Workload Optimization Manager 2.3.17 Installation and Update Guide

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.

Contents

Introduction

Thank you for choosing Workload Optimization Manager, the Intelligent Workload Automation Management solution for Cloud and Virtualized Environments. This guide gives you information you need to install Workload Optimization Manager in your virtual environment, install your license, and get started managing your resources.

If you have any questions, please contact Cisco support.

Sincerely:

The Workload Optimization Manager Team

Task Overview

This *Workload Optimization Manager Installation Guide* provides instructions to accomplish the following tasks:

If you need to:	Perform or go to:
Deploy a new Workload Optimization Manager installation.	■ Review the *Workload Optimization Manager Release Notes*. ■ Ensure you satisfy the minimum requirements. See Minimum Requirements *(on page 7)*. ■ Perform the installation procedure in Installing Workload Optimization Manager *(on page 9)*. ■ Configure any settings if necessary. See General Configuration Tasks *(on page 17)*. ■ Log in for the first time. See License Installation and First-time Login *(on page 26)*. ■ Install your license. See License Installation and First-time Login *(on page 26)*. ■ Configure SSO if necessary. See Single Sign-On Authentication *(on page 28)*. ■ Continue to use your Workload Optimization Manager instance. See the *Workload Optimization Manager User Guide* and the *Workload Optimization Manager Target Configuration Guide*.
Deploy a new Workload Optimization Manager installation on RHEL.	■ Review the *Workload Optimization Manager Release Notes*. ■ Ensure you satisfy the minimum requirements. See Requirements for RHEL and Setup *(on page 36)*. ■ Perform the installation procedure in Installing and Updating on a RHEL Platform *(on page 36)*.

If you need to:	Perform or go to:
Upgrade a license.	Follow the instructions in Upgrading Your Workload Optimization Manager License *(on page 26)*.
Update your existing Workload Optimization Manager installation.	■ Review the *Workload Optimization Manager Release Notes*. ■ Ensure you satisfy the minimum requirements for updating Workload Optimization Manager on supported hypervisors or the RHEL platform: – Minimum Requirements *(on page 7)*. – Requirements for RHEL and Setup *(on page 36)* ■ Perform one of the following update procedures: – Updating Workload Optimization Manager to a New Version *(on page 33)* – Updating the RHEL Deployment *(on page 39)* ■ Upgrade your license, if necessary. See Upgrading Your Workload Optimization Manager License *(on page 26)*. ■ Log in. ■ Continue to use your Workload Optimization Manager instance. See the *Workload Optimization Manager User Guide* and the *Workload Optimization Manager Target Configuration Guide*.

Minimum Requirements

The following are minimum requirements to run Workload Optimization Manager:

Supported Technology		Storage Requirements	Memory	CPUs
VMware	vCenter versions 5.5, 6.0, 6.5, and 6.7	500 GB or greater **NOTE:** Can be thin provisioned depending on the storage requirements.	32 GB	4 vCPUs
Microsoft	Hyper-V as bundled with Windows 2016, 2008 R2, Hyper-V Server 2012, or Hyper-V Server 2012 R2			
Amazon Web Services (AWS)				

NOTE:
Minimum requirements depend on the size of your environment's inventory. The more datastores, hosts, VMs, and applications you have, the more resources you need to run the installation effectively. Also note that other management software might recommend that you run the Workload Optimization Manager VM with lower resources. Please be sure to give Workload Optimization Manager enough resources, using the guidelines above.

If you intend to use price adjustments, Workload Optimization Manager recommends that you increase the memory allocated to the VM that hosts your Workload Optimization Manager instance as follows:

- For price adjustments assigned to one or more billing groups:
  - For the first price adjustment, increase by 4 GB.
  - For each subsequent price adjustment, increase by an additional 1 GB.

See "Billing and Costs" in the *Workload Optimization Manager User Guide* for information about price adjustments.

Workload Optimization Manager supports DHCP or static IP addressing. For information about using static IP addresses, see (Optional) Specifying a Static IP Address *(on page 17)*.

Browser Requirements

Workload Optimization Manager operates with most commonly-used Web browsers (for example, Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari).

The Web browsers must have JavaScript enabled.

In addition, the browser that you use for the Workload Optimization Manager user interface must be synchronized with the Workload Optimization Manager instance to within one minute. Without this synchronization, Workload Optimization Manager can show incorrect metric values.

Also, if you use Google Chrome for the Workload Optimization Manager user interface, you must turn off the Chrome Preview mode before you download reports in order to view those reports.

Installing Workload Optimization Manager

As you get started with Workload Optimization Manager, be aware that there are different downloads available for the supported hypervisors. These downloads all deliver the same version of Workload Optimization Manager with the same capabilities, but they are packaged to install and run on different hypervisor platforms.

You can also install the Cisco software on a VM running Red Hat (see Installing and Updating on a RHEL Platform *(on page 36)*).

Each installation manages virtual environments in exactly the same way. The installation you choose depends on the policies and standards for your enterprise. This document describes installation procedures for each of the Workload Optimization Manager downloads. *The installation you choose has no effect on the technologies you can manage with Workload Optimization Manager. No matter which type of machine hosts Workload Optimization Manager, you can manage all workloads running on the supported hypervisors, as well as those managed via cloud platforms and load balancer targets.*

This section describes how to install a new Workload Optimization Manager instance. If you are updating a current installation to new version, you should not perform a full install – Instead you should update your current installation. See Updating Workload Optimization Manager to a New Version *(on page 33)*.

This section includes installation instructions for the following supported virtual platforms:

- Installing on VMware Systems *(on page 9)*
- Installing on Microsoft Hyper-V *(on page 10)*
- Installing on AWS *(on page 10)*

When you deploy Workload Optimization Manager, you should install it on a VM that does not include underscore characters in its name. If you cannot change the host name, you can use a workaround described in How Can I Work Around the Restriction for Host Names *(on page 43)*.

NOTE:
If you want to use IAM Roles to discover AWS targets, then Workload Optimization Manager has to be deployed on AWS and you have to assign the Workload Optimization Manager instance to the IAM Role. If you need assistance, contact Technical Support.

Installing on VMware Systems

This download of the Workload Optimization Manager instance is in the `.OVA 1.0` format.

To install Workload Optimization Manager:

1. Download the Workload Optimization Manager installation package.

   Refer to the email you received from Cisco for links to the Workload Optimization Manager download pages.
2. Import the OVA file into your VMware infrastructure using VCenter.
3. Start the Workload Optimization Manager appliance and record its IP address.

Users navigate to the appliance IP address to start up the Web User Interface in a browser.

4. If necessary, specify a static IP address for the appliance.

   If your environment does not have DHCP, or if you want to give the Workload Optimization Manager instance a static IP address, see (Optional) Specifying a Static IP Address *(on page 17)*.

5. Perform the required configuration steps for the Workload Optimization Manager instance.

   See General Configuration Tasks *(on page 17)*.

Installing on Microsoft Hyper-V

To install Workload Optimization Manager:

1. Download the Workload Optimization Manager installation package.

   Refer to the email you received from Cisco for links to the Workload Optimization Manager download pages.
2. Expand the .zip file and copy the contents, which includes the Virtual Machine image, to your Hyper-V server (either to your cluster shared volume or to a local hard drive).
3. Use the Import Virtual Machine Wizard in the Hyper-V Manager to import the Virtual Machine into your environment.
4. Make sure your virtual network adapter is connected to the correct virtual network.
5. Ensure the Workload Optimization Manager instance will have sufficient memory.

   Cisco recommends that you use static memory for your Workload Optimization Manager instance. However, you can specify static or dynamic memory for the instance.

   In **Properties** for the instance, navigate to **Hardware Configuration**:

   - For Static Memory, set **Virtual machine memory** to at least 32 GB.
   - For Dynamic Memory, then set **Startup memory** and **Minimum memory** to 32 GB.
6. Start the Workload Optimization Manager appliance and record its IP address.

   Users navigate to the appliance IP address to start up the Web User Interface in a browser.
7. If necessary, specify a static IP address for the appliance.

   If your environment does not have DHCP, or if you want to give the Workload Optimization Manager instance a static IP address, see (Optional) Specifying a Static IP Address *(on page 17)*.
8. Perform the required configuration steps for the Workload Optimization Manager instance.

   See General Configuration Tasks *(on page 17)*.

NOTE:
The Workload Optimization Manager instance configuration includes a NIC that is not connected to any network. After installing the instance, you should use the Hyper-V Manager to configure the network and VLAN settings to suit the requirements of your cluster's network.

Installing on AWS

For an AWS installation, you will install Workload Optimization Manager as an Amazon Machine Image (AMI). To perform this installation, ensure that your deployment follows Workload Optimization Manager and Amazon best practices, including:

- Automatic scheduling and executing of EBS data volume snapshots

  AWS will perform these snapshots daily and store them in a user-created S3 bucket on a rolling 14-day period.
- EBS volume encryption

  Workload Optimization Manager recommends using a Security Group to only allow access to the Workload Optimization Manager instance through HTTPS.

