Symantec Endpoint Protection End-User Guide

For Windows

Symantec Endpoint Protection (SEP) is the evolutionary successor to Symantec Anti-Virus (SAV). SEP provides the anti-virus protection of SAV but also significantly expands upon SAV in important ways. SEP provides protection against spyware and network attacks based on not only traditional exploit signatures, but also via firewalls, device control, application and network monitoring.

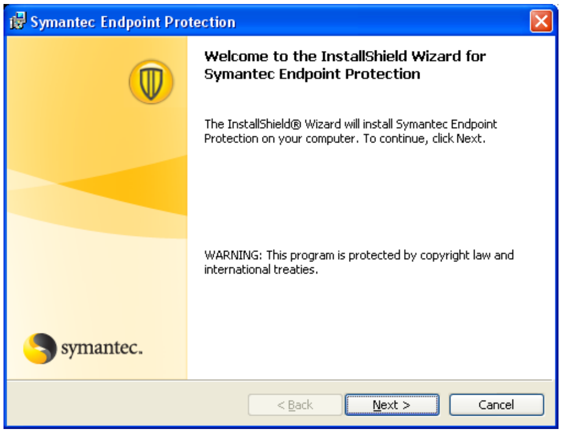
This document will guide the user through the installation process and introduce the most basic components of the SEP interface and provide insight as to what to expect from SEP’s behavior.

LLNL is providing SEP for home use as a no-cost benefit for its’ employees, collaborators, and summer students. The SEP software is provided as-is and this document as the exclusive means of support. **DO NOT CONTACT 4-HELP or any other support organizations at LLNL for support of this software.** The ONLY exception will be the case where the user is having difficulty downloading the SEP installation files from access.llnl.gov . You may report download problems to 4-HELP.

Installation

SEP is available for either 32-Bit or 64-Bit versions of Windows. Regardless of the operating system, the installation is essentially the same.

Run the “Setup.exe” file located in the root directory of the source files you obtained.



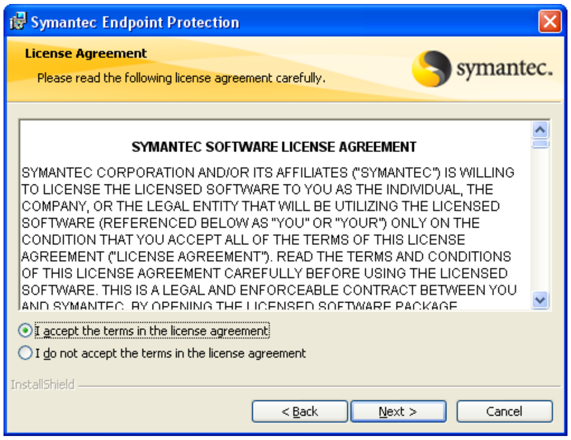
Symantec Endpoint Protection

Welcome to the InstallShield Wizard for Symantec Endpoint Protection

The InstallShield® Wizard will install Symantec Endpoint Protection on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Select the “Next” button.



License Agreement

Please read the following license agreement carefully.

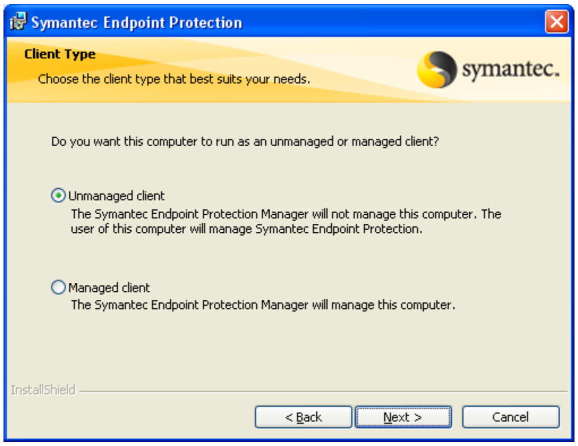
SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT ("LICENSE AGREEMENT"). READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THE LICENSED SOFTWARE PACKAGE

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Select the radio button "I accept the terms of the license agreement." Then click on the "Next" button.



Client Type

Choose the client type that best suits your needs.

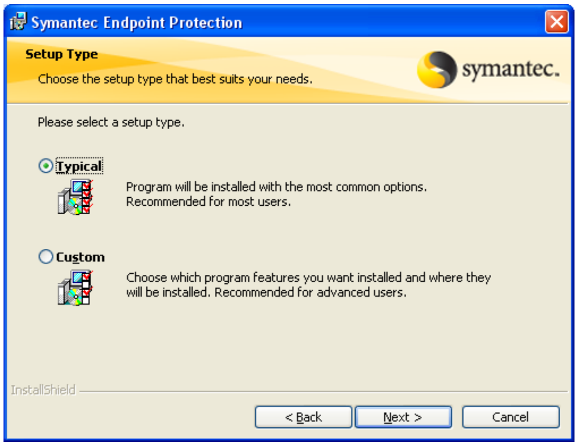
Do you want this computer to run as an unmanaged or managed client?

● Unmanaged client
The Symantec Endpoint Protection Manager will not manage this computer. The user of this computer will manage Symantec Endpoint Protection.

○ Managed client
The Symantec Endpoint Protection Manager will manage this computer.

Select the "Unmanaged Client" radio button.

Select "Typical" for the installation type. A "Typical" installation will require approximately 624 Mb of hard drive space.



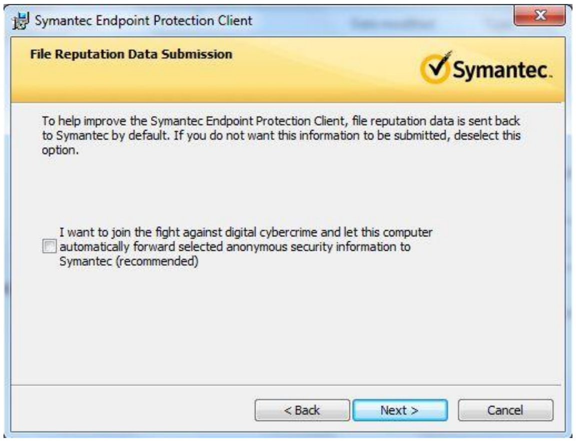
Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● **Typical**
Program will be installed with the most common options. Recommended for most users.

○ **Custom**
Choose which program features you want installed and where they will be installed. Recommended for advanced users.



