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the device for which you want to turn monitoring off.
- 3 Click **Legacy Exclusion Rules**.
- 4 Click **New**.
- 5 Do any of the following:
  - In the **DNS Name** box, type the domain name for the device.
  - In the **SNMP Name** box, type the SNMP name for the device.
  - In the **MAC Address collected via WMI, SNMP, or SSH** box, type the MAC address for the device.

---

The Media Access Control address (MAC address) is a unique identifier assigned to most network adapters or network interface cards (NICs) by the manufacturer for identification.

- In the **MAC address collected via ARP** box, type the MAC address for the device, if it collected using ARP.

**Note:** The **MAC address collected via ARP** box is only available for Onsite Managers that have been upgraded to Managed Workplace 9.0 or higher.

- 6 Click **Save**.

## Viewing Excluded Devices and Returning them to Management

You can view a list of excluded devices for a site. The Excluded Devices screen displays devices that have been excluded from management.

You can return an excluded device to the scan.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the excluded devices that you want to view.
- 3 Click the number below **Excluded Devices**.
- 4 To return an excluded device to the scan, do the following:
  - a Select the check box beside the device.
  - b Click **Reinclude Device**.

## Viewing Exclusion Rules

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the device for which you want to turn monitoring off.
- 3 Click **Legacy Exclusion Rules**.
- 4 Click the name of an exclusion rules to view details.

## Deleting an Exclusion Rule to Return a Device to the Scan

You can turn off the exclusion rule and include the device in the scan.

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the device you want to return to the scan.
- 3 Click **Legacy Exclusion Rules**.
- 4 Select the check box that corresponds with the exclusion rule you want to delete.

---

5 Click **Delete**.

6 Click **Close**.

## About Deleting Devices

When you delete a device, you are deleting the records for that device in Service Center, but you are not preventing it from being discovered. If you don't want the device to be rediscovered, you can

- skip or delete its IP address from the scan range first
- delete and exclude to delete data from a device and exclude it from the scan

Devices that are deleted will no longer be referenced in Service Center or Onsite Manager 5 to 10 minutes after deletion. However, the devices may continue to be referenced in Service Center as unavailable devices for a short period of time.

## Down Devices

A down device is one that is unreachable and not responding to ICMP ECHO or other monitoring protocols, such as ARP cache retrievals. The device may be booted and online, but something is preventing a response. If the device is responding to ARP only, it is indicated with an asterisk. A device might respond to ARP only if, for example, it is a laptop that is turned off, but with a VPro chip that is responding to ARP.



Device Down icon



Device Down icon - responding to ARP but not ICMP ECHO or any other discovery protocol

When a device is not responding to the Onsite Manager discovery scan, Service Center continues to keep full asset, description and addressing information for the device until the specified interval triggers the next clean-up.

Even though a device may be down, you may not want to delete the device.

## What You Can Do

To ensure that the information you see in the dashboards and reports is fresh and accurate, you can

- delete down devices manually
- delete down devices automatically on a schedule after a specified period of inactivity

---

**Notes:**

- For customers that have transient systems periodically introduced to the environment by contractors, consultants, auditors or other external business partners, you can tag these devices as visitors so that they will not accidentally be confused with maintenance opportunities. To avoid these devices from showing up at all, configure a separate, unmonitored DHCP scope for visitors' equipment by using a wireless router.
- If you have a device that's been discovered that you want to exclude, you should exclude it and then wait a bit (to make sure that Onsite Manager is not sending any current information about it) and then delete the device.
- Devices that are monitored by a Device Manager agent must have the agent uninstalled before they can be deleted.

**To delete a device manually on the Onboarding Overview page**

- 1 In Service Center, click **Status > Onboarding Overview**.
- 2 Click the site that contains the device for which you want to turn monitoring off.
- 3 Select the check box that corresponds with the device you want to delete.
- 4 Click **More Actions > Delete**.

**To delete devices with a down status automatically**

You can modify the global interval for the removal of down devices.

**Notes:**

- If an IP address belongs to a server device, it is not deleted automatically.
- If an IP address belongs to a workstation device and the device is down for more than the allotted down device setting, it is deleted on the next scan. For domain environments, if a device is a Standalone Workstation or a Member Workstation, it is considered a workstation. For workgroup environments, if a device is XP, Vista or Windows 7, it is considered a workstation.

**Default:** 30 days for automatic removal

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site that contains the device you want to delete.
- 3 Click the **Configuration** tab.
- 4 In the **Down Device Threshold Settings** section, click **Modify**.



- 
- 5 Type a number of days a device must be consecutively down before it is automatically removed from the system.
  - 6 Click **Save**.
  - 7 Click **Close**.

**See Also**

[To delete a device manually on the Onboarding Overview page](#)  
[Setting How Long to Keep the Data](#)

## Running a Scan Manually

If you want to scan devices immediately, you can run a manual scan.

- 1 In Service Center, click **Site Management > Sites**.
- 2 In the **Site Name** column, click the site for which you want to perform a network scan.
- 3 Click the **Network Discovery** tab.
- 4 In the **Network Scan (Local Network)** section, click **Scan Now**.

The scanning process begins and once complete, the results appear in the **Scan Settings** section.

When the scan completes, check to ensure that each discovered device has at least one management protocol (such as WMI, SNMP or SSH) enabled. This allows Onsite Manager to accurately identify a device.

**See Also**

For more information about network discovery, see the *Setup Guide*.

## Running an MBSA Scan Manually

You will want to run the MBSA scan manually in the following scenarios:

- If you have just added new devices.
- If you have tried to resolve conditions that cause a “Check Not Completed” error, which means MBSA couldn't run against a machine for some reason.

Run the initial network scan before running an MBSA scan.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to run an MBSA scan manually.
- 3 Click the **Configuration** tab.

- 
- 4 In the **External System Integration** section, click **Scan Now**.

### **See Also**

[Setting When to Run an MBSA Scan](#)

## **Enabling or Disabling Power Management for a Site**

Using this procedure, you can enable or disable power management for more than one site.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check box beside the site or sites with which you want to work.
- 3 From the **More Actions** list, select either **Enable Power Management** or **Disable Power Management**.

## **Upgrading and Rebooting Onsite Managers**

### **Upgrading Onsite Managers across different sites**

You can upgrade Onsite Managers at every site, or you can choose to upgrade Onsite Managers at select sites.

- 1 In Service Center, click **Update Center > Products**.
- 2 Select the check box beside each site for which you want to upgrade Onsite Managers, or select the check box at the top to select all sites.
- 3 Click **Advanced Options**.
- 4 Select the **Update Onsite Managers for selected sites** check box.
- 5 Click **Update**.

For information about installing Onsite Manager, see the *Setup Guide*.

### **Rebooting Onsite Managers**

If a reboot is required during the installation or upgrading of Onsite Managers, and the reboot doesn't occur, you can force a reboot from Service Center. By forcing a reboot, a reboot script is run on the device and starts within a minute. The user will not have time to save any open work or be allowed to stop the reboot. Once the system reboots, the installation or upgrade completes.

- 1 In Service Center, click **Update Center > Products**.
- 2 Select the check boxes for the sites where you want Onsite Managers rebooted.
- 3 Click **More Actions**.

---

#### 4 Click **Reboot Onsite Managers in Pending Reboot.**

## Adding Device Managers to a Site

Device Manager is the functional equivalent of Onsite Manager but monitors and manages a single device only. There is a database, but it is bundled with the lightweight application. Device Manager communicates directly with Service Center.

When adding a Device Manager to a site, you must specify an AVG Device Manager for Windows or an AVG Device Manager for OS X.

**Note:** A device managed by Device Manager and on the same network as Onsite Manager will always be managed by Device Manager, not Onsite Manager.

### When to Use Device Manager

Device Manager can be installed on a roaming Windows or Mac laptop, a Windows Server that is out of reach of Onsite Manager, in an environment that doesn't have a server or peer-to-peer network, at kiosks, and so on.

### What You Can Do

You can quickly download and install Device Manager. You can also email the link to users who can install it with one click. Using an automated task, you can even push Device Manager to target devices (only if Onsite Manager is being used).

You can brand Device Manager with an icon that matches your company logo, strengthening your brand right on the managed devices. You can set up a customized right-click menu that gives end users the option to email or call your support team, browse your support network, or other similar options. See [Creating a Support Assistant Policy](#).

## Installing Device Managers

When you created the site, you had the choice to automatically deploy Device Managers to Windows and OS X laptops. See [Creating a Site in Service Center](#). After site creation, you can do any of the following:

- automatically deploy Device Managers to any laptops that have been added since site creation;
- email a Device Manager to a user to install;
- download Device Manager to a device.

---

When you email or download a Device Manager, you must specify either a Device Manager for Windows or a Device Manager for OS X.

The Device Manager installer requires data to be downloaded from Service Center. This means that Device Manager must have access to the Internet to install properly.

**Note:** You cannot install or deploy a Device Manager for OS X to a Mac device that has a web proxy configured.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site where you want Device Managers installed.
- 3 Click the **Device Manager** tab.
- 4 Do one of the following:
  - To automatically deploy Device Manager to laptops, click **Deploy Device Managers (via Onsite Manager)**. Use the filters to narrow down your selection, select the devices to which you want to deploy Device Manager, and click **OK**.
  - To download Device Manager to a device, click **Download** and select either **Windows Device Manager** or **OS X Device Manager**.
  - To email Device Manager to a user to install, click **Email** and select either **Windows Device Manager** or **OS X Device Manager**.

An email launches with the Device Manager download link. Optionally, you can edit the message to the following suggested text:

“Click to download and install the Device Manager utility that allows your computer to be remotely protected.”

The recipient must click the link in the email message and download and install Device Manager or save it to install later.

**Notes:**

- For Device Manager for Windows, because the file you’re sending is an .EXE file, the recipient may get a warning message that the file may be malware. You may want to include a note in your email to reassure the recipient that it is not malware.
- Device Manager for Windows is installed in the following location: <AVG>/Onsite Manager and its copy of OMDesktop.exe is located in the bin directory under Onsite Manager.
- Device Manager for OS X is sent as a .zip file. The user must unzip the file and run the MacDMSetup.pkg file.

---

## Searching for a Device Manager

You can use the Search box to quickly find a specific Device Manager.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site where you want to search for Device Manager.
- 3 Click the **Device Managers** tab.
- 4 In the **Search** box, type the search criteria.

You can search for Device Name, Last Logged-In User or Version to find the Device Manager with which you want to work.

- 5 Click **Search** or press **Enter**.



Search icon

**Tip:** To perform a global search, use the **Device Search** page. See [Searching for a Device](#).

## Updating Device Managers

You can update Device Managers at one or more sites, using the Update Center. When you update Device Managers, both types of Device Managers (for Windows and for OS X) are updated.

- 1 In Service Center, click **Update Center > Products**.
- 2 Select the check boxes for the sites where you want Device Managers upgraded.
- 3 Click **Advanced Options**.
- 4 Select the **Update Device Managers for selected sites** check box.
- 5 Click **Update**.

**Note:** The end user must log off and log in again to complete the upgrade.



If an update fails, logs provide notification. If a Device Manager upgrade fails, there is an indication on the Device Manager page that it failed.

To see the reason why the failure occurred, hover your mouse over the icon.

---

## Rebooting Device Managers

If a reboot is required during the installation or upgrading of Device Managers, and the reboot doesn't occur, you can force a reboot from Service Center. By forcing a reboot, a reboot script is run on the device and starts within a minute. The user will not have time to save any open work or be allowed to stop the reboot. Once the system reboots, the installation or upgrade completes.

### To reboot all Device Managers at more than one site

- 1 In Service Center, click **Update Center > Products**.
- 2 Select the check boxes for the sites where you want Device Managers rebooted.
- 3 Click **More Actions**.
- 4 Click **Reboot Device Managers in Pending Reboot**.

### To reboot specific Device Managers at one site

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site where you want to reboot Device Managers.
- 3 Click the **Device Managers** tab.
- 4 Select the check boxes for the Device Managers you want to reboot.
- 5 Click **More Actions**.
- 6 Click **Reboot Device Managers in Pending Reboot**.

## Uninstalling Device Managers

You can uninstall Device Manager from within Managed Workplace or from the device's Control Panel using remote control.

**Note:** When uninstalling Device Manager from an OS X device, you must uninstall from the application folder where Device Manager was installed. If you attempt to uninstall from the Download (.zip) folder, the uninstall may fail due to security settings on the system.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site where you want Device Managers uninstalled.
- 3 Click the **Device Manager** tab.
- 4 Select the check boxes for the Device Managers you want to uninstall.
- 5 Click **More Actions**.

- 
- 6 Select **Uninstall Device Manager**.

**Note:** If you uninstall Device Manager from the device and then delete the device from Service Center, and then re-install Device Manager, it will not show up until the device is first cleared in Onsite Manager.

## Working with Sites

### Viewing an Overview about a Site

On the **Site Overview** page, you can get a summary view about a specific site, including site information, service plan information, contact information, service module information (if applicable), maintenance schedules currently running on the site, and more. Using the right sidebar, you can quickly access other information about the site.

Service plans are applied to a site on the **Site Overview page**. For more information about viewing and converting the service plan model for a site, see [Applying Service Plans to Existing Sites](#).

#### To view an overview about a site

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.

Depending on the site, the information available to view varies.

#### To view devices at a site by device type

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.
- 3 In the **Network Overview** area, click the number beside any of the following device types:
  - **Device Count** (to view all devices)
  - **Devices Down**
  - **Servers**
  - **Workstations**
  - **OS X**
  - **Printers**
  - **VM Guests**

- 
- **Linux/Unix**
  - **Excluded Devices**

#### **To view the status of automated tasks for a site**

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.
- 3 Click **Automation Calendar** on the right sidebar.

## **Viewing Alerts for a Site**

You can view a list of alerts for a site, including the device or web site that is generating the alert, the alert configuration, and alert category.

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.
- 3 Click **Site Alerts** on the right sidebar.

## **Viewing Devices at a Site**

The Devices page gives you a quick summary of the devices at a site, including the total number of devices, the number of down devices, and the number of active alerts. You can click on a device name to open the device Overview page to view more details.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 Click **Devices** on the right sidebar.

## **Viewing and Changing the Service Plans and Services Applied to a Site**

The **Site Overview** page display which service plans and services have been applied to a site. You can

- view the service plan applied to a site
- apply a different service plan to a site, or change the service delivery model
- view the services that were manually applied to a site, and add more services
- delete manually-applied services from a site



---

### To view the service plan applied to a site

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 The **Service Plan Application** section displays the service plan.

### To change the service plan applied to a site

You can change the service plan that has been applied to a site. For example, if you upsell a customer to a more comprehensive service plan, you can simply apply the service plan from the **Site** page to automatically implement the more comprehensive services.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 In the **Service Plan Application** section, click the gear icon.
- 4 Click the chevron beside the site name.
- 5 Click **Modify**.
- 6 Select a new service plan from the list.
- 7 Click **Save**.

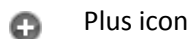
### To view the additional services applied to a site

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 The **Additional Services** section lists all of the services that have been manually applied to the site (i.e., not automatically applied via a service plan). Optionally, click a service name to open the **Service** page.

### To apply a service to a site

You can manually apply a service directly to a device.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site.
- 3 In the **Additional Services** section, click the plus icon.



- 4 Select the check box beside each service you want to add.

- 
- 5 Click **Add**.

### To delete a service that was manually applied to a site

When a service was manually applied to a site, you can remove it from the site at any time.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 In the **Additional Services** section, click the delete icon beside the manually-applied service you want to remove.



Delete icon

## Changing the Service Delivery Model for a Site

You can convert the service delivery model currently in use at a site. For example, if you have an existing site that does not have a service plan applied, from the **Site** page you can select a service plan to apply to the site, or select service plans to apply to groups at the site.

You can also remove service plan application from a site entirely, although this is not recommended as a best practice.

For more information on choosing a service delivery model, see [Determining a Service Delivery Model](#).

### To apply a single service plan to the site

- 1 In Service Center, click **Dashboards**.
- 2 If the Services Dashboard is your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Service Plan Application** area, click the gear icon.
- 5 In the **Manage Service Plan Application** area, click the gear icon to convert the site to a different service plan delivery model.
- 6 Select the **Apply a single Service Plan to all devices in this Site** option button. Then, click the pencil icon to activate a list of all available service plans. Select a service plan from the list and click **OK**.
- 7 Click **Convert**.

- 
- 8 A pop-up appears warning you that the current service plan configuration will be lost and cannot be restored. Click **Remove Configuration and Convert**.

### To apply service plans to groups at the site

- 1 In Service Center, click **Dashboards**.
- 2 If the Services Dashboard is your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Service Plan Application** area, click the gear icon.
- 5 In the **Manage Service Plan Application** area, click the gear icon to convert the site to a different service plan delivery model.
- 6 Select the **Apply Service Plans directly to groups** option button.
- 7 Click **Convert**.
- 8 A pop-up appears warning you that the current service plan configuration will be lost and cannot be restored. Click **Remove Configuration and Convert**.
- 9 Now you will apply service plans to groups. Click the **Apply Service Plan to a new Group** link.
- 10 Select a group from the list.
- 11 In the **Service Plan Applications** area, for the group you just added, select a service plan from the list.
- 12 Click **Save**.
- 13 Repeat steps 9 to 11 for each group to which you want to apply service plans.

### To remove service plan application from a site

- 1 In Service Center, click **Dashboards**.
- 2 If the Services Dashboard is your default dashboard, click the **Central Dashboard** icon.
- 3 Click the name of a site.
- 4 In the **Service Plan Application** area, click the gear icon.
- 5 In the **Manage Service Plan Application** area, click the gear icon to convert the site to a different service plan delivery model.

- 
- 6 Click the **Do not use a Service Plan for this site, I'll configure the site manually** button.
  - 7 Click **Convert**.
  - 8 A pop-up appears warning you that the current service plan configuration will be lost and cannot be restored. Click **Remove Configuration and Convert**.

## Viewing and Changing the Execution Schedules Applied to a Site

### To view the execution schedule applied to a site

The **Applied Schedules** section of the **Site Overview** page displays the execution schedule that was applied to the site.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 The **Applied Schedule** section displays the execution schedule applied to the site. Optionally, click the execution schedule name to open the **Schedules** page, where you can view and modify the schedule settings.

### To change the execution schedule applied to a site

You can change the execution schedule that is applied to the site. If no execution schedule has been applied, you can add one to the site.

- 1 In Service Center, click **Dashboards**.
- 2 Click the name of a site
- 3 In the **Applied Schedule** section, click the **Change Schedule** icon:



- 4 In the **Applied Schedules** list, select a schedule from the list.  
The **Schedule Details** section updates to display the schedule settings for the newly selected schedule.
- 5 Click **Save**.

## Putting a Site on Hold

Putting a site on hold means that Onsite Managers and Device Managers are no longer collecting information, no automation or patch management occurs, and no remote control sessions can be initiated.

---

**Caution:** Report delivery schedules may be lost if a site is put on hold and then approved again.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check box beside the site you want to put on hold.
- 3 Click **Put On Hold**.

## Approving a Site After It's Been On Hold

When Onsite Manager has been installed at a customer site, it appears as a site in Service Center.

**Default:** Sites have an approved status.

Approving a site means Onsite Manager or Device Manager is functioning and using a license.

If you've put a site on hold, you can approve it.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check box beside the site you want to approve.
- 3 Click **Approve**.

## Deleting a Site

Deleting a site means all data for the site is deleted.

**Caution:** All data for the site is deleted immediately and is not recoverable without a database restore.

**Note:** If a Device Manager-only site is deleted, all Device Managers are uninstalled.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check box beside the site you want to delete.
- 3 Click **Delete**.

## Adding Consent to a Site

An option to add consent within Premium Remote Control is available for sites where sensitive information could potentially be accessible. This is a configurable item on a per-Site basis.

If consent is required, your customer is presented with a window to allow or reject the access.

---

**Note:** You can customize your consent message presented to your client.

### Setting Default for New Sites

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click **Premium Remote Control > Set default for new sites**.
- 3 Set your desired default:
  - Default values for consent
  - Default action on timeout
  - Default timeout value

### Changing Consent Settings for a Site

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click **Premium Remote Control Section > Modify**
- 3 Make changes to the consent settings
- 4 Click **Save**.

**Note:** Changes to the Premium Remote Control consent settings can take a few minutes depending on the number of devices in the site

### Premium Remote Control access to a device requiring consent

- 1 Launch Premium Remote Control (via Remote Control page of the device or the Quick Connect link).
- 2 Premium Remote Control is launched on your computer.
- 3 A message window is presented to the customer, indicating that access is being requested.
- 4 The customer allows access.
- 5 You are now connected to the device.
- 6 The session is successfully initiated.

## Viewing Information about a Site

You can view information about a site, such as the installed version of Managed Workplace, the installation date, the Global Unique Identifier (GUID) and public IP address for Onsite Manager. The GUID provides a unique

---

reference number for the software and is used for troubleshooting and setting up integrations with some third-party professional services automation (PSA) systems. You can also view version information about Managed Workplace.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to view the information.

## Changing Contact Information for a Site

You can add attributes about the site to identify it. Use the notes section to record temporary, low-priority information. You could also use the notes to store important high-priority information, such as the following:

- Internet Service Provider including support and sales contact information and account access details
- premises access instructions
- next quarterly business review date

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to change the contact information.
- 3 In the **Details** section, click **Modify**.
- 4 Make the required changes.
- 5 Click **Save**.

## Viewing the Physical Location of a Site on a Map

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to view its map location.
- 3 In the **Details** section, click **View Map**.

## Adding Notes about a Site

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site for which you want to add notes.
- 3 Click **Add Notes**.
- 4 Add a comment or note.
- 5 Click **Save**.

---

## Setting Site Options

### Setting Premium Remote Control Options

AVG Business Premium Remote Control uses ISL Light technology to connect remotely to managed devices, allowing you to file transfer, chat, and perform various administrative functions as you resolve issues remotely. AVG Premium Remote Control requires minimum configuration; the account credentials are automatically created when you enable it in System Settings, and the agent is automatically deployed to all managed devices.

For any site, you can set the option to install Premium Remote Control automatically on all devices when they are added to the site. This will not install Premium Remote Control on existing devices, only on new devices as you add them to the site.

You also have the option to enable consent, which requires the end user to give consent for remote access. If you enable consent, when a technician starts a Premium Remote Control session, your customer is presented with a window to allow or reject the access. The Notification Timeout is the number of seconds that the customer has to respond before the request times out. If the request times out, the session will either allow or reject the connection, depending on the default option you choose.

You can add a custom consent message that will be displayed to the customer when you request a Premium Remote Control connection.

**Best Practice:** For sites where your customers may be working on critical tasks that cannot be interrupted or sensitive information that cannot be shared, enable the require consent option and set the default to Reject.

#### To Set a Site to Install Premium Remote Control on New Devices Automatically

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.
- 4 In the **Premium Remote Control** section, click **Modify**.
- 5 Select the **Automatically Install Premium Remote Control** check box.
- 6 Click **Save**.



---

## To Set Multiple Sites to Install Premium Remote Control on New Devices Automatically

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check boxes beside the sites where you want to install **Premium Remote Control**.
- 3 Click **Premium Remote Control > Automatically install Premium Remote Control**.

## To Turn off Automatically Install Premium Remote Control

- 1 In Service Center, click **Site Management > Sites**.
- 2 Select the check boxes beside the site or sites you want to change.
- 3 Click **Premium Remote Control > Do not automatically install Premium Remote Control**.

## To Require Consent for Premium Remote Control Sessions

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.
- 4 In the **Premium Remote Control** section, click **Modify**.
- 5 Select the **Require Consent** check box.
- 6 In the **Default** area, select one of the following option buttons:
  - **Allow**—Allows Premium Remote Control access if the user does not respond before notification timeout.
  - **Reject**—Rejects Premium Remote Control access if the user does not respond before notification timeout.
- 7 In the **Notification Timeout** box, type a number.
- 8 Optionally, type a message in the **Custom Consent Message** box.
- 9 Click **Save**.

## Setting When to Run an MBSA Scan

Microsoft Baseline Security Analyzer (MBSA) is a utility that audits the security on Windows operating systems and applications and checks all IP addresses defined in Onsite Manager.

---

**Best Practice:** By default MBSA scans are configured to run every Wednesday at 12:30 p.m. The default was chosen because mid-week is the most likely time for all workstations to be powered on and available. To ensure you have security data available as soon as possible, you should manually run the first scan. If you focus on security services, you may want to keep MBSA scans running on a weekly basis, and monitor the results. However, you may want to schedule the scan less frequently once you have established a security baseline and brought up the overall security score as shown in the Executive Summary report.

The MBSA Install Path is detected and populated during installation. Unless the location of the MBSA installation changes, the path should not be changed.

**Notes:**

- The MBSA data collected by Onsite Manager is uploaded to Service Center using an offset so that not all report data is submitted at the same time. This avoids impacting the bandwidth between Onsite Manager and Service Center.
- If MBSA is not already installed on Device Manager, then the MBSA scan will not be executed for that device.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.
- 4 In the **External System Integration** section, click **Modify**.
- 5 In the **MBSA Security Scanning** section, select either the **Weekly** or **Monthly** option button.
- 6 Select the day of the week or day of the month to run the MBSA scan.
- 7 Select the time to run the MBSA scan.
- 8 Click **Save**.

**See Also**

[Running an MBSA Scan Manually](#)

## Setting When to Delete Down Devices

You can enter a number of days a device must be consecutively down before it is automatically deleted from the system.

Basic identity information is retained so that in the event the device is rediscovered at a later date, the original configuration will be restored.

---

**Default:** 30 days for automatic removal

**Notes:**

- Mobile devices and computers with Device Manager installed are not affected by the device down threshold. The agent must be uninstalled for the monitoring to stop.
- If an IP address belongs to a server device, it is not deleted.
- If an IP address belongs to a workstation device and the device is down for more than the allotted down device duration, it is deleted on the next scan. For domain environments, if a device is a Standalone Workstation or a Member Workstation, it is considered a workstation. For workgroup environments, if a device is XP, Vista or Windows 7, it is considered a workstation.

**To set how many days before a device is automatically deleted from a site**

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.
- 4 In the **Down Device Threshold Settings** section, click **Modify**.
- 5 Type the number of days a device must be consecutively down before it is automatically deleted from the system.
- 6 Click **Save**.

## Setting the Website Addresses to Use to Determine Internet Availability

You can specify which websites to use to determine if the network is down or unable to access the Internet. By specifying more than one website, you ensure that the Internet is down and not just the one website.

By default, the following two high availability websites are automatically entered during the Onsite Manager installation process:

`http://www.yahoo.com/`, `http://www.google.com/`

**Note:** This is the ability of Onsite Manager to see the Internet only.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.

- 
- 4 In the **Internet Availability Monitoring** section, click **Modify**.
  - 5 In the **Site URLs** box, type a URL to use as the website that determines internet availability.  
To enter more than one website address, separate them with a comma.
  - 6 Click **Save**.

## Setting the Polling Interval for Printer Monitoring

You can specify how often you want Managed Workplace to poll for printers.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Configuration** tab.
- 4 In the **Printer Monitoring** section, click **Modify**.
- 5 Editing the polling interval.
- 6 Click **Save**.

## Setting Site-Specific Options for Power Management

[Enabling or Disabling Power Management for a Site](#)

[Enabling or Disabling Power Management for a Device](#)

[Overriding the Default Power Costs and Usages at a Site](#)

[Creating a Baseline of Power Management Data for Comparisons](#)

## Setting Alerting Actions for Site Communication Failures

You can set alert actions for a site not communicating at both the system level and by site. It is recommended that you first set your system-level defaults, and then override these defaults as needed on the site level. For more information about setting system-level alert actions for site not communicating, see [Setting System-Wide Alerting Actions for Site Communication Failures](#).

Managed Workplace includes three alerts that notify you of site communication failures:

- **Service Center Receive**—triggers when Service Center has not received information from an Onsite Manager for 65 minutes.

- **Onsite Manager Processing**—triggers when 12 hours has passed since an Onsite Manager has retrieved information, such as configuration changes, from Service Center.
- **Site Not Communicating**—status and asset information is sent to Service Center every two minutes. When two updates have been missed, and the alert conditions for both Service Center Receive and Onsite Manager Processing are met, this alert is triggered.

These three alerts form a hierarchy in which the Service Center Receive and Onsite Manager Processing alerts are subsets of the Site Not Communicating alert. The two lower-level alerts can exist simultaneously. However, if two updates have been missed in addition to the conditions required to trigger the lower-level alerts, then the Site Not Communicating alert triggers. The lower-level alerts self-heal, as they are subsumed by the Site Not Communicating alert.

The following table outlines which alerts are triggered for various combinations of site communication failure conditions:

What if...	Then...
Service Center has not received information from Onsite Manager for 65 minutes	the Service Center Receive alert is triggered.
12 hours has passed since an Onsite Manager has retrieved information from Service Center	the Onsite Manager Processing alert is triggered.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center	both the Service Center Receive and Onsite Manager Processing alerts are triggered.
Service Center has not received information from Onsite Manager for 65 minutes and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.

---

What if...	Then...
12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.

---

**Default:** For each alert type, Managed Workplace creates a trouble ticket and sends an email to all users for the site whose role is set to receive alert notifications. The alerts are also set to self-heal, by default.

**Notes:**

- This option is not available for a site based on Device Managers.
  - The pager feature is only available for on-premise Service Centers with a modem installed on the application server.
- 1 In Service Center, click **Site Management > Sites**.
  - 2 Click the site you want to edit.
  - 3 Click the **Alert Configuration** tab.
  - 4 In the **Site Not Communicating Alert Configuration** section, clear the **Use System Defaults** check box.
  - 5 Click **Modify**.
  - 6 Do the following to change the default alert configuration:
    - To add an alert category when a site is not communicating so that it appears on the **Central Dashboard**, click **Categorize Alert** and add a category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.

- 
- To create a trouble ticket when a site is not communicating, select the **Create Trouble Ticket** check box.
  - To send an email when a site is not communicating, select the **Send Email** check box and configure the settings.
  - To call a pager when a site is not communicating, select the **Call Pager** check box and click **Call Pager**. Select the **All Users for the Site Whose Role is Configured to Receive Pager Alerts** option button. Click **Save**.
  - To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.
- 7 Repeat steps 1 to 6 as needed to configure the alert actions for the Service Center Receive and Onsite Manager Processing alerts.
  - 8 Click **Save**.

#### See Also

[Setting Alert Actions](#)

[Creating Alert Categories](#)

## Setting Alerting Actions for New Devices for a Site

By default, Service Center performs a device discovery network scan on sites every 5 minutes. You can configure an alerting action to notify you when new devices are discovered as the result of the network scan.

**Best Practice:** It is recommended that you first set the system-wide alert actions for new devices, and then override the system defaults on a per-site basis, as required. See also [Setting System-Wide Alerting Actions for New Devices](#).

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **New Device Alert Configuration** area, clear the **Use System Defaults** check box.
- 4 Click **Modify**.
- 5 Ensure that the **Enable New Device Alert** check box is selected.
- 6 Do the following to change the alert configuration:
  - To add an alert category when a new device is discovered so that it appears on the **Central Dashboard**, click **Categorize Alert** and add a

---

category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.

- To create a trouble ticket when a new device is discovered, select the **Create Trouble Ticket** check box.
- To send an email when a new device is discovered, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.
- To call a pager when a new device is discovered, select the **Call Pager** check box and click **Call Pager**. Select the **All Users for the Site Whose Role is Configured to Receive Pager Alerts** option button. Click **Save**.

**Note:** The **Call Pager** check box is only available if you are using an On Premise version of Service Center.

- To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.

7 Click **Save**.

### See Also

[Setting Alert Actions](#)

[Creating Alert Categories](#)

[Setting the Device Discovery Defaults](#)

## Setting Alert Actions for Loss of Monitoring Protocol at a Site

You can set site-wide alert actions that are triggered when WMI or SNMP ceases to work on a device. This alert determines that monitoring has stopped on a device, and that the monitoring protocol has failed. You can then investigate the root cause of the failure and resolve the problem.

This site-wide setting overrides the system default. See [Setting System-Wide Alerting Actions for Loss of Monitoring Protocol](#).

**Note:** When you choose to override the system default, any existing Loss of Monitoring Protocol alerts for the site are cleared. After saving the site-level configuration, if the condition persists, the alerts will be re-triggered within 10 minutes.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of a site.
- 3 Click the **Alert Configuration** tab.



- 
- 4 In the **Loss of Monitoring Protocol Configuration** area, clear the **Use System Defaults** check box.
  - 5 Click **Modify**.
  - 6 Do the following to change the alert configuration:
    - To add an alert category when the monitoring protocol drops on a device so that it appears on the **Central Dashboard**, click **Categorize Alert** and add a category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.
    - To create a trouble ticket when a monitoring protocol is dropped, select the **Create Trouble Ticket** check box.
    - To send an email when a monitoring protocol is dropped, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.
    - To call a pager when a monitoring protocol is dropped, select the **Call Pager** check box and click **Call Pager**. Select the **All Users for the Site Whose Role is Configured to Receive Pager Alerts** option button. Click **Save**.

**Note:** The **Call Pager** check box is only available if you are using an On Premise version of Service Center.

    - To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.
  - 7 Click **Save**.

## Modifying the Alert Configurations

You can modify the alert configuration for site-wide alerts.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the site you want to edit.
- 3 Click the **Alert Configuration** tab.
- 4 Under the title of the alert you want to configure, click **Modify**.
- 5 Make changes to the alert configuration.
- 6 Click **Save**.

---

## Setting the Device Discovery Defaults

**Note:** This option is applicable for both a site based on Device Managers and one based on Onsite Managers.

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to edit the scan settings.
- 3 Click the **Network Discovery** tab.
- 4 In the **Discovery Settings** section, click **Modify**.
- 5 Edit the boxes as required.

**Device Discovery** Specifies how long Managed Workplace will wait after completing the last network scan before starting again. Increasing this value past the default 5 minutes extends how long a device can be unresponsive without Managed Workplace being aware.

**Asset Discovery** Specifies the maximum length of time Managed Workplace will take to poll the hardware and software assets on all the discovered devices. Managed Workplace distributes the scan for all the devices over the entire period allotted. You can safely increase this value from the default 4 hours if little change is likely to occur on the network.

- 6 Click **Save**.

## Managing Site Credentials

If a site includes devices that are outside of the MWService account scope, you can provide credentials for specific technologies and management protocols to ensure all devices are effectively managed. For example, you can provide SSH credentials to manage Mac devices on the network, and for devices managed with SNMP v3, you can provide authentication and privacy protocols.

For each credential type, you can create one site default credential set, and then create as many device override credential sets as required. For example, you can create a default SNMPv3 credential set, and then create a device override SNMPv3 credential set for a device that requires different credentials. You do not have to create a site default for every possible authentication scheme, but you do have to create a site default before you create a device override.

You can delete default credential sets, except for the default Windows credential set. Also, a default credential set cannot be deleted if there is a device level override credential set for the same authentication scheme.

---

## To create a credential set for SNMP versions 1 and 2

An SNMP community string is a text string that is in effect a credential. It is used to authenticate communication with the SNMP device.

By default, Managed Workplace uses public as the community string to locate SNMP devices on the network. However, many companies use a unique community string that acts like a strong password against brute-force attack. Other common community strings are private and admin.

A default SNMP credential set can contain more than one community string. If there is a mix of devices across the network that require one of two community strings, it is possible to specify more than one community string by separating the string with commas and no spaces. For example, `public,private`.

If one of the devices is SNMP-enabled, but is not showing up in the scan, it may be because a different community string was set up for security reasons.

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to provide credentials.
- 3 Click the **Credentials** tab.
- 4 Click **Add**.
- 5 Select **SNMP from the Credential Type** list.
- 6 In the **Community Strings** box, type the SNMP community string.  
**Note:** Community strings are case-sensitive. For example, *Public* and *public* would be separate communities of SNMP devices.
- 7 Optionally, type a description in the **Notes** box.
- 8 Do one of the following:
  - Select the **Default** option button to make this the default SNMP v1 and v2 credential set for this site.
  - Select the **Device override** option button, and then click **Add** to select the devices to which you want to apply this credential set.
- 9 Click **Save**.

## To create a credential set for SNMP version 3

When setting up a credential set for SNMP version 3, you must select the authentication and privacy protocols that the target devices are configured to use.

- 1 In Service Center, **Site Management** > **Sites**.

- 
- 2 Click the site for which you want to provide credentials.
  - 3 Click the **Credentials** tab.
  - 4 Click **Add**.
  - 5 Select SNMPv3 from the **Credential Type** list.
  - 6 In the **User Name** box, type the user name that was configured with snmp-server host.
  - 7 Optionally, specify an SNMP context in the **Context** box.
  - 8 In the **Authentication** area, from the **Algorithm** list, select an authentication protocol.
    - If you selected MD5 or SHA, provide the password in the **Password** and **Confirm Password** boxes.
  - 9 In the **Privacy** area, from the **Algorithm** list, select a privacy protocol.
    - If you selected DES or AES, provide the password in the **Password** and **Confirm Password** box.
  - 10 Optionally, type a description in the **Notes** box.
  - 11 Do one of the following:
    - Select the **Default** option button to make this the default SNMPv3 credential set for this site.
    - Select the **Device override** option button, and then click **Add** to select the devices to which you want to apply this credential set.
  - 12 Click **Save**.

### To create a credential set for SSH

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to provide credentials.
- 3 Click the **Credentials** tab.
- 4 Click **Add**.
- 5 Select SSH from the **Credential Type** list.
- 6 In the **User Name** box, type the SSH user name.
- 7 In the **Password** and **Confirm Password** box, type the SSH password.
- 8 Optionally, type a description in the **Notes** box.
- 9 Do one of the following:

- 
- Select the **Default** option button to make this the default SSH credential set for this site.
  - Select the **Device override** option button, and then click **Add** to select the devices to which you want to apply this credential set.

**10** Click **Save**.

### To create a credential set for VMware vSphere

You can create a VMWare vSphere credential set to connect to a VMWare host, which runs a web service that Managed Workplace uses to collect virtual machine asset information. To obtain the VMWare host user name and password, contact the VMWare administrator.

- 1** In Service Center, **Site Management > Sites**.
- 2** Click the site for which you want to provide credentials.
- 3** Click the **Credentials** tab.
- 4** Click **Add**.
- 5** Select VMware vSphere from the **Credential Type** list.
- 6** In the **User Name** box, type the user name to connect to the VMWare host.
- 7** In the **Password** and **Confirm Password** box, type the VMware host password.
- 8** Optionally, type a description in the **Notes** box.
- 9** Do one of the following:
  - Select the **Default** option button to make this the default VMware vSphere credential set for this site.
  - Select the **Device override** option button, and then click **Add** to select the devices to which you want to apply this credential set.
- 10** Click **Save**.

### To create a credential set for VNC Screen Share

VNC Screen Share allows you to remotely access an OS X device. This credential is required before you can run the OS X Prep Utility on a Mac device, which prepares the device for management. When you run the OS X Prep Utility, VNC is enabled on the device using the password you provide here. Any existing VNC password on the device is overwritten. See [To run the OS X Prep Utility](#).

- 1** In Service Center, **Site Management > Sites**.
- 2** Click the site for which you want to provide credentials.

- 
- 3 Click the **Credentials** tab.
  - 4 Click **Add**.
  - 5 Select VNC Screen Share from the **Credential Type** list.
  - 6 In the **Password** box, type the password to access the VNC Screen Share tool.
  - 7 Retype the password in the **Confirm Password** box.
  - 8 Optionally, in the **Notes** box, you can provide notes about the VNC Screen Share setup.
  - 9 Click **Save**.

### To create a credential set for Windows

The MWSservice service account is the default Windows credential set, and cannot be edited or deleted. You can create a device override Windows credential set for standalone or workgroup devices.

To create a Windows credential set, provide the domain name, and the user name and password for the domain administrator account.

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to provide credentials.
- 3 Click the **Credentials** tab.
- 4 Click **Add**.
- 5 Select Windows from the **Credential Type** list.
- 6 In the **Domain** box, type the Windows domain name.
- 7 In the **User Name** box, type in the domain administrator user name.
- 8 In the **Password** and **Confirm Password** box, type the domain administrator password.
- 9 Select the **Device override** option button, and then click **Add** to select the devices to which you want to apply this credential set.
- 10 Click **Save**.

**Note:** Windows credential sets are also used to communicate with Microsoft Hyper-V host systems.

### To modify a credential set

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to modify a credential set.

- 
- 3 Click the **Credentials** tab.
  - 4 Click the name of the credential set you want to modify.
  - 5 Make changes to the credential set.
  - 6 Click **Save**.

#### To delete a credential set

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the site for which you want to delete a credential set.
- 3 Click the **Credentials** tab.
- 4 Select the check box beside the credential set you want to delete.
- 5 Click **Delete**.

## About Updating Service Center

### About Using Update Center

Service Center includes the Update Center, which allows you to install updates to the following:

- Service Center *products*, including Onsite Manager, Device Manager, Support Assistant, and AVG AntiVirus Client.
- Service Center *components*, including monitoring policies, service modules, automated task scripts, reports, printer transforms, and service desk modules.

When new components and updates to products and components become available, an icon appears beside Update Center in the navigation pane:



This icon indicates that a new or updated item has been added to Update Center.

You can expand the Update Center menu item to determine whether there are available component updates, product updates, or both.

**Note:** Service Center updates are provided through a notification link, which brings you to the partner portal to download a new Service Center package. For more information, see [About Updating Service Center](#).

---

## Viewing Notifications for Product Updates

On the Product Updates page, you can view a summary of the sites for which there is a newer version of Onsite Manager, Device Manager, Support Assistant, or AVG AntiVirus client available.

You can sort the list of sites to view only the sites for which there is an update available, or you can sort sites by the current update status to see the updates that are in progress and those that have completed.

### To view an overview of available product updates

- 1 In Service Center, click **Update Center > Products**.

### To sort the list of available updates

- 1 In Service Center, click **Update Center > Products**.
- 2 Click one of the following icons to sort the list of product updates:



Sorts to show the sites for which there is an upgrade available.



Sorts the sites by update status, which can be any of the following:

- Failed
- No Response
- Pending
- Pending Reboot
- Prerequisite Check Failed
- Primary Installer Retrieved
- Secondary Installer Retrieved
- Succeeded

### To view a history of Onsite Manager installations for a site

- 1 In Service Center, click **Update Center > Products**.
- 2 For each site, you can hover over the clock icon in the **History** column to see a history of Onsite Manager installations.



Hover the cursor over the clock icon to display the Onsite Manager Installation History.



---

### To view more information about the Device Managers or Support Assistants at a site

- 1 In Service Center, click **Update Center > Products**.
- 2 In the **Device Managers** or Support Assistants column, click the number link for the site you want to view more information.

The **Site Management** page opens to either the **Device Managers** tab or the **Support Assistants** tab, depending on the column you clicked.

### To view more information about the AVG AntiVirus clients at a site

- 1 In Service Center, click **Update Center > Products**.
- 2 In the **AVG AntiVirus Clients** column, click the number link for the site you want to view more information.

The **Devices With AntiVirus Installed** page opens to list the devices at the site with AVG AntiVirus client installed. You can then select the check box beside each device you want to update, and then click the **Update** link. For more information about managing AVG AntiVirus in Managed Workplace, see [About AVG AntiVirus in Managed Workplace](#).

## Updating Managed Workplace Products

Service Center products include Onsite Manager, Device Manager, Support Assistant, and AVG AntiVirus client. When updates are available, a green icon appears beside Update Center > Products in the navigation pane.

You can update all Service Center products across all sites, or you can select which products to update at certain sites. Update Center also allows you to quickly identify sites with unsupported versions of Service Center products, which are indicated with a red icon:




Indicates an unsupported version

An unsupported version is defined as a Service Center product that is more than 2 versions previous to the current version of Service Center. When a Service Center product is unsupported, it is not tested for use with the current version of Service Center and might not function at full capacity.

**Note:** When a Support Assistant device is not connected, Service Center buffers the upgrade script until that device reconnects.

### To update Service Center products

- 1 In Service Center, click **Update Center > Products**.

- 
- 2 Do one of the following:
    - To update all sites, select the check box in the header row.
    - To update sites with unsupported versions, select the check box beside each site with an unsupported version icon .
  - 3 Optionally, you can apply updates by component type, by clicking **Advanced Options** and selecting any of the following check boxes:
    - **Update Onsite Managers for selected sites**
    - **Update Device Managers for selected sites**
    - **Update Support Assistants for selected sites**
    - **Update AVG AntiVirus Clients for selected sites**
  - 4 Click **Update**.

### See Also

[Upgrading and Rebooting Onsite Managers](#)

[Updating Device Managers](#)

[To upgrade Support Assistant on one or more devices](#)

## Updating Service Center

Service Center updates are announced in MW Wire, a messaging banner that runs along the top of Service Center.

### To update Service Center

- 1 Click the Service Center update notification link in MW Wire to access the AVG Partner Portal release page.
- 2 From the portal, you can download the Service Center installation package.

For more information on updating Service Center, including detailed steps on running the Service Center installation package, see the *Managed Workplace Setup Guide*, available in the partner portal.

**Note:** If you are using a hosted version of Service Center, you will be notified via MW Wire of available Service Center updates, however your hosting provider is responsible for installing Service Center updates.

---

## Updating and Installing Service Center Components

Update Center provides a means for you to install new components and component updates from within Service Center, without the need to access the Partner Portal for downloads or to import components locally. You can install the following components:

- monitoring policies
- service modules
- reports
- automation (scripts and automation packages)
- printer transforms
- service desk modules

## Viewing a List of Available Components

The Components page allows you to view new components available for install, currently installed components, and available updates to currently installed components:

You can further filter the list by component type, such as monitoring policy or report, by selecting a component type from the list in the Type column.

For some components, Update Center provides a link to a release notes page to provide you with further details before you install. For example, the release notes for a monitoring policy includes the version number, the minimum required version of Service Center, and a description of the monitoring and alerting performed by the monitoring policy. When a release note is available, the component's Description column includes a More Info link that opens the release notes in a browser tab.

**Note:** The Components page only shows available updates for the components currently installed in Service Center.

### To view new components available for installation

- 1 In Service Center, click **Update Center > Components**.
- 2 Click **Get More**.
- 3 Optionally, filter the list by selecting a component type from the **Type** list.

### To view component updates available for installation

- 1 In Service Center, click **Update Center > Components**.

- 
- 2 Click **Updates**.
  - 3 Optionally, filter the list by selecting a component type from the **Type** list.

### To view currently installed components

For verification purposes, you can view a list of the currently installed components in Service Center

- 1 In Service Center, click **Update Center > Components**.
- 2 Click **Installed**.

### To install a new component or component update

- 1 In Service Center, click **Update Center > Components**.
- 2 Do one of the following:
  - To install a new component, click **Get More**.
  - To install a component update, click **Updates**.
- 3 Optionally, filter the list by selecting a component type from the **Type** list.
- 4 Select the check box beside the new component or component update you want to install.
- 5 Click **Install**.

### To view release notes for a component

- 1 In Service Center, click **Update Center > Components**.
- 2 Do one of the following:
  - To view available components, click **Get More**.
  - To view component updates, click **Updates**.
- 3 In the **Description** column for a component, click the **More Info** link.

### To search for a component

- 1 In Service Center, click **Update Center > Components**.
- 2 Do one of the following:
  - To search currently installed components, click **Installed**.
  - To search for available updates to installed components, click **Updates**.
- 3 In the **Search Components** box, type a search string.

---

4 Hit Enter or click the Search icon.

**See Also**

[Installing a Monitoring Policy](#)

[Upgrading to a New or Changed Monitoring Policy](#)

[Installing a Service Module](#)

[Importing a Service Module](#)

[Installing a Report](#)

[Updating a Report](#)

[Working with Printer Transforms](#)



## SETTING UP USER ACCOUNTS AND ROLES

---

*This section provides detailed information about the following topics:*

- *Setting Up User Accounts*
  - *Setting Up Roles*
-

---

# Setting Up User Accounts

## About User Accounts

A user account is a collection of information that tells Service Center which sites, groups, devices, websites and other objects a user can access. Each person accesses Service Center with a user name and password.

Each user must be a member of at least one role.

**Default:** The user for a newly installed Service Center is Admin with no password.

**Note:** For hosted versions of Service Center, the hosting provider may have configured an account and password that will be provided by them prior to first use.

What If...	Then...
A user is not a member of a role	That user will not be able to log into Service Center.
A user is a member of more than one role with different access permissions	The least restrictive security settings apply.

### See Also

[Setting Up Roles](#)

### Example 1: Salesperson

One of the default roles that is included with Managed Workplace is called Sales, which has been designed to provide a sales force with access to useful information in Service Center. Members of the Sales role have read access to the following windows in Service Center:

- **Status > Central Dashboard**
- **Site Management > Windows Inventory**
- **Site Management > SNMP Inventory**
- **Reporting > Reports**
- **Reporting > Delivery Schedules**



---

The role was designed in this manner so that a Salesperson can view the current status of a customer site by viewing the **Central Dashboard**, review the hardware and software assets for potential sales opportunities, and view reports and reports for further information about the site and how often the reporting is provided to the customer.

When a new user is created in Service Center for a Salesperson, they will be assigned the Sales role to define the areas in Service Center they may view. Once the user has been made a member of the Sales role, the object access for the user must also be configured.

The object access defines which sites, groups, devices and websites that the user may access. If an organization has sites in a one-to-one relationship with salespeople, the user for each salesperson would be granted access only to their respective customer sites.

### **Example 2: Specialized Technician**

A new user is being created for a Technician who works exclusively with Cisco Firewall Devices. As such, the standard Tech role that is predefined with Service Center provides more access than this user requires.

A new role called “PIX Tech” is created that matches the existing Tech role, with the following permissions removed (Read and Modify):

- Site Events
- Websites
- Windows Inventory
- Patch Management
- Intel® vPro™

Additionally, the user is created with object access only for the Cisco Firewall Devices at client sites.

## **Creating a User Account**

- 1** In Service Center, click **Configuration > User Management**.
- 2** Click **Create User Account**.
- 3** In the **User Name** box, type the logon name for the user.

**Note:** This is the name the user will need to log into Managed Workplace. It cannot be changed after you create a user account. You could delete the user account and create it again to change the name.

- 4** In the **First Name** box, type the first name of the user.

- 
- 5 In the **Last Name** box, type the last name of the user.
  - 6 If desired, in the **Password** box, type the account password.
  - 7 If you have entered a password, in the **Confirm Password** box, type the account password again.
  - 8 In the **Email** box, type the email address for the user.  
This is the email address where email alerts will be sent, if applicable.  
**Note:** Two user accounts cannot have the same email address.
  - 9 Ensure the **Account is Disabled** check box is cleared.
  - 10 Click **Save**.  
Next, you can configure the user account by adding a role or setting the objects the user account can access.

#### See Also

[Adding a Role to a User Account](#)

[Setting the Objects a User Account Can Access](#)

## Adding a Role to a User Account

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user account for which you want to add a role.
- 3 Click the **Roles** tab.
- 4 Click **Select Role**.
- 5 From the selection list that appears, select the role you want to add to the user account.
- 6 Click **OK**.

#### See Also

[Adding a User Account to a Role](#)

## Deleting a Role from a User Account

If a user account does not have any role assigned to it, the user will be unable to log into Managed Workplace.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user account you want to edit.

- 
- 3 Click the **Roles** tab.
  - 4 Click the **Delete** icon for the role you want to delete.



- 5 Click **Save**.

### See Also

[Deleting a User Account from a Role](#)

## Setting the Objects a User Account Can Access

You can give access to different objects to set security controls for each user. You can set which sites, groups, devices and websites a user can access.

**Sites** When a user is allowed access to a site, that user may access all devices and websites that belong to the site, even in service groups that are not site-specific.

**Service Groups** When a user is allowed access to a service group, that user may access all devices from all sites that belong to the service group.

**Site Groups** When a user is allowed access to a site group, that user may access all devices that belong to the site group.

**Devices** When a user is allowed access to a device, that user may access all controls for the device. If a user is not allowed access to a group that contains the device, the user will be able to access the group but will only see devices to which access has been granted.

**Cloud Services** When a user is allowed access to a cloud service, that user may access all controls for the website.

**Note:** If the user has the role of Administrator, the user automatically has access to all objects. To customize object access, the user must be part of a role other than Administrator. See [Adding a Role to a User Account](#).

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the user for which you want to set object access.
- 3 Click the **Object Access** tab.
- 4 Click **Add**.
- 5 From the **Select the Type of Object to Add** list, select the Object Type (Device, Group, Site or Website).
- 6 Click **OK**.

---

A listing for the selected Object type appears.

- 7 Select all the required items from the list.
- 8 Click **Add**.
- 9 Click **Save**.

**See Also**

[Removing the Objects a User Account Can Access](#)

## Removing the Objects a User Account Can Access

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user for which you want to remove access to an object.
- 3 Click the **Object Access** tab.
- 4 Select the check box that corresponds with the object for which you want to remove user access.
- 5 Click **Remove**.
- 6 Click **Save**.

**See Also**

[Setting the Objects a User Account Can Access](#)

## Deleting a User Account

**Note:** You cannot delete the Administrator account.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the **Delete** icon for the name of the user for which you want to delete.



## Setting Global Account Options

Managed Workplace account options add additional security to Service Center, including defining how users access the web console and protecting against brute force attacks.

---

### To set options for user sessions

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Global Account Settings**.
- 3 Type a number of minutes after which the user will be logged out of Service Center if there has been no activity during that time.

You will need to log out and log in again before this setting is applied to the session.

**Note:** When pages that auto-refresh are open (such as Central Dashboard, Alerts, Alerts Viewer, Network Services dashboard and Patch Management pages), the session will never expire if it refreshes at a faster rate than the session expiry time. Conversely, these pages cause the login page to be displayed if they refresh at a slower rate than the session expiry time. You can adjust the auto-refresh rate of the Central Dashboard and the Alerts page in System Settings.

### To set options for failed logon attempts

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Global Account Settings**.
- 3 Type the number of failed login attempts allowable within a defined period of time.

**Note:** Accounts that are locked out are unable to access the Service Center web console until an Administrator unlocks the account, but notifications for Alerts are still sent to the user.

- 4 Click **Save**.

### To set options for passwords

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Global Account Settings**.
- 3 Under **Password Settings**, select any or all the following check boxes:

**Force user to change password after administrative reset** Users that have been reset to active by an Administrator will have to change their password when they first log in.

**Keep a history of X passwords** Users will not be able to reuse previous passwords.

**Enforce alphanumeric passwords** Passwords must contain letters and numbers.

---

**Enforce special characters in passwords** Passwords must contain at least one special character.

**Password minimum length is X characters** Passwords must contain a minimum of a defined amount of characters.

**Password expires after X days. Send notification X days before password expires** Causes the password to expire after a specified number of days with a warning email sent to the user a defined number of days prior to the expiration.

- 4 Click **Save**.

## Setting User Account Options

### To reset name and email address options for a user account

For example, use this feature if a staff member has left and you want to use the same user account but provide a new email address.

**Note:** You cannot rename the user name of an account. This is the name the user types when logging into Service Center.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user account for which you want to reset the name and email address.
- 3 If desired, type a new name in the **Last Name** or **First Name** box.
- 4 If desired, type a new email address in the **Email** box.
- 5 Click **Save**.

### To provide an SSO login name for a user account

If you are using AVG Business SSO, you can provide the user's SSO login name to link to the user account in Managed Workplace. When the SSO and Managed Workplace user accounts are linked, the user account settings, such as permissions and object access, are passed to the SSO account.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user account for which you want to provide an SSO login name.
- 3 Type the user's Business SSO login name in the SSO Login Name box.

### To reset the password for a user account

- 1 In Service Center, click **Configuration > User Management**.

- 
- 2 Click the name of the user account for which you want to reset the password.
  - 3 Click **Reset Password**.
  - 4 Type a new password, and then confirm it.
  - 5 Click **Save**.
  - 6 Click **Save**.

### To prevent passwords from expiring

You can prevent the password from expiring for any user account. This is particularly useful for accounts that interact with a professional services automation (PSA). If the password expires for a PSA user account, the integration will cease to function until the password is updated.

**Note:** This is not available in VAR Admin environments.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click the name of the user account for which you want to prevent the password from expiring.
- 3 Select the **Password does not expire** check box.
- 4 Click **Save**.

### To disable a user account

A user whose account has been disabled may not log into the Service Center web console until the account has been enabled by an Administrator. A user with a disabled account will not continue to receive notifications in the usual manner.

**Note:** An Administrator account cannot be disabled.

- 1 In Service Center, click Configuration > User Management.
- 2 Click the name of the user account for which you want to disable.
- 3 Select the Account is Disabled check box.
- 4 Click Save.

### To lock or unlock a user account

A user whose account has been locked out may not log into the Service Center web console until the account has been unlocked by an Administrator. An account is locked out to prevent unauthorized access attempts, but does not affect any other aspect of the user account. The user will continue to receive notifications in the usual manner.

---

**Note:** An Administrator account cannot be locked out.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Users**.
- 3 Click the name of the user account that is locked.
- 4 Do one of the following:
  - To lock the user account, select the **Account is Locked Out** check box.
  - To unlock the user account, clear the **Account is Locked Out** check box.
- 5 Click **Save**.

### To set the time zone for a user account

All user accounts are assigned the default time zone when they are created. The default time zone matches that of the Service Center application server's operating system.

If you're managing networks or devices from other time zones, you can specify the user's time zone for alerts or other time-stamped information.

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Users**.
- 3 Click the name of the user account for which you want to set the time zone.
- 4 Select the time zone.
- 5 Click **Save**.

### To set the language for a user account

- 1 In Service Center, click **Configuration > User Management**.
- 2 Click **Users**.
- 3 Click the name of the user account for which you want to set the language.
- 4 Select the language.
- 5 Click **Save**.

**Note:** The language selected must be installed on the Service Center application server. Use the **Regional Settings** tool in **Control Panel** to add any languages your users require.



---

## Setting Up Roles

### About Roles

A role defines the areas of Service Center that may be accessed by users who are members of the role. Additionally, the roles determine whether a user may initiate remote control sessions, receive email alerts, or have trouble tickets assigned to them.

What If...	Then...
An attempt is made to access an area of Service Center that is not permitted by the roles of which a user is a member	The user sees the following message: "You are not authorized to view this page".
A user is a member of more than one role with different access permissions	The least restrictive security settings apply.

### Default Roles

Managed Workplace comes with six default roles:

**Administrator** Members have read and modify access to all objects in Service Center. This role cannot be renamed or have its access permissions modified.

**Technician** Members have read access to all objects in Service Center and modify access to all objects except patch management initial setup, report categories, user management, system settings and service desks. Members can initiate remote control sessions, use remote tools, receive email alerts, and have trouble tickets assigned to them. This role can be renamed or modified.

**Customer** Members have read access to all status and site inventory objects and modify access to allow trouble ticket assignment. Members can have trouble tickets assigned to them. This role can be renamed or modified.

**Sales** Members have read access to the Central Dashboard, site inventory, and reporting. This role can be renamed or modified.

**Guest** Members have read access to all status objects. This role can be renamed or modified.

**Service Manager** Members have read access to all objects in Service Center except report categories, user management, system settings and service desks. Members also have modify access to device management, alerts, trouble

---

tickets, and reporting. Members can initiate remote control sessions and have trouble tickets assigned to them. This role can be renamed or modified.

**End User** Members have modify access to the **Wake Computers** page of Service Center only. Although you can give this role other permissions, it is recommended that you use the default setting so that end users only see the Wake Computers page.

### Using Roles for Security

Coupled with the object access security on the user level that defines which sites, groups, devices and websites a user may access, roles comprise the Managed Workplace security model.

### Example

You can create a restricted Administrator role that is limited to specific objects. If you clear the **Automatically Assign New Sites** check box in the Permissions tab, then users who have this role will not be given access to new sites as they are added. You can also exclude the notifications.

### See Also

[Example 1: Salesperson](#)

[Example 2: Specialized Technician](#)

## Creating a Role

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click **Create Role**.
- 3 In the **Role Name** box, type a name for the role.
- 4 Click **Create Role**.
- 5 To configure the role, click **OK**.
- 6 Click the **Members** tab.
- 7 Click **Add User**.
- 8 From the selection list that appears, select the user you want to add as a member of the role.
- 9 Click **OK**.
- 10 Repeat steps 7 - 9 until all desired users have been added as members of the role.
- 11 Click the **Permissions** tab.

- 
- 12 Configure the permissions for the role.

**Tip:** You can configure a role to see all the tasks but not be able to modify any scripts.

- 13 Click **Save**.

## Adding a User Account to a Role

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click the name of the role for which you want to add a user account.
- 3 Click the **Members** tab.
- 4 Click **Add User**.
- 5 From the selection list that appears, select the user you want to add as a member of the role.
- 6 Click **OK**.
- 7 Repeat steps 4 - 6 until all desired users have been added as members of the role.
- 8 Click **Save**.

### See Also

[Adding a Role to a User Account](#)

[Deleting a User Account from a Role](#)

## Deleting a User Account from a Role

If a user account does not have any role assigned to it, the user will be unable to log into Managed Workplace.

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click the name of the role from which you want to delete a user account.
- 3 Click the **Members** tab.
- 4 Click **Remove** that corresponds with the user account you want to remove.
- 5 Click **Save**.

### See Also

[Deleting a Role from a User Account](#)

[Adding a User Account to a Role](#)

---

## Setting Permissions for a Role

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click the name of the role for which you want to set permissions.
- 3 Click the **Permissions** tab.
- 4 Configure the following permissions for the role:

**Device Management - Remote Control Access** User can access and use Onsite Manager Utilities and/or the Remote Tools.

**Device Management - Mobile Devices** User can view mobile devices and perform remote actions, including locking, wiping, setting or removing the passcode, and marking as lost or found.

**Alerts** User can view and/or modify alert notifications and escalation notifications.

**Status** User can view and/or modify information in the Status screens, including the Central Dashboard and Services Dashboard, the Alerts Viewer, Onboarding Overview, and other status screens.

**Patch Management** User can view and/or modify the Overview, Patch Approval, Reports, Settings, and Approval Groups screens.

**Configuration** User can view and/or modify information in the selected Configuration screens.

**Trouble Tickets** User can be assigned trouble tickets.

**Site Assignment** Users are automatically assigned new sites.

**Reporting** User can view or modify report categories, reports, and report delivery s.

**AVG AntiVirus** User can view or modify the AVG AntiVirus Overview screens, which are used to manage AVG AntiVirus at customer sites.

**Automation** Users can access and/or modify the automation library of scripts and script packages, and the automation calendar to schedule tasks.

**Partner Portal Links** User can access links to the partner portal.

**Site Management** User can view and/or modify information in the **Sites**, **SNMP Inventory**, and **Windows Inventory** screens.

**Update Center** User can access Update Center to update Service Center products and components.

**Wake-on-LAN** User has permission to perform a Wake-on-LAN on customer devices.

---

**Note:** Some of the check boxes for **Modify** are not selectable. This indicates that the specified area cannot be modified.

- 5 Click **Save**.

## Renaming a Role

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click the role you want to rename.
- 3 In the **Role Name** box, type a new name for the role.
- 4 Click **Save**.

## Deleting a Role

When you delete a role, any users that were members of the role no longer have the access provided by the removed role.

**Note:** You cannot delete the Administrator role.

- 1 In Service Center, click **Configuration > Role Management**.
- 2 Click the **Delete** icon that corresponds with the role you want to delete.



Delete icon

- 3 Click **OK**.



C H A P T E R

# 7

## GROUPING

---

*This section provides detailed information about the following topics:*

- *About Grouping*
- *Creating Service and Site Groups*
- *Creating Shared Site Groups*
- *Managing Groups*

---

## About Grouping

You can organize devices and applications in two ways using

- Service groups
- Site groups

Groups allow you to easily manage a large number of systems by filtering devices to run reports, run automated tasks, and perform patch management such as applying patching policies to multiple devices at one time.

Devices can belong to multiple groups; however, in this case, any device alerts will appear on the Central Dashboard under all the groups to which the device belongs.

**Note:** Approval groups are not the same as service or site groups and are only used with Patch Management. See [Creating an Approval Group](#).

### How You Can Use Groups

Groups can be used for a variety of asset management purposes, including

- for custom views or filters of devices (such as alert views)
- for reporting on a group of devices
- to organize your staff into groups supporting certain IT technologies. For example, if you're a Microsoft Exchange Specialist, you can quickly view and manage multiple Exchange servers across multiple clients.
- for persistent state management, whereby you can create grouping rules to automatically add devices to a group when malware is detected, and then run an automated task against those device to remove the malware. When the malware is removed, the device is automatically removed from the group.
- to apply configuration profiles to Android, iOS, and OS X devices
- for user permissions whereby you can assign users to view and access certain groups only

### Understanding Site Groups and Service Groups

**Service Groups** A service group is an organizational container for devices, which may contain devices from multiple sites. The advantage of service groups is the ease of administration when managing like devices or applications. As well, it provides views at the group level and reports at the group level.

You can create as many service groups as you want.



---

**Site Groups** A site group is an organizational container for devices related to a single site. The advantage of site groups is the ease of identifying alerts occurring on a per-site basis.

Any customer may be monitored by multiple Onsite Managers and Device Managers organized into one or more sites in Service Center. When this is the case, you can organize the sites by physical location, and the site groups by function, such as Netstone-Finance, Netstone-Marketing, and so on.

Site group creation is extremely important since it provides you the filters required for enhanced reporting as well as staff organization and a more effective and friendly user interface. Site grouping is also very effective for asset management and scripting.

You can create as many site groups as you want. You can also create shared site groups, which are centrally managed with one site group definition that automatically creates site groups at new sites. For more information, see [Creating Shared Site Groups](#).

### **Automatically Adding Devices to Groups**

You can create automatic inclusion rules that determine the criteria a device must match to be included in the site or service group. As new devices are discovered, they are automatically added to the site and service groups to which they meet the defined inclusion rules. Conversely, if a change is made to a device and it no longer meets the inclusion rules, it is automatically removed from the group.

**Note:** You can also manually add devices to a group. Devices that were added manually are included in the group regardless of whether they match automatic inclusion rules or not. See [Manually Adding Devices to Groups](#).

You can create automatic inclusion rules by defining logical AND or OR statements, and then adding the rule criteria.

See [Creating Rules to Automatically Add Devices to a Group](#).

### **Defining the scope**

When creating automatic inclusion rules, you can optionally limit the scope of devices that will be monitored. The scope of a group's automatic inclusion rules defines against which sites and groups any rules will run, looking for devices with matching criteria. You can choose to use a system-wide scope, which means all devices that appear in Service Center will have the rules check for inclusion, or a custom scope, where you limit the rules execution to sites and groups you specify. You can further refine the scope by adding exclusions to prevent sites, groups or devices you specify from being included, even if they are within the defined scope. For site groups, you can exclude specific devices. For service groups, you can exclude sites, groups, and devices.

---

See [Defining Scope for a Service Group](#).

### Folders

A folder is a top-level organizational unit for service groups. For example, a folder called Workstations could contain a service group for Windows XP Workstations and Windows 7 Workstations.

### See Also

[Creating a Service Group](#)

[Creating a Site Group](#)

[Deleting a Service or Site Group](#)

[Renaming a Service Group Folder](#)

[Moving a Service Group to a Different Group Folder](#)

## Creating Service and Site Groups

Creating a group involves the following steps:

- designate the group as a site group or service group, and provide a name and description. See [Creating a Group](#).
- define rules to determine which devices will be included in the group. See [Creating Rules to Automatically Add Devices to a Group](#).
- manually add devices to the group (optional). See [Manually Adding Devices to Groups](#).
- define the scope. See [Defining Scope for a Service Group](#).
- apply policies to the group (optional). See [Applying Policies to Groups](#).
- apply configuration profiles to the group (optional). See [About Configuration Profiles](#).

### Creating a Group

The steps for creating service groups and site groups are very similar.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click either the **Service Group** tab or the **Site Group** tab.
- 3 Click **New**.
- 4 Do one of the following:

- 
- If you are creating a service group, either select an existing folder in which to store the group, or select the **Create New Group Folder** check box, and then type a name for a new folder in which to store the service group.
  - If you are creating a site group, select the site for which the group is being created from the list.
- 5 Type a name for the group.
  - 6 Optionally, type a description for the group.
  - 7 Click **Create**.

## Creating Rules to Automatically Add Devices to a Group

You can create automatic inclusion rules that define which devices will be included in the site or service group. Devices that match the inclusion rules are automatically added to the group. If a device no longer meets the rule criteria, it is automatically removed from the group.

Rules are created by first defining AND and OR statements, then by adding rules to the statements. For example, if you are creating a rule to include all Windows operating systems, in the default AND group, you would specify that the OS Name contains “Windows”.

To create a rule that specifies that the device must either have a Windows operating system or it must be a member workstation, you would change the AND statement to an OR statement, and then add a second rule that specifies that the OS name contains “Windows”:

Creating automatic inclusion rules involves the following steps:

**Define the rule statement** Creating automatic inclusion rules will usually be very straightforward, but because you can put together very sophisticated rules, it’s best to come up with a statement about the rule using very simple English before you get started.

Here are some example rule statements:

<b>If you want this result...</b>	<b>Example rule statement</b>
The device must be a firewall	firewall
The chassis type must be a laptop, and the operating system must be Windows	(Chassis type is laptop) AND (OS is Windows)

---

If you want this result...	Example rule statement
The network service must be HTTP or HTTPS	(HTTP) OR (HTTPS)
The domain role must be a member workstation or a member server, and the operating system must be Windows 7 or Microsoft Windows Storage Server 2008 R2 Enterprise	(Member Workstation or Member Server) AND (Windows 7 or Microsoft Windows Storage Server 2008 R2 Enterprise)

---

### To create an automatic inclusion rule for a group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab or the **Site Groups** tab.
- 3 Click the name of the group to modify.  
If you need to create a group first, see [Creating a Group](#).
- 4 Click the **Auto-Inclusion** tab.
- 5 Create the conditional statements. See [To create condition statements for a rule](#).
- 6 Create the inclusion criteria. See [Create inclusion criteria for a rule](#).
- 7 Preview the rule. See [Previewing a Group](#).

### To create condition statements for a rule

- Set up the conditional statements by doing any of the following:
  - To create a single AND statement to which you can add one or multiple rules, do nothing.
  - To create a single OR statement, right-click the existing AND statement and select **Modify**. From the **Type** list, select Or.
  - To add an OR group below the existing AND statement, select the AND statement and click **Add**. From the **Type** list, select Or.

### Create inclusion criteria for a rule

- 1 Select the AND or OR statement to which you want to add inclusion criteria.
- 2 Click **Add**.

---

3 From the Type list, select **Rule**.

4 From the Rule list, select one of the following:

**Chassis Type** Filter devices according to chassis type, such as laptop, desktop, notebook, etc. Select either **Equals** or **Not Equal** from the **Operator** list, and select a chassis type from the **Value** list.

**Device MAC Address** Filter devices by the MAC address. Select either **Equals**, **Contains**, or **Starts With** from the **Operator** list, and type the MAC address in the **Value** box.

**Device Model** Filter devices by providing the device model. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list and type the device model name in the **Value** box.

**Device Role Category** Filters devices by device role category. As a best practice, use this rule when you will be applying service plans to shared site groups; the pre-built shared site groups in Managed Workplace are designed to be applied to the device roles defined in this rule. Select **Equals** from the **Operator** list, and then select **Network Device**, **Unknown**, **Windows Server** or **Windows Workstation**.

**Device Model** Filter devices by providing the device model. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list and type the device model name in the **Value** box.

**Domain Role** Filter devices by the domain role. Select either **Equals** or **Not Equal** from the **Operator** list and select a domain role from the **Value** list, such as **Member Workstation** or **Primary Domain Controller**.

**Hardware Type** Filters devices according to hardware type, including desktop, laptop, mobile phone, printer, rack mount, and others. From the **Value** list, select the hardware type.

**Has Warranty Information** Filter devices by whether warranty information exists. Searches for devices with both custom and vendor warranties. Supported vendors include Acer, Compaq, Dell, Gateway, Hewlett-Packard, HP, IBM, Lenovo and Toshiba. Selecting this option from the **Rule** list includes all devices with warranty information.

**Installed Memory (in GB)** Filter devices by the installed memory. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in GBs.

**IP Address** Filter devices by the IP address. Select either **Equals**, **Not Equal**, **Greater Than**, **Less Than**, **Contains** or **Starts With** from the **Operator** list, then type an IP address in the **Value** box.

**Is a Printer** Filter devices to include printers. Selecting this option from the **Rule** list includes all printers.

---

**Is a Virtual Machine** Filter devices to include virtual machines. Selecting this option from the **Rule** list includes all virtual machines.

**Is Intel vPro Device** Filter devices by whether they are Intel vPro devices. Select **True** or **False** from the **Value** list.

**Logical Drive Size (GB)** Filter devices by the logical drive size. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in GBs.

**Manufacturer** Filter devices by the manufacturer. Select **Equals, Not Equal, Contains, Not Contain,** or **Starts With** from the **Operator** list, then type a manufacturer name in the **Value** box.

**Network Role** Filter devices by the network role, such as firewall, router, etc. Select a network role from the **Value** list.

**Network Service** Filter devices by standard network service ports, including commonly-used services such as HTTP, SMTP, and POP3. Custom ports for network services are not filtered. Select a network service from the **Value** list.

**OS Family** Filters devices by OS family, for example Android, iOS, Linux/Unix, and Windows. From the **Value** list, select an OS family.

**OS Name** Filter devices by the operating system name, for example Windows Server 2008 Standard. Select **Equals, Not Equal, Contains, Not Contain,** or **Starts With** from the **Operator** list, then type an operating system name in the **Value** box.

**OS SKU** Filter devices by their unique operating system SKU (Stock Keeping Unit). For example, Windows 7 has several SKUs, including Home Premium, Professional, Home Basic, and Enterprise. Select either **Equals** or **Not Equal** from the **Operator** list, then select a SKU from the **Value** list.

**Note:** The OS SKU rule is not applicable to Windows 2003 and XP operating systems.

**OS Version** Filter devices by the operating system version, which you can determine by executing the `winver` command. For example, for the Windows 7 Enterprise operating system, the OS build version is 7601. Select either **Equals, Not Equal,** or **Starts With** from the **Operator** list, then type an operating system version in the **Value** box.

**Responds to SNMP** Filter devices by whether they respond to Simple Network Management Protocol (SNMP) monitors. From the **Value** list, select **True** to include devices that respond to SNMP monitors, or **False** to include devices that do not respond.

---

**Responds to Specific OID** Filter devices to include those that respond to a specific SNMP object identifier (OID). From the **Value** list, select an OID type, such as Dell Server or HP Switch.

**Responds to SSH** Filters devices by whether they respond to Secure Shell (SSH) monitors. From the **Value** list, select **True** to include devices that respond to SSH monitors, or **False** to include devices that do not respond.

respond.

**Responds to WMI** Filters devices by whether they are WMI enabled. From the **Value** list, select **True** to include devices are WMI enabled, or **False** to include devices that are not.

**Responds to WS-MAN** Filter devices by whether WS-MAN is enabled, which is an option for WMI connectivity. Select **True** or **False** from the **Value** list.

**Software** Filter devices by the software that is installed. You can filter by software name, and optionally you can also filter by the software version.

- a From the **Operator** list, select either **Exists** or **Does Not Exist**.
- b Under **Software Name**, select an operator from the **Operator** list and type the software name in the **Value** box.
- c To further filter by software version, select the **Include Software Version** check box. From the **Operator** list that appears, select an operator and type a version number in the **Value** box.

**SNMP sysDesc** Filter devices by the SNMP system description. For example, to include Apple OS X devices, you could enter "Darwin". Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an SNMP system description in the **Value** box.

**SNMP sysObjectID** Filter devices by the SNMP system object ID. For example, Cisco ASA series devices each have unique sysObjectIDs. To include Cisco ASA 5505 devices, enter the sysObjectID for this device type (1.3.6.1.4.1.9.1.745). Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an SNMP sysObjectID in the **Value** box.

**Software - Mac and Software - Windows** Filter devices by the Mac or Windows applications that are installed. You can filter by software name, and optionally you can also filter by the software version.

- a From the **Operator** list, select either **Exists** or **Does Not Exist**.
- b Under **Software Name**, select an operator from the **Operator** list and type the software name in the **Value** box.

- 
- c To further filter by software version, select the **Include Software Version** check box. From the **Operator** list that appears, select an operator and type a version number in the **Value** box.

**System Role** Filter devices by system role, for example File Server or Routing Service. Select a system role from the **Value** list.

**Windows Service Name** Filter devices by the Windows Service Name. To determine the Windows Service Name, view the device's Properties Page. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type a Windows Service Name in the **Value** box.

- 5 Click **Add**.
- 6 Click **Save**.

### Modifying an Automatic Inclusion Rule

You can modify an automatic inclusion rule by doing any of the following:

- change an And condition to an Or condition, and vice versa;
- change the rule type, rule operator, and value for inclusion.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Group** or **Site Group** tab.
- 3 Click the name of the group to modify.
- 4 Click the **Auto-Inclusion** tab.
- 5 Click the name of the rule you want to modify.
- 6 Make your required changes and click **Update**.
- 7 Click **Save**.

### Deleting an Automatic Inclusion Rule

You can delete an entire automatic inclusion rule, or you can delete individual And, Or, and rule entries. Deleting an entire automatic inclusion rule requires that you first delete the rule entries, and then delete the empty And and Or statements.

**Note:** You cannot delete And or Or statements that have rules defined within.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group to modify.
- 3 Click the **Auto-Inclusion** tab.



- 
- 4 Do one of the following:
    - Select the row for the And group, Or group, or rule that you want to delete. Click the **Delete** button.
    - Click the X in the row you want to delete.

## Automatic Inclusion Rule Examples

### Example 1

You want to create a service group that automatically includes all computers running the Windows 2008 operating system.

The rule statement would simply be: All computers with the Windows 2008 operating system.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the group to modify.
- 4 Click the **Auto-Inclusion** tab.
- 5 Select the AND row and click **Add**.

**Note:** You must click an empty space in the row and not on the text itself.

- 6 From the **Rule** list, select OS Name.
- 7 From the **Operator** list, select Contains.

Selecting “Contains” from the **Operator** list does not require the full text string, therefore including any device that has an operating system with Windows 2008 in the name.

- 8 In the **Value** box, type Windows 2008.
- 9 Click **Add**.

### Example 2

You want to create a service group that includes all machines running the Windows 2008 operating system and are backup domain controllers.

The rule statement would be: Computer must have the Windows 2008 operating system AND have a domain role of backup domain controller.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the group to modify.

- 
- 4 Click the **Auto-Inclusion** tab.
  - 5 Now you will add the Windows 2008 OS rule:
    - a Select the AND row and click **Add**.
    - b From the **Type** list, ensure that Rule is selected.
    - c From the **Rule** list, select OS Name.
    - d From the **Operator** list, select **Contains**.

Selecting “Contains” from the Operator list does not require an exact text string, therefore including any device that has an operating system with Windows 2008 in the name.
    - e In the **Value** box, type Windows 2008.
    - f Click **Add**.
  - 6 Now you will add the backup domain controller rule:
    - a Select the AND row and click **Add**.
    - b From the **Type** list, ensure that Rule is selected.
    - c From the **Rule** list, select Domain Role.
    - d From the **Operator** list, select Equals.
    - e From the **Value** list, select Backup Domain Controller.
    - f Click **Add**.

### Example 3

You want to create a service group that includes devices with a Windows 2008 operating system and the domain role is either primary domain controller or backup domain controller.

The rule statement would be: Computer must be running the Windows 2008 operating system AND the domain role must be either Primary Domain Controller OR Backup Domain Controller.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the group to modify.
- 4 Click the **Auto-Inclusion** tab.
- 5 Add the Windows 2008 operating system rule:
  - a Select the AND row and click **Add**.
  - b From the **Type** list, ensure that Rule is selected.

- 
- c From the **Rule** list, select OS Name.
          - d From the **Operator** list, select Contains.  
Selecting “Contains” from the **Operator** list does not require a full text string, therefore including any device that has an operating system with Windows 2008 in the name.
          - e In the **Value** box, type Windows 2008.
          - f Click **Add**.
  - 6 Add the or condition:
    - a Click the OS Name row and click **Add**.
    - b From the **Type** list, select Or.
    - c Click **Add**.
  - 7 Now you will add the domain roles to the or condition:
    - a Right-click the Or row and select **Add** from the context menu.
    - b From the **Type** list, select Rule.
    - c From the **Rule** list, select Domain Role.
    - d From the **Operator** list, select Equals.
    - e From the **Value** list, select Primary Domain Controller.
    - f Click **Add**.
    - g Right-click the Or row again and select **Add** from the context menu.
    - h From the **Type** list, select Rule.
    - i From the **Rule** list, select Domain Role.
    - j From the **Operator** list, select Equals.
    - k From the **Value** list, select Backup Domain Controller.
    - l Click **Add**.

## Defining Scope for a Service Group

Defining scope for a service group is the practice of determining the range of sites, other groups, and devices that will be included in the group. The scope defines against which sites and groups any rules will run, looking for devices with matching criteria. By default, service groups are set to a system-wide scope. You can narrow the scope by selecting the custom scope option and then doing the following:

- Selecting the sites, groups, and devices to include in the scope.

- 
- If needed, you can exclude specific sites, groups, and devices that were added as children of the objects selected to include in the scope.

Excluding items is sometimes required when a site, group, or device has been indirectly included in the group scope as the result of another site, group, or device being directly included. For example, you might add a site to a group scope that contains certain devices that you do not want included.

**Note:** You cannot define scope for a site group, however you can exclude devices if required. For more information, see [Excluding Devices from the Scope](#).

### **Adding Sites to a Service Group Scope**

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the service group to which you want to define the scope.
- 4 Click the **Auto-Inclusion** tab.
- 5 Select the **Custom scope** option button.
- 6 In the **Scope** area, under **Sites**, click **Add**.
- 7 Select the check box beside each site you want to include.
- 8 Click **Add**.

### **Adding Other Groups to a Service Group Scope**

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the service group to which you want to define the scope.
- 4 Click the **Auto-Inclusion** tab.
- 5 Select the **Custom scope** option button.
- 6 In the **Scope** area, under **Groups**, click **Add**.
- 7 Select the check box beside each site you want to include.
- 8 Click **Add**.

### **Removing Sites and Groups from the Scope**

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group to which you want to define the scope.

- 
- 3 Click the **Auto-Inclusion** tab.
  - 4 In the **Scope** area, do any or all of the following:
    - Under **Sites**, select the check box beside each site you want to remove and click **Remove**.
    - Under **Groups**, select the check box beside each group you want to remove and click **Remove**.
  - 5 Click **Save**.

## Excluding Sites, Groups, and Devices from the Scope

Excluding a site, group, or device from a group scope is not the same as removing the item from the scope. When you exclude an item, you are excluding something that was not directly added to the scope, but would have been added to the group as a result of an associated site or group being included in the scope.

**Note:** Excluding devices from a group does not exclude devices that you manually added to the group. When excluding sites, groups, or devices, you should verify that your exclusion is not overridden by manually added devices. You can view the devices manually added to the group on the Manual Inclusion tab. See [Manually Adding Devices to Groups](#).

### Excluding Sites from the Scope

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group from which you would like to exclude a site.
- 3 Click the **Auto-Inclusion** tab.
- 4 In the **Exclusions** area, under **Sites**, click **Add**.
- 5 In the **Add Sites (Exclusions)** window, select the check box beside each site you want to exclude from the group scope.
- 6 Click **Add**.
- 7 Click **Save**.

### Excluding Groups from the Scope

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group from which you would like to exclude a site or service group.
- 3 Click the **Auto-Inclusion** tab.
- 4 In the **Exclusions** area, under **Groups**, click **Add**.

- 
- 5 In the **Add Groups (Exclusions)** window, select the check box beside each group you want to exclude from the group scope.
  - 6 Click **Add**.
  - 7 Click **Save**.

### Excluding Devices from the Scope

You can exclude devices from both site groups and service groups.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group from which you would like to exclude a device.
- 3 Click the **Auto-Inclusion** tab.
- 4 In the **Exclusions** area, under **Devices**, click **Add**.
- 5 Filter the list of devices by doing any of the following:
  - Use the **Filter By** list to specify the devices you want to see in the list, and click **Filter**.
  - Use the lists under each column header to filter the list even more.
- 6 Do one of the following:
  - Select the check box that corresponds with each device you want to exclude from the policy set scope.
  - Select the check box in the column header to select all the devices.
- 7 Click **Add**.
- 8 Click **Save**.