- Setup and use of Identity and Access Management (IAM) Instance Profiles (Instance Roles) for authentication

  Workload Optimization Manager recommends Instance Roles over Access Keys. Instance Roles are much easier to manage for compliance purposes, and are natively supported by the AWS SDK.

  Further, Workload Optimization Manager recommends enabling cross-account access for your Instance roles by following the steps found here: `https://aws.amazon.com/blogs/security/how-to-enable-cross-account-access-to-the-aws-management-console/`.
- Utilize auto-scaling for HA/recovery purposes

  Through AWS's auto-scaling, Workload Optimization Manager ensures that there is an instance running at all times.

As you perform this installation, the CloudFormation template ensures adherance to these best practices.

Installing using the CloudFormation Template

This template directs you through launching a VM that runs CentOS and that hosts a Workload Optimization Manager instance. This template ensures that your deployment will follow both Workload Optimization Manager and Amazon best practices.

To install Workload Optimization Manager using the CloudFormation template:

1. Download the Workload Optimization Manager CloudFormation template.

   To access the CloudFormation template, please contact Technical Support.
2. Modify the template to set parameters depending on your AWS environment.

   For information, review the CloudFormation Template Summary *(on page 12)*.
3. Log in to your AWS console and choose the CloudFormation service.
4. Create a new Stack.

   When you are prompted for your template:

   a. Click **Upload a template to Amazon S3**.

   b. Choose the template you downloaded and modified.

   c. Click **Next**.
5. On the Specify Details page, enter your stack information.

   Enter a stack name and choose the image size. Click **Next**.

   NOTE:
   Cisco recommends the `m5.xlarge` instance type, but you can also use `m5.large`, `m5.2xlarge`, `m4.xlarge`, `m4.large`, `m4.2xlarge`, `r4.xlarge`, `r4.2xlarge`, `r5.xlarge`, `r5.2xlarge`, `i2.xlarge`, `i3.xlarge`, `c4.2xlarge`, or `c5.2xlarge`.
6. On the Options page, enter any tags you need.

   For example, change the default values for the Key-Value pair to set periodic backups of your data.

   After you add any tags, click **Next**.

   Tags are a convenient way to group instances based on security needs, business requirements, and more. See `https://aws.amazon.com/answers/account-management/aws-tagging-strategies/` for more information.
7. On the Review page, ensure that your selections are correct.

   Once you have reviewed your selections and are satisfied, click **Create**.

(Optional) Creating a Security Group

NOTE:
When you install Workload Optimization Manager via the CloudFormation template, that installation automatically performs this step.

If you install Workload Optimization Manager without using the CloudFormation template, Cisco recommends that you create a security group to restrict access to HTTPS only for the Workload Optimization Manager instance and attach this group to the Workload Optimization Manager instance.

Read the Amazon documentation for more information on security groups. See `http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_SecurityGroups.html`

CloudFormation Template Summary

This section provides additional explanations about portions of the CloudFormation template which may be useful when you are preparing your template.

This snippet creates the structure of the CloudFormation template, used by the rest of the template.

```
Metadata:
        Instances:
        Description: Your Turbonomic instance is created with an encrypted EBS Volume. If you create an e
ncrypted volume and don't specify this property, AWS CloudFormation uses the default master key.
        'AWS::CloudFormation::Designer':
          5979b605-17c1-4e1a-9158-ae132fb86736:
            size:
              width: 60
              height: 60
            position:
              x: 30
              'y': -20
              z: 1
            embeds: []
          ef20cdef-19a0-4d61-9f16-0108bb0330e1:
            size:
              width: 60
              height: 60
            position:
              x: 150
              'y': 10
              z: 1
              embeds: []
              dependson:
                - ea836120-be24-44ab-bd80-e2c9749fad84
                - b4bc499e-9882-4ab9-9c37-e165e51fe589
          ea836120-be24-44ab-bd80-e2c9749fad84:
            size:
              width: 60
              height: 60
            position:
              x: -60
              'y': 210
              z: 1
              embeds: []
          b4bc499e-9882-4ab9-9c37-e165e51fe589:
            size:
              width: 60
              height: 60
            position:
              x: 180
              'y': 210
              z: 1
              embeds: []
              dependson:
                - ea836120-be24-44ab-bd80-e2c9749fad84
              isrelatedto:
                - ea836120-be24-44ab-bd80-e2c9749fad84
         6e649c64-891f-4e11-a83a-2df5cf26d0b5:
           source:
             id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
           target:
             id: ea836120-be24-44ab-bd80-e2c9749fad84
           z: 2
        7c216255-250c-4574-9bcf-fb02673b306e:
          source:
            id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
          target:
            id: b4bc499e-9882-4ab9-9c37-e165e51fe589
          z: 2
        84fca9b5-0bb0-4a88-b0e3-c74af6b00b80:
          source:
            id: b4bc499e-9882-4ab9-9c37-e165e51fe589
          target:
            id: ea836120-be24-44ab-bd80-e2c9749fad84
          z: 2
```

The following snippet sets the allowable deployment templates, and defines your VPC ID to use later in the template.

```
Parameters:
    InstanceTypeParameter:
      Type: String
      Default: m4.xlarge
      AllowedValues:
        - m4.large
        - m4.xlarge
        - m4.2xlarge
      Description: 'Enter m4.large, m4.xlarge, or m4.2xlarge. Default is m4.xlarge.'
    VpcIdParameter:
      Type: 'List<AWS::EC2::VPC::Id>'
      Description: VpcId of your existing Virtual Private Cloud (VPC)
      ConstraintDescription: must be the VPC Id of an existing Virtual Private Cloud.
```

The following snippet maps the various AWS regions to ensure that your Workload Optimization Manager instance is deployed in your default region.

NOTE:
The list of available AMIs by region changes periodically. To obtain the latest list of AMIs for Workload Optimization Manager, go to the AWS Marketplace and log in with your AWS credentials. Click the Manual Launch tab. Then, choose the latest version of Workload Optimization Manager to display the regions and AMI IDs. Make a record of the regions and AMI IDs for use in your template.

```
Mappings:
        RegionMaptoAMI:
        us-east-2:
        AMI:
        - "ami-366f4e53"
        us-east-1:
        AMI:
```

```
        - "ami-7ae9c16c"
        us-west-1:
        AMI:
        - "ami-898fa2e9"
        us-west-2:
        AMI:
        - "ami-f656428f"
        ap-south-1:
        AMI:
        - "ami-f23f419d"
        ap-northeast-2:
        AMI:
        - "ami-76f02f18"
        ap-southeast-1:
        AMI:
        - "ami-756fe316"
        ap-southeast-2:
        AMI:
        - "ami-f32d3d90"
        ap-northeast-1:
        AMI:
        - "ami-e834208f"
        ca-central-1:
        AMI:
        - "ami-28cd724c"
        eu-central-1:
        AMI:
        - "ami-72eb4d1d"
        eu-west-1:
        AMI:
        - "ami-1d7b607b"
        eu-west-2:
        AMI:
        - "ami-eb61778f"
        sa-east-1:
        AMI:
        - "ami-cce289a0"
```

The following snippet creates the Workload Optimization Manager security group, which limits access to the Workload Optimization Manager instance to HTTPS only:

```
Resources:
        TurbononomicSecurityGroup:
        Type: AWS::EC2::SecurityGroup
        Properties:
        GroupName: TurbonomicSecurityGroup
        GroupDescription: Creates and limits access to Turbonomic instance through port 443 only
        VpcId:
        Ref: VpcIdParameter
        SecurityGroupIgress:
        - IpProtocol: tcp
        FromPort: '443'
        ToPort: '443'
        CidrIp: 0.0.0.0/0
        Metadata:
          'AWS::CloudFormation::Designer':
            id: ef20cdef-19a0-4d61-9f16-0108bb0330e1
        DependsOn:
          - Turbonomic
```

The following snippet sets the following items for the Workload Optimization Manager instance:

- Instance size
- Instance region
- Block storage properties, including access, backup, and encryption
- Security Group

NOTE:
`DeleteOnTermination` is set to `false` by default. This ensures that even if the EC2 instance is terminated at a later time, the data will persist.

```
Turbonomic:
   Type: 'AWS::EC2::Instance'
   Properties:
     InstanceType:
       Ref: InstanceTypeParameter
     ImageId:
       'Fn::FindInMap':
         - RegionMaptoAMI
         - Ref: 'AWS::Region'
         - AMI
     BlockDeviceMappings:
       - DeviceName: /dev/sdi
         Ebs:
           VolumeType: gp2
           DeleteOnTermination: false
           VolumeSize: 150
           Encrypted: true
     EbsOptimized: true
     InstanceInitiatedShutdownBehavior: stop
   Metadata:
     'AWS::CloudFormation::Designer':
       id: ea836120-be24-44ab-bd80-e2c9749fad84
```