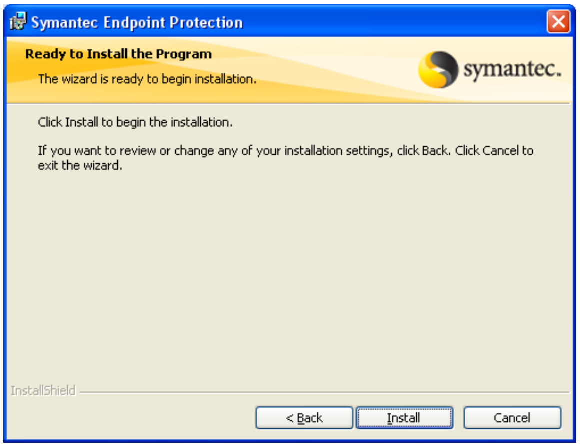
Symantec Endpoint Protection Client

File Reputation Data Submission

To help improve the Symantec Endpoint Protection Client, file reputation data is sent back to Symantec by default. If you do not want this information to be submitted, deselect this option.

□ I want to join the fight against digital cybercrime and let this computer automatically forward selected anonymous security information to Symantec (recommended)

Determine if you wish to supply anonymous data to Symantec. Uncheck if you do NOT wish to.



Symantec Endpoint Protection

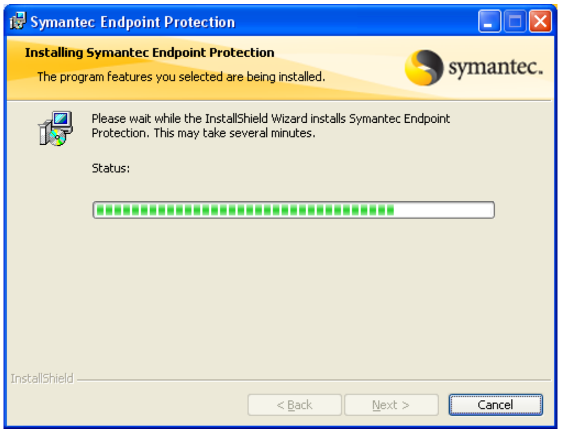
Ready to Install the Program

The wizard is ready to begin installation.

Click Install to begin the installation.

If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

Click “Install” to begin the installation process.



Symantec Endpoint Protection

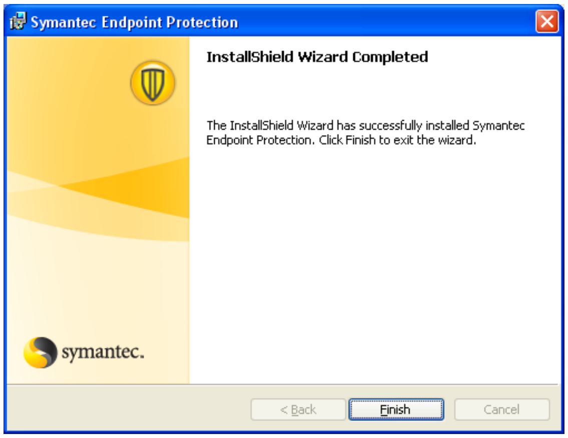
Installing Symantec Endpoint Protection

The program features you selected are being installed.

Please wait while the InstallShield Wizard installs Symantec Endpoint Protection. This may take several minutes.

Status:

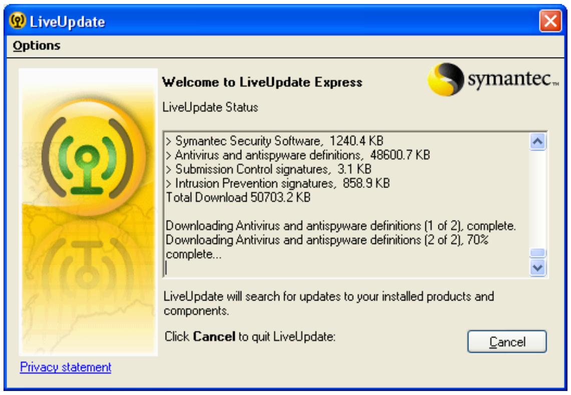
A progress indicator will be visible. Please wait until SEP is installed.



InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Symantec Endpoint Protection. Click Finish to exit the wizard.

Select the “Finish” button.



Welcome to LiveUpdate Express

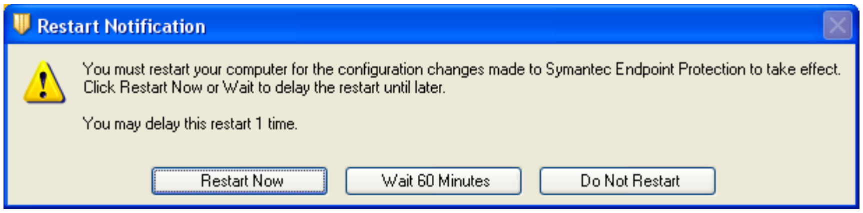
LiveUpdate Status

```
> Symantec Security Software, 1240.4 KB
> Antivirus and antispyware definitions, 48600.7 KB
> Submission Control signatures, 3.1 KB
> Intrusion Prevention signatures, 858.9 KB
Total Download 50703.2 KB

Downloading Antivirus and antispyware definitions (1 of 2), complete.
Downloading Antivirus and antispyware definitions (2 of 2), 70% complete...
```

LiveUpdate will search for updates to your installed products and components.

Click **Cancel** to quit LiveUpdate:

A “LiveUpdate” display will appear and often times before you’ve had a chance to select “Finish” from the previous display. No user interaction is required in this display and it will close automatically upon completion.



You must restart your computer for the configuration changes made to Symantec Endpoint Protection to take effect. Click Restart Now or Wait to delay the restart until later.

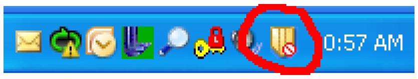
You may delay this restart 1 time.

Select the reboot option you prefer. SEP will not be fully functional until a reboot.

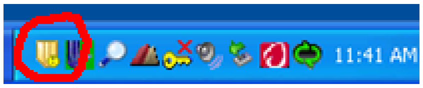
The installation is now complete. After a reboot, SEP will be fully functional.

SEP’s Status:

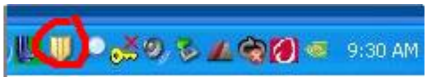
As with SAV, the presence and status of SEP can be quickly determined by looking for the SEP gold shield icon in the Windows system tray. In the view below, the SEP client can be seen circled in RED. A visible gold shield indicates that SEP is installed and running on the client computer.



The red circle with slash indicates that a major problem exits or at least one component of SEP is disabled.