### Removing Sites, Groups, and Devices from Exclusion

When you remove a site, group, or device from exclusion, it is added back into the service group.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group from which you'd like to remove a site, group, or device from exclusion.
- 3 Click the **Auto-Inclusion** tab.
- 4 In the **Exclusions** area, do any or all of the following:
  - To remove a site from exclusion, in the **Sites** area, select the check box beside the site you want to remove and click **Remove**.
  - To remove a group from exclusion, in the **Groups** area, select the check box beside the group you want to remove and click **Remove**.

- 
- To remove a device from exclusion, in the **Devices** area, select the check box beside the device you want to remove and click **Remove**.
- 5 Click **Save**.

## Previewing a Group

After creating the automatic inclusion rules and defining a scope for the group, you can preview the devices that will be included in the group. Previewing lets you verify that the inclusion rules you created will add all the devices you want included in the group.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group to which you want to preview the devices.
- 3 Click the **Auto-Inclusion** tab.
- 4 Click **Preview**.
- 5 When you are finished previewing, click **Close**.
- 6 If you are satisfied with the results, click **Save**.

The **Auto-Inclusion Preview** page displays a list of devices, including information such as the site, IP Address, a description, and a green check mark to indicate whether it is SNMP- or WMI-enabled.

## Running the Automatic Inclusion Rules for a Group

You can manually run the automatic inclusion rules for groups, which can be useful after creating or modifying the rules or a group's scope. When the rule completes its execution, devices will either be added or removed from the groups according to the rules you defined.

Grouping rules run every 30 minutes by default. If the group rules are currently running, your request is queued and will begin after the current rule execution completes.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click **Run Rules**.
- 3 Click **OK**.

## Manually Adding Devices to Groups

Optionally, you can manually add devices to groups. When you add a device to a group, it is included in the group regardless of whether it matches the inclusion rules or whether it exists in the group scope.

---

## To manually add devices to an existing service group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the service group to modify.  
If you need to create a service group first, see [Creating a Group](#).
- 4 Click the **Manual Inclusion** tab.
- 5 Click **Add**.
- 6 Filter the list of devices by doing any of the following:
  - Use the **Filter By** list at the top of the dialog box to specify the devices you want to see in the list.
  - Use the lists under each column header to filter the list even more.

Filters are a quick way to populate groups. For example, you could filter by system role or installed application to quickly populate a group.

**Site** Filters devices based on existing site groups.

**Group** Filters devices based on existing site and service groups.

**Basic Search** Filters devices based on the search criteria you enter. Wildcards are not recognized in this search box.

**Note:** Basic Search uses the All Fields search from the Device Search page, and therefore includes the following boxes in its search: Last Logged in User, Site Name, Service Group, Inventory Tag, Description, Manufacturer, Asset Tag, Model, IP Address and MAC Address.

**System Role** Filters devices based on system roles. Primary Domain Controller is the most important server in a Windows Domain and has all the rules about users, computers and their access levels. This is where you log in when you log into a Domain. Member Server is the Server OS devices that are joined to a Domain. Standalone Server is the Server OS devices that are not joined to a Domain. Member Workstation is the Workstation OS devices that are joined to a Domain. Standalone Workstation is the Workstation OS devices that are not joined to a Domain.

**Installed Application** Filters devices based on applications installed on devices.

**Managed Workplace Component** Filters devices based on whether Onsite Manager is installed, Device Manager is installed or not installed.

**Operating System** Filters devices by operating system. The options are Microsoft Windows, Mac OS, and Linux/Unix.



---

**Windows Service** Filters devices based on a selected Windows Service.

**None** Shows all devices and applies no filter.

7 To filter the list more, do one of the following:

- Use the filter lists under the column headings.
- Type filter criteria in the control under the column heading.

For example, type “DT” to filter all the devices that contain “DT” (which stands for Desktop in this example) in the device name.

**Note:** When using filters to add devices to groups, not all information may be available until the first asset scan for a new site has completed.

8 Do one of the following:

- Select the check box that corresponds with each device you want to add to the group.
- Select the check box in the column header to select all the devices.

9 Click **Add**.

### To manually add devices to an existing site group

1 In Service Center, click **Configuration > Groups**.

2 Click the **Site Group** tab.

3 Click the name of the site group to modify.

If you need to create a site group first, see [Creating a Group](#).

4 Click the **Manual Inclusion** tab.

5 Click **Add**.

6 Filter the list of devices by doing any of the following:

- Use the **Filter By** list at the top of the dialog box to specify the devices you want to see in the list.
- Use the lists under each column header to filter the list even more.

**Note:** When using filters to add devices to groups, not all information may be available until the first asset scan for a new site has completed.

7 Do one of the following:

- Select the check box that corresponds with each device you want to add to the group.
- Select the check box in the column header to select all the devices.

8 Click **Add**.

---

### To remove devices from an existing site or service group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the site or service group to modify.
- 3 Click the **Manual Inclusion** tab.
- 4 Select the check box for the device you want to delete from the group.
- 5 Click **Remove**.

## Applying Policies to Groups

Although you can manually apply policies to groups, it is not considered a best practice. Groups are designed for asset management purposes, and manually applying policies does not take advantage of automatic inclusion rules. It is recommended instead that you set up shared site groups, to which you can then apply a service plan. For more information, see [Creating Shared Site Groups](#).

However, if you prefer to set up your monitoring manually using groups, you can follow the steps below to enable group-based monitoring.

For more information about the types of policies in Managed Workplace, see [Working with Policies and Services](#).

### To manually apply a policy to an existing service group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the service group to modify.  
If you need to create a service group first, see [Creating a Group](#).
- 4 Click the **Policies** tab.
- 5 In the **Policies** area, click **Add**.
- 6 Select a policy type from the list, and click **Add**.

Only policies that were included in Service Center by default, or created manually, are available for selection. For monitoring policies, this also includes monitoring policies that were installed using the Update Center. For more information about installing monitoring policies, see [Installing a Monitoring Policy](#).

- 7 Select the check box beside each policy that you want to apply to the service group.
- 8 Click **Add**.

---

### To manually apply a monitoring policy to an existing site group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Site Groups** button.
- 3 Click the name of the site group to modify.  
If you need to create a site group first, see [Creating a Group](#).
- 4 Click the **Policies** tab.
- 5 In the **Policies** area, click **Add**.
- 6 Select a policy type from the list, and click **Add**.  
Only policies that were included in Service Center by default, or created manually, are available for selection. For monitoring policies, this also includes monitoring policies that were installed using Update Center. For more information about installing monitoring policies, see [Installing a Monitoring Policy](#).
- 7 Select the check box beside each policy that you want to apply to the site group.
- 8 Click **Add**.

## Viewing the Policies Applied to a Group

If you have applied policies to a service or site group, you can view them on the **Groups** page. For more information about policies, see [Working with Policies and Services](#).

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Site Groups** or **Service Groups** tab.
- 3 Click the name of a group.
- 4 Click the **Policies** tab.
- 5 The **Policies** section lists all of the policies applied to the group. To view more information about a policy, click the policy name.

## Applying MDM Configuration Profiles to a Group

If you have created and applied Mobile Device Management (MDM) configuration profiles to a group, you can view them on the **Groups** page. For more information about setting up the different types of configuration profiles, see [About Configuration Profiles](#).

- 1 In Service Center, click **Configuration > Groups**.

- 
- 2 Click the **Site Groups** or **Service Groups** tab.
  - 3 Click the name of a group.
  - 4 Click the **Policies** tab.
  - 5 The **Configuration Profiles** section lists all of the configuration profiles applied to the group. To view more information about a configuration profile, click the profile name.
  - 6 To add a configuration profile, click **Add**.
  - 7 Select a configuration profile type from the list, and click **OK**.
  - 8 Configure the profile as needed, and click **Save**.


## Creating Shared Site Groups

A shared site group functions the same way as a regular site group, however shared site groups are centrally managed from a single group definition. To create shared site groups, you create a shared site group definition that includes the following settings:

- group name
- group definition
- automatic inclusion rules that define what type of devices will be added to the group

After creating a shared site group definition, all newly created sites will automatically have site groups created according to the group definition.

You can also synchronize the shared site group definition to create site groups at your existing sites. When you synchronize a shared site group definition, the automatic inclusion rules are run against all your existing sites and a site group is created at each site.

You can view a list of your shared site groups by going to **Configuration > Groups**, and clicking the **Site Groups** tab. Shared site groups are differentiated from regular site groups by an icon .

If you want to sever the relationship between a shared site group and its corresponding shared site group definition, you can demote the shared site group. For example, for a site called ABC Medical, you want to modify the site group's automatic inclusion rules to filter out Windows 8 devices. You can demote the shared site group at this site only, and make the modifications as needed. The other shared site groups created with the original group definition are not affected.

---

You can delete a shared site group definition that you no longer require. When you delete a shared site group definition, you are given the following options:

- delete the definition, and delete all shared site groups created with that definition
- delete the definition, and demote all shared site groups created with that definition to regular site groups

### To create a shared site group definition

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Configure Shared Site Groups** tab.
- 3 Click **New**.
- 4 On the **Overview** tab, provide a name and description for the shared site group definition.
- 5 Click the **Auto-Inclusion Rules** tab.
- 6 Create the automatic application rules to determine what kind of devices will be included in the shared site groups when they are created. For more information on building these rules, see [Creating Rules to Automatically Add Devices to a Group](#).
- 7 Click **Save**.

### To synchronize a shared site group definition

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Configure Shared Site Groups** tab.
- 3 Select the check box beside the shared site group definition you want to apply to existing sites.
- 4 Click **Sync**.
- 5 A notification message appears asking for confirmation that you want to synchronize the group definition. Click **OK**.

### To delete a shared site group definition

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Configure Shared Site Groups** tab.
- 3 Select the check box beside the group definition you want to delete.
- 4 Click **Delete**.

- 
- 5 The **Shared Site Group Definition Delete Confirmation** window opens. Select one of the following options:
    - Click **Delete** to delete the site group definition and all site groups that were created from that definition.
    - Click **Demote** to delete the site group definition and demote all site groups that were created from that definition.

#### To demote a shared site group to a regular site group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Site Groups** tab.
- 3 From the **Choose Site** list, select the site containing the shared site group instance you want to demote.
- 4 Select the check box beside the shared site group that you want to demote.
- 5 Click **Demote**.
- 6 A notification message appears asking for confirmation that you want to demote the shared site group. Click **OK**.

## Managing Groups


### Replicating Site Groups

You can replicate a site group, which allows you to apply all of the group settings, including policies, automatic application rules, and Mobile Device Management (MDM) configuration policies, to another site. Replicating site groups allows you to easily reproduce group settings from site to site, saving you time and facilitating the use of a common monitoring and management strategy among multiple sites.

You can replicate one or multiple site groups at a time.

**Note:** You can also create shared site group definitions, which are created on the **Configure Shared Site Groups** tab, and then pushed out to create site groups at every site using that definition. This newer functionality has been designed to work with service plans; you can apply service plans to shared site groups to standardize the way you monitor devices across multiple sites. For more information on shared site groups and creating shared site group definitions, see [Creating Shared Site Groups](#).

- 1 In Service Center, click **Configuration > Groups**.

- 
- 2 Click the **Site Groups** button.
  - 3 Select the check box beside the site groups that you want to replicate.  
**Note:** You cannot replicate shared site groups, which are listed on the **Site Groups** tab and are indicated with this icon .
  - 4 Click **Replicate**.
  - 5 In the **Configuration** area, select from the list the site to which you want to apply the replicated group.
  - 6 Click **Replicate**.

## Viewing the Devices Included in a Group

You can view a list of the devices included in a site or service group, to verify which devices are included and whether they were added by manual inclusion or automatically through the use of inclusion rules.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the site or service group.
- 3 Click the **Members** tab.

## Renaming Groups and Service Group Folders

### To rename a site or service group

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Site Groups** or **Service Groups** tab.
- 3 Click the name of the group to modify.
- 4 On the **Overview** tab, click **Modify**.
- 5 In the **Group Name** box, type a new name for the group.
- 6 Click **Save**.

### To rename a service group folder

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the **Service Groups** tab.
- 3 Click the name of the service group that uses the group folder you want to rename.
- 4 On the **Overview** tab, click **Modify**.

---

5 Select the **Create New Group Folder** check box, and then type a name for a new folder in which to store the service group.

6 Click **Save**.

The service group moves to the new folder. If a group folder does not contain any service groups after renaming, the group folder is automatically deleted.

## Moving a Service Group to a Different Group Folder

1 In Service Center, click **Configuration > Groups**.

2 Click the **Service Groups** tab.

3 Click the name of the service group to modify.

4 On the **Overview** tab, click **Modify**.

5 Do one of the following:

- Select an existing folder in which to store the service group.
- Select the **Create New Group Folder** check box, and then type a name for a new folder in which to store the service group.

6 Click **Save**.

The service group moves to the new folder. If a group folder does not contain any service groups after moving, the group folder is automatically deleted.

## Deleting a Service or Site Group

When a service or site group is deleted, all monitoring that member devices receive from the group no longer occurs. The data previously collected is still available for review for all data types.

1 In Service Center, click **Configuration > Groups**.

2 Click the **Service Groups** or **Site Groups** tab.

3 Select the check box beside the group you want to delete.

4 Click **Delete**.



## WORKING WITH ASSETS AND DEVICES

---

*This section provides detailed information about the following topics:*

- *Assets*
  - *Devices*
  - *Viewing a List of Devices*
  - *Viewing Details about a Device*
  - *Viewing Details about a Printer*
  - *Customizing Devices*
  - *Working with a Device*
  - *Purging an IP Address from a Device*
  - *Searching for a Device*
  - *Waking Managed Devices Remotely*
  - *Working with Intel® vPro™ Devices*
-

---

## Assets

### About Asset Management

When you install Onsite Manager at a customer site, it automatically begins scanning assets within the IP addresses you've defined, discovering new devices and collecting detailed data. The asset scan on newly discovered devices is performed automatically and doesn't wait for a predefined interval.

Data is collated and summarized on the Central Dashboard, so you can drill down to details as required.

Use the Managed Windows Inventory and Managed SNMP Inventory views to see assets by site. You can get a quick view of the operating systems, CPU, hard drives and so on at each site. You can then drill down to the actual devices to see more detail.

#### Notes:

- Only asset information that has changed is sent to Service Center. For example, if Microsoft Office is installed on a device, this information is detected by the first asset scan of the device. This information is not resent each subsequent asset scan. However, if Microsoft Office is subsequently updated or uninstalled, this new information is detected by an asset scan and sent to Service Center.
- If a device reboots in between Onsite Manager discovery scans, then Onsite Manager still considers it up and continues incrementing the discovered time (UP/DN on device lists). The Device Overview page displays a value for time since last reboot, which is reported by the device operating system. Device availability alert thresholds are based on the discovered time and not the last operating system reboot.

#### What You Can Do

You can

- perform a device asset scan on demand
- search for a specific asset, such as the CEO's laptop, or search for a set of devices that meet your criteria
- identify versions and licensing across each customer site
- use reports to discover the presence of unauthorized or illegal software, such as peer-to-peer file sharing applications that rob bandwidth
- monitor and manage any hardware with an IP address and an active management protocol, including desktops, laptops (onsite and offsite), servers, managed switches, routers, firewalls, gateways, VoIP switches

---

and phones, printers, faxes or scanners, specialized equipment and environmental control devices, virtual machines and more

- identify inefficient, overloaded and unsupported devices
- automate collection of vendor-assigned asset tags
- track warranty and inventory tag information
- create device aliases to suit the customer's needs and streamline the support process
- view software assets based on applications, Windows services, hot fixes and service packs
- view product keys (for the operating system, Microsoft Office and SQL) for a device
- view last boot time for a device

**Note:** Windows does not treat a computer coming back from sleeping or hibernating as a reboot.

### See Also

For information about the network scan for devices, see [Running a Scan Manually](#).

For information about using reports to create summary and detail asset reports, see [Reporting](#).

## Viewing Windows Inventory

The **Managed Windows Inventory** window provides a summary of assets collected from Windows devices for a given site. You can see all high level hardware and software assets that Onsite Manager has discovered.

**Note:** If a device has both WMI and SNMP enabled, it appears only under the Managed Windows Inventory.

### To view Windows inventory

- 1 In Service Center, click **Site Management > Windows Inventory**.
- 2 Select a site from the list.
- 3 Browse through the tabs to see the different types of inventory.

### To list devices with the asset present

- 1 In Service Center, click **Site Management > Windows Inventory**.

- 
- 2 Click the chevron (>) that corresponds with the Windows inventory item.
  - 3 Click the ^ to close the list.

## Viewing SNMP Inventory

The **Managed SNMP Inventory** page provides a summary of all SNMP-enabled devices for a given site.

**Note:** If a device has both WMI and SNMP enabled, it appears only under the Windows Inventory.

### To view SNMP inventory

- 1 In Service Center, click **Site Management > SNMP Inventory**.
- 2 Select a site from the list.

### To list devices matching the SNMP description

- 1 In Service Center, click **Site Management > SNMP Inventory**.
- 2 Click the chevron (>) that corresponds with the SNMP inventory item.
- 3 Click the ^ to close the list.

## Viewing Mobile Device Inventory

The **Enrolled Mobile Device Inventory** page provides a summary of all mobile devices for a given site.

### To view mobile device inventory

- 1 In Service Center, click **Site Management > Mobile Inventory**.
- 2 Select a site from the list.

## Devices

### About Devices

A device is a unique responding IP-based entity or single logical object found during the discovery scan.

A device can be a desktop, laptop, server, mobile device, switch, router, firewall, gateway, phone, printer, fax, scanner, or specialized equipment. It can also be a Virtual Environment (for example, a VMware host or Guest).

---

The discovery scan uses evidence such as MAC address, IP address, DNS records and NetBIOS or SNMP names to determine unique objects on the network.

**Note:** Monitoring mobile devices is performed by enrollment not by discovery.

### How device names are determined

Although Onsite Manager and Device Manager gather identity information from multiple sources, Managed Workplace chooses one name for each device. This display name is used in Service Center and all reports.

The name evidence that has been collected at the highest priority in the following list will be used.

**1 (Highest) Alias** Configurable by Service Center users and recommended as a best practice. Use a naming convention that provides at-a-glance information to your technicians, or friendly names that will help clients identify devices by role or user in reports.

**2 Computer Name** The name returned by WMI. Windows displays this name on the Computer Name tab of the System Properties.

**3 SNMP** The name returned by SNMP from the OID sysName.0.

**4 NetBIOS** The 15-character name resolved by a WINS (Windows Internet Name Server) server or the LMHOSTS file. It is often the same as the Computer Name, but truncated.

**5 DNS** The name returned by the Domain Name System server or the HOSTS file. All DNS names are returned and used for display purposes. The names used will be separated by commas. If a device has conflicting DNS records in the forward and reverse lookup zones, the conflicting DNS names will not be submitted for use in the device identity algorithm.

**6 (Lowest) IP Address** The address that responded to the network scan will be used as the device name when no other information is available. You can still assign an alias to identify the device more easily, but AVG recommends enabling either a management protocol (WMI or SNMP) or DNS to establish a discovered name before overriding with an alias.

If a subsequent network scan is able to collect higher priority name evidence than prior scans, the display name will change. The device record will remain the same if there was actual identity information present before the change, for example if the MAC addresses for the device were known. However, if the device record was only based on a responding IP address, a new record will be created once identity information is collected.

---

**Tip:** Hover your pointer over a device name in device lists to see complete device name information currently available.

### What you can do

You can

- view lists of devices
- view details about a device
- customize devices by adding alias names, inventory tags, location information, custom warranty details, an end-of-life date, a production date or notes
- change the way service plans, services, and policies are applied to a device
- delete down devices manually or automatically
- purge stale IP addresses from a device
- search for a device
- work with Intel® vPro™ devices

## Viewing a List of Devices

You can view a list of devices in Service Center by clicking **Status > Devices**.

**Tip:** To view a list of devices pre-filtered for a specific group or site, click the number in the **Devices** column on the **Central Dashboard**.

For each device, the **Status** column displays an icon that indicates its current status:



The device is currently up.



The device is currently down.



The device is not responding to ICMP ping, but is responding to ARP. This indicates that the device is most likely down, but partially responding.



The AMT device's hardware has been configured to respond to ping and the operating system has been powered off.



The AMT device's hardware has been configured to not respond to ping and the operating system has been powered off.

Optionally, you can choose to show columns on the **Devices** page that display the following information:

- whether SNMP is enabled
- whether WMI is enabled
- whether SSH is enabled
- the amount of time the device has been up or down.


**Note:** If a device has multiple IP addresses (and if the device has no alias, no DNS name, no SNMP, no WMI and no NETBIOS), the **Device Name** column shows the first 16 IP addresses.

#### To filter the list of devices

**Tip:** Instead of filtering, you could search for a device. See [Searching for a Device](#).

- 1 In Service Center, click **Status > Devices**.
- 2 To filter the list, do one of the following:
  - To filter by site or service group, from the **Browse By** list select either **Site** or **Service Group**. Then select the site and site group or service group.
  - To filter by device role, select a role from the list.
  - Use the filter lists under the column headings.
  - Type filter criteria in the control under the column heading.  
For example, type "DT" to filter all the devices that contain "DT" in the device name.

#### To show the SNMP, WMI, SSH, and Time up/Time down columns on the Devices page

- 1 In Service Center, click **Status > Devices**.
- 2 Click the gear icon .
- 3 Select the check box beside each column you want to show.
- 4 Click **Save**.

---

## See Also

[About Devices](#)

[Viewing Summary Details about a Device](#)

[Searching for a Device](#)

[Customizing Devices](#)

[About Deleting Devices](#)

## Viewing Summary Details about a Device

On the **Device Overview** page, you can get a detailed view about a device, including hardware and software information. Using the right sidebar, you can quickly access other information about the device.

The **Device Overview** page groups information into the following categories:

**Identification** Includes the device name, description, operating system, form factor, manufacturer, model, date the device was discovered, and lists unique identifiers including SNMP name, system name, NetBIOS name, DNS name, and IP address.

**Applied Service Plan** Indicates whether a service plan has been applied to the device, and how it was applied. For example, a service plan can be applied to a site or a group to which the device belongs, or manually to the device.

**Applied Services** Lists the services have been applied to the device. You can enable and disable services, and manually apply a service to the device.

**Applied Schedule** Indicates which execution schedule has been applied to the device, and how it was applied. For example, an execution schedule can be applied to a site or group to which the device belongs, or directly to the device.

**Applied Policies** Lists the policies that have been applied to the device. You can enable or disable policies on the device, and delete policies that were manually applied directly to the device.

**Group Membership** Lists the site groups and service groups to which the device belongs.

**Disk Usage** Provides a visual cue of the disk usage for each local drive.

**Operating System** Provides details about the operating system, including name, version, service pack, architecture, and language.

**System Details** Provides an overview of the system manufacturer, domain role, chassis type, asset and inventory tag, device location, and dates for custom warranty, end-of-life, and production.



---

**System Status** Indicates whether WMI, SNMP, and SSH are enabled, whether WMI connectivity is provided over WS-MAN or DCOM, and provides dates and times for the most recent asset audit, WMI connection, and SNMP monitor.

**Processor and Memory** Lists the processor make and total RAM installed, in GBs.

**Notes** Displays notes about the device, written by you or another Managed Workplace user.

### To view an overview about a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.  
Depending on the type of device, the information available to view varies.

### To view alerts for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Do one of the following:
  - Click **Device Alerts** on the right sidebar.
  - Click the number under **Active Alerts**.

### To view the last logged in user for a device

- 1 In Service Center, click **Status > Devices**.
- The last logged in user appears in the **Operating System** section. Only local logins are collected for last logged in user. Terminal services sessions are not displayed.

### To view manufacturer details for a device

All network interfaces have a Media Access Control (MAC) address. Embedded in this address is the interface manufacturer. Managed Workplace retrieves the MAC address and looks up the device manufacturer, then displays both in the **Device Overview** page. This information can help you identify devices that are neither WMI nor SNMP enabled.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the name of a device.
- 3 Under **Identification**, click the arrow beside IP Address.

- 
- 4 If a MAC address is available, there is an arrow beside the actual IP address that displays below the IP Address link. Click this arrow to display the MAC address and manufacturer details.

### To view the asset tag information for a device

You can visit the vendor's website and view the detailed warranty information for a device.

**Note:** The asset tag is collected automatically from the device. Managed Workplace hides the **Asset Tag** box if it can't automatically retrieve the information.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device for which you want to view asset tag information.
- 3 Click the device name.
- 4 Click the link for the **Asset Tag**, if available.

### To view details about system log events for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **System Log Viewer** on the right sidebar.

### To view the patch management information for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Patch Management** on the right sidebar.

### To view the power management information for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Power Management** on the right sidebar. See [Enabling or Disabling Power Management for a Device](#) and [Overriding Power Plan Settings for a Device](#).

### To view the Automation Calendar to schedule a task on the device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.

- 
- 3 Click **Automation Calendar** on the right sidebar.

#### **To view what hardware is installed on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Hardware** on the right sidebar.

#### **To view what operating system is installed on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Operating System** on the right sidebar.

#### **To view what application software is installed on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Software** on the right sidebar.

#### **To view what virtual machines are hosted on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Virtual Machines** in the right sidebar.

#### **To view what Windows Services are installed on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Software** on the right sidebar.
- 4 From the drop-down list in the top-right, select **Windows Services**.

#### **To view what hotfixes and updates are installed on a device**

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Software** on the right sidebar.
- 4 From the list in the top right area, select **Hotfixes and Updates**.

---

### To view what Microsoft product keys are installed on a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Software** on the right sidebar.
- 4 From the list in the top right area, select **Microsoft Product Keys**.

**Note:** Managed Workplace collects license keys for many types of Microsoft Windows, Office and SQL Server products. This information is collected from the Windows registry of managed devices. In some cases, particular licenses may store this information in unexpected keys. If you find devices which do not have licenses listed in Service Center, please provide AVG Technical Support with a zipped backup of the registry for the affected device. Doing so allows us to add new locations from which we can gather the license information.

### To view what network services have been discovered on a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Network Services** on the right sidebar.
- 4 Do one of the following:
  - To start monitoring a network service, click the **Start Default Monitoring** icon (green triangle).
  - To stop monitoring a network service, click the **Stop Monitoring** icon (red pause sign).

### To view MBSA reports for a device

Microsoft Baseline Security Analyzer (MBSA) is not installed with Onsite Manager unless requested. MBSA is not installed with Device Manager, but it is available to Device Manager on devices with MBSA already in place. MBSA reports are for Windows devices only.

**Note:** MBSA reports are viewable in Internet Explorer only.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **MBSA** on the right sidebar.
- 4 To filter the list, select the grade and time frame options from the list.
- 5 To view a detailed report, click **View Report**.

---

### To view Intel® AMT information for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Intel® AMT** on the right sidebar.

### To view bandwidth usage for a device

**Note:** A bandwidth monitor must be set up first and have completed one polling of the device.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Bandwidth Usage** on the right sidebar.
- 4 Filter the information as desired.

### To view performance counter data on a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Performance Counters** on the right sidebar.

Thumbnails show the results for the last 12 hours for each performance counter monitor.

- 4 To view details about the performance counter within a time range, click a graph and select a time range from the **Time Range** list and then click **Filter**.
- 5 To purge performance counter data, click the **Purge Monitoring Data** link at the bottom of the screen.

**Important:** Purging performance counter monitoring data makes that data instantly inaccessible. This means you cannot get it back or view it in reports. AVG recommends using this only when you no longer want to monitor the counter on a device.

### To view what Windows events occurred on a device in a given time frame

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Windows Events** on the right sidebar.
- 4 To filter the events you see in the list, use the filter options.

- 
- 5 To see more detailed information about an event, click **Details**.
  - 6 If you clicked **Details** in the previous step, click **Research** to get more information about an event.

#### To view SNMP details for text OID data

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **SNMP** on the right sidebar.
- 4 To purge SNMP data, click the **Purge Monitoring Data** link.

**Important:** Purging performance counter monitoring data makes that data instantly inaccessible. This means you cannot get it back or view it in reports. AVG recommends using this only when you no longer want to monitor the counter on a device.

#### To view SNMP details for numeric OID data

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **SNMP** on the right sidebar.
- 4 To view details about the object name, select a time range from the **Time Range** list and click **Filter**.
- 5 To purge SNMP data, click the **Purge Monitoring Data** link.

**Important:** Purging performance counter monitoring data makes that data instantly inaccessible. This means you cannot get it back or view it in reports. AVG recommends using this only when you no longer want to monitor the counter on a device.

#### To view syslog messages for a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.  
The device must be WMI- or SNMP-enabled.
- 3 Click **Syslog** on the right sidebar.

---

## Viewing Details about a Printer

A full range of printing and imaging assets are now collected automatically, introducing monitoring and alerting on a variety of print services, such as toner and print supplies.

Managed Print Services (MPS) provide reduced printer costs and increased printer uptime since you can monitor supplies and maintenance issues.

Managed Workplace discovers network printers automatically. You can now get detailed information about a printer on the **Device Overview Print Services** page. For example, you can get information about toner level and pages printed.

Managed Workplace discovers network printers automatically using SNMP and proprietary protocols. Support for local printers is not yet provided.

Managed Workplace collects automated warranty information for the following printer manufacturers: Apple, Dell, HP, Fujitsu, and Xerox.

**Tip:** You can search for printers using **Device Search**. Click **Status > Device Search**. Select the **Printers** from the **Hardware Type** list and then click **Search**. You can also filter for printers on the **Devices** page using the **Device Role** list.

**Note:** Managed Workplace monitors all printer parameters regardless of whether monitors exist or not.

### To view an overview about a printer

- 1 In Service Center, click **Status > Devices**.
- 2 Click a printer name.

### To view details about print services

- 1 In Service Center, click **Status > Devices**.
- 2 Click a printer name.
- 3 Click **Print Services** on the right sidebar.

To see paper usage for a different time period, select it from the list above the **Paper Usage** graph.

## Viewing Details about a Virtual Machine

Data about virtualized environments is collected and presented on the **Device Overview** page. If the device hosts virtual machines, or is a guest virtual machine, then a Virtual Machine section is visible.

You can

- 
- determine whether a device is a virtual machine, or hosts virtual machines.
  - view the type of virtualization software being used, including version and edition.
  - for host machines, view the number of guest machines being hosted.
  - for virtual machines, view the running state, number of virtual processors, configured memory and storage space configured.

For host machines, you can drill down to view details about the guest virtual machines hosted on that device.

**Note:** In order to have a hyperlink associating the host and guest machines by name, the machines must be part of the same scan range and managed by the same Onsite Manager. If the host and guest machines are Device Managers, or managed by different Onsite Managers, then the guest machines may be detected, but there is no link to view details about the guest machines.

### To view virtual machine details

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.

**Tip:** To filter the list of devices to display virtual machines, from the **Device Role** list, select **VM Guest**.

- 3 In the **Virtual Machine** area, view the following information:
  - host machine name
  - VM software type
  - software version
  - running state
  - number of virtual processors
  - configured memory
  - storage space configured

### To view host machine details

- 1 In Service Center, click **Status > Devices**.

**Tip:** To filter the list of devices to display host machines, from the **Device Role** list, select **VM Host**.

- 2 Click a device name.



---

**3** In the **Virtual Machine - Host** area, view the following information:

- VM software type
- software version
- software edition
- guest count

**Note:** The information available to view depends on the virtualization software.

### To drill to details about guest machines

You can view information about the guest virtual machines on a host machine. The **Device Overview** page for a host machine displays a guest count that includes both monitored and unmonitored guest machines.

You can drill to details about the guest machines to display further information on the **Virtual Machines** page:

- If a guest machine is monitored, you can click the computer name link to open the **Device Overview** page.
- If a guest machine is not monitored, then no link is available but you can still view information including computer name, state, number of processors, memory usage, operating system, and disk space.

**1** In Service Center, click **Status > Devices**.

**2** Click a device name.

**Tip:** To filter the list of devices to display host machines, from the **Device Role** list, select **VM Host**.

**3** In the **Virtual Machines - Host** area, click the **Guest Count** number link.

**4** Optionally, click the name of a monitored guest machine to view details.

## Customizing Devices

You can

- change the device description
- apply a service plan or service directly to the device
- apply an execution schedule to the device, or change the execution schedule applied
- apply a policy to the device
- indicate that a device is a virtual machine

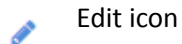
- 
- assign an alias name to a device
  - assign an inventory tag to a device
  - set a location for a device
  - set a custom warranty expiration for a device
  - set an end-of-life date for a device
  - set a production date for a device
  - add a note about a device
  - set a device to be part of a group

### To assign an alias name to a device

Device names are automatically assigned to devices as they are discovered by Onsite Manager. The names, as they initially appear in Service Center are pulled from WMI, SNMP or DNS, and are listed as the discovered name for the device. See [How device names are determined](#).

You can set alias names for devices to make them easier to identify in Service Center. Once an alias name is set for a device, it is used in reports and the Service Center.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to assign an alias name.
- 3 Click the device name.
- 4 Click the edit icon beside **Alias**.



- 5 Type a name and click **Apply**.

### To indicate that a device is a virtual machine

Managed Workplace detects Hyper V and VMWare virtual environments during the asset scan and displays this information on the **Device Overview** page. See [Viewing Details about a Virtual Machine](#).

If the asset scan is unable to detect a virtual machine, you can edit the **Device Overview** page to indicate that the device is a virtual machine.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device that you want to mark as a virtual machine.
- 3 Click the device name.

- 
- 4 Click the edit icon beside **Virtual Machine**.



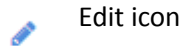
- 5 Select the **Force to yes** option button and click **Apply**.

### To assign an inventory tag to a device

You can specify a unique identifying value for a device, such as a serial number or warranty reference number.

**Note:** The inventory tag is a unique identifier that you can specify.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to assign an inventory tag.
- 3 Click the device name.
- 4 Click the edit icon beside **Inventory Tag**.



- 5 Type an inventory tag and click **Apply**.

### To set a location for a device

You can specify the physical location of the device at the client premises.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to assign a location.
- 3 Click the device name.
- 4 Click the edit icon beside **Location**.



- 5 Type a location and click **Apply**.

### To view the vendor warranty expiration for a device

A vendor warranty is the date a Windows device expires based on warranty information collected from supported vendors. Managed Workplace collects warranty information for the following vendors: Acer, Compaq, Dell, Gateway, HP, IBM, Lenovo, Fujitsu, and Toshiba. To retrieve the warranty information,

---

Managed Workplace requires the asset tag. For IBM and Lenovo, Managed Workplace requires both the asset tag and model number.

Managed Workplace checks hourly for new devices from supported vendors. After the initial retrieval, Managed Workplace refreshes the data monthly.

**Note:** Managed Workplace hides the **Vendor Warranty** box if it can't automatically retrieve the information.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device for which you want to retrieve the vendor warranty expiration.
- 3 Click the device name.

#### To immediately check to see if the vendor warranty has changed

- Click the **Refresh** icon beside **Vendor Warranty**.



Refresh icon

#### To set a custom warranty expiration for a device

You may need to manually set a warranty expiration for a device if Managed Workplace can't collect this information automatically. You may also have negotiated an extended warranty for the customer that goes beyond the default supplied by the vendor. You can use this box to enter that custom warranty expiration.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to assign a warranty expiration.
- 3 Click the device name.
- 4 Click the edit icon beside **Custom Warranty**.



Edit icon

- 5 In the **Custom Warranty** section, click the calendar icon and select a date or type a date. Click **Apply**.

**Tip:** To clear a custom warranty, click the edit icon and delete the date. Click **Apply**.

#### To set an end-of-life date for a device

You can set the expected life expectancy of the device.

- 
- 1 In Service Center, click **Status > Devices**.
  - 2 Locate the device to which you want to assign the end of life.
  - 3 Click the device name.
  - 4 Click the edit icon beside **End-of-Life Date**.

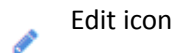


- 5 In the **End-of-Life Date** section, click the calendar icon and select a date or type a date. Click **Apply**.

### To set a production date for a device

You can set the expected production date for the device.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to assign a production date.
- 3 Click the device name.
- 4 Click the edit icon beside **Production Date**.

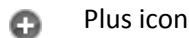


- 5 In the **Production Date** section, click the calendar icon and select a date or type a date. Click **Apply**.

### To add a note about a device

You can add a note about the device. Only one note can be used per device. Timestamps differentiate the notes.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to add a note.
- 3 Click the device name.
- 4 Click the plus icon beside **Notes**.



- 5 Type a note.
- 6 Click **Save**.

---

## Viewing and Changing the Service Plans, Services, and Policies Applied to a Device

The **Device Overview** page displays which service plans, services, and policies have been applied to a device. You can

- view the service plan applied to a device, and determine how it was applied (i.e., via the site or a group to which the device belongs)
- apply a different service plan applied to a device, or remove service plan application
- view services applied to a device, and enable or disable services
- delete services from a device
- view the policies applied to a device, and determine how they were applied
- apply policies directly to a device
- view or change the execution schedule applied to a device

### To view the service plan applied to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 The **Applied Service Plan** section displays the service plan. Optionally, click the service plan name to view or modify the name, description, and icon color.

### To change the service plan applied to a device

When you apply a service plan directly to a device, this manual application will override any future automatic service plan applications. For example, if you apply a service plan to the site to which the device belongs, the service plan you applied on the **Device Overview** page will still be applied to this device.

As a best practice, it is recommended that you apply service plans to sites or groups, for ease of maintenance. For more information, see [Applying a Service Plan to a Site](#).

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.

- 
- 3 In the **Applied Service Plan** section, click the edit icon beside the service plan name.



Edit icon

- 4 Choose a service plan from the list, and click **Save**.

### To view the services applied to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 The **Applied Services** section lists all of the services that have been applied to the device. Hover the mouse over a service name to view how the service was applied, i.e. through which service plan. Optionally, click a service name to open the **Service** page.

### To apply a service to a device

You can manually apply a service directly to a device.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 In the **Applied Services** section, click the plus icon.



Plus icon

- 4 Select a service from the list.
- 5 Optionally, slide the **Disable** slider to disable the added service. You can enable the service on the device at any time.
- 6 Click **Save**.

### To delete a service that was manually applied to a device

When a service was manually applied to a device, you can delete it from the device at any time.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.

- 
- 3 In the **Applied Services** section, click the delete icon beside the manually-applied service you want to remove.



Delete icon

### To enable or disable services applied to a device

You can disable a service that has been applied to a device. This is useful when the service was applied to a device automatically using a service plan, but you do not want the service applied to this particular device.

When a service has been disabled, it is greyed-out in the **Applied Services** section, and you cannot click the service name to open the **Services** page.

After you have disabled a service, you can re-enable it at any time.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 In the **Applied Services** section, for the service you want to disable, move the slider to the left. To re-enable a service, move the slider to the right.

### To view the policies applied to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 The **Applied Policies** area lists all of the policies applied to the device. Hover the cursor over a policy name to view how it was added to the device, i.e. automatically applied because it was applied to the site that the device belongs to.
- 4 Optionally, click the policy name to open the **Policy** page to view details.

### To apply a policy directly to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 In the **Applied Policies** area, click the plus icon:



Plus icon

- 4 Select the type of policy you want to add from the list.
- 5 Select the policy you want to apply from the **Policy** list.



- 
- 6 Click **Apply**.

### To delete a policy that was manually applied to a device

When a policy was manually applied to a device, you can delete it from the device at any time.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 In the **Applied Policies** section, click the delete icon beside the manually-applied policy you want to remove.



Delete icon

### To enable or disable policies applied to a device

You can disable a policy that has been applied to a device. This is useful when the policy was applied to a device automatically using a service plan, but you do not want the policy applied to this particular device.

When a policy has been disabled, it is greyed-out in the **Applied Policies** section, and you cannot click the service name to open the **Policies** page.

After you have disabled a policy, you can re-enable it at any time.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the policy name.
- 3 In the **Applied Policy** section, for the policy you want to disable, move the slider to the left. To re-enable a policy, move the slider to the right.

## Viewing and Changing the Execution Schedules Applied to a Device

### To view the execution schedule applied to a device

The **Applied Schedules** section of the **Device Overview** page displays the execution schedule that was applied to the device, and indicates the way the schedule was applied, i.e. applied to the site to which the device belongs.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 The **Applied Schedule** section displays the execution schedule applied to the device. Optionally, click the execution schedule name to open the **Schedules** page, where you can view and modify the schedule settings.

---

### To change the execution schedule applied to a device

You can change the execution schedule that is applied to the device. If no execution schedule has been applied, you can add one to the device.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the device name.
- 3 In the **Applied Schedule** section, click the **Change Schedule** icon:

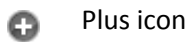


- 4 In the **Applied Schedules** list, select a schedule from the list.  
The **Schedule Details** section updates to display the schedule settings for the newly selected schedule.
- 5 Click **Save**.

## Working with a Device

### To set a device to be part of a group

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device you want to edit.
- 3 Click the device name.
- 4 Click the plus icon beside **Group Membership**.



- 5 Select an existing site or service group to which you want this device to belong.
- 6 Click **Apply**.

To remove a device from a group, click the trash can beside the group of which you no longer want the device to be a member.

### See Also

[Creating Service and Site Groups](#)

### To add a monitor to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.

- 
- 3 Click **Monitors** on the right sidebar.
  - 4 Follow the instructions for adding monitors. See [Adding Your Own Monitors](#).

### To remove a monitor from a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Monitors** on the right sidebar.
- 4 Select the check boxes for the monitors you want to remove.
- 5 Click **More Actions**.
- 6 Click **Delete Monitor**.


### To add a task to a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Automation Calendar** on the right sidebar.
- 4 In the **Calendar**, click **Run Now** to immediately run a task, or click **Schedule** to schedule a task.
- 5 From the **Choose what to execute** list, select a script.
- 6 Schedule the task. See [Adding a Task](#).
- 7 Optionally, set a timeout for the task.
- 8 Optionally, apply an alert configuration to the task.
- 9 Click **Save**.

### To initiate a remote control session on a device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Remote Control** on the right sidebar.

**Tip:** To immediately initiate a remote control session, click the **Remote Control** icon, and then select the remote service from the context menu.

 Remote Control icon

### See Also

---

## [Working Remotely](#)

### To perform a device asset scan on demand

Hardware and software assets are collected at least once every four hours by default. You can refresh this information at any time by requesting the latest assets.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Get Latest Assets** on the right sidebar.

#### Notes:

- If you perform a **Get Latest Assets** on a virtual machine host, VM asset data is collected and the guest virtual machine assets are also scanned.
- If you perform a **Get Latest Assets** on a virtual machine, it is scanned for hardware, software, and operating system data. If the virtual machine host is also part of the scan range, then a **Get Latest Assets** is also performed on the virtual machine host at the same time.

### To exclude a device from management

To find out more about excluding device from management, see [About Excluding Devices from Management](#).

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Exclude Device** on the right sidebar.
- 4 Click **OK**.

### To delete a device

To find out more about deleting devices, see [About Deleting Devices](#).

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Delete Device** on the right sidebar.

## Purging an IP Address from a Device

A stale IP address means that the IP address for a device was previously scanned but has not been detected in recent scans.

---

When another device picks up the same IP address, then the IP address is marked as stale on the original device.

Even though a device may have a stale IP address, you may not want to delete the device. IP addresses may have changed for a device. For example, a device may have been given a new address by DHCP, a manual change or an interface being down.

**Tip:** To prevent discovery of additional valid IP addresses for a device, you can exclude the device from the Onsite Manager scan. See [Excluding Devices Directly](#).

### Prerequisites to Purging an IP Address

To purge a stale IP address from a device, you must have the following:

- more than one IP address listed for the device
- the IP address that you want to purge must have a status of down

### IP Addresses for Workstations

Workstation class machines have only a single IP address tracked by Managed Workplace, even when multiple interfaces are being scanned with separate addressing, and all other IP addresses are removed by the stale IP process.

When a workstation picks up a new IP address, the old address is discarded if it is currently in use by another device and only the current address is displayed. Until this point, it is displayed in red.

### IP Addresses for Servers and SNMP Devices

Unlike workstations, there is no stale IP address cleanup routine run against any server-class Windows device or SNMP device. Few Windows devices are SNMP-enabled, but if one is it would be considered to be a Windows device first (as long as WMI is enabled).

### To purge an IP address from a device

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Browse By** list, select **Site** or **Service Group**, and corresponding selection list entries to show the site, site group or service group that has the device.
- 3 In the **IP Address** column, click the stale IP address, which is red in color.
- 4 Click **Purge IP from this Device**.
- 5 Click **OK**.

---

The purged IP address will no longer be referenced in Service Center or Onsite Manager 5 to 10 minutes after completing this procedure.

## Searching for a Device

You can use the **Device Search** window to quickly find a specific device or many devices in Service Center.

Each time you perform a search, the results appear on a **Results** tab. You can have a maximum of six **Results** tabs. If you perform seven searches, the sixth **Results** tab shows the results for the seventh search.

**Note:** The wildcard symbols (\* and %) are ignored in the **IP Address** box.

What If...	Then...
You want to search all the boxes	Enter search criteria in the <b>All Fields</b> box. All boxes are searched except the <b>Installed Software</b> box.
You enter search criteria in more than one box	Devices that match all conditions are reported back.
You enter partial information in a box	The system searches for anything that contains the entered information.
You enter search criteria in the <b>Device Name</b> box	The system searches the database for Alias Name and discovered names (DNS, SNMP, NetBIOS) as well.
You leave the <b>Results</b> tab open and then log out of Service Center	The <b>Results</b> tabs are still available when you log back into Service Center.

### Examples

To find a device that belongs to a specific user, you can type the user name in the **Last Logged in User** box.

If you enter Dell in the **Manufacturer** box, then all Dell devices are reported back. If you enter server in the **Device Name** box, then all devices with a name that includes 'server' are reported back. However, if you search for both of these at the same time, then all Dell devices with a name that includes 'server' are reported back.

---

### To search for a device

- 1 In Service Center, click **Status > Device Search**.
- 2 Type search criteria in the desired boxes.
- 3 If desired, limit the search results by applying filters from the **Search Filters** section.

**Devices with Alerts** Finds devices with active alerts.

**Intel® vPro™ Devices** Finds Intel® vPro™ Devices.

**Devices Not Allocated to Groups** Finds devices that are not part of site groups or service groups.

- 4 Click **Search**.

### To search for down devices

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **Down Devices** option button.
- 3 Click **Search**.

### To search for devices with alerts

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **Devices with Alerts** check box.
- 3 Click **Search**.

### To search for Intel® vPro™ devices

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **Intel® vPro™ Devices** check box.
- 3 Click **Search**.

### To search for devices not allocated to groups

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **Devices Not Allocated to Groups** check box.
- 3 Click **Search**.

### To search for printers

- 1 In Service Center, click **Status > Device Search**.
- 2 From the **Hardware Type** list, select **Printers**.

- 
- 3 Click **Search**.

#### **To search for mobile devices**

- 1 In Service Center, click **Status > Device Search**.
- 2 From the **Hardware Type** list, select **Mobile Phone** or **Mobile Phone or Tablet**.
- 3 Click **Search**.

#### **To search for virtual machine hosts**

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **VM Host** check box.
- 3 Click **Search**.

#### **To search for virtual machines**

- 1 In Service Center, click **Status > Device Search**.
- 2 Select the **VM Guest** check box.
- 3 Click **Search**.

#### **To restore the search filter defaults**

- In the **Query** tab, click **Restore Defaults**.

#### **To refine the search**

When you refine the search, you are modifying the original search parameters but the results go to a new tab.

- 1 In the **Results** tab, click **Refine**.
- 2 Type search criteria in the desired boxes.
- 3 Click **Search**.

#### **To run the search again**

- In the **Results** tab, click **Refresh**.

#### **To export the search results to CSV or XML**

- In the **Results** tab, click **Export CSV** or **Export XML**.



---

### To close the Results tab

- Click the x in the Results tab.

## Waking Managed Devices Remotely

### About Wake-on-LAN

Managed Workplace can wake any device that supports Wake-on-LAN.

For example, with power management, you typically have computers sleep when not in use. If you have customers who access some of their systems remotely, these systems may be asleep when they want to use them. Managed Workplace provides the ability to allow end users to wake their devices through a web portal. You must give end users at that site a user account to Service Center so that they can wake their computers remotely.

**Note:** You cannot wake computers that are off or set to hibernate.

**Best Practice:** Create one user account per customer site for end users. Alternatively, if the customer has more than 500 devices, create a few logins for the site. For example, create logins for each of the different departments.

### What if waking a computer doesn't work?

Unless a device is AMT-enabled, Managed Workplace uses Wake-on-LAN (WOL) to attempt to wake systems. WOL broadcasts a packet called a Magic Packet targeting the MAC address of the device to be woken. There are a number of reasons why this may not work.

- The Onsite Manager does not have the MAC address for the device. This will be the case if the device is not WMI- or SNMP-enabled.
- The device is not wake-enabled. Typically devices have a BIOS setting that needs to be configured correctly. As well Network Interface Cards must also be configured correctly.
- The device does not support WOL.
- The device has a Device Manager installed. Since these systems monitor themselves, there is no other device to ask to wake it.
- The device is on a different subnet from the Onsite Manager. The wake broadcasts are limited to the subnet in which they originate.

Typically it is a few minutes from the time the wake is requested until the system is accessible.

---

## Creating a User Account for End Users to Wake Computers at a Site

Managed Workplace includes a role called End User that is set up with permissions to access the Wake-on-LAN page in Service Center.

You need to create a user account at each site where power management has been set up, and this user account should have the End User role applied to it.

- 1 Create a user account for each site. See [Creating a User Account](#).
- 2 Add the End User role to the user account. See [Adding a Role to a User Account](#).
- 3 Give the user object access to a device, group or site. See [Setting the Objects a User Account Can Access](#).

**Note:** You can also create a user account for each end user at a site so that that user can only see their own computer.

## Waking a Computer on the Device Overview Page

You can wake a device from the **Device Overview** page as long as Managed Workplace has been able to obtain a MAC address for the device.

- 1 In Service Center, click **Status > Devices**.
- 2 Click the name of the device you want to wake.
- 3 Click **Wake Computer** on the right sidebar.

## Waking a Computer Remotely

- 1 Log in to Service Center using a user account that has the End User role applied to it.
- 2 Select the check box for the device you want to wake.
- 3 Click **Wake Computers**.
- 4 Click **Log Out**.

After a few moments, the computer will be ready to use remotely. Note that Managed Workplace does not provide remoting capabilities to the end user. This must be set up through other means.

## Communicating Steps to End Users for Waking Computers

You must provide steps to end users so that they can log into Service Center to wake their computer if they want to work remotely.

---

For example, here's a sample email you could send to end users. Ensure you provide the following information in the email:

- the address to Service Center
  - the username and password the end user should use
  - optionally, your contact information if users have trouble
- 

As part of our remote management and monitoring service, we have implemented power management at your site. By doing this, our goals are to

- reduce overall energy consumption
- prolong battery life for laptops
- reduce noise
- reduce operating costs for energy and cooling

All these benefits save money and reduce the impact on the environment.

This means that if you want to work remotely, you'll have to first wake your computer if it has been power managed to go to sleep after a period of idle time. (Note that if your computer is off or set to hibernate, you cannot wake it.)

Here are the steps to wake a computer that's set to sleep:

- 1 In a web browser, enter the following address in the address bar:

`<address to Service Center>`

- 2 Log in to Service Center using the following credentials:

Username: `<username>`

Password: `<password>`

- 3 Select the check box for the computer you want to wake.

- 4 Click **Wake Computers**.

- 5 Click **Log Out**.

After a few moments, your computer will be ready to use remotely. If you have trouble waking your computer, please contact `<contact information>`.

Log in using the remote control procedures that your company uses.

---

---

## Working with Intel® vPro™ Devices

### About Intel® vPro™ Devices

Computers built with an Intel® vPro™ chipset are specifically designed to reduce maintenance costs by enabling remote configuration, diagnosis, isolation, and repair of infected computers even when the operating system is unresponsive or the computer is turned off.

To learn more about Intel® vPro™, click [here](#).

**Caution:** Detection and interaction with vPro™ devices is only possible when they are configured in SMB-mode. Devices configured as Enterprise-mode will be handled as not being AMT-enabled.

**Note:** Managed Workplace supports AMT versions 1 to 8.0.0.0.

**Important:** Intel® Active Management Technology™ is by design available to remote systems only. This means that Onsite Managers and Device Managers installed on systems with vPro™ boards will not be able to collect hardware assets and system board events from themselves.

#### To work with Intel® vPro™ devices

- In Service Center, click **Configuration > Intel® vPro™**.

#### See Also

[Setting the Host Name for an Intel® vPro™ Device](#)

[Configuring the Network Settings for an Intel® vPro™ Device](#)

[Enabling or Disabling IDE Redirection \(IDE-R\) for an Intel® vPro™ Device](#)

[Enabling or Disabling Serial-over-LAN \(SOL\)](#)

[Enabling or Disabling User Consent for Intel® KVM](#)

[Configuring the Intel® AMT Administrator Account Credentials](#)

[Viewing the Configuration History of Intel® AMT-Enabled Devices](#)

[Determining the Power Status of Intel® AMT Devices](#)

[Powering-on, Powering-off, or Resetting an Intel® AMT Device Remotely](#)

[Viewing the Status of Intel® AMT-Enabled Devices](#)

[Viewing Intel® AMT Device Events](#)

[Viewing Intel® AMT Device Hardware](#)

---

## Setting the Host Name for an Intel® vPro™ Device

You can specify the computer host name for a selected Intel® AMT device.

**Note:** This is only supported for version 4.0 and later.

**Caution:** For Intel® AMT versions prior to 4.0, if Dynamic Host Configuration Protocol (DHCP) is going to be used to assign the TCP/IP address, then the host name for the Intel® AMT client must be the same as the host name in the operating system.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1** Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
- 2** In the list of Intel® AMT devices, select the check box of the device for which you want to set the host name.
- 3** Click **Set Host Name**.
- 4** In the **Host Name** box, type the host name for the Intel® AMT client and ensure it is the same name as the computer name that is defined in the operating system.
- 5** Click **Save**.

## Configuring the Network Settings for an Intel® vPro™ Device

You can configure Intel® Active Management Technology network settings for the selected Intel® AMT device.

**Note:** This is only supported for version 4.0 and later.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1** Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
- 2** In the list of Intel® AMT devices, select the check box of the device for which you want to configure the network settings.
- 3** Click **Configure Network**.
- 4** In the IP settings for wired connection section, do one of the following:
  - To get the IP settings automatically, select the **Obtain IP settings Automatically (DHCP)** option button.
  - To use static IP settings, select the **Use the Following IP Settings (Static)** option button and enter the IP Address and Subnet Mask information. Optionally, you can enter a Domain Name, a Gateway Address, the Preferred DNS Address, or an Alternate DNS Address.

- 
- 5 Click **Save**.

## Enabling or Disabling IDE Redirection (IDE-R) for an Intel® vPro™ Device

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 In the list of Intel® AMT devices, select the check box of the device for which you want to enable or disable IDE-R.
  - 3 Click **More Actions** and depending on what you want to do, select either **Enable IDE-R** or **Disable IDE-R**.

## Enabling or Disabling Serial-over-LAN (SOL)

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 In the list of Intel® AMT devices, select the check box of the device for which you want to enable or disable SOL.
  - 3 Click **More Actions** and depending on what you want to do, select either **Enable SOL** or **Disable SOL**.

## Enabling or Disabling User Consent for Intel® KVM

**Note:** Enabling or disabling user consent for Intel® KVM in Mozilla Firefox and Google Chrome is not supported.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 In the list of Intel® AMT devices, select the check box of the device for which you want to enable or disable user consent for Intel® KVM.
  - 3 Click **More Actions** and depending on what you want to do, select either **Enable KVM Consent** or **Disable KVM Consent**.

---

## Configuring the Intel® AMT Administrator Account Credentials

To prepare Intel® AMT devices for discovery, you must provide the Global Intel® AMT credentials in Service Center. Global site credentials will be used where valid unless you specify an exception with explicit device credentials. Once the Intel® AMT Administrator account credentials are successfully configured, Managed Workplace can remotely power up and power down the device, monitor events, generate alerts, and collect asset information.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1** Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
- 2** In the list of Intel® AMT devices, enable the check box of the device for which you want to set the credentials.
- 3** Click **More Actions > Configure Credentials**.
- 4** Do one of the following:
  - Select the **Use Site's Default Credentials** option button.
  - Select the **Override Site's Default Credentials** option button. In the **User Name** box, type the Intel® AMT Administrator account user name used with the device. In the **Password** box, type the Intel® AMT Administrator account password that is used with the device and then confirm the password by typing it again in the **Confirm Password** box.
- 5** Click **Save**.

## Viewing the Configuration History of Intel® AMT-Enabled Devices

- In Service Center, click **Configuration > Intel® vPro™**.
- 1** Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
- 2** In the list of Intel® AMT devices, select the check box of the device for which you want to view the configuration history.
- 3** Click **More Actions > View Configuration History**.
- 4** When you are finished viewing the configuration history, click **Close**.

## Determining the Power Status of Intel® AMT Devices

AMT devices will be automatically discovered by the Onsite Manager scan as long as the device has power and the NIC is functioning. This is true even when the device is powered down. As such, these devices will appear as Up. You can

---

modify this behavior by accessing the Intel® Active Management Technology web interface for the device, and disabling the Respond to Ping check box on the Network Settings page. These devices will appear as Down.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 Click the device name of the device for which you want to determine the power status.
  - 3 Click Intel® AMT on the right sidebar.

The power status of the device is indicated in the **Power Status** section.

## Powering-on, Powering-off, or Resetting an Intel® AMT Device Remotely

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 Click the device name.
  - 3 Click **Intel® AMT** on the right sidebar.
  - 4 In the **Power Status** section, depending on what you want to do, click one of the following:
    - **Turn Power On**
    - **Turn Power Off**
    - **Reset**
  - 5 If a confirmation message appears, click **OK**.

## Viewing the Status of Intel® AMT-Enabled Devices

You can see the status of an Intel® AMT-enabled device. Specifically, you can see the Intel® AMT Release number, the Power Status of the device (On or Off), and the Device Status (Up or Down).

**Caution:** Powering down or resetting an Intel® AMT-enabled device may cause user application data loss.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.



- 
- 2 Click the device name.
  - 3 Click **Intel® AMT** on the right sidebar.

You can see status information in the **Intel® AMT Status** section of the window.

## Viewing Intel® AMT Device Events

Intel® AMT events occur at the BIOS level of a device and are classified with severity levels.

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 Click the device name.
  - 3 Click **Intel® AMT** on the right sidebar.
  - 4 Click the **Events** tab.
  - 5 Do the following:
    - To set the number of Intel® AMT events displayed per page, select a value from the **Page Size** list.
    - To filter the results by the Last X Records, select a value from the **Time** list.
    - To filter the results by the source, select a value from the **Event Source** list.
    - To filter the results by severity level, select a value from the **Severity** list.

## Viewing Intel® AMT Device Hardware

- In Service Center, click **Configuration > Intel® vPro™**.
- 1 Click the **Site** or **Service Group** option button and corresponding list entries to show the Site, Site Group or Service Group that has the device.
  - 2 Click the device name.
  - 3 Click **Intel® AMT** on the right sidebar.
  - 4 Click the **Hardware** tab.



## MANAGING MOBILE DEVICES

---

*This section provides detailed information about the following topics:*

- *About Mobile Device Management (MDM)*
  - *Setting Up iOS Mobile Devices for Monitoring*
  - *Setting up Android Mobile Devices for Monitoring*
  - *Viewing Mobile Devices*
  - *Securing Mobile Devices*
  - *Adding a Monitor for Mobile Devices*
  - *About Configuration Profiles*
  - *Setting Up iOS and OS X Configuration Profiles*
  - *Setting up Android Mobile Device Configuration Profiles*
  - *Configuring Email for Mobile Devices*
-

---

## About Mobile Device Management (MDM)

Mobile Device Management (MDM) provides comprehensive monitoring and management capabilities for Apple iOS and Google Android smartphones and tablets.

After a mobile device is enrolled at a site, you can view summary details about the device from within Managed Workplace, including phone numbers, software assets, and hardware details. Advanced features are available depending on the device type; you can view the current geographical location of Android devices, and detect when the device has been rooted. For Apple devices, you can configure Wi-Fi settings to automatically connect to a wireless network. You can also protect business data on the device if it is lost or stolen by using the wipe, lock or set passcode feature.

### Supported Devices

The following devices are supported:

- Apple (minimum supported version iOS 4.0) phones and tablets
- Android (minimum supported version 2.1) phones and tablets

### What You Can Do

You can

- view mobile device details from within Managed Workplace, including phone number and hardware details
- view software assets for mobile devices
- set up monitors for detecting rooted devices and whether the SIM card has been tampered with
- mark a device as lost, and configure whether a lost state automatically triggers an action, such as remotely wiping the device
- set up a monitor to alert if a device has been down for a set period of time
- view current location information for Android devices
- set up security policies for mobile devices
- remotely lock, remove the passcode or even wipe mobile devices

---

## Features by Mobile Device Matrix

The following table identifies what features work with each mobile device:

Feature	Apple	Android
Collect phone number	✓	✓
Alerting of device conditions	✓	✓
Hardware assets	✓	✓
Software assets	✓	✓
Selective wipe (return the device to an unmanaged state)	✓	✓
Remote lock, remove passcode and full wipe	✓	✓
Remote set passcode		✓
Current device location		✓
Restrict access to applications	✓	✓
Configure VPN connection settings	✓	
Security policies	✓	✓
Configure email	✓	✓
Configure Wi-Fi	✓	

## Provisioning Mobile Devices

Monitoring mobile devices is performed by enrollment. You deliver a site-specific provisioning code and a link to users in an email:

- For Android users, you send a link to the enrollment server ([mdm.avg.com](http://mdm.avg.com)), which automatically redirects the user to the Google Play Store to download the AVG Mobile Manager agent on the device. Once the user downloads the agent, they are prompted for the provisioning code. As soon as it is entered, the device is ready for management.
- For Apple users, you send a link to the enrollment server ([mdm.avg.com](http://mdm.avg.com)). When the device user clicks the link, they connect to the enrollment server

---

to retrieve any configuration profiles you have set up. Once the user is connected to the server, they are prompted to enter the provisioning code. However, no agent is downloaded to the device, resulting in fewer clicks for the user.

For more information, see [Enrolling Mobile Devices](#).

**Notes:**

- Mobile devices are scanned every four hours. You can also get the latest assets on a specific device at any time using the Get Latest Assets command on the Device Overview page.
- Each call to the mobile device uses about 31 kb.
- If the mobile device is not able to check in with Service Center, the end user will receive a prompt to open the agent application. Doing so retries the check-in with Service Center.
- MDM for iOS is not supported by Service Centers installed on Windows Server 2003.
- A third-party SSL certificate is required in order to offer mobile device management for both iOS and Android devices. Self-signed certificates are not supported.

## Setting Up iOS Mobile Devices for Monitoring

### About Setting Up iOS Mobile Devices

If you will be monitoring and managing Apple smartphones or tablets for a site, you will need the following:

- An Apple ID (which can be created at <https://appleid.apple.com>).
- A Dun & Bradstreet (D-U-N-S®) number, which is required before enrolling in the Apple Enterprise Developer Program. A D-U-N-S number provides a secure identification system for your company. It is free of charge to obtain a D-U-N-S number. See <https://dnb.com> for more information.
- Enrollment in the Apple Enterprise Developer Program (which can be done at <http://developer.apple.com/programs/ios/enterprise/>). Apple will validate the information you have provided in your application and notify you via email. Enrollment takes about two weeks and costs \$299 annually.

Managed Workplace MDM requires access to APNs (Apple Push Notification service), which is Apple's global notification system. APNs allows a third-party service to securely send messages to any iOS device.

---

You gain access to APNs when you join the Apple Enterprise Developer Program.

**Important:** Once you have successfully enrolled in the Apple Enterprise Developer Program, you must contact Apple and have them list your company as a Mobile Device Management vendor. Until this has been done, you will not have access to create the MDM signing certificate which must be imported into Service Center.

- An MDM Certificate Signing Request (CSR) Signing Certificate. See [Setting Up an MDM Signing Certificate for iOS \(MSP\)](#).

Your customers will need the following:

- An APNs certificate that is the approved version from Apple of the CSR. See [Setting Up an Apple-Approved APNs Certificate for iOS \(Customer\)](#).

**Note:** Certificates for iOS devices are only supported on Service Centers running Windows 2008 or later. You will not see the Certificates option under the Configuration menu if you are not running Windows 2008 or later.

## Setting Up an MDM Signing Certificate for iOS (MSP)

You need an MDM Signing Certificate to manage mobile devices. Only one MDM signing certificate is required. Typically, the MDM signing certificate expires in one year.

**Important:** Before proceeding, you must have completed all prerequisite actions. See [About Setting Up iOS Mobile Devices](#).

Setting up an MDM signing certificate for iOS mobile devices involves the following process:

- 1 In Service Center, create an iOS MDM certificate signing request (CSR). See [Creating an iOS MDM Certificate Signing Request \(CSR\)](#).
- 2 Submit the CSR to Apple.  
<https://developer.apple.com>
- 3 In the Member Center, click **Certificates, Identifiers & Profiles**.
- 4 Click **Certificates**.
- 5 Click the + symbol in the right corner of the window.
- 6 Under **Production**, select MDM CSR.
- 7 Click **Continue**, and then click **Continue** again.
- 8 Click **Choose File** and select the saved MDM Signing Certificate CSR.
- 9 Click **Generate**.

---

10 When it is ready, click **Download** and choose a location to store it locally.

11 Import the MDM signing certificate into Managed Workplace. See [Importing the Apple-Approved MDM CSR Signing Certificate](#).

If you have already created an MDM Signing Certificate with Apple, you can download it by following these steps:

1 In the Member Center, click **Certificates, Identifiers & Profiles**.

2 Click **Certificates**.

3 Select your MDM CSR from the list.

4 Click **Download** and choose a location to store it locally.

5 Import the MDM signing certificate into Managed Workplace. See [Importing the Apple-Approved MDM CSR Signing Certificate](#).

### Creating an iOS MDM Certificate Signing Request (CSR)

1 In Service Center, click **Configuration > Certificates**.

2 Under **MDM CSR Signing Certificate**, click **Create MDM CSR**.

3 Fill in the boxes and click **Create**.

**Legal Company Name** The legally registered name of the company or organization.

**Organization Unit** The name of the department or division in the organization in which the certificate will be used.

**City/Locality** The city in which the company is located. Use official names, not abbreviations.

**State/Province** The province in which the company is located. Use official names, not abbreviations.

**Country/Region** The country in which the company is located.

4 Click **Create**.

5 Click the **Download CSR** link to save the CSR to your desktop.

6 Submit the CSR to Apple for approval.

When Apple approves and provides the MDM signing certificate to the MSP, then the MSP imports the MDM signing certificate in Managed Workplace. See [Importing the Apple-Approved MDM CSR Signing Certificate](#).

### Importing the Apple-Approved MDM CSR Signing Certificate

1 In Service Center, click **Configuration > Certificates**.



- 
- 2 Under **MDM CSR Signing Certificate**, click **Import Certificate**.
  - 3 Click **Browse** to locate the certificate you received from Apple and click **Open**.
  - 4 Click **Import**.

## Setting Up an Apple-Approved APNs Certificate for iOS (Customer)

Each customer with iOS devices to be monitored must have its own unique APNs (Apple Push Notification service) certificate.

**Note:** Apple does not support the use of a proxy server when communicating to a device over APNs.

Here is the process:

- 1 MSP creates APNs CSR for the customer in Managed Workplace and sends to customer. See [Creating an APNs CSR for a Customer](#).
- 2 Customer submits the CSR to Apple.  
<https://identity.apple.com/pushcert>
- 3 Apple approves and provides APNs certificate to customer.
- 4 Customer sends the APNs certificate to MSP.
- 5 MSP imports APNs certificate from customer in Managed Workplace. See [Importing the Apple-Approved APNs Certificate from a Customer](#).

### Creating an APNs CSR for a Customer

You can only create one APNs CSR per customer.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **Pending Customer APNs Certificate Requests**, click **Create APNs CSR**.
- 3 Select the customer site for which you need to generate the APNs certificate.
- 4 Fill in the boxes.

**Legal Company Name** The legally registered name of the company or organization.

**Organization Unit** The name of the department or division in the organization in which the certificate will be used.

**City/Locality** The city in which the company is located. Use official names, not abbreviations.

---

**State/Province** The province in which the company is located. Use official names, not abbreviations.

**Country/Region** The country in which the company is located.

- 5 Click **Create**.
- 6 Click **Download CSR**.  
The file is named as follows:  
`signed_csr_<name of site>`
- 7 Save the CSR to your desktop.
- 8 Email the CSR to the customer.

### Importing the Apple-Approved APNs Certificate from a Customer

After the customer submits the CSR to Apple (<https://identity.apple.com/pushcert>) and Apple approves and provides the APNs certificate to the customer, then the customer sends the APNs certificate to the MSP. Then, the MSP imports the Apple-approved APNs certificate into Managed Workplace.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **Pending Customer APNs Certificate Requests**, select the check box for the customer associated with the APNs certificate you want to import.
- 3 Click **Browse** and locate the file.
- 4 Click **Open**.
- 5 Click **Import**.

After importing the APNs certificate, the certificate appears under Customer APNs Certificate Management. Note that the APNs certificate typically expires after one year.

## Working with iOS Certificates

### Renewing the iOS MDM CSR Signing Certificate

When an existing MDM CSR signing certificate expires, you'll have to upload a new one to replace the existing one.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **MDM CSR Signing Certificate**, click **Create MDM CSR**.
- 3 Fill in the boxes.

**Legal Company Name** The legally registered name of the company or organization.

---

**Organization Unit** The name of the department or division in the organization in which the certificate will be used.

**City/Locality** The city in which the company is located. Use official names, not abbreviations.

**State/Province** The province in which the company is located. Use official names, not abbreviations.

**Country/Region** The country in which the company is located.

- 4 Click **Create**.
- 5 Click **Download CSR**.
- 6 Save the CSR to your desktop.
- 7 Submit the CSR to Apple for approval:  
<https://developer.apple.com>
- 8 When Apple approves and provides the MDM signing certificate to the MSP, in Service Center, click **Configuration > Certificates**.
- 9 Under **MDM CSR Signing Certificate**, click **Replace Certificate**.
- 10 Locate the certificate and click **Open**.
- 11 Click **Import**.
- 12 Click **Browse** and locate the file.
- 13 Click **Open**.
- 14 Click **Import**.

### Deleting the iOS MDM CSR Signing Certificate

If you no longer need to monitor iOS mobile devices at any site, you can delete the MDM CSR signing certificate.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **MDM CSR Signing Certificate**, click **Delete**.
- 3 Click **OK** to confirm the deletion.

### Renewing the APNs Certificate for a Customer

When an existing APNs certificate expires, you'll have to upload a new one to replace the existing one.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **Pending Customer APNs Certificate Requests**, click **Create APNs CSR**.

---

3 Select the customer site for which you need to generate the APNs certificate.

4 Fill in the boxes.

**Legal Company Name** The legally registered name of the company or organization.

**Organization Unit** The name of the department or division in the organization in which the certificate will be used.

**City/Locality** The city in which the company is located. Use official names, not abbreviations.

**State/Province** The province in which the company is located. Use official names, not abbreviations.

**Country/Region** The country in which the company is located.

5 Click **Create**.

6 Click **Download CSR**.

7 Save the CSR to your desktop.

8 Email the CSR to the customer.

The customer will need to browse to the Apple website (<https://identity.apple.com/pushcert>) to renew the expiring certificate and, when prompted, submit the new CSR created above to Apple. When Apple approves and the customer downloads the renewed APNs certificate, then the customer sends the APNs certificate to you. Then, you import the renewed Apple-approved APNs certificate into Managed Workplace.

9 In Service Center, click **Configuration > Certificates**.

10 Under **Pending Customer APNs Certificate Requests**, select the check box for the customer associated with the APNs certificate you want to replace.

11 Click **Browse** and locate the file.

12 Click **Open**.

13 Click **Import**.

After importing the APNs certificate, the certificate appears under Customer APNs Certificate Management and replaces the original. Note that the APNs certificate expiration date has changed.

### **Deleting the Pending APNs Certificate Request for a Customer**

If you no longer are waiting for an APNs certificate from a customer, you can delete it.

- 
- 1 In Service Center, click **Configuration > Certificates**.
  - 2 Under **Pending Customer APNs Certificate Requests**, select the check box for the request you want to delete.
  - 3 Click **Delete**.
  - 4 Click **OK** to confirm the deletion.

### **Deleting the APNs Certificate for a Customer**

If you are no longer managing a site or if the APNs certificate for a site has expired, you can delete the APNs certificate.

- 1 In Service Center, click **Configuration > Certificates**.
- 2 Under **Customer APNs Certificate Management**, select the check box for the customer associated with the APNs certificate you want to delete.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

## **Setting up Android Mobile Devices for Monitoring**

### **About Setting up Android Mobile Devices**

Mobile device management requires that you register with Google Cloud Messaging (GCM), which is Google's push notification system. GCM allows a third-party service to securely send messages to any Android device, and is required to manage and monitor Android devices in Managed Workplace.

If you will be monitoring and managing Google smartphones or tablets for a site, you will need the following:

- A Google account, which can be created at <https://accounts.google.com/signup>.

**Note:** It is recommended that you create a Google account specifically for the GCM service.

- Enrollment in the GCM service, which can be done at <http://developer.android.com/google/gcm/gs.html>. This link is also available from within Service Center, on the Mobile tab in System Settings.

**Note:** New Android functionality requires that the Android device (version 2.2 or higher) has the Market/Google Play application installed and that the user is logged in to their Google account.

---

## Register for Google Cloud Messaging

When you sign up for the Google Cloud Messaging service, you are provided with a Google project number and a server API Key, which you must then enter in Service Center.

Before registering, ensure that you have created a Google account specifically for the GCM service. To create a free account, go to <https://accounts.google.com/signup>.

- 1 Sign in to your GCM service at <http://console.developers.google.com>.
- 2 Click **Create Project**. In the **Project name** box, enter a project name, accept the Terms of Service, and click **Create**.
- 3 Click the **Enable** button.
- 4 Click **Credentials**.
- 5 Click the **Create Credentials** button, then click **API key**.
- 6 Click the **Android key** button.
- 7 In the **Name** box, enter a name.
- 8 Click **Create**. Make a note of the API key for later use.
- 9 Click the name of the project in the menu bar to the right of the search box, then click **Manage all projects**.
- 10 Select the check box next to your project, then click **Settings** in the navigation bar.
- 11 Make a note of the project number for later use.
- 12 Log into AVG Managed Workplace Service Center.
- 13 In Service Center, click **Configuration > System Settings**.
- 14 Click the **Mobile** tab.
- 15 Fill in the following boxes:
  - **Google Project Number**—enter the project number you noted in step 12.
  - **Server API Key**—enter the API key you noted in step 9.
- 16 Click **Save**.

## Modify the GCM Account

You can modify the Google Project number and the API key, for example if the project number gets compromised. When you modify a GCM account, all

---

currently enrolled devices automatically use the new account the next time they check in to Service Center.

**Note:** If you modify a GCM account with an incorrect project number or API key, enrolled Android devices will not respond to Google Cloud Messaging. After entering the correct project number and API key, you must then re-enroll Android devices with the correct GCM settings.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Mobile** tab.
- 3 Under **Account for Google Cloud Messaging**, click **Modify**.
- 4 In the **Project Number** box, enter a new project number.
- 5 In the **Server API Key** box, enter a new **API key**.
- 6 Click **Save**.

## Enrolling Mobile Devices

### About Provisioning Mobile Devices

To set up mobile devices, you generate and deliver a site-specific provisioning code to users in an email. For Android users, you must also include a link where the Mobile Manager agent appropriate for the device can be installed. Once the user downloads the Mobile Manager agent, they will be prompted for their provisioning code. As soon as it is entered, the device is ready for management.

The enrollment process differs slightly for Apple devices, which rely on an agentless solution for mobile management. When you send the provisioning code to Apple device users via email, you must also include a link to the enrollment server URL. When the user clicks the link, the device connects to the enrollment server, which builds the configuration profile and sends it to the device. The Mobile Manager agent is not installed, resulting in fewer configuration steps for the Apple device user.

A provisioning code needs to be provided on a site-by-site basis so that Managed Workplace knows which device belongs to which site. If a new mobile device needs to be monitored, you must send a provisioning code to the end user of the new mobile device.

The provisioning code expires after a set period of time, but you can regenerate one at any time. It is possible to enroll multiple devices under a single code.

---

**Important:** To generate provisioning codes, a role must be set up with Site Management permission. For more information on role management, see [Setting Permissions for a Role](#).

## Generating a Provisioning Code for Mobile Devices at a Site

The steps for generating and emailing a provisioning code is very similar for Apple and Android mobile devices.

- 1 In Service Center, click **Site Management > Sites**.
- 2 Click the name of the site.
- 3 Click the **Mobile** tab.
- 4 Click **Generate Provisioning Code**.
- 5 Note the provisioning code.

The provisioning code is a six-character alpha (case-insensitive) string.

- 6 Notify the mobile device owner about the provisioning code, and include the following address.

<http://mdm.avg.com>

For Android devices, this link detects the device type and downloads the Mobile Manager agent from the Google Play Store.

For Apple iOS devices, this link redirects the user to a website that prompts them for the provisioning code and their user name. They must then follow the onscreen instructions to install the MDM Configuration Profile. An iOS web clip will also be installed on the device, which is used to specify the user's email settings if an email configuration profile is sent to the device.

For example, here's a sample email you could send to end users. Ensure you provide the provisioning code in the email. You may also want to include the expiration date for the code.

.....

Your mobile device needs to be enrolled in our corporate Mobile Device Management (MDM) system.

As part of the enrollment process, you will be asked to provide the following:

- Enrollment Code: <CODE>
- Full name



---

From your mobile device, click the following link and follow the instructions:

<http://mdm.avg.com>

---

After the end user follows the instructions in the email, the mobile device is ready for management and monitoring.

**Notes:**

- If a mobile device is enrolled in the wrong site, then delete the device in Service Center and re-enroll the device using the correct provisioning code for the site.
- If the application is not installed when re-enrolling a device, the device will not appear in Service Center until the scheduled check-in up to four hours later.
- If a site is on hold, the device is still enrolled.
- If a site that contains a mobile device is deleted, the device will be deleted in Service Center. The Mobile Manager agent, the MDM profile and any configuration profiles will need to be manually uninstalled on the mobile device.

## Viewing Mobile Devices

### Viewing a List of Mobile Devices at a Site

You can view a list of all the mobile devices that belong to a customer or site from the Devices list.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.

You can view a list of all the mobile devices that belong to a customer or site from the Central Dashboard.

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of the site.
- 3 Click **Mobile Devices** on the right sidebar.

**Tip:** You can filter by platform using the Platform list.

---

Mobile devices are indicated by a Mobile Device icon.



Mobile Device icon

## Viewing Details about a Mobile Device

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.

As with any device, you can get more information using the commands on the right sidebar:

[Viewing Hardware Installed on a Mobile Device](#)

[Viewing Software Installed on a Mobile Device](#)

[Getting the Latest Assets on a Mobile Device](#)

[Locking a Mobile Device](#)

[Setting the Passcode for a Mobile Device](#)

[Wiping Data from a Mobile Device](#)

## Viewing Hardware Installed on a Mobile Device

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Hardware** on the right sidebar.

## Viewing Software Installed on a Mobile Device

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Software** on the right sidebar.

## Getting the Latest Assets on a Mobile Device

- 1 In Service Center, click **Status > Devices**.

- 
- 2 From the **Device Role** list, select **Mobile**.
  - 3 Click the name of the mobile device.
  - 4 Click **Get Latest Assets** on the right sidebar.

## Locating a Mobile Device

Use to audit the activity of the mobile workforce or to assist law enforcement with recovery operations.

**Note:** This feature is applicable for Apple devices that were deployed before Managed Workplace 2013 R1 FP1. This feature is not applicable for Apple devices that were enrolled using an agentless solution, introduced in Managed Workplace 2013 R1 FP1. For more information, see [About Provisioning Mobile Devices](#).

### To locate a mobile device

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.

The Geo-Tracking section shows live global positioning information about the device. To see historical data about the device, use the MDM Device Summary report.

- 4 Click the map icon to see the device in Google Maps.

## Securing Mobile Devices

### About Securing Mobile Devices

MDM provides users extra security assurance when the device contains personal or other sensitive information your clients want to protect. In the event that a device is lost or stolen, you can configure a lost device action that remotely and automatically locks out access and resets the passcode, or wipes the device of all data and restores it to factory defaults. You can also remotely lock a mobile device, remove or set the passcode, and wipe data.

**Note:** The Lock, Remove Passcode and Wipe commands are applicable for Apple and Android devices. The Set Passcode command is only available for Android devices.

---

**Important:** To secure mobile devices, you must ensure the user account and role are set up to have permissions to device management for mobile device access.

Permission
<b>Device Management</b>
<input type="checkbox"/> Remote Control Access
<input type="checkbox"/> Onsite Manager Utilities
<input type="checkbox"/> Remote Management Tools
<input type="checkbox"/> Mobile Devices
<input type="checkbox"/> Wipe
<input type="checkbox"/> Lock
<input type="checkbox"/> Reset/Remove Passcode
<input type="checkbox"/> Mark As Lost
<input type="checkbox"/> Lost Device Actions/Alert

## Locking a Mobile Device

A passcode protects information and data on the mobile device. Remotely locking a device denies access to the device until the existing passcode is entered correctly.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Lock** on the right sidebar.

## Setting the Passcode for a Mobile Device

A passcode protects information and data on the mobile device. Remotely setting the passcode lets you set a passcode and lock out the user who doesn't have the new passcode.

You can also clear the passcode so that there is no passcode and the user can enter a new one.

**Note:** This feature is applicable for Android devices.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Set Passcode** on the right sidebar.

- 
- 5 Do one of the following:
    - If you want the user to be locked out, in the New Passcode box, type a passcode.
    - If you want the user to enter a new passcode, leave the New Passcode box empty.
  - 6 Click **Set Passcode**.

## Removing the Passcode for a Mobile Device

A passcode protects information and data on the mobile device. Removing the passcode clears the passcode so that there is no passcode and the user can enter a new one.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Remove Passcode** on the right sidebar.

## Wiping Data from a Mobile Device

Wiping restores the device to factory defaults and deletes all the data. You may want to wipe a device if it has been lost or stolen and contains sensitive data.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Wipe** on the right sidebar.

Once you click Wipe and confirm the operation, the device will initiate a factory reset. This cannot be undone.

## Configuring Lost Device Actions for Mobile Devices

You can select which action is triggered when a mobile device is marked as lost. By default, when a device is marked as lost, there is no action triggered. You can choose to set a new passcode and lock the device, or you can wipe the device.

---

**Note:** You can only set passcode and lock for Android devices.

What if...	Then...
the lost device action is set to new passcode and lock	the device immediately locks and the user is prompted to enter a new passcode
the lost device action is set to wipe and the device is turned on	all data on the device is immediately deleted and the device settings are restored to factory defaults
the lost device action is set to wipe and the device is turned off	when the device is powered back on, data on the device is deleted and the device settings are restored to factory defaults

**Important:** If you choose to wipe lost mobile devices, this action is not reversible after the device has been marked as lost. This important security feature prevents unauthorized persons from preventing the wipe from occurring.

**Best Practice:** Lost device actions can be configured system-wide and optionally by site. You can first set up a default lost device action in System Settings, and then override the system settings on a site-by-site basis as required.

### To configure system-wide lost device actions

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Mobile** tab.
- 3 Under **Lost Device Actions and Check-In Actions Alert Configuration**, for iOS devices, select one of the following options:
  - Wipe** the device is wiped of all data and reset to factory defaults
  - Do Nothing** no action is taken
- 4 For Android devices, select one of the following options:
  - Wipe** the device is wiped of all data and reset to factory defaults
  - Lock** the device is locked and the passcode is reset. In the box, enter a passcode that Android users must enter to unlock the device.
  - Do Nothing** no action is taken

- 
- 5 Click **Save**.

### To configure lost device actions for a site

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the name of the site.
- 3 Click the **Mobile** tab.
- 4 Under **Lost Device Actions and Check-In Alert Configuration**, click **Modify**.
- 5 If the **Use System Defaults** check box is selected, clear it.
- 6 For iOS devices, select one of the following options:
  - Wipe** the device is wiped of all data and reset to factory defaults
  - Do Nothing** no action is taken
- 7 For Android devices, select one of the following options:
  - Wipe** the device is wiped of all data and reset to factory defaults
  - Set Passcode and Lock** the device is locked and the passcode is reset. In the box, enter a passcode that Android users must enter to unlock the device.
  - Do Nothing** no action is taken
- 8 Click **Save**.