The following snippet creates an auto scaling group of 1, which ensures that a Workload Optimization Manager EC2 instance is always running:

```
TurbonomicAutoScalingGroup:
    Type: 'AWS::AutoScaling::AutoScalingGroup'
    Properties:
      AvailabilityZones:
        - !GetAtt Turbonomic.AvailabilityZone
      InstanceId:
        Ref: Turbonomic
      Cooldown: '1800'
      MinSize: '1'
      MaxSize: '1'
      DesiredCapacity: '1'
      HealthCheckType: EC2
      HealthCheckGracePeriod: 900
    Metadata:
      'AWS::CloudFormation::Designer':
        id: b4bc499e-9882-4ab9-9c37-e165e51fe589
    DependsOn:
      - Turbonomic
```

The following snippet creates the S3 bucket required for the daily backups:

```
TurbonomicS3BackupBucket:
    Type: 'AWS::S3::Bucket'
    Properties:
      AccessControl: AuthenticatedRead
      BucketName: turbonomic-s3-volume-backup-bucket
    Metadata:
      'AWS::CloudFormation::Designer':
        id: 5979b605-17c1-4e1a-9158-ae132fb86736
```

General Configuration Tasks

After you install the Workload Optimization Manager instance, perform the following configuration tasks:

- (Optional) Specify a static IP address.
- (Best practice) Synchronize the system clock and configure your time servers.
- (Optional) Configure remote MariaDB connections.
- (Required) Ensure the ports that Workload Optimization Manager needs for network communication are open.
- (Optional) Open a non-default port on the Workload Optimization Manager VM to allow communication from a target.
- (Required) Configure a listener for a custom port for reporting.
- (Optional) Enforce secure access by installing a trusted certificate.
- (Optional) Configure email notifications for database disk usage.

(Optional) Specifying a Static IP Address

Many installations use DHCP for dynamic IP address allocation. You can also specify a static address via the virtual machine's IP configuration.

Only if you need to specify a static IP address, choose one of the following methods:

- Use the `ipsetup` script from Workload Optimization Manager.
- Configure the static IP address manually as described in this topic.

The ipsetup Script

Workload Optimization Manager provides the `ipsetup` script to assist you with this task.

1. Open an SSH terminal session to your Workload Optimization Manager instance.

   Use the following default credentials:

   - Username: `root`
   - Password: `vmturbo`
2. Once the session is open, execute the script with the `ipsetup` command.

Manually Configuring a Static IP Address

To specify a static IP address, perform these steps:

1. Open an SSH terminal session to your Workload Optimization Manager instance.

   Use the following default credentials:

   - Username: `root`
   - Password: `vmturbo`
2. Open the connection editor.
   1. Execute the `nmtui` command.

      This opens the user interface for the NetworkManager.
   2. Click **Edit a connection** to open the editor.
3. Add a new connection.

   Click **Add** on the screen to open the New Connection dialog box.
4. Add an Ethernet connection.
   1. Choose **Ethernet** from the list of options and complete the following information (values given are examples only):
      - Profile Name: `eth0`
      - Device: `eth0`
      - IPv4 Configuration: `Manual`
      - Click **Show** and complete the Configuration sub-settings based on your environment.
   2. Click **OK** to return to the configuration list.
5. Verify that the connection you created is present.
6. Click **Quit** to return to the command line.
7. Restart the network services.

   ```
   service network restart
   ```

   The network service restarts successfully.
8. Verify that your machine is accessible and the static IP address is correct.

   ```
   ifconfig eth0
   ```

This procedure applies the IP address to the Workload Optimization Manager instance. You can now access the Web user interface using this IP address.

(Best practice) Synchronizing Time

It is important that you synchronize the clock on the Workload Optimization Manager instance with the devices on the same network. For performance reasons, Cisco recommends that you set your Workload Optimization Manager system clock to your time zone, because Workload Optimization Manager runs regular data maintenance processes at night. Use the Network Time Protocol daemon (`ntpd`) to set your Workload Optimization Manager system clock.

NOTE:
Do not use the yast option to set up an NTP service. To set up NTP, use the instructions below. The yast timezone utility provides an option to set up NTP, but you must not use this yast option.

To configure the NTP server:

1. Open an SSH terminal session to your Workload Optimization Manager instance.
2. Open the ntp configuration file.

   For example, execute the command: `vi /etc/ntp.conf`
3. Find the lines that specify the time servers.
4. Replace these time server lines with the fully-qualified domain names of your time servers.

The safest approach is usually to provide the IP address of the your time server. If you only have one time server, you can delete the second time server entry.

5. Save the file.
6. Make sure the NTP daemon is enabled.

   The NTP daemon should be enabled by default. To enable the daemon, execute the `systemctl enable ntpd` command.
7. Verify the NTP daemon is running.

   Execute: `systemctl status ntpd`
8. Verify that your time is correct.

   Execute the `date` command. You should see results similar to:

   ```
   Thu Oct 18 14:25:45 CST 2018
   ```

(Optional) Configuring remote MariaDB connections for the Workload Optimization Manager instance

If you want to allow remote client connections to the MariaDB database in the Workload Optimization Manager instance, you can replace the local host bind address (127.0.0.1) with the IP address of your Workload Optimization Manager instance.

To configure remote client connections to the MariaDB database, perform these steps:

1. Open an SSH terminal session to your Workload Optimization Manager instance.

   Use the following default credentials:

   - Username: `root`
   - Password: `vmturbo`
2. Open the `bind-addr` configuration file.

   For example, use the `vi /etc/my.cnf.d/bind-addr.cnf` command.
3. Set the `bind_address` parameter to the IP address of your Workload Optimization Manager instance.

   For example: `bind_address=10.10.10.123`
4. Save the file.
5. Restart the MariaDB service.

   Execute the `systemctl restart mariadb` command.

(Required) Ports

Ensure the ports for network communication are open.

Workload Optimization Manager uses the following ports:

Port:	To support:
80	Incoming browser connections over HTTP
443	■ Incoming browser connections over HTTPS ■ Proactive Support (automatically generate support tickets for Workload Optimization Manager issues)

For browser connections with the Workload Optimization Manager instance, you should use either port 80 or 443.

NOTE:
Various targets that you use with Workload Optimization Manager may require you to open ports on those targets to allow communications with Workload Optimization Manager. For more information and a list of default ports, see "Port Configuration" in the *Workload Optimization Manager Target Configuration Guide.*

(Optional) Opening a Non-Default Port

If your target is using a non-default, non-standard port, you can open the port on the Workload Optimization Manager VM to allow communication from the target. To open a port, use the SELinux `audit2allow` diagnostic tool. The audit2allow tool parses the Access Vector Cache (AVC) messages from the audit log and creates the module (`semodule`) to allow access to a port.

To open a non-default, non-standard port, perform these steps:

1. Open an SSH terminal session to your Workload Optimization Manager instance.
2. Change to a temporary directory from which you can run SELinux commands (for example, `/tmp/selinux`).
3. Create the module, myapp.

   Use the `audit2allow` command with the `-M` option:

   ```
   audit2allow -M myapp < /var/log/audit/audit.log
   ```
4. Load the module into the kernel.

   ```
   semodule -i myapp.pp
   ```
5. Retest access to the port.

(Required) Configuring a Listener for a Custom Port for Reporting

If you are using a custom port number as required by your company policy and your reports fail with the exception `Error Generating Report`, you need to configure a listener for the local host interface address (127.0.0.1) on port 443.

To configure the listener, perform these steps:

1. Open an SSH terminal session to your Workload Optimization Manager instance.

   Use the following default credentials:

   - Username: `root`
   - Password: `vmturbo`
2. Open the Apache `ssl.conf` file.

   For example, use the `vi /etc/httpd/conf.d/ssl.conf` command.
3. In the configuration file, search for the listener section.

   Look for the following code:

   ```
   # When we also provide SSL we have to listen to the
   # the HTTPS port in addition.
   #
   ```
4. Add the listener for the local host interface address (127.0.0.1) on port 443.

   In this example, assume that the custom port 1443 already exists. Note that the listener has been added for port 443.

   ```
   # When we also provide SSL we have to listen to the
   ```

```
# the HTTPS port in addition.
#
Listen 1443 https
Listen 127.0.0.1:443 https
```

5. Check the VirtualHost section in the `ssl.conf` file.
   - If the original VirtualHost section for port 443 still exists, ensure that it matches the following VirtualHost section.
   - If the original VirtualHost section was modified for the custom port, add the following VirtualHost section for the listener at the very top of the `ssl.conf` file.

   IMPORTANT:
   The same key pair used for the custom port must be used for the listener.