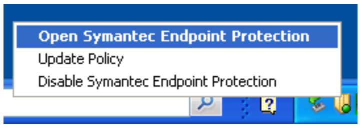
The yellow circle with an exclamation mark (!) indicates a minor problem; for example out-of-date virus definitions.



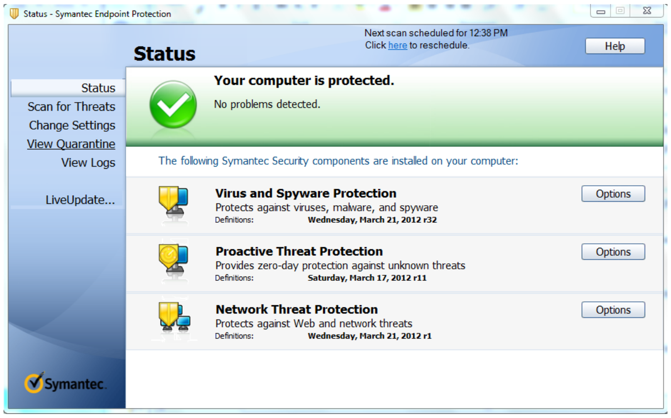
A gold-shield indicates that SEP is operating normally with no issues to report.

Viewing the SEP Interface:

More detail of the client can be viewed by launching the SEP interface. This can be done by right-mouse clicking the SEP icon in the system tray and selecting “Open Symantec Endpoint Protection”.


Open Symantec Endpoint Protection
Update Policy
Disable Symantec Endpoint Protection

On a Windows XP system, you can also simply double-left mouse click on the SEP icon to access the SEP interface.



Next scan scheduled for 12:38 PM
Click here to reschedule.

Your computer is protected.

No problems detected.

The following Symantec Security components are installed on your computer:

Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: **Wednesday, March 21, 2012 r32**

Proactive Threat Protection
Provides zero-day protection against unknown threats
Definitions: **Saturday, March 17, 2012 r11**

Network Threat Protection
Protects against Web and network threats
Definitions: **Wednesday, March 21, 2012 r1**

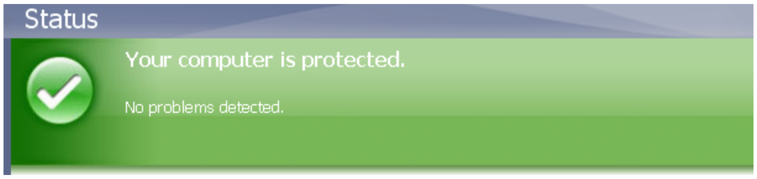
The full display of SEP includes indices on:

Antivirus & Antispyware Protection Status and definition date.

Proactive Threat Protection Status and definition date.

Network Threat Protection Status and definition date.

The horizontal green band and “Check Mark” indicate that all installed components of SEP are up-to-date and functioning correctly.

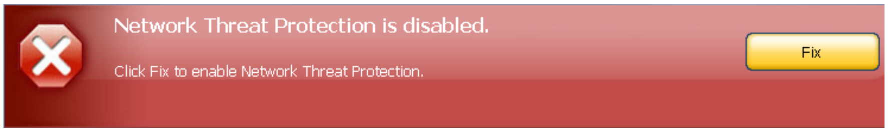


Your computer is protected.

No problems detected.

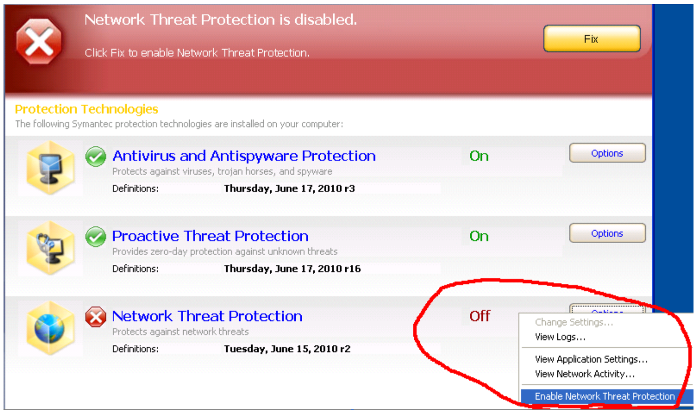
Reactivating a Disabled Feature:

A horizontal red band indicates that a SEP component or feature needs attention. On the far right hand of the red banner a yellow “Fix” button will be displayed. Selecting the “Fix” button will usually resolve the issue. In the case below, the Network Threat Protection (NTP) has been disabled by the user.



Network Threat Protection is disabled.

Click Fix to enable Network Threat Protection.



Network Threat Protection is disabled.

Click Fix to enable Network Threat Protection.

Protection Technologies

The following Symantec protection technologies are installed on your computer:

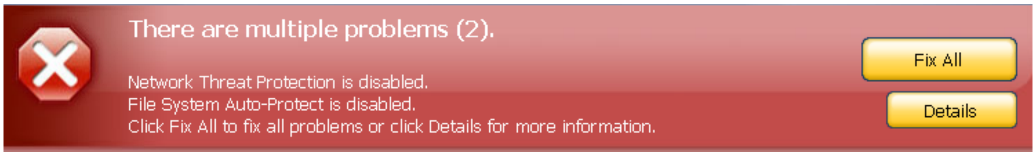
Antivirus and Antispyware Protection — On
Protects against viruses, trojan horses, and spyware
Definitions: Thursday, June 17, 2010 r3

Proactive Threat Protection — On
Provides zero-day protection against unknown threats
Definitions: Thursday, June 17, 2010 r16

Network Threat Protection — Off
Protects against network threats
Definitions: Tuesday, June 15, 2010 r2

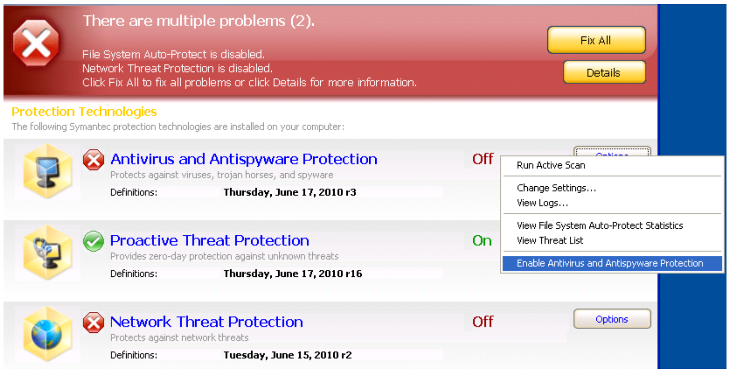
The status of the Network Threat Protection (NTP) feature is also indicated in the area below the banner. By choosing the “Options” button next to NTP, you can also reactivate NTP by selecting “Enable Network Threat Protection” from the sub-menu.