### To configure system-wide alert actions for lost devices

- 1 In Service Center, click **Configuration** > **System Settings**.
- 2 Click the **Mobile** tab.
- 3 Under **Lost Device Actions and Check-In Actions Alert Configuration**, select any of the following:
  - Alert Categories** Click **Categorize Alert** to add or remove alert categories. See [About Alert Categories](#).
  - Alert Actions** Select the **Create Trouble Ticket** check box to automatically generate a trouble ticket when a device is marked as lost. See [Setting an Alert to Create a Trouble Ticket](#).
  - Alert Notifications** Select the **Send Email** check box, then click **Send Email** to specify the users that will receive email alert notifications. See [Setting an Alert to Send an Email](#).
  - Escalation Notification** Select the **Escalate Alert** check box, then click **Escalate Alert** to configure escalation actions. See [Escalating an Alert](#).

- 
- 4 Click **Save**.

### To configure alert actions for lost devices by site

- 1 In Service Center, **Site Management > Sites**.
- 2 Click the name of the site.
- 3 Click the **Mobile** tab.
- 4 Under **Lost Device Actions and Check-In Alert Configuration**, click **Modify**.
- 5 If the **Use System Defaults** check box is selected, clear it.
- 6 Select any of the following:

**Alert Categories** Click **Categorize Alert** to add or remove alert categories. See [About Alert Categories](#).

**Alert Actions** Select the **Create Trouble Ticket** check box to automatically generate a trouble ticket when a device is marked as lost. See [Setting an Alert to Create a Trouble Ticket](#).

**Alert Notifications** Select the **Send Email** check box, then click **Send Email** to specify the users that will receive email alert notifications. See [Setting an Alert to Send an Email](#).

**Escalation Notification** Select the **Escalate Alert** check box, then click **Escalate Alert** to configure escalation actions. See [Escalating an Alert](#).

- 7 Click **Save**.

## Mark a Mobile Device as Lost

Marking a device as lost triggers any configured lost device actions in mobile devices.

**Important:** If you mark a device as lost and the configured lost device action is to wipe the device, this action is not reversible. For example, resetting the mobile device to Mark as Found does not prevent the mobile device from being wiped. This important security feature prevents unauthorized persons from preventing the wipe from occurring.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Mark as Lost** on the right sidebar.



---

## Mark a Lost Mobile Device as Found

You can reset the status of a lost mobile device to found. When a device is marked as found, any existing alerts and trouble tickets generated by the lost device checking in is cleared.

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Mark as Found** on the right sidebar.

## Adding a Monitor for Mobile Devices

You can set up a monitor to alert on mobile device conditions including the following:

- whether an Android device has been rooted. If an Android device has been rooted, the operating system can be completely removed, and the device warranty can become void.
- if the device has been unavailable for a set period of time
- whether the SIM card has been tampered with so that you can validate the device owner
- whether the device is roaming.

You can apply these monitors to individual devices. Or, you can create a new monitoring policy that includes these monitors and apply it to a service group that contains all mobile devices.

**Note:** Mobile devices are scanned every four hours. You can also get the latest assets on a specific device at any time using the Get Latest Assets command on the Device Overview page.

### To apply a monitor to a mobile device

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Mobile Device**.
- 6 Click **Add Monitor**.

- 
- 7 In the **Monitor** tab, type a title for the monitor.
  - 8 Optionally, type a description for the monitor.
  - 9 Do one of the following:
    - To alert if a rooted mobile device is detected, select **Jailbreak Detection**.
    - To alert if a mobile device has not reported in to Service Center for a specified time period, select **Mobile Device Availability**.
    - To alert if SIM card tampering on a mobile device is detected, select **SIM Card Tampering Detection**.
    - To alert if the device is roaming, select **Roaming Detection**.
  - 10 To configure an alert, see [Setting Alert Actions](#).
  - 11 Click **Save**.

#### To add a mobile device monitor to a monitoring policy

- 1 Create a new monitoring policy. See [Creating a Custom Monitoring Policy](#).
- 2 Click **Configuration > Monitors & Alert Rules**.
- 3 Select the **Monitoring Policy** icon.
- 4 From the **Monitoring Policy** list, select the monitoring policy you created in step 1.
- 5 Click **Add Monitor**.
- 6 From the **Choose Monitor Type** list, select **Mobile Device**.
- 7 Click **Add Monitor**.
- 8 In the **Monitor** tab, type a title for the monitor.
- 9 Optionally, type a description for the monitor.
- 10 Do one of the following:
  - To alert if a rooted mobile device is detected, select **Jailbreak Detection**.
  - To alert if a mobile device has not reported in to Service Center for a specified time period, select **Mobile Device Availability**.
  - To alert if SIM card tampering on a mobile device is detected, select **SIM Card Tampering Detection**.
- 11 To configure an alert, see [Setting Alert Actions](#).
- 12 Click **Save**.

---

## About Configuration Profiles

Configuration profiles determine how Android smartphones and tablets, iPad, iOS, and OS X devices are configured and managed. Management functions are completed behind the scenes without any user interaction required.

You can set up the following configuration profiles:

### OS X and iOS

**Passcode** Configures passcode settings for iOS and OS X devices. See [Configuring Passcode Settings for iOS Mobile Devices and OS X Devices](#).

**Network** Configures the Wi-Fi network interface for iOS and OS X devices, including the profile name and Service Set Identifier (SSID). See [Configuring Network Settings for iOS and OS X Devices](#).

**Security and Privacy** Configures Gatekeeper settings, and whether to send diagnostic and usage data to Apple. See [Configuring Security and Privacy Settings for iOS and OS X Devices](#).

**VPN** Configures VPN connection settings for iOS and OS X devices. See [Configuring VPN Settings for iOS and OS X Devices](#).

### iOS Only

**Exchange** Configures settings for Microsoft Exchange Server. See [To configure an iOS email policy for EAS solutions](#).

**Mail** Configures the email client on a managed iOS mobile device. See [To configure an iOS email policy for POP and IMAP solutions](#).

**Restrictions** Configures options for iOS devices, such as whether FaceTime or installation of apps is allowed. See [Configuring Restrictions for iOS Mobile Devices](#).

### OS X Only

**Energy Saver** Configures wake and sleep options to conserve energy on the OS X device. See [Configuring Energy Saver Settings for OS X Devices](#).

**Parental Controls** Configures content filtering and time limit settings on the OS X device. See [Configuring Parental Controls for OS X Devices](#).

**Restrictions** Configures options for OS X devices, such as whether Bluetooth or printing is allowed. See [Configuring Restrictions for OS X Devices](#).

**Software Update** Configures the URL for the Software Update server. See [Configure the OS X Software Update Server](#).

### Android

---

**Passcode** Configures passcode settings for Android mobile devices. See [Configuring Passcode Settings for Android mobile devices](#).

**Exchange** Configures the email client on a managed Android mobile device. See [Configuring Email Policies for Android Mobile Devices](#).

**Restrictions** Configures camera restrictions for Android devices. See [Configuring Restrictions for Android Mobile Devices](#).

Before setting up configuration profiles, you must ensure you have completed the following steps:

- 1 For iOS and OS X devices, you must have an MDM signing certificate, which is used to create an Apple Push Notification service (APNs) certificate. See [Setting Up iOS Mobile Devices for Monitoring](#). For Android devices, you must register with Google Cloud Messaging (GCM). See [Setting up Android Mobile Devices for Monitoring](#).
- 2 For OS X devices, you must run the OS X Prep Utility, which prepares the device for management. You must also install the Management Profile when running this utility. See [To run the OS X Prep Utility](#).
- 3 Finally, you must create a service group or site group. Configuration profiles are applied at the group level, and are automatically installed on all devices in the group that meet the requirements for the configuration profiles. See [Creating Service and Site Groups](#).

**Notes:**

- When an iOS user upgrades from iOS 6.3.1 to iOS 7, iOS Mobile Manager is reset. The MDM base profile remains intact and continues to report to Service Center, and configuration profiles continue to work. However, the device user must launch iOS Mobile Manager, which opens the enrollment page.
- For iOS mobile devices, deleting the device from Service Center will result in the MDM profile and any configuration profiles being uninstalled from the device. If the iOS device happens to be powered off during device deletion, the profiles will be uninstalled when the device is powered back on.
- In the case where the iOS mobile device happens to drop network connectivity prior to the device being deleted or configuration profiles being added/deleted from Service Center, the profile list will be updated when the device regains network connectivity OR the next time the device checks in with Service Center.

---

## Setting Up iOS and OS X Configuration Profiles

### Configuring Passcode Settings for iOS Mobile Devices and OS X Devices

You can configure passcode settings for iOS and OS X devices. All devices enrolled in MDM and that belong to the group to which the configuration profile is applied will have these passcode settings applied.

The most restrictive setting applies.

What if...	Then...
The Apple Passcode policy has been created with an auto-lock setting of 4 minutes	The end user can change this setting to any number between 1 and 4. If the existing device setting was set to auto-lock after 5 minutes, the device would now be set to auto-lock after 4 minutes.
The Apple Passcode policy has been created with an auto-lock setting of 4 minutes, and the end user has changed the setting to 1 minute. If the MSP resets the auto-lock setting to 5 minutes	The end user's setting of 1 minute remains in effect.

**Note:** Only one Apple Passcode policy can be created per group.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Please select a profile** list, under **OS X and iOS**, select **Passcode**.
- 6 Click **OK**.
- 7 Set the options.

**Allow simple value** Permits users to use sequential or repeated characters in their passcodes. (For example, this would allow the passcodes "3333" or "DEFG.")

---

**Require alphanumeric value** Requires that the passcode contain at least one letter or number.

**Minimum passcode length** Specifies the minimum number of characters a passcode can contain.

**Minimum number of complex characters** The number of non-alphanumeric characters (such as \$, &, and !) that the passcode must contain.

**Maximum passcode age** Requires users to change their passcode at the interval you specify. If you specify 0, users never have to change their passcode.

**Maximum Auto-Lock** If the device isn't used for the period of time you specify, it automatically locks. Entering the passcode unlocks it. If you specify 0, the device never automatically locks.

**Passcode history (iOS only)** A new passcode won't be accepted if it matches a previously used passcode. You can specify how many previous passcodes are remembered and compared.

**Maximum grace period for device lock (iOS only)** Specifies how soon the device can be unlocked again after use, without prompting again for the passcode. Setting this to None requires a passcode at every unlock.

**Maximum number of failed attempts** Determines how many failed passcode attempts can be made before the device is wiped.

**Important:** After six failed passcode attempts, the device imposes a time delay before a passcode can be entered again. The time delay increases with each failed attempt. After the final failed attempt, all data and settings are securely erased from the device. The passcode time delay begins after the sixth attempt, so if you set this value to 6 or lower, no time delay is imposed and the device is erased when the attempt limit is exceeded.

**8** Click **Save**.

After you have saved the configuration policy, it is automatically deployed to the enrolled iOS and OS X devices in the group.

## Configuring Network Settings for iOS and OS X Devices

You can set how the iOS mobile device connects to the wireless network. In order for the user to initiate a connection, these settings must be specified and must match the requirements of your network.

By using a network settings policy, end users do not need to know the Wi-Fi password. They will be automatically connected.

- 
- 1 In Service Center, click **Configuration > Groups**.
  - 2 Click the name of the group.
  - 3 Click the **Policies** tab.
  - 4 Under **Configuration Profiles**, click **Add**.
  - 5 From the **Choose Profile Type** list, under **OS X and iOS**, select **Network**.
  - 6 Click **OK**.
  - 7 In the **Profile Name** box, type a name for the policy.
  - 8 In the **Service Set Identifier** box, type the SSID of the wireless network to connect to.
  - 9 Select the **Hidden Network** check box to specify whether the network is broadcasting its identity.
  - 10 Select the **Auto Join** check box to specify whether the device automatically joins the wireless network.
  - 11 From the **Proxy Setup** list, select one of the following:
    - None** The network doesn't use a proxy server.
    - Manual** The network uses the proxy server settings you provide. When this option is selected, you must also enter the Proxy Server and Port number, proxy username and the password used to authenticate with the proxy in the boxes provided.
    - Automatic** The DHCP server is configured to provide the proxy settings, When this option is selected, you must also enter the proxy server URL in the box provided.
  - 12 From the **Security Type** list, select one of the following:
    - None** The network doesn't use authentication.
    - WEP** The network uses WEP authentication only.
    - WPA/WPA 2** The network uses WPA authentication only.
    - Any** The device uses either WEP or WPA authentication when connecting to the network but won't connect to non-authenticated networks.
  - 13 Click **Save**.

After you have saved the iOS mobile device configuration policy, it is automatically deployed to the enrolled iOS and OS X devices in the group.

---

## Configuring Security and Privacy Settings for iOS and OS X Devices

Security and privacy settings allow you to set limits on the data that is uploaded from and downloaded to the device.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **OS X and iOS**, select **Security & Privacy**.
- 6 Click **OK**.
- 7 To send diagnostic and usage data to Apple for analysis, select the **For OS X devices, send diagnostic and usage data to Apple data check box**.

For OS X devices, this allows for diagnostic and usage data to be sent to Apple. For iOS devices, this allows for the user to submit diagnostic and usage data to Apple.

- 8 From the **Gatekeeper (OS X only)** list, select one of the following:
  - Mac App Store** Applications can be downloaded from the Mac App Store.
  - Mac App Store and identified developers** Applications can be downloaded from the Mac App Store and developers with a unique Developer ID from Apple.
  - Anywhere** Applications can be downloaded from any source.
- 9 To prevent users from overriding the Gatekeeper setting, select the **Do not allow user to override Gatekeeper setting (OS X only) check box**.
- 10 Click **Save**.

## Configuring VPN Settings for iOS and OS X Devices

You can configure VPN connection settings, which allows the iOS or OS X device user to connect to the VPN without having to enter the VPN name or password.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.



- 
- 5 From the **Choose Profile Type** list, under **OS X and iOS**, select **VPN**.
  - 6 Click **OK**.
  - 7 In the **Connection Name** box, type the display name of the VPN connection.
  - 8 From the **Connection Type** list, select one of the following:
    - L2TP** Select if you are using a Layer 2 Tunneling Protocol (L2TP) to support your VPN network.
    - PPTP** Select if you are using a Point-to-Point Tunneling Protocol (PPTP) to support your VPN network.
  - 9 In the **Server** box, type the hostname or IP address of the VPN server.
  - 10 In the **Account** box, type the user account name for authenticating the VPN connection.
  - 11 From the **User Authentication** list, select one of the following:
    - Password** Authentication is enabled by a password. When you select this option, you must provide the password in the Password box that appears.
    - RSA SecurID** Authentication is enabled by RSA SecurID, a mechanism that performs two-factor authentication to the VPN.
  - 12 If you are using a shared secret to secure communication, type it in the **Shared Secret** box.
  - 13 To route all network traffic through the VPN connection, select the **Send All Traffic** check box.
  - 14 From the **Proxy Setup** list, select one of the following:
    - None** The network doesn't use a proxy server.
    - Manual** The network uses the proxy server settings you provide. When this option is selected, you must enter the Proxy Server and Port number, proxy username and the password used to authenticate with the proxy server in the boxes provided.
    - Automatic** The DHCP server is configured to provide the proxy settings. When this option is selected, you must enter the proxy server URL in the box provided.
  - 15 Click **Save**.

---

## Configuring Restrictions for iOS Mobile Devices

- 1 You can configure restrictions for iOS devices, such as whether FaceTime or installation of apps is allowed. In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **iOS**, select **Restrictions**.
- 6 Click **OK**.
- 7 Set the options.

**Allow use of camera** When this option is off, cameras are completely disabled and the Camera icon is removed from the Home screen. Users can't take photographs or videos, or use FaceTime.

**Allow FaceTime** When this option is off, users can't place or receive FaceTime video calls.

**Allow Photo Stream (disallowing can cause data loss)** When this option is off, users can't enable Photo Stream. Disallowing Photo Stream will erase Photo Stream photos from the user's device and prevent photos from the Camera Roll from being sent to Photo Stream. If there are no other copies of these photos, they may be lost.

**Allow Shared Photo Streams** When this option is off, users can't share photos with other users over iCloud.

**Allow screen capture** When this option is off, users can't save a screenshot of the display.

**Allow use of iMessage (Supervised devices only)** When this option is off, users can send or receive text messages using iMessage.

**Allow installing apps** When this option is off, the App Store is disabled and its icon is removed from the Home screen. Users are unable to install or update their apps using the App Store or iTunes.

**Allow In-App purchase** When this option is off, users can't make in-app purchases.

**Require iTunes password for all purchases** When this option is selected, users must enter their iTunes password before completing any purchases on their iOS device.

**Allow iCloud backup** When this option is off, users can't back up their device to iCloud.

---

**Allow iCloud document syncing** When this option is off, users can't store documents on iCloud.

**Allow automatic sync while roaming** When this option is off, devices that are roaming will not sync automatically but wait until connected via Wi-Fi to reduce data charges. Allowing automatic synchronization while roaming can lead to larger-than-expected data costs.

**Allow voice dialing** When this option is off, users can't dial their phone using voice commands.

**Force encrypted backups** When this option is off, users can choose whether or not device backups performed in iTunes are stored in encrypted format on their computer. If any profile is encrypted and this option isn't turned off, encryption of backups is required and enforced by iTunes.

**Allow Siri** When this option is off, the Siri voice-recognition application is disabled and its icon is removed from the Home screen.

**Allow Siri while device is locked** When this option is off, users can't use Siri, voice commands, or dictation.

**Allow Passbook while device is locked** When this option is off, users can't access Passbook tickets, coupons, and gift cards when the device is locked.

**Allow accepting untrusted TLS certificates** When this option is off, users will not be asked if they want to trust certifications that cannot be verified. This setting applies to Safari and to Mail, Contacts, and Calendar accounts.

**Allow Installation of configuration Profiles (Supervised devices only)** When this option is off, configuration profiles cannot be installed on the iOS device.

**7** Click **Save**.

After you have saved the iOS mobile device configuration policy, it is automatically deployed to the devices in the group.

## Configuring Energy Saver Settings for OS X Devices

You can conserve energy on managed OS X devices by setting options for sleeping and waking, and setting up a schedule for starting up and shutting down the device.

### To set sleep and wake options for OS X devices

- 1** In Service Center, click **Configuration > Groups**.

- 
- 2 Click the name of the group.
  - 3 Click the **Policies** tab.
  - 4 Under **Configuration Profiles**, click **Add**.
  - 5 From the **Choose Profile Type** list, under **OS X**, select **Energy Saver**.
  - 6 Click **OK**.
  - 7 Do one of the following:
    - To set sleep and wake options for desktop OS X devices, click **Desktop**.
    - To set sleep and wake options for portable desktop devices when the device is powered by battery, click **Portable on Battery**.
    - To set sleep and wake options for portable desktop devices while plugged in, select **Portable Plugged In**.
  - 8 In the **Sleep Options** area, set the following options:
    - To set the period of inactivity before the computer goes to sleep, select the **Put the computer to sleep after** check box, and then use the slider to set the time period.
    - To set the period of inactivity before the display goes to sleep, select the **Put the display to sleep after** check box, and then use the slider to set the time period.
  - 9 To put the device's hard disk to sleep, select the **Put the hard disks to sleep whenever possible** check box.
  - 10 In the **Wake Options** area, set the following options:
    - To wake the device when an administrator attempts to access the device through Ethernet, select the **Wake for Ethernet network administrator access** check box.
    - For desktop devices, to allow the user to press the power button to put the device to sleep, select the **Allow power button to sleep the computer** check box.
  - 11 To start the device after a power failure, in the **Other Options** area, select the **Start up automatically after a power failure** check box.
  - 12 Click **Save**.

### To set a start up and sleep schedule for OS X devices

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.

- 
- 4 Under **Configuration Profiles**, click **Add**.
  - 5 From the **Choose Profile Type** list, under **OS X**, select **Energy Saver**.
  - 6 Click **OK**.
  - 7 Click **Schedule**.
  - 8 To set a schedule for starting up OS X devices:
    - a Select the **Start up the computer** check box.
    - b From the list, select one of the frequency options, for example every day, every weekday, or on a specific day of the week.
    - c Click the clock icon and select a time of day from the Time Picker.
  - 9 To set a schedule for shutting down or putting OS X devices to sleep:
    - a Select the **Shut down or sleep** check box.
    - b Select either the **Shut Down** or **Sleep option** button.
    - c From the list, select one of the frequency options, for example every day, every weekday, or on a specific day of the week.
    - d Click the clock icon and select a time of day from the Time Picker.
  - 10 Click **Save**.

## Configuring Parental Controls for OS X Devices

You can configure parental controls to prevent OS X users from accessing websites you deem unsafe or inappropriate. You can also hide profanity in the Dictionary application.

### Notes:

- Parental control settings apply to all OS X users. Administrative users that are affected by these policies can override these settings by entering their administrative password.
- You must prefix the Allow URLs and Deny URLs with `http` or `https` for the settings to be implemented on the device.
- OS X devices may need to be rebooting for these settings to take effect.

### To set content filtering options for OS X devices

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.

- 
- 4 Under Configuration Profiles, click **Add**.
  - 5 From the **Choose Profile Type** list, under **OS X**, select **Parental Controls**.
  - 6 Click **OK**.
  - 7 Click the **Content Filtering** button at the top of the screen.
  - 8 To prevent inappropriate words from displaying in the Dictionary application, select the **Hide profanity in Dictionary** check box.
  - 9 **To limit access to specific URLs, select the** Limit Access to websites check box, and then do one of the following:
    - To limit access to sites with adult content, select the by trying to limit access to adult websites option button.
    - to allow access to specific websites only, select the by allowing access to the following websites only.

Your content filtering settings might block websites that you want to allow. You can override content filtering for specific websites by adding them to an allowed URLs list.

- 10 In the **Allow URLs** area, click **Add**.
- 11 In the **Allow URL** box, type the URL of the website to which you want to allow access.
- 12 Click **Add**.

You can also specify websites that you want to block, regardless of whether they are blocked by your content filtering settings.
- 13 In the **Deny URLs** area, click **Add**.
- 14 In the **Deny URL** box, type the URL of the website to which you want to block access.
- 15 Click **Add**.

**Tip:** You can remove a URL from the **Allow URLs** and **Deny URLs** lists by selecting the check box beside the URL, and then clicking **Delete**.

### To set time limit options for OS X devices

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **OS X**, select **Parental Controls**.

- 
- 6 Click **OK**.
  - 7 Click the **Time Limits** button at the top of the screen.
  - 8 Select the **Enforce Limits** check box.
  - 9 Do any of the following:
    - To limit computer access during the week, select the **Limit Weekday computer use to** check box, and then use the slider to select a time limit.
    - To limit computer access during the weekend, select the **Limit Weekend computer use to** check box, and then use the slider to select a time limit.
  - 10 Click **Save**.

## Configuring Restrictions for OS X Devices

You can permit and restrict system preferences on OS X devices. For example, you restrict users from accessing Bluetooth or printing and scanning. When a system preference is not enabled, it is not available to the user on the OS X device.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **OS X**, select **Restrictions**.
- 6 Click **OK**.
- 7 Ensure that the **Restrict which system preferences are enabled** check box is selected.
- 8 Do one of the following:
  - To enable all system preferences, click **Enabled All**.
  - To disable all system preferences, click **Enable None**.
  - Select or clear the check boxes beside each system preference application as needed.
- 9 Click **Save**.

---

## Configure the OS X Software Update Server

You can specify the URL of the server that Mountain Lion's Software Update client uses to obtain newer versions of Apple software.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **OS X**, select **Software Update**.
- 6 In the **Software Update** server box, type the URL of the server you are using to provide software updates to managed OS X devices.
- 7 Click **Save**.

## Setting up Android Mobile Device Configuration Profiles

### Configuring Passcode Settings for Android mobile devices

You can configure passcodes for Android devices to enforce a minimum passcode requirement. For example, you can set a minimum passcode length, and you can require users to change their passwords at an interval that you specify. All Android devices enrolled in MDM in the group will have these passcode settings applied.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Please select a profile** list, under **Android**, select **Passcode**.
- 6 Click **OK**.
- 7 From the **Minimum passcode quality** list, select one of the following options:
  - **None**
  - **Pattern, PIN, or Password**
  - **Pin or Password**
  - **Password With at Least One Letter**



- 
- **Password With at Least One Letter and One Number**
  - **Complex Password**

**Note:** The **Complex Password** option is only available for Android 3.0+ devices.

- 8 Set the options:

**Minimum passcode length** Specifies the minimum number of characters a passcode can contain.

**Passcode history** A new passcode won't be accepted if it matches a previously used passcode. You can specify how many previous passcodes are remembered and compared.

**Maximum passcode age** Requires users to change their passcode at the interval you specify. If you specify 0, users never have to change their passcode.

**Maximum Auto-Lock** If the device isn't used for the period of time you specify, it automatically locks. Entering the passcode unlocks it. If you specify 0, the device never automatically locks.

**Maximum number of failed attempts** Determines how many failed passcode attempts can be made before the device is wiped.

- 9 To require that Android 3.0+ devices have data storage encryption enabled, select the **Data storage encryption enabled** check box.

- 10 If you selected **Complex Password** in step 7, you can set the following additional options:

**Minimum number of letters** Specifies the minimum number of letters a complex password can contain.

**Minimum number of lowercase letters** Specifies the minimum number of lowercase letters a complex password can contain.

**Minimum number of uppercase letters** Specifies the minimum number of uppercase letters a complex password can contain.

**Minimum number of non-letters** Specifies the minimum number of non-letters, including numbers and symbols, a complex password can contain.

**Minimum number of numbers** Specifies the minimum number of numbers a complex password can contain.

**Minimum number of symbols** Specifies the minimum number of symbols a complex password can contain.

- 11 Click **Save**.

---

After you have saved the Android mobile device configuration policy, it is automatically deployed to the site.

## Configuring Restrictions for Android Mobile Devices

You can restrict camera use for Android 4.0+ mobile devices. You can exclude devices from the Android Restrictions policy.

### To configure Android restrictions for mobile devices

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **Android**, select **Restrictions**.
- 6 Click **Ok**.
- 7 Select the **Allow use of Camera on 4.0+ devices** check box.
- 8 Click **Save**.

After you have saved the Android restrictions configuration policy, it is automatically deployed to Android devices in the group.

## Configuring Email for Mobile Devices

### Configuring Email Policies for iOS Mobile Devices

You can set how email is configured on iOS mobile devices. You can set up two iOS email policies per group: one for EAS (Exchange Active-Sync) and one for POP3 or IMAP 4 solutions.

When you configure a new email policy or modify an existing one, notifications are sent to iOS mobile device users that already have Mobile Manager installed on their device. For iOS users, you must ask end users to edit the settings in the Self-Service URL section (About page) to include the email address and user name.

After saving the email configuration profile to the group, you must configure user settings per iOS device to complete the profile before it is sent to each device. These settings may include the email address, user name, and domain. There are two ways you can complete the email configuration profile:

- 
- Ensure that the iOS device user uses the iOS webclip to save user email settings.
  - In Service Center, navigate to the **Device Overview** page for the device. In the **Configuration Profiles** section, use the edit tool to edit the email settings. When you save the settings, the email configuration profile will be pushed to the device. The device user will then be required to specify their email password to access email.

### To configure an iOS email policy for EAS solutions

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of the group.
- 3 Click the **Policies** tab.
- 4 Under **Configuration Profiles**, click **Add**.
- 5 From the **Choose Profile Type** list, under **iOS**, select **Exchange**.
- 6 Click **Ok**.
- 7 In the **Policy Name** box, type a name for the policy.
- 8 In the **Account Description** box, type the display name of the account.
- 9 In the **Applicability** box, type the domain part of the email account. For example, “@company.com”.
- 10 In the **Exchange ActiveSync Host** box, type the Microsoft Exchange Server host name or IP address.
- 11 From the **Past Days of Mail to Sync** list, select a time frame to indicate how many days in the past to sync mail.
- 12 Set the following options:
  - Allow messages to be moved** When this option is off, users can't move messages sent or received by this account to different email account. Also prevents using another account to reply to or forward a message from this account.
  - Allow recent addresses to be synced** When this option is off, recently used addresses aren't synced with other devices using iCloud.
  - Use Only in Mail** When this option is selected, the user's email account can only be used to send messages from Mail. It cannot be selected as a sending account for messages created by other apps, such as Photos or Safari.
  - Use SSL** When this option is off, users' mobile devices do not require SSL encryption for email communications.

---

**13** Click **Save**.

After you have saved the email configuration policy, it is automatically applied to iOS devices in the group.

**To configure an iOS email policy for POP and IMAP solutions**

- 1** In Service Center, click **Configuration > Groups**.
- 2** Click the name of the group.
- 3** Click the **Policies** tab.
- 4** Under **Configuration Profiles**, click **Add**.
- 5** From the **Choose Profile Type** list, under **iOS**, select **Mail**.
- 6** Click **Ok**.
- 7** In the **Policy Name** box, type a name for the policy.
- 8** In the **Account Description** box, type the display name of the account.
- 9** In the **Applicability** box, type the domain part of the email account. For example, “@company.com”.
- 10** From the **Account Type** list, select either IMAP or POP.
- 11** If you selected IMAP in the previous step, then in the **Path Prefix** box, type the path if required.
- 12** Set the following options:

**Allow messages to be moved** When this option is off, users can't move messages sent or received by this account to different email account. Also prevents using another account to reply to or forward a message from this account.

**Allow recent addresses to be synced** When this option is off, recently used addresses aren't synced with other devices using iCloud.

**Use Only in Mail** When this option is selected, the user's email account can only be used to send messages from Mail. It cannot be selected as a sending account for messages created by other apps, such as Photos or Safari.

- 
- 13** Under the **Incoming Mail** section, in the **Mail Server** and **Port** boxes, type the IMAP or POP address and the port number used by the incoming email server.

Email Protocol	Mail Server Example	Port Example
IMAP	imap.youremailserver.com	143 or 993 (if SSL is enabled)
POP	pop.youremailserver.com	110 or 995 (if SSL is enabled)

- 14** From the **Authentication Type** list, select the authentication to use.
- Password** The network uses password authentication.
- MD5 Challenge-Response** The network uses challenge-response authentication mechanism for authentication.
- NTLM** The network uses NTLM (NT LAN Manager) security protocols.
- HTTP MD5 Digest** The network uses an application of MD5 challenge-response authentication.
- 15** If communication with the incoming email server is encrypted using SSL, select the **Use SSL** check box.
- 16** Under the **Outgoing Mail** section, in the **Mail Server** and **Port** boxes, type the IMAP or POP address and the port number used by the outgoing email server.

Email Protocol	Mail Server Example	Port Example
SMTP	smtp.youremailserver.com	587

- 17** From the **Authentication Type** list, select the authentication to use.
- Password** The network uses password authentication.
- MD5 Challenge-Response** The network uses challenge-response authentication mechanism for authentication.
- NTLM** The network uses NTLM (NT LAN Manager) security protocols.
- HTTP MD5 Digest** The network uses an application of MD5 challenge-response authentication.
- 18** If communication with the outgoing email server is encrypted using SSL, select the **Use SSL** check box.

---

**19** Click **Save**.

After you have saved the email configuration policy, it is automatically applied to iOS devices in the group.

## Configuring Email Policies for Android Mobile Devices

You can set how email is configured on Android mobile devices. For Android users, Mobile Manager presents an Account Setup Required notification icon that, when tapped, provides information about the email server name and SSL requirements. Users can then set up their corporate email account by clicking Begin Account Setup and providing the required information.

**Important:** For Android mobile device users, no automatic notification is sent when an existing email policy is modified or removed, therefore it is a good practice to notify Android users of these changes.

**Note:** Although Android devices support many different email formats, Managed Workplace Android email policies support Exchange Active-Sync only.

### To configure an Android email policy for EAS solutions

- 1** In Service Center, click **Configuration > Groups**.
- 2** Click the name of the group.
- 3** Click the **Policies** tab.
- 4** Under **Configuration Profiles**, click **Add**.
- 5** From the **Choose Profile Type** list, under **Android**, select **Exchange**.
- 6** Click **Ok**.
- 7** In the **Policy Name** box, type a name for the policy.
- 8** In the **Account Description** box, type the display name of the account.
- 9** In the **Applicability** box, type the domain part of the email account. For example, “@company.com”.
- 10** In the **Exchange ActiveSync Host** box, type the Microsoft Exchange Server host name or IP address.
- 11** If communication with the outgoing email server is encrypted using SSL, select the **Use SSL** check box.
- 12** Select the **Accept All SSL Certificates** check box to allow the device to accept all SSL certificates, which is recommended for servers which are self-signed.
- 13** Click **Save**.

---

After you have saved the email configuration policy, it is automatically applied to Android devices in the group.

## Deleting a Configuration Policy

If you no longer need a configuration policy, you can delete it. When a configuration policy is deleted, it is removed from all devices in the group to which it was applied.

- 1 In Service Center, click **Configuration > Groups**.
- 2 Click the name of a group.
- 3 Click the **Policies** tab.
- 4 Select the check box for the policy you want to delete.
- 5 Click **Delete**.
- 6 Click **OK** to confirm the deletion.

## Removing a Mobile Device from Monitoring

### Removing a Mobile Device from Monitoring in Service Center

- 1 In Service Center, click **Status > Devices**.
- 2 From the **Device Role** list, select **Mobile**.
- 3 Click the name of the mobile device.
- 4 Click **Delete Device** from the right sidebar.

For all mobile devices, the Mobile Manager agent must be uninstalled manually from the mobile device by the end user. See [Uninstalling the Mobile Manager Agent from a Mobile Device](#).

If the user launches the Mobile Manager agent manually from the iOS mobile device after the mobile device has been deleted from Service Center, they can still select the Report Status button to submit status back to Service Center. However, remote commands will not function against the device.

**Note:** For iOS mobile devices, the MDM profile and any configuration profiles are automatically uninstalled from the device if the iOS mobile device is connected to Wi-Fi.

---

## Uninstalling the Mobile Manager Agent from a Mobile Device

if the end user no longer is required to be under MDM, he or she can uninstall the Mobile Manager agent from the mobile device. In addition, note that the end user can uninstall the Mobile Manager agent at any time.

### To uninstall the Mobile Manager agent from iOS

- 1 On the device, locate the icon of the Mobile Manager app.
- 2 Tap and hold down the icon.
- 3 When it starts to jiggle, tap the X next to the icon.
- 4 When prompted, select **Delete** to remove the app.

**Note:** Manually uninstalling the Mobile Manager agent does not uninstall the MDM profile or any configuration profiles that have been pushed down to the mobile device. Service Center continues to monitor the device and remote commands (such as wipe and lock) can still be used against the device.

To remove the MDM profile for the Mobile Manager agent, navigate to Settings > General > Profiles > Remove iOS Team Provisioning Profile and tap Remove.

If the Mobile Manager agent is not uninstalled, the end user will get prompted regularly with this message: “Please launch Mobile Manager to upload status.”

### To uninstall the Mobile Manager agent from Android

- 1 On the device, go to Settings > **Location & Security**.
- 2 Locate and press **Select device administrators**.
- 3 Clear **Mobile Manager**.
- 4 When prompted, press **Deactivate** and click **OK** to confirm the deactivation.
- 5 Go to **Settings > Applications > Manage Applications** and click **Mobile Manager**.
- 6 When prompted, press **Uninstall** to remove the app and click **OK** to confirm the uninstall.



# CHAPTER 10

## MONITORING

---

*This section provides detailed information about the following topics:*

- *Monitoring in Managed Workplace*
- *Monitoring Policies*
- *Installing and Importing Monitoring Policies*
- *Using Monitoring Policies*
- *Optimizing Monitoring Policies*
- *Creating a Custom Monitoring Policy*
- *Adding Your Own Monitors*

---

## Monitoring in Managed Workplace

### About Monitoring

Managing a site includes monitoring devices, applications, security, and other tasks. Monitors watch for certain conditions at a site. When a monitored event occurs, it generates an alert and can send an email, create a trouble ticket, escalate, self-heal, or run a script.

#### What Can You Monitor?

You can monitor the conditions for a variety of devices, including servers, hard drives, applications and more.

You can set up monitors for

- collecting AMT events from Intel® vPro™ devices
- establishing device availability with ICMP ECHO requests
- determining warranty status
- evaluating the results of MBSA reports
- detecting unwanted conditions on mobile devices
- monitoring the availability and response time of network services
- capturing the status of Microsoft updates
- measuring performance counter values
- evaluating technical and fulfillment print services
- gathering System Center Essentials (SCE) alerts
- monitoring SNMP OIDs
- receiving SNMP trap messages
- receiving syslog messages
- parsing the contents of Windows events logs
- controlling the state of Windows services
- measuring bandwidth usage on network interfaces
- parsing the contents of text-based log files
- monitoring performance and availability of websites

---

## How Does Monitoring Work?

After you've set a monitor, Service Center sends the rules to Onsite Managers and Device Managers that check the thresholds that you set. If you've set up an alert, you are notified when a condition is met. Depending on the monitor, you can set a rule for running the check as well as how often it should run.

Some monitors collect information (such as performance counters, SNMP OIDs, Windows Events), some receive information (such as Syslogs, SNMP Traps) and some take actions (such as Windows Services).

## How Do You Set Up Monitoring?

To set up monitoring, you can

- optimize an existing monitoring policy for your needs
- create your own monitoring policies
- add your own monitors to monitoring policies
- apply a monitoring policy to a site or service group
- apply a monitor directly to a device

**Note:** Some monitoring types cannot be added to a monitoring policy. For example, bandwidth monitors can only be applied directly to a device.

### See Also

[Turning a Monitor in a Monitoring Policy On or Off](#)

[Creating a Custom Monitoring Policy](#)

[Adding Your Own Monitors](#)

# Monitoring Policies

## About Monitoring Policies

A monitoring policy is a collection of monitors and associated alert rules for a specific application, operating system or hardware device. Monitoring policies can be grouped into services, which are then collected into service plans applied to sites or groups for monitoring. Monitoring policies can also be applied directly to groups and devices, although this is not the best practice.

The **Monitoring Policy** page lists the modules that are currently installed in Service Center. You can choose to enable or disable monitors in the monitoring policy, and you can create automatic inclusion rules that define the criteria a

---

device must match to be monitored by the monitoring policy. Many monitoring policies have already have automatic inclusion rules pre-defined.

You can activate monitoring by doing one of the following:

- add the monitoring policy to a service, which can be included in a service plan or applied to a shared site group. This is the preferred method.
- apply the monitoring policy directly to a site group or service group.
- manually add devices to a monitoring policy.

The **Collecting** column shows how many monitors are enabled and therefore being collected.

### **Where Are the Monitoring Policies?**

Monitoring policies are located in Service Center on the **Configuration > Policies > Monitoring** page.

You can install additional monitoring policies via the Update Center, in Service Center. To access Update Center, click **Update Center > Components**, or click **Get More** on the **Configuration > Policies > Monitoring** page.

### **How Many Monitoring Policies Are There?**

Managed Workplace ships with hundreds of monitoring policies in Service Center that you can add to services and service plans to provide instant monitoring.

### **Who Creates Monitoring Policies?**

Monitoring policies are created by a team of IT professionals working with information provided by the vendors and input from the Partner community.

### **When Are Monitoring Policies Updated and Released?**

Updating, developing and releasing monitoring policies is a continuous process. To ensure that you don't have to wait for new releases of the application, monitoring policies are available in Service Center as soon as they have been through the quality certification program. By clicking **Update Center > Components**, you can view and install new monitoring policies and updates to existing monitoring policies.

---

## How Are You Notified of New Monitoring Policies?

When new and updated monitoring policies are available, a green icon appears beside **Update Center > Components** in the navigation pane to indicate that there is a new component available for upgrade.

## Installing and Importing Monitoring Policies

### Installing vs. Importing

A core set of monitoring policies are available in Service Center. There are two ways you can add more monitoring policies to Service Center:

**Installing a monitoring policy** New monitoring policies are automatically made available in Update Center. You can view a list of available monitoring policies and install the ones that you require. Installing a monitoring policy from Update Center is the fastest and easiest way to access new monitoring policies.

**Importing a monitoring policy** Monitoring policies can be exported from one instance of Service Center and imported into another.

### Installing a Monitoring Policy

Service Center includes a standard set of monitoring policies that you can access by going to **Configuration > Policies > Monitoring**. You can install a new monitoring policy by going to **Update Center** and selecting a monitoring policy from the list of new monitoring policies available for install. This list is updated periodically as new monitoring policies are released by AVG.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click **Get More**.  
**Update Center** opens, with the list filtered to display the monitoring policies available for installation.
- 3 Select the check box beside the monitoring policy you want to install.
- 4 Click **Install**.

[Updating and Installing Service Center Components](#)

---

## Importing a Monitoring Policy

In addition to installing a monitoring policy directly from Update Center, you can import a monitoring policy that you've exported from another Service Center instance.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click **More Actions** and then **Import Monitoring Policy**.
- 3 Click **Choose File** and locate the file.
- 4 Click **Open**.
- 5 Click **Import**.

## Using Monitoring Policies

### About Using Monitoring Policies

You can activate monitoring using monitoring policies in two ways:

**Add the monitoring policy to a service** Policies are added to services, which are then included in service plans. When you apply a service plan to a site or group, the automatic application rules in the included policies take effect. For more information on adding policies to services, see [Creating Services](#).

**Apply the monitoring policy to a group or device** You can also apply a monitoring policy directly to a group or device. This method of monitoring requires a manual maintenance strategy, and automatic inclusion rules do not apply. See [Applying a Monitoring Policy to a Group or Device](#).

### Creating Automatic Inclusion Rules for a Monitoring Policy

You can create automatic inclusion rules to define the criteria a device must meet to be monitored by the monitoring policy. Devices that match the inclusion rules are automatically monitored. If a device no longer meets the rule criteria, it is automatically removed from monitoring. Automatic inclusion rules only go into effect when you add the monitoring policy to a service, which is then applied to a site or group either directly or as part of a service plan. You can also associate the monitoring policy with a site or service group. For more information on creating and managing service plans, see [Creating Service Plans](#).

Rules are created by first defining AND and OR statements, then by adding rules to the statements. For example, if you are creating a rule to automatically

---

monitor all devices running on a Windows 7 operating system, in the default AND group, you would specify that the OS Name contains "Windows 7".

To create a rule that specifies that the device must either have a Windows 7 or a Windows 2008 operating system, you would change the AND group to an OR group, and then add a second rule that specifies that the OS Name contains "Windows 2008".

For more examples of automatic inclusion rules, see [Automatic Inclusion Rule Examples](#).

### Planning out automatic inclusion rules

Creating automatic inclusion rules will usually be very straightforward, but because you can put together very sophisticated rules, it's best to come up with a statement about the rule using very simple English before you get started. Here are some example rule statements:

- if the device must be a firewall, the rule statement would simply be: firewall
- if the chassis type must be a laptop, and the operating system must be Windows 7: (Chassis type is laptop) AND (OS is Windows 7)
- the network service must be HTTP or HTTPS: (HTTP) OR (HTTPS)
- the domain role must be a member workstation or a member server, and the operating system must be Windows 7 or Windows 2008: (Member Workstation or Member Server) AND (Windows 7 or Windows 2008)

### To create an automatic inclusion rule for a monitoring policy

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy to modify.
- 3 Click the **Automatic Application** tab.
- 4 Create the conditional statements. See [Creating condition statements for a monitoring policy automatic inclusion rule](#).
- 5 Create the inclusion criteria. See [Creating inclusion criteria for a monitoring policy automatic inclusion rule](#).
- 6 Preview the rule. See [Previewing an Automatic Inclusion Rule](#).

### Creating condition statements for a monitoring policy automatic inclusion rule

Set up the conditional structure of the rule by adding AND or OR statements. By default, rules include a single AND statement.

- 
- Set up the conditional statements by doing any of the following:
    - To create a single AND statement to which you can add one or multiple rules, do nothing.
    - To create a single OR statement, right-click the existing AND statement and select Modify. From the Type list, select Or.
    - To add an OR statement below the existing AND statement, select the AND statement and click Add. From the Type list, select Or.

### Creating inclusion criteria for a monitoring policy automatic inclusion rule

For each AND or OR statement, you must define at least one inclusion criteria.

- 1 Select the AND or OR statement to which you want to add inclusion criteria.
- 2 Click **Add**.
- 3 From the **Type** list, select **Rule**.
- 4 From the **Rule** list, select one of the following:

**Chassis Type** Filter devices according to chassis type, such as laptop, desktop, notebook, etc. Select either **Equals** or **Not Equal** from the **Operator** list, and select a chassis type from the **Value** list.

**Device MAC Address** Filter devices by the MAC address. Select either **Equals**, **Contains**, or **Starts With** from the **Operator** list, and type the MAC address in the **Value** box.

**Device Model** Filter devices by providing the device model. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list and type the device model name in the **Value** box.

**Device Role Category** Filters devices by device role category. As a best practice, use this rule when you will be applying service plans to shared site groups; the pre-built shared site groups in Managed Workplace are designed to be applied to the device roles defined in this rule. Select **Equals** from the **Operator** list, and then select **Network Device**, **Unknown**, **Windows Server** or **Windows Workstation**.

**Domain Role** Filter devices by the domain role. Select either **Equals** or **Not Equal** from the **Operator** list and select a domain role from the **Value** list, such as **Member Workstation** or **Primary Domain Controller**.

**Hardware Type** Filters devices according to hardware type, including desktop, laptop, mobile phone, printer, rack mount, and others. From the **Value** list, select the hardware type.



---

**Has Warranty Information** Filter devices by whether warranty information exists. Searches for devices with both custom and vendor warranties. Supported vendors include Acer, Compaq, Dell, Gateway, Hewlett-Packard, HP, IBM, Lenovo and Toshiba. Selecting this option from the **Rule** list includes all devices with warranty information.

**Installed Memory (in GB)** Filter devices by the installed memory. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in GBs.

**IP Address** Filter devices by the IP address. Select either **Equals**, **Not Equal**, **Greater Than**, **Less Than**, **Contains** or **Starts With** from the **Operator** list, then type an IP address in the **Value** box.

**Is a Printer** Filter devices to include printers. Selecting this option from the **Rule** list includes all printers.

**Is a Virtual Machine** Filter devices to include virtual machines. Selecting this option from the **Rule** list includes all virtual machines.

**Is Intel vPro Device** Filter devices by whether they are Intel vPro devices. Select **True** or **False** from the **Value** list.

**Logical Drive Size (GB)** Filter devices by the logical drive size. Select either **Greater Than** or **Less Than** from the **Operator** list, then type a number in the **Value** box, in GBs.

**Manufacturer** Filter devices by the manufacturer. Select **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type a manufacturer name in the **Value** box.

**Network Role** Filter devices by the network role, such as firewall, router, etc. Select a network role from the **Value** list.

**Network Service** Filter devices by standard network service ports, including commonly-used services such as HTTP, SMTP, and POP3. Custom ports for network services are not filtered. Select a network service from the **Value** list.

**OS Family** Filters devices by OS family, for example Android, iOS, Linux/Unix, and Windows. From the **Value** list, select an OS family.

**OS Name** Filter devices by the operating system name, for example Windows Server 2008 Standard. Select **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an operating system name in the **Value** box.

**OS SKU** Filter devices by their unique operating system SKU (Stock Keeping Unit). For example, Windows 7 has several SKUs, including Home Premium, Professional, Home Basic, and Enterprise. Select either **Equals** or **Not Equal** from the **Operator** list, then select a SKU from the **Value** list.

---

**Note:** The OS SKU rule is not applicable to Windows 2003 and XP operating systems.

**OS Version** Filter devices by the operating system version, which you can determine by executing the winver command. For example, for the Windows 7 Enterprise operating system, the OS build version is 7601. Select either **Equals**, **Not Equal**, or **Starts With** from the **Operator** list, then type an operating system version in the **Value** box.

**Responds to SNMP** Filter devices by whether they respond to Simple Network Management Protocol (SNMP) monitors. From the **Value** list, select **True** to include devices that respond to SNMP monitors, or **False** to include devices that do not respond.

**Responds to Specific OID** Filter devices to include those that respond to a specific SNMP object identifier (OID). From the **Value** list, select an OID type, such as Dell Server or HP Switch.

**Responds to SSH** Filters devices by whether they respond to Secure Shell (SSH) monitors. From the **Value** list, select **True** to include devices that respond to SSH monitors, or **False** to include devices that do not respond.

**Responds to WMI** Filters devices by whether they are WMI enabled. From the **Value** list, select **True** to include devices are WMI enabled, or **False** to include devices that are not.

**Responds to WS-MAN** Filter devices by whether WS-MAN is enabled, which is an option for WMI connectivity. Select **True** or **False** from the **Value** list.

**SNMP sysDesc** Filter devices by the SNMP system description. For example, to include Apple OS X devices, you could enter "Darwin". Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an SNMP system description in the **Value** box.

**SNMP sysObjectID** Filter devices by the SNMP system object ID. For example, Cisco ASA series devices each have unique sysObjectIDs. To include Cisco ASA 5505 devices, enter the sysObjectID for this device type (1.3.6.1.4.1.9.1.745). Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type an SNMP sysObjectID in the **Value** box.

**Software - Mac and Software - Windows** Filter devices by the Mac or Windows applications that are installed. You can filter by software name, and optionally you can also filter by the software version.

- a From the **Operator** list, select either **Exists** or **Does Not Exist**.
- b Under **Software Name**, select an operator from the **Operator** list and type the software name in the **Value** box.

- 
- c To further filter by software version, select the **Include Software Version** check box. From the **Operator** list that appears, select an operator and type a version number in the **Value** box.

**System Role** Filter devices by system role, for example File Server or Routing Service. Select a system role from the **Value** list.

**Windows Service Name** Filter devices by the Windows Service Name. To determine the Windows Service Name, view the device's Properties Page. Select either **Equals**, **Not Equal**, **Contains**, **Not Contain**, or **Starts With** from the **Operator** list, then type a Windows Service Name in the **Value** box.

- 5 Click **Add**.
- 6 Click **Save**.

## Modifying an Automatic Inclusion Rule

You can modify an automatic inclusion rule by doing any of the following:

- change an And condition to an Or condition, and vice versa
- change the rule type, rule operator, and value for inclusion

- 1 In Service Center, click **Configuration > Monitoring > Policies**.
- 2 Click the name of the monitoring policy to modify.
- 3 Click the **Automatic Application** tab.
- 4 Right-click in the row for the And statement, Or statement, or rule that you want to modify and click **Modify**.

**Note:** You must right-click an empty space in the row and not on the text itself.

- 5 Make your required changes and click **Update**.
- 6 Click **Save**.

## Deleting an Automatic Inclusion Rule

You can delete an entire automatic inclusion rule, or you can delete individual And, Or, and rule entries. For example, you can delete inclusion rules that are too restrictive or do not detect the proper devices.

Deleting an entire automatic inclusion rule requires that you first delete the rule entries, and then delete the empty And and Or statements.

**Note:** You cannot delete And or Or statements that have rules defined within.

- 
- 1 In Service Center, click **Configuration > Monitoring > Policies**.
  - 2 Click the name of the monitoring policy to modify.
  - 3 Click the **Automatic Application** tab.
  - 4 Select the row for the And statement, Or statement, or rule that you want to delete.
  - 5 Click **Delete**.

## Previewing an Automatic Inclusion Rule

After creating the automatic inclusion rules, you can preview the devices that will be monitored by the monitoring policy. You can preview devices on a site by site basis. Previewing lets you verify that the inclusion rules you created will add all the devices you want monitored by the monitoring policy.

- 1 In Service Center, click **Configuration > Monitoring > Policies**.
- 2 Click the name of the monitoring policy to which you want to preview the devices.
- 3 Click the **Automatic Application** tab.
- 4 Click **Preview**.
- 5 Select a site from the **Preview By Site** list.
- 6 When you are finished previewing, click **Close**.
- 7 If you are happy with the results, click **Save**.

## Automatic Inclusion Rule Examples

### Example 1

You want a monitoring policy to automatically monitor printers.

The rule statement would be: (is a printer).

- 1 In Service Center, click **Configuration > Monitoring > Policies**.
- 2 Click the name of the monitoring policy to modify.
- 3 Click the **Automatic Application** tab.
- 4 Right-click the AND row and select **Add** from the context menu.
- 5 From the **Rule** list, select **Is a Printer**.
- 6 Click **Add**.

---

## Example 2

You want a monitoring policy to monitor Lexmark printers.

The rule statement would be: (is a printer) AND (manufacturer is Lexmark).

- 1 In Service Center, click **Configuration > Monitoring > Policies**.
- 2 Click the name of the monitoring policy to modify.
- 3 Click the **Automatic Application** tab.
- 4 Now you will add a rule that devices must be a printer:
  - a Right-click the AND row and select **Add** from the context menu.
  - b From the **Rule** list, select **Is a Printer**.
  - c Click **Add**.
- 5 Now you will add a rule that the manufacturer must be Lexmark:
  - a Right-click the AND row and select **Add** from the context menu.
  - b From the **Rule** list, select **Manufacturer**.
  - c From the **Operator** list, select **Contains**.
  - d In the **Value** list, type **Lexmark**.
  - e Click **Add**.

## Example 3

You want a monitoring policy to monitor every printer that is manufactured by either Lexmark or Xerox.

The rule statement would be: (is a printer) AND (manufacturer is Lexmark OR manufacturer is Xerox).

- 1 In Service Center, click **Configuration > Monitoring > Policies**.
- 2 Click the name of the monitoring policy to modify.
- 3 Click the **Automatic Application** tab.
- 4 Now you will add a rule that devices must be a printer:
  - a Right-click the AND row and select **Add** from the context menu.
  - b From the **Type** list, ensure that **Rule** is selected.
  - c From the **Rule** list, select **Is a Printer**.
  - d Click **Add**.
- 5 Now you will add an OR condition:

- 
- a Right-click the AND row and select **Add** from the context menu.
    - b From the **Type** list, select **Or**.
    - c Click **Add**.
  - 6 Now you will add the Lexmark manufacturer rule:
    - a Right-click the Or row and select **Add** from the context menu.
    - b From the **Type** list, ensure that **Rule** is selected.
    - c From the **Rule** list, select **Manufacturer**.
    - d From the **Operator** list, select **Contains**.
    - e In the **Value** list, type **Lexmark**.
    - f Click **Add**.
  - 7 Now you will add the Xerox manufacturer rule:
    - a Right-click the Or row and select **Add** from the context menu.
    - b From the **Type** list, ensure that **Rule** is selected.
    - c From the **Rule** list, select **Manufacturer**.
    - d From the **Operator** list, select **Contains**.
    - e In the **Value** list, type **Lexmark**.
    - f Click **Add**.
  - 8 Click **Save**.

**Note:** When you are finished creating monitoring policy inclusion rules, you must add the monitoring policy to a service in a service plan for the rules to take effect. For more information, see [Creating Service Plans](#).

## Modifying Monitoring Policy Details

You can rename a monitoring policy to a name that makes sense in your environment. You can also modify its description.

You can assign search tags to monitoring policies to make them easier to locate when adding the monitoring policy to a service, or when applying it directly to a group. When adding a monitoring policy to a service or applying one to a group, you can narrow the list of monitoring policies to choose from by selecting one of the search tags from a drop list in the upper right corner. Any monitoring policies to which you have assigned that search tag are listed, allowing you to easily locate and add the monitoring policies you require. Note

---

that when you assign a search tag to a monitoring policy, you are selecting from a list of predefined search tags, such as “application” or “Linux”.

**Note:** Managed Workplace allows you to rename a monitoring policy with the same name as an existing monitoring policy. This is because internally Managed Workplace uses a GUID (Globally Unique Identifier). This GUID is automatically generated for each monitoring policy, is unique when created, and will not be duplicated (and it is not visible in the user interface).

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click **Modify**.
- 4 Edit the name and description, if desired.
- 5 To assign a search tag to the monitoring policy, click in the **Tags** box. A list appears with pre-populated search tags. Click the name of the tag you want to associate with the monitoring policy.
- 6 Click **Save**.

## Exporting a Monitoring Policy

You can export a monitoring policy to keep as a backup, or to import into another instance of Service Center.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Select the check box beside the name of the monitoring policy.
- 3 Click **More Actions > Export Monitoring Policy**.
- 4 Click **Save** to save the .MWPM file to your computer.

## Copying a Monitoring Policy

You can copy a monitoring policy, which is useful when you want to create a very similar monitoring policy to one that already exists, but you don't want to start from scratch.

When you copy a monitoring policy, you can choose to make it an offline version of the original monitoring policy. Offline monitoring policies are given a new Globally Unique Identifier (GUID), which is not visible in the interface and identifies the copied monitoring policy as discrete from the original. Offline monitoring policies are not upgradeable with updates from Update Center. If you do not make the copy offline, it will have the same GUID as the original and any future updates will be applied to both monitoring policies.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.

- 
- 2 Select the check box beside the name of the monitoring policy you want to copy.
  - 3 Click **Copy**.
  - 4 In the **Policy Name** box, change the name of the monitoring policy, if required. Copied monitoring policies are automatically given a (1) suffix.
  - 5 In the **Description** box, provide a description of the monitoring policies.
  - 6 To prevent future updates from being applied to the monitoring policy, select the **Offline** check box.
  - 7 Click **Create**.

## Deleting a Monitoring Policy

You can delete a monitoring policy you no longer need. Deleted monitoring policies are still available in the Update Center Components page. If the monitoring policy was one you created, it is deleted and no longer available.

If you have two monitoring policies with the same Globally Unique Identifier (GUID), for example as the result of copying a monitoring policy, and you delete one of the monitoring policies, the other monitoring policy will not be affected.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Select the check box beside the name of the monitoring policy.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

### See Also

[Deleting a Service Module](#)

## Upgrading to a New or Changed Monitoring Policy

You can update a monitoring policy by installing a newer version from Update Center.

- 1 Export the current version of the monitoring policy as a backup. See [Exporting a Monitoring Policy](#).
- 2 Delete the current version of the monitoring policy that you want to replace. See [Deleting a Monitoring Policy](#).
- 3 In Service Center, click **Update Center > Components**.
- 4 Click **Updates**.



- 
- 5 In the **Type** column, select **Monitoring Policies** from the list.
  - 6 Select the check box beside the monitoring policy you want to update.
  - 7 Click **Update**.  
**Note:** After the update has installed, the monitoring policy is updated wherever it is being used; you do not have to re-add the monitoring policy to a service plan.
  - 8 Add any monitors that you had in the previous version. See [Adding a New Monitor to a Monitoring Policy](#).

**Note:**

[Updating and Installing Service Center Components](#)

## Applying a Monitoring Policy to a Group or Device

As an alternative to creating automatic inclusion rules and adding monitoring policies to services, you can apply a monitoring policy directly to a group or device.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 From the list of monitoring policies, click the name of the monitoring policy you want to apply to a group or device.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following to apply the monitoring policy to a group or device:
  - In the **Applied Groups** area, click **Add**. Filter on the Group Type, if desired. Click the group and click **OK**.
  - In the **Applied Devices** area, click **Add**. Filter the list of devices. Select the check box beside the device and click **OK**.

## Removing a Monitoring Policy from a Group or Device

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Do one of the following:
  - To remove a monitoring policy from a group, in the **Applied Groups** area select the check box for the group and click **Remove**.
  - To remove a monitoring policy from a device, in the **Applied Devices** area select the check box for the device and click **Remove**.

---

## Excluding Devices from a Monitoring Policy

You can exclude specific devices from a monitoring policy. When you add a device to the exclusion list, it will never have this monitoring policy applied, even if the device meets the criteria outlined in the automatic application rules, and the monitoring policy is applied to the site or group to which the device belongs.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy from which you want to exclude devices.
- 3 Click the **Excluded Devices** tab.
- 4 Click **Add**.
- 5 Use the filters at the top to narrow your selection, and click **Filter**.
- 6 Select the check box beside each device you want to exclude from the policy.
- 7 Click **OK**.
- 8 Click **Save**.

## Optimizing Monitoring Policies

### Adding a New Monitor to a Monitoring Policy

You can customize a monitoring policy by adding a new monitor to it.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click the **Monitors** tab.
- 4 Click **Add Monitor**.
- 5 Select the type of monitor you want to add to the monitoring policy from the list.

**AMT Events** Use to add your own AMT Event monitors. See [Adding a Monitor for AMT \(Active Management Technology\) Events](#).

**Device Availability** Use to establish device availability with ICMP ECHO requests. See [Setting Options for Device Availability Monitors](#).

**Device Warranty** Use to add a monitor that notifies you when a warranty is about to expire. See [Adding a Monitor for Device Warranty](#).

---

**MBSA Reports** Use to evaluate the results of MBSA reports. See [Adding a Monitor for Microsoft Baseline Security Analyzer \(MBSA\) Reports](#).

**Mobile Devices** Use to monitor mobile device conditions, such as SIM card tampering. See [Adding a Monitor for Mobile Devices](#).

**Network Services** Use to monitor the availability and response times of network services. See [Adding a Monitor for Network Services](#).

**Patch Status** Use to capture the status of Microsoft updates. See [Adding a Monitor for Patch Status](#).

**Performance Counters** Use to measure performance counter values. See [Adding a Monitor for Performance Counters](#).

**Print Services** Use to monitor and alert on print service issues, such as a paper jam or when toner is low. See [Adding a Monitor for Print Services](#).

**SCE** Use to gather System Center Essentials (SCE) alerts. See [Adding a Monitor for Microsoft System Center Essentials \(SCE\)](#).

**SNMP** Use to receive SNMP messages. See [Adding a Monitor for SNMP Object Identifiers \(OIDs\)](#).

**SNMP from MIB** Use to receive SNMP messages from MIB. See [Adding a Monitor for SNMP OIDs from MIB](#).

**SNMP Traps** Use to receive SNMP trap messages. See [Adding a Monitor for SNMP Traps](#).

**Syslog Messages** Use to receive syslog messages. See [Adding a Monitor for Syslog Messages](#).

**Windows Events** Use to parse the contents of Windows events logs. See [Adding a Monitor for Windows Events](#).

**Windows Services** Use to control the state of Windows services. See [Adding a Monitor for Windows Services](#).

- 6 Click **Add Monitor**.
- 7 Type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Apply rules to the monitor. See [Setting Alert Actions](#).
- 10 Click **Save**.

## Turning a Monitor in a Monitoring Policy On or Off

You can turn a monitor on or off. If you are not interested in reporting the data the monitor collects, or it is not likely to translate into billable actions for you,

---

turning the monitor off is appropriate. This will reduce noise in Service Center and the disk footprint used by the database.

For example, the Microsoft Windows 7 monitoring policy contains monitors for a number of subsystems that may not be used by your customers, such as the handwriting recognition component. Unless you have a customer that uses tablet devices, as are often found in medical practices, you may want to simply turn off these monitors.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click the **Monitors** tab.
- 4 Select the check box for monitor that you want to enable or disable.
- 5 Click **Enable** or **Disable**.
- 6 Click **Close**.

#### **See Also**

[Deleting a Monitor from a Monitoring Policy](#)

## **Deleting a Monitor from a Monitoring Policy**

You may need to delete a monitor if you made a mistake when creating it that was not correctable.

**Note:** It may be better to turn this monitor off instead of deleting it in case you need it later. See [Turning a Monitor in a Monitoring Policy On or Off](#).

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click the **Monitors** tab.
- 4 Select the check box for monitor that you want to delete.
- 5 Click **More Actions > Delete Monitor**.

## **Setting How Often a Monitor Runs**

Monitoring policies released by AVG aim to achieve a balance between regular sampling of data and the resources required to obtain and store it. It's important that your team understand how frequent the polling interval is for important monitors, since the default values may not be appropriate in all situations.

---

For example, the Dell Servers monitoring policy gathers the operational status of hard drives every 15 minutes. If your service plan states that you react to disk faults within 10 minutes, the polling interval must be reduced to 5 minutes.

**Note:** Some monitors run automatically and cannot be d.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click the **Monitors** tab.
- 4 Click the name of the monitor.
- 5 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 6 Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, from the list select either **Daily Interval** or **Specific Interval**, and use the corresponding lists to define the monitoring.
- 7 Click **Save**.

## Overriding an Alert in a Monitoring Policy

You can override the following alert actions that are part of a monitor:

- email notifications
- escalation notifications
- trouble ticket actions

This allows you to change the behavior for alert actions in bulk.

For example, when you have integrated Service Center with a Professional Services Automation (PSA) solution such as ConnectWise or Autotask, and you want to control your workflow in the remote system, you must ensure that all alerts will create trouble tickets that are passed to the remote system. Open each monitoring policy and check all monitors with alerts, and override the Create Trouble Ticket action so one is created.

- 1 In Service Center, click **Configuration > Policies > Monitoring**
- 2 Select the check box beside the name of the monitoring policy.

- 
- 3 Click **More Actions** and then do one of the following:
    - Click **Override Send Email Alert Notifications** and follow the instructions in the dialog box.
    - Click **Override Escalation of Alert Notifications** and follow the instructions in the dialog box.
    - Click **Override Create Trouble Ticket Action** and follow the instructions in the dialog box.
  - 4 Click **OK**.

## Creating a Custom Monitoring Policy

You can create your own monitoring policies for monitoring. Although editing an existing monitoring policy is easier, creating one from scratch ensures monitors are applied the way you want.

To create your own monitoring policy, you must determine how the managed device or application exposes its status, determine appropriate alert actions and thresholds, and test the final product to ensure there are no functional issues with your configuration.

For example, you may encounter a customer who must continue to use a legacy version of an application due to business constraints. It's not likely that prioritization will occur so that AVG will design a monitoring policy for software that has been deprecated, but you must monitor the application to satisfy the service agreement with the customer. The solution is to design your own monitoring policy.

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click **New**.
- 3 In the **Policy Name** box, type a name.
- 4 Optionally, type a description for the monitoring policy.
- 5 Click **Create**.
- 6 Add a new monitor to the monitoring policy. See [Adding a New Monitor to a Monitoring Policy](#).
- 7 Add automatic inclusion rules to the monitoring policy. See [Creating Automatic Inclusion Rules for a Monitoring Policy](#).

---

## Adding Your Own Monitors

### About Adding Your Own Monitors

You may find that the monitors in a monitoring policy cover most of the monitoring needs you have. However, there may be cases where you want to apply a specific monitor to a group or device separately from a monitoring policy.

For example, the monitoring policies for SQL monitor default instances because the instance name is required to collect performance counters and monitor the Windows services. Generally default instances are used, but you have a single customer with an important database on a named instance. Creating the monitors directly on the device allow the monitoring to occur as needed, without creating a monitoring policy for use with a single device.

**Note:** Some monitor types (Bandwidth, Custom Log, and Cloud Service monitors) cannot be created within monitoring policies and cannot be applied automatically using service plans. You must discretely add these monitor types to the device or cloud service under management.

#### What You Can Do

You can add monitors to individual devices

- using the **Configuration > Monitors & Alert Rules** option
- using the **Monitors** tab on the **Alerts** page for an individual device

#### See Also

[Adding a Monitor for AMT \(Active Management Technology\) Events](#)

[Adding a Monitor for AVG AntiVirus](#)

[Adding a Monitor for Bandwidth](#)

[Adding a Monitor for Custom Log Files](#)

[Setting Options for Device Availability Monitors](#)

[Adding a Monitor for Device Warranty](#)

[Adding a Monitor for Microsoft Baseline Security Analyzer \(MBSA\) Reports](#)

[Adding a Monitor for Mobile Devices](#)

[Adding a Monitor for Network Services](#)

[Adding a Monitor for Patch Status](#)

[Adding a Monitor for Performance Counters](#)

---

[Adding a Monitor for Print Services](#)

[Adding a Monitor for Microsoft System Center Essentials \(SCE\)](#)

[Adding a Monitor for SNMP Object Identifiers \(OIDs\)](#)

[Adding a Monitor for SNMP OIDs from MIB](#)

[Adding a Monitor for SNMP Traps](#)

[Adding a Monitor for Syslog Messages](#)

[Adding a Monitor for Windows Events](#)

[Adding a Monitor for Windows Services](#)

[Adding a Monitor for Basic Websites or Cloud Services](#)

## Adding a Monitor for AMT (Active Management Technology) Events

AMT (Active Management Technology) is a feature of Intel® vPro™ processors. It provides status information from the hardware so that it can be read by Managed Workplace.

**Note:** AMT Event monitors only function correctly if the devices being monitored have successfully been detected as AMT-enabled. See [Working with Intel® vPro™ Devices](#).

### Default Monitoring Policy

A default monitoring policy for Intel® vPro™ comes with Managed Workplace. This monitoring policy creates an alert on all critical events and emails the alert to all valid recipients.

**Note:** Self-heal is not available for AMT events.

### What You Can Do

You can add the Intel® vPro™ monitoring policy to a service, and then add the service to a service plan. See [Creating Services](#). You can then monitor the information captured by the default monitoring policy for vPro™. Both non-critical and non-recoverable events may present opportunities for your sales team.

You can create your own AMT Event monitors to collect the events from all or specified sources. You use search strings and the following severity levels:

- ALL
- UNSPECIFIED
- MONITOR



- 
- INFORMATION
  - OK
  - NON\_CRITICAL
  - CRITICAL
  - NON\_RECOVERABLE

### For more information

See the vendor documentation for the computer with vPro™ to find out what events are traceable.

### To collect events from AMT sources

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **AMT Events**.
- 6 Click Add Monitor.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 Do one of the following:
  - To collect events from all AMT sources, select the **All** check box.
  - To collect events from a specified AMT source, clear the **All** check box and type a source in the **Source** box.
- 11 Select a severity level from the **Severity** list.
- 12 Type a text string to search for in the **Details Search** box.
- 13 To configure an alert, see [Setting Alert Actions](#).
- 14 Click **Save**.

## Adding a Monitor for AVG AntiVirus

There are 5 monitors associated with AVG AntiVirus in Managed Workplace:

- AVG AntiVirus - Device Needs Restart

- 
- AVG AntiVirus - Protection Disabled
  - AVG AntiVirus - Threat Detected
  - AVG AntiVirus - Virus Definition Out-Of-Date
  - AVG AntiVirus - Virus Scan Overdue

These monitors are also included in the AVG Managed Workplace Antivirus monitoring policy, which is used in conjunction with the AntiVirus policies to monitor AVG AntiVirus at your customer sites. If you choose to create your own monitoring policy for AVG AntiVirus, you must add these monitors.

For more information on setting up AVG AntiVirus monitoring, see [Setting up AVG AntiVirus Monitoring](#).

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select one of the following monitors:
  - AVG AntiVirus - Device Needs Restart
  - AVG AntiVirus - Protection Disabled
  - AVG AntiVirus - Threat Detected
  - AVG AntiVirus - Virus Definition Out-Of-Date
  - AVG AntiVirus - Virus Scan Overdue
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 To configure an alert, see [Setting Alert Actions](#).
- 10 Click **Save**.

## Adding a Monitor for Bandwidth

A bandwidth monitor measures specific usage of bandwidth of an interface through either WMI or SNMP.

You can set up alerts for throughput above or below a specified threshold, measured in absolute kbps or percentage of the total available.

**Note:** Bandwidth monitors cannot be added to monitoring policies.

---

## When To Use

Use to monitor

- the ISP firewall connection via SNMP for an end-customer site
- specific server NICs
- the interfaces on an Ethernet or VoIP switch

## Bandwidth Monitors on SNMP Interfaces

When using this feature with SNMP interfaces, this is the format used in the Identifier list:

```
ifdesc [ifidx] [ifspeed] [iftype] [ifidx]
```

- `ifdesc` is the SNMP Interface description (for example, FastEthernet0/1)
- `ifidx` is the SNMP index entry into the interface table (what Managed Workplace actually uses to find the interface)
- `ifspeed` is the SNMP interface speed (not always present)
- `iftype` is assigned by the Internet Assigned Numbers Authority (IANA)

On a switch or router, the SNMP interface description is related to the MAC address for the interface, but it is not the MAC address itself. The mapping between the two is both link layer and vendor-specific. For example, serial lines do not have a MAC address, VLANs may have an Administrator-defined MAC address mapping.

On a Cisco switch, if you take the last two hex digits of the MAC address for each of the FastEthernet ports and convert it to decimal, you will get the number shown after the slash (for example, MAC #00-02-4B-C1-23-01 = FastEthernet0/1, MAC #00-02-4B-C1-23-0A = FastEthernet0/10). The zero in “FastEthernet0” refers to the media type.

Some SNMP devices allow the Administrator to modify the interface description to use more user-friendly names. By doing this you can make selecting the right interface easier. Note that while the interface description usually maps in an obvious way to physical ports on the network element (left to right sequential numbering, for example), this mapping is also vendor- and sometimes model-specific.

Managed Workplace does not show the IP or MAC address in the list because the information is only known to Onsite Manager if it is monitoring all ports on the network element. This occurs when Onsite Manager is configured to scan all those ports and this information is displayed in the description box if it is available.

---

### To add a monitor for Bandwidth

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Bandwidth**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 In the **Interface Selection** section, select an Identifier from the list.
- 11 Optionally, in the **Speed** box, type the value.
- 12 From the **Duplex Mode** list, select either **Half Duplex** or **Full Duplex**.
- 13 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 14 Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring. Click **OK**.
- 15 To configure an alert, see [Setting Alert Actions](#).
- 16 Click **Save**.

## Adding a Monitor for Custom Log Files

A Custom Log File monitor parses text files for content that you specify, and raises an alert if the character string is found inside the file. You can specify whether the case or whole word must be found, and you can use regular expressions to add power and flexibility to the search.

**Note:** Custom Log monitors cannot be added to monitoring policies.

---

## When to Use

Custom Log File monitors are useful when you encounter applications that do not expose their status by any other means. When this occurs, typically applications continue appending to text logs to record status events for use during troubleshooting.

Additionally, custom logs present a significant opportunity for you to design your own solutions when combined with Managed Workplace's scripting. Partners without development resources available will still have technicians capable of creating batch files that pipe results to a text file.

## To add a monitor for Custom Logs

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Custom Logs**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 In the **Custom Log Monitor** section, type the full UNC path to the log file in the **File Path** box.

For example, `\\ComputerName\SharedFolder\Resource`.

**Note:** The log file must be accessible via UNC path from Onsite Manager. Network-mapped drives are user specific and are not accessible to Windows Services.

- 10 If authentication is required to access the log file, in the **Authentication** section, do the following:
  - a Type a logon name in the **User Name** box.  
The user can be a local or a Domain user (defined with Domain\User) providing the user has read access to the log file.
  - b Type the associated password in the **Password** box.
- 11 In the **Search String** box, type the search values (either as a text string or using regular expressions).
- 12 If desired, do one of the following:

- 
- To return only similarly cased entries in the log, select the **Match Case** check box.
  - To prevent finding the search string contained in another word, select the **Match Whole Word** check box.
  - To use regular expressions in the **Search String** box, select the **Use Regular Expressions** check box.

**13** To configure an alert, see [Setting Alert Actions](#).

**14** Click **Save**.

## Setting Options for Device Availability Monitors

A Device Availability monitor checks whether a device is responding to an ICMP ECHO request in less than 3000 milliseconds and lets you know whether the device is up or down.

ICMP Ping checks a remote host for availability. Devices normally respond to ping requests within milliseconds. However, on a very congested network it may take up to three seconds or longer to receive an echo packet from the remote host.

The availability of a device is always monitored.

**Note:** If you have a server that has a remote card in it (such as an iLO/DRAC) and the main IP of the server goes down, you will not receive a device down alert because the other IP address of the iLO/DRAC is still responding. iLO (Integrated Lights-Out) cards should be configured not to respond to ping in the same manner as AMT-enabled devices.

### What You Can Do

Since device availability is always monitored, you can

- set the alert notification options for a device that is down
- set how long Service Center should wait before alerting you that a device is down

**Note:** For non-critical devices or devices that report availability through another monitoring policy, ignore this monitor type.

### To set the alert notification and how long Service Center should wait before alerting that a device is down

- 1** In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2** From the **Site** list, select the site where the device is located.

- 
- 3 From the **Device** list, select the device to which you want to add a monitor.
  - 4 Click **Add Monitor**.
  - 5 From the **Choose Monitor Type** list, select **Device Availability**.
  - 6 Click **Add Monitor**.
  - 7 In the **Monitor** tab, type a title for the monitor.
  - 8 Optionally, type a description for the monitor.
  - 9 Click **Alerts**.
  - 10 Click **Add**.
  - 11 Type a title for the alert.
  - 12 Optionally, type a description for the alert.
  - 13 Click **Add Alert Rule**.
  - 14 From the **Trigger Alert When Device is Down For** list, select the length of time Service Center should wait before alerting you.
  - 15 Click **Save**.
  - 16 Do one of the following:
    - To send an email, see [Setting Alert Actions](#).
    - To create a trouble ticket, see [Setting an Alert to Create a Trouble Ticket](#).
    - To self-heal, see [Setting an Alert to Self-heal](#).
    - To run a script, see [Setting an Alert to Run a Script](#).
    - To escalate the alert, see [Escalating an Alert](#).
  - 17 Click **Save**.

### See Also

[Excluding Devices Directly](#)

## Adding a Monitor for Device Warranty

You can add a monitor that notifies you when a warranty is about to expire.

Managed Workplace collects warranty information for Windows devices for the following vendors: Acer, Compaq, Dell, Gateway, HP, IBM, Lenovo and Toshiba. However, Managed Workplace requires both the asset tag and model number to retrieve the warranty information for IBM and Lenovo.

---

Managed Workplace also now collects automated warranty information for the following printer manufacturers: Apple, Dell, Hewlett Packard and Xerox. As with all automatic warranty collection in Managed Workplace, this information is used by your sales team to identify opportunities to replace outdated hardware or offer your own branded extended warranty of service plans.

**Tip:** You can install the Warranty Expiration monitoring policy and apply it to monitored devices. Then Managed Workplace will alert and send an email when either a vendor or a custom warranty is going to expire in 60 days. If you clear the alert for vendor warranty expiration, for example, you will still be alerted about the custom warranty expiration. However, when you clear one of the Warranty Expiration alerts, it does not alert again.

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Device Warranty**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Click **Alerts**.
- 10 Click **Add Alert Configuration**.
- 11 Type a title for the alert.
- 12 Optionally, type a description for the alert.
- 13 Click **Add Alert Rule**.
- 14 From the **Trigger Type** section, do the following:
  - To create an alert that notifies you when the vendor warranty expires, select the **Vendor Warranty** check box.
  - To create an alert that notifies you when the custom warranty expires, select the **Custom Warranty** check box.
  - To create an alert when either warranty expires, select both check boxes.
- 15 In the **Alert (days)** box, type the number of days before or after the expiry that you want to be alerted.
- 16 Click **Save**.



---

**17** Do one of the following:

- To send an email, see [Setting Alert Actions](#).
- To create a trouble ticket, see [Setting an Alert to Create a Trouble Ticket](#).
- To self-heal, see [Setting an Alert to Self-heal](#).
- To run a script, see [Setting an Alert to Run a Script](#).
- To escalate the alert, see [Escalating an Alert](#).

**18** Click **Save**.

## Adding a Monitor for Microsoft Baseline Security Analyzer (MBSA) Reports

A default monitoring policy for Microsoft Baseline Security Analyzer (MBSA) comes with Managed Workplace. The default monitoring policy creates an alert for all MBSA categories for all monitors except check passed. This can result in a high number of alerts for almost all networks. This monitoring policy is included by default in the built-in service plans in Managed Workplace. For more information on the built-in service plans, see [About the Built-in Service Plans in Managed Workplace](#).

By default, Microsoft Baseline Security Analyzer (MBSA) reports are run on a weekly basis at each of your sites. The results determine whether Microsoft security best practices have been implemented on the network on a per-machine basis.

MBSA Categories:

- Windows
- SQL Server
- IIS
- Desktop Application
- Security Update

MBSA Monitors:

- Unable To Scan
- Check Failed (Critical)
- Check Failed (Not Critical)
- Best Practice

- 
- Check Not Performed
  - Additional Information
  - Not Approved

### What You Can Do

Use this monitor to receive notifications when specific issues are present on the network.

Since MBSA reports are monitored through the monitoring policy, you can

- import and apply the MBSA monitoring policy. See [Importing a Monitoring Policy](#) and [Applying a Monitoring Policy to a Group or Device](#).
- set the alert notification option for an MBSA monitor. See [Setting Alert Actions](#).
- turn a monitor in the MBSA monitoring policy off. See [Turning a Monitor in a Monitoring Policy On or Off](#).

### To add a monitor for Microsoft Baseline Security Analyzer (MBSA) Reports

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select MBSA Reports.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Click the **Alerts** tab.
- 10 Click **Add**.
- 11 Type a title for the alert.
- 12 In the **Alert Rules** area, click **Add**.
- 13 Do one of the following:
  - To monitor all MBSA categories, ensure the **All MBSA Categories** option button is selected.

- 
- To monitor for a specific MBSA category, select the **Select MBSA Category** option button and then select a category from the **MBSA Category** list.
- 14 If you chose to monitor for a specific MBSA category in the previous step, do one of the following:
    - To monitor all conditions for the selected MBSA category, ensure **All MBSA Checks from List** is selected.
    - To monitor for a specific condition, select an item from the list or Ctrl+click to select more than one item.
  - 15 Click **Save**.
  - 16 To configure an alert, see [Setting Alert Actions](#).
  - 17 Click **Save**.

## Adding a Monitor for Mobile Devices

You can set up a monitor to alert on mobile device conditions including the following

- whether the device has been jailbroken (Apple) or rooted (Android)
- if the device has been unavailable for a set period of time
- whether the SIM card has been tampered with so that you can validate the device owner

You can apply these monitors to individual devices. Or, you can create a new monitoring policy that includes these monitors and add it to a service that is included in a service plan.

**Note:** Mobile devices are scanned every four hours. You can also get the latest assets on a specific device at any time using the **Get Latest Assets** command on the **Device Overview** page.

### To apply a monitor to a mobile device

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **Mobile Device** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.

- 
- 8 Optionally, type a description for the monitor.
  - 9 Do one of the following:
    - To alert if a jailbroken mobile device is detected, select **Jailbreak Detection**.
    - To alert if a mobile device has not reported in to Service Center for a specified time period, select **Mobile Device Availability**.
    - To alert if SIM card tampering on a mobile device is detected, select **SIM Card Tampering Detection**.
    - To alert if the mobile device goes roams, select **Roaming Detection**.
  - 10 To configure an alert, see [Setting Alert Actions](#).
  - 11 Click **Save**.

### To add a mobile device monitor to a monitoring policy

- 1 Create a new monitoring policy. See [Creating a Custom Monitoring Policy](#).
- 2 Click **Configuration > Monitor & Alert Rules**.
- 3 Click **Monitoring Policy**.
- 4 From the **Monitoring Policy** list, select the monitoring policy you created in step 1.
- 5 Click **Add Monitor**.
- 6 Select **Mobile Device** from the list and click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Do one of the following:
  - To alert if a jailbroken mobile device is detected, select **Jailbreak Detection**.
  - To alert if a mobile device has not reported in to Service Center for a specified time period, select **Mobile Device Availability**.
  - To alert if SIM card tampering on a mobile device is detected, select **SIM Card Tampering Detection**.
  - To alert if the mobile device goes roams, select **Roaming Detection**.
- 10 To configure an alert, see [Setting Alert Actions](#).
- 11 Click **Save**.

---

## Adding a Monitor for Network Services

A Network Services monitor checks the availability of the TCP or UDP port for a network service. It also gathers information about the server application or hardware providing the service.

**Note:** Network services monitors are based on the IP address of a device. While you are able to configure the monitoring to occur on all addresses on a device, the addresses themselves must remain static. If a device changes IP addresses, network services monitoring stops functioning until you reapply the monitors using the current addresses.

**Caution:** Monitoring more than 100 network services at a single site may result in degraded performance of Onsite Manager. This should not be an issue for most sites; however, if more monitoring is required, a second Onsite Manager should be used.