   ```
   <VirtualHost 127.0.0.1:443>
   ErrorLog logs/ssl_error_log
   TransferLog logs/ssl_access_log
   LogLevel warn
   SSLEngine on
   SSLCertificateFile /etc/pki/tls/certs/localhost.crt
   SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
   <Files ~ "\.(cgi|shtml|phtml|php3?)$">
        SSLOptions +StdEnvVars
   </Files>
   <Directory "/var/www/cgi-bin">
        SSLOptions +StdEnvVars
   </Directory>
   SSLHonorCipherOrder On
   SSLCipherSuite HIGH:!NULL:!MD5:!DSS:!3DES
   SSLProtocol -all +TLSv1.2
   SSLCipherSuite ALL:+HIGH:!ADH:!EXP:!SSLv2:!SSLv3:!DSS:!3DES:!MEDIUM:!LOW:!NULL:!aNULL
   CustomLog logs/ssl_request_log \
        "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
   </VirtualHost>
   ```

6. Write and quit the `ssl.conf` file.

   Press **esc**, type `:wq!`, and press **Enter**.
7. Restart the http service.

   ```
   service http restart
   ```

(Optional) Enforcing Secure Access

If your company policy requires a trusted certificate, Workload Optimization Manager enables you to install a trusted certificate from a known certificate authority.

1. Request a certificate.

   a. Open an SSH terminal session to your Workload Optimization Manager instance.

      The default credentials are:
      - Username: `root`
      - Password: `vmturbo`

b. Change to the /private directory where you will store the private key.

```
cd /etc/pki/tls/private
```

c. Execute the command to create the private key file.

```
openssl genrsa -out turbonomic.key 2048
```

d. Create a file containing the information used to generate the CSR.

```
vi certsignreq.cfg
```

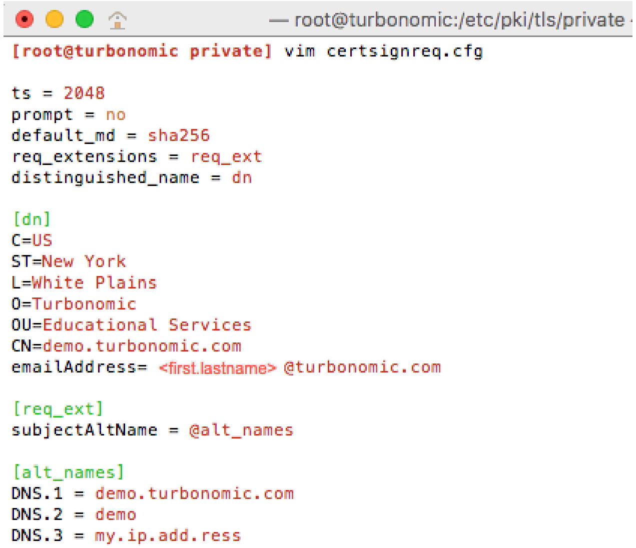
e. In the file, insert the following code and specify the fields:

```
[req]
ts = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[dn]
C=<country, 2 letter code>
L=<city>
O=<company>
OU=<organizational unit name>
CN=<FQDN>
emailAddress=<email address>

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = <FQDN>
DNS.2 = <server’s short name>
DNS.3 = <server’s IP address>
```

NOTE:
For the CN field, specify the fully-qualified domain name of the Workload Optimization Manager instance.

Alternate names are other ways to access the Workload Optimization Manager instance. In the alternate names ([alt_names]) section, the value for the DNS.1 field is required. For the DNS.1 field, specify the fully-qualified domain name of the Workload Optimization Manager instance. Values for the DNS.2 and DNS.3 fields are optional. You can add more DNS.<n> fields if needed.

For example:



```
[root@turbonomic private] vim certsignreq.cfg

ts = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[dn]
C=US
ST=New York
L=White Plains
O=Turbonomic
OU=Educational Services
CN=demo.turbonomic.com
emailAddress= <first.lastname> @turbonomic.com

[req_ext]
subjectAltName = @alt_names

[alt_names]
DNS.1 = demo.turbonomic.com
DNS.2 = demo
DNS.3 = my.ip.add.ress
```

f. Write and quit the file.

   Press **esc**, type `:wq!`, and press **Enter**.

g. Create the certificate request file.

   Execute the command:

   ```
   openssl req -new -sha256 -nodes -out turbonomic.csr -key turbonomic.key -config
   certsignreq.cfg
   ```

h. Transfer the certificate request file to your local machine.

   The path to the certificate request file (turbonomic.csr) on your remote machine is /etc/pki/tls/private.

i. Send this file to your certificate authority.

   Your certificate authority will use this file to create the certificate for you.

   If your certificate authority gives you an encoding choice between DER and Base 64, choose **Base 64**.

2. Rename the certificate file.

   When you receive the certificate file from your certificate authority (CA), check the name of the certificate file.

   Rename it to `turbonomic.crt`.

   For an Intermediate Certificate Bundle, certificate authorities (for example, GoDaddy or Symantec) may use intermediate certificates as a proxy to their root certificate for security purposes – if so, you will also receive a certificate chain bundle. If this is the case, also name the certificate chain with the `.crt` extension (for example: `<intermediate>.crt`).

3. Upload the certificate.

   Transfer the above certificate file(s) to the /etc/pki/tls/certs directory of the Workload Optimization Manager instance.

4. Apply the certificate.

   a. Open an SSH terminal session to your Workload Optimization Manager instance.

      The default credentials are:

      - Username: `root`
      - Password: `vmturbo`

   b. Make a backup file of the ssl.conf file.

      ```
      cp /etc/httpd/conf.d/ssl.conf /etc/httpd/conf.d/ssl.conf-LOCALHOST
      ```

   c. Open the ssl.conf file.

      ```
      vi /etc/httpd/conf.d/ssl.conf
      ```

   d. Edit the ssl.conf file to specify the file paths for the new key and crt files.

      - Replace the `localhost.crt` with the name of the new certificate (`turbonomic.crt`).

        ```
        # Server Certificate
        ```

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
```

- Also, replace the `localhost.key` with the name of the new key file (`turbonomic.key`).

  ```
  # Server Private Key
  SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
  ```

- If you received an intermediate certificate bundle, replace the `server-chain.crt` with the name of the new intermediate file (`<intermediate>.crt`).

  ```
  # Server Certificate Chain
  SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt
  ```

e. Write and quit the ssl.conf file.

   Press **esc**, type `:wq!`, and press **Enter**.

f. Restart the httpd service.

   ```
   service httpd restart
   ```

5. (Optional) Set up secure LDAP.

   a. Save the SSL Certificate information from your LDAPS Server to a .CER file.

      For example, view the certificate properties and click **Save As** or **Export** to create a .CER file.

   b. Transfer this .CER file from your system to the Workload Optimization Manager appliance.

      For example, use the SCP (secure copy) command with the default credentials (root/vmturbo) to copy the .CER file to the /tmp directory of the Workload Optimization Manager instance.

   c. In the Workload Optimization Manager instance, copy the .CER file to the /anchors directory.

      For example, copy the `rootca.cer` file to the `/usr/share/pki/ca-trust-source/anchors/` directory.

   d. Run the `update-ca-trust` command as root.

      This automatically updates the built-in cacerts jks and puts the certificates in the proper location to be used by curl without additional options.

   e. Restart the Tomcat service.

      ```
      service tomcat restart
      ```

(Optional) Configure Email Notifications for Database Disk Usage

You can configure Workload Optimization Manager to notify you by email whenever the database is down or storage exceeds 80% utilization. To configure this notification, you will first execute a script that initializes the configuration. Then to set up a regular check of disk consumption, you will set up a cron job to execute the scripts Workload Optimization Manager provides on its server.

To perform the one-time configuration for this notification:

1. Execute one of the notification scripts.

   To initialize the configuration, you can execute either of the provided scripts. To do so, execute one of the following commands:

   - `/srv/tomcat/script/appliance/turbo_check_db.sh`
   - `/srv/tomcat/script/appliance/turbo_check_disk.sh`

2. Provide the information as the script prompts you for it.

   The script displays the following prompts:

   ```
   [root@turbonomic appliance] ./turbo_check_db.sh
   Configuration file does not exist.
   Creating default configuration file.
   ```

```
Database name (Default: vmtdb):
Database user (Default: root):
Database password:
Database port (Default: 3306):
Email address to send notifications to:
```

Be sure to give the email address where you want to receive the notifications.

Running the script creates a configuration file that saves the settings you provide.

To set up regular checks that run every 30 minutes, append the following lines to your crontab file:

```
*/30 * * * * /srv/tomcat/script/appliance/turbo_check_db.sh >/dev/null 2>&1
*/30 * * * * /srv/tomcat/script/appliance/turbo_check_disk.sh >/dev/null 2>&1
```

After you set up the cron job, if the database goes down, or if disk usage exceeds 80%, the scripts send an email alert to the recipient that you specified in the initial configuration. In addition, the scripts write alerts to the log file: `/var/log/tomcat/monitor.log`.

License Installation and First-time Login

Before you begin, make sure you have your full or trial license key file that was sent to you in a separate email. Save the license file on your local machine so you can upload it to your Workload Optimization Manager installation.

To use Workload Optimization Manager for the first time, perform the following steps:

1. Type the IP address of your installed Workload Optimization Manager instance in a Web browser to connect to it.
2. Log in to Workload Optimization Manager.
   - Use the default credential for **USERNAME**: `administrator`.
   - Type a password for **PASSWORD**.
   - Type the password again to verify it for **REPEAT PASSWORD**.
   - Click **CONFIGURE**.
3. Decide whether to enable Usage Data and Analytics.

   Click **AGREE** or **No**.

   You can always change this setting later. For information, see "Administrative Tasks" in the *Workload Optimization Manager User Guide*.
4. Continue setting up your Workload Optimization Manager installation.

   Click **LET'S GO**.
5. Open the **Enter License** fly-out.

   Click **IMPORT LICENSE**.
6. Upload your license key file.
   a. In the Enter License fly-out, you can upload the license in one of the following ways:
      - Drag the license key file into the Enter License fly-out.
      - Browse to the license key file.

      Be sure to upload only .xml or .lic files.

   b. Click **SAVE**.

Upgrading Your Workload Optimization Manager License

If you purchased a license to upgrade from a trial version to a full version, or if you purchased a license to add more workload capacity to your installation, you will receive a new license in an email message. Save the license file on your local machine so you can upload it to your Workload Optimization Manager installation.

To install this new license, perform the following steps:

1. Navigate to the License Configuration page.

   Choose **Settings > License**.
2. Open the **Enter License** fly-out.

   Click **IMPORT LICENSE**.
3. Upload your license key file.
   a. In the Enter License fly-out, you can upload the license in one of the following ways:
      - Drag the license key file into the Enter License fly-out.
      - Browse to the license key file.

      Be sure to upload only .xml or .lic files.

   b. Click **SAVE**.

Once you install the new license, the additional workload capacity automatically becomes available to you.

Single Sign-On Authentication

If your company policy supports Single Sign-On (SSO) authentication, Workload Optimization Manager enables SSO authentication by using Security Assertion Markup Language (SAML) 2.0.

At a high-level, the process involves:

- Creating external groups or at least one external user for SSO. See "Managing User Accounts" in the *Workload Optimization Manager User Guide*.
- Configuring Workload Optimization Manager to connect to the SAML Identity Provider (IdP). See Configuring Single Sign-On *(on page 28)*.

When SSO is enabled, use your SSO credentials to log in to your Workload Optimization Manager instance. Do not use your local or Active Directory (AD) credentials for the login. The Identity Provider (IdP) will perform the authentication.

NOTE:
When you enable SSO, Workload Optimization Manager only accepts authentication from the IdP you configure. Remote requests via the Workload Optimization Manager REST API do not use SSO.

If you wish to use the Workload Optimization Manager REST API and SSO for end-user authentication simultaneously, you can do so by setting the SAML_ENABLE policy when you configure SSO (see Configuring Single Sign-On *(on page 28)*). If you set the SAML_ENABLE policy, end-user authentication to the application is delegated to your IdP, and an audited class of locally defined users is made available for use for the REST API integration.

Another choice is the SAML_ONLY security policy. If you set the SAM_ONLY policy, all authentication is delegated to your IdP. For security reasons, REST API requests will not execute when the SAML_ONLY policy is configured.

Prerequisites

Before you begin, make sure the IdP is set up for SSO. You can use a proprietary or public IdP. For examples of settings for a public Okta IdP, see What Are the Typical Settings for an IdP? *(on page 44)*.

Configuring Single Sign-On

To configure Single Sign-On, perform these steps:

1. (Required) Create external groups or at least one external user for SSO.

IMPORTANT:
When SSO is enabled, Workload Optimization Manager only permits logins via the SSO IdP. Whenever you navigate to your Workload Optimization Manager installation, it redirects you to the SSO Identity Provider (IdP) for authentication before displaying the Workload Optimization Manager user interface.

Before you enable SSO for your Workload Optimization Manager installation, *you must configure at least one SSO user with Workload Optimization Manager administrator privileges*. If you do not, then once you enable SSO you will not be able to configure any SSO users in Workload Optimization Manager. To authorize an SSO user as an administrator, use **EXTERNAL AUTHENTICATION** to do one of the following:

- Configure a single SSO user with administrator authorization.

  Add an external user. The username must match an account that is managed by the IdP.
- Configure an SSO user group with administrator authorization.

  Add an external group. The group name must match a user group on the IdP, and that group must have at least one member.

For information about creating external groups or external users for SSO, see "Managing User Accounts" in the *Workload Optimization Manager User Guide*.

2. (Required) Ensure that the NTP server is configured and the system time on your Workload Optimization Manager instance is correct.

   For instructions, see (Best practice) Synchronizing Time *(on page 18)*.
3. Open an SSH terminal session to your Workload Optimization Manager instance.
4. Download the metadata from your IdP.
5. Examine your metadata.

   Compare your metadata to the sample provided in Example of IdP Metadata *(on page 30)*.

   If your metadata includes optional attribute tags that are not listed in the example, you must remove those optional attribute tags since they are not supported.
6. Import the IdP metadata into the saml.xml file.
   a. Create the `saml.xml` file.

      ```
      vi /srv/tomcat/data/config/saml.xml
      ```
   b. Copy the IdP metadata into the `/srv/tomcat/data/config/saml.xml` file.
   c. Save the file.
7. Modify the Tomcat configuration file.
   a. Open the Tomcat configuration file.

      ```
      vi /etc/tomcat/tomcat.conf
      ```
   b. Set the CATALINA_OPTS variable.

      Choose one of the following:

      - SAML_ONLY: Allows SAML authentication only. Workload Optimization Manager REST API integration is not supported.
      - SAML_ENABLE: Allows SAML authentication and supports Workload Optimization Manager REST API integration (local and LDAP authentications).

      For example: `CATALINA_OPTS="-Dadmin.policy.localusers=SAML_ONLY"`
   c. Save the file.
8. Copy the properties file.

   ```
   cp /srv/tomcat/data/config/saml.template.properties /srv/tomcat/data/config/
   saml.properties
   ```
9. Modify the properties file.
   a. Open the saml.properties file.

      ```
      vi /srv/tomcat/data/config/saml.properties
      ```
   b. Set the `IDP.entityId` property to the same value as the IdP's Audience Restriction property.

      For example: `IDP.entityId=urn:test:turbo:markharm`

c. Set the Workload Optimization Manager public IP address.

   For example: `Turbonomic.Location=10.10.10.123`

d. Save the file.

10. Generate the SAML configuration file.

    Run the `config_saml.sh` script to parse the values in the properties file and transfer them to the SAML configuration file, `saml-security.xml`.

    a. Change to the directory for the SAML configuration script.

    ```
    cd /srv/tomcat/script/appliance/
    ```

    b. Execute the SAML configuration script.

    ```
    ./config_saml.sh
    ```

11. Add a trusted custom IdP certificate.

    The public domain default key store only trusts two public IdPs, Okta and SSO Circle. If you are using a proprietary IdP or other public IdPs, contact your security administrator to add the IdP certificates to the default key store.

    Default key store location: `/srv/tomcat/webapps/vmturbo/WEB-INF/security/samlKeystore.jks`

    Key store password: `nalle123`

12. Restart the Tomcat service.

    ```
    service tomcat restart
    ```

13. Verify that the configuration is successful.

    a. Navigate to the Workload Optimization Manager User Interface.

       You will be automatically redirected to your IdP for authentication.

    b. Log in with the username that is a member of the external group or external user previously configured.

    c. Verify that the system time on your Workload Optimization Manager instance is correct.

       If the time is not synchronized, this might cause an `HTTP Status 401 -authentication failed` exception in the browser.

    d. If the configuration is not successful, look for an `HTTP Status 500` exception in the `/var/log/tomcat/catalina.out` log file. If this exception exists, review your metadata for invalid optional attribute tags.

Example of IdP Metadata

This section provides an example of IdP metadata which may be useful when you are examining the optional attributes in your metadata.

If your metadata includes optional attribute tags that are not listed in the example, you must remove those optional attribute tags since they are not supported.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="http://www.okta.com/exkexl6xc9MhzqiC30h7">
<md:IDPSSODescriptor WantAuthnRequestsSigned="false"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<md:KeyDescriptor use="signing">
<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:X509Data>
<ds:X509Certificate>
 MIIDpDCCAoygAwIBAgIGAWMnhv7cMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
 A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
 MBIGA1UECwwLU1NPUHJvdmlkZXIxEzARBgNVBAMMCmRldi03NzEyMDIxHDAaBgkqhkiG9w0BCQEW
 DWluZm9Ab2t0YS5jb20wHhcNMTgwNTAzMTk0MTI4WhcNMjgwNTAzMTk0MjI4WjCBkjELMAkGA1UE
 BhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTALBgNV
 BAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXYtNzcxMjAyMRwwGgYJ
```

```
     KoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
     ugxQGqHAXpjVQZwsO9n8l8bFCoEevH3AZbz7568XuQm6MK6h7/O9wB4C5oUYddemt5t2Kc8GRhf3
     BDXX5MVZ8G9AUpG1MSqe1CLV2J96rMnwMIJsKeRXr01LYxv/J4kjnktpOC389wmcy2fE4RbPoJne
     P4u2b32c2/V7xsJ7UEjPPSD4i8l2QG6qsUkkx3AyNsjo89PekMfm+Iu/dFKXkdjwXZXPxaL0HrNW
     PTpzek8NS5M5rvF8yaD+eE1zS0I/HicHbPOVvLal0JZyN/f4bp0XJkxZJz6jF5DvBkwIs8/Lz5GK
     nn4XW9Cqjk3equSCJPo5o1Msj8vlLrJYVarqhwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQC26kYe
     LgqjIkF5rvxB2QzTgcd0LVzXOuiVVTZr8Sh57l4jJqbDoIgvaQQrxRSQzD/X+hcmhuwdp9s8zPHS
     JagtUJXiypwNtrzbf6M7ltrWB9sdNrqc99d1gOVRr0Kt5pLTaLe5kkq7dRaQoOIVIJhX9wgynaAK
     HF/SL3mHUytjXggs88AAQa8JH9hEpwG2srN8EsizX6xwQ/p92hM2oLvK5CSMwTx4VBuGod70EOwp
     6Ta1uRLQh6jCCOCWRuZbbz2T3/sOX+sibC4rLIlwfyTkcUopF/bTSdWwknoRskK4dBekFcvN9N+C
     p/qaHYcQd6i2vyor888DLHDPXhSKWhpG
     </ds:X509Certificate>
     </ds:X509Data>
     </ds:KeyInfo>
     </md:KeyDescriptor>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
     </md:NameIDFormat>
     <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
     </md:NameIDFormat>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="https://dev-771202.oktapreview.com/app/ibmdev771202_turbo2_1/exkexl6xc9MhzqiC30h7/sso/sam
l"/>
     <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="htt
ps://dev-771202.oktapreview.com/
     app/ibmdev771202_turbo2_1/exkexl6xc9MhzqiC30h7/sso/saml"/>
     </md:IDPSSODescriptor>
     </md:EntityDescriptor>
```