Here, two issues are being flagged for attention; Network Threat Protection and File System Auto-Protect have been disabled. By selecting the “Fix All” button, both features can be reactivated.



There are multiple problems (2).

Network Threat Protection is disabled.
File System Auto-Protect is disabled.
Click Fix All to fix all problems or click Details for more information.



There are multiple problems (2).

File System Auto-Protect is disabled.
Network Threat Protection is disabled.
Click Fix All to fix all problems or click Details for more information.

Protection Technologies

The following Symantec protection technologies are installed on your computer:

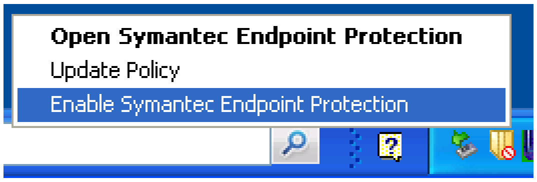
Antivirus and Antispyware Protection — Off
Protects against viruses, trojan horses, and spyware
Definitions: Thursday, June 17, 2010 r3

Proactive Threat Protection — On
Provides zero-day protection against unknown threats
Definitions: Thursday, June 17, 2010 r16

Network Threat Protection — Off
Protects against network threats
Definitions: Tuesday, June 15, 2010 r2

You can also choose to re-enable features individually by selecting the specific features’ “Options” button and the appropriate “Enable...” sub-menu.

A quick way to re-enable SEP is to simply to right-mouse click on the SEP icon in the system tray.



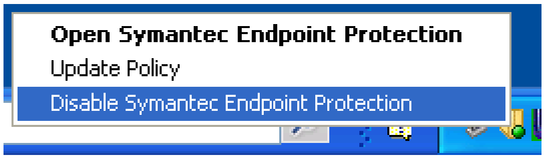
Open Symantec Endpoint Protection
Update Policy
Enable Symantec Endpoint Protection

Disabling SEP or a Specific Feature:

Users can disable the Antivirus and Antispyware (AV/AS) and the Network Threat Protection (NTP) components of SEP by right-mouse clicking on the SEP icon in the system tray and selecting “Disable Symantec Endpoint Protection”.

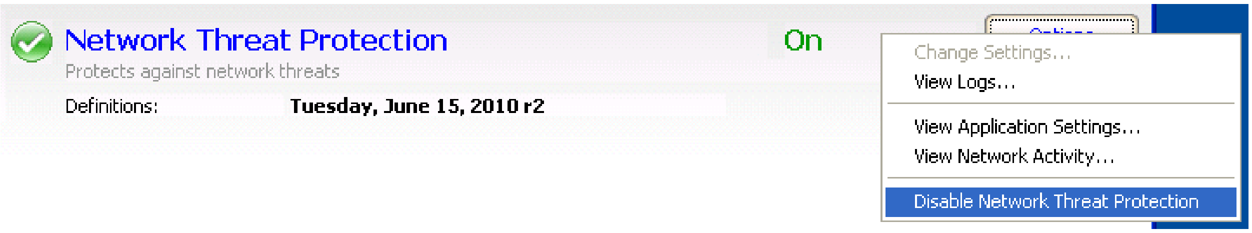
Disabling NTP may be useful if trouble-shooting a network based application that appears to not be working. Disable NTP only if necessary.

Disabling AV/AS is sometimes necessary to install software. **Disablement of AV/AS puts your system at risk!** Disable AV/AS only when absolutely necessary and only for as long as needed.


Open Symantec Endpoint Protection
Update Policy
Disable Symantec Endpoint Protection

Disabling SEP may be necessary to trouble-shoot application issues or to install software. Avoid disabling SEP on public wireless networks. Disable SEP only if absolutely necessary!

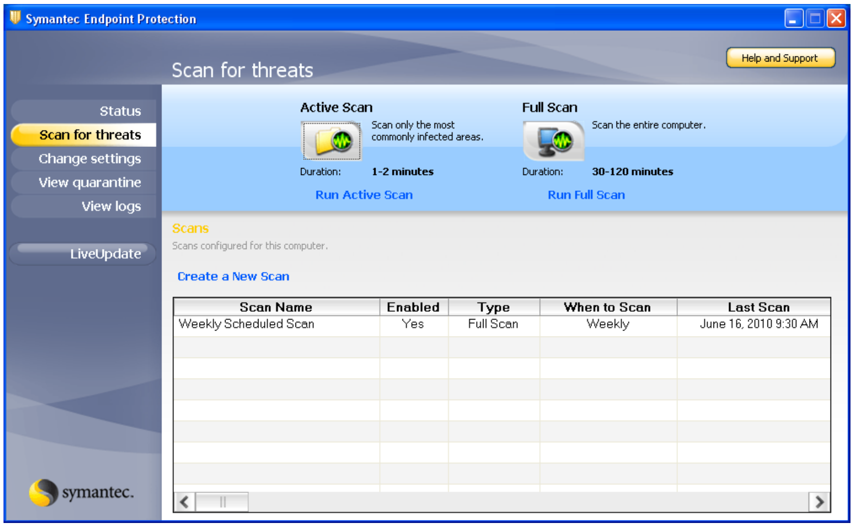
The full SEP interface can be used to disable individual features similarly to how they where enabled by choosing the corresponding “Options” button and selecting “Disable…”


Network Threat Protection
Protects against network threats
On
Change Settings...
View Logs...
View Application Settings...
View Network Activity...
Disable Network Threat Protection

Definitions: Tuesday, June 15, 2010 r2

SEP Console, “Scan for threats” Menu:

You can also choose to run a scan immediately by selecting either “Active Scan” or “Full Scan”. The “Active Scan” is relatively quick and will scan system memory, the registry and certain system files. “Full Scan” will in addition, scan every file on the system and consequently take longer to perform.



Active Scan: Scan only the most commonly infected areas. Duration: 1-2 minutes

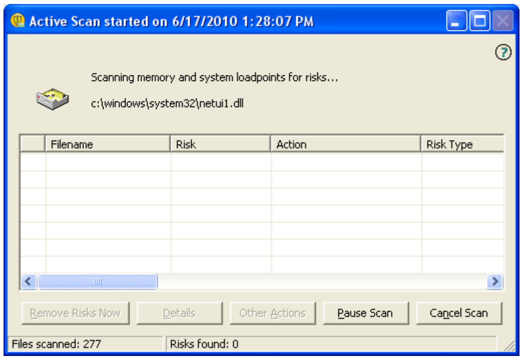
Full Scan: Scan the entire computer. Duration: 30-120 minutes

Scans

Scans configured for this computer.