The following are the default ports for the network services that Managed Workplace looks for:

Network Service	Default Port
FTP	21
Telnet	23
SMTP	25
DNS	53
HTTP	80
POP3	110
NNTP	119
IMAP4	143
LDAP	389
HTTPS	443

### What You Can Do

Use a network services monitor to

- track the availability of network services
- detect activity on the most common services, such as HTTP, DNS or FTP

- 
- check the availability of a port
  - determine the round-trip time of a request from the Onsite Manager server to the service
  - provide backup reporting for relevant monitoring policies (for example, monitor the SMTP service in addition to using the Microsoft Exchange 2003 monitoring policy)

### To add a monitor for Network Services

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **Network Services** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 From the **Network Services** list, select the service to monitor.
- 11 From the **IP Address** list, select the IP address on which the service will be monitored.
- 12 In the **Port** box, type the port used by the service.
- 13 From the **Timeout** box, select an appropriate time to wait for a response.  
After the timeout period elapses, the service is considered not available.
- 14 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 15 Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, select either **Daily Interval** or **Specific Interval** from the list and use the corresponding lists to define the monitoring.
- 16 To configure an alert, see [Setting Alert Actions](#).
- 17 Click **Save**.

---

## See Also

[Adding or Deleting a Custom Network Service](#)

## Adding a Monitor for Patch Status

A Patch Status monitor checks whether a patch has been applied and alerts you of its status:

- installed pending reboot
- failed
- installed
- needed
- not needed
- unknown

**Default:** When monitoring is in place, the status of all patches on all devices are monitored. This configuration is solely for what conditions cause alerts to be triggered.

**Note:** Managed Workplace integrates with Windows Server Update Services (WSUS) to provide Patch Status monitors. These monitors only function correctly if the devices being monitored have been added to a Windows Update Agent Policy and the devices are reporting into patch management successfully.

### What You Can Do

Since patch status for devices is always monitored, you can

- set the alert notification option for a specific patch status
- add a patch status monitor to a monitoring policy

For example, if you have prompt delivery of Microsoft updates specified in your SLAs, you will want to be alerted when a patch fails to install, especially on critical devices or if a server requires a reboot due to a patch.

**Note:** The device might take up to 22 hours to check into WSUS so the alert may not trigger until then.

### To add a monitor for patch status

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.

- 
- 3 From the **Device** list, select the device to which you want to add a monitor.
  - 4 Click **Add Monitor**.
  - 5 Select **Patch Status** from the list, and click **Add Monitor**.
  - 6 In the **Monitor** tab, type a title for the monitor.
  - 7 Optionally, type a description for the monitor.
  - 8 To configure an alert, see [Setting Alert Actions](#).  
For example, you can trigger an alert when any patch has a status of failed, installed, needed, not needed or unknown.
  - 9 Click **Save**.

## Adding a Monitor for Performance Counters

A Performance Counter monitor checks metrics about the health of the hardware or application.

### Notes:

- Performance Counter monitors only function correctly if the devices being monitored are displaying as WMI-enabled in Service Center.
- Performance Counter data can be monitored for devices behind a network load balancer as long as the IP address used is included in the network scan range for Onsite Manager and is not the virtual IP of the load balancer.
- You can monitor all available instances of a performance counter on a device, which is useful when monitoring logical disk drives. For example, you can configure a single performance counter monitor to examine the logical drive letters discovered on each device, instead of creating a separate performance counter monitor for each logical drive letter.

### Understanding the Relationship Between Parent and Child Monitors

There are a few considerations regarding parent and child monitors that you must keep in mind when creating a performance counter monitor:

- changing a parent's monitor or alert configuration does not change existing child monitors. It only affects new child monitors that are created after the changes are saved.
- changing a child's monitor or alert configuration does not change the parent's configurations.
- changing a child's monitor or alert configuration does not change other child monitor's configurations.



- 
- a child monitor that is deleted will be recreated the next time the scan detects it.
    - to stop the monitoring and alerting, the monitor has to be disabled.
    - to stop the monitor from being created, a regular expression needs to be used that will not detect it or disable the parent. Disabling the parent will also prevent other counters, that may be wanted, from being created.
  - deleting the parent monitor will delete all child monitors that were created by the parent, even if the child has been modified.
  - deleting the parent monitor does not delete child monitors that were created by other parent monitors.
  - disabling the parent does not disable existing child monitors.
  - disabling the child does not disable the parent or other child monitors.

### To add a monitor for a performance counter

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Performance Counters**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 Select the performance object to monitor from the **Performance Object** list.
- 11 From the **Object Instance** list, select the instance, if needed.
- 12 To monitor all performance counter instances, select the **All Available Instances** check box unless you are setting up a monitor for logical disk free space. Drive space monitors function differently and require the use of a regular expression.
  - Select the **Instance Selection by Regular Expression** check box, and then enter the following regular expression in the **Regular Expression** box: `^[C-Z] :$` . This can also be used to limit your search. For example, if a device has two hard drives, a drive C and a drive M, you

---

could exclude certain drives by entering `^[C-L] : $`, which would monitor the C drive but not the M drive.

- 13** From the **Counter** list, select the counter.  
If available, the **Counter Help** appears, which provides a description of the counter.
- 14** If you selected the **All Available Instances** check box, the **Discovery Interval** list is available. From this list, select an appropriate time to set how frequently Onsite Manager scans for new performance counters on the target device.
- 15** From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 16** Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring. Click **OK**.
- 17** To configure an alert, see [Setting Alert Actions](#).
- 18** Click **Save**.

### See Also

[Adding or Deleting Performance Counters](#)

## Adding a Monitor for Print Services

You can monitor and alert on a variety of print services, including the following scenarios:

- when the printer issues a critical or warning message
- when the printer is down
- when there is a paper jam or other custom warning
- when the printer cover is open
- when toner levels are low
- when other supplies (such as fusers and drums) are low
- when the printer has printed a specific amount of pages

---

### To add a monitor for print services

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Print Services**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 From the **Monitor Type** list, select the monitor type.
- 11 To configure an alert, see [Setting Alert Actions](#).
- 12 Click **Save**.

## Adding a Monitor for Microsoft System Center Essentials (SCE)

A Microsoft System Center Essentials (SCE) monitor integrates with monitors from Microsoft System Center Essentials (SCE). SCE provides mid-market businesses a unified IT management solution that manages tasks across virtual and physical servers, PCs, hardware, software and IT services from a single console.

### What You Can Do

You can automatically monitor for SCE alerts. SCE-related issues have their own alert category and appear on the Central Dashboard of Service Center.

Alerts are synchronized between Service Center and SCE so that if you close an SCE alert in the SCE console, the alert is automatically closed in Service Center.

**Note:** SCE monitoring is applied directly to the SCE application server, not its management clients.

### To add a monitor for Microsoft System Center Essentials (SCE)

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.

- 
- 5 From the **Choose Monitor Type** list, select **SCE**.
  - 6 Click **Add Monitor**.
  - 7 In the **Monitor** tab, type a title for the monitor.
  - 8 Optionally, type a description for the monitor.
  - 9 Ensure the **Enabled** check box is selected.
  - 10 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
  - 11 Do one of the following to set when the monitor runs:
    - To set the monitor to run all the time, do nothing.
    - To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring. Click **OK**.
  - 12 To configure an alert, see [Setting Alert Actions](#).
  - 13 Click **Save**.

## Adding a Monitor for SNMP Object Identifiers (OIDs)

A Simple Network Management Protocol (SNMP) object identifier (OID) monitor checks for a specific piece of status or identification information. SNMP OIDs are found on many devices, including routers and access servers, switches and bridges, hubs, computer hosts or printers.

There are two types of MIBs: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables.

You can create a tabular monitor for a known base OID, and Managed Workplace will automatically create monitors for all elements within that table.

### Notes:

- Onsite Manager pulls SNMP information from managed devices using a GET request, whereas SNMP traps are sent from the managed device to the Manager.
- Onsite Manager pulls a maximum 1,024 scalar monitors from each tabular monitor definition.
- If you add an SNMP monitor and set it as tabular, but the OID is scalar, nothing will be collected since there are no related OIDs.

---

**Tip:** To find out whether an OID is tabular or scalar, you can browse the MIB in Managed Workplace using the Create SNMP for MIB monitoring page. See [Adding a Monitor for SNMP OIDs from MIB](#). Or you can use a tool such as iReasoning to perform an SNMP walk on the device. See [Using iReasoning to Add SNMP OID Information to Service Center](#).

## What You Can Do

You can

- gather status information from network appliances
- monitor all operating systems (Windows, Unix/Linux, Mac OS)
- monitor environmental status, such as temperatures and fan speeds
- collect information on firmware versions and device location

## Understanding the Relationship Between Parent and Child Monitors

There are a few considerations regarding parent and child monitors that you must keep in mind when creating an SNMP OID monitor:

- changing a parent's monitor or alert configuration does not change existing child monitors. It only affects new child monitors that are created after the changes are saved.
- changing a child's monitor or alert configuration does not change the parent's configurations.
- changing a child's monitor or alert configuration does not change other child monitor's configurations.
  - to stop the monitoring and alerting, the monitor has to be disabled.
  - to stop the monitor from being created, a regular expression needs to be used that will not detect it or disable the parent. Disabling the parent will also prevent other counters, that may be wanted, from being created.
- deleting the parent monitor will delete all child monitors that were created by the parent, even if the child has been modified.
- deleting the parent monitor does not delete child monitors that were created by other parent monitors.
- disabling the parent does not disable existing child monitors.
- disabling the child does not disable the parent or other child monitors.

## To add a monitor for an SNMP OID

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.

- 
- 2 From the **Site** list, select the site where the device is located.
  - 3 From the **Device** list, select the device to which you want to add a monitor.
  - 4 Click **Add Monitor**.
  - 5 Select **SNMP** from the list and click **Add Monitor**.  
**Note:** The SNMP monitor type is only available if the device is SNMP-enabled.
  - 6 In the **Monitor** tab, type a title for the monitor.
  - 7 Optionally, type a description for the monitor.
  - 8 Ensure the **Enabled** check box is selected.
  - 9 Select the **New SNMP OID** option button.
  - 10 In the **Object Name** box, type the OID text identifier.
  - 11 In the **OID** box, type the OID numeric value.
  - 12 From the **Object Type** list, select either **Numeric**, **Text**, **Date and Time**, or **Physical Address**.
  - 13 To collect tabular OIDs, select the **Tabular** check box.
  - 14 In the **Description** box, type a description for the OID.
  - 15 If you selected the **Tabular** check box, select an appropriate time to from the **Discovery Interval** list to set how frequently tabular children scalar OIDs are captured.
  - 16 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
  - 17 Do one of the following to set when the monitor runs:
    - To set the monitor to run all the time, do nothing.
    - To change when the monitor runs, select either **Daily Interval** or **Specific Interval** from the list and use the corresponding lists to define the monitoring. Click **OK**.
  - 18 To configure an alert, see [Setting Alert Actions](#).
  - 19 Click **Save**.

### See Also

[Adding or Deleting SNMP OIDs](#)

---

## Adding a Monitor for SNMP OIDs from MIB

The monitor called Simple Network Management Protocol (SNMP) Object Identifiers (OIDs) from MIB is a selection available only when creating monitoring policies using a Management Information Base (MIB). MIB is a repository of all SNMP OIDs for a device.

### What You Can Do

You can build a monitoring policy working directly with the MIB file provided by the vendor, which ensures you are aware of all the potential data that can be collected and eliminates the possibility of entering incorrect values.

**Note:** The MIB file must be uploaded first. MIB files have a .mib file extension.

### To upload the MIB file into Service Center

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click **New**.
- 3 Provide a name and description, and click **Create**.
- 4 Click the **Monitors** tab.
- 5 Click **Add Monitor**.
- 6 Select **SNMP from MIB** from the list, and click **Add Monitor**.
- 7 Click **Upload MIBs to Library**.
- 8 Click **Choose File**, select the file and click **Open**.
- 9 Click **Upload**.

The **Results** section confirms the upload was successful, listing the number of files added.

- 10 Click **Finished**.
- 11 From the **Browse Library list**, select the MIB file that you just uploaded and click **Load MIB**.

### To add a monitor for SNMP OIDs from MIB

- 1 Follow the steps in [To upload the MIB file into Service Center](#).
- 2 In the **Loaded MIBs** pane, select the check box beside each MIB for which you want to see the OIDs.

The OIDs appear in the **MIB Browser** pane. If available, a description of the OID will appear in the **Selected Object Description** pane. If there are

---

dependencies or errors related to an MIB, the information appears in the message box below the viewer area.

- 3 In the **MIB Browser** pane, select the check box beside each OID you want to add as a monitor in the monitoring policy.
- 4 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 5 Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, select either the **Daily Interval** or **Specific Interval** from the list and use the corresponding lists to define the monitoring.
- 6 Click **Add Selected Objects**.
- 7 If required, provide the Index value for each OID and click **Save**.

The **Monitoring Policy** window opens and the selected OIDs have been added as monitors in the monitoring policy.
- 8 To configure an alert, see [Setting Alert Actions](#).
- 9 Click **Save**.

#### To delete an MIB file from Service Center

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Select the monitoring policy name where the monitor is located.
- 3 Click the **Monitors** tab.
- 4 Select **SNMP from MIB** from the list.
- 5 Click **Add Monitor**.
- 6 From the **Browse Library** list, select the MIB file that you want to delete.
- 7 Click **Delete from Library**.

#### To unload an MIB file from the library

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Select the monitoring policy name where the monitor is located.
- 3 Click the **Monitors** tab.
- 4 Select **SNMP from MIB** from the list.
- 5 Click **Add Monitor**.



- 
- 6 In the **Loaded MIBs** pane, select the check box beside each MIB for which you want to unload.
  - 7 Click **Unload Selected**.

## Adding a Monitor for SNMP Traps

An SNMP Trap monitor checks messages received (or trapped) from devices. Traps are the logical equivalent to an alert from the vendor's perspective, so they are important to consider when designing your own monitoring policies or considering how to customize your own monitors.

**Note:** Onsite Manager has to be defined as an SNMP Trap receiver on the devices being monitored.

### What You Can Do

You can

- find out when a network device detects potential intrusions
- be notified when a redundant Internet connection has been enabled

### To add a monitor for an SNMP Trap

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **SNMP Traps** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 From the **Generic Type** list, select one of the following:
  - (All)** Use to monitor all traps.
  - Cold Start** Use to monitor when the SNMP device boots.
  - Warm Start** Use to monitor when the SNMP device reboots.
  - Link Down** Use to monitor when a network interface card (NIC) fails.
  - Link Up** Use to monitor when a network interface card (NIC) reinitializes.

---

**Authentication Failure** Use to monitor when an SNMP device gets a request from an unrecognized community name.

**EGP Neighbor Loss** Use to monitor when communication with the EGP (Exterior Gateway Protocol) peer fails.

**Enterprise Specific** Use to monitor vendor-specific error conditions and error codes. In the Enterprise OID, enter the id.

- 11** To configure an alert, see [Setting Alert Actions](#).

**Note:** If you configure this alert, you can set the Variable Binding, or what data gets passed by the SNMP Trap. From the **Variable Binding** list, you can select **Any** to pass any data or you can select either **Contains** or **Does Not Contain** and type a value.

- 12** Click **Save**.

**Note:** If you selected **All** from the **Generic Type** list, a warning message may appear informing you of the possible impact on storage costs, due to the large amount of data storage required. You must click **Yes** to continue adding the SNMP Trap monitor.

## Adding a Monitor for Syslog Messages

A Syslog Messages monitor checks information in log messages across IP networks. Syslogs are sent by many operating systems and infrastructure devices, most notably Unix-based systems and security devices.

As with SNMP traps, syslog messages are the logical equivalent to an alert from the vendor's perspective and are sent from the device to Onsite Manager.

**Note:** You must understand how the device is sending the exact message you want to capture. It's a good idea to capture all syslogs for a period of time if documentation about the syslogs is not available. For more information, contact the device vendor or search their knowledgebase.

Syslog Facilities:

- All
- kernel messages
- user-level messages
- system daemons
- security/authorization messages
- messages generated internally by syslogd
- line printer subsystem

- 
- network news subsystem
  - UUCP subsystem
  - CRON facility
  - clock daemon
  - security/authorization messages
  - FTP daemon
  - NTP subsystem
  - log audit
  - log alert
  - local use 0 - local use 7

**Note:** Syslog facilities are case-sensitive, as per the original RFC based on Berkeley Style Distributions of Unix.

Syslog Severity:

- All
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

### What You Can Do

You can

- collect information about Unix systems and applications they host
- receive critical security information from firewalls

**Note:** The Syslog Messages monitors only function correctly if Onsite Manager has been defined as a Syslog Message receiver on the devices being monitored.

---

### To add a monitor for Syslog Messages

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **Syslog Messages** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 Select a Facility from the drop-down list.
- 11 Select a **Severity** from the drop-down list.
- 12 Type part of a syslog message in the **Syslog Message** box.
- 13 To configure an alert, see [Setting Alert Actions](#).
- 14 Click **Save**.

**Note:** If you selected **All** from the **Facility** or **Severity** lists, a warning message may appear informing you of the possible impact on storage costs, due to the large amount of data storage required. You must click **Yes** to continue adding the Syslog Messages monitor.

### Adding a Monitor for Windows Events

A Windows Events monitor collects events from the Windows Events Logs, which contain significant events on the computer. Typically these events are used to troubleshoot or monitor the health of the system or applications. When creating a Windows Events monitor, you can:

- choose to monitor the application, system, or security event log, or a tiered event log;
- select multiple event sources, IDs, and levels to monitor;
- for event IDs, specify a range of IDs to monitor, and specify IDs to exclude from monitoring;
- search for event details

---

## Monitoring Tiered Event Logs

You can monitor the tiered Windows Event logs available in NT 6.0 and later, by specifying the log name when creating the Windows Events monitor. When specifying a tiered event log, do not use the event log names and sources that appear on the General tab of the Windows Event Viewer, as they may not accurately reflect the true values for these boxes. It is recommended that you open the XML view of the event, and use the Channel and Provider Name specified on the Details tab. For example, for a Hyper V event log, the channel is “Microsoft-Windows-Hyper-V-Worker-Admin” and the provider name is “Microsoft-Windows-Hyper-V-Worker”.

**Note:** The ability to remotely monitor the tiered Windows Event logs in NT 6.0 and later requires that you modify the managed device firewall rules to permit Remote Event Log Management. To confirm that the remote device firewall permits remote event log management, on the managed device, navigate to Control Panel > All Control Panel Items > Windows Firewall > Allowed Programs.

## Windows Events monitors vs. Legacy Windows Events monitors

Windows Events monitors created in versions previous to Managed Workplace 2013 R1 are referred to in Service Center as Legacy Windows Events monitors. These monitors contain limited configuration capabilities compared to the Windows Events monitors introduced with Managed Workplace 2013 R1. You can continue to use these monitors in your monitoring and alerting configuration, and you can change their configuration, however they cannot be created going forward.

**Note:** Event suppressions in legacy Windows Events monitors might override events specified for monitoring in a Windows Events monitor. For example, a legacy Windows Events monitor has been configured to monitor the Application log but to suppress event ID 1309. You then create a new Windows Events monitor to collect events from the Application log, with the event source ASP.NET 2.0, and any event ID. Then, event IDs 1309 and 1310 are triggered, both collected from the Application log, with event source ASP.NET 2.0. Event ID 1309 will not be collected, due to the suppression of that event ID in the legacy monitor.

## To add a monitor for Windows Events

**Tip:** You can use the Managed Workplace Remote Tool Event Viewer to view what events are typical on a system. The Event Viewer is available by going to a device overview page and clicking **Remote Tools** from the right sidebar. See [Using Event Viewer](#).

**1** In Service Center, click **Configuration > Monitor & Alert Rules**.

- 
- 2 From the **Site** list, select the site where the device is located.
  - 3 From the **Device** list, select the device to which you want to add a monitor.
  - 4 Click **Add Monitor**.
  - 5 Select **Windows Events** from the list  
**Note:** This option will not be available if the selected device does not support WMI.
  - 6 Click **Add Monitor**.
  - 7 In the **Monitor** tab, type a title for the monitor.
  - 8 Optionally, type a description for the monitor.
  - 9 Ensure the **Enabled** check box is selected to turn monitoring on.
  - 10 Do one of the following:
    - To monitor all event levels, select the **All** option button.
    - To monitor specific event levels, select the **Specify Level** option button, and then select the check box beside each event level that you want to monitor.**Note:** Tiered logs and Critical and Verbose event levels can only be collected from devices running Windows Vista, Windows 2008, or higher, and will not be collected if the Onsite Manager operating system is pre-Windows 2008.
  - 11 Do one of the following:
    - To select one of the most common Windows event log to monitor, select it from the **Event Log** list.
    - To specify a tiered Windows event log to monitor, select (**Specify Log**) and type the full name of the log in the **Log Name** box. For example, to collect Bits-Client Operational events, type "Microsoft-Windows-Bits-Client/Operational".
  - 12 Do one of the following:
    - To collect events from all sources, select **All** from the **Event Sources** list.
    - To select a source from which to collect events, select (**Specify Source**) and type the source in the corresponding box. You can specify multiple sources by using commas to separate the sources.
  - 13 Do one of the following:
    - To collect events without filtering by event ID, leave the **Event ID** box blank.

- 
- To specify the inclusion and exclusion of event IDs, in the **Event ID** box, type single event IDs separated by commas, or specify a range (for example, 1-10). To exclude an event or range of events, prefix the event ID with a minus sign (for example, -5).

**Note:** You must define a range of event IDs before defining an exclusion from the range. For example, 1-6555, -1111.

**14** To search the details of the event, select the **Search the Event's Details** check box and type a text string to find in the **Search for** box, if required.

- Optionally, specify a search option to filter your results by selecting any of the **Match Case**, **Match whole word**, and **Use regular expression** check boxes.

**15** Click **Save**.

**Note:** If you chose to monitor all event levels or event sources, a warning message may appear informing you of the possible impact on storage costs, due to the large amount of data storage required. You must click **Yes** to continue adding the Windows Events monitor.

### To set the alert configuration for a Windows Events monitor

The alert configuration for Windows Events monitors operate independently from the monitoring rules, which means that you can configure the alert rules to trigger when an event is collected from *any* Windows Events monitor. When you select the **From any Monitor** option, which is available for alerting on event levels, sources, and IDs, an alert is triggered when any Windows Events monitor collects an event that meets the alert rules. The **From any Monitor** option is selected by default, so if you do not want to alert on event levels, sources, and IDs not defined in the monitor, you must select a different option for each.

- 1** Click the **Alerts** tab.
- 2** Click **Add Alert Configuration**.
- 3** Type a title for the alert.
- 4** Optionally, type a description for the alert.
- 5** In the **Alert Rule** area, click **Add**.

The **Windows Event Rule Filtering Configuration** area displays the monitoring configuration selections for the Windows Events monitor. You can use this as a reference when setting up your alert rule configuration.

- 6** To configure the event levels for alerting, do the following:
  - To alert on any event level from any Windows Events monitor, select **(From any Monitor)** from the list.

- 
- To alert on a specific event level, select **Equal To** from the list, and then select an event level from the corresponding list.
  - To alert when a specific event level is not matched, select **Not Equal To** from the list, and then select an event level from the corresponding list.
- 7** To configure the event source for alerting, do the following:
- If the monitoring configuration was set to “All” for event sources, then the alert is configured for all event sources, and the **Event Source** list is disabled.
  - To alert on any event source from any Windows Events monitor, select **(From any Monitor)** from the list.
  - To alert on a specific event source, select **Equal To** from the list, and then select an event source from the corresponding list.
  - To alert when a specific event source is not matched, select **Not Equal To** from the list, and then select an event source from the corresponding list.
- 8** To configure the event IDs for alerting, do the following:
- To alert on any event ID from any Windows Events monitor, select **(From any Monitor)** from the list.
  - To alert on a specific event ID, select **Equals** from the list, and then type the event ID in the corresponding box.
  - To alert when a specific event ID is not matched, select **Not Equal** from the list, and then type the event ID in the corresponding box.
- Note:** When alerting on event IDs, you can specify one event ID. You cannot specify exceptions or a range of event IDs.
- 9** To alert on event details, select the **Search the Event’s Details** check box. If the monitor was configured to search for details, the search string is provided in the **Search for** box. You can modify the search string if desired.
- Optionally, specify a search option to filter your results by selecting any of the **Match Case**, **Match whole word**, and **Use regular expression** check boxes.
- 10** To specify that a number of Windows Events that must occur within a time period for the alert to trigger, select the **Alert after number of occurrences within period** check box. Type a number in the **Number of occurrences** box, and then select a time period from the list.
- Note:** When specifying the number of occurrences, you can enter any number between 1 and 999.



- 
- 11 Click **Save**.

## To Edit a Legacy Windows Events Monitor

If you are working with a Windows Events monitor that was created pre-Managed Workplace 2013 R1, the following steps are required to edit the monitor:

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **Windows Events** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure either the **Collect Events** option button is selected to turn monitoring on.

If you want to turn monitoring off, select the **Suppress Event Collection** option button.

- 10 Do one of the following:
  - To select an existing Windows event log to monitor, select it from the **Choose Log** list.
  - To define a new Windows event log to monitor, select **(Specify Log)** and type the name of the log in the corresponding box.
- 11 Do one of the following:
  - To collect events from all sources, select **All** from the **Choose Source** list.
  - To select a source from which to collect events, select **(Specify Source)** and type the source in the corresponding box.
- 12 Do one of the following:
  - To collect events with all event IDs, select **All** from the **Choose Event ID** list.
  - To select an event ID from which to collect events, select **(Specify Event ID)** and type the event ID in the corresponding box.
- 13 Select a severity level for the event from the **Severity** list.

- 
- 14 To search the details of the event, select the **Search the Event's Details** check box and type a text string to find in the **Search for What** box, if required.
  - 15 To search the details of the event for Onsite Managers prior to Managed Workplace 2011, select the **Enable Legacy Search of Event's Details** check box and type a text string to find in the **Search for What** box, if required.
  - 16 To configure an alert, see [Setting Alert Actions](#).
  - 17 Click **Save**.

## Adding a Monitor for Windows Services

A Windows Services monitor checks that services remain running on a system in order to perform specific tasks that do not require user intervention. Most mission-critical applications on Windows servers use at least one service and many use more than one.

**Note:** Windows Services monitors only function correctly if the devices being monitored have WMI enabled in Service Center.

### What You Can Do

You can configure what happens when Managed Workplace notices that a Windows service is running or not.

### To add a monitor for Windows Services

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the device to which you want to add a monitor.
- 4 Click **Add Monitor**.
- 5 Select **Windows Services** from the list.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Ensure the **Enabled** check box is selected.
- 10 Do one of the following:
  - To select an existing Windows Service to monitor, select it from the **Display Name** list.

- 
- To define a new Windows Service to monitor, select the **Other** check box and type the name of the service in the corresponding box.
- 11 From the **Monitoring Type** list, select the type of monitoring:
    - Off - No Monitoring** Does not monitor.
    - Low - Do not restart the service but raise an alert if one is configured** Does not attempt to restart the Windows service. If an alert is configured, one will be raised.
    - Medium - Restart the service, but only raise an alert if restart fails and if an alert is configured** Attempts to restart the Windows service. If an alert is configured, one will be raised only if the restart fails.
    - High - Restart the service and raise an alert if one is configured**  
Attempts to restart the Windows service. If an alert is configured, one will be raised. Alerts will be self-healed during the next polling.
  - 12 To configure an alert, see [Setting Alert Actions](#).
  - 13 Click **Save**.

## Adding a Monitor for Basic Websites or Cloud Services

You can monitor a basic website or cloud services that include JavaScript redirection or require credentials.

- A basic website monitor includes details to monitor a simple website that does not require credentials. It is a simple HTTP request.
- A cloud service monitor includes credential information and then tests the health of the cloud service. It can handle anything a browser can handle.

Use basic website or cloud service monitors to monitor the availability and response times of

- cloud services (for example, Microsoft Office 365 or Google Docs)
- customer site intranet websites (for example, a SharePoint portal)
- external facing private websites (for example, Outlook Web Access pages)
- the primary website for the customer

You can configure alerts based on the availability or response times of websites or cloud services, as well as the actual content of the page, which allows for monitoring for error messages returned by web services. The page content may be static HTML pages or dynamic page content generated using Microsoft ASP.NET, PHP or Cold Fusion.

---

The monitoring framework for cloud services uses .cloud files, based on our core policy-based monitoring framework. These files enable the monitoring and management of cloud services that use JavaScript redirects or require session credentials.

**Notes:**

- Each site can have only one cloud service monitor.
- Onsite Manager must be able to reach the website or cloud service.
- Internet Explorer is a required component on the Onsite Manager machine for cloud services monitoring.
- Cloud service monitors cannot be added to monitoring policies.
- Sites without Onsite Manager cannot monitor cloud services. Device Managers cannot monitor cloud services.
- Alert rules for both Basic Website and Cloud Service is based on Response Time.
- The Onsite Manager executes one cloud service monitor at a time. It can take a few minutes to return the results of the monitor. If you have several cloud service monitors, they will queue and execute serially.
- The cloud service monitor does not use the proxy server configuration of the Onsite Manager but uses Internet Explorer settings instead. You must manually change the proxy settings in Internet Explorer for the Managed Workplace Service Account user profile.
- Onsite Manager monitors cloud services using the local copy of Internet Explorer. While a polling interval is underway, requests for other cloud services monitors are queued and will be completed once the active connection is released. To avoid issues with inconsistent polling intervals, stagger your cloud services monitoring whenever possible.

**Adding a Basic Website Monitor**

**To name the basic website monitor**

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 Click the **Cloud Service** icon.
- 3 From the **Site** list, select the site that contains the Onsite Manager that will be doing the monitoring.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Cloud Service**.
- 6 Click **Add Monitor**.

- 
- 7 In the **Monitor** tab, type a title for the monitor.
  - 8 Optionally, type a description for the monitor.
  - 9 From the **Cloud Service** list, select **Basic Website**.

#### To identify the website that requires monitoring

- 1 In the **Website Details** section, type the **Home Page URL** for the website.  
This does not need to match the monitored URL. For example, you could monitor a child page of the home page.
- 2 In the **URL Options** section, select either http or https from the **URL list**.  
**Note:** When monitoring a website that requires a secure connection (https), the certificate for the website must be installed on the Onsite Manager machine, which does the actual monitoring, if it was not issued by a Certificate Authority.
- 3 Type the rest of the URL including the port and virtual directory, if applicable.

#### To specify how long to wait before notification of a website performance issue

- Type an amount in seconds in the **Timeout** box.  
This is the time in seconds the monitor tries to connect to the website before reporting that it is unreachable. You can be alerted when the estimated response time is greater than the timeout value you specified.  
If you don't want to receive a lot of false alerts due to connection slowdown or other network related problems, you should set this value high enough.

#### To specify page redirects for a website monitor

- Select the **Allow Redirect** check box if the website redirects to another page.  
Page redirects are built into many websites to direct users to different parts of the website based on specific conditions defined in the website programming. Since a redirect may be intentional, you can specify whether you want the page redirect interpreted as an acceptable response or a failure. If you define it as an acceptable response, the monitor follows the redirect to the next page and tests that page. You should configure the monitor not to follow redirects unless the page you're monitoring is supposed to send a redirect command.

#### To specify login credentials behind an initial login for a website monitor

- Type any Post Data that needs to be passed to the web page.

---

When you want to monitor a website that is behind a login, you have to give the monitor the information to POST for the login credentials. Most commonly you will want to do this to ensure that everything is working for users as expected, since often the login pages are static and wholly unrelated to the web application they are securing.

For example, being able to reach the logon page for your hosted Exchange server is important, but it's much more important to be able to actually log in successfully.

For example, the code for the web form appears as follows:

```
<form id="frmPost" action="response.aspx"
method="post">
    <span class="body"><b>User First Name :</b></
span> <input id="FirstName" type="text" />
    <br />
    <span class="body"><b>User Last Name :</b></
span> <input id="LastName" type="text" />
    <br />
    <input name="btnSubmit" id="btnSubmit"
type="Submit" />
</form>
```

The following must be populated in the **Post Data** box when configuring the website monitor:

```
FirstName=Brian&LastName=Smith&btnSubmit=Submit+Query
```

**Note:** If you are not familiar with web programming, there are free applications that you can find on the Internet for revealing the POST data.

### To search for a phrase on a page to check the health of the website

You can choose certain pages within your Web application (a specific Web page that is being hit by many users, for example) and have the monitor check for a specific character string within the page to ensure the expected content is there.

For example, some web services have status pages that use the word "FAILURE" when there is a problem. You would use this word to check the health of the website.

- 1 Select the part of the page you want searched from the **Search Range** list.

**Header** Use to search only the header.

---

**Content** Use to search only the content that is not part of the header.

**Header and Content** Use to search both the header and the content.

- 2 Select either the **Contains** or **Does not Contain** option button depending on if you want the string of text to be found.
- 3 Type the string for which you want to search in the **Search String** box.
  - To make the search case-sensitive, select the **Match case** check box.
  - To prevent the search string from being found as part of another word, select the **Match whole word** check box.
  - To use regular expressions in the search, select the **Use regular expressions** check box.

**Note:** Managed Workplace reads the HTML code as written, not as rendered by a web browser. For example, the following string is on the website for AVG:

“How do I start my morning? I check Managed Workplace, see what’s going on with all my client networks”

The string to enter in the **Search String** box must be the following:

“How do I start my morning? I check Managed Workplace, see what’s going on with all my client networks”

#### To specify user agent requirements for the website monitor

- 1 From the **User Agent** list, select the web browser to which the standards should conform.
- 2 From the **User Language** list, select the language the monitor should use.

#### To specify login credentials for the website monitor

- 1 Select one of the following authentication types:

**None** Use if the page to be monitored does not require login credentials. Log in as anonymous.

**Basic** Use if the page to be monitored requires login credentials in the form of a user name and password. Before transmission, the user name is appended with a colon and concatenated with the password and is not encrypted. The resulting string is encoded with the Base64 algorithm.

**Digest** Use if the page to be monitored requires login credentials and the user identity must be secured using MD5 cryptographic hashing.

**Negotiate** Use if the page to be monitored uses Microsoft Negotiate as a security support provider (SSP).

---

**NTLM** Use if the page to be monitored uses NTLM (NT LAN Manager), which is a Microsoft authentication protocol used with the SMB protocol.

**Kerberos** Use if the page to be monitored uses Kerberos, which is a computer network authentication protocol.

- 2 If you selected an authentication type besides None, type the User Name in the box.
- 3 If you selected an authentication type besides None, type the Password in the box.
- 4 If you selected an authentication type besides None, type the account Domain, if applicable, in the **User Domain** box.

#### To specify when you want this monitor to run

- 1 From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.
- 2 Do one of the following to set when the monitor runs:
  - To set the monitor to run all the time, do nothing.
  - To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring. Click **OK**.

#### Adding a Cloud Service Monitor

- 1 In Service Center, click **Configuration > Monitor & Alert Rules**.
- 2 Click the **Cloud Service** icon.
- 3 From the **Site** list, select the site that contains the Onsite Manager that will be doing the monitoring.
- 4 Click **Add Monitor**.
- 5 From the **Choose Monitor Type** list, select **Cloud Service**.
- 6 Click **Add Monitor**.
- 7 In the **Monitor** tab, type a title for the monitor.
- 8 Optionally, type a description for the monitor.
- 9 Do one of the following:
  - From the **Cloud Service** list, select one of the cloud service options (for example, Office 365).



- 
- Click **Import Other Cloud Service**. Browse to locate the .cloud file, provide a name to use in the **Cloud Service** drop-down list and optionally provide a description. Then click **Save**.

**Note:** After you import a .cloud file, you cannot delete it from the **Cloud Service** list. You can, however, stop using it by deleting the Cloud Service monitor and using a different one.

**10** Enter the **User Name** and **Password** information.

Use a dedicated Cloud Service account for monitoring purposes only. You should use a dedicated account so that personal email or work email is not being monitored and to have better transaction times (for example, the monitor is not waiting for the page to load emails).

**11** In the **Text to Find** box type the string that should exist on the page to indicate the cloud service is running.

For reference, the URLs used by the cloud services are as follows:

- Google Docs: <https://docs.google.com>
- Office 365: <https://login.microsoftonline.com/login.srf>

Log in to the account and then locate a string to use. Recommended defaults for each cloud service are as follows:

- For Google Docs, type the following: My Collections
- For Office 365, type the following: My Profile

**Note:** The search parameter is not case-sensitive.

The text you choose may be affected by custom settings of the cloud service user account. For example, the account may be set to default to a different page on login. If in doubt, log into the cloud service user account manually to determine an appropriate search string.

**12** Click **Test Cloud Service** to ensure what you entered works.

**13** From the **Polling Interval** list, select an appropriate time to set how frequently the data is captured.

**14** Do one of the following to set when the monitor runs:

- To set the monitor to run all the time, do nothing.
- To change when the monitor runs, click **Run Always** to open the **Select Interval** dialog box and select either the **Daily Interval** or **Specific Interval** option button and use the corresponding lists to define the monitoring. Click **OK**.

---

## Using iReasoning to Add SNMP OID Information to Service Center

When you want to review what SNMP information a product exposes, whether to add to a predefined monitoring policy or build your own, you will need to perform an SNMP walk on the device. This is a process of querying the device with a GETNEXT statement to poll the entire hierarchy available, which is useful when you do not have access to the Management Information Base (MIB) file from the device vendor.

Freeware, such as [iReasoning's MIB Browser application](#), can be used to perform an SNMP walk.

### To perform an SNMP walk using iReasoning's MIB Browser application

- 1 Launch iReasoning's MIB Browser software.
- 2 From the **Tools** menu, select **Options**.
- 3 Click the **Default Values** tab and enter the **Agent Read Community**.  
This is the same as the Community String used by Onsite Managers, `public`, which is usually set by default and Agent SNMP Version. (Managed Workplace supports version 1 and 2.)
- 4 Click **OK**.
- 5 Enter the IP for the device to which you want to connect in the **Address** box.
- 6 From the **OID** list, select `.1.3.`
- 7 From the **Operations** menu, select **Walk**.
- 8 Click **Go**.

Once the operation completes, you will see the entire MIB.

- 9 Click the **Name/OID**.

Reviewing the name and value often provides information as to what the purpose of the OID is. This will show the OID at the top in the **OID** box.

For example, the default Lexmark Printer monitoring policy does not collect the device-reported system uptime. If you want to collect this value, you can locate the OID and follow the process listed below to make this OID available in Service Center.

### To make the OID globally available in Service Center

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.

- 
- 3 Under the **SNMP OIDs** section, click **Add**.
  - 4 Enter the Name from the iReasoning MIB Browser as the Object Name and enter the OID.

Once this has been added, the OID will be globally available as a monitor to be used in a monitoring policy or device level monitor.

## System Log Viewer

### Viewing System Log Information

You can use the System Log Viewer window to see a list of all system logs that have been generated by Managed Workplace.

**Note:** If you have permission to see the System Log Viewer, you are seeing an Administrator view of it, which means you can see all errors for all devices and sites, even if you don't have permission to see those devices and sites.

#### To view system log information

- 1 In Service Center, click **Configuration > System Log Viewer**.
- 2 Select the desired filters.
- 3 Click **Filter**.

#### To reset the filters for system log information

- Click **Reset Filters**.

#### To view details about a system log item

- 1 Click the system log item.  
While viewing the system log message details, you can click **Up** or **Down** to scroll through the other system logs to view their message details.
- 2 Click **Close** to close the system log message.



# CHAPTER 11

## ALERTING

---

*This section provides detailed information about the following topics:*

- *Alerting*
  - *Setting Alert Actions*
  - *Clearing Alerts*
  - *Creating Alert Categories*
  - *Scheduling When Alerts are Delivered*
  - *Best Practices for Alerting*
-

---

# Alerting

## About Alerting

An alert is an indication that a monitor meets a pre-defined condition. The Central Dashboard shows the number of active alerts.

For information about the Alerts Viewer, see [Alerts Viewer](#).

For information about the Alerts page, see [Alerts](#).

You can also view and clear alerts on a mobile device using the Mobile Service Manager. See [Working with Mobile Service Manager](#).

### What You Can Do

You can customize what actions you want to take place and how you want to be notified if a condition is met for a monitor.

Possible alert notifications and actions include the following:

- email a technician or manager
- run a script
- self-heal
- create a Trouble Ticket
- escalate the alert after a certain elapsed time to an email

### Example

You can alert on low disk space for a machine in two ways: using a monitoring policy or applying a monitor and alert configuration to a device.

By default, if the Microsoft Windows 7 monitoring policy is applied to a device that uses Microsoft Windows 7, the LogicalDisk % Free Space Alert is automatically enabled and checked every 30 minutes.

To apply this monitor and alert configuration to a device, you would create a Performance Counter monitor and

- select LogicalDisk as the Performance Counter
- select the drive you want to monitor
- set the % Free Space counter
- set the threshold information If this alert condition is met
- send an email to the technician

---

## Setting Alert Actions

### Locating Monitors

To be able to set alert actions, you must first locate the monitor.

#### To locate a monitor in a monitoring policy so that you can customize what alert actions to take

- 1 In Service Center, click **Configuration > Policies > Monitoring**.
- 2 Click the name of the monitoring policy.
- 3 Click the **Monitors** tab.
- 4 Click the name of the monitor that you want to edit.
- 5 Click the **Alerts** tab.

#### To locate a device-level monitor so that you can customize what alert actions to take

Use the **Monitor & Alert Rules** option on the left sidebar:

- 1 In Service Center, click **Configuration > Monitors & Alert Rules**.
- 2 From the **Site** list, select the site where the device is located.
- 3 From the **Device** list, select the name of the device that contains the monitor you want to edit.
- 4 Locate the monitor in the folders.
- 5 Click the name of the monitor that you want to edit.
- 6 Click the **Alerts** tab.

Use the **Alerts** option on the right sidebar:

- 1 In Service Center, click **Status > Devices**.
- 2 Click the name of the device that contains the monitor you want to edit.
- 3 Click **Monitors** on the right sidebar.
- 4 Click the name of the monitor that you want to edit.
- 5 Click the **Alerts** tab.

#### See Also

[About Adding Your Own Monitors](#)

---

## Setting an Alert to Send an Email

You can set an alert to email you when a condition is met.

The alert email sent to users includes information such as:

- alert type.
- severity of the alert.
- details of the alert.
- ticket details, if configured.
- remedial steps, if configured.
- links to knowledge base articles with more information, if configured.

In most cases, the alert email also includes buttons that initiate suggested actions to correct the problem.

**Note:** Users set to receive emails must have the receive alert notifications permission in an assigned role. See [Setting the Objects a User Account Can Access](#) and [Setting User Account Options](#).

For example, you may want to be notified when there is a password issue, such as an Account Locked Due To Bad Passwords.

1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).

2 Click the **Alerts** tab.

3 Click the name of the alert.

4 Click the **Send Email** check box.

5 Select one of the following:

**All users** Use to send an email to all users whose role is to receive alert notifications.

By default, Administrators and Technicians receive alert notifications by email.

**Specify email addresses** Use to specify certain recipients who should be notified. In the From box, type the email address from where the alert is emailed.

6 In the **Alert Emailed From** area, type the name of the email address that will appear in the **From** box. By default, this email address is alert@yourservicecenter1.com.

7 Click **Save**.



---

## Adding Remediation Information to an Alert Email

When you set up an alert email, you can add suggested steps for the technician to follow to resolve the issue. You can also add a link to a knowledge base or website with more information.

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 In the **Remediation Steps** box, type the steps to take to resolve the issue.
- 5 In the **Knowledgebase URL** box, type a URL.
- 6 Click **Save**.

## Setting Alert Severity

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 In the **Severity** list, select a severity.
- 5 Click **Save**.

## Setting an Alert to Create a Trouble Ticket

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Click the **Create Trouble Ticket** check box.
- 5 Click **Save**.

## Setting an Alert to Self-heal

You can automatically remove alerts from the Central Dashboard if the condition triggering the alert no longer exists.

---

**Note:** Self-heal is not available for all monitor types. Some monitors scan for single events (such as AMT Events, MBSA Reports, SNMP Traps, Syslog Messages and Windows Events). These cannot self-heal.

#### To set an alert to self-heal

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Select the **Self-Heal** check box.
- 5 Click **Save**.

#### To set an alert to self-heal and clear any trouble tickets created as part of this alert configuration

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Select the **Create Trouble Ticket** check box.
- 5 Select the **Self-Heal** check box.
- 6 In the **Self-Healing Configuration** window, select the **Clear Trouble Ticket** check box.

**Note:** This check box is only available if the **Create Trouble Ticket** check box was selected on the **Alert Configuration** dialog box.

- 7 Click **Save**.

#### To set an alert to self-heal and notify recipients when the alert self-heals

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Select the **Self-Heal** check box.
- 5 In the **Self-Healing Configuration** window, select the **Enable Self-heal Notification** check box.

- 
- 6 From the **Notify if alert is cleared within** list, do one of the following:
    - Select how long to wait before notifying recipients.
    - Select **any time** if you want to be notified whenever an alert self-heals.
  - 7 Click **Save**.

**Best Practice:** Self-healed alerts will still be recorded as part of a device's alert history and in reports. If you have devices where CPU or memory alerts occur frequently, but are self-healed, this still presents an upgrade opportunity you can offer your client.

## Setting an Alert to Run a Script

Use the Run Script alert action to automate reactions to alerts. You define whether the script is run on the device that triggered the alert or on Onsite Manager, if one exists.

For example, you could use the **Run on Device** option and start a defragmentation job when a drive is discovered to be more than 20% fragmented.

For example, you could use the **Run on Onsite Manager** option and issue a Wake-On-LAN command for a device that has triggered a Device Down alert.

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Select the **Run Script** check box.
- 5 Optionally, from the **Script Category** list, select a category or type a category.

The category you select filters the **Script** list. As you type, Managed Workplace performs a search.
- 6 From the **Script** list, select a script or type the name of the script that you want to run in response to the alert.

As you type, Managed Workplace performs a search.
- 7 If the script requires parameters, fill these out as necessary.
- 8 Do one of the following:
  - Run on Device** Runs the script on the device that generated the alert.

---

**Run on Onsite Manager** Runs the script on Onsite Manager. When this option is selected for a Device-Manager only site, the script runs on the device.

- 9 Click **Save**.

## Escalating an Alert

You can escalate an alert. This means that if an alert has not been cleared or self-healed in a set amount of time, you can send an email to bring it to the attention of another user. Typically this is used so that unresolved high-priority alerts are viewed by a second-level technician or the business owner.

- 1 Locate the name of the monitor you want to configure. See [Locating Monitors](#).
- 2 Click the **Alerts** tab.
- 3 Click the name of the alert.
- 4 Select the **Escalate Alert** check box.
- 5 Select a time after which the alert escalation will take effect.
- 6 Do one or both of the following:
  - To set a time for the alert to be escalated, type numbers in the **Hours** and **Minutes** boxes.
  - To send an email, select the **Send Email** check box. See [Setting an Alert to Send an Email](#)
- 7 Click **Save**.

## Suppressing Alerts

You can suppress unwanted alerts to better allow you to focus on the alerts that are relevant or require action. When an alert is suppressed, it is hidden from view in all screens that display active alerts, including the **Central Dashboard** and the **Alerts** page. Suppressing alerts allows you to purge unwanted alerts while maintaining your existing alerting strategy. For example, if a device has consistently low memory, and this is not a concern, you can suppress memory alerts for this device without disrupting your existing monitoring and alerting configurations.

When you suppress an alert, you can either suppress it indefinitely, or you can set an end date for the suppression. You can view a list of suppressed alerts and reactivate them whenever necessary. Reactivating an alert removes it

---

from the list of suppressed alerts and will cause an alert to trigger again if the condition is still present.

You can suppress alerts from the **Alerts** page in Service Center, and directly from an alert email.

## Suppressing an Alert

- 1 In Service Center, click **Status > Alerts**.
- 2 Select the check box beside any alert you want to suppress.
- 3 Click **Suppress**.
- 4 Do one of the following:
  - To suppress the alert indefinitely, select the **Forever** option button.
  - To suppress the alert until a specified date, select the **Suppress Until** option button, and then click the calendar icon and select a date or type a date.
- 5 Click **OK**.

## Suppressing an Alert from an Alert Email

- In the alert email, click the **Suppress Alert Forever** link.  
The alert is suppressed indefinitely. You can still view and reactivate the alert from Service Center if required.

## Viewing Suppressed Alerts

- 1 In Service Center, click **Status > Alerts**.
- 2 Click the **Advanced Filtering** icon.
- 3 From the **Status** list, select **Suppressed**.
- 4 Click **Filter**.

## Reactivating a Suppressed Alert

- 1 In Service Center, click **Status > Alerts**.
- 2 Click the **Advanced Filtering** icon.
- 3 From the **Status** list, select **Suppressed**.
- 4 Click **Filter**.

- 
- 5 Select the check box beside any suppressed alert you want to reactivate.
  - 6 Click **Reactivate**.

## Clearing Alerts

- 1 In Service Center, click **Status > Alerts**.
- 2 Do one of the following:
  - To clear one or more selected alerts, select the check box beside any alert you want to clear and then click **Clear**. Enter an alert resolution note, if desired, and click **OK**.
  - To clear all alerts, click **Clear All**. Enter an alert resolution note, if desired, and click **OK**.

**Best Practice:** If you find yourself clearing alerts without actually doing anything to resolve the condition, then you should discuss with your team whether you should continue to receive the alert.

## Viewing Cleared Alerts for a Device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Do one of the following:
  - Click **Device Alerts** on the right sidebar.
  - Click the number under **Active Alerts**.
- 4 Click **Cleared**.

## Creating Alert Categories

### About Alert Categories

When you first install Service Center, there are no predefined alert categories. However, if you import the predefined Managed Workplace monitoring policies, any alert categories that are used in the monitoring policies are added to Service Center.

When you create a new monitor and alert rule, by default the alert is uncategorized. It's a good idea when you create a new monitor and alert rule

---

to add an alert category. Alerts and some reports are created by alert categories, so organizing them strategically yields many benefits.

As you become more familiar with Managed Workplace and begin to tailor it to monitor specific environments, you may want to create new alert categories.

On the **Alert Categories** page, a category folder is the top-level identifier of an alert category. You can expand a folder by clicking the triangle beside the folder name.

**Best Practice:** When you create a new alert category, create it under a category folder that has similar alerts. You can create new category folders as required.

### See Also

[Creating an Alert Category](#)

[Editing an Alert Category](#)

[Renaming an Alert Category](#)

[Adding an Alert to an Alert Category](#)

[Filtering Alerts by Alert Category](#)

[Deleting an Alert Category](#)

## Creating an Alert Category

### Best Practices

- Because there are no monitoring policies for cloud service monitors, no default alert categories are created. You may want to create a category for cloud service monitors if you will use them. Otherwise, alerts generated by websites and cloud services will go to the uncategorized column on the Central Dashboard by default.
- For example, you may want to create an alert category under Device Availability to filter on how long a device is down: 5 minutes, 15 minutes or 60 minutes.

**1** In Service Center, click **Configuration > Alert Categories**.

**2** Click **Add**.

**3** Do one of the following:

- To add a category under an existing category, select an existing **Category Folder** from the list.

For example, select Device Availability from the list.

- 
- To add a new category, select the **Other** check box and type a name for the new folder in the box that displays.
- 4 In the **Category** box, type a name for the new alert category.  
For example, type Device Down 5 Minutes as the category.
  - 5 Click **Save**.

**Note:** You must set up alerts to use this new category. See [Categorizing an Alert](#).

## Editing an Alert Category

- 1 In Service Center, click **Configuration > Alert Categories**.
- 2 Open the folders by clicking the chevron (>) and locate the name of the category you want to edit.
- 3 Click the name of the category you want to edit.
- 4 Make any required changes.
- 5 Click **Save**.

## Renaming an Alert Category

- 1 In Service Center, click **Configuration > Alert Categories**.
- 2 Open the folders by clicking the chevron (>) and locate the name of the category you want to rename.
- 3 Click the name of the category you want to rename.
- 4 Type a new name in the **Category** box.
- 5 Click **Save**.  
Managed Workplace creates a new alert category.
- 6 Locate the name of the original category and click the **Delete** icon.



Delete icon

## Categorizing an Alert

- 1 In Service Center, click **Configuration > Monitors & Alert Rules**.
- 2 Locate the name of the monitor that contains the alert you want to configure.



- 
- 3 Click the **Alerts** tab.
  - 4 Click the name of the alert configuration.
  - 5 In the **Alert Categories, Actions, and Notifications** area, click **Categorize Alert**.
  - 6 Select the name of the alert category on the left and click the right-pointing arrow to add it to the right box.
  - 7 Click **OK**.

## Filtering Alerts by Alert Category

- 1 In Service Center, click **Dashboards**.
- 2 Click the Central Dashboard icon if it is not displayed by default.
- 3 Click the red alert number under the alert category.
- 4 Click the **Advanced Filtering** icon.
- 5 Filter the list of alerts using the **Category** list.
- 6 Click **Filter**.

## Deleting an Alert Category

You can delete alert categories as required. When you delete an alert category, any existing alert rules that are associated with the alert category will have the category removed. However, monitoring and alerting will still take place, but the alerts will appear in the **Uncategorized** column on the **Central Dashboard**.

**Note:** The top-level alert category folder will automatically be deleted when you delete the last category in the folder.

- 1 In Service Center, click **Configuration > Alert Categories**.
- 2 Open the folders by clicking the chevron (>) and locate the name of the category you want to delete.
- 3 Click the **Delete** icon for the category you want to delete.



- 4 Click **OK**.

---

## Scheduling When Alerts are Delivered

### About Alerts

**Note:** Alert schedules are being replaced by maintenance schedules. See [Creating a Maintenance Schedule](#).

An alert schedule determines when alerts should be delivered and when they should be ignored, and whether notifications or trouble tickets should be ignored.

#### Notes:

- Alerts automatically adjust to Daylight Saving Time.
- If a user has permission to see the site, he or she automatically has access to alerts for the associated site.
- If a user is not an administrator, he or she must be given explicit access to a service group to have access to the alert schedule for the group since service groups can span sites.

#### When to Use an Alert Schedule

Use an alert schedule to

- turn alerting off entirely
- disable alert notification by email
- disable trouble ticket creation

#### What You Can Do

You can set up an alert schedule or set behavior for specific daily intervals.

#### Priorities

When conflicting alert schedules apply to both a device and a site, the alert schedule applied to a device is used. In all other cases and combinations, the least restrictive alert applies.

#### Examples

You may only want to receive alerts for a specific Service Level Agreement (SLA) during regular business hours of 8:00 a.m. to 4:00 p.m. Or you may not want to receive any alerts on a statutory holiday.

---

## Creating an Alert Schedule

**Note:** Alert schedules are being replaced by maintenance schedules. See [Creating a Maintenance Schedule](#).

Use the Time Intervals to set ranges of time. The first range starts at 0:00 a.m. and goes to the specified time (in this case, 6:00 a.m.). The next range starts at the specified time (in this case, 6:00 a.m.) and goes until the next time you specify (12:00 p.m.), and so on.

- 1 In Service Center, click **Configuration > Alert Schedules**.
- 2 Click **Add**.
- 3 Ensure that the **Enable Alert Schedule** check box is selected to activate the new alert schedule.
- 4 From the **Options** list, select the option that corresponds with the subject of the alert (Device, Service Group, Site Group, Alert Category, or Site).
- 5 Specify the Device, Service Group, Site Group, Alert Category, or Site to which you want to apply the alert by selecting it from the corresponding list.
- 6 Select either the **Always** or **Specific Interval** option button.
  - If you select the **Always** option button, the schedule will always be active.
  - If you select the **Specific Interval** option button and then select a time frame using the **From** and **To** lists, the schedule will be active during the specified time period.
- 7 Select the check boxes that correspond with the days of the week you want the schedule to be active.
- 8 Use the **Time Intervals** columns to further define when you want the schedule to be active, and the actions you want to happen in each time frame.

For example, to turn off email alerts for a time interval, clear the **E/P** check boxes.

For example, to turn off the creation of trouble tickets for a time interval, clear the **TT** check boxes.
- 9 Click **Save**.

## Disabling and Enabling an Alert Schedule

**Note:** Alert schedules are being replaced by maintenance schedules. See [Creating a Maintenance Schedule](#).

---

### To disable an alert

- 1 In Service Center, click **Configuration > Alert Schedules**.
- 2 Click **Disable** beside the alert schedule you want to disable.

### To enable an alert

- 1 In Service Center, click **Configuration > Alert Schedules**.
- 2 Click **Enable** beside the alert schedule that is disabled.

### See Also

[Deleting an Alert Schedule](#)

## Deleting an Alert Schedule

- 1 In Service Center, click **Configuration > Alert Schedules**.
- 2 Click **Delete** beside the alert schedule you want to delete.

### See Also

[Disabling and Enabling an Alert Schedule](#)

## Best Practices for Alerting

### Analyze Alerts

You can review the default alerting behaviors from monitoring policies and determine if those actions are in line with your SLAs and business needs. Choosing whether to monitor an item can be vastly different than monitoring that item and taking action based on a circumstance of that monitor.

Alerts that are self-healed delete themselves so you never waste time investigating them. This reduces alert noise. Enabling the self-heal functionality of an alert sets the software to automatically delete an alert that has been created if it is noted that the condition is no longer present. This behavior can also be configured to send out a notification that the alert has been self-healed.

To configure the alert, you need to use the same process as with optimizing monitoring policies. For each failure point or negative condition you identify, ensure that the alert meets one of these criteria:

- It is covered in the current Service Level Agreement (SLA) and is therefore already paid.
- It is an actionable item outside the current SLA and subject to billing.

- 
- It is not currently billable but feeds into project work recommendations.

You can also control your alerting as another means of establishing tiers of service. This is done by configuring well-planned alert schedules.

**For more information**

[Setting an Alert to Send an Email](#)

[Setting an Alert to Create a Trouble Ticket](#)

[Setting an Alert to Self-heal](#)

[Setting an Alert to Run a Script](#)

[Escalating an Alert](#)

[Escalating an Alert](#)

## Analyze Results

Review the monitoring in place using the **Site Configuration Summary** report included with Managed Workplace. This report provides a snapshot of the current monitoring configurations, including

- monitoring policies applied to service and site groups
- monitoring policies applied to devices

Use this report to help you evaluate your current monitoring configuration and to check whether there are any unmanaged devices. Also, it will ensure that monitoring is not replicated when you upgrade to a new monitoring policy.

You should also be running the **New Device Discovery** report on a daily or weekly basis to ensure that you have the most complete monitoring coverage possible.

You can also get a quick look at what's not under management using the device search option to show devices not in groups.

**For more information**

[Reporting](#)

[Searching for a Device](#)

---

## Alert on Success

Typically, you will use alerting to be notified when things go wrong or fail in a client's environment. You can also use alerting to be notified on success conditions.

For example, if your client has an especially critical system (such as their accounting or Exchange servers), monitoring both successful and critical activity can give you a thorough view of that system. This ensures that you will be notified as soon as things go wrong even when critical failure alerts fail to get through to you.

In any alerting system whenever more than one thing goes wrong, there is always the possibility that something else may impede the alert notification. These other impediments might be related to

- the original failure itself (for example, a power failure affecting all systems being monitored)
- the presence of another issue in the environment (for example, network congestion, firewall failure, and so on)
- a coincidental problem affecting Onsite Manager's ability to relay the notification (for example, when two different problems impact the critical system as well as Onsite Manager)

Depending on your relationship with your client, you may need to provide proof of the work you are doing on their behalf. Success alerts can be used to show that you have successfully completed your commitment to do work (such as successful backups or patches), and you can use the alert reporting in Managed Workplace to document these successes.

You can create an alert category that contains success alerts. After setting up the alert configurations, you can build a report that shows this alert category for a site. When you run the report for a site, it will list all the success alerts that you have received during the specified reporting period.

### For more information

[Creating Alert Categories](#)

[Reporting](#)

# CHAPTER 12

## AUTOMATING TASKS

---

*This section provides detailed information about the following topics:*

- *About Automation in Managed Workplace*
  - *Scripts, Automation Packages, and Tasks*
  - *Creating Automation Packages*
  - *Preparing Scripts and Packages for Use in a Policy or Task*
  - *Creating Automation Policies*
  - *Adding, Importing, and Exporting Scripts and Packages*
  - *Managing Scripts, Automation Packages, and Quick Tasks*
  - *Scheduling Tasks*
  - *Working with Tasks*
-

---

## About Automation in Managed Workplace

### About Automating Tasks

Managed Workplace includes a library of scripts and automation packages that you can use to automate remediation and regular maintenance on devices across sites and service groups. A script executes a single action, and a package is a bundle of scripts that are set up to execute a sequence of actions.

You can create *automation policies*, which is a script or package with additional settings including:

- schedule settings that determine whether the automation policy follows the default execution schedule, which is used by automation, patch, and AV policies to run maintenance tasks without disrupting the customer's business. You can also overrule the execution schedule by defining a custom schedule, for running the task. For more information on execution schedules, see [Setting Up Execution Schedules](#).
- automatic application rules that determine the criteria a device must meet in order for the task to run on the device.
- manual application and excluded devices, which allows you to select which devices must or must not have this task run.

For more information on automation policies, see [Creating Automation Policies](#).

You can also schedule a task directly in the **Calendar (Automation > Calendar)**, while Onsite Manager or Device Manager executes the instructions.

**Note:** Scheduled tasks function very similarly to tasks created using an automation policy, however scheduled tasks are applied directly to devices or groups that you select, and cannot be added to services for use in a service plan.

You can create a quick task, which is a task in which you pre-fill some or all of the script parameters, so that when you run the task you do not have to fill everything in. For more information on quick tasks, see [Adding a Quick Task](#).

Regardless of how you schedule a task, you can:

- run scripts on Windows, Mac OS, and Unix/Linux devices;
- use any of the scripts available in the script Library, and use Update Center to get more scripts as they become available and to update existing scripts;
- run your own scripts;



- 
- bundle scripts together to create a package, using rules and logic to determine the script sequence and dependencies between scripts;
  - run a task immediately, schedule a task to run once, or create a recurring schedule for the task;
  - view scheduled tasks using a daily, weekly, or monthly calendar view, or an agenda view;
  - use the calendar to keep track of task progress and results, and rerun failed tasks;
  - designate a script or package as a favorite, for ease of use.

## About the Automation Dashboards

There are three dashboards for automation:

- The **Calendar** window displays all the tasks that have been scheduled, and displays all previously-run tasks.
- The **Favorites** window displays all quick tasks, scripts, and packages that you have designated as a favorite.
- The **Library** window displays all the scripts, packages and quick tasks that are available to use in Managed Workplace.

## Automation Requirements

In order for Onsite Manager to execute the automated task on remote Windows devices, the following prerequisites must be met in the target device:

- If you are using PowerShell scripts, some scripts will require that PowerShell 2.0 or 3.0 is enabled.
- The Workstation Windows Service is running.
- The Server service is running.
- The Remote Admin share (ADMIN\$) is available.
- The Windows Network is running and Printer and File Sharing are activated.
- Ports 135 and 445 must be open. By default most firewalls will block any incoming traffic to these ports.
- There is enough disk space to copy the script.
- The device is WMI-enabled.

---

In order for Onsite Manager to execute automated tasks on remote Mac and Unix/Linux devices, the following prerequisites must be met in the target device:

- Port 22 is open.
- Supported SSH ciphers are implemented, for example aes128-cbc and 3des-cbc. These are implemented by default in Mac and Linux devices, but not by default in some Unix platforms, including Solaris.
- SSH is enabled.
- The interpreter for the scripts being run need to be installed on the system. AVG scripts that run on these platforms are written in Python, which is available by default on Mac OS X and most Linux deployments.

**Tip:** You can configure a role to see all the tasks but not be able to modify any scripts. See [Setting Permissions for a Role](#).

---

## Scripts, Automation Packages, and Tasks

### Scripts

In Managed Workplace, a script consists of one or more files that are transferred to devices to perform an action along with some metadata. This includes the script name, the file to be executed, a category, a version, a minimum version of Managed Workplace, and the author. Meta data may also include parameters. For scripts that are contained in .ZIP files, the file to be executed within the .ZIP file is also in the meta data.

Managed Workplace includes a library of scripts that you can use to perform a number of maintenance and remediation tasks on devices, including:

- install applications such as WinRAR, Google Chrome, Adobe Reader, and Microsoft Security Essentials;
- desktop management functions such as creating local user, change computer name, delete files, and disable guest account;
- Active Directory management such as creating and deleting Active Directory users, changing domain administrator password, listing all domain users, and disabling a domain user account;
- Windows Server management tasks such as creating a network share, and restarting MWExpertSystem.

**Note:** The scripts provided by AVG are read-only. If you want to modify a script provided by AVG, copy it on the **Library** page, and modify the copy.

More advanced users can create their own scripts, and add them to Managed Workplace. The **Library** also includes three script templates, one for PowerShell, one for VBScript, and one for Python, that you can copy and export from Managed Workplace, modify as needed, and then re-import. For more information, see [Adding a Quick Task](#).

### Automation Packages

An automation package is a group of two or more scripts bundled together to be executed in sequence. Managed Workplace includes several automation packages that you can use to perform multi-script actions within a single task. The scripts in an automation package can have parent-child relationships, in which the child script only executes based on a designated outcome from the parent script.

For more ideas on what you can do with a script package, and to learn how to create one, see [Creating Automation Packages](#).

---

## Tasks and Quick Tasks

A task is a script or automation package that has been scheduled to either run immediately or at some point in the future. Tasks include the script or automation package to be run, the time or recurring time when it is to run, and can include advanced configurations such as alerting and timeout behavior. See [Scheduling Tasks](#).

A quick task is a script or automation package with some or all of the parameters pre-set, for ease of use. You can set up multiple quick tasks on a single script or package, which is helpful when you want to pre-set the script parameters to certain values. You can also schedule quick tasks just like a regular task. See [Adding a Quick Task](#).

## Creating Automation Packages

You can bundle scripts together in a package to create tasks that run more than one script. The scripts in a package run one after the other, in the order that you arrange them. You can also set up parent/child relationships between scripts, in which the child script runs conditionally on the result from the parent script. For example, you can set up a condition that if the parent script fails, the child script will execute.

Managed Workplace includes many automation packages that you can modify and use as needed, or you can create your own. When you create or modify a script package, you can enter script parameter values, set up package termination conditions, and set up notification flags for generating alerts based on individual script results. These settings are then used when you schedule the script package as an automated task.

## Create a Script Package

When you create a script package, you must indicate the target platform type; either Windows OS, Mac OS, or Unix/Linux. Only scripts that are compatible with the platform type that you select will be available to be added to the package.

When you create a package, you provide a name, version, and script category. You can optionally provide a description of the package and the author name.

- 1 In Service Center, click **Automation** > **Library**.
- 2 Click **New Package**.
- 3 From the **Choose Package Type** list, select the package platform type.
- 4 Click **OK**.

- 
- 5 In the **Package Name** box, type a name for the package.
  - 6 In the **Version** box, give the package a version number. Version numbers must be in the format of <num>.<num>.<num>.<num>.
  - 7 In the **Author** box, type your name.
  - 8 From the **Category** list, choose a scripting category for the package.
  - 9 In the **Description** box, provide a description of the package.

You are now ready to begin adding scripts to the package.

### See Also

[To add scripts to a package](#)

[To add child scripts to a package](#)

[Change the Order of Scripts in a Package](#)

## Adding Scripts and Child Scripts to a Package

You can add any script in Managed Workplace that matches the package platform type, either Windows OS, Mac OS, or Unix/Linux. Only scripts of the same platform type, or scripts that can work on any platform type, are available to be added to the package.

There is an overall limit of 50 scripts in a package, including both parent and child scripts.

**Note:** If you plan on adding child scripts to a package, you must first add the parent script to the package, using the procedure below.

### To add scripts to a package

- 1 In the **Package Content** area, click **Add Scripts**.
- 2 Select the check box beside each script you want to add to the package.
- 3 Click **Add**.
- 4 Click on each script to review the script parameters. If the script has optional parameters or required parameters that have values entered, the parameters won't be displayed when running the package as a task.

### To add child scripts to a package

You can set up a child-parent relationship between scripts. A child script will only execute if a defined outcome from the parent script is met. This condition for the child script can be based on the standard output of the parent script,

---

the standard error, or the return code. Managed Workplace allows you to set up child scripts up to 5 levels deep.

You can add multiple child scripts to a parent script. These scripts can be moved up and down to change the sequence of execution, however you cannot move a child script up or down to another parent script. See [Change the Order of Scripts in a Package](#).

- 1 In the **Package Content** area, select the script to which you want to add a child script. You can select a script by clicking anywhere in the script row.
- 2 Click **Add Child Scripts**.
- 3 Select the check box beside each script you want to add as a child script.
- 4 Click **Add**.

## Change the Order of Scripts in a Package

After adding scripts to a package, you can move them up and down to change the order in which they run. There are several things you must keep in mind when changing the order of scripts in a package:

- if you have configured a package termination condition for a script, ensure that this does not result in an unintended premature termination of the package if you move it up in the script order.
- when you move a parent script, the child scripts are moved with it.
- you can change the order of child scripts within a parent script, but you cannot move a child script up or down to another parent script.

- 1 In the **Package Content** area, select the script that you want to move up or down.
- 2 Click either **Move Up** or **Move Down**.

## Preparing Scripts and Packages for Use in a Policy or Task

Before you schedule a script or automation package for use in a policy or task, you can modify them by doing any of the following:

- for scripts, you can create a copy of the script, and then modify how the script is run by changing the parameters, and by specifying whether the script has a dedicated execution and setting whether to run on Onsite Manager.

- 
- for automation packages, you can add a notification flag for script results for which you think the task scheduler will want to create an alert. This notification flag also emails script execution results to the scheduler.
  - for scripts in a package, specify a script outcome that will result in the termination of the package execution.
  - for both scripts and automation packages, you can set up a quick task, in which you specify some or all of the parameters that will be run when the quick task is scheduled. For more information, see [Adding a Quick Task](#).

You can also prepare your own scripts for use in Managed Workplace. For more information, see [About Adding Scripts](#).

## Viewing Script Details

You can view script details for any script in the **Library**. The **Script Details** page includes information such as the target platform, how the script is supposed to run (for example, on Onsite Manager, or as a dedicated execution), and lists any parameters added to the script. You can modify the script from the Script Details page, if desired.

**Note:** If the script is authored by AVG, you must create a copy of the script and then modify the copy. See [Copying Scripts, Automation Packages, and Quick Tasks](#).

The **Script Details** page can be accessed in a number of ways:

- by clicking a script name in the **Library**
- from within a package, by clicking a package name in the **Library**, and then clicking a script name.

## Set Up Alert Conditions for Scripts in a Package


You can set an alert condition, called a notification, to any script result in a package, which can then be used to generate an alert when the automation package is used in a scheduled task. Notifications are useful when you want to set up individual alerts for scripts in a package, as opposed to an alert for the package as a whole.

To set up alert notifications on a script in a package, you specify the script result that would trigger an alert, and you can provide the message that will appear in the body of any alert emails generated, for example “Succeeded”. An alert email from a scheduled task can include many of these messages in a single email, and you can set up multiple alert conditions for each script.

---

**Tip:** You should know the return code, standard output, or standard error on which you want to alert before setting up the notification in Service Center.

- 1 In Service Center, click **Automation > Library**.
- 2 To access the script package you want to modify, do one of the following:
  - In the **Name** column, begin typing the name of the script package.
  - Click the triangle beside the **Category** in which the script package resides.

**Note:** Script packages are indicated with a package icon .


- 3 Click the name of the script package.
- 4 In the **Package Content** area, click the name of the script for which you want to set a notification condition.
- 5 In the **Notifications** area, click **Add**.
- 6 From the **Condition** list, select the type of condition.
- 7 In the **Value** box, type the text of the return code, standard error, or standard output that you selected in the previous step.
- 8 In the **Script Notification Message** area, type the message that will appear in the body of any alert emails.
- 9 Click **Save**.

**Note:** When scheduling the package as a task, this alert notification appears as “Package Notification Flag Set” when setting up an alert rule. See [To add an alert if the script fails to be executed or returns output that is not considered a successful execution](#).

## Set Up Package Termination Conditions

You can identify the script outcomes that will result in the termination of the package execution when it is scheduled as a task. If you set a termination condition on a parent script, the child scripts associated with it will not run.

- 1 In Service Center, click **Automation > Library**.
- 2 To access the script package you want to modify, do one of the following:
  - In the **Name** column, begin typing the name of the script package.
  - Click the > beside the **Category** in which the script package resides.

**Note:** Script packages are indicated with a package icon .

- 3 Click the name of the script package.



- 
- 4 In the **Package Content** area, click the name of the script for which you want to set a package termination condition.
  - 5 In the **Package Termination Conditions** area, click **Add**.
  - 6 From the **Condition** list, select the type of condition.
  - 7 In the **Value** box, type the text of the return code, standard error, or standard output that you selected in the previous step.
  - 8 Click **Save**.

## Adding a Quick Task

A quick task is a script or package with some or all of the parameters filled in. When you set up a quick task, you decide which parameters you want defined for the quick task, and which parameters you want to provide at execution time:

- when you fill in a quick task parameter, this parameter becomes a static value, which means that when you schedule the quick task, this value is already provided. For example, setting up a quick task to disable the Guest account on a device or group of devices.
- when you leave a required parameter blank, you are prompted to fill in the parameter when scheduling the quick task. For example, setting up a quick task to disable any account. When you schedule the quick task, you must specify which account to disable.

Only required parameters with no pre-set value will be prompted for when running a quick task.

### Example: Add several quick tasks to send messages to users

You want to create a quick task to send a message to a user that you will be rebooting their device. You would select the Send Message to Users (Windows) script, and in the **Parameters** area, type the notification message in the **Message** box.

After the quick task is created, it is saved in the **Library**, and it is available to run immediately or to be scheduled. You can then add more quick tasks using the same Send Message to Users (Windows) script, but with different messages entered in the **Message** box. For example, you could create one quick task that sends a service outage message, and another quick task that sends a data center down message. These three quick tasks are now available in the **Library**.

---

### To add a quick task

- 1 In Service Center, click **Automation > Library**.
- 2 Click **New Quick Task**.
- 3 In the **Name** box, type a name for the quick task.
- 4 In the **Version** box, type a version number for the quick task. Version numbers must be in the format of <num>.<num>.<num>.<num>.
- 5 In the **Author** box, type the author name.
- 6 From the **Category** list, select a category for the quick task.
- 7 Optionally, in the **Description** box, provide a description for the quick task. This description should provide information for users about the quick task, for example for a Send Message to Users quick task, you could explain this quick task notifies users of a planned service outage.

## Creating Automation Policies

Automation policies help you standardize the way that you perform routine maintenance tasks on your customer networks. You can create your own automation policies, or use one of the pre-built automation policies available in Managed Workplace. For example, Managed Workplace includes a *Microsoft Windows Desktop Maintenance* automation policy that audits for installed Antivirus applications, defrags volumes, deletes temporary files, enables RDP, scans for unauthorized network shares, and performs other maintenance tasks.

An automation policy includes a script or script package, a schedule for when the task is run, and rules that define on which devices the task will run. These rules take effect when you add this policy to a service in a service plan, and the service plan is applied to a site or group. For more information, see [Applying Service Plans to Existing Sites](#) and [Applying Service Plans to Site Groups](#).

You can set up an execution schedule that determines when the scripts in the automation policy will run. Execution schedules are used by automation, patching, and AVG AntiVirus policies to ensure that these vital services are performed at a time that does not disrupt the customer's business. For information on setting up execution schedules, see [Setting Up Execution Schedules](#).

## Creating Automation Policies

An automation policy includes the following:

- a script or script package

- 
- a schedule for when the script will run, either by using an execution schedule, or by creating a custom schedule
  - automatic inclusion rules that determine which type of devices on which the script will run
  - optionally, manually applied sites, groups, and devices
  - optionally, devices that are excluded from the policy

The automated tasks that are created using an automation policy are displayed in the **Calendar**, in addition to any scheduled tasks you have created by going to **Automation > Calendar**, selecting a time block, and clicking **Schedule**.

After creating an automation policy, you can add it to a service for use in a service plan. For more information, see [Creating Services](#).

### To create an automation policy

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Click **New**.
- 3 Provide a policy name and description.
- 4 Click **Create**.
- 5 Click the **Settings** tab.
- 6 Click **Create**.

### To select the script or script package that will run

- 1 From the **Choose what to execute** list, select a favorite script, or select (Item from library) and then do the following:
  - a From the **Choose an item from the library** list, filter the list of scripts in the **Choose an item by name** list by selecting the operating system on which the script runs. Choose from Windows, Mac OS, or Unix/Linux.
  - b From the **Choose an item by name** list, select a script or script package.

### To run the automation policy using an execution schedule

When you set up an automation policy to use execution schedules, you must select whether the policy will use the daily, weekly, or monthly schedule for automated tasks, as defined in the execution schedule.

- 
- 1 In the **Schedule** area, select the **Run as per applicable Execution Schedule** option button. For more information about execution schedules, see [Setting Up Execution Schedules](#).
  - 2 Select one of the following option buttons:
    - daily
    - weekly
    - monthly

### To set up an automation policy schedule that overrides applicable execution schedules

- 1 In the **Schedule** area, select the **Override Execution Schedules** option button.
- 2 In the **Start Time** box, type a start time for when the automated task will begin. Alternatively, you can click the clock icon to select a time from the list.
- 3 Specify how often to run the task by selecting one of the following:
  - To run a task daily, select the **Daily** option button, and then specify how often the task will run each day by selecting a frequency from the **Run daily** list. By default, daily tasks run once a day.
  - To run a task weekly, select the **Weekly** option button. Then specify what day or days to run the task.
  - To run a task monthly, select the **Monthly** option button. Then select either a specific date or a recurring day in the month.

### To set timeout limits for the automation policy

- 1 Click **Show Advanced Configuration**.
- 2 In the **Timeouts** area, set the following timeouts:
  - To set a timeout for the execution of the task, from the **Execution** list select the length of time the task can execute before the timeout occurs.
  - To set a timeout for when the device is unreachable, from the **Device Unreachable** list select the length of time the task can be unreachable before the timeout occurs.

**Note:** The **Device Unreachable** timeout does not apply to scripts that run on Onsite Manager or Device Manager.

---

### To wake computers to run a task

You have the option to wake a computer if it is asleep so that the task can be run at the scheduled time.

- 1 Click **Show Advanced Configuration**.
- 2 In the **Miscellaneous** area, click the **Wake computers if asleep** check box.

### To add an alert if the script fails to be executed or returns output that is not considered a successful execution

- 1 Click **Show Advanced Configuration**.
- 2 In the **Alerts - Execution Results** section, click **Add**.
- 3 Type a title for the alert.
- 4 Optionally, type a description for the alert.
- 5 In the **Alert Rule** area, click **Add**.

**Note:** The options for adding an alert rule differ depending on whether you are scheduling a script or an automation package to run.

- 6 If you are scheduling a script to run as a task, select the parameters that will generate an alert:

**Return Code** Indicates the execution outcome of the script. The return codes can vary because they can be defined inside the script itself.

**Standard Output** Indicates the output produced, if any, by a task to the StOut. Standard output is used to express anything the script needs to communicate. This can be error messages, success messages, or lists of data.

**Standard Error** Indicates the error produced by the script.

**Note:** The **Return Code**, **Standard Output**, and **Standard Error** are values that are scripted or programmed into the script or executable that is being run.

- 7 Click **Save**.

### To add an alert for delivery failure

- 1 Click **Show Advanced Configuration**.
- 2 In the **Alerts - Delivery Failure** area, click **Add**.
- 3 Do the following:
  - To add an alert category when a script fails to be delivered, click **Categorize Alert** and add a category from the list.

- 
- To remove an alert category for when a script fails to be delivered, click **Categorize Alert** and remove a category from the list.
  - To create a trouble ticket when a script fails to be delivered, select the **Create Trouble Ticket** check box.
  - To set the alert to self-heal when a script fails to be delivered, select the **Self-Heal** check box. To specify the setting for self-heal, click the **Self-Heal** link. To clear the associated Trouble Ticket, ensure the **Clear Trouble Ticket check** box is selected. To send a notification, select the **Enable Self-Heal Notification** check box and specify the time delay. Then click **Save**.
  - To send an email when a script fails to be delivered, select the **Send Email** check box and select either **All Users** to send an email to all users whose role is to receive alert notifications or select **Specify Emails** to specify certain recipients who should be notified. In the From box, type the email address from where the alert is emailed.
  - To escalate an alert if an alert has not been cleared or self-healed in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect. Select the **Send Email** check box and follow the instructions in the previous bullet.
  - To automate reactions to an alert, select the **Run Script** check box and select the **Category** and **Script** name, and set any parameters if necessary.

4 Click **Save**.

## Applying Automation Policies

### Creating Rules to Automatically Include Devices

Automatic approval rules determine which devices are eligible to have the automation policy applied. For example, if you are creating an automation policy for Windows servers only, you can set up an automatic approval rule to include devices with the word “server” in the OS name.

The approval rules do not come into effect until the automation policy has been applied, either by adding it to a service and then applying the service to a group or site, or by adding it to a service in a service plan, which can also be applied to a group or site.

The process for setting up approval rules is the same for automation policies as it is for all other policy types (i.e, monitoring, patch, and AVG AntiVirus). For more detailed instructions on setting up automatic approval rules, including examples, see [Creating Automatic Inclusion Rules for a Monitoring Policy](#).

- 
- 1 In Service Center, click **Configuration > Policies > Automation**.
  - 2 Click the name of the automation policy to which you want to create an automatic inclusion rule.
  - 3 Click the **Automatic Application** tab.
  - 4 Create the automatic inclusion rule by clicking **Add** to create a rule.
  - 5 Repeat step 4 until the rule is complete.
  - 6 Click **Save**.

### **Adding Devices or Groups to an Automation Policy**

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Click the name of the automation policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following to apply the automation policy to a group or device:
  - In the **Applied Groups** area, click **Add**. Filter on the Group Type, if desired. Click the group and click **OK**.
  - In the **Applied Devices** area, click **Add**. Filter the list of devices. Select the check box beside the device and click **OK**.

**Note:** You can view the automation policies applied to service and site groups on the **Groups** page, by going to **Configuration > Groups**, clicking the group name, and then clicking the **Policies** tab. For more information, see [Viewing the Policies Applied to a Group](#).

### **Removing Devices or Groups from an Automation Policy**

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Click the name of the automation policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following:
  - To select one device or group at a time, select the check box that corresponds with each device you want to remove.
  - To select all the devices or groups at once, select the check box at the top of the column.
- 5 Click **Remove**.

---

## Excluding Devices from an Automation Policy

You can exclude specific devices from an automation policy. When you add a device to the exclusion list, it will never have this automation policy applied, even if the device meets the criteria outlined in the automatic application rules, and the automation policy is applied to the site or group to which the device belongs.

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Click the name of the automation policy from which you want to exclude devices.
- 3 Click the **Excluded Devices** tab.
- 4 Click **Add**.
- 5 Use the filters at the top to narrow your selection, and click **Filter**.
- 6 Select the check box beside each device you want to exclude from the policy.
- 7 Click **OK**.
- 8 Click **Save**.

**Tip:** You can exclude multiple devices in a site or group by selecting **Site** or **Group** from the **Filter By** list, and then selecting the check box at the top of the list of returned devices to exclude all devices listed.

## Renaming an Automation Policy

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Click the name of the automation policy that you want to edit.
- 3 Click **Modify**.
- 4 Type a new name in the **Policy Name** box.
- 5 Click **Save**.

## Deleting an Automation Policy

When you delete an automation policy, you are removing the automated task from any devices that have the policy applied.

- 1 In Service Center, click **Configuration > Policies > Automation**.
- 2 Select the check box beside the automation policy you want to delete.
- 3 Click **Delete**.



---

## Adding, Importing, and Exporting Scripts and Packages

You can add your own scripts into Managed Workplace, and you can export scripts from Managed Workplace, modify them using their native script editor, and then import back into Managed Workplace.

- Adding a script into Managed Workplace adds just the script file. You must then provide a script name and category, and configure the parameters.
- Importing a script into Managed Workplace imports the script and script metadata, including the script name, category, and parameter configurations.

**Note:** Managed Workplace includes 3 script templates that you can export, modify, and then add back into Service Center. See [Using Script Templates](#).

### About Adding Scripts

You can add your own scripts to Managed Workplace, which is recommended for users who have some scripting knowledge. When adding your own scripts, keep the following in mind:

- Managed Workplace supports scripts for Windows, Mac OS, and Unix/Linux devices.
- Scripts can also be executables.
- You must install a command interpreter on the device if it is not native.
- If you're using PowerShell, it must be enabled on the device.
- When creating a task using a PowerShell script, there is an option to enable PowerShell on the target device if it is not already enabled.