Disabling Single Sign-On

If for some reason you no longer want to use SSO, you can disable it for your Workload Optimization Manager installation. To disable Single Sign-On, perform these steps:

1. Open an SSH terminal session to your Workload Optimization Manager instance.
2. Modify the Tomcat configuration file to disable the CATALINA_OPTS variable.
   a. Open the Tomcat configuration file.

      `vi /etc/tomcat/tomcat.conf`

   b. Insert a comment character or delete the line for the CATALINA_OPTS variable.

      For example:`# CATALINA_OPTS="-Dadmin.policy.localusers=SAML_ONLY"`

   c. Save the file.
3. Navigate to the Tomcat configuration directory on your local machine.

   The directory is: `/srv/tomcat/data/config`
4. Remove files from the Tomcat configuration directory.

   Delete:

   - The metadata file: `/srv/tomcat/data/config/saml.xml`
   - The SAML configuration file: `/srv/tomcat/data/config/saml-security.xml`
   - The SAML properties file: `/srv/tomcat/data/config/saml.properties`
5. Restart the Tomcat service.

   ```
   service tomcat restart
   ```

6. Verify that the configuration is successful.
   a. Navigate to the Workload Optimization Manager User Interface.

      You will no longer be redirected to your IdP for authentication. You will be redirected to the default Workload Optimization Manager login screen.
   b. Log in with a local account or an Active Directory (AD) account.

Support for Single Logout

If you are using the SSO feature, Workload Optimization Manager supports the Single Logout feature provided by Security Assertion Markup Language (SAML) 2.0. When you click **Logout** in the Workload Optimization Manager session that has SSO enabled, the SAML 2.0 Single Logout feature terminates the Workload Optimization Manager session, the browser session, the Identity Provider (IdP) session, and sessions at other Service Providers (SP) connected to the same IdP session.

If you want to use this feature, contact your security administrator to configure it.

The following are requirements:

- The `Single Logout` setting must be enabled on the IdP.
- The IdP needs to trust the Workload Optimization Manager SAML key store certificate.

If the IdP does not enable or support Single Logout, you need to manually log out from the IdP to fully log out from Workload Optimization Manager.

If you close the browser without clicking **Logout** or if your browser session times out, you can log in again provided the Workload Optimization Manager or the IDP session is valid.

Updating Workload Optimization Manager to a New Version

We continually innovate and improve all aspects of Workload Optimization Manager. This means that we periodically release newer versions of Workload Optimization Manager. You should check regularly to see if a new version is available.

When a new version is available, it's important to properly update your existing installed server, rather than just install a new one. When you first installed Workload Optimization Manager, you put into place sophisticated data collection and analysis processes. Internal to the installation is an integrated database that retains performance data from across your virtual environment. Workload Optimization Manager uses this historical data for right-sizing, projecting trends, and other analysis. This means that the database is important to Workload Optimization Manager *and becomes more so over time*. Properly updating your installation of Workload Optimization Manager preserves the database for continued use.

To update your Workload Optimization Manager installation:

1. Check whether you have adequate disk space on the Workload Optimization Manager VM.

   To check the disk space usage on your server, SSH into the Workload Optimization Manager instance as `root` (the default password is `vmturbo`). Then issue the command: `df -kh`

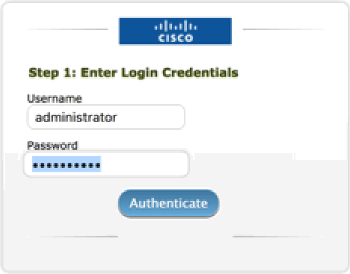
   To perform an update, you should have at least 5 GB of disk free space. The required amount depends on the size of your database, and you should have enough space in the database partition to accomodate a full copy of the database. For example, if you have a large environment and a large database, then 15 GB is a more reasonable estimate of the required space.
2. Save a snapshot of your current Workload Optimization Manager VM.

   Before updating, you should properly shut down (not power off) the Workload Optimization Manager VM and perform a snapshot (or clone the VM). This provides a reliable restore point you can turn to in the event that trouble occurs during the update. After you have the snapshot, bring the VM back online.
3. Download the offline installation package.

   Navigate to `http://www.cisco.com` to find the latest update packages for Workload Optimization Manager. Download the package to your local machine. Save the download to a location you can return to.
4. Open the Workload Optimization Manager Update Page.

   Your Workload Optimization Manager serves an Update Page from the following URL:

   `https://YOUR_WOM_URL_or_IP/update.html.` For example, if you view Workload Optimization Manager from the address `10.10.222.333`, then you would navigate your browser to `https://10.10.222.333/update.html.`.
5. Log into Update Page.



Step 1: Enter Login Credentials

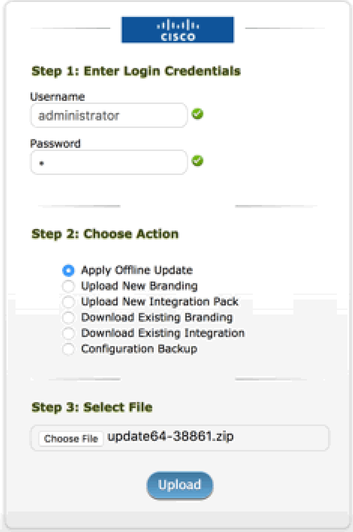
Username: administrator

Password: ••••••••••

Give the credentials for your default Workload Optimization Manager administrator account:

- User: `administrator`
- Password: The password you set for this account

6. Upload the update package to apply an offline update.



Step 1: Enter Login Credentials

Username: administrator ✓

Password: • ✓

Step 2: Choose Action

● Apply Offline Update
○ Upload New Branding
○ Upload New Integration Pack
○ Download Existing Branding
○ Download Existing Integration
○ Configuration Backup

Step 3: Select File

Choose File update64-38861.zip

- Choose the **Apply Offline Update** action
- Select the update package that you want to apply

  Click **Choose File** to browse to the update package that you saved on your local machine.
- Click **Upload** to apply the update package

7. Clear your browser data and refresh your browser.

   If you use the Classic UI, you also need to clear the Flash cache. Refer to *When do I need to clear my local Adobe Flash cache? (on page 41)* for more information.

   After clearing the browser data and refreshing your browser, you have full access to Workload Optimization Manager features. However, features that rely on current analysis data will not be available until after a full market cycle – usually 10 minutes. For example, the Lists of Pending Actions will not show any actions until after a full market cycle.

8. Verify the new version.

   Navigate to **Settings > Updates** and click **About**.

9. (Optional) Allow remote client connections.

   For instructions, see

   BROKEN LINK!!! (Optional) Configuring remote MariaDB connections for the instance

   .

10. Notify other users to clear their browser data and refresh their Workload Optimization Manager browser sessions.

    If the other users use the Classic UI, they also need to clear the Flash cache. Refer to *When do I need to clear my local Adobe Flash cache? (on page 41)* for more information.

IMPORTANT:

DO NOT RESTART the Workload Optimization Manager VM until the software update is complete, and the Workload Optimization Manager user interface refreshes in your browser. If you believe the update will not complete, contact your Cisco Support Representative.