Scan Name	Enabled	Type	When to Scan	Last Scan
Weekly Scheduled Scan	Yes	Full Scan	Weekly	June 16, 2010 9:30 AM

Selecting either scan type will launch a scan and a visible progress indicator.



Scanning memory and system loadpoints for risks...

c:\windows\system32\netui1.dll

Filename	Risk	Action	Risk Type

Files scanned: 277 Risks found: 0

You can pause or cancel a scan you initiate or the weekly scan.

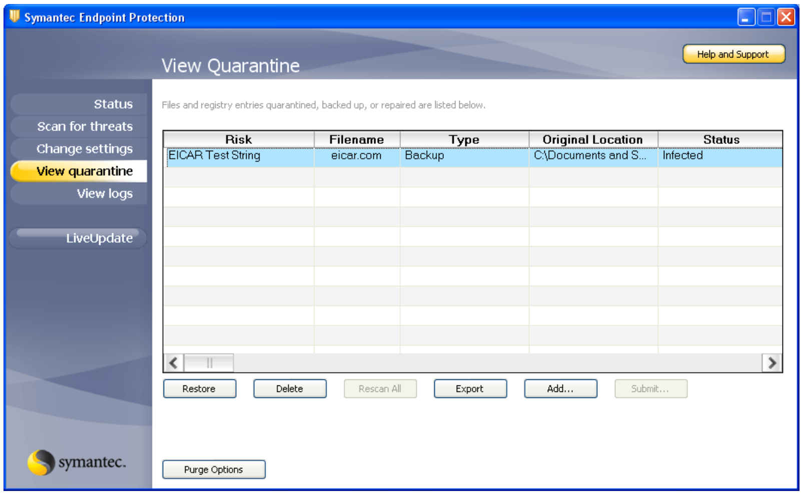
If a threat is found, you will be given the options:

“Remove Risk Now”= Removes or quarantines the threat.

“Details” = Provides additional information about the threat.

SEP Console, “View Quarantine” Menu:

Threats not automatically repaired will be quarantined and displayed.



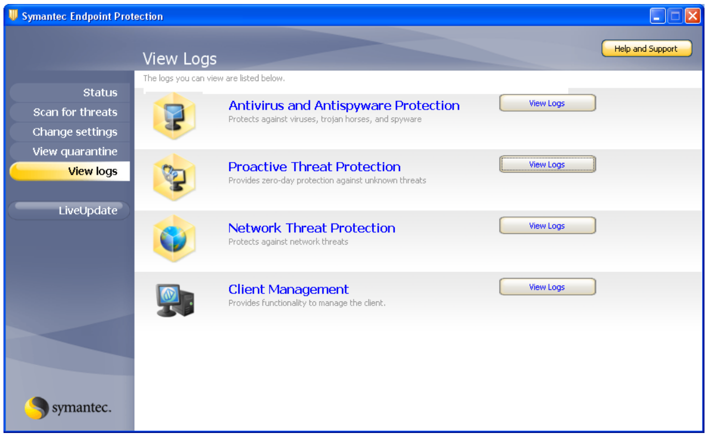
Files and registry entries quarantined, backed up, or repaired are listed below.

Risk	Filename	Type	Original Location	Status
EICAR Test String	eicar.com	Backup	C:\Documents and S...	Infected

Of the user selectable options, you should choose “Delete”.

SEP Console, “View Logs” Menu:

All of SEP individual components log their activities which can be viewed from this interface.



View Logs

The logs you can view are listed below.

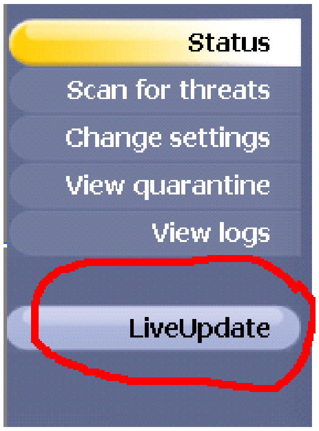
Antivirus and Antispyware Protection
Protects against viruses, trojan horses, and spyware

Proactive Threat Protection
Provides zero-day protection against unknown threats

Network Threat Protection
Protects against network threats

Client Management
Provides functionality to manage the client.

SEP Console, “LiveUpdate” Menu:



“LiveUpdate” will update the definition files for:

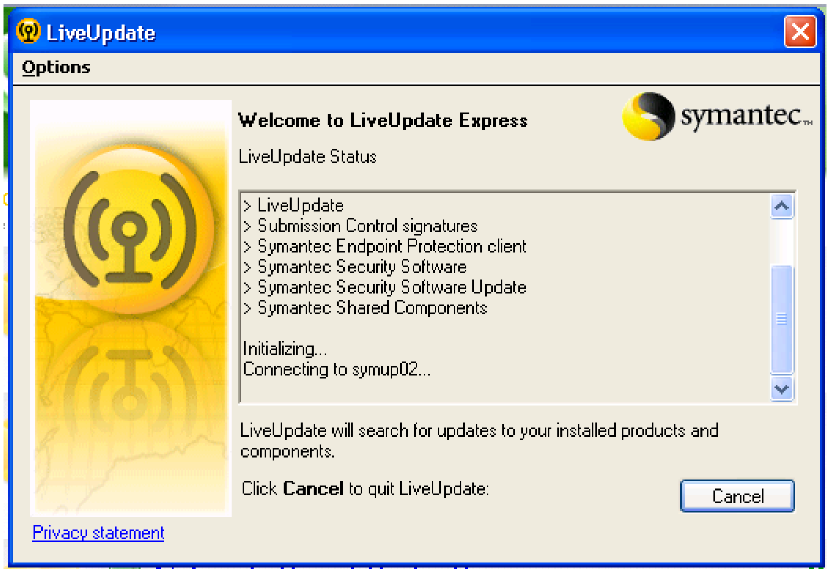
Antivirus and Antispyware

Proactive Threat Protection

Network Threat Protection

Launching “LiveUpdate” is rarely needed since the computer will automatically update its’ definition files.

In the rare case that you suspect your definitions are out of date, selecting “LiveUpdate” will launch the display shown below. The process of updating requires no user intervention and will close when complete.