### Recognized Script Languages

Managed Workplace recognizes the following script languages:

Language	Windows	Mac OS X	Unix/Linux
Executable (no extension or .exe)	Yes	Yes	Yes
PowerShell (.ps1)	Yes	No	No
VBScript (.vbs)	Yes	No	No
Perl (.pl)	Yes	Yes	Yes

---

Language	Windows	Mac OS X	Unix/Linux
Batch (.bat)	Yes	No	No
JavaScript (.js)	Yes	Yes	Yes
Command (.cmd)	Yes	No	No
Python (.py)	Yes	Yes	Yes
Shell (.sh, .csh, .bash, .ksh)	No	Yes	Yes

---

### Scripting Best Practices and Notes

When adding your own scripts, keep the following in mind:

- Managed Workplace allows a script to be created with the same name as an existing script. This is because internally Managed Workplace uses a GUID (Globally Unique Identifier). This GUID is automatically generated for each script, is unique when created, and will not be duplicated (and it is not visible in the user interface).
- Maximum script file size: For hosted Service Center environments, 1GB for all scripts and parameters. For on premise Service Center deployments, 1 GB per script or parameter.
- Maximum number of simultaneous scripts running: 5 and after that the scripts queue.
- Scripts are never deleted automatically by Service Center.
- Many Managed Workplace scripts change settings that are also configurable using group policy. Ensure no competing policy exists when using these scripts, otherwise options you have set may be changed back when the policy is applied at next boot.
- When writing a script and you want to call another script that is bundled with the package, you have to provide a full path name.

To determine the full path name from within PowerShell, use the following command:

```
$myDir = Split-Path -Parent
$MyInvocation.MyCommand.Path
```

To determine the full path name from within VBScript, use the following command:

---

```
dir =  
left(WScript.ScriptFullName, (Len(WScript.ScriptFull  
Name) - (len(WScript.ScriptName))))
```

To determine the full path name from within Python, use the following command:

```
scriptPath =  
os.path.dirname(os.path.abspath(inspect.getfile(in  
spect.currentframe())))
```

To determine the full path name from within a .BAT script, use the following command:

```
set dir=%~dp0
```

## Scripting Configuration Options

When adding your own scripts to Managed Workplace, there are several options you can select that determine how the script is run.

### Run on Onsite Manager

Scripts can be configured to run on Onsite Manager. Running a script on Onsite Manager causes the execution to occur on the Onsite Manager device, targeting the devices specified.

Typically this option is used in conjunction with script variables that resolve to values corresponding to the targeted devices. See [Variables](#).

### Dedicated Execution

You can set if you want a script to run without any other dedicated execution scripts running at the same time. For example, if you're installing software, you would only want that script to run before another one starts.

### Target Type

You can specify that a script will run on any platform, or on specific platforms. Supported platforms include Windows, Mac OS, and Linux/Unix. It is recommended that you select the "any platform" option when creating a script to run on Onsite Manager, as the task will be targeting multiple devices.

### About Script Parameters

Scripts can have any number of parameters associated with them. Parameters must be filled in if they are required, whether or not there is a default value. If there is a default value and you remove it, you cannot save the script.

---

There are two ways that parameters can be passed. The first is using key-value pairs, as explained below. You can also pass parameters by entering a command as if you were using a command line, or specify that the script has no parameters.

**Key/Value** Parameters are passed to scripts as key-value pairs in the form <key>=<value>. The keys for each parameter on the Script Details page must match the keys expected by the scripts. It is possible to use scripts that do not accept key-value pairs as defined above. The values for these parameters will simply be passed to the script at run-time.

The parameters are listed in the order displayed in the user interface. You can move parameters up and down in the list when setting up your script.

**Note:** Keys for a parameter cannot be changed after saving the script.

**Optional Parameters** Parameters can be tagged as optional. If a parameter is optional and the user does not specify a value when creating a task, the parameter is not passed to the script.

**Variables** Parameters accept Windows environment variables and Managed Workplace-specific variables.

Managed Workplace-specific variables	Description
%CUSTGUID%	The customer GUID.
%DeviceDNSName%	The DNS name of the target device.
%DeviceGUID%	The device's GUID.
%DeviceIP%	The IP address of the target device.
%DeviceMacAddress%	The MAC address of the target device.
%DeviceSystemName%	The host name of the target device.
%SCMessagingURL%	The SC Messaging URL.
%SCURL%	The Service Center URL.
%VARNAME%	The VAR name.

---

**Label** The label supplied when creating a script is displayed to the user as a form label when they add a task.

**Types** Parameters can be

- an integer, which can have a minimum and maximum value specified and a default value.
- a string, which can have a maximum length specified and a default value.
- a file, which will enable the user to click a **Browse** button to locate a file on their system and have the file uploaded and included in the task sent to devices. This can be used for software installation, for example.
- a flag, which is passed as an integer, with the value 1 for true and 0 for false. The script will act based on the presence of this parameter. For example, a script might install software silently if the **Silent** flag is present. This is represented in Managed Workplace as a check box. Flags cannot be optional because they are always true or false.

**Note:** PowerShell refers to flag parameters as switch parameters.

- a list, which will enable the user to select from a number of string values using a drop list.
- a password, in which the value will be masked on entry and on display. The value is stored in a two-way encrypted format in the database, but they are passed to scripts in clear text.

**Default** Parameters, except for file and password parameters, can have a default value. These are populated in value boxes in tasks when they are first added but can be changed at a later time.

## Adding a Script to Managed Workplace

To set up tasks to use custom written scripts, you must first add the scripts you need to the script library and specify any meta data for the script. This includes the name, underlying script file, category, version, minimum Managed Workplace version, author, description and all the parameters.

- 1 In Service Center, click **Automation > Library**.
- 2 Click **New Script**.
- 3 In the **Script Name** box, type a name for the script.
- 4 In the **Version** box, type a number.

Versions for scripts must be in the form of `<num>.<num>[.<num>[.<num>]]`, though only a single number is required.

- 5 In the **Author** box, type the author name.

---

6 Click **Browse** and locate the script file or .ZIP file, and then click **Open**.

7 If the script file you added was a compressed file (such as a .ZIP), then select the starting file from the **Starting File** list.

The starting file in the .ZIP file must be at the root level of the .ZIP file and have a file extension that is recognized by Managed Workplace.

8 Select a category from the list or type a new one.

Script categories allow for easier organization of scripts. A category can be created by typing in a new name. If you type a new name, Managed Workplace creates a new category.

9 In the **Minimum Managed Workplace Version** box, type the version of Managed Workplace that this script supports.

By default, the Minimum Managed Workplace Version is not automatically populated with the current version of Service Center, but this is usually the value you want to enter. If you need to specify that it only works with the current version, type the current version number. If this is done, the script will be sent to Onsite Managers that are not the specified version number but will stay in a state of "Pending Upgrade" until Onsite Manager is upgraded or the schedule expires. Note however, that they can be assigned to devices on older Onsite Managers. If this is done, the script will be run on the device when Onsite Manager is upgraded, unless the execution time is in the past and the retry period has expired.

You can locate Managed Workplace build numbers in the correct format by clicking **Help > About**.

When there is a new version of a script, Onsite Manager checks the minimum version and determines whether to download the file from Service Center.

10 If you want the script to run on Onsite Manager, select the **Run on Onsite Manager** check box.

11 If the script must run without another dedicated execution script running, select the **Dedicated execution** check box.

12 In the **Target Type** area, do the following:

- To specify that the script can run on any platform type, select the **Any platform** option button.
- To specify that the script can run on specific platforms, select the **Specific platform** option button, and then select the check box beside the operating systems on which the script will run.

13 In the **Description** box, type a description.

---

This description is shown to users when they create tasks for the script. It is a good idea to describe how to use any parameters for the script.

Now you are ready to add parameters to the script. If you do not want to add parameters, select the **No Parameters** option button.

### To add parameters to a script using a command line

Managed Workplace allows you to use scripts as if you were running them directly on the system using command lines. When adding parameters to a script, you can simply specify the parameters as if you were running them on the command line. For example, the following is a PowerShell command line parameter:

```
-server "http://someserver" -force
```

**Note:** The format of command line parameters varies by scripting language.

- 1 Click the **Use Command Line Parameters** button.
- 2 To set a default value, in the **Default Value** box, type the command.
- 3 Click **Save**.

### To add an integer parameter

- 1 Click the **Use Parameter List** button.
- 2 Click **Add**.
- 3 From the **Choose Parameter Type** list, choose **Integer**.
- 4 Click **OK**.
- 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
- 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
- 7 To set the minimum and maximum values for a script parameter, type a minimum and maximum in the appropriate boxes.
- 8 To set a default value for the script parameter, type a default in the **Default** box.
- 9 To set this parameter as optional, select the **Optional Parameter** check box.
- 10 Click **OK**.

### To add a string parameter

- 1 Click the **Use Parameter List** button.

- 
- 2 Click **Add**.
  - 3 From the **Choose Parameter Type** list, choose **String**.
  - 4 Click **OK**.
  - 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
  - 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
  - 7 To set the maximum length for the string parameter, type a length in the **Maximum Length** box.
  - 8 To set a default value for the string parameter, type a default in the **Default** box.
  - 9 To set this parameter as optional, select the **Optional Parameter** check box.
  - 10 Click **OK**.

#### **To add a file parameter**

- 1 Click the **Use Parameter List** button.
- 2 Click **Add**.
- 3 From the **Choose Parameter Type** list, choose **File**.
- 4 Click **OK**.
- 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
- 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
- 7 To set this parameter as optional, select the **Optional Parameter** check box.
- 8 Click **OK**.

#### **To add a flag parameter**

- 1 Click the **Use Parameter List** button.
- 2 Click **Add**.
- 3 From the **Choose Parameter Type** list, choose **Flag**.
- 4 Click **OK**.



- 
- 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
  - 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
  - 7 Provide a default value for the flag parameter, by either selecting the **Default Value** check box for a true value, or leaving the **Default Value** check box cleared for a false value.  
**Note:** Flag parameters must have a default value.
  - 8 Click **OK**.

### To add a list parameter

- 1 Click the **Use Parameter List** button.
- 2 Click **Add**.
- 3 From the **Choose Parameter Type** list, choose **List**.
- 4 Click **OK**.
- 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
- 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
- 7 In the **List Entries** box, type the first entry in the list to the **Add unique list entry** box, then click the plus sign **+**.

**Tip:** When specifying items in a list, you can include content in the list that will not be shown to the user that is filling in the parameters, by using a pipe character (|) and then providing the hidden content after the pipe character. The value after the pipe character is passed to the script. For example, if a script takes one of several integer values, but you want to present string values to the user, you can enter the following:

```
First Entry | 1
```

- 8 Repeat step 7 until you have added all entries in the list.
- 9 Optionally, select an entry in the list, and use the up and down arrow buttons to move the entry in the list. The list items are presented to the user in the same order that they appear in the **List Entries** box.
- 10 To select a default value for the list, select an entry from the **Choose a default** list.
- 11 To set this parameter as optional, select the **Optional Parameter** check box.

---

12 Click **OK**.

### To add a password parameter

- 1 Click the **Use Parameter List** button.
- 2 Click **Add**.
- 3 From the **Choose Parameter Type** list, choose **Password**.
- 4 Click **OK**.
- 5 To set a label for a script parameter, type a label in the **Parameter Label** box.
- 6 To identify this parameter as unique, in the **Parameter Key** box, type a unique identifier. This key is the key expected by the script.
- 7 To set this parameter as optional, select the **Optional Parameter** check box.
- 8 Click **OK**.

### To change the order of script parameters

After adding parameters to a script, you can change the order in which they appear to the user scheduling the task, by moving parameters up and down in the list.

- 1 Select the check box beside one or more parameters.
- 2 Click one of the following:
  - **Move Up**
  - **Move Down**

### To delete a script parameter

- 1 Select the check box beside a script parameter.
- 2 Click **Delete**.

### To save a script

When you have finished adding parameters to your script, click **Save**. The script is now ready to be used in a policy or a task.

---

## Importing a Script

You can import a Managed Workplace Script (an .MWS) file into Managed Workplace. When you import an .MWS file, it includes all the meta data for the script, including the name, author, and description.

Importing a script is recommended when you are moving the script from one Service Center environment to another. For example, from a test environment to a production environment, or for cases when you share scripts with other partners using the forums on the partner portal.

**Note:** The .MWS file is a .ZIP file with the extension changed.

When a script is imported, its category is added to the system, if it doesn't already exist.

Version checking is performed when importing a script that is already on the system. You are warned if you attempt to import an older version of the script than is present on the system. Additionally, any scheduled tasks based on this script are updated to the new script. This is important to keep in mind in situations in which script parameters have been modified in the newer version; if an optional parameter is changed to required, for example, the task based on this script will no longer function and will be deleted. You must then reschedule the task after importing the newer version of the script.

Importing a script is different than adding a new script to Service Center. When you add a new script, you are adding just the script file, and then configuring the metadata and parameters. For more information on adding scripts, see [About Adding Scripts](#).

- 1 In Service Center, click **Automation > Library**.
- 2 From the **More Actions** list, select **Import**.
- 3 Click **Browse** and locate the script to import, and then click **Open**.
- 4 Click **OK**.

## Exporting a Script

When you export a script, information from the script is stored in an .MWS file along with all required script files. The file contains the original script file or files (or .ZIP file) along with an .XML file that contains the meta data for the script. By doing this, if the script is imported into another system, the meta data is preserved.

- 1 In Service Center, click **Automation > Library**.
- 2 Select the check box beside the name of the script that you want to export.

- 
- 3 From the **More Actions** list, select **Export**.

## Using Script Templates

Managed Workplace includes three script templates that you can use as the basis for creating a custom script:

- PowerShell
- Python
- VBScript

To use a script template, do the following steps:

- 1 In Service Center, click **Automation > Library**.
- 2 In the **Category** column, select **Script Templates** from the list.
- 3 Select the check box beside the script template you want to customize.
- 4 Click **Export**.
- 5 Click **Save** and specify a location.
- 6 The script is saved as an .mws file. To open the script file, rename the file with a .zip extension.
- 7 The .zip file contains the script file and an XML file containing the script metadata. Extract the script file and open it in a text editor.

Each template implements the same functionality, demonstrating:




- param mechanisms, which tell you how to handle the parameter types;
  - a command that you can run to determine in which directory the script files are located;
  - a script example
- 8 Replace the script example portion with your custom script, and save.
  - 9 In Service Center, click **Automation > Library > New Script**.

---


# Managing Scripts, Automation Packages, and Quick Tasks

## Viewing Scripts, Automation Packages, and Quick Tasks

The Library lists all of the scripts, automation packages, and quick tasks available for use. Each automation item type is signified with an icon:

Icon	Automation Item
	Script
	Automation package
	Quick task

To easily find items, you can group items by category, and you can sort the columns. Some columns also include drop lists for you to further filter your search results.

- 1 In Service Center, click **Automation > Library**.
- 2 To filter items, do any of the following:
  - To group the list of scripts by category, click the gear icon  and select **Group by Category**.
  - Click a column name to sort by that column.
  - To filter the list, use the lists under the column headers.
- 3 Click the name of the script, automation package, or quick task you want to view.

## Copying Scripts, Automation Packages, and Quick Tasks

You can create copies of scripts, packages, and quick tasks, which you can then modify as needed. Creating copies is useful when you want to reuse most of the configurations, and just want to make a few small changes to suit a slightly different purpose.

**Note:** Scripts and automation packages created by AVG cannot be modified directly, which prevents any custom changes you make from being overwritten when you install an update to the script from Update Center. To modify an

---


script or package authored by AVG, you must create a copy using the steps below, and then you can modify the copy.

- 1 In Service Center, click **Automation > Library**.
- 2 Select the check box beside the script, automation package, or quick task you want to copy.
- 3 From the **More Actions** list, select **Copy**.
- 4 Provide a new name for the script, package, or quick task.
- 5 Optionally, update the description.
- 6 Click **Copy**.

You are now ready to modify the copy.

## Designate a Script, Automation Package, or Quick Task as a Favorite

You can designate scripts, packages, and quick tasks as favorites, to help you easily find automation items that you use often. When you designate an item as a favorite, it is added to the **Favorites** page, and it is also added to the top of the **Choose what to execute list** when creating a policy or a task.

Favorites are also available from quick links , which allow you to run your favorite scripts, packages, and quick tasks from the following locations in Service Center:

- **Device List** page
- **Device Overview** page
- **Device Search** page
- **Execution Summary** page
- **System Log Viewer**
- **Alerts Page**

For example, if you are viewing alerts on the **Alerts** page, you might come across a device with low disk space. You can right-click the quick link beside the device, and select “Run Automated Task”.

Any scripts, packages, or quick tasks that you have designated as a favorite are listed first.

Note that you can also select **Item from library**, and select any script, package, or quick task in the library to run against the device.

---

### To designate a script, package, or quick task as a favorite

- 1 In Service Center, click **Automation** > **Library**.
- 2 Locate the script, automation package, or quick task that you want to designate as a favorite.
- 3 Click the star beside the script, package, or quick task. The star becomes yellow to indicate that the item is a favorite.

**Tip:** To remove an item from your favorites, click the star again.

## Viewing Your Favorite Scripts, Packages, and Quick Tasks

From the **Favorites** page, you can view your favorite scripts, packages, and quick tasks. You can also schedule a task from the **Favorites** page.

- 1 In Service Center, click **Automation** > **Favorites**.
- 2 Optionally, click the script, package, or quick task you want to schedule, and then click **Run Now** or **Schedule**.

**See Also** [Designate a Script, Automation Package, or Quick Task as a Favorite](#)

## Installing a Script or Automation Package

You can install a new script or automation package by going to Update Center and selecting a script from the list of new scripts available for install. This list is updated periodically as new scripts are released by AVG.

- 1 In Service Center, click **Automation** > **Library**.
- 2 From the **More Actions** list, select **Get More**.

The **Components** page opens with a list of scripts and automation packages available for installation.

- 3 Select the check box beside the script you want to install.
- 4 Click **Install**.

**See Also**

[Updating and Installing Service Center Components](#)

## Updating a Script or Automation Package

You can update a script or automation package in Service Center by installing an update from Update Center. Script updates are created periodically by AVG and added directly to Update Center for you to install.

---

When an update is available, a **New** icon appears beside **Update Center > Components** in the navigation pane to indicate that there is a new component available for upgrade. The **Library** page also displays an update icon next to a script if an update exists.

- 1 In Service Center, click **Update Center > Components**.
- 2 Click **Updates**.
- 3 In the **Type** column, select Automation from the list.
- 4 Select the check box beside the script or package update you want to install.
- 5 Click **Update**.

**See Also**

[Updating and Installing Service Center Components](#)

## Deleting a Script

When you delete a script:

- any policies using the script will cease to function
- any tasks using the deleted script will be deleted, unless they are currently running. If Onsite Manager already has the file, then it will be able to run. If it doesn't, then the task fails.

Deleting a script has no impact on historical information.

- 1 In Service Center, click **Automation > Library**.
- 2 Select the check box beside the name of the script that you want to delete.
- 3 From the **More Actions** list, select **Delete**.
- 4 Click **OK**.



---

## Scheduling Tasks

### Adding a Task

The following table provides an overview of the different goals you might have when creating tasks, and how you can achieve those goals:

If you...	Then...
want to schedule patch updates on devices once a month, a few days after Microsoft releases patches on the third Tuesday of the month.	Schedule a recurring task that installs patch updates on devices, and takes place on the fourth Tuesday of each month.
want to set up a task with the parameters pre-set, that you know you will reuse often. For example, a task that sends users a message that you will be performing maintenance on their devices, and they might experience an interruption.	Create a quick task, and type in the message notifying users of the planned maintenance. Add the quick task to your favorites. The quick task can be run directly on a device using a quick link.
want to execute a basic command line task	Set up a task to run immediately.

When you add a task, you perform these steps:

- 1 Choose whether to run the task immediately, or schedule it to run at a future time.
- 2 Select the script or automation package to include.
- 3 Set the task parameters.
- 4 Add the task to a device or group.
- 5 For tasks scheduled to run at a future time, optionally add a recurrence.
- 6 Set advanced configuration settings such as alert configurations and task timeout settings.

When you save the task, it is added to the **Calendar**, which you can then use to view upcoming tasks, check the progress and results of completed tasks, and edit tasks if necessary. See [Viewing Tasks](#).

---

### To add a task and select a script

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Do one of the following:
  - Click **Run Now** to run the task immediately.
  - Click **Schedule** to run the task at a future time.
- 3 From the **Choose what to execute** list, do one of the following:
  - If you have flagged scripts or packages as favorites, they will appear in this list. Click a favorite.
  - Click **(Item from library)**, and then either use the filters to narrow down the list of scripts and packages, or if you know the name of the script or package you want to use, start typing it in the **Choose an item by name** list.

### To add a task to a device

- 1 In the **Target Devices** area, click **Add**.
- 2 Filter the results by selecting the appropriate items and click **Filter**.
- 3 Select the check boxes for the devices to which you want to apply the task.
- 4 Click **Add**.
- 5 Repeat steps 1 to 4 until all the devices to which you want to apply the task are included.

### To add a task to a group

- 1 In the **Target Groups** area, click **Add**.
- 2 Select the check boxes for the groups to which you want to apply the task.
- 3 Click **Add**.
- 4 Repeat steps 1 to 3 until all the devices to which you want to apply the task are included.

### To run the task once at a scheduled time

You can set a task to run at a scheduled time, or to run the next time the target device reboots.

- 1 In the **Schedule** area, click the calendar icon and select a date or type a date.
- 2 Click the clock icon and select a time of day or type a time.

- 
- 3 To run the task after a device reboots, select the **Run on next reboot after this time** check box.

When you select this check box, the task will run the next time the device reboots after the date and time you selected in steps 1 and 2.

- 4 Click **Schedule**.

### To run a task on a recurring schedule

- 1 In the **Schedule** area, click the calendar icon and select a date or type a date.
- 2 Click the clock icon and select a time of day or type a time.
- 3 Click **Add Recurrence**.
- 4 Do one of the following:
  - To run a task daily, select the **Daily** option button, and then specify how often the task will run each day by selecting a frequency from the **Run daily** list. By default, daily tasks run once a day.
  - To run a task weekly, select the **Weekly** option button. Then specify what day or days to run the task.
  - To run a task monthly, select the **Monthly** option button. Then select either a specific date or a recurring day in the month.
- 5 Click **Schedule**.

**Note:** Managed Workplace does not allow you to set a task to run on the 29th, 30th, or 31st of the month, as the task will not run on any months that do not have those days, i.e. February. Use **Last Day** instead.

### To set a timeout on a task

- 1 Click **Show Advanced Configuration**.
  - 2 In the **Timeouts** area, set the following timeouts:
    - To set a timeout for the execution of the task, from the **Execution** list select the length of time the task can execute before the timeout occurs.
    - To set a timeout for when the device is unreachable, from the **Device Unreachable** list select the length of time the task can be unreachable before the timeout occurs.
- Note:** The **Device Unreachable** timeout does not apply to scripts that run on Onsite Manager or Device Manager.
- 3 Click **Schedule**.

---

### To wake a computer to run a task

You have the option to wake a computer if it is asleep so that the task can be run at the scheduled time.

- 1 Click **Show Advanced Configuration**.
- 2 In the **Miscellaneous** area, click the **Wake Computers** check box.
- 3 Click **Schedule**.

### To email execution results to the task scheduler

You can choose to have the task execution results emailed to yourself.

- 1 Click **Show Advanced Configuration**.
- 2 In the **Miscellaneous** area, click the **Email Results** check box.
- 3 Click **Schedule**.

### To add an alert if the script fails to be executed or returns output that is not considered a successful execution

You can specify alerts when the script fails to be executed or returns output that is not considered a successful execution.

- 1 Click **Show Advanced Configuration**.
- 2 In the **Alerts - Execution Results** area, click **Add**.
- 3 Type a title for the alert.
- 4 Optionally, type a description for the alert.
- 5 In the **Alert Rules** area, click **Add**.

**Note:** The options for adding an alert rule differ depending on whether you are scheduling a script or an automation package to run.

- 6 If you are scheduling a script to run as a task, select the parameters that will generate an alert:

**Return Code** Indicates the execution outcome of the script. The return codes can vary because they can be defined inside the script itself.

**Standard Output** Indicates the output produced, if any, by a task to the StOut. Standard output is used to express anything the script needs to communicate. This can be error messages, success messages, or lists of data.

**Standard Error** Indicates the error produced by the script.

---

**Note:** The Return Code, Standard Output, and Standard Error are values that are scripted or programmed into the script or executable that is being run.

- 7 If you are scheduling an automation package to run as a task, select one or both of the following:
  - To alert on the package result, select the **Package Result** check box, and then select the package result that will generate an alert (**Any**, **Completed Successfully**, or **Completed With Errors**).
  - To alert on the notification conditions set for scripts in the package, select the **Package Notification Flag Set** check box. This generates an alert based on the alert conditions that were set on individual scripts in the package when the package was created or modified. For more information, see [Set Up Alert Conditions for Scripts in a Package](#).
- 8 Do the following:
  - To add an alert category when a script fails to be executed, click **Categorize Alert** and add a category from the list.
  - To remove an alert category for when a script fails to be executed, click **Categorize Alert** and remove a category from the list.
  - To create a trouble ticket when a script fails to be executed, select the **Create Trouble Ticket** check box.
  - To set the alert to self-heal when a script fails to be executed, select the **Self-Heal** check box. To specify the setting for self-heal, click the **Self-Heal** link. To clear the associated Trouble Ticket, ensure the **Clear Trouble Ticket** check box is selected. To send a notification, select the **Enable Self-Heal Notification** check box and specify the time delay. Then click **Save**.
  - To send an email when a script fails to be executed, select the **Send Email** check box and select either **All users** to send an email to all users whose role is to receive alert notifications or select **Specify email addresses** to specify certain recipients who should be notified. In the **From** box, type the email address from where the alert is emailed.
  - To escalate an alert if an alert has not been cleared or self-healed in a set amount of time, select the **Escalate Alert** check box and select a time after which the alert escalation will take effect. Select the **Send Email** check box and follow the instructions in the previous bullet.
  - To automate reactions to an alert, select the **Run Script** check box and select the **Category** and **Script** name, set any parameters if necessary and specify whether you want it to run on the device or Onsite Manager.

---

## 9 Click **Schedule**.

### To add an alert if the script fails to be delivered

You can specify alerts for delivery failures when you schedule a task to run in the future.

**Note:** Script alerting is not available for **Run Now** type tasks. When configuring a task with the **Run Now** option, it is sent immediately to the target devices. Because monitor and alert rules are updated to Onsite Managers every two minutes, if you want to configure a task to run as soon as possible but want to ensure that you are able to receive alerts, you must use the **Schedule** link to begin adding a task.

#### 1 Click **Show Advanced Configuration**.

#### 2 In the **Alerts - Delivery Failures** area, click **Add**.

#### 3 Do the following:

- To add an alert category when a script fails to be delivered, click **Categorize Alert** and add a category from the list.
- To remove an alert category for when a script fails to be delivered, click **Categorize Alert** and remove a category from the list.
- To create a trouble ticket when a script fails to be delivered, select the **Create Trouble Ticket** check box.
- To set the alert to self-heal when a script fails to be delivered, select the **Self-Heal** check box. To specify the setting for self-heal, click the **Self-Heal** link. To clear the associated Trouble Ticket, ensure the **Clear Trouble Ticket** check box is selected. To send a notification, select the **Enable Self-Heal Notification** and specify the time delay. Then click **Save**.
- To send an email when a script fails to be delivered, select the **Send Email** check box and select either **All users** to send an email to all users whose role is to receive alert notifications or select **Specify email addresses** to specify certain recipients who should be notified. In the **From** box, type the email address from where the alert is emailed.
- To escalate an alert if an alert has not been cleared or self-healed in a set amount of time, select the **Escalate Alert** check box and select a time after which the alert escalation will take effect. Select the **Send Email** check box and follow the instructions in the previous bullet.
- To automate reactions to an alert, select the **Run Script** check box and select the **Category** and **Script** name, set any parameters if necessary

---


and specify whether you want it to run on the device or Onsite Manager.

- 4 Click **Schedule**.

## Working with Tasks

### Viewing Tasks

You can use the **Calendar** to view the status of executed tasks, and to view future scheduled tasks. The **Calendar** shows tasks that were created using an automation policy, and tasks that were scheduled right on the **Calendar** page.

**Tip:** Tasks that were created with an automation policy have a triangle icon . When you mouse over the icon, a tooltip displays the name of the automation policy. For more information on automation policies, see [Creating Automation Policies](#).

You can view tasks in day, week, or month calendars, or you can select an **Agenda** view that displays a list of tasks in a 7 or 30 day time period.

Tasks in the **Calendar** are color coded to indicate the status:

Task Color	Status
Green	All script executions were successful.
Red	At least one script execution failed.
Blue	No script failures, but at least one script execution is still pending.
Grey	The task has not yet executed.

#### To filter tasks in the Automation Calendar

Use the filter options to narrow your view to sites, site groups or service plans.

- 1 In Service Center, click **Automation > Calendar**.
- 2 Use the filters at the top of the **Calendar** page to only show the tasks at a site, group, or service plan, and click **Filter**.

#### To view the tasks scheduled in a day

- 1 In Service Center, click **Automation > Calendar**.
- 2 Click the **Day** button.

---

### To view the tasks scheduled in a week

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Click the **Week** button.

### To view the tasks scheduled in a month

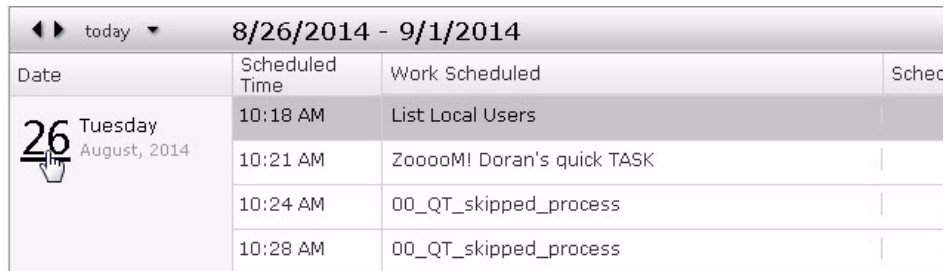
- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Click the **Month** button.

### To view tasks in a list view

The **Agenda** view allows you to view tasks in a list similar to what was available in pre-9.0 versions of Managed Workplace when viewing the **Task Timeline**. The **Agenda** view lists all of the tasks for the current week.

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Click the **Agenda** button.

**Tip:** When viewing tasks using the **Agenda** view, you can click a date to switch to the **Day** calendar view for that day:



◀▶ today ▾ 8/26/2014 - 9/1/2014			
Date	Scheduled Time	Work Scheduled	Sched
26 Tuesday August, 2014	10:18 AM	List Local Users	
	10:21 AM	ZooooM! Doran's quick TASK	
	10:24 AM	00_QT_skipped_process	
	10:28 AM	00_QT_skipped_process	

### To refresh the Automation Calendar

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Click the **Refresh** link.

## Following Up on Executed Tasks

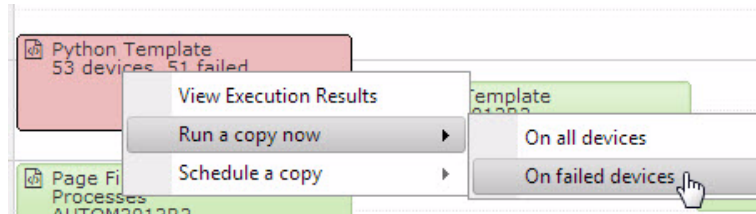
You can use the **Calendar** to verify whether tasks have succeeded or failed, and view details of the task execution.

You can rerun tasks directly from the **Calendar**. You can rerun tasks now, or schedule tasks to run again in the future, regardless of the task outcome. For



---

tasks that have failed, you can choose to re-run the task on the failed devices only.



### To rerun a task immediately

- 1 In Service Center, click **Automation > Calendar**.
- 2 Right-click a task, and select **Run a copy now**, then select one of the following:
  - **On all devices**
  - **On succeeded devices** (for tasks that have succeeded) or **On failed devices** (for tasks that failed).

**Note:** If the task was created using an automation policy, clicking **Run a copy now** creates a standalone task in the **Calendar** using the settings in the automation policy as a template.

- 3 If required, change any of the options for running the task.
- 4 Click **Run Now**.

### To rerun a task at a future time

- 1 In Service Center, click **Automation > Calendar**.
- 2 Right-click a task, and select **Schedule a copy**, then select one of the following:
  - **On all devices**
  - **On succeeded devices** (for tasks that have succeeded) or **On failed devices** (for tasks that failed).

**Note:** If the task was created using an automation policy, clicking **Schedule a copy** creates a standalone scheduled task in the **Calendar** using the settings in the automation policy as a template.

- 3 If required, change any of the options for scheduling the task.
- 4 Click **Schedule**.

---

## To view task execution results

You can view detailed results of executed tasks. When viewing script execution results, you get the following information:

- return code
- standard error, if any
- standard output, if any
- execution details, including outcome, start time, and execution time
- script details, including name, version, author, and parameters, if any.

For tasks based on an automation package, the execution results lists each script and includes a **Details** link to view execution results for each individual script.

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Right-click a task, and select **View Execution Results**.

## To export the standard output to a text file

**Note:** This option is only available if there is Standard Output to export.

- 1 In Service Center, click **Automation** > **Calendar**.
- 2 Right-click a task, and select **View Execution Results**.
- 3 Click **Export Standard Output to File**.
- 4 Click **Open** or **Save**.

**Tip:** If the results include html tags, you can save the file as .HTM or .HTML in order for it to render properly.

## Changing a Task

If you edit a task that was created from the **Calendar**, the previous task is replaced. So, for example, if a recurring task is configured to run on one device and it is edited to run on another device (that is, the original device is removed), the task will no longer run on the original device. If you want the task to run on both devices, the new devices should be added to the task or a new task created using the **Copy** option.

If you edit a task that was created using an automation policy, clicking **Edit** opens the **Automation Policy** page to the **Settings** tab, where you can make your changes.

- 1 In Service Center, click **Automation** > **Calendar**


- 
- 2 Locate the task you want to edit using the **Day, Week, Month, or Agenda** view.

**Note:** You can only edit a task that has not yet run. These tasks are grey in the **Calendar**:

2 pm	 Page File Utilization Top 20 Processes AUTOM2012R2	C
3 pm	 List Running Processes AUTOM2012R2	C

- 3 Right-click the task, and select **Edit**.
- 4 Make the required changes.
- 5 Click **Schedule**.

## Deleting a Task

Tasks are never deleted automatically by the system. You can only delete tasks that were created using the Calendar; you cannot delete tasks that were created using an automation policy. Tasks created using a policy have a black triangle icon .

**Note:** You cannot delete tasks that have already executed, or are in process.

### To delete a task

- 1 In Service Center, click **Automation > Calendar**.
- 2 Click on the task you want to delete.
- 3 Click **Delete**.



# CHAPTER 13

## MANAGING AVG ANTIVIRUS

*This section provides detailed information about the following topics:*

- *About AVG AntiVirus in Managed Workplace*
  - *Setting Up AntiVirus Policies*
  - *Managing AVG AntiVirus in Managed Workplace*
-

---

## About AVG AntiVirus in Managed Workplace

Managed Workplace includes an AVG AntiVirus integration within Service Center, allowing you to configure antivirus policies and deploy them to devices in your customer sites without leaving Service Center. This AntiVirus integration is included with your Managed Workplace license, however you must purchase AntiVirus licenses from your AVG sales representative to use this feature. AVG AntiVirus offers an entry point for you to upsell security services in addition to traditional remote monitoring and management.

Antivirus security is an important component of any managed services offering, and having AVG AntiVirus integrated with Managed Workplace allows you to:

- set up as many antivirus policies as you require;
- deploy the antivirus policies to devices;
- run antivirus scans;
- keep track of AVG AntiVirus licenses on device;
- alert on threats detected, and act on those alerts as needed;
- run reports.

For example, you can create unique antivirus policies for workstations and servers. Or, you can create antivirus policies that correspond with the levels of service you provide via service level agreements.

## Using AVG AntiVirus in Managed Workplace

If you are already a AVG CloudCare customer, or you are using a different antivirus solution, you can still make use of AVG AntiVirus in Managed Workplace. The following table provides an overview of how you can use AVG AntiVirus in Managed Workplace, in relation to the current antivirus services that you may be offering:

<b>If you...</b>	<b>Then...</b>
Already have an AVG CloudCare or BAU license, and already have AVG AntiVirus installed on customer devices	If you choose to use the Managed Workplace AVG AntiVirus feature, then installing the client on devices will not affect existing installations.

---

If you...	Then...
<p>Are already using the AVG Cloud-Care service module in Managed Workplace</p>	<p>You can continue to use the Cloud-Care service module, in conjunction with AVG AntiVirus in Managed Workplace. These two features provide complementary capabilities:</p> <ul style="list-style-type: none"> <li>• Use the CloudCare service module to report and alert on all CloudCare services, including AVG AntiVirus, AVG Content Filtering, and AVG Online Backup.</li> <li>• Use AVG AntiVirus in Managed Workplace to create AntiVirus configuration policies, and deploy AntiVirus to devices at your customer sites. Also includes AntiVirus alerting, license tracking, and reporting.</li> </ul>
<p>Are using a third-party AntiVirus solution.</p>	<p>You can continue using this third-party solution; use of AVG AntiVirus in Managed Workplace is optional. You can also choose to offer both services, depending on your service agreements and the type of anti-virus monitoring that you want to provide.</p>

---

## Setting Up AntiVirus Policies

An AntiVirus configuration policy is a collection of settings and preferences that determine how AVG AntiVirus is configured on devices, and includes manual or automatic application rules that determine to which devices it will be applied.

Managed Workplace includes two default AntiVirus policies that you can use with or without modifications; a workstation policy and a server policy. You can also create as many customized AntiVirus policies as you require.

Use AntiVirus policies to determine:

- 
- how unwanted programs and spyware are handled
  - how email is scanned and how infected messages and attachments are reported
  - when to run scans and when to apply virus definition and program updates;
  - which level of firewall security to apply
  - configuration of identity protection and web browsing protection.

You can:

- Copy an existing AntiVirus policy, including one of the default policies included with Managed Workplace, or create a new policy;
- Configure the settings in the AntiVirus policy to determine which AntiVirus settings are applied;
- Automatically apply the policy to devices by setting up automatic application rules;
- Add policies to services, for use in service plans;
- Manually apply the policy to specific groups and devices;
- Remove policies you no longer require.

## About the Default AntiVirus Policies

Managed Workplace includes two default AntiVirus policies:

- The Workstation AV Policy is set up with some common settings to protect workstation computers.
- The Server AV Policy is set up to prevent automatic updates and reboots.

The default policies are pre-configured with automatic application rules that detect a device's domain role (workstation for the Workstation AV policy, and server for the Server AV policy) and deploys AVG AntiVirus to any device that matches the domain role.

You can use these default AntiVirus policies as is, or you can modify the configuration settings and automatic application rules. You cannot modify the summary information. To modify the default policies, it is recommended that you first create a copy, and then modify the copy. See [Copying an AntiVirus Policy](#).



---

## Creating a New AntiVirus Policy

When setting up a new AntiVirus policy, you begin by providing a name and description and by specifying the deployment options that determine which components of AVG AntiVirus will be installed, and whether you will initiate the AVG client install or whether it will be automatically installed. Once you click **Create**, the deployment options cannot be changed.

To install AntiVirus on devices, follow this procedure and select the options to install AntiVirus automatically or initiate the install manually.

- 1 Click **Configuration > Policies > AVG AntiVirus**.
- 2 Click **New**.
- 3 In the **Policy Name** box, type a name for the AntiVirus policy.
- 4 In the **Description** box, type a description of the policy.
- 5 Select one of the following:
  - To automatically install the AVG AntiVirus client on devices, click the **Automatically install the AntiVirus client** option button.
  - To initiate the installation of the AVG AntiVirus client after the policy has been applied, click the **Allow me to initiate the install** option button. Choose this option if you prefer to install the AVG AntiVirus client off-hours, without disrupting the device user, for example.

**Tip:** If you choose to initiate installation, you can regularly check the **Devices Needing Antivirus Installation** page to view a list of devices and install AVG AntiVirus from within Managed Workplace. See [Initiating the Installation of AntiVirus on Devices](#).

- 6 To automatically remove antivirus products from a competitor, select the **Remove competitive antivirus products** check box.
- 7 Select the check box beside each of the AntiVirus components you want to install.
  - **Email Protection - Personal Email Scanner** Scans every email message sent or received; whenever a virus is detected in an email, it is removed to the Virus Vault immediately. The component can also filter out certain types of email attachments, and add a certification text to infection-free messages.
  - **Email Protection - Microsoft Outlook Add-in** Integrated in Microsoft Outlook, scans every email message sent or received; whenever a virus is detected in an email, it is removed to the Virus Vault immediately. The component can also filter out certain types of email attachments, and add a certification text to infection-free messages.

- 
- **Identity Protection** An anti-malware component that protects from of malware using behavioral technologies and provides zero day protection for new viruses.
  - **Web Browsing Protection** Consists of two services: LinkScanner Surf-Shield and Online Shield.  
**LinkScanner** protects you by analyzing the web pages behind all the links on any web page you're viewing and making sure they're safe.  
**Online Shield** scans the content of visited web pages (and possible files included in them) before these are displayed in your web browser or downloaded to your computer. Online Shield detects dangerous JavaScript and recognizes malware contained in pages and stops downloading immediately. With this feature enabled, clicking a link or typing in a URL to a dangerous site will automatically block you from opening the web page, protecting you from being infected.
  - **Firewall** Controls all traffic on every network port of your computer. Based on the defined rules, Firewall evaluates applications that are either running on your computer (and want to connect to the Internet/local network), or applications that approach your computer from outside trying to connect to your PC. For each of these applications the Firewall then either allows or forbids the communication on the network ports. By default, if the application is unknown (i.e. has no defined Firewall rules), the Firewall will ask you if you wish to allow or block the communication attempt.

**Note:** The AntiVirus components that you select determine which settings will be available for configuration on the Settings tab.

- 8 Click **Create**.

## Installing AntiVirus on Devices

The following are the steps to install AVG AntiVirus on devices. In order to install AVG AntiVirus on devices, you must have a valid AVG AntiVirus license for each device.

- 1 Decide on your AntiVirus policy.
  - Use one of the default AntiVirus policies. If you use a default AntiVirus policy, AntiVirus is not installed automatically on devices. You can install on each device individually. See [About the Default AntiVirus Policies](#).
  - Create a new AntiVirus policy. If you ceate a new AntiVirus policy, you can choose to install AntiVirus individually, by device, or install AntiVirus on devices automatically. See [Creating a New AntiVirus Policy](#).

- 
- 2 Apply the chosen AntiVirus policy to sites, groups, or devices. To create rules to apply the AntiVirus policy, see [Creating Rules to Automatically Apply an AntiVirus Policy](#). To apply an AntiVirus policy to devices and groups manually, see [Manually Applying an AntiVirus Policy to Devices and Groups](#).
  - 3 If you choose an AntiVirus policy that doesn't install AntiVirus on devices automatically, initiate the manual install of AntiVirus on the devices. [See Initiating the Installation of AntiVirus on Devices](#).

## Copying an AntiVirus Policy

When you copy an AntiVirus policy, a new policy is created with a number appended to the policy title to differentiate the copy from the original, for example (1), (2), etc. The Overview information is copied and cannot be modified in the copy, except for the name and description. The configuration settings and automatic application rules are also copied, and can be modified as needed.

**Note:** Automatic application rules and manually applied groups and devices are not copied.

- 1 Click **Configuration > Policies > AVG AntiVirus**.
- 2 Select the check box beside the AntiVirus policy you want to copy.
- 3 Click **Copy**.

The copied AntiVirus policy appears at the bottom of the **AVG AntiVirus Policies** list.

- 4 Click the AntiVirus configuration policy copy name to change the name and description, and modify the automatic application rules, manual application, and settings.

## Creating Rules to Automatically Apply an AntiVirus Policy

Managed Workplace includes a rule-building interface that you can use to define the criteria a device must meet in order for the AntiVirus policy to be applied. This interface is the same as the one that you use to create automatic application rules for other policy types, such as monitoring policies and automation policies.

Rules are created by first defining AND and OR statements, then by adding rules to the statements. For example, if you are creating a rule to automatically deploy an AntiVirus policy to all devices running on a Windows 7 operating system, in the default AND group, you would specify that the OS Name contains "Windows 7".

---

To create a rule that specifies that the device must either have a Windows 7 or a Windows 2008 operating system, you would change the AND group to an OR group, and then add a second rule that specifies that the OS Name contains "Windows 2008".

For instructions on creating and modifying automatic application rules, see [To create an automatic inclusion rule for a monitoring policy](#). Note that the method for creating automatic applications rules is the same for AntiVirus policies as it is for other policy types.

## Manually Applying an AntiVirus Policy to Devices and Groups

You can select groups and devices to which you want to apply the AntiVirus policy.

- 1 Click **Configuration > Policies > AVG AntiVirus**.
- 2 Click the name of the AVG policy to which you want to apply devices and groups.
- 3 Click the **Manual Application** tab.
- 4 To apply the policy to a group, do the following:
  - In the **Applied Groups** section, click **Add**.
  - From the **Group Type** list, select **Service Groups** or **Site Groups**.
  - Select the check box beside each group you want to add.
  - Click **Add**.
- 5 To apply the policy to a device, do the following:
  - In the **Applied Devices** section, click **Add**.
  - Use the filters at top of the window to narrow down the devices displayed, and click **Filter**.
  - Select the check box beside each device you want to add.
  - Click **OK**.
- 6 Click **Save**.

## Configuring the Settings for an AntiVirus Policy

A policy is a group of system settings that determine how AVG AntiVirus will be configured on a device. The **Settings** tab lists the types of settings that you can apply, which depend upon which deployment options you selected when creating the AntiVirus policy. For example, by default the Firewall setting is not

---

enabled. You must enable Firewall when creating an AntiVirus policy for the Firewall section to be available on the **Settings** tab.

The **Settings** tab is a jumping-off point for configuring the level of protection you want to provide for computer, email, identity, web browsing, and firewall. You can also configure scan, update, and schedule settings.

- 1 Click **Configuration > Policies > AVG AntiVirus**.
- 2 Click the name of the AVG policy to which you want to configure settings.
- 3 Click the **Settings** tab.
- 4 Do any of the following:
  - [Configure Computer Protection Settings](#)
  - [Configuring Email Protection Settings](#)
  - [Configure Identity Protection Settings](#)
  - [Configure LinkScanner Protection](#)
  - [Configure Online Shield Protection](#)
  - [Configure Password Protection Settings](#)
  - [Configure Firewall Settings](#)
  - [Configure Scan Settings](#)
  - [Configure Schedule Settings](#)
  - [Configure Update Settings](#)
  - [Configure Exception Settings](#)

**Note:** If you are editing the Server AV policy, the following settings are not included by default and are therefore not available to be edited: Email, Identity, LinkScanner, and Online Shield.

### Configure Computer Protection Settings

Computer Protection settings includes both antivirus and anti-rootkit settings.

- 1 Ensure the **Enable Computer Protection** check box is selected.
- 2 Click **Modify**.

### To configure AntiVirus Settings

- 1 Select the **Antivirus** tab.
- 2 Select the **Enable Resident Shield** check box to easily switch on/off resident protection. Resident Shield scans files as they are copied, opened,

---

or saved. When a virus or any kind of threat is detected, you will be warned immediately. We recommend that you leave this setting on.

- 3 Select any of the following check boxes:

**Ask me before removing threats** If you leave this unchecked, AVG will automatically heal the infection, or if it is not possible to heal, it will move the object into the Virus Vault.

**Report potentially unwanted programs and spyware threats**

Check to activate the Anti-Spyware engine and scan for spyware, as well as for viruses. Spyware represents a questionable malware category; even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated for increased computer security.

**Report enhanced set of potentially unwanted programs** Select to detect extended packages of spyware: programs that are harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases computer security even more, however it can possibly block legitimate programs.

**Scan files on close** This type of scanning ensures that AVG scans active objects (e.g., applications and documents) when they are being opened and closed in order to protect the computer against sophisticated viruses.

**Scan boot sector of removable media** Scan the boot sector of a floppy disk or the partition table of a hard disk for a boot-sector virus, which is spread to computer systems by booting.

**Use heuristics** Heuristics analysis is the dynamic emulation of the scanned object's instructions in a virtual computer environment.

**Scan files referred in registry** AVG will scan all executable files added to the startup registry to avoid a known infection being executed upon the next computer startup.

**Enable thorough scanning** Activates the most thorough scanning algorithms, which scan areas of the computer that rarely get infected. This check box is cleared by default, as this method of scanning is time-consuming and should only be used when you suspect the computer has been infected.

**Enable instant messaging protection (only applicable to workstations)** Verifies that instant messaging communication and data downloaded within Peer-to-Peer networks (networks allowing direct connection between clients, without a server, which is potentially dangerous; typically used to share music files) are virus free.

- 
- 4 To specify expert settings for Resident Shield, click **Expert Settings**, and do the following:
    - Choose to either scan all files or scan only infectable files and selected document types. If you choose selected document types, you can specify file extensions that must be scanned under all circumstances.
    - Select the **Always scan files without extensions** check box to ensure that even files with no extension and with an unknown format will be scanned by the Resident Shield. We recommend selecting this check box, as files without extensions are suspicious.
  - 5 Click **Save**.

### Configure Anti-Rootkit Settings

Rootkits are programs or other technology that camouflage the presence of malicious software on the computer. Some rootkits are not a threat and are part of legitimate software. Other rootkits are malicious and are designed to take control of a computer system, without authorization from the users or system administrators. Use the Anti-Rootkit settings to detect and effectively remove dangerous rootkits.

- 1 Select the **Anti-Rootkit** tab.
- 2 To scan applications, select the **Scan applications** check box.
- 3 To scan drivers, select the **Scan drivers** check box.

**Note:** Both the **Scan applications** and **Scan drivers** check boxes are selected by default. We recommend that you leave these options selected.
- 4 Select one of the following scanning modes:
  - Select **Quick rootkit scan** to scan all running processes, loaded drivers, and the system folder (typically C:\Windows).
  - Select **Full rootkit scan** to scan all running processes, loaded drivers, the system folder (typically C:\Windows), plus all local disks (including the flash disk, but excluding floppy disks and CD drives).
- 5 Click **Save**.

### Configuring Email Protection Settings

Email protection includes email scanning, certification of incoming and outgoing mail, attachment filtering, and server activation.

- 1 In the **Email Protection** area, do the following:

- 
- Select **Enable for Incoming Messages** to apply the Email Protection settings to all incoming messages.
  - Select **Enable for Outgoing Messages** to apply the Email Protection settings to all outgoing messages.

2 Click **Modify**.

### To configure Email Scanner Settings

On this tab, you can set the parameters for scanning incoming and outgoing email for spyware, unwanted programs, and password-protected or suspicious attachments.

1 Select the **Email Scanner** tab.

2 In the **Email Scanning** section, select any of the following:

- Select **Check incoming mail** to scan all email messages delivered to the device's email client.
- Select **Check outgoing email** to scan all emails sent from the device's email account.
- Select the **Modify subject of virus infected messages** check box if you want to be warned the scanned email message was detected as infectious. In the box, fill in the desired email message subject. This text will then be added to the "Subject" box for each detected email message for easier identification and filtering. The default value is **\*\*\*VIRUS\*\*\***, which we recommend you keep.

3 In the **Scanning Properties** section, select any of the following:

**Use heuristics** Select to use the heuristics detection method when scanning email messages. When this option is selected, you can filter email attachments not only by extension but also the actual contents of the attachment will be considered.

#### **Report potentially unwanted programs and spyware threats**

Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended packages of spyware: programs that are harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases the device's security, however it can possibly block legitimate programs.



---

**Scan inside archives** Select to scan contents of archives attached to email messages.

- 4 In the **Email Attachments Reporting** section, select any of the following:

**Report password-protected archives** Archives (ZIP, RAR, etc.) that are protected by password are not possible to scan for viruses; select this check box to report these as potentially dangerous.

**Report password-protected documents** Documents protected by password are not possible to scan for viruses; select this check box to report these as potentially dangerous.

**Report files containing macros** A macro is a predefined sequence of steps aimed to make certain tasks easier for a user (MS Word macros are widely known). Because a macro can contain potentially dangerous instructions, you can select this check box to ensure that files with macros are reported as suspicious.

**Report hidden extensions** Hidden extensions can make a suspicious executable file, e.g. "something.txt.exe", appear as a harmless plain text file, e.g. "something.txt". Select this check box to report hidden extensions as potentially dangerous.

**Move reported attachments to Virus Vault (incoming emails only)**

Specify whether you wish to be notified via email about password protected archives, password protected documents, files containing macros and files with hidden extension detected as an attachment of the scanned email message. If such a message is identified during scanning, define whether the detected infectious object should be moved to the Virus Vault.

- 5 Click **Save**.

### Configure Certification Settings

On this tab, you can mark the specific check boxes to decide whether you want to certify incoming or outgoing mail. For each of these options you can further specify whether certification is only added to email messages with attachments.

- 1 Select the **Certification** tab.
- 2 Do any of the following:
  - To certify incoming email, select the **Certify incoming email** check box. To certify attachments on incoming email, select the **With attachments only** check box.

- 
- To certify outgoing email, select the **Certify outgoing email** check box. To certify attachments on outgoing email, select the **With attachments only** check box.
- 3 In the **Email certification text** box, write the desired certification text. By default, the certification text consists of basic information that states “No virus found in this message”. You can extend or change this message, if desired.
  - 4 In the **Language used for email certification text** box, define the language in which the automatically generated certification text should be displayed.  
**Note:** Only the default text will be displayed in the requested language; your customized text will not be translated automatically.
  - 5 Click **Save**.

### Configure Mail Filtering Settings

The Mail Filtering tab allows you to set up parameters for scanning email attachments.

- 1 Click the **Mail Filtering** tab.
- 2 If you want to automatically remove all message attachments detected as infectious or potentially dangerous, select the **Remove attachments (incoming emails only)** check box.
- 3 To define specific types of attachments that should be removed, select any of the following:
  - Remove all executable files** All \*.exe files will be deleted.
  - Remove all documents** All \*.doc, \*.xls, and \*.xlsx files will be deleted.
  - Remove files with these comma-separated extensions** Will remove all files with the defined extensions.
- 4 Click **Save**.

### Configure Servers Settings

The **Servers** tab allows you to edit parameters of POP3, IMAP, and SMTP Email Scanner servers. The parameters that you set are the same for each Email Scanner server type.

- 1 Click the **Servers** tab.
- 2 Click **Add Server**.
- 3 From the **Server Type** list, select a protocol.

- 
- 4 Click **OK**.
  - 5 In the **Server Name** box, specify the name of the server.
  - 6 In the **Type of Login** area, specify one of the following:
    - Automatic** Login will be carried out automatically, according to the device's email client settings.
    - Fixed host** In this case, the program will always use the server specified here. Specify the address or name of the mail server. The login name remains unchanged. You may use a domain name (e.g., pop.acme.com) or an IP address (e.g., 123045.67.89). If the mail server uses a nonstandard port, you can specify this port after the server name by using a colon as the delimiter (e.g., pop.acme.com:8200).
    - Note:** The standard port for POP3 communication is 110. The standard port for IMAP communication is 143. The standard port for SMTP communication is 25.
  - 7 In the **Additional Settings** area, you can specify the following:
    - Local port (used in email client)** Specify the port on which the communication from the email application should be expected. This port must be specified in the email application as the port for communication using the protocol that you specified.
    - Connection** From the list, specify which kind of connection to use. If you choose a secure connection, the data sent is encrypted without the risk of being traced or monitored by a third party. This feature is also only available when the destination mail server supports it.
  - 8 In the **Email Client Server Activation** section, select the check box to activate the specified server. Clearing this check box deactivates the server.
  - 9 Click **Add**.
  - 10 Click **Save**.

### Configure Identity Protection Settings

Identity Protection offers real-time protection from malware with a focus on preventing identity thieves from stealing information, such as passwords, bank account and credit card numbers, and other personal data. Identity Protection provides zero-day protection from viruses and other malware by monitoring real-time process activity for over 285 different behavioral patterns.

- 1 Ensure that the **Enable Identity Protection** check box is selected.
- 2 Click **Modify**.

- 
- 3 Select the **Activate Identity Protection** check box. This check box is selected by default.
  - 4 Specify what to do when a threat is detected:
    - Always prompt** When a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
    - Automatically quarantine detected threats** All possibly detected threats are moved to the Virus Vault immediately. Keeping the default settings, when a threat is detected, you will be asked whether it should be moved to quarantine to make sure no applications you want to run are removed.
    - Automatically quarantine known threats** All applications detected as possible malware are automatically and immediately moved to the Virus Vault.
  - 5 Click **Save**.

### Configure LinkScanner Protection

AVG LinkScanner alerts users and blocks them from accessing dangerous webpages before they click a page link. In Managed Workplace, you can enable Surf-Shield, which blocks users from accessing known malicious sites.

- 1 In the **Web Browsing Protection** section, ensure that the **Enable LinkScanner Protection** check box is selected.
- 2 Click **Modify**.
- 3 Select the **Enable Surf-Shield** check box to activate real-time protection against exploitive sites as they are accessed. Known malicious site connections and their exploitive content are blocked as they are accessed by the user via a web browser (or any other application that uses HTTP).
  - Note:** This check box is selected by default.
- 4 Click **Save**.

### Configure Online Shield Protection

AVG Online Shield provides web browsing protection, which scans files before they are downloaded from the Internet.

- 1 In the **Web Browsing Protection** section, ensure that the **Enable Online Shield Protection** check box is selected.
- 2 Click **Modify**.

- 
- 3 To activate the entire Online Shield service, select the **Enable Online Shield** check box.

**Note:** This check box is selected by default.

- 4 To configure advanced settings, click the **Expert Settings** button and select any of the following:

**Check archives** Scan the content of archives possibly included in the web page to be displayed.

#### **Report potentially unwanted programs and spyware threats**

Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended packages of spyware programs that are harmless when acquired from the manufacturer directly, but can be misused for malicious purposes later. This is an additional measure that increases the computer's security, however it may block legitimate programs and is therefore not selected by default.

**Use heuristics** Scan the content of the page to be displayed using the heuristic analysis method (dynamic emulation of the scanned object's instructions in a virtual computer environment).

**Enable thorough scanning** In specific situations, such as when you are suspicious of the computer being infected, you may select this option to activate the most thorough scanning algorithms that will scan even those areas of the computer that rarely get infected. Note that this method is time consuming.

**Scan encrypted (TLS and SSL) network traffic** Scan also encrypted network communication, that is, connections over security protocols (SSL and its newer version, TLS). This applies to websites using HTTPS, and email client connections using TLS/SSL. The secured traffic is decrypted, scanned for malware, and encrypted again to be delivered safely to your computer.

**Maximum file size to be scanned by Online Shield** Use the slide bar to specify the maximum size of a file that is still to be scanned. Even if the downloaded file exceeds the limit, and therefore will not be scanned, Resident Shield will still detect it immediately.

- 5 Click **Save** when you are finished with the **Expert Settings** page.
- 6 In the **Threat Notification Mode** area, select one of the following:

---

**Standard pop-up dialog (recommended)** Threat notifications appear as pop up dialogs.

**Tray balloon notification** Threat notifications appear as a balloon message in the system tray.

**Tray icon signalization** Threat notifications appear as an icon in the system tray.

7 Click **Save**.

## Configure Proxy Settings

If you use a proxy server (a kind of buffer between your computer and external networks) to connect to the Internet, and you also want to use a proxy for downloading AVG updates, you will need to specify the settings here.

Select the appropriate option from the drop-down menu on the top of the page, and if you choose to use proxy, enter the details below. Note that if you choose the option 'Try connection using proxy and if it fails, connect directly', the specified proxy settings will be applied, and if unsuccessful, the system will attempt to connect directly.

If the proxy settings script cannot be found on the device, after the attempt to connect fails, the system will attempt to connect directly.

### You can choose either Manual, or Auto completion of proxy settings:

**Manual** In the **Server** box, enter a valid proxy server name or IP address, and in the **Port** box, the port number (the default value 3128 has been pre-set for you).

If the specified proxy server requires authentication, check the Use proxy authentication box and enter a valid User name and a Password.

In the Authentication type drop-down menu, you can either leave the default value or set the preferred protocol: Basic or NTLM (NT LAN Manager, advanced Microsoft authentication protocol).

**Auto** Specify where the proxy details should be acquired:

From script: if you have a script designed to obtain the proxy server address, enter the full path to the script.

Here are some examples of valid formats for specifying the full path:

- **file://localhost/c:/WINDOWS/ProxySettings.txt**
- **file:///c:/WINDOWS/ProxySettings.txt**
- **file://localhost/c:/WINDOWS/ProxySettings.txt**
- **file://\123.123.123.123\share\ProxySettings.txt**

---

**Note:** If the proxy settings script cannot be found on the device, the specified proxy settings will be applied, and if unsuccessful, the system will attempt to connect directly.

## Configure Password Protection Settings

You can set up a password for uninstalling or accessing the AVG AntiVirus client on device. Setting up a password ensures that the device user does not alter or remove the AVG AntiVirus policy settings.

- 1 In the **Password Protection** area, click **Modify**.
- 2 Select any of the following options:
  - **Activate Password Protection for the uninstall of AVG CloudCare client-side components**
  - **Activate Password Protection for the AVG CloudCare AntiVirus endpoint interface**
- 3 In the **Password** and **Confirm Password** boxes, type the password to uninstall or access the AVG AntiVirus client. Passwords must be between 8 and 20 characters.
- 4 Click **Save**.

## Configure Firewall Settings

Use the Firewall settings to determine the level of security against hacking attempts online.

- 1 In the **Firewall** area, click **Modify**.
- 2 Select one of the following options:
  - Automatic Mode (recommended)** Firewall automatically allows or blocks applications depending on their behavior and their membership in the internal database of trusted applications.
  - Interactive Mode** Firewall will ask you to allow or block every application that attempts access.
  - Block Access to Internet** Blocks every attempt to or from the Internet.
  - Turn firewall protection off (not recommended)** Firewall does not protect the computer. All application traffic is allowed.
- 3 Click **Save**.

---

## Configure Scan Settings

The **Scan Settings** allows you to set the parameters for each manual scan type: whole computer, specific files or folders, shell extension, and removable device.

- 1 In the **Scan Settings** area, click **Modify**.

### To configure Whole Computer Scan

The **Whole Computer Scan** tab allows you to edit the parameters of the default scan. This is the scan that is initiated when the device user clicks **Scan Now** from the AVG AntiVirus client, or when you click the **Scan Now** link from the **AntiVirus Device Overview** page in Managed Workplace.

- 1 Click the **Whole Computer Scan** tab.
- 2 Select any of the following:

**Heal/Remove virus infections without asking (You will always be asked for rootkits)** If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be removed to the Virus Vault. You will not receive an alert that a virus has been healed.

**Report potentially unwanted programs or spyware threats** Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended package of spyware: programs that are harmless when acquired from the manufacturer directly but can be misused for malicious purposes later. This is an additional measure that increases the computer's security, however it can possibly block legitimate programs and is therefore not selected by default.

**Scan for tracking cookies** This parameter of the Anti-Spyware component defined that cookies should be detected. HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

**Scan inside archives** This parameter defined that scanning should check all files stored inside archives, e.g. ZIP, RAR.



---

**Use heuristics** Heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning.

**Scan system environment** Scanning will also check the system areas of the computer.

**Enable thorough scanning** If you are suspicious about the computer being infected, you can select this check box to activate the most thorough scanning algorithms which will scan areas of the computer that rarely get infected. Note that this method is time-consuming.

**Scan for rootkits** Scanning will check for rootkits.

**Scan files without extensions** Scanning will check for files without extensions, which are suspicious.

**3** Specify which type of files to scan:

**All file types** Scans all file types, except for the file type that you specify in the **Define excluded extensions** box.

**Selected file types** You can specify that you want to scan only files that are possibly infectable, scan media files, and you can define by extension which files should always be scanned.

**Note:** If you do not scan media files, it will reduce scanning time because video and audio files are often quite large and not likely to be infected by a virus.

**4** In the **Adjust Scanning Speed** section, use the slider to specify the desired scanning speed dependent on system resource usage.

**5** In the **Additional Scan Reports** section, select any of the following:

**Report password-protected archives** Archives (ZIP, RAR etc.) that are protected by password cannot be scanned for viruses.

**Report password-protected documents** Documents protected by password cannot be scanned for viruses.

**Report locked files** Locked files cannot be scanned for viruses.

**Report files containing macros** A macro is a predefined sequence of steps aimed to make certain tasks easier for a user (MS Word macros are widely known). A macro can contain potentially dangerous instructions.

**Report hidden extensions** Hidden extensions can make a suspicious executable file, e.g. "something.txt.exe" appear as a harmless plain text file, e.g. "something.txt". Select this check box to mark these as potentially dangerous.

---

**Note:** Any items of these types that are found will appear in the Virus Vault report categorized as **Information**.

- 6 Click **Save**.

### To configure Specific Files or Folder Scan

Use the **Specific Files or Folder Scan** tab to determine the parameters for when the device user selects the **Scan Specific Files or Folders** option in the AVG AntiVirus client.

- 1 Click the **Specific Files or Folder Scan** tab.
- 2 Select any of the following:

**Heal/Remove virus infections without asking (You will always be asked for rootkits)** If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be removed to the Virus Vault. You will not receive an alert that a virus has been healed.

**Report potentially unwanted programs or spyware threats** Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended package of spyware: programs that are harmless when acquired from the manufacturer directly but can be misused for malicious purposes later. This is an additional measure that increases the computer's security, however it can possibly block legitimate programs and is therefore not selected by default.

**Scan for tracking cookies** This parameter of the Anti-Spyware component defined that cookies should be detected. HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

**Scan inside archives** This parameter defined that scanning should check all files stored inside archives, e.g. ZIP, RAR.

**Use heuristics** Heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning.

**Scan system environment** Scanning will also check the system areas of the computer.

---

**Enable thorough scanning** If you are suspicious about the computer being infected, you can select this check box to activate the most thorough scanning algorithms which will scan areas of the computer that rarely get infected. Note that this method is time-consuming.

**Scan files without extensions** Files without an extension can be suspicious.

- 3 Specify which type of files to scan:

**All file types** Scans all file types, except for the file type that you specify in the **Define excluded extensions** box.

**Selected file types** You can specify that you want to scan only files that are possibly infectable, scan media files, and you can define by extension which files should always be scanned.

**Note:** If you do not scan media files, it will reduce scanning time because video and audio files are often quite large and not likely to be infected by a virus.

- 4 In the **Adjust Scanning Speed** section, use the slider to specify the desired scanning speed dependent on system resource usage.

- 5 In the **Additional Scan Reports** section, select any of the following:

**Report password-protected archives** Archives (ZIP, RAR etc.) that are protected by password cannot be scanned for viruses.

**Report password-protected documents** Documents protected by password cannot be scanned for viruses.

**Report locked files** Locked files cannot be scanned for viruses.

**Report files containing macros** A macro is a predefined sequence of steps aimed to make certain tasks easier for a user (MS Word macros are widely known). A macro can contain potentially dangerous instructions.

**Report hidden extensions** Hidden extensions can make a suspicious executable file, e.g. "something.txt.exe" appear as a harmless plain text file, e.g. "something.txt". Select this check box to mark these as potentially dangerous.

**Note:** Any items of these types that are found will appear in the Virus Vault report categorized as **Information**.

- 6 Click **Save**.

---

## To configure the Shell Extension Scan

Use the **Shell Extension Scan** tab to determine the parameters for when the device user performs a shell extension scan, which is used by right-clicking a file or folder to scan, without having to open AVG AntiVirus.

- 1 Click the **Shell Extension Scan** tab.
- 2 Select any of the following:

**Heal/Remove virus infections without asking (You will always be asked for rootkits)** If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be removed to the Virus Vault. You will not receive an alert that a virus has been healed.

**Report potentially unwanted programs or spyware threats** Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended package of spyware: programs that are harmless when acquired from the manufacturer directly but can be misused for malicious purposes later. This is an additional measure that increases the computer's security, however it can possibly block legitimate programs and is therefore not selected by default.

**Scan for tracking cookies** This parameter of the Anti-Spyware component defined that cookies should be detected. HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

**Scan inside archives** This parameter defined that scanning should check all files stored inside archives, e.g. ZIP, RAR.

**Use heuristics** Heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning.

**Scan system environment** Scanning will also check the system areas of the computer.

**Enable thorough scanning** If you are suspicious about the computer being infected, you can select this check box to activate the most thorough scanning algorithms which will scan areas of the computer that rarely get infected. Note that this method is time-consuming.

---

**Scan files without extensions** Files without extensions can be suspicious.

- 3 Specify which type of files to scan:

**All file types** Scans all file types, except for the file type that you specify in the **Define excluded extensions** box.

**Selected file types** You can specify that you want to scan only files that are possibly infectable, scan media files, and you can define by extension which files should always be scanned.

**Note:** If you do not scan media files, it will reduce scanning time because video and audio files are often quite large and not likely to be infected by a virus.

- 4 In the **Adjust Scanning Speed** section, use the slider to specify the desired scanning speed dependent on system resource usage.

- 5 In the **Additional Scan Reports** section, select any of the following:

**Report password-protected archives** Archives (ZIP, RAR etc.) that are protected by password cannot be scanned for viruses.

**Report password-protected documents** Documents protected by password cannot be scanned for viruses.

**Report locked files** Locked files cannot be scanned for viruses.

**Report files containing macros** A macro is a predefined sequence of steps aimed to make certain tasks easier for a user (MS Word macros are widely known). A macro can contain potentially dangerous instructions.

**Report hidden extensions** Hidden extensions can make a suspicious executable file, e.g. "something.txt.exe" appear as a harmless plain text file, e.g. "something.txt". Select this check box to mark these as potentially dangerous.

**Note:** Any items of these types that are found will appear in the Virus Vault report categorized as **Information**.

- 6 In the **Displaying of scan progress and results** section, specify whether to open AVG AntiVirus to display scan progress when a scan starts, and whether to open AVG AntiVirus when the scan completes to display results. You can also specify to only open AVG AntiVirus if a threat is detected.
- 7 Click **Save**.

---

## To configure the Removable Device Scan

Use the **Removable Device Scan** tab to determine the parameters for when the device user scans a removable device, including USB sticks, memory cards, external hard drives, cameras, etc. All of these devices can be automatically scanned for viruses and malware when they are inserted into the computer.

- 1 Select the **Enable Removable Device Scan** check box.
- 2 Select any of the following:

**Heal/Remove virus infections without asking (You will always be asked for rootkits)** If a virus is identified during scanning it can be healed automatically if a cure is available. If the infected file cannot be healed automatically, the infected object will be removed to the Virus Vault. You will not receive an alert that a virus has been healed.

**Report potentially unwanted programs or spyware threats** Select to activate the Anti-Spyware engine, and scan for spyware as well as for viruses. Spyware represents a questionable malware category: even though it usually represents a security risk, some of these programs can be installed intentionally. We recommend keeping this feature activated as it increases the computer's security.

**Report enhanced set of potentially unwanted programs** Select to detect extended package of spyware: programs that are harmless when acquired from the manufacturer directly but can be misused for malicious purposes later. This is an additional measure that increases the computer's security, however it can possibly block legitimate programs and is therefore not selected by default.

**Scan for tracking cookies** This parameter of the Anti-Spyware component defined that cookies should be detected. HTTP cookies are used for authenticating, tracking, and maintaining specific information about users, such as site preferences or the contents of their electronic shopping carts.

**Scan inside archives** This parameter defined that scanning should check all files stored inside archives, e.g. ZIP, RAR.

**Use heuristics** Heuristic analysis (dynamic emulation of the scanned object's instructions in a virtual computer environment) will be one of the methods used for virus detection during scanning.

**Scan system environment** Scanning will also check the system areas of the computer.

**Enable thorough scanning** If you are suspicious about the computer being infected, you can select this check box to activate the most thorough

---

scanning algorithms which will scan areas of the computer that rarely get infected. Note that this method is time-consuming.

**Scan files without extensions** Files without extensions can be suspicious.

**3** Specify which type of files to scan:

**All file types** Scans all file types, except for the file type that you specify in the **Define excluded extensions** box.

**Selected file types** You can specify that you want to scan only files that are possibly infectable, scan media files, and you can define by extension which files should always be scanned.

**Note:** If you do not scan media files, it will reduce scanning time because video and audio files are often quite large and not likely to be infected by a virus.

**4** In the **Adjust Scanning Speed** section, use the slider to specify the desired scanning speed dependent on system resource usage.

**5** In the **Additional Scan Reports** section, select any of the following:

**Report password-protected archives** Archives (ZIP, RAR etc.) that are protected by password cannot be scanned for viruses.

**Report password-protected documents** Documents protected by password cannot be scanned for viruses.

**Report locked files** Locked files cannot be scanned for viruses.

**Report files containing macros** A macro is a predefined sequence of steps aimed to make certain tasks easier for a user (MS Word macros are widely known). A macro can contain potentially dangerous instructions.

**Report hidden extensions** Hidden extensions can make a suspicious executable file, e.g. "something.txt.exe" appear as a harmless plain text file, e.g. "something.txt". Select this check box to mark these as potentially dangerous.

**Note:** Any items of these types that are found will appear in the Virus Vault report categorized as **Information**.

**6** Click **Save**.

## Configure Schedule Settings

The **AntiVirus Schedules** page allows you to set the schedule for the following events:

**Scheduled Scan** You can configure scheduling options, scan settings, whether to scan the whole computer or specific files or folders.

---

**Definition Update** You can set up detailed parameters of the antivirus definition's update schedule.

**Program Update** You can set up detailed parameters to schedule AVG program fixes and improvements.

### To configure the Scheduled Scan

- 1 In the **Schedule Settings** section, click **Modify**.
- 2 Click the **Scheduled Scan** tab.
- 3 Select the **Enable this task** check box to activate the scheduled scan.
- 4 On the **Schedule** sub-tab, configure the following:
  - In the **Schedule Selection** section, specify whether to schedule scans according to the Execution Schedule set up for AVG AntiVirus. For more information on setting up an execution schedule, see [Setting Up Execution Schedules](#).
  - To override the execution schedule, select the **Override Execution Schedule** option button, and specify the time intervals for the scan schedule. The timing can either be defined by the repeated update launch after a certain period of time (**Run every...**), by defining an exact date and time (**Run at specific times...**), or by computer reboot (**Run on computer startup**).
  - In the **Advanced scheduling options** section, choose whether to run the update on computer startup if the task was missed, and whether to run the scan when the computer is in low-power mode.
- 5 On the **Settings** sub-tab, configure the scan settings. For more information on scan settings see [Configure Scan Settings](#).
- 6 On the **Location** sub-tab, configure the following:
  - To scan the whole computer, select the **Whole computer scan** option button.
  - To scan specific locations of the computer, select the **Scan specific files or folders option** button, and then select the check box for each location you want to scan.
- 7 Click **Save**.

### To configure the Definition Update Schedule

- 1 In the **Schedule Settings** section, click **Modify**.
- 2 Click the **Definition Update Schedule** tab.



- 
- 3 Select the **Enable this task** check box to activate the definition update schedule.
  - 4 Select the **Run automatically** check box to run the definition update schedule automatically.
  - 5 In the **Schedule Selection** section, specify one of the following:
    - Specify whether to schedule definition updates according to the Execution Schedule set up for AVG AntiVirus. For more information on setting up an execution schedule, see [Setting Up Execution Schedules](#).
    - To override the execution schedule, select the **Override Execution Schedule** option button, and specify the time intervals for the definition update schedule. The timing can either be defined by the repeated update launch after a certain period of time (**Run every...**), or by defining an exact date and time (**Run at specific times...**).
    - to define an exact date and time for the schedule, select the Run at specific times option button, and then use the list to select a day and time.
  - 6 In the **Advanced scheduling options** section, choose whether to run the update on computer startup if the task was missed.
  - 7 Click **Save**.

### To configure the Program Update Schedule

- 1 In the **Schedule Settings** section, click **Modify**.
- 2 Click the **Program Update Schedule** tab.
- 3 Select the **Enable this task** check box to activate the program update schedule.
- 4 In the **Schedule Selection** section, specify one of the following:
  - to run the program update schedule using the Execution Schedule for AVG AntiVirus, select the **Run as per applicable Execution Schedule** option button. For more information on execution schedules in Managed Workplace, see [Setting Up Execution Schedules](#).
  - To override the execution schedule, select the **Override Execution Schedule** option button, and specify the time intervals for the program update schedule. The timing can either be defined by the repeated update launch after a certain period of time (**Run every...**), by defining an exact date and time (**Run at specific times...**), or by computer reboot (**Run on computer startup**).
- 5 In the **Advanced scheduling options** section, choose whether to run the update on computer startup if the task was missed.

- 
- 6 Click **Save**.

## Configure Update Settings

You can specify when to update files in cases where the update process requires the computer to restart.

- 1 In the **Update Settings** section, click **Modify**.
- 2 Select one of the following option buttons:
  - **Require confirmation from the user**
  - **Restart immediately**
  - **Complete at next computer restart**
- 3 Click **Save**.

## Configure Exception Settings

Exception settings enable you to define items that AVG will ignore. Typically, you need to define an exception if AVG AntiVirus keeps detecting a program or file as a threat, or blocking a safe website as dangerous. Add such file, folder, or website to this exception list, and AVG will not report or block it anymore.

### Configure Exception Settings for a File

- 1 In the **Exception Settings** section, click **Modify**.
- 2 Click **Add Exception**.
- 3 From the **Exception Type** list, select **File**.
- 4 Click **OK**.
- 5 In the **Enter path to a file** box, enter a full path to the file (for example, "C:\WINDOWS\SERVICING\TRUSTEDINSTALLER.EXE").
- 6 Optionally, select one of the following:
  - Select the **Even when the file is moved to a new location** check box to exclude the file even if it is moved or copied to another location, as long as the file itself doesn't change.
  - Select the **Even when the file has been changed or updated** check box to exclude the file only in this specific location and under its current name, even if its contents are modified.
- 7 Select the check box beside each AntiVirus service that you want to treat the file as an exception.
- 8 Click **Add**.

---

### Configure Exception Settings for a Folder

- 1 In the **Exception Settings** section, click **Modify**.
- 2 Click **Add Exception**.
- 3 From the **Exception Type** list, select **Folder**.
- 4 Click **OK**.
- 5 In the **Enter path to a folder** box (for example, "C:\Users\You\Documents\ Exceptions").
- 6 Click the **Resident Shield** or **Manual and Scheduled Scan** check boxes to specify if the exception should be used by the Resident Shield, during scans, or both.
- 7 Click **Add**.

### Configure Exception Settings for a URL

- 1 In the **Exception Settings** section, click **Modify**.
- 2 Click **Add Exception**.
- 3 From the **Exception Type** list, select **URL**.
- 4 Click **OK**.
- 5 Enter the web address that you want to exclude from AntiVirus protection. Allowed web address protocols include http, https, ftp, www, and IP addresses. You can also specify a web address without the protocol, for example "google.com", however you must include the domain suffix, for example .com or .ca.  
**Note:** Wildcards are not supported.
- 6 Select the **Online Shield** check box if you want the Online Shield to treat this URL as an exception.
- 7 Click **Add**.

## Removing an AntiVirus Policy

When you remove an AntiVirus policy, any devices that were managed using that policy go into an unmanaged state, which means that AntiVirus is still installed on the device, but it does not receive any management commands or policy updates from the Onsite Manager. For example, changes to the policy settings will not be applied to the device, and clicking **Scan Now** will fail.

---

If you remove an AntiVirus policy that is applied to devices, you should either first uninstall AntiVirus from that device, or apply a different AntiVirus policy to the device.

- 1 Click **Configuration > Policies > AVG AntiVirus**.
- 2 Select the check box beside the AntiVirus policy you want to remove.
- 3 Click **Delete**.

## Setting up AVG AntiVirus Monitoring

After you have set up your AntiVirus policies, you must set up monitoring for Managed Workplace to begin collecting and alerting on your AVG AntiVirus environments.

Managed Workplace includes a monitoring policy called "AVG Managed Workplace AntiVirus" that includes the following monitors:

- AVG AntiVirus - Device Needs Restart
- AVG AntiVirus - Protection Disabled
- AVG AntiVirus - Threat Detected
- AVG AntiVirus - Virus Definition Out-Of-Date
- AVG AntiVirus - Virus Scan Overdue

You can add this monitoring policy to a service in a service plan, which is then applied to a site or group. As a best practice, it is recommended that you include this monitoring policy in the same service that also includes the AntiVirus policies you have set up. For information on adding a policy to a service, see [Creating Services](#).

## Managing AVG AntiVirus in Managed Workplace

After you have set up your AntiVirus policies, you are ready to begin deploying and managing AVG AntiVirus at your customer sites. This section covers how you can implement, monitor, and maintain AVG AntiVirus in Managed Workplace.

AVG AntiVirus in Managed Workplace includes 3 dashboards that each provide unique views of AVG AntiVirus deployment and status - a multi-site overview dashboard, a site-level dashboard, and a device-level dashboard.

---

## AVG AntiVirus Overview Dashboard

The AVG AntiVirus Overview dashboard provides an aggregated look at the number of active AntiVirus alerts, and deployment and license summaries for AVG AntiVirus across all sites.

From the AVG AntiVirus Overview dashboard, you can:

- view a list of all AntiVirus alerts, or view AntiVirus alerts by category,
- drill down to view sites configured with AntiVirus and sites not configured with AntiVirus
- access the AVG AntiVirus support and forum websites
- view a chart depicting AVG AntiVirus license use across all sites.

**Note:** There can be a delay of up to 24 hours after the initial AV deployment for the charts on the AVG AntiVirus dashboard to display information.

### To view the AVG AntiVirus Overview dashboard

- In Service Center, click **AVG AntiVirus**.

## AVG AntiVirus Site Dashboard

The AVG AntiVirus site dashboard provides a more detailed alert and deployment summary for a site with devices with AVG AntiVirus installed.

From the AVG AntiVirus Site Dashboard, you can:

- view a list of all AntiVirus alerts at the site, or view AntiVirus alerts by category,
- drill down to view devices with AntiVirus installed and devices needing AntiVirus installation,
- scan all devices at the site,
- update the virus definitions for all devices at the site.

### To view the AVG AntiVirus Site dashboard

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 Click the name of a site.

---

## AVG AntiVirus Device Dashboard

The AVG AntiVirus device dashboard includes details about the AntiVirus components installed on the device, a configuration summary, details about the client version, and links to scan the device and update virus definitions.

From the AVG AntiVirus Device Dashboard, you can:

- view Protection Summary information, including the AntiVirus client and database versions, time stamp of last virus definition update, and results from the last scan
- view Configuration Policy Summary information, which indicates which AntiVirus policy settings are enabled
- scan the device
- update the virus definitions
- enable or disable AntiVirus on the device.

### To view the AVG AntiVirus device dashboard

There are many ways that you can drill down to the AVG AntiVirus device dashboard. The AVG AntiVirus Overview screens are designed to allow you drill down to view devices with AntiVirus alerts, devices that require AntiVirus to be installed, etc. The following procedure is just one way you can access the AVG AntiVirus device dashboard.

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 Click a number in the **Devices with AntiVirus** column.
- 4 Click the name of a device.

**Tip:** If AntiVirus is installed on a device, you can access the AVG AntiVirus device dashboard from the Device Overview page, by clicking **AVG AntiVirus** in the Summary sidebar.

## Managing AVG AntiVirus Deployment

There are several ways that you can manage the deployment of AVG AntiVirus at your customer sites:

- view a list of devices that require AntiVirus installation, and install directly on those devices
- enabling and disabling AntiVirus on devices

- uninstalling AntiVirus from devices you no longer want to monitor
- keep track of available AntiVirus licenses.

## About Installing AntiVirus on Devices

The following table shows the various configurations possible for installing AVG AntiVirus on devices:

<b>Automatic Application Rules or Manually Applied to Groups and Devices</b>	<b>Allow me to initiate the install selected</b>	<b>Result</b>
Automatic	Yes	The configuration policy is automatically pushed out to devices that match the automatic application rules. You must then manually install AntiVirus. See <a href="#">Initiating the Installation of AntiVirus on Devices</a> .
Automatic	No	AntiVirus is automatically installed on devices that match the automatic application rules. As new devices are discovered that match the automatic application rules, AntiVirus is automatically installed.
Manual	Yes	The configuration policy is pushed out to the devices you selected when setting up the configuration policy. You must then manually install AntiVirus on these devices. See <a href="#">Initiating the Installation of AntiVirus on Devices</a> .