Workload Optimization Manager applies the update in stages. The software updates immediately, along with certain configuration files. The update process restarts your Workload Optimization Manager server as soon as possible.

For some versions the update must restructure the database. This can take a number of hours, depending on the size of your environment and your database. To enable a quick server restart, the update performs this restructuring in the background while the server is running. Workload Optimization Manager will manage your environment, but your access to historical data might be incomplete. For example, you might not be able to view reports until the database restructuring is complete.

Installing and Updating on a RHEL Platform

Cisco delivers a server that runs on the Red Hat Linux (RHEL) 7.x platform installed on a VM with x86 architecture. This is to support environments for which administrative policies require RHEL.

NOTE:
The most common delivery of Workload Optimization Manager is on a VM with x86 architecture, that runs CentOS as an OS. The CentOS deliveries include all the necessary components – If an upgrade to the CentOS platform becomes necessary, Cisco releases a new delivery that includes the platform update. This section describes the less common deployment on a VM running RHEL. For RHEL platforms, you are responsible for keeping the platform up-to-date.

Requirements for RHEL and Setup

Whether you are performing a new installation, or updating an existing Workload Optimization Manager installation, you should ensure that your platform is up-to-date.

In addition, you must run an openJDK version that corresponds with the Workload Optimization Manager version you want to run. Current Workload Optimization Manager versions require openJDK 1.8.

Cisco makes the following setup recommendations for your RHEL VM:

- The VM should have 4 vCPUs and 32 GB of RAM.
- You should create a boot partition for the OS kernel, giving it 500 MB.
- The VM storage requirement is 500 GB or greater. It can be thin provisioned depending on the storage requirements.
- You should create LVM volumes for the following purposes:
  - A swap partition following Red Hat recommendation for partition schemes.
  - The swap partition size should match the allocated RAM size (for example, 32 GB RAM and 32 GB swap partition)
  - 30 GB for system logs to be stored on `/var/log/`
  - 20 GB for system temp storage on `/tmp/`
  - 50 GB for the product installation on the root partition (`/`)
  - Use the remaining space, approximately 380 GB, for the database on `/var/lib/mysql`

In addition, the VM must meet the following prerequisites:

- The OS platform is RHEL 7.x.
- The firewall is configured to allow connections on ports 80 and 443.
- The `unzip` utility must be installed.
- The VM does not include underscore characters in its name. If you cannot change the host name, you can use a workaround described in How Can I Work Around the Restriction for Host Names *(on page 43)*.

- The following DejaVu fonts are installed:
  - dejavu-fonts-common
  - dejavu-sans-fonts
  - dejavu-sans-mono-fonts
  - dejavu-serif-fonts

  To check for the fonts, use the command:

  ```
  rpm -qa | grep dejavu
  ```

  If the DejaVu fonts are not installed, perform the instructions in How Do I Add Fonts to Enable Reporting for the RHEL Platform? *(on page 42)*.

(Optional) If your RHEL platform uses SELinux, ensure that the following are set up:

- Configure SELinux to allow communication between Apache and Tomcat:
  1. Edit the `/etc/selinux/config` file. In the file, search for `SELINUX=permissive` and set it to `SELINUX=enforcing`.
  2. Restart your RHEL operating system.

     ```
     systemctl reboot
     ```

  3. Enable communication between Apache and Tomcat.

     Execute the following command:

     ```
     setsebool -P httpd_can_network_connect=1
     ```

- Install the `policycoreutils-python-2.2.5-11.el7_0.1.x86_64` package.

  Execute the following commands:

  ```
  yum provides /usr/sbin/semanage
  yum install policycoreutils-python
  ```

Browser Requirements

Workload Optimization Manager operates with most commonly-used Web browsers (for example, Internet Explorer, Mozilla Firefox, Google Chrome, and Apple Safari).

The Web browsers must have JavaScript enabled.

In addition, the browser that you use for the Workload Optimization Manager user interface must be synchronized with the Workload Optimization Manager instance to within one minute. Without this synchronization, Workload Optimization Manager can show incorrect metric values.

Also, if you use Google Chrome for the Workload Optimization Manager user interface, you must turn off the Chrome Preview mode before you download reports in order to view those reports.

Installing on a RHEL VM

To create a RHEL deployment of Workload Optimization Manager, you will create a VM running RHEL 7.x, download a Workload Optimization Manager update, and install the necessary components. In addition, you will have to modify the directory structure on your VM, make changes to the database config file, and start up the required services.

1. Create a VM running the RHEL 7.x operating system.
2. Install the Workload Optimization Manager product on your RHEL VM.

   You can configure an offline update to install the initial version of Workload Optimization Manager:

   a. Contact your Cisco representative for the Workload Optimization Manager update package.
   b. Save the package to the `/tmp` directory on the RHEL server.
   c. When you have identified the offline update version that you want, open a shell with root permissions and perform the following commands. Note that <cwom_update_package_name.zip> is the name of the offline update package.

```
cd /tmp
unzip <cwom_update_package_name.zip>
cp /tmp/cisco_temp.repo /etc/yum.repos.d/
```

3. Install the other required components.

   To install the components, execute the following commands, in this order:

   a. apache/mod_ssl

      ```
      yum install mod_ssl
      ```

   b. The Java Runtime Environment

      Note that you must install the JRE version that matches the version of Workload Optimization Manager that you are installing. This example shows installation for JRE 1.8:

      ```
      yum install java-1.8.0-openjdk
      update-alternatives --config java
      ```

      At command, choose the version of Java that corresponds to the version just installed (see Requirements for RHEL and Setup *(on page 36)*).

   c. The Workload Optimization Manager bundle

      ```
      yum install cwom-bundle --nogpgcheck
      ```

4. Set up the correct file structure.

   Execute the following commands to set up the required directory structure:

   ```
   ln -s /srv/www/htdocs /srv/www/html
   rmdir /var/www/cgi-bin
   rmdir /var/www/html
   ln -s /srv/www/cgi-bin /var/www/cgi-bin
   ln -s /srv/www/htdocs /var/www/html
   rm -rf /var/lib/tomcat6/ /var/lib/tomcat/
   ln -s /srv/tomcat6/ /var/lib/
   ln -s /srv/tomcat/ /var/lib/
   mkdir -p /var/lib/mysql/tmp
   chown mysql:mysql /var/lib/mysql/tmp
   mkdir /var/lib/wwwrun
   chown -R apache.apache /var/lib/wwwrun
   ```

5. Initialize the database that was installed in the Workload Optimization Manager bundle.

   Execute the following commands:

   ```
   cd /srv/rails/webapps/persistence/db/
   ./initialize_all.sh
   ```

6. Start the associated services.

   You can restart the VM or you can execute the following commands to start the services:

   ```
   service tomcat start
   service httpd start
   ```

7. Ensure that time is synchronized between the VM and the physical machine that hosts the VM.

   Confirm that the NTP service is running.

   For a host that is managed by VMware vSphere, disable the **Synchronize Guest Time With Host** option for the VM. You can find that setting in **Options > VMware Tools > Advanced**.

8. Change the context of the /cgi-bin directory to enable the execution of cgi scripts.

   Execute the following commands:

```
semanage fcontext -a -t httpd_sys_script_exec_t "/srv/www/cgi-bin(/.*)?"
restorecon -Rv /srv/www/cgi-bin/
```

9. Enable http(s) communication by adding http and https to firewalld.

   Execute the following commands:

   a. Edit the /etc/firewalld/zones/public.xml file.

      Modify the settings in the public zone section. For example:

      ```
      <zone>
      <short>Public </short>
      <description>For use in public areas. You do not trust the other
              computers on networks to not harm your computer. Only selected
              incoming connections are accepted. </description>
      <service name="dhcpv6-client"/>
      <service name="ssh"/>
      <service name="http"/>
      <service name="https"/>
      </zone>
      ```

   b. Reload the firewalld.

      ```
      firewall-cmd --complete-reload
      ```

   c. Restart the firewalld service.

      ```
      systemctl restart firewalld
      ```

10. (Optional) Allow remote MariaDB client connections.

    a. Open the `bind-addr` configuration file.

       For example, use the `vi /etc/my.cnf.d/bind-addr.cnf` command.

    b. Set the `bind_address` parameter to the IP address of your Workload Optimization Manager instance.

       For example: `bind_address=10.10.10.123`

    c. Save the file.

    d. Restart the MariaDB service.

       Execute the `systemctl restart mariadb` command.

    NOTE:
    If you allow remote MariaDB client connections, be sure to add the line `<service name="mysql"/>` in the `/etc/firewalld/zones/public.xml` file.

11. (Optional) Set up SSO authentication. For instructions, see Single Sign-On Authentication *(on page 28)*.

Updating the RHEL Deployment

After you have deployed Workload Optimization Manager on a RHEL platform, you can update that installation with new versions of Workload Optimization Manager as they become available.