Welcome to LiveUpdate Express

LiveUpdate Status

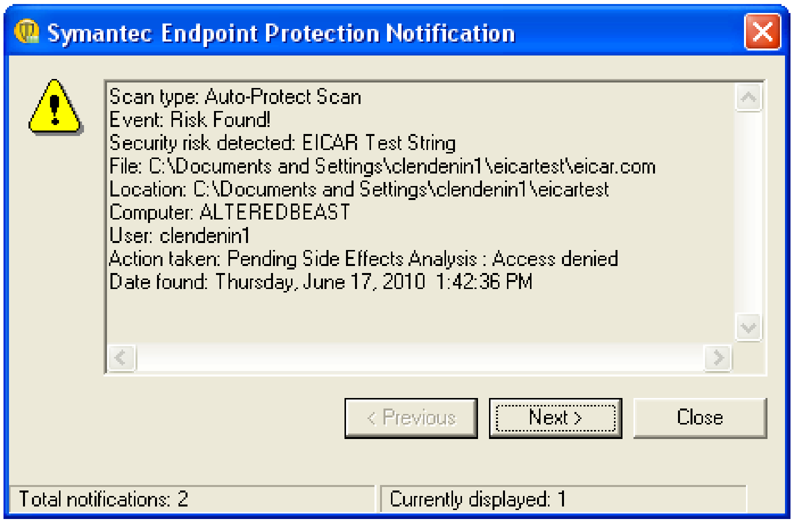
```
> LiveUpdate
> Submission Control signatures
> Symantec Endpoint Protection client
> Symantec Security Software
> Symantec Security Software Update
> Symantec Shared Components

Initializing...
Connecting to symup02...
```

LiveUpdate will search for updates to your installed products and components.

Click **Cancel** to quit LiveUpdate:

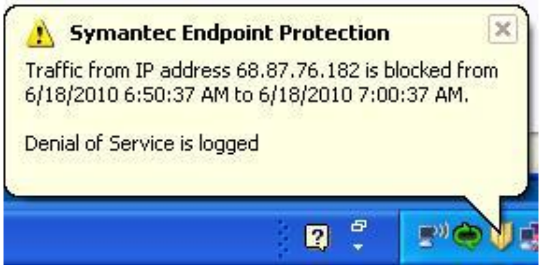
SEP Interaction: A Threat is Found!

Normally if a threat (virus or otherwise) is found, SEP will typically notify the user of the threat and what action has been taken. In the case of a virus, a display is presented, the virus is cleaned from the infected file (or the file is quarantined.) and SEP's actions are logged.



```
Scan type: Auto-Protect Scan
Event: Risk Found!
Security risk detected: EICAR Test String
File: C:\Documents and Settings\clendenin1\eicartest\eicar.com
Location: C:\Documents and Settings\clendenin1\eicartest
Computer: ALTEREDBEAST
User: clendenin1
Action taken: Pending Side Effects Analysis : Access denied
Date found: Thursday, June 17, 2010  1:42:36 PM
```

SEP Interaction: Network Based Threat Detected



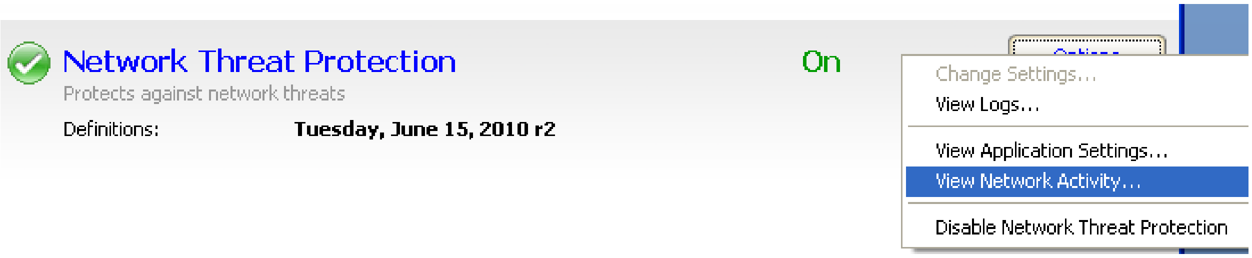
Traffic from IP address 68.87.76.182 is blocked from 6/18/2010 6:50:37 AM to 6/18/2010 7:00:37 AM.

Denial of Service is logged

At times, you may see a small dialog box displayed above the SEP icon in the system tray. This can occur when SEP blocks access to a remote system due to a network threat. No intervention is required on your part. A remote system will remain blocked for ten (10) minutes

A Closer look at the NTP “Options” button:

An interesting applet can be launched that will display applications accessing the network. From the NTP “Options” button, select “View Network Activity….”



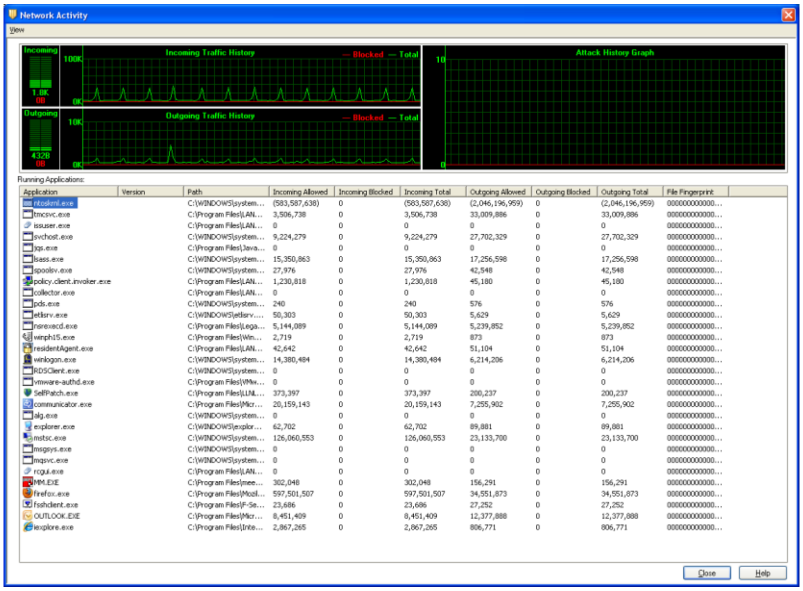
Network Threat Protection On

Protects against network threats

Definitions: Tuesday, June 15, 2010 r2

Change Settings...
View Logs...
View Application Settings...
View Network Activity...
Disable Network Threat Protection

The Network Activity applet will launch…



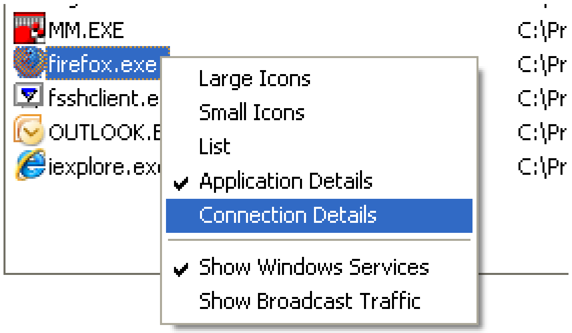
Running Applications:

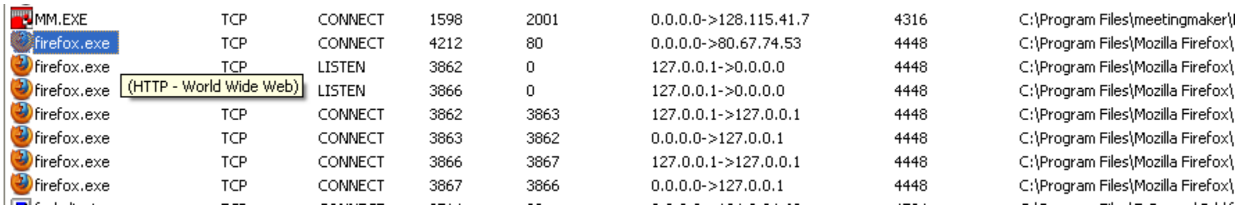
Application	Version	Path	Incoming Allowed	Incoming Blocked	Incoming Total	Outgoing Allowed	Outgoing Blocked	Outgoing Total	File Fingerprint
ntoskrnl.exe		C:\WINDOWS\system...	(583,587,638)	0	(583,587,638)	(2,046,196,959)	0	(2,046,196,959)	000000000000...
tmcsvc.exe		C:\Program Files\LAN...	3,506,738	0	3,506,738	33,009,886	0	33,009,886	000000000000...
issuser.exe		C:\Program Files\LAN...	0	0	0	0	0	0	000000000000...
svchost.exe		C:\WINDOWS\system...	9,224,279	0	9,224,279	27,702,329	0	27,702,329	000000000000...
jqs.exe		C:\Program Files\Java...	0	0	0	0	0	0	000000000000...
lsass.exe		C:\WINDOWS\system...	15,350,863	0	15,350,863	17,256,598	0	17,256,598	000000000000...
spoolsv.exe		C:\WINDOWS\system...	27,976	0	27,976	42,548	0	42,548	000000000000...
policy.client.invoker.exe		C:\Program Files\LAN...	1,230,818	0	1,230,818	45,180	0	45,180	000000000000...
collector.exe		C:\Program Files\LAN...	0	0	0	0	0	0	000000000000...
pds.exe		C:\WINDOWS\system...	240	0	240	576	0	576	000000000000...
etlisrv.exe		C:\WINDOWS\etlisrv....	50,303	0	50,303	5,629	0	5,629	000000000000...
nsrexecd.exe		C:\Program Files\Lega...	5,144,089	0	5,144,089	5,239,852	0	5,239,852	000000000000...
winph15.exe		C:\Program Files\Win...	2,719	0	2,719	873	0	873	000000000000...
residentAgent.exe		C:\Program Files\LAN...	42,642	0	42,642	51,104	0	51,104	000000000000...
winlogon.exe		C:\WINDOWS\system...	14,380,484	0	14,380,484	6,214,206	0	6,214,206	000000000000...
RDSClient.exe		C:\WINDOWS\system...	0	0	0	0	0	0	000000000000...
vmware-authd.exe		C:\Program Files\VMw...	0	0	0	0	0	0	000000000000...
SelfPatch.exe		C:\Program Files\LLNL...	373,397	0	373,397	200,237	0	200,237	000000000000...
communicator.exe		C:\Program Files\Micr...	20,159,143	0	20,159,143	7,255,902	0	7,255,902	000000000000...
alg.exe		C:\WINDOWS\system...	0	0	0	0	0	0	000000000000...
explorer.exe		C:\WINDOWS\explor...	62,702	0	62,702	89,881	0	89,881	000000000000...
mstsc.exe		C:\WINDOWS\system...	126,060,553	0	126,060,553	23,133,700	0	23,133,700	000000000000...
msgsys.exe		C:\WINDOWS\system...	0	0	0	0	0	0	000000000000...
mqsvc.exe		C:\WINDOWS\system...	0	0	0	0	0	0	000000000000...
rcgui.exe		C:\Program Files\LAN...	0	0	0	0	0	0	000000000000...
MM.EXE		C:\Program Files\mee...	302,048	0	302,048	156,291	0	156,291	000000000000...
firefox.exe		C:\Program Files\Mozil...	597,501,507	0	597,501,507	34,551,873	0	34,551,873	000000000000...
fsshclient.exe		C:\Program Files\F-Se...	23,686	0	23,686	27,252	0	27,252	000000000000...
OUTLOOK.EXE		C:\Program Files\Micr...	8,451,409	0	8,451,409	12,377,888	0	12,377,888	000000000000...
iexplore.exe		C:\Program Files\Inte...	2,867,265	0	2,867,265	806,771	0	806,771	000000000000...

A graphical view of network activity will be provided and anything blocked will be noted in red on the graph.

Below the graphs, will be a list of applications utilizing the network. Note the respective information in the columns.

You can select an individual application, right-mouse click on it, and select “Connection Details” for port information and remote access information. Good stuff!





MM.EXE	TCP	CONNECT	1598	2001	0.0.0.0->128.115.41.7	4316	C:\Program Files\meetingmaker\
firefox.exe	TCP	CONNECT	4212	80	0.0.0.0->80.67.74.53	4448	C:\Program Files\Mozilla Firefox\
firefox.exe	TCP	LISTEN	3862	0	127.0.0.1->0.0.0.0	4448	C:\Program Files\Mozilla Firefox\
firefox.exe		LISTEN	3866	0	127.0.0.1->0.0.0.0	4448	C:\Program Files\Mozilla Firefox\
firefox.exe	TCP	CONNECT	3862	3863	127.0.0.1->127.0.0.1	4448	C:\Program Files\Mozilla Firefox\
firefox.exe	TCP	CONNECT	3863	3862	0.0.0.0->127.0.0.1	4448	C:\Program Files\Mozilla Firefox\
firefox.exe	TCP	CONNECT	3866	3867	127.0.0.1->127.0.0.1	4448	C:\Program Files\Mozilla Firefox\
firefox.exe	TCP	CONNECT	3867	3866	0.0.0.0->127.0.0.1	4448	C:\Program Files\Mozilla Firefox\

Note: Changing the display to “Connection Details” affects the display of all listed applications.