---

<b>Automatic Application Rules or Manually Applied to Groups and Devices</b>	<b>Allow me to initiate the install selected</b>	<b>Result</b>
Manual	No	AntiVirus is installed on the devices you selected when setting up the configuration policy. If you update the configuration policy settings to add more devices, AntiVirus is automatically installed on these devices.

---

### Initiating the Installation of AntiVirus on Devices

You can view a list of devices that need AntiVirus installed, which means that you have installed an AntiVirus policy on the device, but you have chosen to initiate the installation manually. This list also displays devices in which a previous attempt to install, whether manually or automatically, has failed.

**Note:** AntiVirus does not support cloning devices. If you are going to clone the device, install AntiVirus after cloning.

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 In the **Devices Needing AntiVirus Installation** column, click a number to view a list of devices requiring AntiVirus at that site.
- 4 Select the check box beside a device, and then click **Install**.

**Note:** The **Devices Missing an AntiVirus Policy** column displays a count of all Windows devices for that site that don't have an AntiVirus policy applied. Note that this device count only includes devices on which Managed Workplace AVG AntiVirus is installed; not devices on which CloudCare AntiVirus is installed.

### Managing AntiVirus on Device Managers

When you install Device Manager, the AntiVirus client is included as part of the installation package. However, AntiVirus is not activated until you apply a configuration policy to the Device Manager that determines which components to install, which scan settings to apply, etc.

You apply configuration policies to a Device Manager the same way you would to other devices, either by manually selecting the device, or creating automatic



---

application rules that include the device. See [Manually Applying an AntiVirus Policy to Devices and Groups](#) and [Creating Rules to Automatically Apply an AntiVirus Policy](#).

**Note:** If you have not updated a Device Manager to Managed Workplace 9.0, you will not be able to apply a configuration policy. See [Updating Device Managers](#).

## Enabling and Disabling AntiVirus

After you have installed AVG AntiVirus on a device, you must enable it to begin monitoring with AV. You can also disable AntiVirus on a device you no longer want to monitor.

### Enabling or Disabling AntiVirus on a device

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Alert Summary** area, click the number beside **Sites with active "antivirus disabled" alerts**.
- 3 Click the name of a device.
- 4 In the sidebar, click **AVG AntiVirus**.
- 5 In the **Management** area, click one of the following:
  - **Enable AntiVirus**
  - **Disable AntiVirus**

**Note:** If AntiVirus is enabled on a device, only the **Disable AntiVirus** link is visible, and vice versa.

### Updating the AntiVirus Client on a Device

You can update the AVG AntiVirus client on devices, which updates virus definitions and may contain program changes and improvements, new features, language files, etc.

**Tip:** You can also update the AVG AntiVirus client on devices by going to **Update Center > Products**, clicking **Advanced Options**, and then selecting the **Update AVG AntiVirus** clients for selected sites check box.

**Note:** As long as the device has an Internet connection, the AVG AntiVirus client updates automatically on a daily basis, so typically a manual update is not required. You may want to update manually if you suspect that the device does not have the latest updates installed.

- 1 In Service Center, click **AVG AntiVirus**.

- 
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
  - 3 In the **Devices with AntiVirus** column, click the device number for the site for which you want to update AntiVirus clients.
  - 4 Select the check box beside each device that you want to update.
  - 5 Click **Update**.

### **Uninstalling AntiVirus from a Device**

You can uninstall AVG AntiVirus from a device from within Managed Workplace.

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 In the **Devices with AntiVirus** column, click a number for the site that contains devices from which you want to uninstall AntiVirus.
- 4 Select the check box beside each device from which you want to uninstall AntiVirus.
- 5 Click **Uninstall**.

### **Keeping Track of AVG AntiVirus Licenses**

The AVG AntiVirus multi-site page includes a pie chart that displays the number of seats you are using versus the number of seats that you are entitled to.

- In Service Center, click **AVG AntiVirus**.

The **License Summary** area displays the pie chart of seats in use versus available seats.

## **Managing AntiVirus Alerts**

You can view and take action on AVG AntiVirus alerts at the multi-site, site, and device level. The AVG AntiVirus Overview screens are designed so that you can view alerts by category, or view all alerts at the multi-site, site, or device level. You can then take action on individual alerts by creating tickets, viewing and modifying the monitoring configuration, and clearing or suppressing the alert.

---

## Viewing AntiVirus Alerts by Category

Both the multi-site and site page views include an Alert Summary section where you can view AntiVirus alerts in the following categories:

- threats detected
- virus definition out of date
- antivirus disabled
- virus scan overdue
- restart required

## Viewing All AntiVirus Alerts

Each AVG AntiVirus page also includes an Active Alerts link at the top that you can click to view a list of all alerts across all sites, at that site, or for that device.

## Managing AntiVirus Alerts

- 1 In Service Center, click **AVG AntiVirus**.
- 2 Do one of the following:
  - In the **Alert Summary** section, click the number beside the alert category you want to view.
  - Click the **Active Alerts** link at the top of the page.
- 3 Address the alert in one of the following ways:
  - To view the site-level AVG AntiVirus dashboard, click the link in the **site** column.
  - To view the device-level AVG AntiVirus dashboard, click the link in the **Device/Website** column.
  - To view and potentially modify the alert configuration, click the link in the **Alert Configuration** column.
  - To create a trouble ticket to take action on the alert, click the **Create Ticket** link.
  - To clear an alert, select the check box beside the alert, and then click **Clear**. For more information about clearing alerts, see [Clearing Alerts](#).
  - To clear all alerts, click **Clear All**.
  - To suppress an alert, select the check box beside the alert, and then click **Suppress**. For more information about alert suppression, see [Suppressing an Alert](#).

---

## Keeping Devices Secure

AVG AntiVirus in Managed Workplace allows you to perform the following functions to keep devices secure:

- Perform an on-demand whole computer scan on a device, without having to wait for a regularly-scheduled scan. You can also scan all devices at a site.
- Update virus definitions on a device or all devices at a site. The AVG database of known viruses is stored in the device on a local disk so that AVG can use it at any time to detect known viruses. When a new virus threat is analyzed, a definition of it is created and is added to the database when you update virus definitions.

### Scanning a Device

Typically, you would scan a device when you suspect that it has been infected, or after you have updated the virus definitions. You can scan a device directly on the AVG AntiVirus device page.

- 1 Do one of the following:
  - On the multi-site page, in the **Alert Summary** area, click the number beside **Sites with virus scan overdue**.
  - On the site page, in the **Alert Summary** area, click the number beside **Devices with virus scan overdue**.
- 2 Click the name of a device to open the device level page.
- 3 In the **Management** area, click **Scan Now**.
- 4 When the scan begins, a message will display at the top of the page stating "The requested action was queued successfully". Click the red **X** to close this message.

### Scanning All Devices at a Site

You can initiate a scan on all devices at a site.

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 Click the name of a site.
- 4 In the **Management** area, click **Scan Now**.

- 
- 5 When the scan begins, a message will display at the top of the page stating “The requested action was queued successfully”. Click the red **X** to close this message.

### Updating Virus Definitions on a Device

You can quickly search for and act upon devices that have out of date virus definitions.

- 1 Do one of the following:
  - On the multi-site page, in the **Alert Summary** area, click the number beside **Sites with virus definition out of date**.
  - On the site page, in the **Alert Summary** area, click the number beside **Devices with virus definition out of date**.
- 2 Click the name of a device to open the device level page.
- 3 In the Management area, click **Update Virus Definitions**.
- 4 When the update begins, a message will display at the top of the page stating “The requested action was queued successfully”. Click the red **X** to close this message.

### Updating Virus Definitions at a Site

You can update virus definitions on all devices with AntiVirus installed at a site.

- 1 In Service Center, click **AVG AntiVirus**.
- 2 In the **Deployment Summary** area, click the number beside **Sites configured with AntiVirus**.
- 3 Click the name of a site.
- 4 In the **Management** area, click **Update Virus Definitions**.
- 5 When the update begins, a message will display at the top of the page stating “The requested action was queued successfully”. Click the red **X** to close this message.



# CHAPTER 14

## REPORTING

---

*This section provides detailed information about the following topics:*

- *Reports*
  - *Creating a Report*
  - *Previewing a Report*
  - *Managing Reports*
  - *Organizing Reports into Categories*
  - *Scheduling a Report*
  - *Working with Archived Reports*
-

---

# Reports

## About Reports

Delivering quality reports to customers is a key part of your service. Showing customers the value you provide through reports is essential to prove the worth of your business. They also help sell your services to potential customers.

Managed Workplace comes with many site and device reports that are ready to use. For example, here are some popular reports:

**Executive Summary Report** Shows an overview of a site across Windows servers and workstations and includes a network health score, top problem devices, alert summary, and work completed among other things.

**Windows Server Health** Shows descriptive information about a Windows server as well as its availability, disk space used, and various other performance counters for a specified time period. You must have active monitoring in place.

**Work Completed Summary** Shows the work (tickets closed, scripts executed, alerts cleared, and remote repairs) that has been performed on a site.

**Note:** If you're running Managed Workplace on Asian systems and reporting in Asian characters, you need to be running SQL 2008.

### What You Can Do

You can

- create your own user-defined reports for your own needs
- filter the data you see in a report for a specific time period
- organize your reports into categories
- brand reports with your own logo
- automatically email scheduled reports to staff and customers
- install new reports and updates to existing reports
- export reports to a variety of formats including PDF, HTML and Microsoft Excel

The Reports window lists all the reports that have been imported from the Managed Workplace library. You can import more reports that you use frequently or install reports from the Update Center. You can also create new reports or modify existing reports.



---

## Report Types

There are two types of reports in Managed Workplace:

**Site Reports** Provides information about a site.

**Device Reports** Provides information about devices at a site.

In addition to these reports, there are also patch management reports that are generated within Service Center for viewing, but they cannot be exported.

## Predefined Reports

A number of useful predefined reports come with Managed Workplace. Predefined reports cannot be modified.

When you generate a report, either from a delivery schedule or manually as a preview, you must provide a time frame. However, some reports function by taking a snapshot of the information currently in the database, where timestamps are not recorded.

For example, anything that generates graphs will have the data tracked with time stamps. This includes network services, performance counter data, and summary counts of events or alerts.

But asset information for a device's hardware or software is not tracked with timestamps. Nor is information about the Service Center's monitoring configurations.

## Predefined Aggregate Reports

Several predefined aggregate reports come with Managed Workplace. Aggregate reports are multi-site or multi-Onsite Manager reports.

Use aggregate reports to monitor information from several sites in one report. For example, if your client has more than one Onsite Manager and you want to deliver one report covering all Onsite Managers versus separate reports for each Onsite Manager.

## User-Defined Reports

You can create several reports for your own use. You can include a variety of report sections in your report and customize it just the way you need.

---

## Creating a Report

### About Creating a Report

When creating reports, you should only request the data that is relevant to the report's intended audience. The more items chosen from the report options for a report, the longer it will take to generate the report. This is especially true when reporting on patch management items, where there are many filtering options and patches, performance can be less than optimal depending on how much data is being parsed.

#### Questions to Consider Before Creating a Report

Do you want to report on specific devices or a site?

Do you want to brand the report by including a logo on the front page?

What information do you want in your report?

Do you want the report to include which device is getting the most alerts?

#### Tips for Creating a Report

Creating a report using the Report Builder is an iterative process.

- Know what you want to include in the report.
- Figure out which section in the report builder it exists in. The available sections are different for site and device reports. Explore the results of including data from each section so that you can decide what information you want presented in your report.
- To select a different report section, click the underlined text and then select the check box.
- Use the **Preview** to double-check the results. Note that once you click Preview for a report, you can filter it and then click Preview again to view the report.

#### Overview of Report Sections

When creating a report, you select any of the following sections to include:

**Alerts** This section displays a summary of alerting activity at the site or device, including but not limited to the top alert categories generated, alert resolution time, and the option to include suppressed alerts.

**Note:** Alerts that self-heal are not included in reports; reports will show active alerts only.

---

**Asset Baseline (for site reports)** Displays device information for device types that you specify, which can be Windows, OS X, iOS, Android, printers, Linux, and other devices. You can also apply filters to all device types, including warranty expiry date, device end-of-life date, and discover date within the reporting period.

**Asset Inventory (for device reports)** Displays both hardware and software asset information about a device, including specifications, attributes, and a list of services running on the device. You can report on asset inventory for both Windows and non-Windows devices.

**Automation Details** Displays details for task outcomes, which you can filter to include successful executions, script errors, delivery or system errors, and skipped tasks. You can also choose to show only the most recent task results for recurring tasks.

**Automation Summary** Displays a summary of results for tasks based on recurrence type, including one time executions, and daily, weekly, and monthly executions.

**Device Attributes (for site reports)** Displays warranty expiry, end-of-life, and inventory and asset tag information for devices at a site.

**Hardware Assets (for site reports)** Displays a summary of hardware assets, including devices by type, processors, physical memory, and physical and logical disks. Also displays inventory information, including monitors, network cards, sound cards, video cards, and more. You can choose to display inventory information for both Windows and OS X devices.

**Network Statistics** Includes information on device availability, including device availability by date, bandwidth statistics, total uptime and downtime, and network services availability.

**Patch Management** Displays patch management summary information at a site or device. For site reports, this section displays a count of patches by status, and summaries of device status and patch status. For device reports, this section displays summary information of patches applied to the device.

**Performance** For site reports, this section displays top devices by CPU utilization, memory available, and used hard drive space. For device reports, this section displays information about each performance counter being monitored on the device. You can also choose to filter the results to only list selected counters.

**Remote Control** For site reports, this section displays remote control summaries, including session summaries, total session time and count, and remote session details. For device reports, shows a list of remote sessions, including who initiated the session, the protocol, the client, and start and end times.

---

**Security (for site reports)** Displays MBSA security scan results for the site, grouped by grade.

**SNMP** For site reports, lists the top devices by the SNMP OID that you specify. Also displays the top SNMP trap messages. For device reports, displays a list of SNMP OIDS, which you can optionally filter to show only certain OIDs.

**Software Assets (for site reports)** Displays inventory information for operating systems, including Windows, OS X, and iOS and Android devices. Also displays installed software inventory, and software details by device. For software inventory, you can display both Windows and non-Windows software.

**Trouble Tickets** For site reports, displays graphs to show trouble ticket summaries by user, trouble ticket resolution times, and trouble ticket trends. Also displays more detailed trouble ticket summaries, allowing you to filter by assignee, priority, and status. For device reports, displays the trouble tickets that were created for the device.

**Windows Events Summary** For site reports, displays two tables: a summary table of top events, organized by event log and severity, and a table of devices that generated the highest number of events, based on a single user-defined filter. For each event, displays the event ID, severity, timestamp of first occurrence, timestamp of last occurrence, sample description, and total count is listed. For device reports, displays a table that summarizes events generated by the device. Displays event ID, severity, timestamp of first occurrence, sample description, and total count for each event.

**Windows Events Details** Displays Windows Events returned by up to 10 user-defined filters that search the Windows Events Logs by event source, including or excluding events according to their event IDs, or filtering by event severity. Users can assign a highlight color and precedence, which is displayed in tables, along with each event's ID, source, log, severity, time of event, and description. For site reports, a table of events is displayed by site. For device reports, a table of events is displayed by device. Both site and device reports include a pie chart of results selected by choosing a highlight color and precedence. Events that do not have a defined highlight color are not included in the pie chart, but still appear in tables. If an event is returned by two different filters, it is included in the filter with the highest precedence. Both site and device reports are limited to a maximum of 10,000 events. If the report executes against multiple devices, the limit of 10,000 events is divided equally between each device's Windows Event Details section. For example, if a report is run against 500 devices, each device's table displays a maximum of 20 entries.

**Aggregate Site Device List** For site reports, displays a count of devices. Counted devices include:

- Total devices

- 
- Total servers
  - Total workstations
  - Total printers
  - Total mobile devices
  - Total network devices (Devices not classified as other hardware types)
  - Total devices with AVG Antivirus installed (Does not include devices using AVG CloudCare)

## Creating a Report

If you are familiar with SQL Reporting Services, you can create custom reports against the Service Center database, but any new reports that you create cannot be imported into Service Center. You can use the predefined report files (.RDL) as a starting point, but you should not import it into Service Center after you've modified it.

If you are using an image file as a logo on the front page of the report, note the following:

- Managed Workplace supports .GIF, .JPG, .JPEG and .PNG formats.
- The image size must be 660 x 276 pixels for the logo to appear correctly.
- For an Executive Summary report, the image size must be 276 x 96 for the logo to appear correctly.
- If the image file has smaller dimensions than those recommended above, the image will be centered on the report.
- If the image file is larger, it will be shrunk to fit and may have a fuzzy appearance.

- 1 In Service Center, click **Reporting > Reports**.
- 2 Click **Create**.
- 3 In the **Properties** tab, type a name for the report.
- 4 Select a category for the report from the **Category** list.
- 5 Optionally, type a description for the report.  
The description appears in Service Center, not in the report.
- 6 Select either the **Site** or **Device** option button to define the type of report.
- 7 In the **Logo** section, do one of the following:
  - To not include a logo, select **No Image**.

- 
- To use an existing image as a logo on the front page, select **Existing Image** and select one from the list.
  - To use a new image as a logo on the front page, select **New Image** and click **Browse** to locate the file.
- 8 Click the **Content** tab.
  - 9 In the **Report Sections** area, select the check boxes that correspond with the sections you want to include in the report.
  - 10 For each selected section, select the check boxes that correspond with the desired section content. (This is on the right side of the window.)
  - 11 Click **Save**.

## Exporting Managed Workplace Screens to a File

In addition to creating reports using the Report Builder, you can also generate an on-the-fly report that leverages the filtering and data selection abilities inherent in commonly-used UI pages in Managed Workplace, including:

- Alerts Page
- Onboarding Overview dashboards
- Ticket Management
- Windows, SNMP, and Mobile Inventory

This type of reporting allows you to generate Excel, CSV, Word, and PDF files that replicates the information you are viewing. For example, on the Alerts page, you can filter to only show active alerts at a particular site, and then export to an Excel file that you can then use for reporting purposes. Similarly, in the Onboarding Overview dashboard, you can filter the view to only display devices with onboarding issues at a certain site, and then export that content to a Excel file that serves as a report that shows your customer a list of the devices that you will be troubleshooting.

- 1 In Service Center, access any of the following pages:
  - Alerts (**Status > Alerts**)
  - Onboarding Overview (**Status > Onboarding Overview**)
  - Ticket Management (**Trouble Tickets > Ticket Management**)
  - any Inventory page (**Site Management > Windows Inventory**, **Site Management > SNMP Inventory**, or **Site Management > Mobile Inventory**)
- 2 Click **Export**, and then select one of the following:

- 
- Excel
  - CSV
  - Word
  - PDF

**Notes:**

- The type of file format available for export varies.
- For more information about the limitations of exporting to various file types, see [https://technet.microsoft.com/en-us/library/ms157153\(v=sql.100\).aspx](https://technet.microsoft.com/en-us/library/ms157153(v=sql.100).aspx).

## Copying a Report

You can copy a report when you want to create a new report that is very similar to an existing one. When you copy a report, you are prompted to provide a new name and save it. Copied reports are automatically saved in the same report category as the original report, however report customizations are not copied. You can then make any necessary changes to the configuration of the report.

**Note:** When you update an original report, the copied report is also updated. For more information, see [Updating a Report](#).

- 1 In Service Center, click **Reporting > Reports**.
- 2 Locate the report you want to copy.
- 3 Select the check box beside the report.
- 4 Click **Copy**.
- 5 In the **Name** box, type a name for the report.
- 6 Click **Save**.

## Previewing a Report

### Previewing a Report

**To preview a report**

- 1 In Service Center, click **Reporting > Reports**.
  - To view the reports with a folder view, ensure the **Grouped** check box is selected.

- 
- To view a list of reports, clear the **Grouped** check box.
- 2 Locate the report you want to preview.
  - 3 Click **Preview**.
  - 4 In the **Report Viewer** window, filter the report as desired and click **Preview**.

### To export a previewed report

- 1 Preview a report. See [Previewing a Report](#).
- 2 In the **Report Viewer** window, select one of the following output formats for the report:
  - Portable Document Format (PDF)
  - Web Archive (MHTML)
  - Excel Workbook (XLS)
  - TIFF
  - XML
  - CSV
  - Word
- 3 Click **Export > Open** or **Save** depending on your preference.

**Note:** For more information about the limitations of exporting to various file types, see [https://technet.microsoft.com/en-us/library/ms157153\(v=sql.100\).aspx](https://technet.microsoft.com/en-us/library/ms157153(v=sql.100).aspx).

### To refresh a previewed report

- 1 Preview a report. See [Previewing a Report](#).
- 2 In the **Report Viewer** window, click the **Refresh** icon.



Refresh icon

### To print a previewed report

- 1 Preview a report. See [Previewing a Report](#).
- 2 In the **Report Viewer** window, click the **Print** icon.



---

## Viewing a Report that Shows Information from More than One Onsite Manager or Site

Several predefined aggregate reports come with Managed Workplace. Aggregate reports are multi-site or multi-Onsite Manager reports.

Use aggregate reports to monitor information from several sites in one report. For example, if your client has more than one Onsite Manager and you want to deliver one report covering all Onsite Managers versus separate reports for each Onsite Manager.

### To use predefined aggregate reports

- 1 Install a predefined aggregate report from Update Center. See [Installing a Report](#).
- 2 Click the name of the aggregate report to open the Report Builder.
- 3 In the **Name** box, type a unique name that identifies this report for your customer.
- 4 Click the **Content** tab.
- 5 Select the check boxes beside the sites to include in the report.
- 6 Select the Company Information to display on the cover page.
- 7 Click **Save**.

### To view the predefined aggregate report

- 1 In Service Center, click **Reporting > Reports**.
- 2 Locate the aggregate report you want to preview.
- 3 Click **Preview**.
- 4 In the **Report Viewer** window, filter the report as desired and click **Preview**.

## Creating Report Policies

A report policy includes the following:

- one or more reports
- the schedule on which the reports will run
- the intended report email recipients, and the email subject and message
- formatting options such as locale, time zone, output format, and font

- 
- for device report policies, the rules that define what type of devices will be included in the reports
  - manually added devices and groups

When you create a report policy, you specify whether it will include site reports or device reports. For report policies that include site reports, when the policy is added to a service in a service plan and applied to a site, the policy will be automatically applied to all devices at a site. For this reason, you cannot create automatic inclusion rules for a report policy that includes site reports.

### To create a report policy

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Click **New**.
- 3 From the list, select whether to create a site report or a device report.
- 4 Click **Add**.
- 5 Provide a policy name and description.
- 6 Click **Create**.
- 7 Click the **Settings** tab.
- 8 Click **Modify**.

### To add reports to a report policy

- 1 In the **Reports** area, click **Add**.
- 2 Select the check box beside each report you want to add, and click **Add**.

### To schedule when the reports will run

- 1 In the **Schedule** area, in the **Start Time** box, type a start time for when reporting will begin to run. Alternatively, you can click the clock icon to select a time from the list.
- 2 In the **Recurrence Pattern** area, select whether you want reporting to run daily, weekly, monthly, or quarterly.
- 3 In the **Select the number of days of data to run in the report** area, indicate the time period the report will cover by selecting a number from the first list, and either **days**, **weeks**, or **months** from the second list.

### To configure email settings

You can configure whether to email reports to a site's contact, and you can provide the subject line and email message content.

---

**Note:** The report policy will use the site contact's email address as defined in Site Management. To verify that a site has an email contact, go to **Site Management > Sites**, and click the site name. On the **General** tab, in the **Site Details** section, click **Modify** to add an email address if one does not already exist.

- 1 In the **Email** area, click the **Email Reports to the site's contact** check box. This check box is selected by default.
- 2 In the **Subject** box, type the subject line. By default, the **Subject** box is populated with the name of the report policy. You can change this if desired.
- 3 In the **Message** box, type the email message.

### To set formatting and regional options

You can set formatting and regional options such as locale, time zone, font, and output file.

- 1 In the **Options** area, select one of the following output formats for the report:

**Portable Document Format (PDF)** This format becomes an attachment in an email.

**Web Archive (MHTML)** This format embeds right into an email. This web page archive format combines resources that are typically represented by external links (such as images, Flash animations, Java applets, audio files) together with HTML code into a single file.

**Excel Workbook (XLS)** This format becomes an attachment in an email. This format is useful if you want to edit or manipulate the data in Excel.

**TIFF** This format becomes an attachment in an email.

**XML** This format becomes an attachment in an email. Saving the report in XML format allows you to import the report data into another system. For example, if you have developed a web portal that clients can log into and view information about their company such as reports, performance statistics, etc. XML is a clean way of exporting and importing data from one system to another.

**CSV** This format becomes an attachment in an email. This format can be loaded into any spreadsheet program. You can also use .CSV files to import the data into another system.

**Microsoft Office Word** This format becomes an attachment in an email. This format can be loaded into Microsoft Word.

- 2 If required, select the time zone and locale for the report policy.

---

For example, if you are creating a report policy that will be applied to customers in a different time zone or locale, select their time zone and locale.

- 3 From the **Font** list, select the font you want the report to use.
- 4 Click **Save**.

## Applying Report Policies

### Creating Rules to Automatically Include Devices

Automatic approval rules determine which devices are eligible to have the reporting policy applied. For example, if you are creating a reporting policy for Windows servers only, you can set up an automatic approval rule to include devices with the word “server” in the OS name.

The approval rules do not come into effect until the reporting policy has been applied, either by adding it to a service and then applying the service to a group or site, or by adding it to a service in a service plan, which can also be applied to a group or site.

The process for setting up approval rules is the same for reporting policies as it is for all other policy types (i.e, monitoring, patch, and AVG AntiVirus). For more detailed instructions on setting up automatic approval rules, including examples, see [Creating Automatic Inclusion Rules for a Monitoring Policy](#).

**Note:** You can only set automatic inclusion rules for report policies that include device reports; report policies with site reports will automatically report on all devices at a site.

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Click the name of the report policy to which you want to create an automatic inclusion rule.
- 3 Click the **Automatic Application** tab.
- 4 Create the automatic inclusion rule by clicking **Add** to create a rule.
- 5 Repeat step 4 until the rule is complete.
- 6 Click **Save**.

### Adding Devices or Groups to an Report Policy

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Click the name of the report policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.

- 
- 4 Do one of the following to apply the report policy to a group or device:
    - In the **Applied Groups** area, click **Add**. Filter on the Group Type, if desired. Click the group and click **OK**.
    - In the **Applied Devices** area, click **Add**. Filter the list of devices. Select the check box beside the device and click **OK**.

**Note:** You can view the report policies applied to service and site groups on the **Groups** page, by going to **Configuration > Groups**, clicking the group name, and then clicking the **Policies** tab. For more information, see [Viewing the Policies Applied to a Group](#).

### Removing Devices or Groups from a Report Policy

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Click the name of the report policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following:
  - To select one device or group at a time, select the check box that corresponds with each device you want to remove.
  - To select all the devices or groups at once, select the check box at the top of the column.
- 5 Click **Remove**.

### Renaming a Report Policy

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Click the name of the report policy that you want to edit.
- 3 Click **Modify**.
- 4 Type a new name in the **Policy Name** box.
- 5 Click **Save**.

### Deleting a Report Policy

When you delete a report policy, the reports in the policy will no longer report on devices that have the policy applied.

- 1 In Service Center, click **Configuration > Policies > Reporting**.
- 2 Select the check box beside the report policy you want to delete.
- 3 Click **Delete**.

---

## Viewing Report Policy Execution Results

The **Report Policy Execution History** page provides a summary of successful and failed reports from the report policies that you have applied. You can filter the results by service plan, site, report status (i.e. succeeded or failed), and time period.

Reports are grouped into report category, i.e. **Network Audit Reporting** or **Windows Patch Reporting**. You can expand the groups by clicking the chevron beside each group to view the reports within.

### To view report policy execution results

- 1 In Service Center, click **Status > Report Policies**.
- 2 Filter the results by selecting a service plan, site, status, and time period from the lists, and click **Filter**.

### To run a report

- 1 In Service Center, click **Status > Report Policies**.
- 2 Click the chevrons to expand
- 3 Click the check box beside the report you want to run. You can select one report at a time.
- 4 Click **Run Now**.

## Managing Reports

### Viewing a List of the Predefined Reports

- 1 In Service Center, click **Reporting > Reports**.
- 2 Do one of the following:
  - To view the reports with a folder view, ensure the **Grouped** check box is selected. Use the chevron (>) to open a folder.
  - To view a list of reports, clear the **Grouped** check box.

### Changing the Report Category for a Report

- 1 In Service Center, click **Reporting > Reports**.
- 2 Locate the report for which you want to change the report category.
- 3 Click the name of the report.

- 
- 4 From the **Category** list, select a different report category.
  - 5 Click **Save**.

## Installing a Report

A large default set of reports are included in Service Center. You can install a new report by going to Update Center and selecting a report from the list of new reports available for install. This list is updated periodically as new reports are released by AVG.

When a new report is available, a green icon appears beside **Update Center > Components** in the navigation pane to indicate that there is a new component available for install.

**Note:** After installing a report from Update Center, it is no longer available for installation. However, you can copy an installed report and customize it, and the original report will still be available in Reporting > Reports to create additional copies, if required. See [Copying a Report](#).

- 1 In Service Center, click **Reporting > Reports**.
- 2 Click **Get More**.

The **Components** page opens with a list of reports available for installation.

- 3 Select the check box beside each report you want to install.
- 4 Click **Install**.

When the report has installed, it is removed from the available reports list in Update Center, and appears in the Reports list (**Reporting > Reports**), under the **Uncategorized** category.

### See Also

[Updating and Installing Service Center Components](#)

## Importing a Report

You can import a report into Service Center by importing a Report Package file (.LPIR). The imported report is then available in the list of reports on the Reports page.

- 1 In Service Center, click **Reporting > Reports**.
- 2 Click **Import**.
- 3 Click **Browse** and locate the Report Package file (.LPIR) to import.
- 4 Click **Open**.

- 
- 5 Click **Import**.

### See Also

[Installing a Report](#)

## Updating a Report

You can update a report in Service Center by installing an update from Update Center. Report updates are created periodically by AVG and added directly to Update Center for you to install.

When an report update is available, a green icon appears beside **Update Center > Components** in the navigation pane to indicate that there is a new component available for upgrade.

- 1 In Service Center, click **Reporting > Reports**.

- 2 Click **Get More**.

The **Components** page opens with a list of reports available for installation.

- 3 Click **Updates** to view the list of report updates.

- 4 Select the check box beside the report update that you would like to install.

- 5 Click **Install**.

### See Also

[Updating and Installing Service Center Components](#)

## Deleting a Report

- 1 In Service Center, click **Reporting > Reports**.

- 2 Locate the report you want to delete.

- 3 Click the **Delete** icon.



Delete icon

- 4 Click **OK**.



---

## Organizing Reports into Categories

### About Report Categories

Report categories help you organize reports into groups. Managed Workplace comes with several predefined categories.

You may find that grouping reports based on your own categories helps to organize your operations more closely than using the predefined categories. If this is the case, you can create and remove report categories as required.

Any reports that are created without specifically selecting a report category will be collected under **Uncategorized**.

### Creating a Report Category

- 1 In Service Center, click **Reporting > Categories**.
- 2 Click **Add**.
- 3 In the **Name** box, type a name for the category.
- 4 In the **Description** box, type a description for the type of reports being categorized.
- 5 Click **Save**.

### Renaming a Report Category

- 1 In Service Center, click **Reporting > Categories**.
- 2 In the list of report categories, click the category you want to rename.
- 3 In the **Name** box, type a new name for the category.
- 4 Optionally, in the **Description** box, type a new description for the type of reports being categorized.
- 5 Click **Save**.

### Assigning a Report to a Report Category

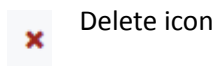
- 1 In Service Center, click **Reporting > Reports**.
- 2 Locate the report to which you want to assign a category.
- 3 Click the name of the report.
- 4 From the **Category** list, select a report category.

- 
- 5 Click **Save**.

## Deleting a Report Category

To remove a report category without removing the reports and delivery schedules that are associated with the report category, modify the reports prior to removing the report category and assign the reports a new category, (for example, Uncategorized).

- 1 In Service Center, click **Reporting > Categories**.
- 2 In the list of report categories, click the **Delete** icon that corresponds with the category you want to remove.



- 3 Click **OK**.

## Scheduling a Report

### Creating a Delivery Schedule for a Report

Delivery Schedules define when to automatically run reports.

#### To name the scheduled report

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click **Create Schedule**.
- 3 In the **Status** tab, type a name for the delivery schedule.

#### To select the report to schedule and the output format

- 1 Click the **Settings** tab.
- 2 Select either **Site**, **Device** or **Multi-Site** depending on the type of report you're scheduling.

The **Report** list is filtered based on your selection. For example, if you select the **Site** option button, then only site reports appear in the list. Similarly, if you select the **Multi-Site** option button, only aggregate site reports appear.

- 3 To locate the report, select a category from the **Category** list and then select the report from the **Report** list.

---

**Note:** You must include a report.

- 4 Select one of the following output formats for the report:

**Portable Document Format (PDF)** This format becomes an attachment in an email.

**Web Archive (MHTML)** This format embeds right into an email. This web page archive format combines resources that are typically represented by external links (such as images, Flash animations, Java applets, audio files) together with HTML code into a single file.

**Excel Workbook (XLS)** This format becomes an attachment in an email. This format is useful if you want to edit or manipulate the data in Excel.

**TIFF** This format becomes an attachment in an email.

**XML** This format becomes an attachment in an email. Saving the report in XML format allows you to import the report data into another system. For example, if you have developed a web portal that clients can log into and view information about their company such as reports, performance statistics, etc. XML is a clean way of exporting and importing data from one system to another.

**CSV** This format becomes an attachment in an email. This format can be loaded into any spreadsheet program. You can also use .CSV files to import the data into another system.

**Microsoft Office Word** This format becomes an attachment in an email. This format can be loaded into Microsoft Word.

- 5 If required, select the time zone and locale for the report.

If you are creating a report for a customer in a different time zone or locale, select their time zone and locale.

### To select sites and devices to include in the scheduled report

- 1 Click the **Subjects** tab.

Depending on whether you selected **Site** or **Device** in the **Settings** tab, you can filter what sites and devices to include in the report.

**Note:** If you selected the **Multi-Site** option button when selecting the report, then you cannot select any sites on this page because you select the sites when you import the aggregate site reports. See [To use predefined aggregate reports](#).

- 2 Select the check box for each subject to include and click the >> button.

---

Make sure to select the site when reporting against service groups or devices so that the recipient only sees information appropriate to their site.

**Note:** For site or device reports, you must include at least one subject.

### To set the scheduled report to be emailed or archived

**Best Practice:** Email the report to yourself or archive. This way you have the exact report that was sent to your customer.

- 1 Click the **Delivery** tab.
- 2 To archive a copy of the report to the Service Center database so the report can be viewed from the Report History, select the **Save Report to Archive** check box.
- 3 To email a copy of the report, select the **Email Report** check box and then do the following:
  - a Select a priority for the email message from the **Priority** list.
  - b Type the email address of each recipient (separating recipient addresses with a semicolon), or click the address book icon to open the **Email Contacts** dialog box, where you can select each Service Center user by enabling the corresponding check box.
  - c Type the email subject line contents in the **Subject** box.
  - d Type the email message in the **Email Message** box.

**Note:** You must include at least one delivery method. For each site included in the **Subjects** tab, you must include at least one email address. You must include a subject for the email. Ensure you enter a valid email address. If you selected the **Multi-site** option button when selecting the report, then you must select the sites to include in the report when you import the aggregate site reports. See [To use predefined aggregate reports](#).

### To schedule when to deliver the report




- 1 Click the **Schedule** tab.
- 2 Click either the **Daily**, **Weekly**, **Monthly** or **Quarterly** option button to define how often you want the report delivered.

**Note:** A quarterly report runs three months after you configure it, rounding to the closest month.

- 3 Use the corresponding schedule section that appears based on the selected option button to further define the delivery schedule.

- 
- 4 To set how many days of data to include in the scheduled report, select the reporting period.
  - 5 Click **Save**.

## Viewing the List of Scheduled Reports

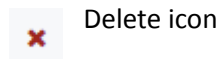
- In Service Center, click **Reporting > Delivery Schedules**.
    -  Schedule executed and delivered successfully
    -  Schedule created but not yet executed
    -  Schedule executed but delivery errors occurred
  - To change how many scheduled reports display on this page, select 5, 10, 20, or 100 from the **Page Size** list.
  - To filter which scheduled reports to display on this page, use the **Category** list.
- Note:** No delivery schedules will appear until you choose a category and click **Reload**.
- To sort the list of scheduled reports in ascending or descending order, click a column header.

## Running a Scheduled Report Immediately

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click **Run Now** to execute the scheduled report immediately.

## Deleting a Scheduled Report

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click the **Delete** icon beside the scheduled report you want to delete.



- 3 Click **OK**.

---

## Working with Archived Reports

### About Archiving

Archiving a report saves a copy of what is delivered in the Service Center database. It's a good idea to keep a record of the reports you send a client.

For information about how to archive a scheduled report, see [To set the scheduled report to be emailed or archived](#).

### Viewing the Historical Information for a Report

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click the name of the scheduled report for which you want to see the historical information.  
**Tip:** Site reports that were run against multiple sites include the site name to help you identify which site each report was run against.
- 3 In the **Status** tab, note the information in the **History** section.

### Exporting an Archived Report to a ZIP File

You can export an archived report or more than one archived report into a .ZIP file.

Zipping multiple report files into one file

- makes it easier to email more than one report to a client.
- allows for easier file storage. Since the file is compressed, only one file needs to be maintained instead of multiple files.

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click the name of the scheduled report that you want to export to a .ZIP file.
- 3 Click **Export to ZIP** and either **Open** or **Save** the .ZIP file.

### Deleting an Archived Report

- 1 In Service Center, click **Reporting > Delivery Schedules**.
- 2 Click the name of the scheduled report for which you want to see the historical information.

- 
- 3 In the **History** section, select the check box beside archived report you want to delete.
  - 4 Click **Delete**.





# CHAPTER 15

## USING SERVICE MODULES

---

*This section provides detailed information about the following topics:*

- *Service Modules*
- *Setting Up a Service Module*

*For information about using service modules with Managed Workplace, see the Integration Guide: Backup and Disaster Recovery and Integration Guide: Antivirus.*

---

---

## About Service Modules

A service module is an enhanced monitoring policy that includes a dashboard, monitors, reports and scripts.

### Service Modules versus Monitoring Policies

A service module is a superset of the related monitoring policy. For example, the Symantec\_Backup\_Exec\_2010 monitoring policy is included in the Symantec Backup Exec 2010 service module.

You shouldn't import both the monitoring policy and the related service module. You only need the service module. For example, if you're already using the Symantec Backup Exec monitoring policy, and you want to use the service module instead, you need to remove the individual monitoring policy.

## Setting Up a Service Module

### Installing a Service Module

You can install a new service module by going to Update Center and selecting a service module from the list of new service modules available for install. This list is updated periodically as new service modules are released by AVG.

- 1 In Service Center, click **Configuration > Service Modules**.
- 2 Click **Get More**.

The **Components** page opens with a list of service modules available for installation.

- 3 Select the check box beside the service module you want to install.
- 4 Click **Install**.

#### See Also

[Updating and Installing Service Center Components](#)

### Importing a Service Module

You can import service modules that you have exported from Service Center.

- 1 In Service Center, click **Configuration > Service Modules**.
- 2 Click **Add**
- 3 Click **Browse** to locate the service module

- 
- 4 Click **Import**.

**Notes:**

- If you export a service module, only the monitoring policies are exported.

## Updating a Service Module

You can update a service module in Service Center by installing an upgrade from Update Center. Service module upgrades are created periodically by AVG and added directly to Update Center for you to install.

When an upgrade is available, a green icon appears beside **Update Center > Components** in the navigation pane to indicate that there is a new component available for upgrade.

- 1 In Service Center, click **Update Center > Components**.
- 2 Click **Updates**.
- 3 In the **Type** column, select **Service Modules** from the list.
- 4 Select the check box beside the service module update you want to install.
- 5 Click **Install**.

**See Also**

[Updating and Installing Service Center Components](#)

## Viewing an Overview of All Service Modules

You can view an overview of all service modules in Service Center, including information such as each service module name, version, and notes. The information available for each service module varies.

Each service module name is a link that you can click to view additional information about the service module, which is aggregated at either a device level, a site level, or a multi-site level. The level of data aggregation depends on how the service module was authored.

- 1 In Service Center, click **Status > Service Modules**.
- 2 Optionally, click a service module name to view an overview.

## Viewing Monitoring Information about a Service Module

You can view the monitoring configuration of a service module to view a list of included monitoring policies. A warning message appears if those monitoring policies do not have automatic inclusion rules applied, which is required for monitoring to occur when the service module is added to a service plan.

---

### To view information about a service module

- 1 In Service Center, click **Configuration > Service Modules**.
- 2 Click the name of a service module.

## Deleting a Service Module

You can delete a service module you no longer need.

- 1 In Service Center, click **Configuration > Service Modules**.
- 2 Select the check box beside the name of the service module.
- 3 Click **Delete**.
- 4 Click **OK** to confirm the deletion.

# CHAPTER 16

## WORKING REMOTELY

---

*This section provides detailed information about the following topics:*

- *Remote Control*
  - *Initiating a Remote Control Session*
  - *Working with the Remote Tools*
  - *Viewing the Remote History*
  - *Troubleshooting Remote Connections*
  - *Using Onsite Manager Utilities*
-

---

## Remote Control

### About Remote Control

Remote control enables you to connect to client devices using various methods (services), including Remote Desktop, Remote Assistance, UltraVNC and so on.

All Managed Workplace remote sessions take place over HTTP or HTTPS so you don't have to forward any ports to your Service Center or worry about the port being allowed outbound on your clients' networks. Because the standard web ports are being used, sessions will succeed even when a proxy server is present on the remote network.

**Note:** There is no connection limit to the number of remote control sessions.

#### What You Can Do

You can

- use the shortcut icon in device lists so you can connect instantly without having to access the Device Overview page.
- see the device and site connected to in the top left-hand corner of the Remote Desktop window. This is useful if you have more than one session open.

#### Remote Control Requirements

The computer on which you initiate a remote control session must have the following installed:

- Microsoft .NET Framework 3.5 or higher
- client software for the selected protocol

To use remote control and the remote tools, you must ensure the user account and role are set up to have permissions to device management for remote control access. By default, Administrators, Technicians and Service Managers are set up with these permissions. See [Setting Permissions for a Role](#).

#### Notes:

- Using remote control (that is, Remote Desktop, Remote Assistance, and so on) in Mozilla Firefox and Google Chrome requires a plugin to support the Microsoft RunOnce technology.
- Remote control does not work in Safari and Opera.
- Remote control does not work on non-Windows operating systems.

---

## Browser and Operating System Support for Remote Control and Remote Tools

This table identifies what feature works in which browser:

Browser	Remote Control	Remote Tools
Internet Explorer	Yes	Yes (plugin)
Google Chrome	No	No
Mozilla Firefox	Yes (plugin)	Yes (plugin)
Apple Safari	No	Yes (plugin)
Opera	No	Yes (plugin)

**Note:** Remote control will fail if you are prompted for a plugin and choose not to install it. If you also select the Don't Show this Message Again check box, you will not be offered the choice to install the required plugin on subsequent attempts, and the connection will fail without further messages. To be prompted for plugin installation again, you must remove the cookies for the Service Center site and then install the plugin when prompted.

This table identifies what feature works in which operating system:

Operating System	Remote Control	Remote Tools
Windows	Yes	Yes
Non-Windows	Yes (requires the server software for the selected protocol)	No

**Note:** The remote tools are not supported on Windows 2000 computers because .NET 3.5 is required on the target device. Windows 2000 does not support .NET 3.5.

### Selecting Which Remote Control Option to Use

In addition to the following remote control options available with Managed Workplace, you can set up an additional remote control link to launch a third-party remote control tool. See [Setting Remote Control Options](#).

**AVG Business Premium Remote Control** Uses ISL Light technology to remote to a Windows or Mac device, allowing you to take control of the local

---

computer. AVG Premium Remote Control is built in to Service Center, and deploys automatically to all managed devices, allowing for a seamless integration with minimum configuration. To use AVG Premium Remote Control, Windows devices must have the Admin share open, and Mac devices must have SSH enabled and the SSH credentials must be on the sudoer's list.

**Note:** AVG Premium Remote Control requires that you download a client to your computer. Service Center will detect if you have the AVG Premium Remote Control client installed, and if it is not a link will be available on the Device page for you to download the application.

**AVG Business Premium Remote Control - On Demand** Some devices are not always managed by AVG Managed Workplace. In this scenario, Premium Remote Control On Demand is available to connect you to the customer's unmanaged device.

**Remote Desktop** Uses the Microsoft Terminal Services client, commonly referred to as RDP client. This is present on all Windows operating systems. You can connect to the console session or share local and remote resources.

Remote Desktop allows you to take control of the remote computer without first requesting access. To do this you must have administrator rights on the local machine. After you log in, you will have complete control of the local computer.

Use Remote Desktop when a user is not on the other end. This option is useful for performing a routine maintenance task on a workstation.

**Note:** Remote Desktop uses the smallest IP address available (comparing each subnet class sequentially).

**Remote Assistance** Starts the Windows Remote Assistance tool that lets you view the client's screen and chat about what you both see.

Managed Workplace provides one-click launch for Remote Assistance that is initiated by the technician. There is no need for MSN Messenger. The end user doesn't have to launch the request (although the end user does have to accept the connection request).

Use Remote Assistance when a user is on the other end to allow access or requests for control. This option is useful for teaching or showing a user how to perform a task.

**Note:** Remote Assistance works on any Windows device that is WMI-enabled (and where the admin file share can be accessed by Onsite Manager).

**VNC** Uses a VNC client to connect to a remote VNC server that has been previously installed. The main advantage of VNC over RDP is VNC is supported across all modern operating systems, including Macintosh, Linux/UNIX and Windows.



---

**Note:** When initiating a VNC session to the Onsite Manager computer, loopback must be enabled for the VNC server. Refer to the documentation for the VNC Server product for instructions on how to configure this.

**UltraVNC** Pushes a VNC server out to a remote computer and uses the VNC client to connect to it. No prior installation is required, and the server is optionally automatically removed after the session ends.

If an attempt is made to establish a session using the UltraVNC option and an existing VNC server is discovered on the target device, the session will fail and you must then use the standard VNC remoting option.

Since the server software is pushed to the target computer, this means that any security software (such as Windows Defender or Spybot Search & Destroy) could potentially block the installation until a local user accepts it.

**Note:** If you uninstall the server once the session ends, the file `\Program Files\TightVNC\VncHooks.dll` may be left on the target computer. This file does not always unload from memory. This is a known issue with the TightVNC server application used by this remoting option.

**Telnet** Uses the default Windows Telnet client to connect to devices supporting this protocol.

**Note:** Telnet is no longer installed by default on modern Windows operating systems. Users must ensure that the Telnet client is installed by following the instructions in their operating system's help.

**PuTTY** Uses the PuTTY client to handle Secure Shell (SSH) connections.

**Intel® AMT** Allows the control of a remote computer that is powered down, has no operating system, or a failed operating system using a technology that is integrated into the hardware of a PC based on the Intel® vPro™ platform.

**Intel® KVM** Launches a VNC session to redirect remote keyboard, mouse and monitor control of a PC based on the Intel® vPro™ platform. This feature requires some initial BIOS configuration. It is supported on PCs with vPro™ version AMT 6.0 or higher. This feature provides better VNC performance and an optional user consent feature.

**Onsite Manager Utilities** Launches the Onsite Manager Utilities.

**Note:** You must enable prompting for file download in the custom level security settings of your Internet Options in Internet Explorer. It will prompt you to install a file called Remote Access Gateway. Onsite Manager Utilities do not work with Device Managers.

**Web Console** Launches an RDP session to the Onsite Manager server and opens an Internet Explorer connection to the target device.

---

**Note:** You must enable prompting for file download in the custom level security settings of your Internet Options in Internet Explorer. The web console feature does not work with Device Managers.

**Other** Attempts to connect to remote devices with the client application configured as the “other” options in System Settings. See [Setting Remote Control Options](#).

## Initiating a Remote Control Session

### Using the Shortcut Icon

When a device is listed in Service Center, a shortcut icon is displayed. You can use this icon as a quick way to initiate a remote control session or start a remote tool.

 Shortcut icon

The options presented are ones that are available for the selected device. If you’ve used that option before, the settings you used last time are saved.

The context menu for Remote Control displays a star beside the last used tool.

### Initiating a Remote Control Session Using AVG Business Premium Remote Control

The AVG Business Premium Remote Control agent must be installed on the managed device. In most cases, the agent is automatically installed on the device when Premium Remote Control is enabled on the Site Management page. However, in some cases it might not be installed, in which case you can install it on the device from the Device page when initiating a remote session.

**Tip:** Did you know you can record your AVG Business Premium Remote Control support session? To view the recorded session, you can download the ISL player from <http://www.islonline.com/tools/thank-you-recording-player.htm>.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select **Premium Remote Control**.

- 
- 5 If the AVG Business Premium Remote Control agent is not detected on the device, click the **Install Premium Remote Control** button to install it remotely. This installs the agent automatically and requires no action from the device user.
  - 6 To enable a chat window during the remote session, select the **Enable chat** check box. Note that using chat requires additional connection time.
  - 7 If the AVG Business Premium Remote Control client is not installed on your computer, click the link to install it.

**Note:** Once the AVG Business Premium Remote Control client is installed on your machine, you will be prompted for your AVG Business SSO credentials. If you are not using AVG Business SSO, you can simply close this window and AVG Business Remote Control will launch.

**Tip:** If you need to remove the AVG Business Premium Remote Control agent from a device, Managed Workplace includes scripts to uninstall AVG Premium Remote Control. To run the script on a device, go to **Automation > Library**, and select one of the following scripts:

- Uninstall AVG Business Premium Remote Control MAC
- Uninstall AVG Business Premium Remote Control WIN

## Initiating a Remote Control Session Using AVG Business Premium Remote Control - On Demand

Using AVG Business Premium Remote Control, you can launch an on-demand session from a Windows or Mac computer. Customers can accept on-demand sessions from Windows or Mac computers, regardless which type of computer they received the invitation from.

### Launching an On-Demand Session - Windows

- 1 Click the **Premium Remote Control On Demand** button on the top bar and click **Premium Remote Control On Demand** on the menu.
- 2 The startup executable is downloaded to your computer. Run the executable.
- 3 The Premium Remote Control application starts and you are automatically logged in.
- 4 A session window is launched, which displays:
  - The session code
  - An **Invite** button, which will create an email with a link to the session
  - An **Options** button which allows you to modify the session options

- 
- 5 Click **Invite** > Enter an email address and click **Send**
    - a Or click the Open an e-mail link to open the invitation in your Email client. The email template is sent from your local mail client to avoid spam filter problems.
  - 6 Your customer clicks on the link in the e-mail and then clicks **Allow Access**.

**Notes:** On Demand session history can be accessed via the Premium Remote Control On Demand button and choosing Session History.

You can enter session notes for each individual session.

### Launching an On-Demand Session - Mac OS

- 1 Click the **Premium Remote Control On Demand** button on the top bar and click **Premium Remote Control On Demand** on the menu.
- 2 PrcOnDemand.dmg is downloaded to your computer.
- 3 Click PrcOnDemand.dmg to mount it.
- 4 Double-click the **AVG Business Premium Remote Control** icon.
- 5 A session window is launched, which displays:
  - The session code
  - An **Invite** button, which will create an email with a link to the session
  - An **Options** button which allows you to modify the session options
- 6 Click **Invite** > Enter an email address and click **Send**
  - a Or click the Open an e-mail link to open the invitation in your Email client. The email template is sent from your local mail client to avoid spam filter problems.

**Notes:** On Demand session history can be accessed via the **Premium Remote Control On Demand** button and choosing **Session History**.

You can enter session notes for each individual session.

### On-Demand E-mail Templates

The email template can be modified by doing the following

- 1 Navigate to **Configuration > System Settings**.
- 2 Select the **Remote Control** page.
- 3 Modify the email template in the **AVG Premium Remote Control** section.
- 4 Click **Save**.
- 5 To return to the default template, click **Restore Default** and **Save**.

---

### Accepting an On-Demand Session - Windows

- 1 The customer clicks the link in the invitation email and then clicks **Allow Access**. An executable is downloaded to your customer's computer and automatically connects to your session.

### Accepting an On-Demand Session - Mac OS

- 1 Your customer clicks on the link in the e-mail and then clicks **Allow Access**.
- 2 A .dmg is downloaded to your customer's computer. The .dmg is named AVG Business Premium Remote Control [session#], where [session#] is the number of the session.
- 3 The customer clicks the .dmg to mount it, then double-clicks the AVG Business Premium Remote Control installer.

## Initiating a Remote Control Session Using Remote Desktop

Remote Desktop must be enabled on the target device. See Microsoft Help and Support.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the **Remote Services** section, from the **Service** list, select **Remote Desktop**.
- 6 Confirm the Remote Machine IP address is correct.
- 7 Confirm the Remote Machine Port is correct.  
**Note:** This port is used between Onsite Manager and the device. Communications between Onsite Manager and Service Center occur over HTTP or HTTPS.
- 8 To redirect local drives from the tech device to the remote device, which allows for easier file transfers between the tech device and the remote device, select the **Redirect Local Drives** check box.
- 9 To connect to console, and log into the server as if you were sitting directly in front of it rather than creating a brand new session, select the **Connect to Console** check box.
- 10 Click **Connect**.

- 
- 11 If a prompt appears warning that a program is executing, click **OK** to continue.

### See Also

[Initiating a Remote Control Session Using Remote Assistance](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Control Session Using Remote Assistance

Remote Assistance enables you to shadow Windows workstation desktops, chat with the logged in user and take control, if required. The Windows-native remote assistance utility is used, but the end user does not need to initiate the request.

**Note:** Remote Assistance must be installed on both the technician's device and the target device. If Remote Assistance is installed, but disabled on the target device, it will be temporarily enabled for the duration of the session and then disabled once again when the session ends.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select **Remote Assistance**.
- 5 Confirm the Remote Machine IP address is correct.
- 6 Confirm the Remote Machine Port is correct.  
**Note:** This port is used between Onsite Manager and the device. Communications between Onsite Manager and Service Center occur over HTTP or HTTPS.
- 7 Click **Connect**.
- 8 If a prompt appears warning that a program is executing, click **OK** to continue.

---

If you are prompted for a password, press Ctrl+V to paste the password that was passed and stored on the Clipboard.

### See Also

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Control Session Using VNC, Telnet, or PuTTY

**Note:** Telnet is no longer installed by default on newer Windows operating systems. Clients must ensure that the Telnet client is installed by following the instructions in their operating system's help.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the **Remote Services** section, from the **Service** list, select VNC, Telnet, or PuTTY.
- 6 Confirm the Remote Machine IP address is correct.
- 7 Confirm the Remote Machine Port is correct.

**Note:** This port is used between Onsite Manager and the device. Communications between Onsite Manager and Service Center occur over HTTP or HTTPS.

- 8 If required, in the **Local Application Path** box, type the path to the client software, or if available, click Browse (...) to locate the client executable.

**Note:** Modern browser security settings may prevent you from using the **Browse** button to capture the file path of the client software. In Internet Explorer you must either add Service Center to the trusted sites list or set

---

the security setting for **Include Local Directory Path When Uploading Files to a Server** to enabled.

The **Application Parameters** box is populated with the information needed to establish the session.

- 9 If required, in the **Application Parameters** box, type additional arguments to adjust the functionality.
- 10 Click **Connect**.
- 11 If a prompt appears warning that a program is executing, click **OK** to continue.

### See Also

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Control Session Using UltraVNC

**Note:** By default, UltraVNC is installed on the Onsite Manager machine. If the install failed, you will have to manually install UltraVNC by downloading the zip package from <http://s3-us-west-2.amazonaws.com/levelplatforms/MW2013/winvnc.1.0.8.2.zip>. Unzip the package, and then copy the files to Onsite Manage\bin\MWUltraVNC.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the **Remote Services** section, from the **Service** list, select UltraVNC.
- 6 Confirm the Remote Machine IP address is correct.
- 7 Confirm the Remote Machine Port is correct.



- 
- 8 If pushing the application to the device, select the **Install Remote Agent If Not Installed** check box.
  - 9 In the **Local Application Path** box, type the path to the client software, or click the ... button to locate the client executable.  
  
The **Application Parameters** box is populated with the information needed to establish the session.
  - 10 If required add arguments to the **Application Parameters** box to adjust the functionality.
  - 11 If you want the application removed once the session closes, select the **Uninstall Remote Agent When Complete** check box.
  - 12 Click **Connect**.
  - 13 If a prompt appears warning that a program is executing, click **OK** to continue.

### See Also

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Control Session Using Onsite Manager Utilities

The Onsite Manager Utilities enable you to manage remote computers without affecting the logged in user. For example, you can run network diagnostic tests such as Ping Device and Trace Route to Device, perform remote management and troubleshooting tasks using Registry Editor or computer management, or take control of the remote computer using the Command Prompt, all without affecting the user that is logged into the remote computer.

### Notes:

- Many of the new Remote Tools perform the tasks that the Onsite Manager Utilities perform. For example, you can now use the Remote CMD Prompt remote tool. See [Using Remote Tools](#).
- You can work with many computers using a single Onsite Manager Utilities session. To open additional tabs to connect to other devices on the same

---

Onsite Manager, select the device to target from the list and click the chevron (>) beside it.

- Onsite Manager Utilities do not work with Device Manager.
- 1 In Service Center, click **Status > Devices**.
  - 2 Locate the device to which you want to initiate a remote control session.
  - 3 Click the device name and then click **Remote Control** from the right sidebar.
  - 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
  - 5 In the Remote Services section, from the **Service** list, select **Onsite Manager Utilities**.
  - 6 In the **Onsite Manager Utilities Configuration** section, confirm the Remote Machine IP address is correct.
  - 7 Click **Connect**.
  - 8 In the main menu on the left side of the window, click a tool name.
  - 9 When you are done using the Onsite Manager Utilities, click **Close** to close the window.

### See Also

[Using Onsite Manager Utilities](#)

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Session to Access the Web Console of Managed Devices

You can establish a remote session to access the web console of a managed device, such as a switch or a router.

**Note:** The web console feature does not work with Device Managers.

- 1 In Service Center, click **Status > Devices**.

- 
- 2 Click the device name and then click **Remote Control** from the right sidebar.
  - 3 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
  - 4 In the **Remote Services** section, from the **Service** list, select **Web Console**.
  - 5 In the **Web Console Configuration** section, select either HTTP or HTTPS from the list and then type the URL information.
  - 6 Click **Connect**.

### See Also

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Session to Access Intel® AMT-Enabled Devices

You can establish a remote session to access Intel® AMT-enabled devices, which allows you to remotely access the BIOS screen, gain access to a device's command line prompt, as well as view boot process messages during a start-up of that computer.

You can also emulate an IDE disk, floppy disk, or CD/DVD drive over a standard network connection, which allows you to reboot an Intel® AMT-enabled device from a bootable image located in Onsite Manager (C:\Program Files\AVG\Onsite Manager\IDER Boot Images). Once an IDE-R session is established, the Intel® AMT-enabled device can boot from a remote floppy image (.IMG file) or remote CD image (.ISO file). This enables you to facilitate remote diagnosis and repair an Intel® AMT-enabled device that fails to boot.

You can boot any operating system and use any application providing the terminal emulation mode is

- VT100 / UTF-8
- ANSI / Extended-ASCII

If you want to see the remote session history of an Intel® AMT-enabled device, see [Viewing the Remote History](#).

---

**Caution:** Use of AMT-based remote options may cause user application data loss.

**Note:** Initiating a remote session to access Intel® AMT-enabled devices with Device Manager is not supported.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select Intel® AMT.
- 5 Confirm the Remote Machine IP address is correct.
- 6 Select the Emulation Type from the list.
- 7 Do one of the following:
  - To view boot process messages, select the **Normal Boot** button.
  - To change the BIOS settings, select the **Boot to BIOS** button.
  - To boot from the remote floppy image (.IMG file) or remote CD image (.ISO file), select the **IDE Redirection** button.
- 8 Put the files in the following location (assuming Program Files are on the C drive):
  - For 32-bit systems: C:\Program Files\AVG\Onsite Manager\IDER Boot Images
  - For 64-bit systems: C:\Program Files (x86)\Onsite Manager\IDER Boot Images
- 9 Click **Connect**.

If this is the first time you are attempting to perform any of the above tasks remotely, then you will be asked to install the AMT Terminal application. Follow the installation wizard instructions and once complete, you must click Connect again.
- 10 If required, you can power down, power up, or reset an Intel® AMT-enabled device by clicking either Power Off, Power On, or Reset.

### See Also

[Viewing the Status of Intel® AMT-Enabled Devices](#)

[Initiating a Remote Control Session Using Remote Desktop](#)

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

---

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM](#)

## Initiating a Remote Session to Access Intel® AMT-Enabled Devices with Intel® KVM

You can establish a remote session to an Intel® AMT-enabled device using Intel® KVM if Onsite Manager is MW2010 or newer and the device is AMT 6.0 or newer. The Intel® KVM option only displays if these conditions are met.

The KVM feature must be enabled in the BIOS using an administrator account. The following features must be enabled:

- manageability feature
- KVM opt-in
- KVM opt-in remote configuration

You can provide the end user with control over remote sessions. If user consent is enabled, a code (six numbers) appears on the remote display when the KVM session initiates. The remote user will have to communicate that code to the technician who must enter it in the prompt displayed on the screen.

**Note:** Initiating a remote session to access Intel® AMT-enabled devices with Intel® KVM in Mozilla Firefox and Google Chrome is not supported.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select Intel® KVM.
- 5 Confirm the Remote Machine IP address is correct.
- 6 Click **Connect**.

If **User Consent** is enabled, you are prompted for the code that you must obtain from the end user.

### See Also

[Initiating a Remote Control Session Using Remote Desktop](#)

---

[Initiating a Remote Control Session Using VNC, Telnet, or PuTTY](#)

[Initiating a Remote Control Session Using UltraVNC](#)

[Initiating a Remote Control Session Using Onsite Manager Utilities](#)

[Initiating a Remote Session to Access the Web Console of Managed Devices](#)

[Initiating a Remote Session to Access Intel® AMT-Enabled Devices](#)

## Initiating a Remote Control Session by Launching TeamViewer

If you have configured TeamViewer as your custom third-party remote control tool in System Settings, you can initiate a TeamViewer session on a device. When TeamViewer has been configured, it appears in the Service list when selecting a remote control tool to use on a device. For more information on setting up TeamViewer access in Service Center, see [Configuring a Custom Third Party Integration](#).

**Note:** TeamViewer must be installed on both the tech PC and the end user's device.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select TeamViewer.
- 5 Onsite Manager retrieves the device's TeamViewer client ID and populates it in the **Client ID** box. If this box is not automatically populated, you must enter it here.
- 6 Do one of the following:
  - If you entered a global password for TeamViewer in **System Settings**, the global password is populated in the **Password** box, in incertitude format. The global password overrides the client TeamViewer password on the device.
  - If a global password was not configured for TeamViewer, you can enter the client password in the **Password** box by clicking the **Edit** icon and typing the password, or you can enter the password when the TeamViewer client is launched on the device.
- 7 The application path indicates the folder where TeamViewer is installed on the tech PC. This path was configured in System Settings. If this path does not match the location where you have TeamViewer installed, do the following:

- 
- Click the ... button.
  - Browse to locate the installation folder.
  - Click **OK**.

**8** Click **Connect**.

**Tip:** If you have made changes to the TeamViewer settings, click **Save** to save them, or **Undo** if you made a mistake. At any time, you can click **Restore System Default** to return the TeamViewer configurations to the defaults set in System Settings.

## Initiating a Remote Control Session by Launching LogMeIn Pro

LogMeIn Pro uses a web-based remote access mechanism, while the client PC must have the end-user software installed. Access is gained to the client PC by logging on to the Web UI through the credentials set in Managed Workplace, and then selecting the client PC from the list.

When the LogMeIn Pro client is installed on a client PC, Onsite Manager retrieves the Client ID to allow access. Additionally, your LogMeIn Pro Company ID and PSK (encryption key) must be entered in System Settings. These credentials are provided to you when you create a LogMeIn account. For more information on configuring LogMeIn Pro in System Settings, see [Configuring a Custom Third Party Integration](#).

- 1** In Service Center, click **Status > Devices**.
- 2** Locate the device to which you want to initiate a remote control session.
- 3** Click the device name and then click **Remote Control** from the right sidebar.
- 4** In the **Remote Services** section, from the **Service** list, select LogMeIn Pro.
- 5** If Onsite Manager could not collect a Client ID from the device, the **Hostname** box appears for you to provide the remote machine host name.
- 6** Click **Connect**.

LogMeIn Pro launches in a web browser. You will be prompted to log in to the local computer. After entering the local log in credentials, click the **Remote Control** link to remote to the device.

**Tip:** If you have made changes to the LogMeIn Pro settings, click **Save** to save them, or **Undo** if you made a mistake. At any time, you can click **Restore System Default** to return the LogMeIn Pro configurations to the defaults set in System Settings.

---

## Initiating a Remote Control Session by Launching ScreenConnect

ScreenConnect uses a web-based remote access mechanism, while the client PC must have the end-user software installed. For information on setting up ScreenConnect, see [Configuring a Custom Third Party Integration](#).

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 In the **Remote Services** section, from the **Service** list, select ScreenConnect.
- 5 In the **Machine Identifier** box, type the device's machine name. By default, the Hostname parameter is entered in this box to automatically populate the machine name.
- 6 Click **Connect**.

**Tip:** If you have made changes to the ScreenConnect settings, click Save to save them, or Undo if you made a mistake. At any time, you can click Restore System Default to return the ScreenConnect settings to the defaults set in System Settings.

## Initiating a Remote Control Session by Launching a Third-Party Remote Control Tool

Service Center can be configured to launch one additional third-party remote control tool. This additional option appears either as the application name, or as "Other" in the Remote Service list, and in the Remote Control shortcut menu. This additional option is added to Service Center in System Settings. For more information, see [Configuring the "Other" Remote Control Application](#).

**Note:** The following procedures provide steps for launching third-party tools that have been tested for integration with Managed Workplace, however any third-party tool that launches the application on the technician's computer, or as a URL on the client or technician computer can be integrated with Managed Workplace.

### To initiate a remote control session using GoToAssist

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.



- 
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
  - 5 In the **Remote Services** section, from the **Service** list, select GoToAssist.
  - 6 Confirm the Remote Machine IP address is correct.
  - 7 In the **URL** box, paste the session-specific URL. For example, `https://broker.gotoassist.com/a/mycompany?Question=AB123-456-789`.  
This URL can be copied from within GoToAssist by clicking the **Copy URL** button.
  - 8 Click **Connect**.
  - 9 If a prompt appears warning that a program is executing, click **OK** to continue.

#### To initiate a remote control session using LogMeIn Rescue

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the **Remote Services** section, from the **Service** list, select LogMeIn Rescue.
- 6 Confirm the Remote Machine IP address is correct.
- 7 In the **URL** box, paste the session-specific URL. For example, `https://secure.logmeinrescue.com/R?i=2&Code=123456`.  
This URL can be copied from the **Create New Session** window in LogMeIn Rescue, by clicking the **Link** tab and clicking the **Copy Link to Clipboard** button.
- 8 Click **Connect**.
- 9 If a prompt appears warning that a program is executing, click **OK** to continue.

#### To initiate a remote control session using LogMeIn Pro

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.

- 
- 3 Click the device name and then click **Remote Control** from the right sidebar.
  - 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
  - 5 In the **Remote Services** section, from the **Service** list, select LogMeIn Pro.
  - 6 Confirm the Remote Machine IP address is correct.
  - 7 In the URL box, paste the device-specific URL. For example, `https://secure.logmein.com/mycomputers_connect.asp?hostid=1234567890`.

This URL can be copied from within LogMeIn Pro by navigating to the following location:

- a From the **Home** page, click **Properties**.
  - b On the **Host Properties** page, click the **General Settings** tab.
  - c Right-click the Connect to this Computer link, and select **Copy shortcut**.
- 8 Click the **Save** link. This saves the URL in Service Center for this particular device so that every time you remote to the device using the Other option, the configuration is pre-filled and you can connect right away.
  - 9 Click **Connect**.
  - 10 If a prompt appears warning that a program is executing, click **OK** to continue.

### To initiate a remote control session using DameWare

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the **Remote Services** section, from the Service list, select DameWare.
- 6 Confirm the Remote Machine IP address is correct.
- 7 Do one of the following:
  - If the **Local Application Path** box is populated, confirm that it is the correct path.

- 
- If the **Local Application Path** box is blank, or points to an incorrect path, click the ... button. In the **Set Local Client Application Path for {0}** page, click the Browse button to navigate to the folder where Dameware is installed. Click OK.
- 8 If required add arguments to the **Application Parameters** box to adjust the functionality.
  - 9 Optionally, you can click the **Save** link. This saves the local application path for your Service Center user account, which is helpful if you have the application saved in a folder that is not the default.
  - 10 Click **Connect**.
  - 11 If a prompt appears warning that a program is executing, click **OK** to continue.

### To initiate a remote control session using Bomgar

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5 In the Remote Services section, from the **Service** list, select Bomgar.
- 6 Confirm the Remote Machine IP address is correct.
- 7 In the **URL** box, paste the session-specific URL. For example, `http://trial.bomgar.com/?ak=1234567890abcdef1234567890abcdef`.  
This URL can be copied from within Bomgar by doing the following:
  - a In the **Start Support Session** window, click the **Email** button.
  - b Copy the URL from the email generated in your email client.
- 8 Click **Connect**.
- 9 If a prompt appears warning that a program is executing, click **OK** to continue.

---

## Saving Remote Control Session Settings

You can save the remote control session settings so that the next time you try to establish a remote session using the same remote service, Service Center remembers the settings that were last used.

Depending on the application, the following settings are saved:

- If the application launches a URL on the technician's computer, saving at the device level associates the URL with the device.
- If the application launches on the technician's computer, saving at the device level associates the local application path with the Service Center user.
- If the application launches a URL on the client computer, saving at the device level associates the URL with the device.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to initiate a remote control session.
- 3 Click the device name and then click **Remote Control** from the right sidebar.
- 4 Do one of the following:
  - To save the settings, click **Save**.
  - To put the settings back to what they were before you made any changes, click **Restore**.
  - To put the settings back to the default settings, click **Restore System Default**.

## Working with the Remote Tools

### About Remote Tools

Managed Workplace provides many remote tools to make fixing problems on customer computers easier. These tools are real-time and can be used without interfering with the user's session.

---

Use the remote tools to create real-time remote sessions on any WMI-enabled Windows device monitored by the Onsite Manager or with a Device Manager installed.

### Remote Tools Requirements

**Important:** Both the target computer and the technician's computer must trust the SSL certificate in use by the Service Center and SCMessaging websites.

The target computer must have the following:

- Microsoft .NET Framework 3.5 or higher
- Ability to run automated scripts on the target device, which means it must be WMI-enabled and be able to access the \$ADMIN share

The technician's computer must have the following:

- a user account and role set up to have permissions to Remote Management Tools
- Silverlight-capable browser

### Notes:

- In Managed Workplace R2, the remote tools only worked on devices where a Device Manager was installed or on the Onsite Manager machine. Now, these tools work on any WMI-enabled device monitored by Onsite Manager.
- The remote tools are not supported on Windows 2000 computers since .NET 3.5 is required on the target device. Windows 2000 does not support .NET 3.5.

**Event Viewer** Use to view event logs that can be viewed via the local Event Viewer. This tool is useful for troubleshooting. See [Using Event Viewer](#).

**File Manager** Use to manage files on a user's computer. You can also use this tool to upload files from your computer to the target computer or download files from the target computer to your computer. See [Using File Manager](#).

**Local Users and Groups** Use to manage user accounts and groups on a user's computer. See [Using Local Users and Groups](#).

**Reboot Manager** Use to restart or shutdown a user's computer, including forced restart and shutdown. See [Using Reboot Manager](#).

**Process Explorer** Use to find software running on a computer (for example, a process associated with the operating system, a desktop session and so on). See [Using Process Explorer](#).

---

**Remote CMD Prompt** Use to start Windows command line interface (CMD.EXE), which enables you to list the contents of a directory or run commands such as ping, ipconfig, dir, netstat, among other things. See [Using Remote CMD Prompt](#).

**Screenshot** Use to capture a screenshot of the user's computer. See [Using Screenshot](#).

**Startup Manager** Use to manage the Windows startup procedure and control which programs to automatically start up for all users or individual users. See [Using Startup Manager](#).

**Windows Services Manager** Use to view services that are running on a user's computer. See [Using Windows Services Manager](#).

**Notes:**

- Managed Workplace allows unauthenticated proxy settings for remote communications.
- All communications between the target device and the technician's device can be secured through the use of HTTPS for SC Messaging.


## Using Remote Tools

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device on which you want to use the remote tools.
- 3 Click the device name and then click **Remote Tools** from the right sidebar.


**Tip:** To immediately use one of the remote tools, click the **Remote Control** icon, and then select the remote tool from the context menu.

 Remote Control icon

- 4 Select one of the tools by clicking a button or by selecting it from the drop-down menu.

 Remote Tools drop-down menu icon

**Tip:** To return to the **Home** page that shows all the remote tools, click the **Home** button.

 Home icon

---

## Using Event Viewer

Use Event Viewer for viewing event logs on a user's computer that can be viewed via the local Event Viewer. This can be useful for troubleshooting. Event Viewer displays detailed information about significant events (for example, programs that don't start as expected or updates that are downloaded automatically) on a computer. You can view the following event logs:

- Application
- Security
- System
- Custom Logs

## Using File Manager

Use to manage files on the local drives of a user's computer. Many operations support a single object (file or folder) at a time.

You can also use this tool to upload files from your computer to the target computer or download files from the target computer to your computer.

You can view and work with files and folders on any logical drive attached to the target system. Hidden files and folders are displayed as in Windows, and you can manipulate hidden and read-only attributes.

### Notes:

- The File Manager remote tool does not work for network-mounted drives.
- The File Manager remote tool shows 500 files or folders per page. Click the Load Next x Items in the status bar to page through the results.

### To upload a file from your computer to the target computer

- 1 Browse to the location on the target computer where you want the file to be uploaded.
- 2 In the file list window, click the **Upload** button.
- 3 Locate the file on your computer and click **Open**.
- 4 Click **OK**.

### To download a file from the target computer to your computer

- 1 In the file list window, select the file you want to download.
- 2 Click the **Download** button.
- 3 Locate where you want to download the file.

- 
- 4 In the **File Name** box, provide a name.
  - 5 Click **Save**.
  - 6 Click **OK**.

## Using Local Users and Groups

Use to manage user accounts and groups for the primary domain only.

### To create a new user

- 1 In the **User** tab, right-click and select **New User**.
- 2 Fill in the boxes.
- 3 Click **Create**.

### To set the password for a user

- 1 In the **User** tab, right-click and select **Set Password**.
- 2 Fill in the boxes.
- 3 Click **OK**.

### To rename a user

- 1 In the **User** tab, right-click the user and select **Rename**.
- 2 Type the new name and press **Enter**.

### To delete a user

- 1 In the **User** tab, right-click the user and select **Delete**.
- 2 Click **OK**.

### To view the properties of a user

- In the **User** tab, right-click the user and select **Properties** or double-click the user name.

### To create a new group

- 1 In the **Groups** tab, right-click and select **New Group**.
- 2 Fill in the boxes.
- 3 Click **Create**.



---

### To rename a group

- 1 In the **Groups** tab, right-click the group and select **Rename**.
- 2 Type the new name and press **Enter**.

### To delete a group

- 1 In the **Groups** tab, right-click the group and select **Delete**.
- 2 Click **OK**.

### To view the properties of a group

- In the **Groups** tab, right-click the group and select **Properties** or double-click the group name.

### Using Reboot Manager

Use to restart or shutdown a user's computer, including forcing a restart or shutdown.

A forced restart or shutdown does not allow the end user to save their work; a regular restart or shutdown asks the user to save their work before performing the action.

### Using Process Explorer

Use to find software running on a computer (for example, a process associated with the operating system, a desktop session and so on).

A summary is displayed above the list that shows total processes, CPU usage and memory usage.

Managed Workplace polls for data every 5 seconds.

**Note:** The Process Explorer shows processes running for all users.

**Tip:** You can reorder the columns using drag and drop.

### To end a process

- Right-click the process and select **End**.

### To find out more information about a process

- Right-click the process and select **Google**.

---

## Using Remote CMD Prompt

Use to start Windows command line interface (cmd.exe), which enables you to list the contents of a directory or run commands such as ping, ipconfig, dir, netstat, among other things.

You cannot use this tool to interact with applications that run outside the shell. As well, you cannot use this tool to interact with an application that takes over the shell, such as PowerShell or wmic.exe. Also, because the prompt is inside a browser window, you cannot use the Tab key to auto-complete object names since control will pass to another part of the browser.

**Note:** The Remote CMD Prompt remote tool cannot open a command prompt as an administrator. It will run under nt authority\system.

## Using Screenshot

Use Screenshot to capture a screenshot of a user's desktop, which you can use to do things like get a quick view of a user's error message or see if anyone is using the computer to determine if you can reboot it. It also shows who was last logged in and when.

### Notes:

- If the user has multiple monitors, then the screenshot will only be taken of the primary monitor (that is, the one with the **Start** menu).
- If a user is remotely logged in via RDP, then the screenshot is taken of the active session.
- If the user locked the desktop, it will still show the screenshot of the desktop (not the locked screen).
- If nobody is logged in, then no screenshot is shown.
- If there is no active desktop on a device where you're trying to use the Screenshot remote tool, you'll see the following error:

Could not obtain screenshot.

Try again at a later time or contact the end user.

## Using Startup Manager

Use to manage the Windows startup procedure and control which programs to automatically start up for all users or individual users.

**Note:** A user-specific startup item can be enabled for all users.

---

### To view the startup items for a specific user

- From the **User** list, select the user for which you want to see the startup items.

### To find out more information about a startup item

- Right-click the startup item and select **Google**.

### To enable or disable a startup item for a specific user

- 1 From the **User** list, select the user for which you want to see the startup items.
- 2 Select the check box for the startup item you want to enable or disable.
- 3 Click **Apply**.

### To enable or disable all startup items

- 1 Click either **Enable All** or **Disable All**.
- 2 Click **Apply**.

### To enable or disable a startup item for all users

- 1 From the **User** list, select **All**.
- 2 Select the check box for the startup item you want to enable or disable for all users.
- 3 Click **Apply**.

## Using Windows Services Manager

Use to view services that are running on a computer.

### To start, stop, pause, resume or restart a service

- Right-click the service and select one of the options.

### To view the properties of a service

- Right-click the service and select **Properties**.

---

## Disconnecting from the Target Device

- Click the **Disconnect** button.



Disconnect icon

When you click the **Disconnect** button, the **Remote History** page displays.

**Default:** Managed Workplace automatically disconnects after five minutes of idle time.

When you click **Remote Tools** from the right sidebar, Managed Workplace starts a timer that keeps track of how long the Remote Tools are in use and what tools were used during the session. You can use this information to keep better track of time spent in assistance. This data is displayed in the **Remote History**.

## Viewing the Remote History

Use the remote history to see information about previous remote sessions. This page shows the user account that initiated the remote option, what remote tool was used, when the session started and the duration of the session.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to view the remote session history.
- 3 Click the device name and then click **Remote History** from the right sidebar.

If you want to see more details about a specific session, click the chevron (>) beside the initiator.

## Adding a Note to a Remote Session

You can add a note to a remote control or remote tool session to provide information about the work that was completed.

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to view the remote session history.
- 3 Click the device name and then click **Remote History** from the right sidebar.
- 4 Click the pen icon in the **Notes** column.

- 
- 5 In the **Session Notes** area, type the note text.
  - 6 Click **Save**.

## Edit a Remote Session Note

- 1 In Service Center, click **Status > Devices**.
- 2 Locate the device to which you want to view the remote session history.
- 3 Click the device name and then click **Remote History** from the right sidebar.
- 4 Click the note icon in the **Notes** column.
- 5 In the **Session Notes** area, edit the note text.
- 6 Click **Save**.

## Troubleshooting Remote Connections

Here is an explanation of some common error messages you may receive when attempting to establish a remote connection:

**OM Server Not Available** The MWExpertSystem and OMNetworkService services are not properly responding on Onsite Manager. Restart the services and attempt to connect again.

**A connection attempt failed because the connected party did not properly respond after a period of time, or established connection failed because connected host has failed to respond.** The target device has not been configured to accept incoming remote sessions from the Onsite Manager computer. Enable the remoting options on the target device and attempt to connect again.

## Using Onsite Manager Utilities

The Onsite Manager Utilities enable you to manage remote computers without affecting the logged in user.

### Notes:

- Onsite Manager Utilities do not work with Device Manager.
- If a WMI-enabled device has a credential management override, then Onsite Manager Utilities will not have access to the device, resulting in greyed-out functionality. If this occurs, you can verify that a credential

---

override has been applied to the device in the Credentials tab in Site Management. See [Managing Site Credentials](#).

For example, you can run network diagnostic tests such as Ping Device and Trace Route to Device, perform remote management and troubleshooting tasks using Registry Editor or computer management, or take control of the remote computer using the Command Prompt, all without affecting the user that is logged into the remote computer.

**File Explorer** Allows you to view, delete or modify files on any remote Windows computer.

**Event Viewer** Allows you to view and manage the Windows Event Log for the remote computer.

**Windows Services** Allows you to view, stop, restart or edit the properties of any services installed on the remote computer.

**Task Manager** Allows you to view running processes and user sessions on the remote computer and investigate process session ID information via a built in Google search.

**Registry Editor** Allows you to view, delete, or modify the registry of any remote Windows computer.

**System Information** Allows you to quickly obtain the system information from any Windows computer including uptime statistics, boot information, page file statistics, for example.

**IP Config/all** Displays the current network configuration for every interface on a Windows computer.

**Trace Route to Device** Performs a trace route from Onsite Manager to any remote device to help troubleshoot networking problems.

**Ping Device** Performs a ping from Onsite Manager to any remote device.

**Telnet** Uses the default Windows Telnet client to connect to devices supporting this protocol.

**Remote Shell** Launches a remote DOS session on any Windows computer.

**Reboot** Instructs a Windows computer to reboot.

**Shutdown** Instructs a Windows computer to power down.

To help you troubleshoot multiple devices, you can launch one utility or more utilities for any device, and you can connect to multiple devices at one time.

**Caution:** The existing Windows Service Account used for monitoring is leveraged to enable remote access to the utilities that apply only to Windows, such as Remote DOS, System Information, and Registry Editor. So, the Service

---

Account must have full Administrator access to the Domain, including remote logon, with no restrictions.

### **To establish a remote session to use the Onsite Manager Utilities**

- 1** In Service Center, click **Status > Devices**.
- 2** Click the **Site** or **Service Group** button and corresponding selection list entries to show the site or group that has the device with which you want to establish a remote session.
- 3** Click the **Device Name**.
- 4** Click **Remote Control** on the right sidebar.  
If an Internet Explorer dialog box appears, warning you that the page is accessing information that is not under its control, click **Yes**.
- 5** In the **Remote Services** section, from the **Service** list, select **Onsite Manager Utilities**.
- 6** In the **Onsite Manager Utilities Configuration** section, confirm the Remote Machine IP address is correct.
- 7** Click **Connect**.
- 8** In the main menu on the left side of the window, click a tool name.
- 9** When you are done using the Onsite Manager Utilities, click **Close** to close the window.





# CHAPTER 17

## MANAGING PATCHES

---

*This section provides detailed information about the following topics:*

- *Patch Management*
  - *Understanding the Default Patch Management Settings*
  - *Setting Up Patch Management in Managed Workplace*
  - *Reviewing Updates*
  - *Approving Updates*
  - *Stopping Patch Management*
-

---

## About Patch Management

Patch management involves acquiring, testing, and installing updates on a managed computer.

The goal of patch management is to create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

By using patch management, you can

- control updates to Microsoft applications and operating systems
- increase security on the client-side network against known vulnerabilities in operating system and application software
- ensure standard patch levels across managed systems
- automate the updates to ensure security

You can set up patch management so that it's completely automated, or you can set up controls so that you can test patches before approving them. The decision is up to you about how automatic or manual you want patch management to be.