NOTE:
You should be sure that the DejaVu fonts are installed and the JDK version is compatible with the new Workload Optimization Manager version. For information, see Requirements for RHEL and Setup *(on page 36)*.

Offline Update

Perform these steps:

1. Download a new offline deliverable and unzip it to the /tmp directory. Note that <cwom_update_package_name.zip> is the name of the offline update package.

   ```
   rm -rf /tmp/cisco
   cd /tmp
   unzip <cwom_update_package_name.zip>
   ```

2. Execute these commands to update the installed components.

   ```
   yum clean all
   cd /tmp/cisco
   yum -y localupdate x86_64/* i586/* | tee /var/lib/wwwrun/manual_cisco_update.txt
   ```

3. Clear your browser data and refresh your browser.

   If you use the Classic UI, you also need to clear the Flash cache. Refer to When do I need to clear my local Adobe Flash cache? *(on page 41)* for more information.

   After clearing the browser data and refreshing your browser, you have full access to Workload Optimization Manager features. However, features that rely on current analysis data will not be available until after a full market cycle – usually 10 minutes. For example, the Lists of Pending Actions will not show any actions until after a full market cycle.

4. Verify the new version.

   Navigate to **Settings > Updates** and click **About**.

5. (Optional) Allow remote MariaDB client connections.

   a. Open the `bind-addr` configuration file.

      For example, use the `vi /etc/my.cnf.d/bind-addr.cnf` command.

   b. Set the `bind_address` parameter to the IP address of your Workload Optimization Manager instance.

      For example: `bind_address=10.10.10.123`

   c. Save the file.

   d. Restart the MariaDB service.

      Execute the `systemctl restart mariadb` command.

6. Notify other users to clear their browser data and refresh their Workload Optimization Manager browser sessions.

   If the other users use the Classic UI, they also need to clear the Flash cache. Refer to When do I need to clear my local Adobe Flash cache? *(on page 41)* for more information.

FAQs

To ensure that you have the most rewarding experience with Workload Optimization Manager, we have collected the top installation issues that people experience. If you have any further questions, contact Workload Optimization Manager Technical Support.

Do I need special software to run the Workload Optimization Manager client?

If you use the Classic UI, make sure that you have installed an up-to-date Flash plug-in to your browser. If your URL takes you to a blank page, it is possible that the Flash plug-in is not installed.

When do I need to clear my local Adobe Flash cache?

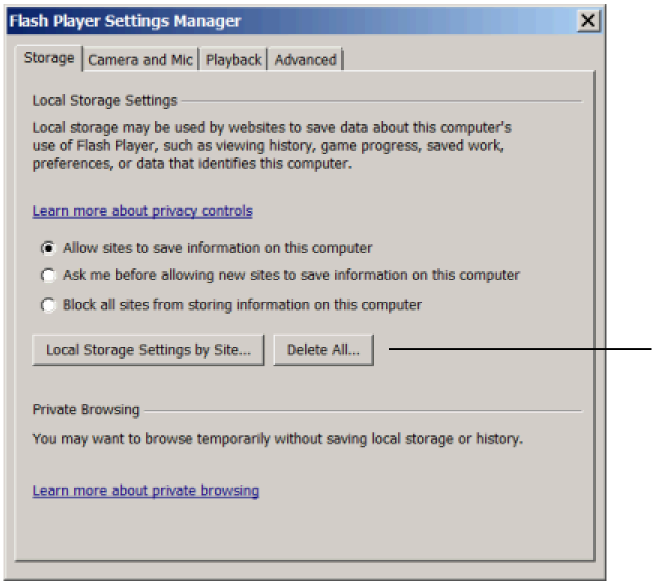
If you use the Classic UI, after you update the Workload Optimization Manager instance, you must then clear the Flash cache. Clearing the Flash cache ensures that the Workload Optimization Manager user interface will be fully refreshed in the browser.

To clear the cache, you can open the Flash Settings Manager locally on your system, or can access the Settings Manager through the following Adobe site:

```
http://www.macromedia.com/support/documentation/en/flashplayer/help/
settings_manager07.html
```

To open the Settings Manager locally on the system, click:

- Windows: **Start > Settings > Control Panel > Flash Player**
- Macintosh: **System Preferences (under Other) > Flash Player**
- Linux Gnome: **System > Preferences > Adobe Flash Player**
- Linux KDE: **System Settings > Adobe Flash Player**



Flash Player Settings Manager
Storage
Camera and Mic
Playback
Advanced
Local Storage Settings by Site...
Delete All...

Local Storage Settings

Local storage may be used by websites to save data about this computer's use of Flash Player, such as viewing history, game progress, saved work, preferences, or data that identifies this computer.

Learn more about privacy controls

● Allow sites to save information on this computer

○ Ask me before allowing new sites to save information on this computer

○ Block all sites from storing information on this computer

Private Browsing

You may want to browse temporarily without saving local storage or history.

Learn more about private browsing

Click **Local Storage Settings by Site** to clear just the Operations Manager appliance, or click **Delete All** clear the cache for all sites that have run on your computer.

Why can I not execute some of the recommendations made by Workload Optimization Manager?

To automate the Workload Optimization Manager recommendations, review the *Workload Optimization Manager User Guide* for complete information about setting policies. Policies are located in **Settings > Policies**.

Workload Optimization Manager supports the following action modes:

- Disabled – Do not recommend or perform the action.
- Recommended – Recommend the action so a user can perform it using the given hypervisor or by other means.
- Manual – Recommend the action, and provide the option to perform that action through the user interface.
- Automated – Workload Optimization Manager performs the action automatically.

Some actions are set to Recommend or Disabled by default. To enable execution of these actions, you must change them to Manual or Automated.

Other actions cannot be executed by Workload Optimization Manager. These actions will only have Disabled or Recommended as an option.

How Do I Add Fonts to Enable Reporting for the RHEL Platform?

To check if the DejaVu fonts are installed, use the command:

```
rpm -qa | grep dejavu
```

If the DejaVu fonts are not installed, perform these steps:

1. Open a shell with root permissions and execute this YUM command to install the DejaVu fonts.

   ```
   yum install -y dejavu-fonts-common dejavu-sans-fonts dejavu-sans-mono-fonts dejavu-serif-fonts
   ```

2. Create the new configuration file.

   `vi /etc/fonts/local.conf`
3. Copy this code into the `/etc/fonts/local.conf` file.

```
<?xml version='1.0'?>
<!DOCTYPE fontconfig SYSTEM 'fonts.dtd'>
<fontconfig>
<alias>
   <family>serif</family>
   <prefer><family>Utopia</family></prefer>
</alias>
<alias>
   <family>sans-serif</family>
   <prefer><family>Utopia</family></prefer>
</alias>
<alias>
   <family>monospace</family>
   <prefer><family>Utopia</family></prefer>
</alias>
<alias>
   <family>dialog</family>
   <prefer><family>Utopia</family></prefer>
</alias>
<alias>
   <family>dialoginput</family>
   <prefer><family>Utopia</family></prefer>
</alias>
</fontconfig>
```

4. Save the file.

How Can I Work Around the Restriction for Host Names Containing Underscore Characters?

By default, Apache no longer supports host names with underscore characters in the name. When you deploy Workload Optimization Manager, you should install it on a VM that does not include those characters in its name. If the host name includes an underscore character, Apache responds with a 400 error when you try to open the user interface.

If you cannot change the host name, you can modify the Apache configuration file to enable legacy behavior as a workaround. To do so, perform these steps:

1. Open a secure shell to your Workload Optimization Manager machine using the default credentials: `root/vmturbo`.
2. Open the Apache configuration file.

   `vi /etc/httpd/conf/httpd.conf`
3. Enable the HttpProtocolOptions unsafe setting.
   a. Remove the comment character to enable the HttpProtocolOptions unsafe setting.
   b. Insert the comment character to disable the HttpProtocolOptions strict setting.

      For example:

```
    HttpProtocolOptions unsafe
    # HttpProtocolOptions strict
```

4. Save the file.
5. Restart the httpd service.

```
service httpd restart
```

What Are the Typical Settings for an IdP?

Before you begin configuring Single Sign-On (SSO), you need to make sure the IdP is set up for SSO.

Here are typical settings for a public Okta IdP which may be useful when you set up your IdP.

SAML Settings: GENERAL	
Setting	Example
Single Sign On URL	https://10.10.10.123/vmturbo/saml/SSO
Recipient URL	https://10.10.10.123/vmturbo/saml/SSO
Destination URL	https://10.10.10.123/vmturbo/saml/SSO
Audience Restriction	urn:test:turbo:markharm
Default Relay State	
Name ID Format	Unspecified
Application username	The username for the account that is managed by Okta
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digital Algorithm	SHA256
Assertion Encryption	Unencrypted
SAML Single Logout	Enabled
Single Logout URL	https://10.10.10.123/vmturbo/rest/logout
SP Issuer	turbo
Signature Certificate	Example.cer (CN=apollo)
authnContextClassRef	PasswordProtectedTransport
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/$(org.externalKey)