### Notes:

- Patch management is not supported when devices are connected over VPN. If you have devices at separate locations for a single customer, we recommend that you deploy an Onsite Manager for each site, or that you deploy Device Managers.
- The terms *patch* and *update* are interchangeable.

### Understanding Patch Management

Managed Workplace duplicates the management model of Windows Server Update Services (WSUS) for all Microsoft updates. When you make decisions about what to do with patches for groups of computers, the native Windows functionality handles the installation based on rules you set in the Patch policies (see [What is a Patch Policy?](#)).

Computers with Device Manager installed receive information about patches from Service Center and download the files from Microsoft Update directly (see [What is Microsoft Update?](#)). End users will see notifications and messages from Service Center.

**Note:** All non-Microsoft software updates are handled through automation only. For example, to update Adobe products, you can use the built-in Ninite scripts. Go to **Automation > Library** and search for "Install or Update" for a list of scripts provided with Managed Workplace for updating software.

---

## Synchronizing Updates

Microsoft updates are differentiated by product (or product family) and classification.

**Product** A product is a specific product or product family from which the individual product is derived. For example, Microsoft Windows is a product family from which Windows Server 2003 is a member. You can get updates for current and future versions of the product.

**Classification** A classification is the type of update. For any given product or product family, updates could be available among multiple update classifications (for example, Windows XP family Critical Updates and Security Updates). Microsoft provides critical and security-related patches on the second Tuesday of the month and non-security patches on the fourth Tuesday.

### What is a Patch Policy?

A patch policy is a collection of rules that manages updates on devices or groups.

When a patch policy is first applied to a device, it will check into the Onsite Manager to download a cookie, download an agent and upload its patch status. The device will check in with patch management in under an hour, if there are no communication or configuration issues.

Once patch management is enabled, a device will check in for any new instructions with the Onsite Manager or Service Center at least once every 22 hours.

### What is a Windows Update Agent?

A Windows Update Agent is included on all modern Microsoft operating systems so that updates can be managed by users or administrators. On an unmanaged device, the rules are provided through the Windows Control Panel. Using Managed Workplace, the rules are provided through Patch policies.

### What is Microsoft Update?

Microsoft Update is a repository that provides downloadable updates for Microsoft operating systems and applications. Microsoft Update works with updating software in Windows. The updating software identifies which version of Windows and other Microsoft products is being used on the device.

**Note:** Windows Update is the classic update service that only offers updates for Windows. Microsoft Update extends this service to cover other Microsoft programs.

---

For more information about Microsoft Update, visit the [Microsoft website](#).

### **Prerequisites for Patch Management**

Devices that you want to patch manage must be WMI-enabled.

On Domain networks, WSUS-related Group Policy Object (GPO) must be set to Not Configured since Managed Workplace does not use GPO settings to define the update server for managed clients. Any WSUS policies that are in place on the Domain will interfere with the normal operations of patch management.

## **Understanding the Default Patch Management Settings**

Whether you are using Managed Workplace for the first time, or you have upgraded from a previous version, patch management in Service Center includes default settings that you can use to get up and running with patch management quickly and with minimal configuration.

**Note:** In previous versions of Managed Workplace, there was an **Initial Setup** wizard in the **Patch Management** menu that you had run through to configure your patch management settings. With Managed Workplace 10.0 this wizard is no longer required, as Managed Workplace is pre-configured with some standard patch management defaults.

So what are some of the standard patch management settings in Managed Workplace?:

- By default, patch management is set up to manage all Windows products, and to include security updates and critical patches;
- Managed Workplace includes two pre-built patch policies; one for Windows Workstations and one for Windows Servers. For more information, see [Understanding the Pre-Built Patch Policies](#).

Any of these settings can be modified to suit your unique patching needs.

---

## Understanding the Pre-Built Patch Policies

Managed Workplace includes two pre-built patch policies that are configured to patch manage Windows workstations and Windows servers. You can use these patch policies as-is, or you can modify the settings as needed.

The following table provides an overview of the two patch policies available in Managed Workplace:

Patch Policy	Description
Microsoft Windows Server Patching	<ul style="list-style-type: none"><li>• set up to notify for download and notify for install so nothing is downloaded or installed without your explicit approval</li><li>• do not install minor updates silently</li><li>• when devices are added to this policy, they are also automatically added to the Unassigned Computers approval group</li><li>• automatic inclusion rules pre-set to include devices that are servers, WMI-enabled, but do not 2000 or 2003 in the OS name</li></ul>
Microsoft Windows Workstation Patching	<ul style="list-style-type: none"><li>• set up to notify for download and notify for install so nothing is downloaded or installed without your explicit approval</li><li>• do not install minor updates silently</li><li>• when devices are added to this policy, they are also automatically added to the Unassigned Computers approval group</li><li>• automatic inclusion rules pre-set to include devices WMI-enabled, but to exclude servers</li></ul>

To activate patch management using one of these policies you must:

- 1 Add the policies to a service or service plan, or apply the patch policies directly to a device or group of devices. See [About Service Plans](#).
- 2 Approve the patches for installation. You can do this automatically by setting up approval rules, or you can approve patches and groups of patches manually. [Approving Updates for Installation](#) and [Automatically Approving Updates for an Approval Group](#).

---

To set up patch management for a device, follow these steps:

- 1 You discover a new device that isn't patch managed.
- 2 Does a patch policy exist that can be applied to this device? If not, create a patch policy. Set the rules and apply the policy to the device, which can be done through services and service plans, or by applying the policy directly to the device. See [Creating a Patch Policy](#).
- 3 When a patch policy is first applied to a device, Onsite Manager will configure the Windows update agent on the target device so that the device becomes patch managed by Managed Workplace. The target device will report patch status to Managed Workplace within the detection frequency timeline as defined within the Windows update agent.
- 4 Optionally, configure which Microsoft updates to synchronize, where updates are stored and how often to check for updates. See [Setting Which Microsoft Updates to Synchronize](#), and [Setting Whether to Store Updates Locally or Not Locally](#).
- 5 Optionally, you can set up automatic approval, such as automatic approval for revisions to patches that you've already approved for installation. See [Automatically Approving Updates for an Approval Group](#).

### Process for Approving Patches

To approve a patch, follow these steps:

- 1 Microsoft releases patches on a weekly basis, usually on Tuesdays. Some patches, notably definition updates or critical security patches, may be released more frequently. Check the **Patch Management Overview** page once or twice a day for new patches not yet approved.
- 2 Review the patches available in the **Patch Approval** window and research the update. See [Reviewing Updates](#).
- 3 Do you want to approve the update? Is it applicable for all computers? If not, do you need to approve it for a subset of computers? If so, you need an approval group that includes that subset. See [Creating an Approval Group](#).
- 4 By default, patches are set to be Not Approved. You can set how you want to handle the patch: approve for installation (Install), approve for removal, decline or leave as Not Approved. See [Approving Updates](#).
- 5 Once a decision about the patch has been set, the action is retrieved by all Onsite Managers and Device Managers.

When patch caching is enabled, the patch is downloaded to the update cache folder on the Onsite Manager machine only if the approved patch is

---

needed by a device at the site. The settings in the patch policy define how and when an approved patch is installed.

Device Managers configure Windows with the settings in the patch policy, and a helper application downloads needed patches directly from Microsoft. Based on the choices made when configuring a patch policy, users on the Device Manager computer may or may not be notified about download or installation activity. If they are notified, the user can select which patches to download and install.

## Setting Up Patch Management in Managed Workplace

Follow these steps to set up Patch Management in Managed Workplace:

- 1 Set up a patch policy, if you are not using one of the pre-built patch policies. See [Creating a Patch Policy](#).
- 2 Add the patch policy to a service for use in a service plan, or apply it manually. See [Creating Services](#).
- 3 Optionally, set up an execution schedule for the patch policy to use. See [Setting Up Execution Schedules](#).
- 4 Set up approval groups. See [Setting Up Approval Groups](#).
- 5 Set up synchronization options. See [Setting Synchronization Options](#).
- 6 Set automatic approval options. See [Automatically Approving Updates for an Approval Group](#).

## Creating a Patch Policy

A patch policy is a collection of rules that manages updates on devices.

### What You Can Do

You can

- specify how frequently the patch managed device will check for new updates
- specify the time frame in which updates are installed after they are downloaded
- specify whether users are prompted for updates to be installed or if updates are installed automatically
- specify the reboot behavior after the update has been applied

- 
- specify to which devices the patch policy applies through automatic application rules, or by selecting specific devices and groups

Patch policies also determine to which devices the policy is applied. You can set up automatic inclusion rules, or manually apply a patch policy to devices and groups. Note that automatic inclusion rules only take effect when the patch policy is included as part of a service delivery model (i.e., added to a service or service plan that is then applied to a site or group).

You can create as many patch policies as you require.

**Note:** If a device is included in more than one Patch policy, the Patch policy with the lowest detection frequency is applied to the device. If both policies have the same detection frequency, the policy that was created first is applied.

### To create a patch policy

- 1 In Service Center, click **Configuration > Policies > Patching**.
- 2 Click **New**.
- 3 In the **Create New Policy** section, type a name and description for the policy.
- 4 Click **Create**.
- 5 Click the **Settings** tab, and click **Modify**.
- 6 From the **Detection Frequency** list, select how often you want the devices to check for new patches.

The default 22 hours is good for almost all circumstances. You may want to have devices that receive definition updates check more frequently.

- 7 In the **Automatic Updates Options** section, select one of the following option buttons:

**Notify for download and notify for install** Local users will be notified in the notification area (System Tray or Notification Area) that updates are ready to be downloaded/installed.

**Auto download and notify for install** Updates will be automatically downloaded and local users will be notified in the notification area (System Tray or Notification Area) that updates are ready to be installed.

**Auto download and auto install** Updates will be automatically downloaded and installed.

**Automatic updates options configurable on clients managed by Onsite Managers** Local users may adjust the update settings in Windows.



---

**Note:** The **Automatic updates options configurable on clients managed by Onsite Managers** option is not permitted for managed devices with a Device Manager installed. When a Patch policy with this setting is applied to these devices, **Notify for download and notify for install** are used instead.

- 8 If you selected the **Auto download and auto install** option button, do the following:
  - a To have the Patch policy use an execution schedule to schedule patches, select the **Install as per applicable Execution Schedule** option button. For more information about execution schedules, see [Setting Up Execution Schedules](#).
  - b To have the Patch policy override any execution schedules applied to a site or group, select the **Override Execution Schedules option** button. For more information about overriding the execution schedule, see [To set up a patch schedule that overrides any applicable execution schedules](#).

**Note:** If you select the **Install as per applicable Execution Schedule** option, and there is no execution schedule applied, patch management will default to the **Notify for download and notify for install** option.

- 9 Select the **Immediately install minor updates (updates that do not interrupt Windows services or require a restart)** check box to have updates installed immediately if they do not interrupt Windows services or require a restart.
- 10 Select the **Allow non-administrative users to approve or decline updates on clients managed by Onsite Managers** check box to allow regular users to select updates to install.
- 11 In the **Approval Group Assignment** section, do any of the following:
  - Select the **Assign the newly added devices of this Patch Policy to the following Approval Group** check box to automatically add all devices that will get applied to this policy to an approval group that you select from the list. This option helps you facilitate the installation of patches by automatically approving patches for the devices in this policy.
  - Optionally, select the **Apply changes to existing devices in this policy** check box to add the existing devices in this policy to the approval group that you selected.
- 12 Click **Save**.

---

## To set up a patch schedule that overrides any applicable execution schedules

When setting up a patch policy, you can indicate that the policy uses the applicable execution schedule that was set up for the site or group to which the devices in the policy belong. If you do not want to use the applicable execution schedule, you can override it and create a custom patching schedule within the policy.

You may want to override execution schedules if you have special requirements for your patching schedule. For example, you may have set up an execution schedule for a customer site that takes place Friday evenings at 8pm. However, for patching, you might want to set up your patching to occur the day after Microsoft releases patches, which typically occurs on the first Tuesday of every month. Overriding execution schedules grants you the flexibility to create a patching schedule that meets your specific patching requirements.

To set up a custom patching schedule, you must select the **Auto download and auto install** option when setting up the **Automatic Update Options** for the policy.

- 1 In Service Center, click **Configuration > Policies > Patching**.
- 2 Click **New** to create a policy, or click the name of an existing policy.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Automatic Update Options** area, select **Auto download and auto install** from the list.
- 6 Select the **Override Execution Schedules** option button.
- 7 In the **Start Time** box, type a start time for when patching will begin. Alternatively, you can click the clock icon to select a time from the list.
- 8 In the **Recurrence Pattern** area, select whether you want patches to run daily, weekly, or monthly.
- 9 In the Reboot Options section, select an option:
  - To allow the operating system to determine the reboot behavior, select **Use operating system default behavior**. The behavior will vary by operating system.
  - To wait until the user is logged off to reboot, select **Do not auto-reboot when a user is logged on**.
  - To reboot immediately when the update requires, select **Force a reboot when an update requires one**.

- 
- Important:** Some Microsoft updates will cause a server to reboot if you choose the **Do not reboot** option button. This behavior does not come from Managed Workplace, but is native to Windows. AVG recommends reading all details of a patch before applying it to a server.
- 10** If you selected the **Auto reboot after installation** option, set the following reboot prompt settings:
    - a** In the **Prompt to reboot after** list, specify a time after which a prompt will appear on the device.
    - b** In the **Repeat prompt to reboot every** list, specify in minutes how often to repeat the prompt.
  - 11** In the **Missed Installation Options** area, select the **wait X minutes after the next system startup to install** option button and enter a value for X in minutes between 1 and 60, or select the **wait until next scheduled time to install** option to define how missed installations are handled.
  - 12** Select the **Immediately install minor updates** check box to automatically install updates that do not interrupt Windows services or require a restart.  
**Note:** This option does not apply to Windows 10 or Windows Server 2016.
  - 13** Select the **Allow non-administrative users to approve or disapprove deposes on clients managed by Onsite Managers** check box to allow end users do not have an administrative role to approve or disapprove updates on devices managed by Onsite Manager.  
**Note:** This option does not apply to Windows 10 or Windows Server 2016.
  - 14** Click **Save**.

## Applying Patch Policies

### Creating Rules to Automatically Include Devices

Automatic approval rules determine which devices are eligible to have the patch policy applied. For example, if you are creating a patch policy for workstations only, you can set up an automatic approval rule to exclude devices with the word “server” in the OS name.

The approval rules do not come into effect until the patch policy has been applied, either by adding it to a service and then applying the service to a group or site, or by adding it to a service in a service plan, which can also be applied to a group or site.

The process for setting up approval rules is the same for patch policies as it is for all other policy types (i.e, monitoring, automation, and AVG AntiVirus). For more detailed instructions on setting up automatic approval rules, including examples, see [Creating Automatic Inclusion Rules for a Monitoring Policy](#).

- 
- 1 In Service Center, click **Configuration > Policies > Patching**.
  - 2 Click the name of the patch policy to which you want to create an automation inclusion rule.
  - 3 Click the **Automatic Application** tab.
  - 4 Create the automatic inclusion rule by clicking **Add** to create a rule.
  - 5 Repeat step 4 until the rule is complete.
  - 6 Click **Save**.

### Adding Devices or Groups to a Patch Policy

- 1 In Service Center, click **Configuration > Policies > Patching**.
- 2 Click the name of the patch policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following to apply the patch policy to a group or device:
  - In the **Applied Groups** area, click **Add**. Filter on the Group Type, if desired. Click the group and click **OK**.
  - In the **Applied Devices** area, click **Add**. Filter the list of devices. Select the check box beside the device and click **OK**.

**Note:** You can view the patch policies applied to service and site groups on the **Groups** page, by going to **Configuration > Groups**, clicking the group name, and then clicking the **Policies** tab. For more information, see [Viewing the Policies Applied to a Group](#).

### Removing Devices or Groups from a Patch Policy

- 1 In Service Center, click **Configuration > Policies > Patching**.
- 2 Click the name of the patch policy to which you want to add devices or groups.
- 3 Click the **Manual Application** tab.
- 4 Do one of the following:
  - To select one device or group at a time, select the check box that corresponds with each device you want to remove.
  - To select all the devices or groups at once, select the check box at the top of the column.
- 5 Click **Remove**.

---

## Excluding Devices from a Patch Policy

You can exclude specific devices from a patch policy. When you add a device to the exclusion list, it will never have this patch policy applied, even if the device meets the criteria outlined in the automatic application rules, and the patch policy is applied to the site or group to which the device belongs.

- 1 In Service Center, click **Configuration > Policies > Patching**.
- 2 Click the name of the patch policy from which you want to exclude devices.
- 3 Click the **Excluded Devices** tab.
- 4 Click **Add**.
- 5 Use the filters at the top to narrow your selection, and click **Filter**.
- 6 Select the check box beside each device you want to exclude from the policy.
- 7 Click **OK**.
- 8 Click **Save**.

**Tip:** You can exclude multiple devices in a site or group by selecting **Site** or **Group** from the **Filter By** list, and then selecting the check box at the top of the list of returned devices to exclude all devices listed.

## Renaming a Patch Policy

- 1 In Service Center, click **Configuration > Policies > Patch**.
- 2 Click the name of the patch policy that you want to edit.
- 3 Click **Modify**.
- 4 Type a new name in the **Policy Name** box.
- 5 Click **Save**.

## Deleting a Patch Policy

When you delete a patch policy, you are removing patch management from any devices that have the policy applied. If this patch policy has been included in a service, you should first ensure the service has another patch policy included before deleting this patch policy.

- 1 In Service Center, click **Configuration > Policies > Patch**.
- 2 Select the check box beside the patch policy you want to delete.
- 3 Click **Delete**.

---

## Setting Up Approval Groups

An approval group is a container for devices against which you either manually or automatically approve updates.

There are two default approval groups:

**All Computers** Contains every managed device reporting into patch management.

**Unassigned Computers** Contains every managed device belonging to the All Computers approval group and no others. Devices are automatically put in this group when a Windows Update Agent Policy is first applied. They will remain there until they are moved to another approval group.

**Note:** A device can only belong to one approval group in addition to the All Computers approval group.

### Why Use an Approval Group?

Use approval groups for testing patches, restricting installation of patches and controlling the installation of patches.

Approval groups can also be used to set up automatic approval. See [Automatically Approving Updates for an Approval Group](#).

Although creating your own approval groups is optional, they ease management because you work with greater numbers of similar devices at one time. It also simplifies keeping a standard update level across your client base so technicians are always working on similarly updated operating systems and applications.

### What You Can Do

You can

- create an approval group to apply patches to a subset of All Computers
- move devices between approval groups
- set up automatic approval for specific approval groups
- apply different patch approval settings for each approval group
- delete an approval group you no longer use

**Best Practice:** Don't use automatic approval for higher risk devices. The time it takes to manage patches is minimal when using approval groups, so it isn't worth the risk.

---

### Example 1

For example, you can create an approval group called Critical Servers and another one called Workstations.

- New patches for the Critical Servers approval group can be set to Not Approved until you have tested them on non-production devices and confirmed their quality.
- New patches for the Workstations approval group can be set to Install.

### Example 2

If you have an approval group that contains a 2008 Server, a 2003 Server with Exchange 2007 and an XP desktop and you approve an Exchange 2007 patch, only the system that needs the patch will install the patch.

### Example 3

If you have a site where Internet Explorer 9 is installed, then the OEM software user at the site will crash. You can create an approval group called “Do not approve IE9” or another logical name, move the patch managed devices affected into this approval group and never approve IE9 for that approval group.

### Example 4

You can use approval groups to control the installation of .NET patches. Devices sometimes have problems after installing .NET updates. When you want to install .NET patches, you can move selected devices into a .NET approval group. When the installation is complete, you can verify that the devices have no problems and then move the devices out of the .NET approval group.

## Creating an Approval Group

- 1 In Service Center, click **Patch Management > Settings > Approval Groups**.
- 2 Click **Add**.
- 3 Type a name for the new approval group.

**Note:** Approval group names cannot contain special characters ("~!@#\$%^&\*()=+[]{}|:;' "<>/).

- 4 Click **Add**.

This approval group is empty. Next, you must move devices into this approval group.

---

## Moving Devices into an Approval Group

Devices can only belong to the All Computers approval group and one other approval group.

What If...	Then...
A device is moved into an approval group	The computer will end up with all the approved updates for that group. If they are installed, they do not need to be re-installed. If they are still needed, they will be installed.
A device is moved into an approval group that does not allow installs for a patch it already has	It will not remove any updates that are already installed.

- 1 In Service Center, click **Patch Management > Settings > Approval Groups**.
- 2 From the **Approval Group** list, select the approval group that contains the devices you want to move.
- 3 Do one of the following:
  - To select one device at a time, select the check box that corresponds with each device you want to add to the approval group.
  - To select all the check boxes at once, select the check box at the top of the column.
- 4 Click **Move selected devices**.
- 5 From the drop-down list, select the approval group to which you want to move the devices.
- 6 Click **OK**.

The devices now belong to the All Computers approval group and this approval group.

## Deleting an Approval Group

When you delete an approval group, all devices that were members of the group are automatically moved into the Unassigned Computers approval group.

**Note:** You cannot delete the All Computers or the Unassigned Computers approval groups.



- 
- 1 In Service Center, click **Patch Management > Settings > Approval Groups**.
  - 2 From the **Approval Group** list, select the approval group that you want to delete.
  - 3 Click **Delete**.

## Setting Synchronization Options

This section covers the following topics:

[Setting Which Microsoft Updates to Synchronize](#)

[Setting Whether to Store Updates](#)

### Setting Which Microsoft Updates to Synchronize

You can set

- which products to patch manage
- which patch classifications to download

Changes to the **Products** and **Classifications** settings are applied to all patch managed sites and become the default for any new sites added to patch management.

#### To set which products to patch manage

The **Products** list displays which Microsoft products are currently supported by the Patch Management system. This is a global setting for all sites, so any product that is needed by any site must be configured here.

- 1 In Service Center, click **Patch Management > Settings > Synchronization**.
- 2 To add or remove products, under **Products**, click **Change**.
- 3 Do the following:
  - Select the check box for any listed products for which you want to start managing patches.
  - Clear any check boxes for any products for which you want to stop managing patches.
- 4 Click **Save**.
- 5 Click **Save**.

---

## To set which classifications to download

The **Classification** list displays which Microsoft classifications are currently supported by the Patch Management system. This is a global setting for all sites, so any product that is needed by any site must be configured here.

- 1 In Service Center, click **Patch Management > Settings > Synchronization**.
- 2 To add or remove classifications, under **Classifications** click **Change**.
- 3 Do the following:
  - Select the check box for any listed classifications for which you want to start managing patches.
  - Clear any check boxes for any classifications for which you want to stop managing patches.
- 4 Click **Save**.
- 5 Click **Save**.

## Setting Whether to Store Updates Locally or Not Locally

You can set whether the updates are downloaded on an as-needed basis from Microsoft Update or stored locally (cached) on Onsite Manager. Regardless of whether you download on an as-needed basis, or download to the Onsite Manager cache, only the patches that are required are downloaded.

The choice is a trade-off between disk space and Internet bandwidth used to do the patching.

For example, in a country where bandwidth is not metered significantly (such as Canada), you may not want to store them locally if space on Onsite Manager is at a premium. However, in a country where bandwidth is metered significantly (such as Australia or South Africa), you may want to download only one copy of each patch to save your client's bill for downloads.

**Note:** You need at least 40 GB free space for storing Microsoft updates if storing patches locally. If the cache directory path that you specify does not have 40 GB free space, you will receive an error message and must select a different cache directory.

When you store updates locally for a site, you can specify the drive and path to use. When you store updates locally for all new sites, updates will automatically be stored on the drive with the most available space, using the path AVG Managed Workplace\Update Cache.

## To set whether to store updates locally or not locally

- 1 In Service Center, click **Patch Management > Settings > Synchronization**.

- 
- 2 In the **Site Options** section, using the **Site** list, do one of the following:
    - Select the site to configure.
    - Select **New Site Defaults** to set the initial configuration for patch management for new sites.
  - 3 Do one of the following:
    - To not store the updates locally on Onsite Manager, select the **Store updates on Microsoft Update** option button.
    - To store the updates locally on Onsite Manager, select the **Store updates locally on Onsite Manger (Requires 40 GB of disk space)** option button.

**Note:** If you are storing updates locally for a site, under **Storage**, you can specify the **Drive** and **Path** to use if you do not want to use the default provided.
  - 4 Click **Save**.

## Reviewing Updates

This section covers the following topics:

[Viewing an Overview of Patch Management](#)

[Viewing Patches](#)

[Viewing Patch Status](#)

## Viewing an Overview of Patch Management

The **Patch Management Overview** window provides a summary of the approval settings for available Microsoft Updates and the number of devices being patch managed. Additionally, the overview provides a checklist of actions that are waiting to be taken in the form of a to do list.

The approval of a patch is always reflected immediately on the **Overview** page. However, the **Status** (**Installed**, **Failed**, **Needed**, and so on) comes from Onsite Manager and is updated within the hour.

**Tip:** You may want to set up an alert that notifies you if a server requires a reboot after installing a patch. See [Adding a Monitor for Patch Status](#).

- In Service Center, click **Patch Management > Overview**.

Here is a summary of what you see in the **Patches** section:

---

**Approved - Install (Including Mixed)** The number of Microsoft Updates that have any approval status other than Declined. If you want more information about the approved patches, click the corresponding number to display the **Patch Approval** window.

**Approved - Remove (Including Mixed)** The number of Microsoft Updates that have been approved for removal. If you want more information about the approved patches, click the corresponding number to display the **Patch Approval** window.

**Approved - Mixed** The number of Microsoft Updates that have different approval statuses in different patch policies. If you want more information about the approved patches, click the corresponding number to display the **Patch Approval** window.

**Patches Declined** The number of Microsoft Updates that have an approval status of Declined. If you want more information about the patches that have been declined, click the corresponding number to display the **Patch Approval** window.

**Patches Not Approved** The number of Microsoft Updates that have not been approved. After Patch Tuesday, it's a good idea to check this item to see if there are any patches to review and approve. If you want more information about patches that have not been approved or if you want to approve them, click the corresponding number to display the **Patch Approval** window.

**Patches Failed** The number of Microsoft Updates that have failed to install. If you want more information about the failed patches, click the corresponding number to display the **Patch Report** window.

**Patches Needed** The number of updates that are needed by managed devices. Updates that are needed will be installed automatically if the agent policy is set to do that.

Based on the synchronization settings that tell Managed Workplace what patches to look for, Managed Workplace communicates with update services to check whether the update is needed by the computers it's managing. Critical Updates and Security Updates are automatically approved for detection.

**Total Computers** The number of devices that are being patch managed.

**Computers with Patch Errors** The number of devices that have experienced errors while attempting to install the Microsoft Updates. If you want to see more information about the computers with patch installation errors, click the corresponding number to display the Managed Device Report window.

---

**Computers Needing Patches** The number of devices that need Microsoft Updates approved for the installation to occur. If you want to see more information about the computers that need patches installed, click the corresponding number to display the **Device Report** window.

**To Do** Keeps track of actions that have to be performed and are required for effective operations. Refer to the list on a daily basis to ensure your customers have access to the most current Microsoft Updates.

## Viewing Patches

All available patches are listed in the **Patch Approval** window filtered according to the options set at the top.



This patch supersedes other patches. Before declining superseded patches, it is recommended that you approve the superseding patch first and verify that the superseded patches are no longer needed by any computers.



This patch is superseded by another patch. Before declining superseded patches, it is recommended that you approve the superseding patch first and verify that the superseded patches are no longer needed by any computers.



This is a WSUS patch and should be approved for installation to ensure computers can be updated correctly.



This patch has expired. An expired update is an update that has been invalidated by Microsoft. An expired update can also be an update that has been superseded by the release of another update (new or revised) that fixes or enhances functionality or applicability offered by the expiring update. In this case, the superseding update should be approved in place of the expired update. An update that is expired can no longer be approved for detection or installation.

### What You Can Do


You can

- approve single patches or many patches at one time
- search for patches by title
- view all patches that are not approved
- view all patches released after a specified date

- 
- research what new Microsoft updates are available and approve them for use at your customer sites
  - use the filtering options to locate the patches on which you want to take action
  - set a deadline to force a patch to be installed by a specific date and time. Setting a deadline for a patch installation supersedes all other rules that may prevent the installation.

**Note:** You can set a deadline in the past to force immediate installs.

### To view available patches

- 1 In Service Center, click **Patch Management > Patch Approval**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .

The **Advanced Filtering** section includes the following options:

**Products and Classifications** Shows the patches that match the product or classification type you select.

**Approval** Shows the patches that match the approval status (Install, Remove, Not Approved, Mixed, or Declined).

**Status** Shows the patches that are needed, failed, or are installed.

**Release Date** Shows the patches that have been released within the time frame that you select.

**Title Contains** Shows the patches that were declined for installation.

**Tip:** Use the **Release Date** filter when you want to see released patches based on a time period.

- 3 Click the patch title to see more details.

In the **Patch Details** window, you'll see detailed information about the patch.

**General Information** Provides general information and installation information about the selected patch, including links to Microsoft knowledgebase articles where you can find more information.

**Status** Provides the information about the selected patch with respect to each approval group.

**Revisions** Provides revision information about the patch.


---

## Viewing Patch Status

You can view

- patches for an approval group
- patches at a site
- patches based on a date
- all needed patches
- all failed patches
- all installed patches
- all unknown patches
- all patches that are not needed


### To view details about patches

- 1 In Service Center, click **Patch Management > Reports > Patch Report**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Use the filters to display only the patches for which you want to view details, and then click **Filter**.
  - To find out more details about the patch, click the name of the patch.
  - To see the computer that meets the filtering criteria, click the triangle beside the patch name.

**Note:** All devices and their patches appear in the list if the device has at least one patch that matches the selected status filter.

For example, if you filter the list by selecting **All Computers** from the **Approval Group** list and you select the **Failed** check box, the table could display a summary of patches with a status of Failed. When expanding the patch in the table, only the devices with the selected status appear.

### To view details about patches by device

- 1 In Service Center, click **Patch Management > Report > Device Report**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Filter the report as needed.
  - To find out more details about the device, click the name of the patch. See [Viewing Summary Details about a Device](#).


- 
- To see the patch or patches that meet the filtering criteria, click the triangle beside the computer name.

**Note:** All devices and their patches appear in the list if the device has at least one patch that matches the selected status filter.


## Run Patches on Devices Immediately

You can use the **Patch Report** and **Device Report** pages to immediately run patches on devices that require patching, or on which the previous patch has failed.

### To patch devices by filtering for patches that are needed or failed

- 1 In Service Center, click **Patch Management > Reports > Patch Report**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Filter the report by **Service Plan, Site, Approval Group, Release Date, Status (Installed, Needed, or Failed)**, and whether to **Hide Declined Updates**.
- 4 Click **Filter**.
- 5 Select the check box beside each patch you want to run. To run all failed or needed patches, select the check box in the header row.
- 6 Click **Patch Now**.

### To patch devices by filtering for devices that require patches

- 1 In Service Center, click **Patch Management > Reports > Device Report**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Filter the report by **Service Plan, Site, Approval Group, and Release Date**, and then select the **Installed, Needed or Failed** check boxes.
- 4 Click **Filter**.
- 5 Select the check box beside each device you would like to patch. To install all failed or needed patches for all devices, select the check box in the column header.
- 6 Click **Patch Now**.



---

## Approving Updates

This section covers the following topics:

[Approving Updates for Installation](#)

[Declining Patches](#)

[Approving Updates for Removal](#)


[Automatically Approving Updates for an Approval Group](#)

### Approving Updates for Installation

By default, patches are set to be **Not Approved**. If you don't approve a patch, it remains as **Not Approved**, which means it is effectively put on hold or ignored. In this case, the update will remain in the default list of available updates, but will not be installed.

You can approve the installation of updates for all the computers in your network or for different approval groups.

In the patches list, you can research what new Microsoft updates are available and approve them for use at your customer sites.

- 1 In Service Center, click **Patch Management > Patch Approval**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Do one of the following:
  - To select one patch at a time, select the check box of each patch for which you want to change the default approval setting.
  - To select all patches, select the check box in the column header.
- 4 Click **Change Approvals**.
- 5 Do one of the following:
  - To approve the update for all computers, from the **Approval** list select **Install**.
  - To approve the update for a specific approval group, in the Approval column, click the link and select **Install** from the list.
- 6 Do one of the following to set when the patch should be installed (Install has been selected from the Approval list):
  - To not set a deadline, ensure **None** is showing beside **Deadline**.

---

Depending on how often the agent policy is set to check for updates (the default is every 22 hours), the device will install a patch when it checks into update services and gets the instruction to do so. The deadline is used to force the patch to be installed by a certain time in the event that the **Notify for Download and Notify for Install** or the **Auto Download and Notify for Install** option button is selected in the patch policy and the local user on the box delays the operation when the notification pops up.

- To set a deadline but let users determine patch installation time, click **None** and ensure the **Use client settings to determine patch installation time** is selected and click **OK**.
- To set a deadline but specify a patch installation time, click **None** and select the **Install patch by the selected date and time**. Then select the date and time and click **OK**.

**Note:** You can set a deadline in the past to force immediate installs.

#### 7 Click **OK**.

The patches are dealt with in the order that they appear on the **Patch Approvals** page. If any patches require you to accept or decline an End User License Agreement (EULA), you will be prompted before the patch is approved for installation. For example, you want to approve these patches:

- a 7548456
- b 7589456 (EULA)
- c 7656585
- d 7636958 (EULA)
- e 7785483

If these patches are all selected and set for approved, then a, c and e would get approved, and then you would be prompted to accept the EULA for b and then d. If you decline the EULA for a patch, the patch is ignored in this round and put back in the “Not Approved” list. You will be re-prompted to accept or decline the EULA if you want to approve the patch at another time.

#### **See Also**

[Automatically Approving Updates for an Approval Group](#)


[Declining Patches](#)

[Approving Updates for Removal](#)

---

## Declining Patches

When you decline a patch, the patch will not be installed, and it will no longer appear in the list of updates.

- 1 In Service Center, click **Patch Management > Patch Approval**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Do one of the following:
  - To select one patch at a time, select the check box of each patch for which you want to change the default approval setting.
  - To select all patches, select the check box in the column header.
- 4 Click **Change Approvals**.
- 5 Do one of the following:
  - To decline the update for all computers, under **All Computers**, from the **Approval** list, select **Declined**.
  - To decline the update for a specific approval group, beside the Computer Group, click the link and select **Not Approved**.
- 6 Click **OK**.

### See Also

[Approving Updates for Installation](#)


[Automatically Approving Updates for an Approval Group](#)

[Approving Updates for Removal](#)

## Approving Updates for Removal

When you approve an update for removal, the patch is uninstalled. The update is removed from the default list of available updates.

**Note:** The patch must support the uninstall action.

- 1 In Service Center, click **Patch Management > Patch Approval**.
- 2 To filter the patch list to display the patches you want to see, click the **Advanced Filtering** icon .
- 3 Do one of the following:
  - To select one patch at a time, select the check box of each patch for which you want to change the default approval setting.
  - To select all patches, select the check box in the column header.

- 
- 4 Click **Change Approvals**.
  - 5 Do one of the following:
    - To remove the update from all computers, under **All Computers**, from the **Approval** list, select **Remove**.
    - To remove the update for a specific approval group, beside the **Computer Group**, click the link and select **Remove**.
  - 6 Do one of the following to set a deadline for when the patch should be removed:
    - To not set a deadline, ensure **None** is showing beside **Deadline**.

Depending on how often the agent policy is set to check for updates (the default is every 22 hours), the device will remove a patch when it checks into Onsite Manager and gets the instruction to do so. The deadline is used to force the patch to be removed by a certain time in the event that the **Notify for Download and Notify for Install** or the **Auto Download and Notify for Install** option button is selected in the patch policy and the local user on the box delays the operation when the notification pops up.
    - To set a deadline but let users determine patch removal time, click **None** and ensure the **Use client settings to determine patch installation time** is selected and click **OK**.
    - To set a deadline but specify a patch removal time, click **None** and select the **Install patch by the selected date and time**. Then select the date and time and click **OK**.

**Note:** You can set a deadline in the past to force immediate installs.
  - 7 Click **OK**.

[Approving Updates for Installation](#)

[Automatically Approving Updates for an Approval Group](#)

[Declining Patches](#)

## Automatically Approving Updates for an Approval Group

To minimize the time it takes to manage patches, you can automatically approve updates for an approval group. For example, if you want to automatically approve all patches for Workstations so that those devices are always up-to-date with the latest updates, you can set up automatic approval for a Workstation approval group. You could also set up that all computers receive all critical and security updates.

---

### To set up automatic approval for an approval group

- 1 In Service Center, click **Patch Management > Settings > Automatic Approval**.
- 2 Click **Add**.
- 3 From the **Approval Group** list, select the Approval Group for which you want to create an approval rule.
- 4 Select the check boxes for each classification you want to automatically approve and then click **Save**.
- 5 Repeat steps 1 to 4 for each approval group to which you want to create an approval rule.

### To apply a new approval rule to existing patches

When you create an approval rule, you can apply it to patches that have already been downloaded to a device.

- 1 In Service Center, click **Patch Management > Settings > Automatic Approval**.
- 2 Select the check box beside the approval rule that you want to apply to existing patches.
- 3 From the **More Actions** list, select **Run Patch Approval Rules on Existing Patches**.

### See Also

[Approving Updates for Installation](#)

[Declining Patches](#)

[Approving Updates for Removal](#)

## Stopping Patch Management

You can stop patch management at the device level, by removing the applied patch policy.

### Stopping Patch Management for a Device

- 1 In Service Center, click **Status > Devices**.
- 2 Use the filters at the top to narrow down the list of devices.
- 3 Click the name of the device on which you want to stop patch management.

- 
- 4 In the **Applied Policies** area, move the slider to turn off the applied patch policy.

# CHAPTER 18

## SETTING UP POWER MANAGEMENT

---

*This section provides detailed information about the following topics:*

- *Power Management*
  - *Getting Ready to Use Power Management*
  - *Viewing Summary Information about Power Management*
  - *Working with Power Plans*
  - *Setting and Overriding Power Plan Precedence*
  - *Power Plan Settings and Options*
-

---

## About Power Management

### What is Power Management?

Power management involves managing and monitoring power usage and costs on a managed computer. Managed Workplace monitors when systems are on, off or asleep and then uses this information to estimate savings in power usage and costs based on a set of assumptions (typical power usage and average power cost).

The goal of power management is to create a consistently configured environment that is optimized for power consumption.

Use power management to

- reduce overall energy consumption
- prolong battery life for laptops
- reduce noise
- reduce operating costs for energy and cooling

All these benefits save money and reduce the impact on the environment.

To learn more about power management and work with a Power Management savings calculator, click [here](#).

### What is a Power Plan?

A power plan is a collection of hardware and system settings that can impact the energy usage of managed Windows devices. Use power plans to reduce the amount of power computers use, maximize performance, or balance the two.

### Managed Workplace Power Plan versus Windows Power Plan

Windows Power Plans include a number of settings that affect power usage by systems. By default, Windows comes with three Power Plans: Power Saver, Balanced and High Performance. Managed Workplace allows MSPs to override locally set values using local group policy. The user's settings, including the power plan, are not touched so that if the Managed Workplace settings are removed, the system reverts to the local settings.

If power settings are managed from a Domain Controller, they will override settings configured in Managed Workplace. Disable this feature on Domain Controller if you are using Managed Workplace Power Management.



---

## Why Use a Power Plan?

Studies show that a properly configured power-managed computer can cut energy costs by 30-40%. Some power companies offer business energy cost rebates for those businesses who adopt green IT initiatives.

## Prerequisites for Power Management

Power management is supported with version 6.4 and later Onsite Managers and Device Managers.

Power management is supported on Windows Vista, Windows 2008 and up.

Managed Workplace automatically excludes virtual machines from power management for stats and reporting. Ensure that virtual machines are marked as virtual. See [Marking a Machine as a Virtual Machine](#).

Devices must be WMI-enabled and power management enabled. You may have to configure NICs and BIOS to enable Wake-on-LAN for a device. You need Wake-on-LAN capability if you've set computers to go to sleep through power management so that end users can wake their computers.

## Sleep, Hibernate and Hybrid Sleep

Sleep is a power-saving state that allows a computer to quickly resume full-power operation (typically within several seconds) when you want to start working again.

Hibernate is a power-saving state designed primarily for laptops. While sleep puts work and settings in memory and draws a small amount of power, hibernation puts open documents and programs on the hard disk, and then turns off the computer. Hibernate uses the least amount of power compared to sleep or hybrid sleep. Hibernate saves more energy because the computer goes off completely, but it takes longer for the computer to resume from hibernation, so it's not as convenient. As well, computers that are set to hibernate cannot be accessed remotely.

Hybrid sleep is designed primarily for desktop computers. Hybrid sleep is a combination of sleep and hibernate since it puts any open documents and programs in memory and on the hard disk, and then puts the computer into a low-power state so that the computer can resume quickly. That way, if a power failure occurs, Windows can restore work from the hard disk. When hybrid sleep is turned on, putting a computer into sleep automatically puts the computer into hybrid sleep. Hybrid sleep is typically turned on by default on desktop computers.

**Note:** If you apply power plan settings to computers and end users need to wake their computers remotely, you need to communicate the steps to end users about how they can wake their computers remotely.

---

## Power Plan Precedence

If devices belong to more than one group and a different power plan is applied to each group, then it's possible that a device has two or more power plans applied to it. The precedence you set to the power plan determines which power plan gets applied.

A power plan applied directly to a device is given the highest precedence.

## Reports for Power Management

There are three reports available for monitoring power management:

- Site Power Management Baseline Comparison
- Site Power Management Cost Savings Estimate
- Site Power Management Summary

## Scripts for Power Management

You can use these scripts to perform power management tasks:

- Enable or Disable Hibernation
- Force Hibernation
- Force Sleep
- Get Power Report (which obtains a Microsoft report from the device)
- Restart Computer
- Shut Down Computer

## What You Can Do

You can

- add a new power plan
- copy a power plan to use as a baseline for a new power plan
- delete a power plan you no longer use
- modify whether power management is enabled by default for new sites
- set the default power costs and usages to apply to a site

## See Also

[Getting Ready to Use Power Management](#)

---

[Working with Power Plans](#)

[Setting and Overriding Power Plan Precedence](#)

## Getting Ready to Use Power Management

### About Power Cost and Usage

A variety of power cost and usage calculators and information exists on the Internet. You can use this information to find the energy consumption cost of laptops and desktops at a site.

Managed Workplace monitors when systems are on, off or asleep and then uses this information to estimate savings in power usage and costs based on a set of assumptions (typical power usage and average power cost).

#### What is Kilowatt Hour?

The kilowatt hour is a unit of energy equal to 1000 watt hours or 3.6 megajoules and is the billing unit for energy delivered to consumers by electric utilities.

#### Power Cost and Usage

You need to find out what the site's electrical company charges for a kilowatt hour (kWh).

For example, if the average cost (currency/kWh) is 12 cents per hour, then you would enter .12 in the Typical Power Cost box.

You can input average power readings in watts/hour for laptops and desktops.

#### Baseline Power Consumption

You can compare the savings after applying power management to a site, if you know the average power cost is for a site and what typical desktop and laptop power usage is (Managed Workplace offers defaults for these numbers). Then you can determine the cost savings of applying power management.

## Setting Defaults for Power Management

### Setting Whether Power Management Is On for New Sites

You can set whether power management is on or off for new sites. If you plan on monitoring and managing power at all your sites, you can set the default to

---

on. That way, any new customers you onboard will already be flagged for power management.

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Under **Global Default Options**, click **Modify**.
- 3 Do one of the following:
  - To enable power management for new sites, select the **Enable Power Management for New Sites** check box.
  - To disable power management for new sites, clear the **Enable Power Management for New Sites** check box.
- 4 Click **Save**.

### Setting the Default Power Costs and Usages for All Sites

You can set

- typical power cost in kilowatt hour (kWh) and the currency to use
  - default desktop power usage (watts/hour)
  - default laptop power usage (watts/hour)
- 1 In Service Center, click **Configuration > Power Management**.
  - 2 Under **Global Default Options**, click **Modify**.
  - 3 To set the currency to use for power cost calculations, select either Dollars, Euros, Yen or Pounds from the **Currency** list.
  - 4 In the **kWh** box, type the typical power cost, which is the amount that the electrical company charges for a kWh.
  - 5 In the **Desktop Power Usage** box, type the typical watts/hour that a desktop machine uses.
  - 6 In the **Laptop Power Usage** box, type the typical watts/hour that a laptop machine uses.
  - 7 Click **Save**.

## Site-Specific Options for Power Management

[Enabling or Disabling Power Management for a Site](#)

[Enabling or Disabling Power Management for a Device](#)

[Overriding the Default Power Costs and Usages at a Site](#)

[Creating a Baseline of Power Management Data for Comparisons](#)

---

## Enabling or Disabling Power Management for a Site

### To enable or disable power management for multiple sites

Using this procedure, you can enable or disable power management for more than one site.

- 1 In Service Center, **Site Management > Sites**.
- 2 Select the check box beside the site to which you want to enable or disable power management.
- 3 From the **More Actions** list, select either **Enable Power Management** or **Disable Power Management**.

### To enable or disable power management for a site

Using this procedure, you can only enable or disable power management for one site.

- 1 In Service Center, **Site Management > Sites**.
- 2 Click the name of the site with which you want to work.
- 3 Click the **Configuration** tab.
- 4 Under **Power Management**, click **Modify**.
- 5 Do one of the following:
  - To enable power management for a site, select the **Enable Power Management** check box.
  - To disable power management for a site, clear the **Enable Power Management** check box.
- 6 Click **Save**.

## Enabling or Disabling Power Management for a Device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Power Management** on the right sidebar.
- 4 Click the **Edit** icon beside **Power Management**.
- 5 Select the **Enabled** check box.
- 6 Click **Save**.

---

## Overriding the Default Power Costs and Usages at a Site

Though you can set a global default for power costs and usages for all sites, one site may need to have different power costs and usage defaults.

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the name of the site with which you want to work.
- 3 Click the **Configuration** tab.
- 4 In the **Power Management** section, click **Modify**.
- 5 To override the default currency to use for power cost calculations, click the **Override** check box and then select either Dollars, Euros, Yen or Pounds from the list.
- 6 To override the default power cost, click the **Override** check box and then type the typical power cost, which is the amount that the electrical company charges for a kWh.
- 7 To override the default desktop power usage, click the **Override** check box and then type the typical watts/hour that a desktop machine uses.
- 8 To override the default laptop power usage, click the **Override** check box and then type the typical watts/hour that a laptop uses.
- 9 Click **Save**.

## Creating a Baseline of Power Management Data for Comparisons

You can show the value of power management to your customer by capturing a baseline that shows data before computers are power managed and after you've set up power management at the site. To do this, you need to create a baseline for comparison.

Use a typical two-week period at a site. For example, don't pick a two-week period that includes holidays, such as Christmas.

After setting the baseline, wait two weeks and then run the Power Management Baseline Comparison report to show your customers the value of implementing power management at the site.

Here's the workflow when an existing customer wants power management set up and you want to see the impact of implementing power management:

- 1 After installing MW2011 R3 or later, wait two weeks to collect typical data without power management enabled.
- 2 Use the new Baseline feature to capture data from a typical two week period in the past.
- 3 Apply power management to the site.

- 
- 4 Wait two weeks to collect typical data with power management enabled.
  - 5 Run the new power management reports to show the cost savings based on the assumptions made for using power management at the customer site over the reporting period. Two weeks is usually representative enough to be accurate.

**Note:** The baseline must be a period in the past. It is recommended to use at least a two-week period of data. You will not be able to create a baseline until enough data is collected.

**Best Practice:** Set the baseline at least two weeks after a Managed Workplace 2011 R3 version 6.4 or later Onsite Manager has been installed so that data has been collected at a site.

- 1 In Service Center, **Site Management** > **Sites**.
- 2 Click the name of the site with which you want to work.
- 3 Click the **Configuration** tab.
- 4 In the **Power Management** section, click **Modify**.
- 5 Under the **Current Baseline Period**, type the start date or use the date picker.
- 6 Type the End date or use the date picker.
- 7 Click **Save**.

## Marking a Machine as a Virtual Machine

A virtual machine *host* is the computer that runs one or more virtual machines, and is a real hardware-based computer. A virtual machine *guest* is one of the non-hardware based computers running on the virtual hardware created by VMWare or others on the host computer. So, any power reporting about the guests is irrelevant, because the power is consumed by the host.

Virtual machines have the ability to skew attempts to report on the impact of power management settings since they have little impact on power consumption.

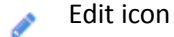
For example, a virtual machine that is turned off for days results in little power savings.

Managed Workplace automatically flags a device as a virtual machine if the manufacturer is Microsoft, VMWare or Xen. If Managed Workplace has not flagged a device as a virtual machine, you can manually set this property on its Device Overview page so that it is not included in any power management calculations.

---

**Note:** Power capabilities collected from systems running Hyper-V and VMs running on these systems are not reliable.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name of a virtual machine.
- 3 Click the **Edit** icon beside **Virtual Machine**.



- 4 Do one of the following:
  - If you want to continue to have Managed Workplace automatically detect if the device is a virtual machine, select the **Auto Detect** option button.
  - If you know that the device is a virtual machine, select the **Force to Yes** option button.
- 5 Click **Apply**.

## Viewing Summary Information about Power Management

You can see a summary of power management across sites. It shows how many devices are power managed versus how many devices are eligible for power management. It also shows the average percentage of eligible devices that have been off or asleep in the selected time range.

### To see summary information at one site

- 1 In Service Center, click **Status > Power Management**.
- 2 To drill down to see one site, click the name of the site.

### To see summary information across sites

- 1 In Service Center, click **Status > Central Dashboard**.
- 2 Click the name of a site.
- 3 Click **Power Management** in the right sidebar.



---

## Working with Power Plans

### Adding a Managed Workplace Power Plan

When you add a power plan, you perform these steps:

- 1 Name the power plan and set the options.
- 2 Apply a power plan to a group or device.

#### To name a power plan and set the options

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Click **Create**.
- 3 In the **Power Plan Name** box, type a name.
- 4 In the **Description** box, type a description.
- 5 Set the power plan options. See [Power Plan Settings](#) for details about the options.

#### To apply a power plan to a group

- 1 Under **Applied Groups**, click **Add**.
- 2 Filter the results by selecting **Site Groups** or **Service Groups**.
- 3 Select the check boxes for the groups to which you want to apply the power plan.
- 4 Click **Add**.
- 5 Repeat steps 1 to 4 until all the groups to which you want to apply the power plan are included.
- 6 Click **Save**.

#### To apply a power plan to a device

- 1 Under **Applied Devices**, click **Add**.
- 2 Filter the results by selecting the appropriate items and click **Filter**.
- 3 Select the check boxes for the devices to which you want to apply the power plan.
- 4 Click **Add**.
- 5 Repeat steps 1 to 4 until all the devices to which you want to apply the power plan are included.

- 
- 6 Click **Save**.

**Note:** If a power plan had already been applied to a device, it is replaced with the power plan you just applied.

## Removing a Device or Group from a Power Plan

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Click the name of the power plan you want to rename.
- 3 Do one of the following:
  - Under **Applied Groups**, select the check boxes for the groups you want to remove from the power plan and click **Delete**.
  - Under **Applied Devices**, select the check boxes for the devices you want to remove from the power plan and click **Delete**.
- 4 Click **Save**.

## Renaming a Power Plan

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Click the name of the power plan you want to rename.
- 3 Type a new name in the **Power Plan Name** box.
- 4 Click **Save**.

## Copying a Power Plan

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Select the check box for the power plan you want to copy.
- 3 Click **Copy**.

Managed Workplace creates a new power plan and gives it the next precedence that is available. For example, if three power plans exist, the new copy would have a precedence of 4.

## Deleting a Power Plan

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Select the check boxes for the power plans you want to delete.
- 3 Click **Delete**.

---

## Enabling or Disabling Power Management for a Device

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Power Management** on the right sidebar.
- 4 Click the **Edit** icon beside the **Power Management** label.



Edit icon

- 5 Select the **Enabled** check box to enable power management or clear it to disable power management for the device.
- 6 Click **Save**.

## Overriding Power Plan Settings for a Device

**Note:** Power management must be enabled for the site to which the device belongs.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.
- 3 Click **Power Management** on the right sidebar.
- 4 Click the **Edit** icon beside the **Active Power Plan** label.



Edit icon

- 5 Select the **Configure Override** check box.
- 6 Select the option button for the power plan you want to apply to the device.
- 7 Click **Save**.

If a power plan had already been applied to a device, it is replaced with the power plan you just applied.

---

## Setting and Overriding Power Plan Precedence

### Setting Power Plan Precedence for Groups

Power plan precedence is a numerical value (where 1 is high) used to set the priority of a power plan.

A device receives its power plan settings from the group to which it belongs.

It is possible to have the same device in more than one group and therefore to have two or more power plans applied to one device. In this case, you must set power plan precedence so that conflicts are resolved.

What if...	Then...
A device does not have a power plan applied directly to it	The power plan with the highest precedence assigned to any group to which the device belongs is used.
A power plan is applied to a device	The power plan applied to a device is given the highest precedence and ignores the power plan assigned by groups.
A device is in more than one group and a different power plan is applied to each group	The power plan with the highest precedence is used.

- 1 In Service Center, click **Configuration > Power Management**.
- 2 Click **Manage Precedence**.
- 3 Select the power plan and use the up or down arrow to change its precedence.
- 4 Click **Save**.

### Overriding Power Plan Precedence for a Device

You can override the default power plan precedence and give a power plan on a specific device higher precedence.

A power plan assigned to a device is given the highest precedence.

- 1 In Service Center, click **Status > Devices**.
- 2 Click a device name.

- 
- 3 Click **Power Management** on the right sidebar.
  - 4 Click the **Edit** icon.
  - 5 Ensure the **Configure Override** check box is selected.
  - 6 Select one of the power plans from the list.
  - 7 Click **Save**.

## Power Plan Settings and Options

### Power Plan Settings

The following tables list the power plan settings available and provides a description for each.

### Vista + Settings

Setting	Description
Allow Standby States	Allows a computer to be in a standby state, which is a low energy usage state from which a computer can return quickly. It could be either Sleep, Hibernate or Hybrid Sleep.
Critical Battery Notification Action	Specifies the action that Windows takes when battery capacity reaches the critical battery notification level.
Low Battery Notification Action	Specifies the action that Windows takes when battery capacity reaches the low battery notification level.
Hibernate After	Specifies the time after which the computer should hibernate.
Lid Close Action	Specifies the action that Windows takes when the laptop lid is closed.

---

<b>Setting</b>	<b>Description</b>
Power Button Action	Specifies the action that Windows takes when the Power button is pressed.
Require a Password on Wake-up	Specifies whether the user is prompted for a password when the system resumes from a sleep state.
Sleep After	Specifies the time after which the computer should sleep.
Sleep Button Action	Specifies the action that Windows takes when the Sleep button is pressed.
Start Menu Power Button Action	Specifies the action that Windows takes when a user selects the Sleep option from the Start menu.
Turn On Applications to Prevent Sleep Transitions	When enabled, this setting allows applications and services to prevent the system from sleeping.
Turn Off Hybrid Sleep	Disables hybrid sleep and the system will not generate a hiberfile when transitioning to sleep. This means that the state of the computer is not saved to disk, but will be treated the same as sleep.
Turn Off Adaptive Display Timeout	Manages how Windows controls the setting that specifies how long a computer must be inactive (including activity with a mouse or keyboard) before Windows turns off the computer's display.
Turn Off the Display After	Specifies the period of inactivity before Windows turns off the display.

---

Setting	Description
Turn Off Hard Disk After	Specifies the period of inactivity before Windows turns off the hard disk.

### Window 7 + Settings

Setting	Description
Allow Automatic Sleep with Open Network Files	Allows applications and services to prevent automatic sleep.
Reduce Display Brightness After	Specifies the period of inactivity before Windows automatically reduces brightness of the display.
Reserve Battery Notification Level (Percentage)	Specifies the percentage of battery capacity remaining that triggers the reserve power mode.
Specify the Unattended Sleep Time-out	Specifies the period of inactivity before Windows transitions to sleep automatically when a user is not present at the computer.

### Options

Some settings let you choose Not Set or Never. This table explains these two options:

Option	Description
Do not set	Managed Workplace does not touch this setting so the user can configure.
Never	Managed Workplace sets the parameter to Never and the user is unable to change the setting.





# CHAPTER 19

## WORKING WITH TROUBLE TICKETS

---

*This section provides detailed information about the following topics:*

- *Working with Trouble Tickets*

*For information about integrating with a Professional Services Automation (PSA) or service desk, such as Salesforce, ConnectWise, Autotask, Tigerpaw and others, see the Integration Guide: Service Desks.*

---

---

## Working with Trouble Tickets

### About Trouble Tickets

The Ticket Management window displays all trouble tickets that have been created in Service Center or sent to Service Center by Support Assistant, and has many filtering options available to define what is displayed in the list of trouble tickets.

Trouble Tickets are created by alert actions, by Service Center users or by Support Assistants.

#### What You Can Do

You can

- pass a trouble ticket to a Professional Services Automation (PSA) or service desk system or to another Service Center
- use permissions to allow a Customer role to assign Trouble Tickets
- create Service Center users for your customers and allow them to create trouble tickets to request service
- show customers how many tickets have been closed using the Work Completed Summary report

#### See Also

*Integration Guide: Service Desks*

### Viewing Trouble Tickets

The Ticket Management window displays all trouble tickets that have been created in Service Center or sent to Service Center by Support Assistant.

- 1 In Service Center, click **Trouble Tickets > Ticket Management**.
- 2 Do any of the following to filter the view of trouble tickets:
  - To show all trouble tickets, in the **View** list, select All Tickets.
  - To filter the trouble tickets by service plan, in the **View** list, select Browse by Service Plan and then select the Site and Site Group.
  - To filter the trouble tickets by site, in the **View** list, select Browse by Site and then select the Site and Site Group.
  - To filter the trouble tickets by Service Group, in the **View** list, select Browse by Service Group and then select the service group.

- 
- To filter the trouble tickets by who they're assigned to, in the **View** list, select Assigned To and then select the user.
  - To filter the trouble tickets by status, in the **Ticket Status** list, select a status.
  - To see a specific trouble ticket, in the **Search Ticket ID** box, enter the trouble ticket ID and click **Filter**.
  - To change how many tickets to display per page, select an option from the **Page Size** list.

## Adding a Trouble Ticket

Trouble tickets may be created manually or automatically as an alert action. All trouble tickets can be carried over to any third-party integrations that exist in the system.

- 1 In Service Center, click **Trouble Tickets > Add Ticket**.
- 2 Select the site from the **Site** list.
- 3 From the **Priority** list, select either Low, Medium or High as the priority level.
- 4 From the **Category** list, select one of the following categories:
  - Onsite Manager Alerts
  - Service Requests
  - Hardware Problems
  - Software Problems
- 5 From the **Severity** list, select either Info, Warning or Error as the severity level.
- 6 From the **Assign To** list, select the user to which you want to assign the trouble ticket.

**Default:** Tickets are assigned to the first valid user for the object generating the alert in the database. This is typically the Admin user account.
- 7 Type a title for the issue in the **Title** box.
- 8 Type any relevant details in the **Comment** box.
- 9 If the trouble ticket should be emailed to the assigned user, select the **Email Ticket to Assignee** check box.
- 10 Click **Submit**.

---

## Changing a Trouble Ticket

- 1 In Service Center, click **Trouble Tickets > Ticket Management**.
- 2 Do one of the following:
  - In the **Title** column, click the title of the trouble ticket you want to update.
  - Type the ticket number in the **Search Ticket ID** box and click **Filter**.
- 3 Do any of the following:
  - To change the title, type a new one in the **Title** box.
  - To change who is assigned the ticket, select a different user from the **Assigned To** list.
  - To change the category, select a new category from the **Category** list.
  - To change the status, select a different one from the **Status** list. If viewing the ticket details for the first time, you should change the status from New to Open.
  - To change the priority, select a new priority from the **Priority** list.
  - To change the severity, select a new severity from the **Severity** list.
- 4 Click **Update**.

## Printing a Trouble Ticket

- 1 In Service Center, click **Trouble Tickets > Ticket Management**.
- 2 Do one of the following:
  - In the **Title** column, click the title of the trouble ticket you want to update.
  - Type the ticket number in the **Search Ticket ID** box and click **Filter**.
- 3 Click **Printer Friendly**.
- 4 Click the **Printer** icon.
- 5 Select a printer and configure the print options.
- 6 Click **Print**.

## Closing Trouble Tickets

- 1 In Service Center, click **Trouble Tickets > Ticket Management**.

- 
- 2 Do one of the following:
    - Select the check box beside the title of the trouble ticket you want to close.
    - Type the ticket number in the **Search Ticket ID** box and click Filter. Then select the check box beside the title of the trouble ticket you want to close.
  - 3 To close the ticket, click **Close Tickets**.



# CHAPTER 20

## CUSTOMIZING SUPPORT ASSISTANT

---

*This section provides detailed information about the following topics:*

- *Customizing Support Assistants*
  - *Creating a Support Assistant Policy*
  - *Editing a Support Assistant Policy*
  - *Copying a Support Assistant Policy*
  - *Deleting a Support Assistant Policy*
  - *Keeping Track of Support Assistant Deployment*
  - *Using Support Assistant from a Device*
-

---

# Customizing Support Assistants

## About Customizing Support Assistant

You can customize the appearance and functionality of Support Assistant in a user's environment using Support Assistant policies.

### About Support Assistant

Support Assistant is your company's brandable presence on managed Windows and Mac devices and includes a context menu and an icon which is delivered in one of two ways:

- as a recommended feature of the Device Manager when the profile used is configured to display an icon in the notification area
- independently by configuring an automated task

The brandable icon can be a 16 x 16 pixel image of your corporate logo, or any other icon that you choose. You can also add another icon to indicate a fault state so the user knows when something is not working properly with the Device Manager.

You can determine what additional functionality is offered on the context menu, which end users access by clicking the icon. For example, you can include text-based messages for the end user, shortcuts to email and web addresses, allow them to request live chat or remote assistance, and offer the ability to send trouble tickets to Service Center.

### About Support Assistant Policies

A Support Assistant policy sets options and defines the appearance of Support Assistant in a user's environment.

You can create more than one Support Assistant policy for use across different sites or service plans.

### Considerations for Using Support Assistant Policies

Do you want end users to be able to create tickets? You can add options to the context menu for the Support Assistant policy that enables end users to submit trouble tickets. Or, you can provide other ways for users to contact you (such as your email, website or telephone number) and not enable the ticketing options.

Do you offer customers a tiered service? You could use different icons at different sites based on the service plan that you've provided for them



---

## What You Can Do

For Support Assistants, you can

- include an uninstall password so that end users cannot remove Support Assistant
- customize the icon users see in the notification area
- provide a context menu that provides links to URLs, a specific support email address or enables users to submit tickets

## See Also

[Installing Device Managers](#)

## Creating a Support Assistant Policy

Creating a Support Assistant policy involves the following steps:

- 1 [Configuring the Name and Options for the Support Assistant Policy](#)
- 2 [Configuring the Icon Users See on Their Desktops](#)
- 3 [Configuring the Context Menu Your Customers See](#)
- 4 [Setting an Uninstall Password for the Support Assistant](#)

## Configuring the Name and Options for the Support Assistant Policy

### To create and name the Support Assistant policy

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click **New**.
- 3 In the **Policy Name** box, type a name.
- 4 Optionally, in the **Description** box, type a description.
- 5 Click **Create**.
- 6 Click the **Settings** tab.
- 7 Click **Modify**.

### To customize how Support Assistant is displayed

- 1 In the **Customizations** area, select any or all the following:
  - Display icon in notification area** If selected, displays the support assistant icon in the notification area, which is located on the right side of the taskbar by default.

---

**Show service notifications** If selected, notifications are displayed in the notification area, which is located on the right side of the taskbar by default. Notifications include whether Device Manager can communicate with Service Center. As well, if you hover the mouse over the icon, a message shows whether Device Manager can connect to Service Center.

**Display service shutdown option in context menu** If selected, allows your end user to use the context menu to shut down Device Manager. You may want to include this option so that end users can ensure no network traffic is generated by the Device Manager in billable environments such as a hotel.

**Require user consent for remote access** If selected, the end user needs to give consent for remote access. When selected, you'll see another box where you need to enter how long to wait for user consent. You will also see the **Message for Remote Session Consent** box below.

### To create the branded messaging for the Support Assistant policy

- 1 In the **Branded Messages** area, type the name of the service in the **Service Name** box.

This is the name users see when they hover the mouse over the icon in the notification area. For branding purposes, you could use your business name for the service name.

- 2 In the **Message for Remote Session Consent** box, type a message that the user sees when you request a remote session.
- 3 In the **Service Shutdown Menu Item Text** box, type the text users will see in the context menu for the option to shutdown the service.

### Configuring the Icon Users See on Their Desktops

By default, an operational icon appears in the notification area in the taskbar when the service is installed and running:



Operational icon

Shows when the service is communicating with Service Center.



Fault icon

Shows when the service is not able to communicate with Service Center.

**Note:** This option is ignored by Support Assistant.

---

## To change the icon for the service

- 1 Do one of the following:
  - To change the Operational icon, select the check box beside **Operational Icon** and click **Upload Custom Icon**.
  - To change the Fault icon, select the check box beside **Fault Icon** and click **Upload Custom Icon**.

**Note:** You have the option of using only one icon also. In this case, both Operational and Fault icon are the same.
- 2 Click **Choose File**, locate the icon file (.ICO) you want to use and click **Open**.

**Note:** You can only upload icons that are 16 x 16 pixels. Do not use icons that contain a space character in the name.
- 3 Click **Upload**.

## To change the icon for the service back to the default icon

- Do one of the following:
  - To change the Operational icon, select the check box beside **Operational Icon** and click **Use System Default Icon**.
  - To change the Fault icon, select the check box beside **Fault Icon** and click **Use System Default Icon**.

## Configuring the Context Menu Your Customers See

When users click the icon in the notification area in the taskbar, they will see the context menu for the service. You can customize the context menu to include any of the following items:

- a link to an email address
- a text message
- an option to submit a ticket
- a link to a web page

## Ticket Options

There are three options you can use to allow end users to submit tickets to Service Center. You can use a combination of all three.

**Predefined ticket** A type of ticket that you create and configure and requires no additional information from the user. You set the ticket title, description, priority and severity. When users select this option from the context menu of

---

Support Assistant, a ticket is automatically created in Managed Workplace. For example, you can use this type of ticket to help users request a callback.

**Basic ticket** A type of ticket that asks users for one piece of information. Use this option if you want to prefill the ticket information but allow the user to provide a brief summary of their issue or even just provide contact information. You can customize the name of the box the user sees. For example, you can use this type of ticket to ask users for the telephone number at which they would like to be reached.

**Detailed ticket** A type of ticket that asks users for a combination of three pieces of information: ticket title, description or priority. Use this option when you want the user to provide detailed ticket information. You can't customize the names of the boxes the user sees.

**Note:** After a user submits a ticket, a ticket is created in Managed Workplace. If a service desk integration is set up, the ticket is submitted to the Professional Services Automation (PSA) or service desk system as well.

### Ticketing Information Sent to Managed Workplace

When you set up options for end users to submit a ticket, the following information is sent to Managed Workplace no matter what ticket option you use:

- URL of the device from which the ticket was submitted that you can use to go quickly to the target device
- user ID (login name) of the person who submitted the ticket

The ticket is stored in a category called **Service Requests** and the status is set to **New**.

### To add a link to an email address in the context menu for the service

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.
- 6 Select the **Email** option button.
- 7 In the **Menu Text** box, type the text for the menu item.
- 8 In the **Email Address** box, type the email address.

- 
- 9 To include a link to the device in the body of the email, select the **Include link to device in message body** check box.

When you receive the e-mail and select this link, you will be taken to the device that submitted the ticket. If you are not already logged on to Service Center, you will initially be asked to log in before taken to the device. You may also want to open a ticket in Managed Workplace to track the progress of this request.

- 10 Click **Add**.

### To add a text-based message to the context menu for the service

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.
- 6 Select the **Text** option button.
- 7 In the **Menu Text** box, type the text for the menu item.
- 8 Click **Add**.

### To add an option to submit a predefined ticket to the context menu for the service

A predefined ticket enables you to assign preconfigured values to the ticket boxes and provides a quick way for the end user to submit a ticket.

For example, you can add a title called "Request Remote Assistance" and when an end user clicks this menu item, a ticket is automatically created and sent to Service Center.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.
- 6 Select the **Ticket Submission** option button.
- 7 In the **Menu Text** box, type the text for the menu item.
- 8 In the **Confirmation Window Message** box, type the message you want users to see after they have submitted a ticket.

---

When users submit a ticket, they will see this message along with the ticket number.

- 9 From the **User View** section, select the **Predefined ticket (no user input required)** option button.
- 10 From the **Ticketing Field Configuration** section, in the **Title** box, type the title of the ticket.
- 11 In the **Description** box, type a description of the ticket.
- 12 From the **Priority** list, select a priority.
- 13 From the **Severity** list, select a severity.
- 14 From the **Assign To** list, select to whom the ticket should be assigned.  
The options in this list are the user accounts set up in Managed Workplace.
- 15 To send an email to the user account in the **Assign To** list, select the **Email ticket to assignee** check box.
- 16 Click **Add**.

### To add an option to submit a basic ticket to the context menu for the service

A basic ticket requires some information from the end user. The box displayed to the end user can be either one line or multi-line.

The maximum number of characters that a user can enter in this box is 1024 characters.

For example, you can add a title called “Request Callback” so that end users can request a telephone call. Then the ticket can include a prompt for the telephone number of the user. In this case, you would clear the **Show multi-line text box for requested data** check box to show a form box that is one line.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.
- 6 Select the **Ticket Submission** option button.
- 7 In the **Menu Text** box, type the text for the menu item.
- 8 In the **Confirmation Window Message** box, type the message you want users to see after they have submitted a ticket.

- 
- 9 From the **User View** section, select the **Basic ticket information required from user** option button.
  - 10 In the **Label for Requested Data** box, type the label the user will see in the ticket submission form.
  - 11 Do one of the following:
    - To show a box that is a single line, clear the **Show multi-line text box for requested data** check box.
    - To show a box that is a multi-line box, select the **Show multi-line text box for requested data** check box.
  - 12 From the **Ticketing Field Configuration** section, in the **Title** box, type the title of the ticket that is sent to Service Center.
  - 13 In the **Description** box, type a description of the ticket that is sent to Service Center.
  - 14 From the **Priority** list, select a priority for this type of ticket.
  - 15 From the **Severity** list, select a severity for this type of ticket.
  - 16 From the **Assign To** list, select to whom the ticket should be assigned.  
The options in this list are the user accounts set up in Managed Workplace.
  - 17 To send an email to the user account in the **Assign To** list, select the **Email ticket to assignee** check box.
  - 18 Click **Add**.

### To add an option to submit a detailed ticket to the context menu for the service

A detailed ticket requires the end user to provide information before a ticket is submitted. For some boxes, you can choose to assign preconfigured values or you can ask the user to provide this information. By prefilling the boxes with information, you can help the end user know what information you're expecting. If the user doesn't replace this text, it's included in the ticket and sent to Managed Workplace.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.

- 
- 6 Select the **Ticket Submission** option button.
  - 7 In the **Menu Text** box, type the text for the menu item.
  - 8 In the **Confirmation Window Message** box, type the message you want users to see after they have submitted a ticket.
  - 9 From the **User View** section, select the **Detailed ticket information required from user** option button.
  - 10 Optionally, select the following check boxes.
    - Show Title** When selected, shows a **Title** box when the user submits a ticket and asks the user for a title of the ticket. When cleared, you must enter the title in the **Title** box so that the ticket information can be complete in Managed Workplace.
    - Show Description** When selected, shows a **Description** box when the user submits a ticket and asks the user for a description of the ticket. When cleared, you must enter the description in the **Description** box so that the ticket information can be complete in Managed Workplace.
    - Show Priority** When selected, shows a **Priority** list when the user submits a ticket and asks the user to select a priority for the ticket. When cleared, select the default priority for all tickets.
  - 11 From the **Severity** list, select a severity.
  - 12 From the **Assign To** list, select to whom the ticket should be assigned.

The options in this list are the user accounts set up in Managed Workplace.
  - 13 To send an email to the user account in the **Assign To** list, select the **Email ticket to assignee** check box.
  - 14 Click **Add**.

#### To add a link to a web page in the context menu for the service

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click **Add**.
- 6 Select the **Web Page** option button.
- 7 In the **Menu Text** box, type the text for the menu item.
- 8 In the **Web Page Address** box, type the URL of the web page.



- 
- 9 Click **Add**.

#### **To edit an item on the context menu for the service**

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, click the name of the context menu item you want to edit.
- 6 Make the desired changes.
- 7 Click **Save**.

#### **To move an item up or down in the context menu for the service**

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, select the check box for the context menu item you want to move.
- 6 Click **Move Up** or **Move Down**.

#### **To delete an item from the context menu for the service**

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 In the **Context Menu** area, select the check box for the context menu item you want to delete.
- 6 Click **Delete**.
- 7 Click **OK**.

#### **Setting an Uninstall Password for the Support Assistant**

You can control whether device users can uninstall Support Assistant from their device by setting an uninstall password.

- 
- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
  - 2 Click the name of the Support Assistant policy you want to modify.
  - 3 Click the **Settings** tab.
  - 4 Click **Modify**.
  - 5 In the Uninstall Password section, select the **Require password to uninstall service** check box.
  - 6 Type a password in the **Uninstall Password** box and confirm it by typing it again in the **Confirm Uninstall Password** box.

## Editing a Support Assistant Policy

After deploying Support Assistants with a specific policy, you can edit the policy. Changes to the policies are pushed down to managed devices when you click **Save**. Service Center will queue the update for any devices that are offline at the time and complete it when the device becomes available.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to modify.
- 3 Click the **Settings** tab.
- 4 Click **Modify**.
- 5 Make the required changes.
- 6 Click **Save**.

## Copying a Support Assistant Policy

You can copy a Support Assistant policy to use as the base for a new policy you want to create. Copied Support Assistant policies are automatically provided the same name as the original, with a number appended starting with (1). You can then change the name of the copy as desired.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Select the check box beside the policy you want to copy.
- 3 Click **Copy**.

## Deleting a Support Assistant Policy

You can delete a Support Assistant policy you no longer need.

---

**Note:** When you delete a Support Assistant policy that has been applied to devices, Support Assistant will be automatically uninstalled from those devices.

- 1 In Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Select the check box beside the policy you want to delete.
- 3 Click **Delete**.

## Updating Support Assistant at a Site

You can update the Support Assistant at a site if there is a new version of Support Assistant available.

**Tip:** You can also update Support Assistant on a device by device basis, by going to **Status > Support Assistant**. For more information, see [To upgrade Support Assistant on one or more devices](#).

### Notes:

- When a Support Assistant device is not connected, Service Center buffers the upgrade script until that device reconnects.
- Support Assistant is installed in the following location: <AVG>/Support Assistant and its copy of OMDesktop.exe is located in that directory.

### To update Support Assistants across different sites

- 1 In Service Center, click **Update Center > Products**.
- 2 Select the check boxes for the sites where you want Support Assistants upgraded.
- 3 Click **Advanced Options**.
- 4 Click the **Update Support Assistants for selected sites** check box.
- 5 Click **Update**.

**Note:** The end user must log off and log in again to complete the upgrade.



If an update fails, logs provide notification. If a Support Assistant upgrade fails, there is an indication on the Support Assistant page that it failed.

To see the reason why the failure occurred, hover your mouse over the icon.


---

## Uninstalling a Support Assistant from a Site or Device

You can uninstall Support Assistant from within Managed Workplace or from the device's Control Panel using remote control.

Support Assistant is automatically uninstalled from a device when you remove the Support Assistant policy from the device. The steps for uninstalling Support Assistant differ according to whether you want to remove it from one device, or if you want to remove it from all devices at a site.

### To uninstall Support Assistant from a device

- 1 In Service Center, click **Status > Devices**.
- 2 Use the filters at the top of the page to narrow your selection of devices.
- 3 Click a device name to open the **Device** page.
- 4 On the **Device** page, scroll down to the **Applied Policies** area.
- 5 Disable the Support Assistant policy on the device by moving the slider .

### To uninstall Support Assistant from multiple devices at once

- 1 in Service Center, click **Configuration > Policies > Support Assistant**.
- 2 Click the name of the Support Assistant policy you want to remove from devices.
- 3 Click the **Excluded Devices** tab.
- 4 Click **Add**.
- 5 From the **Filter By** list, select the filter to narrow down the list of devices. This allows you to filter devices by site or group, among others.
- 6 Click **Filter**.
- 7 Select the check box beside each device you want to exclude from the Support Assistant policy. To select all devices listed, select the check box at the top of the column.
- 8 Click **OK**.
- 9 Click **Close**.

The devices are added to the exclusion list for the Support Assistant policy, and Support Assistant is automatically uninstalled from these devices.

**Note:** If a Support Assistant is uninstalled locally on the device using Add/Remove Programs in Control Panel, or by running the "Uninstall Support Assistant" script in the **Automation Library**, the Support Assistant policy is not




---

automatically removed from the device. To ensure that Support Assistant is not automatically reinstalled on the device as per the Support Assistant policy automatic application rules, you must also remove the policy from the device.




## Keeping Track of Support Assistant Deployment

The **Support Assistant** page helps you keep track of successful, pending, and failed Support Assistant installations across all your sites. From this page, you can upgrade Support Assistant on one or more devices, retry a failed installation, and click to open a **Device** page or a **Support Assistant Policy** page to view more information and make modifications as needed.

The following table lists the icons indicating the status of a Support Assistant installation:

Installation Status	Icon
Successful	
Pending	
Failed	

### To view a list of deployed Support Assistants

- 1 In Service Center, click **Status > Support Assistant**.
- 2 To sort the list, do any of the following:
  - To sort devices by those with a Support Assistant upgrade available, click the **Sort by upgrade available** icon .
  - To sort devices by upgrade status, click the **Sort by upgrade status** icon .
- 3 To filter the devices by site, select a site from the drop list in the top right of the page.
- 4 To view the **Device** page for a device, click the device name.
- 5 To view more information about the Support Assistant policy applied to a device, click the Support Assistant policy name.
- 6 To view the Support Assistant installation history for a device, hover the cursor over the **Installation History** icon .

---

### To upgrade Support Assistant on one or more devices

- 1 In Service Center, click **Status > Support Assistant**.
- 2 To filter the devices by site, select a site from the drop list in the top right of the page.
- 3 Select the check box beside each device for which you want to upgrade Support Assistant.

**Tip:** To upgrade Support Assistant for all devices listed, select the check box at the top of the check box column.

- 4 Click **Upgrade**.

### To retry a Support Assistant installation

- 1 In Service Center, click **Status > Support Assistant**.
- 2 To filter the devices by site, select a site from the drop list in the top right of the page.
- 3 Select the check box beside each device for which you want to retry installing Support Assistant.

**Tip:** To retry Support Assistant installation for all devices listed, select the check box at the top of the check box column.

- 4 Click **Retry Installation**.

## Using Support Assistant from a Device

You can provide information to end users about the Support Assistant that is installed on their desktops. Depending on how you set up the Support Assistant policy, you may want to tell them how to submit a ticket or how to contact you using the Support Assistant.

Not all notification area icons are displayed by default. Icons are displayed in the notification area overflow unless promoted to the notification area by the user. You may also want to mention how to make the icon show up all the time on the user's desktop by telling them to right-click the icon and select **Customize**.

### To use Support Assistant from a device

- Click the Support Assistant icon in the notification area of the taskbar and select a menu item.

# CHAPTER 21

## CUSTOMIZING SERVICE CENTER

---

*This section provides detailed information about the following topics:*

- *Branding Service Center*
  - *Customizing Service Center*
-

---

## Branding Service Center

### Branding Service Center

The **Branding** tab allows you to add images to brand the Service Center user interface with your company logos.

A primary logo appears at the top of the sidebar (above the main menu) and appears on every window in Service Center. You can also include a secondary logo and a banner graphic.

You can use images with the following file extensions: .JPG, .JPEG, .GIF, .TIFF, .PNG or .BMP. Images are automatically scaled proportionally in the user interface once uploaded.

If you click the primary logo, it returns you to the Central Dashboard. You can add a hyperlink for the primary logo so that if the image is clicked, a new window displaying the URL appears.

#### Notes:

- The primary company logo is scaled to 165 pixels wide.
- The maximum width for both the secondary company logo and banner graphic combined is 850 pixels. These two images are scaled to 60 pixels high.
- Scaling of the images maintains the image's original aspect ratio.
- If you're using a hosted version of Managed Workplace, adding a logo, secondary logo or banner graphic may not be available.

**Tip:** For the primary company logo, use a .PNG file of your logo on a transparent background.

#### To add a logo to Service Center

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Branding** tab.
- 3 Do one of the following for the primary company logo:
  - Select **Existing Image** and then select an image from the list.
  - Select **New Image > Select**. In the **Open** dialog box, locate the new image file and click **Open**. Click **Save**.
- 4 If you want to include a secondary logo, do one of the following:
  - Select **Existing Image** and then select an image from the list.



- 
- Select **New Image > Select**. In the **Open** dialog box, locate the new image file and click **Open**. Click **Save**.
- 5 If you want to include a banner graphic, do one of the following:
- Select **Existing Image** and then select an image from the list.
  - Select **New Image > Select**. In the **Open** dialog box, locate the new image file and click **Open**. Click **Save**.

### To stop using an image

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Branding** tab.
- 3 Select **No Image** for the image you no longer want to use.
- 4 Click **Save**.

### To add a hyperlink for the primary logo in Service Center

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Branding** tab.
- 3 In the **Enter an optional hyperlink...** box, type the URL address.
- 4 Click **Save**.

### To delete a logo from the Existing Image list

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Branding** tab.
- 3 For the image you no longer want to use, select **Existing Image** and then select the image from the list.
- 4 Click **Delete**.
- 5 In the confirmation window, click **OK**.
- 6 Click **Save**.

## Applying Themes to Service Center

You can apply color themes to Service Center.

**Note:** For hosted versions of Service Center, theme options are only available if the hosting provider has made them available.

- 1 In Service Center, click **Configuration > System Settings**.

- 
- 2 Click the **Themes** tab.
  - 3 In the **Select Theme** section, select a theme from the list.
  - 4 Click **Set Theme**.

## Customizing Service Center

### Setting Refresh Options for the Central Dashboard and Alert Lists

You can set the auto-refresh times for the Central Dashboard and for Alert lists.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 To set the auto-refresh time for the Central Dashboard, enter a value in minutes on the **Central Dashboard Refresh Rate** box.
- 4 To set the auto-refresh time for the Alerts listing, enter a value in minutes in the **Alerts Refresh Rate** box.

**Note:** The **Alerts Viewer** is a live view that displays alerts as they are received by Service Center. The auto-refresh settings have no effect on its operations.

- 5 Click **Save**.

### Enabling or Disabling Website Usage Tracking

To help AVG track which pages are most used in Service Center and in the online help, website tracking usage is automatically enabled. Web tracking usage is powered by Google Analytics, and all statistics gathered are private and not used for any other purpose. However, you can disable web tracking usage if preferred.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 To prevent Google Analytics from tracking the pages clicked in Service Center, clear the **Enable website tracking usage** check box.

### Setting Regional Preferences

You can set the default languages for Service Center and reports. You can also set a default font for reports, and create font exceptions for additional report

---

languages, if desired. For example, you can set your default report language to English, and assign Verdana as the default font. Then, you can create font exceptions by applying different fonts to other report languages. For example, you can specify that Japanese reports use Gothic, or German reports use Arial.

**Note:** Changing the font for reports does not change the font for existing reports; the selected font will only be applied to new reports going forward.

### To set default locales for Service Center and reports

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the **Regional Preferences** section, click **Modify**.
- 4 From the **Default locale for UI** list, select a language for the Service Center UI.
- 5 From the **Default locale for reports** list, select a default language for reports.
- 6 Click **Save**.

### To set the default font for reports

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the **Regional Preferences** section, click **Modify**.
- 4 In the **Default Report Fonts** area, from the **Default font** list, select a default font that will be applied to all reports.
- 5 Click **Save**.

### To create font exceptions for report languages

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the **Regional Preferences** section, click **Modify**.
- 4 Click **Add**.
- 5 From the **Language** list, select a language.
- 6 From the **Font** list, select a font.
- 7 Click **Save**.

---

### To edit font exceptions for report languages

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the **Regional Preferences** section, click **Modify**.
- 4 Select the check box beside the report language you want to edit.
- 5 Click **Edit**.
- 6 Make any changes as required.
- 7 Click **Save**.

### To delete font exceptions for report languages

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the **Regional Preferences** section, click **Modify**.
- 4 Select the check box beside the report language you want to delete.
- 5 Click **Delete**.

**Note:** When you delete a font exception for a report language, any future reports created in that language will use the default font for reports. Existing reports in that language will continue to use the font that had been selected as the exception.

## Setting Onsite Manager Installer Preferences

You can set the default installation configuration settings for Onsite Manager, including whether to install optional components such as MBSA and SQL Server Management Studio Express. During the installation, these settings can be overridden by choosing to perform an advanced installation.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **General** tab.
- 3 In the Onsite Manager Installer Settings area, click **Modify**.
- 4 To change the default Onsite Manager installation path, select the **Custom Location** check box, and in the **Full installation path** box, type a new path.
- 5 To prevent Onsite Manager from automatically scanning the local subnet, clear the **Auto Scan** check box.

- 
- 6 To change the root path for the Microsoft SQL Server Express instance, in the Microsoft SQL Server Express area, select the **Custom Location** check box, and in the **Full installation path** box, type a new path.
  - 7 To install Microsoft Baseline Security Analyser (MBSA), in the Microsoft Baseline Security Analyser area, select the **Install Component** check box.
  - 8 To change the default MBSA installation path, select the **Custom Location** check box, and in the **Full installation path** box, type a new path.
  - 9 In the Microsoft SQL Server Management Studio Express area, select the **Install Component** check box to install SQL Server 2008 R2 Management Studio Express.
  - 10 Click **Save**.

## Adding or Deleting Performance Counters

The **Network Objects** tab provides a list of all Performance Counters that are available for monitoring. Additional Performance Counters can be added here, or any that are not in use can be removed.

### To add a Performance Counter to the Service Center database manually

**Note:** The **WMI Class Name** and **WMI Property Name** boxes are used for non-English monitoring with Managed Workplace. A Managed Workplace script called Get Performance Counter Class can be used to determine the WMI class and properties if you do not know these.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 In the **Performance Counters** section, click **Add**.
- 4 Do one of the following:
  - Select the Performance Object from the **Performance Object** list.
  - If the Performance Object does not exist, select the **Other** check box, and enter the Performance Object in the box that appears.
- 5 Do one of the following:
  - Select the Object Instance from the **Object Instance** list.
  - If the Object Instance does not exist, select the **Other** check box, and enter the Object Instance in the box that appears.

- 
- 6 Do one of the following:
    - Select the Instance Counter from the **Instance Counter** list.
    - If the Instance Counter does not exist, select the **Other** check box, and enter the Instance Counter in the box that appears.
  - 7 Do one of the following:
    - Select the WMI Class Name from the **WMI Class Name** list.
    - If the WMI Class Name does not exist, select the **Other** check box, and enter the WMI Class Name in the box that appears.
  - 8 Do one of the following:
    - Select the WMI Property Name from the **WMI Property Name** list.
    - If the WMI Property Name does not exist, select the **Other** check box, and enter the WMI Property Name in the box that appears.
  - 9 Click **Save**.

### To delete a Performance Counter from the Service Center database manually

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 Select the check box beside the performance counter you want to delete.
- 4 In the **Performance Counters** section, click **Delete**.

This Performance Counter will no longer be available for monitoring. Any monitors or monitoring policies currently using this counter will no longer be able to capture this data, but the historical information will still be available for reporting.

### See Also

[Adding a Monitor for Performance Counters](#)

## Adding or Deleting SNMP OIDs

The **Network Objects** tab provides a list of all SNMP OIDs that are available for monitoring. Additional SNMP OIDs can be added here, or any that are not in use can be removed.

There are two types of MIBs: scalar and tabular. Scalar objects define a single object instance whereas tabular objects define multiple related object instances grouped in MIB tables. You can choose to collect tabular OIDs.

---

You can create a tabular monitor for a known base OID, and Managed Workplace will automatically create monitors for all elements within that table

**Note:** Onsite Manager pulls a maximum 1,024 scalar monitors from each tabular monitor definition.

### To add an SNMP OID to the Service Center database manually

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 In the **SNMP OIDs** section, click **Add**.
- 4 Type the Object Name.
- 5 Type the OID.
- 6 From the **Object Type** list, select either **Numeric** or **Text**.
- 7 To collect tabular OIDs, select the **Tabular** check box.
- 8 If desired, in the **Description** box, type a description of the OID.
- 9 Click **OK**.

### To remove an SNMP OID from the Service Center database manually

**Note:** An SNMP OID cannot be removed if it is used by any monitoring rule.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 Select the check box beside the SNMP OID you want to delete.
- 4 In the **SNMP OIDs** section, click **Delete**.

This SNMP OID will no longer be available for monitoring, but the historical information will still be available for reporting.

### See Also

[Adding a Monitor for SNMP Object Identifiers \(OIDs\)](#)

## Adding or Deleting a Custom Network Service

The Network Objects **tab** provides a list of all Network Services that are available for monitoring. Additional Network Services can be added here, or any that are not in use can be removed.

**Note:** When you add a custom network service, it becomes available when configuring monitors, but it will not be automatically detected by the network scan.

---

### To add a network service to the Service Center database manually

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 In the **Network Services** section, click **Add**.
- 4 Type the name of the Network Service in the **Name** box.
- 5 Type the port number in the **Port** box.
- 6 Type the protocol in the **Transport Protocol** box.  
**Note:** Only TCP is currently supported.
- 7 Type the timeout in milliseconds in the **Timeout** box.
- 8 Click **OK**.

### To remove a network service to the Service Center database manually

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Network Objects** tab.
- 3 Select the check box beside the network service you want to delete.
- 4 In the **Network Services** section, click **Delete**.

#### See Also

[Adding a Monitor for Network Services](#)

## Setting How Long to Keep the Data

You can modify the data retention values on a global level, which allows you to keep only the data that is required. This helps to manage the disk footprint of the database.

This value is set to ensure that while users are on vacation and their system is off, it does not get deleted as a stale device.

**Note:** For hosted versions of Service Center, the data retention time is limited by the value set by the host. The host can set a limit for each VAR.

When a device is not responding to the Onsite Manager discovery scan, Service Center retains full asset, description and addressing information for the device, unless another device picks up the same IP address, at which point the IP is marked as stale on the original device. When a workstation picks up a new IP address, the old address is discarded and only the current address is displayed.



---

Workstation class computers have only a single IP address tracked by Managed Workplace, even when multiple interfaces are being scanned with separate addressing, and all other IP addresses are removed by the stale IP process.

Unlike Workstations, there is no stale IP address cleanup routine run against any server-class Windows device or SNMP device.

In some cases, devices that have been removed may continue to be referenced in Service Center as unavailable devices until the specified interval specified triggers the next clean-up. As a remedy, you can specify a shorter interval for cleaning up stale IP addresses, or you can remove devices with stale IP addresses manually.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Data Retention** tab.
- 3 Type a value in days in the **Number of Days of Data to Keep** box.
- 4 Click **Save**.

#### **See Also**

[About Deleting Devices](#)

## Viewing or Changing the Communication Settings

The **Communication Settings** tab allows you to

- view or modify the information provided to Onsite Managers and Device Managers to enable communications with Service Center
- view or modify the information provided to Onsite Managers and Device Managers to enable the remote control capabilities available in Service Center

**Note:** In hosted Service Centers, you can view the communications settings. In on-premise Service Centers, you can change the communications settings.

#### **To view the Service Center website communication settings**

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Communication Settings** tab.

#### **To change the Service Center website communication settings**

**Note:** Changing the Service Center website communication settings is only available for on-premise Service Centers.

---

The information in the Service Center Website Communication Settings section is automatically populated with the following URLs:

- Public Service Center URL
- Public SCMessaging URL
- Internal SCMessaging URL
- Public SCMdm URL
- Internal SCMdm URL

The public URLs are the Internet-facing addresses to which Onsite Managers, Device Managers, and managed mobile devices will report. The internal addresses perform the same function, but work on the same network as the Service Center application server, where a different address may be required due to networking concerns.

These URLs are provided during the installation of Service Center, and may be required for Device Managers and Onsite Managers to access Service Center from both within and outside of a firewall. This information can be modified, if required. The information is provided to Device Managers and Onsite Manager to enable communications with Service Center.

The Public SCMessaging URL must point to the scwebservices.asmx file, which is used to provide the communications.

**Notes:**

- The web page that appears when you browse this URL only provides a mechanism for receiving data and does not confirm that there are no communications issues between Onsite Manager and Service Center.
- Not all features are available if you are accessing the Service Center using a URL that is something other than what appears as the public SCMessaging URL.
- If you change any communication settings, you must restart the Service Center Monitor Windows service on the application server before the changes will take effect.

- 1** In Service Center, click **Configuration > System Settings**.
- 2** Click the **Communication Settings** tab.
- 3** In the **Service Center Website Communication Settings** section, click **Modify**.
- 4** Modify the Public Service Center URL and the Public SCMessaging URL boxes as required.
- 5** Click **Save**.

---

## Setting Default Email Options

You can use the **Alert Configuration** tab to configure the From email address and the SMTP server address so that Service Center can send email alerts and system notifications.

### To set the default email address

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **Email Settings** section, type an email address in the **Message Settings** box.

Depending on the configuration of the SMTP server, this may or may not need to be a valid email address. Most mail servers now verify that a real email address is used. They will bounce or capture messages with a fictive address in mail filters. The mail server doing the screening is linked to the email address of the recipient. If a fictive address is used in the **From** box, the message may not reach the destination if the recipient's mail server is screening messages, which is a common practice.

**Note:** For alert notifications, this email address is used as the From address. For report deliveries, this email address is used as the Reply To address.

### To set the SMTP options

**Note:** The SMTP options are only available for on-premise Service Centers with a modem installed on the application server.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **Server Name** box, type the IP address or FQDN for the SMTP server.
- 4 Type the port in the **Server Port** box.
- 5 If Transport Layer Security (TLS) is used by the mail server to which you will be connecting, select the **Requires TLS** check box.
- 6 Select one of the following option buttons:
  - Anonymous** Allows anonymous logins.
  - Basic** Uses the username and password you specify for the mail server.
- 7 Click **Save**.

---

### To test the email

**Note:** The test email feature is only available for on-premise Service Centers.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **To** box, type a valid email address.
- 4 Enter a subject in the **Subject** box.
- 5 Click **Send**.

## Turning Log Monitoring On or Off

You can have the system check for any possible monitoring failures (such as which monitor is not collecting data). If enabled, you can define the interval that you want the system to check for possible failures (hourly, daily or weekly). The Administrator can be notified when failures occur via a log in the System Viewer and a subsequent email. Email notifications can be set up to be delivered on a selected interval.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **Monitor Failure Settings** section, select the **Enable Log Monitoring** check box.
- 4 From the **Polling Interval** list, select the interval that you want the system to check for monitoring failures.
- 5 Click **Save**.

## Setting System-Wide Alerting Actions for Site Communication Failures

You can set alert actions for a site not communicating at both the system level and at a site level. It is recommended that you first set your system-level defaults, and then override these defaults as needed on the site level. For more information about setting site level alert actions for site not communicating, see [Setting Alerting Actions for Site Communication Failures](#).

Managed Workplace includes three alerts that notify you of site communication failures:

- **Service Center Receive**—triggers when Service Center has not received information from an Onsite Manager for 65 minutes.

- **Onsite Manager Processing**—triggers when 12 hours has passed since an Onsite Manager has retrieved information, such as configuration changes, from Service Center.
- **Site Not Communicating**—status and asset information is sent to Service Center every two minutes. When two updates have been missed, and the alert conditions for both Service Center Receive and Onsite Manager Processing are met, this alert is triggered.

These three alerts form a hierarchy in which the Service Center Receive and Onsite Manager Processing alerts are subsets of the Site Not Communicating alert. The two lower-level alerts can exist simultaneously. However, if two updates have been missed in addition to the conditions required to trigger the lower-level alerts, then the Site Not Communicating alert triggers. The lower-level alerts self-heal, as they are subsumed by the Site Not Communicating alert.

The following table outlines which alerts are triggered for various combinations of site communication failure conditions:

What if...	Then...
Service Center has not received information from Onsite Manager for 65 minutes	the Service Center Receive alert is triggered.
12 hours has passed since an Onsite Manager has retrieved information from Service Center	the Onsite Manager Processing alert is triggered.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center	both the Service Center Receive and Onsite Manager Processing alerts are triggered.
Service Center has not received information from Onsite Manager for 65 minutes and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.

---

What if...	Then...
12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.
Service Center has not received information from Onsite Manager for 65 minutes and 12 hours has passed since an Onsite Manager has retrieved information from Service Center and two updates have been missed.	the Site Not Communicating alert is triggered. Any existing Service Center Receive and Onsite Manager Processing alerts will self-heal, as the Site Not Communicating alert takes precedence.

---

**Default:** When a site is not communicating, Managed Workplace creates a trouble ticket and sends an email to all users for the site whose role is set to receive alert notifications. It is also set to self-heal, by default.

**Note:** This option is not available for a site based on Device Managers.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 Click **Modify**.
- 4 Do the following to change the default alert configuration:
  - To add an alert category when a site is not communicating so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.
  - To create a trouble ticket when a site is not communicating, select the **Create Trouble Ticket** check box.
  - To send an email when a site is not communicating, select the **Send Email** check box and configure the settings.
  - To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.

- 
- 5 Repeat steps 1 to 5 as needed to configure the alert actions for the Service Center Receive and Onsite Manager Processing alerts.
  - 6 Click **Save**.

### See Also

[Setting Alert Actions](#)

[Creating Alert Categories](#)

## Setting System-Wide Alerting Actions for New Devices

By default, Service Center performs a device discovery network scan on sites every 5 minutes. You can configure an alerting action to notify you when new devices are discovered as the result of the network scan.

**Best Practice:** It is recommended that you first set the system-wide alert actions for new devices, and then override the system defaults on a per-site basis, as required. See also [Setting Alerting Actions for New Devices for a Site](#).

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **New Device Alert Configuration** area, click **Modify**.
- 4 Ensure that the **Enable New Device Alert** check box is selected.
- 5 Do the following to change the alert configuration:
  - To add an alert category when a new device is discovered so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.
  - To create a trouble ticket when a new device is discovered, select the **Create Trouble Ticket** check box.
  - To send an email when a new device is discovered, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.
  - To escalate an alert if an alert has not been resolved in a set amount of time, select the **Escalate Alert** check box and select a time after which the Alert Escalation will take effect.
- 6 Click **Save**.

---

## See Also

[Setting Alert Actions](#)

[Creating Alert Categories](#)

[Setting the Device Discovery Defaults](#)

## Setting System-Wide Alerting Actions for Loss of Monitoring Protocol

You can set system-wide alert actions that are triggered when WMI or SNMP ceases to work on a device. This alert determines that monitoring has stopped on a device, and that the monitoring protocol has failed. You can then investigate the root cause of the failure and resolve the problem.

You can set the system-wide alert actions for loss of monitoring protocol, and then override these actions at the site level, if required. See [Setting Alert Actions for Loss of Monitoring Protocol at a Site](#).

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 In the **Loss of Monitoring Protocol Alert Configuration** section, click **Modify**.
- 4 Do the following to change the alert configuration:
  - To add an alert category when the monitoring protocol drops on a device so that it appears on the Central Dashboard, click **Categorize Alert** and add a category from the list. To set up a new alert category, see [Creating an Alert Category](#). Click **Save**.
  - To create a trouble ticket when a monitoring protocol is dropped, select the **Create Trouble Ticket** check box.
  - To send an email when a monitoring protocol is dropped, select the **Send Email** check box and configure the settings. If multiple devices are discovered from the same scan, they will be included in the same email.

## Modifying the Alert Configurations

You can modify the alert configuration for system-wide alerts.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Alert Configuration** tab.
- 3 Under the title of the alert you want to configure, click **Modify**.
- 4 Make changes to the alert configuration.



- 
- 5 Click **Save**.

## Creating Custom Ticket Statuses

You can create custom ticket statuses in Managed Workplace for more comprehensive ticket status mapping with your Connectwise, Salesforce, or Remedy PSA configuration, or simply to create more descriptive ticket statuses for use within Service Center.

If your PSA configuration includes additional ticket statuses that do not easily match up with the four ticket statuses available with Managed Workplace, you can create custom statuses in Service Center, and then map these custom statuses to the appropriate ticket status in your PSA. For more information, see the *Managed Workplace Integration Guide - Service Desks*.

When you create a custom ticket status, you can optionally designate it as a closed status. A closed status indicates that the ticket is not active and no further action is required. For example, you can create an on-hold or resolved ticket status and designate it as closed. You can create multiple closed statuses as required.

**Note:** If you have a Autotask, Tigerpaw, Fieldpoint, Solutions 360, or a custom PSA integration installed, you can create custom ticket statuses, but the only attribute that will be passed to the PSA is whether the ticket is a closed status. For this reason, it is only recommended to create custom ticket statuses if you also have a Connectwise or Salesforce PSA installed.

### To create a custom ticket status

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Ticketing** tab.
- 3 Click **New**.
- 4 Type a name in the **Ticket Status Name** box.
- 5 If the custom status is a closed ticket status, select the **Closed Status** check box.
- 6 Click **OK**.

### To edit a custom ticket status

**Note:** You cannot edit the Managed Workplace system ticket statuses.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Ticketing** tab.
- 3 Click **Edit** in the row for the custom ticket status you want to edit.

- 
- 4 Select or clear the **Closed Status** check box.
  - 5 Click **OK**.

### To delete a custom ticket status

You can delete a custom ticket status if it is not currently mapped to a PSA or service desk ticket status. If it is mapped, a notification message appears, and you must unmap the custom status before deleting it.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Ticketing** tab.
- 3 Select the check box beside the status you want to delete.
- 4 Click **Delete**.

## Working with Printer Transforms

A printer transform is a collection of information about a printer. It is only required if a printer doesn't adhere to the standard printer MIB (which defines the SNMP locations to find print information). Normally, printers will adhere to this standard, but occasionally some data is not in the standard location. In those cases a printer transform can be used that tells the system the custom location of the data. Once applied, Managed Workplace uses the transform to determine the custom location whenever it discovers a printer of that make or model.

Printer transforms are available to install from the Update Center Components page. There are printer transforms available for Hewlett Packard, Lexmark and OKI Data, and new ones will be added in the future. You may want to install all printer transforms for the printers you manage and monitor.

### What You Can Do

When you install a printer transform, it is applied to each site registered with the Service Center regardless of whether you are managing that type of printer at the site or not. After installing, Managed Workplace automatically collects information about that type of printer according to the transform.

When an upgrade for a printer transform is available, a green icon appears beside Update Center > Components in the navigation pane to indicate that there is a new component available for upgrade. You can update printer transforms via the Update Center.

You can export a printer transform and save it as an .XML file.

If you no longer want to use a printer transform, you can delete it.

---

## Details about Printer Transforms

Here is a list of the additional data that is collected by some of the printer transforms currently available:

- Total Color Page Count for Hewlett Packard, Lexmark and OKI Data
- Total Mono Page Count for Hewlett Packard, Lexmark and OKI Data
- Printer Serial Number for Lexmark and OKI Data

## To install a printer transform

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Printer Transforms** tab.
- 3 Click **Get More**.

The **Components** page opens with a list of printer transforms available for installation.

- 4 Select the check box beside each printer transform you would like to install.
- 5 Click **Install**.

## See Also

[Updating and Installing Service Center Components](#)

## To import a printer transform

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Printer Transforms** tab.
- 3 Click **Import**.
- 4 Click **Browse** and locate the file, and then click **Open**.

## To export a printer transform

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Printer Transforms** tab.
- 3 Select the check box beside the name of the printer transform.
- 4 Click **Export**.

## To update a printer transform

- 1 In Service Center, click **Update Center > Components**.

- 
- 2 Click **Updates**.
  - 3 In the **Type** column, select **Printer Transforms** from the list.
  - 4 Select the check box beside the name of each printer transform you want to update.
  - 5 Click **Install**.

### See Also

[Updating and Installing Service Center Components](#)

### To delete a printer transform

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Printer Transforms** tab.
- 3 Select the check box beside the name of the printer transform.
- 4 Click **Delete**.

## Setting Remote Control Options

You can use the **Remote Control** tab to set up system-wide credentials for the remote control tools you frequently use. You can configure access to AVG Business Premium Remote Control, which is a built-in remote control feature that requires minimum configuration. You can also connect using UltraVNC, a custom third party integration with TeamViewer, LogMeIn Pro, or ScreenConnect, and you can set up an “other” remote control tool integration.

**Custom Third Party Integration versus “Other” Option** The custom third party integration provides a direct connection with TeamViewer, LogMeIn Pro, or ScreenConnect. You can set up all three integrations, however only the tool that is selected in System Settings will be available when launching a remote session on a device. The “other” option is a more generic configuration. It can be used with any remote access tool that meets the requirements, and has been tested on GoToAssist, LogMeIn Rescue, LogMeIn Pro, DameWare, and Bomgar.

### Configuring AVG Business Premium Remote Control Access

AVG Business Premium Remote Control uses ISL Light technology to provide remote access to managed devices. Premium Remote Control consists of the following components:

- AlwaysOn - An agent that is automatically installed on all eligible managed devices.

- 
- AVG Business Premium Remote Control.exe - A client that you install on your computer. When you initiate a remote control session with Premium Remote Control, the client opens automatically for you to connect to the managed device.

When you enable AVG Business Premium Remote Control, a remote control account is automatically set up, without the need for configuration. The agent is then automatically installed on managed devices across all sites that meet the following criteria:

- A Windows device with the Admin share open;
- A Mac device with SSH enabled. The credentials for SSH must also be on the sudoer's list.

**1** In Service Center, click **Configuration > System Settings**.

**2** Click the **Remote Control** tab.

**3** By default, the installation path for the AVG Premium Remote Control agent is:

%Program Files%\AVG\Premium Remote Control\AVG Control.exe

To change the installation folder, type a new installation path in the **Application Path** box.

**4** If you have not yet installed the Premium Remote Control client, click the link to download the client to your computer.

**Note:** Once the AVG Business Premium Remote Control client is installed on your machine, you will be prompted for your AVG Business SSO credentials. If you are not using AVG Business SSO, you can simply close this window and AVG Business Premium Remote Control will launch on the device.

**5** Click **Save**.

**Tip:** If you need to remove the AVG Business Premium Remote Control agent from a device, Managed Workplace includes scripts to uninstall AVG Premium Remote Control. To run the script on a device, go to **Automation > Library**, and select one of the following scripts:

- Uninstall AVG Business Premium Remote Control MAC
- Uninstall AVG Business Premium Remote Control WIN

## Configuring Ultra VNC Access

**1** In Service Center, click **Configuration > System Settings**.

**2** Click the **Remote Control** tab.

- 
- 3 In the **UltraVNC** section, fill in the following:
    - By default, UltraVNC will use port 5900 to access the remote machine. To change this, type a different port number in the **Remote Machine Port** box.
    - To automatically install the remote UltraVNC agent if it is not installed on the remote machine, select the **Install remote agent if not installed** check box.
    - In the **Password** box, type the UltraVNC password.
    - Optionally, select the **Uninstall remote agent when complete** check box to uninstall the UltraVNC agent from the remote machine after the session has ended.
    - In the **Application** path, type the file location where UltraVNC is installed.
  - 4 Click **Save**.

**Note:** Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

### Configuring a Custom Third Party Integration

You can set up access credentials to TeamViewer, LogMeIn Pro, and ScreenConnect. The integration type that you select will appear as an option when launching a remote session on a device. You can select only one integration. By default, no custom third party integration is selected.

#### To configure TeamViewer access

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Remote Control** tab.
- 3 In the **Custom Third Party Integration** area, select the **TeamViewer** option button.
- 4 In the **Application Path** box, type the file location where TeamViewer is installed on the technician's computer.
- 5 In the **Global Password** box, type the TeamViewer password. This password will override the client password on the remote machine. Optionally, you can leave this box blank, and then provide a password when launching a TeamViewer session.
- 6 Click **Save**.

---

**Note:** Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

### To configure LogMeIn Pro access

When configuring LogMeIn Pro, you must provide a Company ID and a PSK encryption key, which you must request from LogMeIn support.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Remote Control** tab.
- 3 In the **Custom Third Party Integration** area, select the **LogMeIn Pro** option button.
- 4 In the **Company ID** box, type your company ID.
- 5 In the **PSK** box, enter the PSK encryption key provided to you by LogMeIn.
- 6 Click **Save**.

**Note:** Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

### To configure ScreenConnect access

ScreenConnect uses a web-based remote access mechanism, while the client PC must have the end-user software installed. When you configure system-wide ScreenConnect settings, you provide the base URL to your self-hosted ScreenConnect site. Optionally, you can also specify which folder to open by default, e.g. “/Host # All Machines”.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Remote Control** tab.
- 3 In the **Custom Third Party Integration** area, select the **ScreenConnect** option button.
- 4 In the **Base URL** box, enter the base ScreenConnect URL.
- 5 Optionally, in the **Folder** box, enter the name of the subsection of the ScreenConnect UI that you want to open when ScreenConnect is launched.
- 6 Click **Save**.

**Note:** Click the **Clear Overrides** button to delete all device and user level overrides and to save changes. A dialog box will prompt you to confirm the action.

---

## Configuring the “Other” Remote Control Application

If you are using third-party remote control tool to assist your customers, you can create a link to launch this application from within Managed Workplace. You can do this by configuring an “other” option when initiating a remote control session, in one of the following:

- From a device page, by clicking **Remote Control** in the sidebar.
- In the **Remote Control** shortcut menu, which is available by clicking the shortcut icon beside a device name in a device list. The **Remote Control** shortcut menu displays the third-party tool specified as the “Other” option, and any remote control options available for the selected device.

You can create a shortcut link to any remote control tool that meets the following requirements:

- the tool is launched from a URL, either on the client computer or the technician’s computer, or the tool is launched as an application on the technician’s computer.
- preferably, the URL link or application executable contains all information required to fully establish remote connectivity.

The following remote control applications have been tested for integration with Managed Workplace:

Remote Control Tool	Launch Method
GoToAssist	Launch URL on client computer
LogMeIn Rescue	Launch URL on client computer
LogMeIn Pro	Launch URL on technician computer
DameWare	Launch application on technician computer
Bomgar	Launch URL on client computer

### Notes:

- You can create one shortcut link to a third-party remote control tool.
- When creating a shortcut link to Dameware, you must enter the application parameter `m: {ipaddress}`, and this setting should not be altered at the device level. This parameter passes the IP address for the specific device to the DameWare application and will automatically create an entry or load an existing entry in DameWare for the IP address. Additionally, Dameware does not support



---

connection through the Onsite Manager socket, so this option should not be selected when configuring the global settings. DameWare offers a proxy utility that can be installed on the client network, which can be used as an alternate method of connecting. To download this utility, go to <http://www.dameware.com/downloads.aspx>.

When setting up the third-party selection item, you provide the following information:

- The name of the third-party tool as it will appear in the Remote Control shortcut menu;
- whether to launch a URL on the technician's computer, launch the application on the technician's computer, or launch a URL on the client's computer;
- if launching an application on the technician's computer, the application path and parameters. You must also specify whether a socket connection is required, including the port number.

**Note:** The configuration that you provide can be overridden at the device level. For more information, see [Initiating a Remote Control Session by Launching a Third-Party Remote Control Tool](#).

### To add an "other" link to the Remote Control shortcut menu

**Best Practice:** For remote control applications that launch a URL on either the client computer or technician computer, it is recommended that you leave the URL box blank, as in most cases the technician will enter a session-specific URL when initiating the remote control session.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Remote Control** tab.
- 3 In the **Name** box, type the name of the third-party remote control tool.
- 4 Do one of the following:
  - Click the **Launch URL on Tech computer** option button, and optionally, type the global default URL for the remote control application in the **URL** box.
  - Click the **Launch Application on Tech computer** option button. In the **Application path** box, type the path to the folder where the application is installed. If required, in the **Application Parameters** box, provide any required application parameters. If the application require a socket connection to the Onsite Manager server, select the **Socket connection required** check box, and in the **Port** box, type the port number.

- 
- Click the **Launch URL on Client computer** option button, and optionally, type the global default URL for the remote control application in the URL **box**.

5 Click **Save**.

## Configuring Secure Sign On

AVG Business SSO (Secure Sign On) is a stand-alone application that is included with your Managed Workplace license. With AVG Business SSO, you log in to your computer using your Active Directory account, and from there you can access the AVG Business SSO User Portal to launch your most frequently used applications, including Managed Workplace, AVG CloudCare, your PSA solution, and many more.

AVG Business SSO includes the following components:

**Business SSO User Portal** A web-based dashboard that displays the applications you can sign in to, including Managed Workplace.

**Business SSO Cloud Manager** The administrative interface of AVG Business SSO, which you use to manage the User Portal by adding and removing users and applications.

**Business SSO Cloud Connector** An on-premise component that you install in your Active Directory environment -or, if you are reselling, in your client's Active Directory environment - that acts as a source for user accounts for AVG Business SSO.

To set up AVG Business SSO, you must perform the following steps:

- 1 Configure Service Center to use SSL, if you have not done so already. SSL is required for SSO to be configured in Service Center.  
**Note:** If you are using a hosted environment, your Service Center is already configured to use SSL and no action is required.
- 2 Register for SSO by contacting your AVG salesperson. You will receive an email with access to the Business SSO user portal.
- 3 Log in to your domain controller.
- 4 Log in to the Business SSO user portal, switch to the Cloud Manager view, and download SSO Cloud Connector to the domain controller. See [Downloading Cloud Connector to your Domain Environment](#).
- 5 Add the Managed Workplace application to the Business SSO user portal, if it is not already there. See [Adding the Managed Workplace Application to the SSO Portal](#).
- 6 Configure SSO in Service Center. See [Configuring SSO in Service Center](#).

- 
- 7 Invite users to the User Portal from the Cloud Manager. See [Inviting Users to the Business SSO Portal](#).

## Downloading Cloud Connector to your Domain Environment

The Cloud Connector is a software package that you install on a Windows computer inside your firewall that lets you use your Active Directory accounts to authenticate users with Active Directory accounts for access to the administrator and user portals.

- 1 Log in to the SSO User Portal.
- 2 To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.
- 3 Click the **Settings** tab.
- 4 In the left pane, click **Cloud Connectors**.
- 5 Click **Add Cloud Connector**.
- 6 Run through the guided steps to download Cloud Connector to your domain environment. Note that you must register the Cloud Connector by entering your admin user name and password.

Now that Cloud Connector is installed in your domain environment, you are ready to add the Managed Workplace application to the SSO portal.

## Adding the Managed Workplace Application to the SSO Portal

The AVG Business SSO includes thousands of applications that you can add, including Managed Workplace. When you register for the User Portal, the Managed Workplace application is included by default. If the Managed Workplace application is not included, you must add it to the user portal to enable Managed Workplace SSO.

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Secure Sign On** tab.
- 3 In the **Service Provider Information** area, copy the Service URL. You will be pasting this URL into Cloud Manager in a few steps.
- 4 Log in to the SSO User Portal.
- 5 To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.
- 6 Click the **Apps** tab.
- 7 Click **Add Web Apps**.
- 8 In the search box, type Managed Workplace.

---

9 Click the **Add** button beside Managed Workplace.

10 Click **Yes** to add the application.

11 Click **Close**.

Managed Workplace now appears in the **Apps** list. Now you will download the signing certificate to be uploaded to Service Center.

12 In the **Service URL** box, paste the URL you copied in step 3.

13 Copy the URL from the **Identity Provider Sign-In URL** box. You will be pasting this URL in Service Center.

14 Scroll down and click the **Download Signing Certificate** link. You will be uploading this certificate to Service Center.

Now you are ready to complete the SSO configuration in Service Center.

### Configuring SSO in Service Center

After adding the Managed Workplace app to the Business SSO portal, you must upload the security certificate into Service Center, and paste the sign-in URL.

1 In Service Center, click **Configuration > System Settings**.

2 Click the **Secure Sign On** tab.

3 In the **Identity Provider Information** section, click **Modify**.

4 Select the **Enable identity provider** check box.

5 Click **Upload** to upload the certificate you downloaded from Cloud Manager.

6 In the **Identity Provider Sign in URL** box, paste the URL you copied from Cloud Manager.

7 Click **Save**.

### Inviting Users to the Business SSO Portal

If you have downloaded Cloud Connector to your domain environment, users are automatically added to the Business SSO user portal using their Active Directory accounts. As a final step, you must invite users to access the portal. When you invite a user, an email is automatically sent with their log in credentials to the user portal.

1 Log in to the SSO User Portal.

2 To access Cloud Manager, click your user name in the top right corner, and then click **Switch to Cloud Manager**.

3 Click the **Users** tab.

- 
- 4 Select the check box beside each user you want to invite.
  - 5 From the **Actions** list, select **Send email invite for user portal setup**.
  - 6 Click **Yes** to proceed.

## Collecting Diagnostics for Support Purposes

Managed Workplace includes a diagnostics tool that you can run to collect information on your Service Center, Onsite Manager, and Device Manager installations to help AVG support technicians determine whether your environments meet system requirements, and help them quickly determine the root issue. Support diagnostics can decrease time to resolution, and help AVG technicians determine whether they need to escalate your issue for resolution.

The **Support Diagnostics** tab includes a history of the diagnostics that were run in the past 72 hours. After 72 hours, this data is purged. At any time you can download the diagnostic data displayed on the **Support Diagnostics** tab. The data is a collection of log files condensed in a zip file, for easy email delivery to the AVG support team.

### To collect Onsite Manager diagnostics for a site

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Support Diagnostics** tab.
- 3 Expand the **Add OMs to Diagnostics Query** section by clicking the expanding arrow.
- 4 In the **Add to Diagnostic Query** column, click the green arrow to select the OM site.  
  
The site is added to the **Diagnostics Query** section at the bottom of the screen.
- 5 Repeat steps 2 to 4 until you have added all of the Onsite Managers on which you want to run diagnostics.
- 6 Click **Run Diagnostics**.

### To collect Device Manager diagnostics

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Support Diagnostics** tab.
- 3 Expand the **Add DMs to Diagnostics Query** section by clicking the expanding arrow.

- 
- 4 In the **Add to Diagnostic Query** column, click the green arrow to select a Device Manager.

The Device Manager is added to the **Diagnostics Query** section at the bottom of the screen.

- 5 Repeat steps 2 to 4 until you have added all of the Device Managers on which you want to run diagnostics.
- 6 Click **Run Diagnostics**.

#### To download diagnostic data

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Support Diagnostics** tab.
- 3 Do one of the following:
  - To download diagnostics that you have just selected, in the **Diagnostics Query** section, click **Download Diagnostics**.
  - To download diagnostics that were run in the past 72 hours, in the **Diagnostics Performed in last 72 hours** section, click **Download Diagnostics**.

The diagnostic data for all of the Onsite Manager sites and Device Managers that were added to the **Diagnostics Query** section is downloaded to a .zip file.

## Configuring Modems

#### To set up a modem

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Modem** tab.
- 3 In the **Modem Configuration** section, select the correct options in the boxes.
- 4 Click **Save**.

#### To test a modem

- 1 In Service Center, click **Configuration > System Settings**.
- 2 Click the **Modem** tab.
- 3 In the **Test Modem Configuration** section, select the correct options in the boxes.
- 4 Click **Send**.







CHAPTER  
**22**

## **WORKING WITH MOBILE SERVICE MANAGER**

---

*This section provides detailed information about the following topics:*

- *Mobile Service Manager*
  - *Logging In and Out on a Mobile Device*
  - *Viewing an Alert on a Mobile Device*
  - *Clearing an Alert on a Mobile Device*
-

---

## Working with Mobile Service Manager

### About Mobile Service Manager

You can access Service Center from your mobile device and then view, suppress, and clear alerts. By choosing the Mobile Service Manager button, you will be able to work with alerts on your mobile device. If you click Service Center, you will see the full Service Center website (which is best viewed from a tablet or desktop).

**Note:** In the browser settings for your device, ensure cookies are enabled.

### Logging In and Out on a Mobile Device

#### To log in to Service Center from a mobile device

- 1 Launch a browser on your mobile device.
- 2 Browse to the Service Center web console.
- 3 Type your user name, password and VAR domain, if required.
- 4 To work with alerts, click the **Mobile Service Manager** button. To work with the full Service Center website, click **Service Center**.

#### To log out of Mobile Service Center

- Tap **Log Out**.

### Viewing an Alert on a Mobile Device

A list of open alerts is displayed in Mobile Service Manager. Alerts are listed in chronological order with new ones first. Initially, you see the latest 25 alerts. You can click the More button to see 25 more alerts.

You only see alerts that your user account allows you to see.

**Note:** You can view up to 500 alerts on a mobile device.

#### To view more alerts

- Tap the **More** button.

#### To refresh the screen

- Tap the **Refresh** button.

---

### To view an alert

- Tap the alert.

## Suppressing an Alert on a Mobile Device

When you suppress an alert from a mobile device, you can choose to suppress it forever, or until a specified date.

- 1 Tap the alert.
- 2 Scroll to the bottom of the alert and tap **Suppress**.
- 3 Do one of the following:
  - Tap the **Forever** option to suppress the alert indefinitely.
  - Tap **Suppress Until**, and then tap a date from the calendar to suppress the alert until a specified date.
- 4 Tap **OK**.

## Clearing an Alert on a Mobile Device

You can clear one alert at a time. When you clear an alert, you can enter resolution notes.

- 1 Tap the alert.
- 2 Scroll to the bottom of the alert and tap **Clear**.
- 3 Type in any resolution notes.
- 4 Tap **OK**.



## GLOSSARY

**Active Management Technology (AMT)** Technology developed by Intel® included with vPro™ chips, that provides Managed Workplace with the ability to capture system board level events and remotely power cycle devices.

**Alert** The notification used to inform operators of Managed Workplace that data being monitored is in a user-defined state. Alerts appear on the Central Dashboard and Alerts Viewer for Service Center, and may additionally trigger email notifications or trouble ticket creation. Some types of alerts can clear themselves, or self-heal, when the condition no longer exists.

**Alert Actions** Alert actions are automated processes that can be set for each alert configuration. The available actions include creating a trouble ticket, self-healing when the condition no longer exists and running a script.

**Alert Category** Organizational units for the presentation of alert indicators on the Central Dashboard. Alert categories can also be used to add specificity to reporting and alert schedules. Alert categories are automatically added to the Central Dashboard when monitoring policies that use them are imported.

**Alert Notifications** Alert notifications are rules set in each alert configuration that define who is contacted when the condition occurs, and by what means.

**Alerts Viewer** Designed for network operation centers' wallboards and displays and prioritizes alerts in real-time as they appear on the Central Dashboard. Audible cues can be configured to notify operators that new alerts have arrived.

**Application Programming Interface (API)** The Managed Workplace API allows qualified Partners with programming resources to inter-operate with Service Center, describing the methods and calls used to insert or extract data from the database via a web service.

**Approval Group** Approval groups are used only with Patch Management so that Microsoft updates can be approved for multiple devices at once. AVG recommends that approval groups be organized by operating system type.

**Authentication** Authentication is when an identity is proven to a network application or resource. This is usually handled either through credentials, such

---

as a username and password pair, or a cryptographic operation, such as using a private and public key pair. In Managed Workplace, users authenticate their identities with login credentials to Service Center. Authentication also takes place between Onsite Manager and Service Center when communications occur, with or without the use of Secure Sockets Layer certificates.

**Central Dashboard** The primary display for alerts in the Service Center interface, the Central Dashboard organizes alert indicators by sites, groups, and alert categories.

**Data Point** A data point is the measurement of the status of a device or application for a single sample. The frequency at which the samples are taken is referred to as the polling interval.

**Device** A unique responding hardware device Onsite Manager identifies on a network.

**Device Alias** A user-input identifier for a device. AVG recommends using device aliases so Service Center users can easily identify devices. This is especially true on networks where the discovered names of devices are very similar due to a strict DNS naming convention.

**Device Manager** The functional equivalent of Onsite Manager but monitors and manages a single device only. There is a database, but it is bundled with the lightweight application.

**Discovered Name** The identifier that Onsite Manager assigns to a device it discovers on a network, the discovered name is taken from DNS, the device host name or the sysName.0 OID.

**Domain Name System (DNS)** A system by which IP addresses are matched to friendly host names. DNS will need to be accessed to create host name records so that the URLs used to access Managed Workplace may be resolved.

**Dynamic Host Configuration Protocol (DHCP)** A protocol used by networked computers to automatically receive IP addresses and corresponding networking information, such as the Internet Gateway and Subnet Mask.

**Escalation Notification** A setting in each alert configuration that allows operators to define who to notify when an alert condition has gone unresolved for a predetermined length of time.

**Foundation Technology** Managed Workplace integrates with a number of Microsoft applications for its core functionality, including ASP.NET, IIS, SQL Server, MBSA and WSUS. These are referred to as the foundation technologies.

**Groups** Groups are organizational containers against which monitoring policies are applied. There are two types: service groups and site groups.

---

**Hypertext Transfer Protocol (HTTP)** A protocol used to transport data over networks, primarily the Internet.

**Internet Control Message Protocol (ICMP)** A protocol used by Managed Workplace to determine whether devices are able to respond to an ICMP ECHO request, which defines whether the devices are considered Up or Down.

**Internet Information Services (IIS)** Microsoft's web server, which also handles mail and news. Managed Workplace uses IIS to host various websites, services and application pools, and can use the built-in virtual SMTP mail server.

**Internet Protocol (IP)** A protocol used for communications across packet-switching internetworks.

**Internet Security and Acceleration (ISA)** Microsoft's stateful packet and application layer firewall, which also handles Virtual Private Networks and Web Caching (proxy server).

**Managed Device** A managed device is one from which Onsite Manager is collecting information. To collect as much information as possible, and to enable all features of Managed Workplace, either WMI or SNMP management protocols need to be enabled. Managed devices running a Windows operating system can have both management protocols enabled.

**Management Information Base (MIB)** A collection of objects (OIDs) in a (virtual) database used to manage devices on a network. MIB files may be used when creating monitors in Service Center.

**Media Access Control (MAC)** A unique identifier for a network adapter. Managed Workplace uses the MAC address as part of the evidence to identify unique devices.

**Microsoft Baseline Security Analyzer (MBSA)** A utility that audits the security on Windows operating systems and applications. Onsite Manager by default will run MBSA scans against all Windows devices on a network once a week.

**Microsoft Desktop Engine (MSDE)** A free, scaled-down version of Microsoft SQL, with a 2 GB database size limit. This has been replaced by Microsoft SQL 2005 Express, which has a 4 GB database size limit. Onsite Manager may use either of these to host its database (MWData). SQL Express is included with the Onsite Manager installer.

**Network Services** Applications requiring open TCP ports that Onsite Manager is able to monitor. A default list of the most common network services are automatically scanned and discovered, but custom network services may also be added through Service Center.

**Object Identifier (OID)** A unique object listed in the Management Information Base (MIB) for a Device.

---

**Onsite Manager (OM)** Onsite Manager is the component of Managed Workplace installed on remote networks to collect monitoring data, run scripts, route remote control sessions and deploy software updates.

**Patch Management** A Managed Workplace feature that integrates with servers at remote sites to centralize their management. This allows Partners to approve and install Microsoft updates to a wide variety of operating systems and applications.

**Performance Counter** Performance Counters represent data on specific aspects of a system or service. Monitoring of performance counters is one of the primary means of collecting information about Windows devices in Managed Workplace.

**Monitoring Policy** A monitoring policy is a collection of monitors and associated alert rules for a specific application or hardware device. AVG provides an ever-growing library of predefined monitoring policies delivered with each release, and makes new monitoring policies available in the Update Center as they are created.

**Polling Interval** A monitor's polling interval is the frequency with which the status of the monitored device or application is sampled. Each sample that is taken is referred to as a data point.

**Ports** The Transport Layer Protocols TCP and UDP use identifiers called ports to logically separate services from one another. Access to certain ports by direction (inbound or outbound) can be configured in firewalls and other network infrastructure devices.

**Professional Services Automation (PSA) Systems** PSA systems are used to manage the delivery of client projects, and the resources that are required for those projects, such as skilled personnel and equipment. In addition to project management, other typical functions include time recording, billing, and reporting. Managed Workplace can integrate with Salesforce, Autotask, ConnectWise, Tigerpaw, and others.

**Proxy Server** A server that allows clients to make indirect network connections to other networks. Onsite Managers can be configured to communicate with Service Center through a proxy.

**Remote Desktop Protocol (RDP)** The protocol used to connect remotely to Microsoft Terminal Services. Client software is included with all modern versions of the Windows operating system (those released following Windows 2000).

**Secure Shell (SSH)** A protocol that uses public-key encryption to establish a secure remote connection to a device. Managed Workplace uses the PuTTY client application to establish these connections.



---

**Secure Sockets Layer (SSL)** A cryptographic protocol that provides secure communications over internetworks for data transfers by confirming the identity of the connected devices. SSL may optionally be used to secure the web pages used for the communications and operations of Managed Workplace.

**Service Center (SC)** Service Center refers to both the centralized database and application servers that collect incoming monitoring data from remote networks and also the user interface that operators use to view and manipulate the data.

**Service Center Monitor** A Windows service installed on the Service Center application server that receives the monitoring telemetry from Onsite Managers.

**Service Group** The recommended organizational container for devices in Managed Workplace, which may contain devices from multiple sites. The advantage of service groups comes from the ease of administration they offer when managing like devices or applications.

**Simple Mail Transfer Protocol (SMTP)** The favored protocol used for email transmission. Managed Workplace makes use of an SMTP server to send email alerts.

**Simple Network Management Protocol (SNMP)** A protocol used to monitor devices for conditions requiring attention. An implementation of SNMP is available for most operating systems, and most hardware devices make use of this protocol to report status. SNMP is the primary means by which Managed Workplace monitors network devices and non-Windows operating systems.

**Site Group** An organizational container for devices related to a single customer site. The advantage to using site groups comes from the ease of identifying alerts occurring on a per-site basis, and they also provide a means by which you can easily apply monitoring policies for customers with unique requirements.

**SNMP Trap** A message sent from an SNMP-enabled device, advising of a condition being present on the device. Onsite Manager is an SNMP Trap receiver, and must be configured as such in the SNMP-enabled device to capture the SNMP Traps sent out.

**SNMP-enabled** Devices are considered to be SNMP-enabled when configured with a community string that is listed in the Onsite Manager network scan. Matching community strings allows Onsite Manager to query the status of the devices using the SNMP protocol. Hardware devices, most operating systems and applications can all report status using SNMP.

**Structured Query Language (SQL)** A computer language used to perform operations against a database. Managed Workplace requires that Microsoft

---

SQL Server 2000/2005 be used to house the Service Center database (SCData). Onsite Manager may be housed on Microsoft SQL Server 2000/2005, or the stripped down free versions, MSDE (Microsoft Desktop Engine) or SQL 2005 Express.

**Subnet** A subnet is a partitioned range of logical addresses (IP addresses).

**Syslog** A protocol and standard used for sending status messages between devices on an IP network. Onsite Manager is a syslog receiver and by default captures all syslog messages sent to it.

**Telnet** A client/server protocol that is implemented in Managed Workplace remoting. This may be used to remote into devices that are configured as a Telnet server.

**Transmission Control Protocol (TCP)** A transmission protocol that exchanges streams of data from sender to receiver in a connection full session. This is the primary protocol used to transport information from Onsite Manager to Service Center.

**Trouble Ticket** A trackable list of notes for a specific issue that has occurred. Tickets may be created as alert actions or manually, and may also be synchronized with third-party (Professional Services Automation (PSA) systems.

**Uniform Resource Locator (URL)** A uniform syntax used to locate resources over a network.

**User Datagram Protocol (UDP)** A connectionless protocol, typically used to broadcast messages over a network.

**Virtual Network Computing (VNC)** A client/server desktop sharing suite that makes use of the RFB protocol. Managed Workplace supports any VNC implementation being used to establish remote sessions.

**Virtual Private Network (VPN)** A means of creating a private network communicating over a public network.

**Virtual Service Center (VSC)** A Service Center used by a Partner that is not installed on their premises, but is instead made available by a Managed Workplace hosting provider.

**Windows Events** Windows Events are information events recorded in Windows log files that may be read using the Event Viewer. Managed Workplace monitors Windows Events for definable conditions, and generates alerts when the conditions are discovered on a device.

**Windows Management Instrumentation (WMI)** A component of the Windows Operating System that is used as an interface through which operating system components can provide information and notifications. WMI

---

is the primary means by which Managed Workplace retrieves information about Windows devices.

**Windows Remote Management (WinRM)** Microsoft's implementation of WS-Man.

**WMI-enabled** Devices are considered to be WMI-enabled when Onsite Manager has the ability to query the technology for status updates. Only Windows devices can be WMI-enabled.

**WS-Management (WS-MAN)** - A management system based on open DMTF and Internet standards that provides a common way for systems to access and exchange management information over a networked infrastructure. Managed Workplace accesses WMI over WS-MAN when it is available on a device.



---

© 2016 AVG Technologies. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, without the prior written permission of AVG Technologies. While every precaution has been taken in the preparation of this document, AVG Technologies assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Managed Workplace is a registered trademark of AVG Technologies.

Adobe and Acrobat are registered trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Microsoft, Windows, and Windows Server are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries.

All other brands, product names, company names, trademarks, and service marks are the properties of their respective owners.

This guide was updated on October 19, 2016 1:34 pm



---

## A

accounts, user, 160

adding

- basic ticket option to Support Assistant, 590
- cloud services monitors, 352
- custom network service, 607
- detailed ticket option to Support Assistant, 591
- device to task, 415
- email address to Support Assistant, 588
- group to task, 415
- hyperlink for logo, 601
- IP addresses to scan, 110
- logo, 600
- monitor for mobile devices, 265, 323
- monitors to devices, 226
- notes about devices, 221
- performance counters, 605
- power plan, 569
- predefined ticket option to Support Assistant, 589
- range of IP addresses to scan, 110
- role to user account, 162
- SNMP OIDs, 606
- SNMP V1/V2 community strings to scan, 121
- subnet scan, 110
- task to device, 227
- text-based message to Support Assistant, 589
- user account to role, 171
- web link to Support Assistant, 592

aggregate reports, 465, 473

alert categories

- description, 366

alert configurations, viewing, 45

alert on success, 374

alerting, 50, 358

alerts

- best practices, 372
- categorizing, 368
- clearing, 366
- clearing for websites, 40
- creating categories, 367–368
- creating schedules, 371

---

- creating trouble tickets, 41
- deleting categories, 369
- deleting schedule, 372
- description, 42, 50, 358
- detail, description, 44
- disabling schedule, 372
- email notification, 360
- enabling schedule, 372
- escalating, 364
- filtering by category, 369
- pager notification, 364
- refresh options, 602
- renaming categories, 368
- running a script, 363
- schedules, 370
- setting, 359
- setting number in Alerts Viewer, 44
- setting schedules, 370
- site not communicating, 137
- suppressing, 364
- trouble ticket notification, 361
- viewing cleared, 366
- viewing list, 44

Alerts Viewer

- description, 42
- renaming, 43
- setting number of alerts, 44
- setting sounds, 43
- sorting, 44
- viewing, 43
- viewing full screen, 43

alias names, assigning to devices, 218

AMT event monitors, 312

AMT-enabled devices

- KVM, remote control, 509
- remote control, 507

Android Restrictions policy

- configuring, 282

AntiVirus

- creating a new policy, 425
- installing, 425–426

APNs certificate



---

- creating, 249
- deleting, 253
- importing, 250
- setting up, 249

APNs certificate request, deleting, 252

Apple Restrictions policy

- configuring, 274
- description, 267

applications, viewing on devices, 211

applying

- policy modules to devices, 305
- policy modules to groups, 305
- power plan to device, 569
- power plan to group, 569
- service modules to devices, 226
- Windows Update Agent Policy to devices, 540
- Windows Update Agent Policy to groups, 540

approval groups

- creating, 543
- deleting, 544
- description, 542
- moving devices, 544

Approve sites, 133

approving

- patches automatically, 556
- patches manually, 553
- patches, process, 534
- sites, 133

archiving reports, 484, 486

Asset Discovery, 146

asset management, 202

asset tag, viewing for device, 219

assets

- description, 35
- getting on mobile devices, 258
- scanning, 228
- viewing SNMP, 35
- viewing SNMP-enabled inventory, 35
- viewing Windows, 35

assigning

- alias names to devices, 218
- inventory tag to device, 219

---

## B

- backing up policy modules, 303
- bandwidth monitors, 314
- baseline
  - creating for power management, 566
  - power consumption, 563
- basic ticket
  - adding to Support Assistant, 590
  - description, 588
- best practices
  - alerting, 372
  - analyzing results, 373
- branding, Service Center, 600

## C

- categories
  - alerts, 366
  - reports, 478, 481
- categorizing alert, 368
- Central Dashboard
  - description, 34
  - hiding service groups, 37
  - hiding site groups, 37
  - refresh options, 602
  - showing service groups, 37
  - showing site groups, 37
  - viewing, 34
- changing
  - password, 33
  - tasks, 418
- clearing
  - alerts, 366
  - website alerts, 40
- closing
  - Results tab, 233
  - trouble tickets, 580
- cloud services monitors, 347
- cloud services, adding monitors, 352
- colors, setting for Service Center, 601
- community strings
  - adding to scan, 121

---

- computers, waking, 234
- configuring
  - Intel® AMT credentials, 239
  - network settings for Intel® vPro™ devices, 237
- contact information, changing, 135
- context menu
  - Device Manager, 587
  - moving items up and down, 593
  - Support Assistant, 587
- copying
  - Device Manager system tray profile, 594
  - power plan, 570
  - tasks, 419
- creating
  - alert categories, 367–368
  - alert schedules, 371
  - AMT event monitors, 312
  - APNs certificate, 249
  - approval groups, 543
  - bandwidth monitors, 314
  - cloud services monitors, adding, 347
  - custom log file monitors, 316
  - Device Warranty monitors, 319
  - groups using Local Users and Groups, 520
  - MBSA report monitors, 321
  - MDM certificate signing request, 248
  - Microsoft System Center Essentials (SCE) monitors, 331
  - monitors, 311
  - network services monitors, 325
  - new user using Local Users and Groups, 520
  - patch status monitors, 327
  - performance counter monitors, 328
  - policy modules, 310
  - report categories, 481
  - report schedules, 482
  - reports, 466, 469
  - roles, 170
  - service groups, 178
  - site groups, 178
  - SNMP from MIB monitors, 335, 337
  - SNMP monitors, 332
  - SNMP Trap monitors, 337

---

- trouble tickets, 579
- trouble tickets for website alerts, 41
- user accounts, 161
- website monitors, adding, 347
- Windows Event monitors, 340
- Windows Services monitors, 346

custom log file monitors, 316

customizing

- devices, 217
- Service Center, 600

## D

- data retention, setting, 608
- declining patches manually, 555
- defaults, setting power costs and usages, 564
- defining addresses to monitor, 108
- deleting
  - alert categories, 369
  - alert schedule, 372
  - APNs certificate, 253
  - APNs certificate request, 252
  - approval groups, 544
  - archived reports, 486
  - context menu item for Device Managers, 593
  - custom network services, 607
  - devices, 228
  - down devices automatically, 120
  - exclusion rules, 118
  - existing logo, 601
  - groups using Local Users and Groups, 521
  - IP address from scan, 112
  - logo from Service Center, 601
  - MDM CSR signing certificate, 251
  - MIB files, 336
  - mobile device configuration policies, 282
  - monitor from policy module, 308
  - performance counters, 605
  - policy modules, 304
  - power plan, 570
  - report categories, 482
  - reports, 480

---

- role from user account, 162
- roles, 173
- scheduled reports, 485
- scripts, 408
- service groups, 200
- service modules, 492
- site groups, 200
- sites, 133
- SNMP OIDs, 606
- Support Assistant system tray profile, 598
- tasks, 419
- user account from role, 171
- user accounts, 164
- users using Local Users and Groups, 520
- Windows Update Agent Policy, 541

delivery schedules, 482

deploying

- Device Managers, 124

description

- alert, 42
- Alerts details, 44
- Alerts Viewer, 42
- approval groups, 542
- assets, 35
- basic ticket, 588
- Central Dashboard, 34
- detailed ticket, 588
- Device Manager, 32, 123
- devices, 204
- grouping, 36, 176
- Intel® vPro™ devices, 236
- monitoring, 37
- Network Services dashboard, 37
- Onsite Manager, 32
- Patch Policy, 531, 536
- predefined ticket, 587
- report, 46
- roles, 169
- Service Center, 32
- service group, 36, 176
- site group, 36, 177
- sites, 98

---

- Support Assistant, 584
- support assistant policy, 584
- user account, 160
- Websites dashboard, 38
- Windows Inventory, 203
- Windows Update Agent, 531
- detailed ticket
  - adding to Support Assistant, 591
  - description, 588
- device
  - overriding power plan settings, 571
  - removing power plan, 570
- Device Discovery, 146
- Device Managers, 123
  - context menu, 587
  - copying system tray profile, 594
  - deleting context menu item, 593
  - description, 32
  - downloading, 124
  - editing system tray profile, 594
  - emailing installation link, 124
  - icons, 586
  - installing, 124
  - rebooting, 126–127
  - searching, 125
  - uninstalling, 126
  - upgrading, 125, 595
  - using, 598
- device names, 205
- device reports, 465
- Device Warranty monitors, 319
- devices
  - adding monitors, 226
  - adding notes, 221
  - adding task, 227, 415
  - applying policy modules, 305
  - applying service modules, 226
  - assigning alias names, 218
  - assigning inventory tag, 219
  - customizing, 217
  - deleting, 228
  - deleting down devices automatically, 120

---

- description, 204
- disabling power management, 571
- enabling power management, 571
- filtering, 45, 207
- last logged in user, 209
- modifying scan, 108
- names, 205
- overview, 209
- purging IP addresses from devices, 228
- putting in group, 226
- removing monitors, 227
- searching for down devices, 231
- searching for guest virtual machines, 232
- searching for Intel® vPro™ devices, 231
- searching for mobile devices, 232
- searching for ones not allocated, 231
- searching for ones with alerts, 231
- searching for printers, 231
- searching for virtual machine hosts, 232
- service groups, 192, 194
- setting auto delete, 138
- setting end-of-life date, 220
- setting location, 219
- setting production dates, 221
- setting warranty expiration, 220
- site groups, 193, 200
- viewing, 206
- viewing alerts, 209
- viewing applications, 211
- viewing asset tag information, 219
- viewing bandwidth usage, 213
- viewing details, 45, 208
- viewing hardware, 211
- viewing hotfixes, 211
- viewing Intel® AMT information, 213
- viewing MBSA reports, 212
- viewing network services, 212
- viewing operating systems, 211
- viewing patch management, 210
- viewing performance counter data, 213
- viewing product keys, 212
- viewing SNMP details, 214

- 
- viewing syslog messages, 214
  - viewing system log events, 210
  - viewing warranty expiration, 219
  - viewing Windows events, 213
  - viewing Windows Services, 211
  - disabling
    - alert schedules, 372
    - all startup items, 523
    - IDE redirection for Intel® vPro™ devices, 238
    - power management for device, 565
    - power management for devices, 571
    - power management for site, 565
    - serial-over-LAN for Intel® vPro™ devices, 238
    - startup items, 523
    - startup items for a user, 523
    - user account, 167
  - disconnecting remote tools, 524
  - discovery, editing settings, 146
  - down device, 119
  - downloading Device Managers, 124

## E

- editing
  - discovery settings, 146
  - system tray profile, 594
  - Windows Update Agent Policy, 540
- email
  - alert setting, 360
  - Device Manager installation link, 124
  - reports, 484
  - resetting for user account, 166
  - setting default, 611
  - setting for alerts, 360
  - testing, 612
- email address, adding to Support Assistant, 588
- Email policy
  - configuring, 282, 286
- enabling
  - alert schedule, 372
  - all startup items, 523
  - IDE redirection for Intel® vPro™ devices, 238



---

- power management for device, 565
- power management for devices, 571
- power management for site, 565
- serial-over-LAN for Intel® vPro™ devices, 238
- startup items, 523
- startup items for a user, 523
- user consent for Intel® KVM, 238
- end-of-life date, setting for devices, 220
- enrolling mobile devices, 245
- environment variables, 396
- escalating alerts, 364
- Event Viewer remote tool
  - description, 517
  - using, 519
- exclude, 116
- exclusion rules
  - deleting, 118
- expired updates, 549
- exporting
  - archived reports, 486
  - policy modules, 303
  - previewed report, 472
  - scripts, 408
  - search results, 232

## F

- failed logon attempts, settings, 165
- File Manager remote tool
  - description, 517
  - using, 519
- filtering
  - alerts by category, 369
  - by printers, 207
  - by servers, 207
  - by workstations, 207
  - device list, 45, 207
  - network services, 38
  - resetting for syslog, 355
  - sites in Windows Inventory dashboard, 203
  - websites, 39
- found mobile devices, 265

---

## G

- generating provisioning code, 256
- geo-tracking mobile devices, 259
- group folders
  - description, 178
  - renaming, 199
- group, removing power plan, 570
- grouping
  - description, 36, 176
  - devices, 226
- groups
  - adding task, 415
  - applying policy modules, 305

## H

- hibernate, description, 561
- Hide Groups, 37
- Hide Sites, 37
- hiding
  - left sidebar, 35
  - service groups, 37
  - site groups, 37
- hotfixes, viewing on devices, 211
- hybrid sleep, description, 561

## I

- icons
  - Device Manager, 586
  - Support Assistant, 586
- ignoring IP addresses, 111
- importing
  - APNs certificate, 250
  - MDM CSR signing certificate, 248
  - policy modules, 294
  - reports, 480
  - scripts, 403
  - service modules, 490
- initiating
  - remote control from Device Overview page, 227
  - remote to web console, 506

---

## installing

- AntiVirus, 425–426
- Device Manager using email, 124
- Device Managers, 124

## Intel® AMT devices

- configuring credentials, 239
- description, 497
- determining power status, 239
- powering remotely, 240
- viewing configuration history, 239
- viewing events, 241
- viewing hardware, 241
- viewing status, 240

## Intel® KVM

- description, 497
- enabling user consent, 238

## Intel® vPro™ devices

- configuring network settings, 237
- description, 236
- disabling IDE redirection, 238
- disabling serial-over-LAN, 238
- enabling IDE redirection, 238
- enabling serial-over-LAN, 238
- setting host name, 237

## Internet availability, 139

## inventory tag, assigning to device, 219

## iOS, setting up for monitoring, 246

## IP addresses

- adding to scan, 110
- ignoring, 111
- removing from scan, 112
- searching, 230
- servers, 229
- SNMP, 229
- workstations, 229

## iReasoning, using, 354

## J

## jailbroken mobile devices, monitoring, 265, 323

---

## K

kilowatt hour, 563

## L

language

setting for user account, 168

last logged in user

searching, 230

viewing, 209

Local Users and Groups remote tool

description, 517

using, 520

locating

mobile devices, 259

location

setting for device, 219

viewing for sites, 135

locking

mobile devices, 260

user account, 167

log monitoring, turning on or off, 612

logging in

Mobile Service Manager, 634

Service Center, 33

logging out

Mobile Service Manager, 634

Service Center, 33

login credentials, website monitors, 349, 351

login password, 33

logo

adding, 600

deleting from Service Center, 601

making hyperlink, 601

lost devices

configuring, 261

lost mobile devices, 264

## M

MAC address, searching, 230

maintenance schedules

---

- adding to execution schedules, 72
- managing mobile devices, 244
- manually running network scan, 121
- MBSA
  - description, 137
  - options, 137
  - report monitors, 321
  - reports, viewing for devices, 212
  - running scan, 121
- MDM, 244
- MDM certificate signing request, creating, 248
- MDM CSR signing certificate, 247
  - deleting, 251
  - importing, 248
  - renewing, 250
- MIB files
  - deleting, 336
  - unloading, 336
  - uploading, 335
- Microsoft System Center Essentials (SCE) monitors, 331
- Microsoft Update, 531
- mobile device management, 244
- mobile devices
  - adding monitor, 265, 323
  - availability monitoring, 265, 323
  - configuring lost device actions, 261
  - enrolling, 245
  - getting latest assets, 258
  - jailbroken monitoring, 265, 323
  - locating, 259
  - locking, 260
  - mark as found, 265
  - mark as lost, 264
  - provisioning, 255
  - removing from monitoring, 287
  - removing passcode, 261
  - searching, 232
  - setting passcode, 260
  - setting up iOS, 246
  - SIM card tampering monitoring, 265, 323
  - table of features, 245
  - viewing, 257

---

- viewing details, 258
- viewing hardware details, 258
- viewing software details, 258
- wiping, 261
- Mobile Manager agent
  - uninstalling, 288
- Mobile Service Manager
  - description, 634
  - logging in, 634
  - logging out, 634
  - viewing alerts, 634
- monitoring
  - description, 37, 290
  - how it works, 291
  - reviewing, 373
  - what you can monitor, 290
- monitoring policies
  - definition, 291
  - description, 291
  - example, 292
  - how many, 292
  - updates, 292
- monitors
  - adding cloud services, 352
  - AMT events, 312
  - bandwidth, 314
  - cloud services, 347
  - creating, 311
  - creating syslog message monitors, 338
  - custom log files, 316
  - deleting from policy module, 308
  - Device Warranty, 319
  - locating device-level, 359
  - locating in policy modules, 359
  - MBSA reports, 321
  - Microsoft System Center Essentials (SCE), 331
  - network services, 325
  - patch status, 327
  - performance counter, 328
  - print services, 330
  - setting frequency, 308
  - SNMP, 332

---

SNMP from MIB, 335, 337

SNMP Traps, 337

syslog messages, 338

turning on or off, 307

warranty, 319

website, 347

Windows Events, 340

Windows Services, 346

moving

devices into approval groups, 544

service group to different folder, 200

## N

names, resetting for user account, 166

naming

scheduled report, 482

website monitors, 348

network discovery, process, 109

network scan, running, 121

network services

adding custom, 607

deleting custom, 607

filtering, 38

monitors, 325

viewing details, 38

viewing on devices, 212

Network Services dashboard

description, 37

viewing, 38

notes

adding for devices, 221

adding for sites, 135

## O

object access

removing, 164

setting, 163

Onsite Manager Utilities

description, 497

remote control, 505

Onsite Managers

---

- description, 32
- rebooting, 122
- options, power plan, 575
- overriding
  - power cost, 566
  - power plan precedence, 572
  - power plan settings for device, 571
  - power usage, 566

## P

- pager
  - alerts, setting, 364
- parameters, scripts, 395
- passcode
  - locking, 260
  - removing, 261
  - setting, 260
- Passcode policy
  - configuring for Android devices, 280
  - configuring for iOS devices, 269
  - description, 267
- passwords
  - changing, 33
  - resetting for user account, 166
  - setting options, 165
- patch management
  - approving automatically, 556
  - approving manually, 553
  - declining manually, 555
  - description, 530
  - overview, 547
  - patches, 549
  - planning, 532
  - removing manually, 555
  - setting classifications, 546
  - setting languages to download, 546
  - setting products, 545
  - setting up, 532
  - stopping, 557
  - storing files, 546
  - superseded patches, 549



---

- synchronization, 545
- understanding, 530
- viewing details, 551
- viewing patches, 549
- WSUS patches, 549

Patch Policy

- description, 531, 536

patch status monitors, 327

patches

- description, 549
- expired, 549

pausing Windows Service, 523

performance counters

- adding, 605
- deleting, 605
- monitors, 328

permissions, setting for role, 172

planning for patch management, 532

policies

- creating new Antivirus, 425

policies, deleting for mobile devices, 282

policy modules

- applying, 305
- applying to devices, 305
- applying to groups, 305
- creating, 310
- deleting, 304
- deleting monitor from, 308
- exporting, 303
- importing, 294
- notification, 293
- removing from devices, 305
- removing from groups, 305
- renaming, 302
- requesting, 294
- service groups, 194
- site groups, 193
- turning monitor on or off, 307
- upgrading, 304

power costs

- descriptions, 563
- overriding for site, 566

---

- setting defaults, 564
- power management
  - baseline power consumption, 563
  - creating baseline, 566
  - description, 560
  - disabling for device, 565, 571
  - disabling for site, 565
  - enabling for device, 565, 571
  - enabling for site, 565
  - power cost, 563
  - power usage, 563
  - prerequisites, 561
  - scripts, 562
  - summary, 568
  - turning on for new sites, 563
- power plan
  - adding, 569
  - applying to device, 569
  - applying to group, 569
  - copying, 570
  - deleting, 570
  - description, 560
  - Managed Workplace vs Windows, 560
  - options, 575
  - overriding setting for device, 571
  - precedence, 562
  - precedence, overriding, 572
  - removing from device or group, 570
  - renaming, 570
  - reports, 562
  - setting precedence, 572
- power status, determining for Intel® AMT devices, 239
- power usage, 563
  - overriding for site, 566
  - setting defaults, 564
- powering Intel® AMT devices remotely, 240
- precedence
  - power plan, 562
  - setting for power plans, 572
- predefined
  - reports, 465
  - scripts, 405

---

---

- predefined ticket
  - adding to Support Assistant, 589
  - description, 587
- Premium Remote Control
  - cancel automatic install, 103
  - installing automatically, 103
  - options, 136
  - setting options for new sites, 104
- previewing reports, 471
- print services monitors, creating
  - print services monitors, 330
- printer transforms, 618
- printers
  - monitoring polling interval, 140
  - overview, 215
  - searching, 231
  - viewing details, 215
- printing
  - previewed report, 472
  - trouble tickets, 580
- Prioritize Alerts, Alerts Viewer, 44
- Process Explorer remote tool
  - description, 517
  - using, 521
- product keys, viewing on devices, 212
- provisioning codes, generating, 256
- provisioning mobile devices, 255
- purging IP addresses from devices, 228
- Put on Hold, 132
- PuTTY
  - description, 497
  - remote control, 503

## R

- Reboot Manager remote tool
  - description, 517
  - using, 521
- rebooting
  - Device Managers, 126–127
  - Onsite Managers, 122
- refining search, 232

---

- refreshing
  - options, 602
  - previewed report, 472
- rejecting sites, 133
- Remote Assistance, 496
  - description, 496
  - remote control, 502
- Remote CMD Prompt remote tool
  - description, 518
  - using, 522
- remote control
  - AMT-enabled devices, 507
  - AMT-enabled devices and KVM, 509
  - description, 494
  - history, 524
  - initiating, 501–504
  - Intel® AMT, 497
  - Intel® KVM, 497
  - PuTTY, 497
  - Remote Assistance, 496
  - Remote Desktop, 496
  - requirements, 494
  - saving settings, 516
  - session history, 524
  - Telnet, 497
  - troubleshooting, 525
  - UltraVNC, 497
  - web console, 497
- Remote Desktop
  - description, 496
  - remote control, 501
- remote tools, 516
  - disconnecting, 524
  - Event Viewer, 517
  - File Manager, 517
  - Local Users and Groups, 517
  - Process Explorer, 517
  - Reboot Manager, 517
  - Remote CMD Prompt, 518
  - Screenshot, 518
  - Startup Manager, 518
  - using, 518

---

- Windows Services, 518
- removing
  - exclusion rules, 118
  - IP addresses from scan, 112
  - mobile device from monitoring, 287
  - monitors from devices, 227
  - passcode, 261
  - patches manually, 555
  - policy modules from devices, 305
  - policy modules from groups, 305
  - power plan from device, 570
  - power plan from group, 570
  - range of IP addresses, 112
  - subnet scan, 112
  - Windows Update Agent Policy, 541
  - Windows Update Agent Policy from devices, 540
  - Windows Update Agent Policy from groups, 540
- renaming
  - alert categories, 368
  - Alerts Viewer window, 43
  - group folders, 199
  - groups using Local Users and Groups, 521
  - policy modules, 302
  - power plan, 570
  - report categories, 481
  - roles, 173
  - service groups, 199
  - users using Local Users and Groups, 520
  - Windows Update Agent Policy, 541
- renewing MDM CSR signing certificate, 250
- reports
  - about creating, 466
  - aggregate, 465, 473
  - archiving, 484, 486
  - assigning categories, 481
  - categories, 481
  - changing category, 478
  - creating, 469
  - creating categories, 481
  - creating schedules, 482
  - deleting, 480
  - deleting archived reports, 486

---

- deleting categories, 482
- deleting scheduled reports, 485
- description, 46, 464
- device, 465
- emailing, 484
- exporting archived report, 486
- exporting previewed report, 472
- importing, 480
- naming schedule, 482
- power plan, 562
- predefined, 465
- previewing, 471
- printing, 472
- refreshing, 472
- renaming categories, 481
- running, 485
- scheduling, 482
- scheduling when to deliver, 484
- site, 465
- tips, 466
- types, 465
- user-defined, 465
- viewing for more than one Onsite Manager, 473
- viewing for more than one site, 473
- viewing history, 486
- viewing list, 478
- viewing schedule, 485

requesting policy modules, 294

requirements, remote control, 494

resetting

- Alerts Viewer sort order, 44
- email for user account, 166
- filters for syslog, 355
- mobile device to factory defaults, 261
- name for user account, 166
- password for user account, 166

restarting Windows Service, 523

Restore Defaults, search settings, 232

restricted script, 395

Results tab, closing, 233

resuming Windows Service, 523

reviewing

- 
- monitoring, 373
  - SNMP information, 354
  - roles
    - adding user account, 171
    - creating, 170
    - defaults, 169
    - deleting, 173
    - deleting user account, 171
    - description, 169
    - renaming, 173
  - running
    - MBSA scan, 121
    - network scan, 121
    - scheduled reports, 485

## S

- saving remote control settings, 516
- scan
  - adding IP addresses, 110
  - deleting IP address, 112
  - for assets, 228
  - modifying, 108
  - removing IP addresses, 112
  - running manually, 121
- scheduling
  - reports, 482, 484
- Screenshot remote tool
  - description, 518
  - using, 522
- scripting
  - troubleshooting, 397
  - variables, 396
- scripts
  - alert setting, 363
  - deleting, 408
  - exporting, 408
  - importing, 403
  - parameters, 395
  - power management, 562
  - predefined, 405
  - setting for alerts, 363

---

- viewing, 405
- search
  - exporting results, 232
  - phrase, website monitors, 350
  - refining, 232
  - running again, 232
- searching
  - description, 230
  - devices with alerts, 231
  - down devices, 231
  - for Device Managers, 125
  - guest virtual machines, 232
  - Intel® vPro™ devices, 231
  - MAC address, 230
  - mobile devices, 232
  - printers, 231
  - unallocated devices, 231
  - virtual machine hosts, 232
- self-heal, setting for alerts, 361
- servers, IP addresses, 229
- service account, validating and viewing, 137
- Service Center
  - branding, 600
  - description, 32
- service groups
  - adding devices, 192
  - applying policy modules, 194
  - creating, 178
  - deleting, 200
  - deleting devices from, 194
  - description, 36, 176
  - hiding in Central Dashboard, 37
  - moving to different folder, 200
  - renaming, 199
  - showing in Central Dashboard, 37
- service modules
  - applying to devices, 226
  - deleting, 492
  - description, 490
  - importing, 490
- setting
  - alert schedules, 370

---



---

- alerts, 359
- alerts to call a pager, 364
- alerts to create trouble tickets, 361
- alerts to run a script, 363
- alerts to self heal, 361
- alerts to self-heal, 361
- alerts to send emails, 360
- auto deletion of devices, 138
- classifications to patch manage, 546
- data retention, 608
- default email address, 611
- devices as part of group, 226
- email options, 611
- end-of-life date for devices, 220
- frequency for monitors, 308
- host name for Intel® vPro™ devices, 237
- languages to download for patch management, 546
- location for devices, 219
- MBSA options, 137
- number of failed logon attempts, 165
- object access, 163
- passcode, 260
- password, using Local Users and Groups, 520
- passwords, 165
- patch management, 532
- power plan precedence, 572
- Premium Remote Control defaults, 104
- Premium Remote Control site options, 103
- printer monitoring polling interval, 140
- production dates for devices, 221
- products to patch manage, 545
- refresh options, 602
- role permissions, 172
- SMTP options, 611
- user session options, 165
- warranty expiration for devices, 220
- website address for Internet availability, 139
- website communications, 609
- WSUS URL, 137

setting up

- APNs certificate, 249
- iOS devices, 246

---

- MDM signing certificate, 247
- sharing
  - tasks, 408
- Show Groups, 37
- Show Sites, 37
- showing
  - service groups in Central Dashboard, 37
  - sidebar, 35
  - site groups in Central Dashboard, 37
- sidebar
  - hiding, 35
  - showing, 35
- site communication, setting alerts, 137
- site groups
  - adding devices, 193
  - applying policy modules, 193
  - creating, 178
  - deleting, 200
  - deleting devices from, 200
  - description, 36, 177
  - hiding in Central Dashboard, 37
  - showing in Central Dashboard, 37
- site reports, 465
- sites
  - adding notes, 135
  - approving, 133
  - cancelling automatic install of Premium Remote Control agent on new devices, 103
  - changing status, 132
  - deleting, 133
  - description, 98
  - installing Premium Remote Control agent on new devices, 103
  - installing Premium Remote Control on devices automatically, 136
  - MBSA options, 137
  - overview, 127
  - putting on hold, 132
  - rejecting, 133
  - setting default options when creating new, 104
  - setting WSUS URL, 137
  - turning power management on, 563
  - viewing location, 135
  - viewing status, 34
  - viewing summary, 127

---

- skip, 110
- sleep, description, 561
- SMTP, setting options, 611
- SNMP from MIB, 335, 337
- SNMP Inventory dashboard
  - viewing, 204
  - viewing details, 204
- SNMP IP addresses, 229
- SNMP iReasoning, 354
- SNMP monitors, 332
- SNMP OIDs
  - adding, 606
  - deleting, 606
- SNMP Traps, 337
- sorting
  - Alerts Viewer, 44
  - columns, 35
  - resetting in Alerts Viewer, 44
- sounds, Alerts Viewer, 43
- stale IP addresses, 228
- starting Windows Service, 523
- startup items
  - enabling and disabling, 523
  - enabling and disabling all, 523
  - enabling and disabling for a user, 523
- Startup Manager remote tool
  - description, 518
  - using, 522
- status, changing for site, 132
- stopping
  - patch management, 557
  - Windows Service, 523
- storing patch files locally, 546
- superseded patches, 549
- Support Assistant
  - context menu, 587
  - copying system tray profile, 594
  - deleting system tray profile, 598
  - description, 584
  - editing system tray profile, 594
  - icons, 586
  - uninstalling, 127

---

- using, 598
- Support Assistant policies
  - best practices, 584
  - considerations, 584
- support assistant policies
  - description, 584
- Support Assistants
  - updating, 595
- suppressing
  - alerts, 364
- synchronizing patches, 545
- syslog message, 338
- syslog, viewing details, 355
- system tray profile
  - editing for Device Manager, 594
  - editing for Support Assistant, 594
- system tray profiles
  - copying for Device Manager, 594
  - copying for Support Assistant, 594
  - editing context menu, 593

## T

- tampered mobile devices, monitoring, 265, 323
- tasks
  - adding device, 415
  - adding group, 415
  - changing, 418
  - copying, 419
  - deleting, 419
  - description, 397
  - sharing, 408
- Telnet
  - description, 497
  - remote control, 503
- testing email, 612
- text-based message, adding to Support Assistant, 589
- themes, 601
- ticketing options, Support Assistant, 587
- time zone, setting for user account, 168
- timeout for website monitors, 349
- tips, report creation, 466

---

- transforms, printer, 618
- trouble tickets
  - alert setting, 361
  - changing, 580
  - closing, 580
  - creating, 579
  - creating for website alerts, 41
  - description, 578
  - printing, 580
  - setting for alerts, 361
  - viewing, 578
- troubleshooting
  - remote control, 525
  - scripting, 397
- turning monitors on or off, 307

## U

- UltraVNC
  - description, 497
  - remote control, 504
- uninstalling
  - Device Managers, 126
  - Mobile Manager agent, 288
  - Support Assistant, 127
- unloading MIB files, 336
- unlocking user account, 167
- updating
  - Support Assistant, 595
- upgrading
  - Device Managers, 125, 595
  - policy modules, 304
- uploading MIB files, 335
- user accounts
  - adding role, 162, 171
  - creating, 161
  - deleting, 164
  - deleting role, 162, 171
  - description, 160
  - disabling, 167
  - locking, 167
  - object access, 163

---

- removing object access, 164
- setting language, 168
- setting time zone, 168
- unlocking, 167
- waking computers, 234

user session settings, 165

Using, 598

using

- Device Manager, 598
- Event Viewer remote tool, 519
- File Manager remote tool, 519
- Local Users and Groups remote tool, 520
- Process Explorer remote tool, 521
- Reboot Manager remote tool, 521
- Remote CMD Prompt remote tool, 522
- remote tools, 518
- Screenshot remote tool, 522
- Startup Manager remote tool, 522
- Support Assistant, 598
- Windows Services remote tool, 523

## V

- validating service account credentials, 137
- variables, 396
- viewing
  - alert configurations, 45
  - alerts, 44
  - alerts for devices, 209
  - alerts on Mobile Server Manager, 634
  - Alerts Viewer, 43
  - available patches, 549
  - bandwidth usage for a device, 213
  - Central Dashboard, 34
  - cleared alerts, 366
  - configuration history for Intel® AMT devices, 239
  - details about devices, 208
  - details about patches, 551
  - details about printers, 215
  - device asset tag information, 219
  - device details, 45
  - device overview, 209

---

- device system log events, 210
- devices, 206
  - group properties using Local Users and Groups, 521
  - hardware on a device, 211
  - information about sites, 134
  - Intel® AMT device events, 241
  - Intel® AMT device hardware, 241
  - Intel® AMT information for devices, 213
  - last logged in user, 209
  - mobile device details, 258
  - mobile device hardware details, 258
  - mobile device software details, 258
  - mobile devices, 257
  - Network Services dashboard, 38
  - network services details, 38
  - operating systems on devices, 211
  - patch management for devices, 210
  - performance counter data on devices, 213
  - power management summary, 568
  - predefined reports, 478
  - printer overview, 215
  - report history, 486
  - scheduled reports, 485
  - scripts, 405
  - service account credentials, 137
  - site overview, 127
  - site status, 34
  - SNMP details for a device, 214
  - SNMP inventory, 35
  - SNMP Inventory dashboard, 204
  - startup items, 523
  - status of Intel® AMT devices, 240
  - summary about sites, 127
  - syslog details, 355
  - syslog messages for a device, 214
  - system log information, 355
  - trouble tickets, 578
  - user properties using Local Users and Groups, 520
  - warranty expiration for devices, 219
  - website alert history, 41
  - website availability, 39
  - website details, 39

---

- website response times, 40
- Websites dashboard, 39
- Windows assets, 35
- Windows events for a device, 213
- Windows Inventory dashboard, 203
- Windows Services on devices, 211
- virtual machine hosts
  - searching, 232
- virtual machines
  - searching, 232
- virtual machines, identifying, 567
- VNC
  - description, 496
  - remote control, 503
  - remote desktop, 496

## W

- wake-on-LAN, 233
- waking
  - computers, 234
  - computers at a site, 234
- warranty
  - setting expiration for devices, 220
  - viewing expiration for devices, 219
- warranty monitors, 319
- web console
  - description, 497
  - remote control, 506
- web link
  - adding to Support Assistant, 592
- website alerts, trouble tickets, 41
- website communications, setting, 609
- website monitors, 347
  - login credentials, 349, 351
  - naming, 348
  - search phrase, 350
  - specifying timeout, 349
- websites
  - filtering, 39
  - viewing alert history, 41
  - viewing availability, 39



---

- viewing details, 39
- viewing response times, 40
- Websites dashboard
  - description, 38
  - viewing, 39
- Windows Events, 340
- Windows Inventory dashboard
  - description, 203
  - filtering, 203
  - viewing, 203
- Windows Services, 346
- Windows Services remote tool
  - description, 518
  - using, 523
- Windows Update Agent Policy
  - applying to devices, 540
  - applying to groups, 540
  - deleting, 541
  - description, 539
  - editing, 540
  - removing from devices, 540
  - removing from groups, 540
  - renaming, 541
- Windows Update Agent, description, 531
- wiping mobile devices, 261
- work area, 34
- workstations, IP addresses, 229
- WSUS patches, 549
- WSUS URL, setting, 137