Off-site Altering of Windows SEP’s Firewall Rules

Overview

Symantec Endpoint Protection (SEP) for Windows has the ability to detect network characteristics that the client system is communicating on and to alter its’ configuration in response to the network detected. This ability is called “location awareness”. Location awareness is the key mechanism for how SEP on LLNL laptops and tablets alters its’ firewall rules such that it’s more trusting on LLNL networks and more protective when off-site.

SEP determines that the client is on-site by polling for authorized LLNL DNS servers. If these are detected, the firewall rules accept all network traffic that is sourced from typical networks on site. Otherwise, the firewall will be configured to be more protective in an off-site situation.

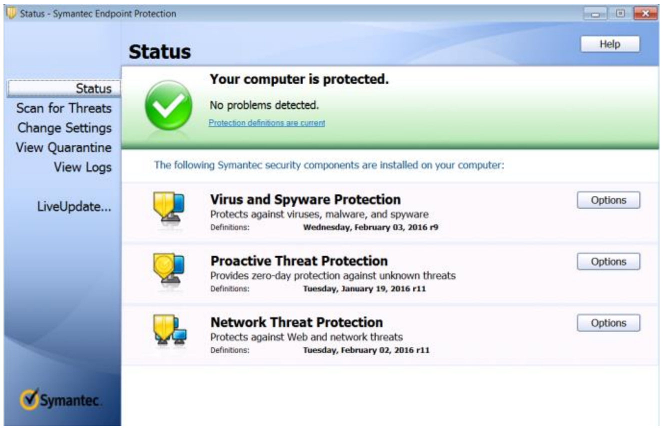
Off-site Firewall Rule Alterations

Based on testing, you should not have problems accessing publically available networks that you might find in hotels, restaurants, or home networks. However, there is a chance that the SEP firewalls rules could block access to some public wireless networks or certain features of a home network. Assuming you have Windows administrative privileges on your laptop or tablet, and are logged on with those credentials, you can make changes to the SEP firewall if necessary.

To alter the SEP firewall rules (logged on with administrative rights) launch the SEP application by clicking on the icon in the system tray (lower right-hand corner near date and time display). Sometimes the system-tray icons are hiding behind the ▲ icon. Click on the ▲ icon to reveal the running applications.

Right click on and select "**Open Symantec Endpoint Protection**".

The SEP application will launch and you'll see the SEP interface.



Status - Symantec Endpoint Protection

Status

Your computer is protected.

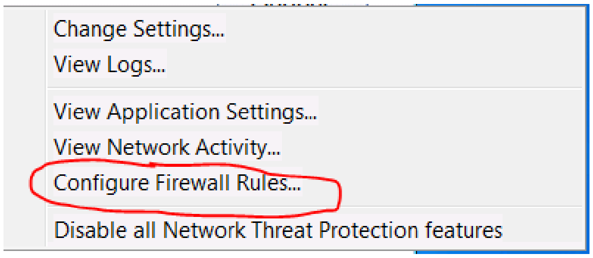
No problems detected.

Protection definitions are current

The following Symantec security components are installed on your computer:

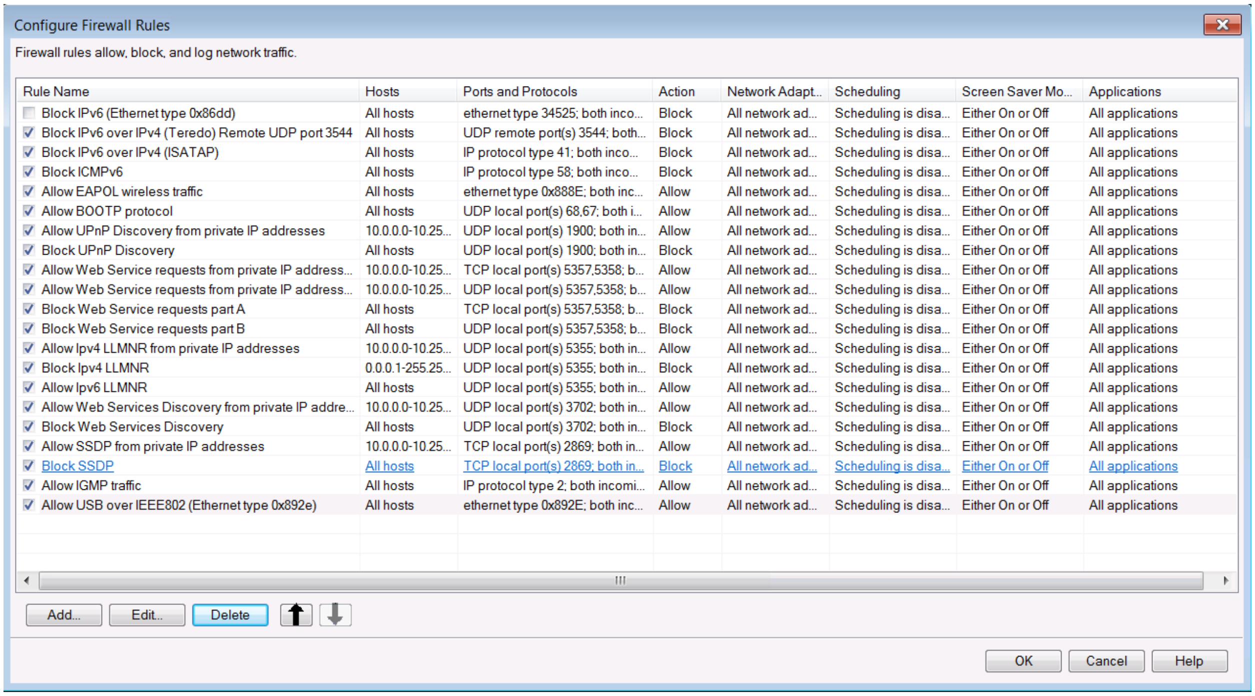
Virus and Spyware Protection Protects against viruses, malware, and spyware Definitions: Wednesday, February 03, 2016 r9	Options
Proactive Threat Protection Provides zero-day protection against unknown threats Definitions: Tuesday, January 19, 2016 r11	Options
Network Threat Protection Protects against Web and network threats Definitions: Tuesday, February 02, 2016 r11	Options

Look for the Options button aligned with the **Network Threat Protection** feature and click on it. From the fly-out menu, select "Configure Firewall Rules…."



Change Settings...
View Logs...
View Application Settings...
View Network Activity...
Configure Firewall Rules...
Disable all Network Threat Protection features

The firewall rules interface will launch and will list a set of firewall rules.



Configure Firewall Rules

Firewall rules allow, block, and log network traffic.

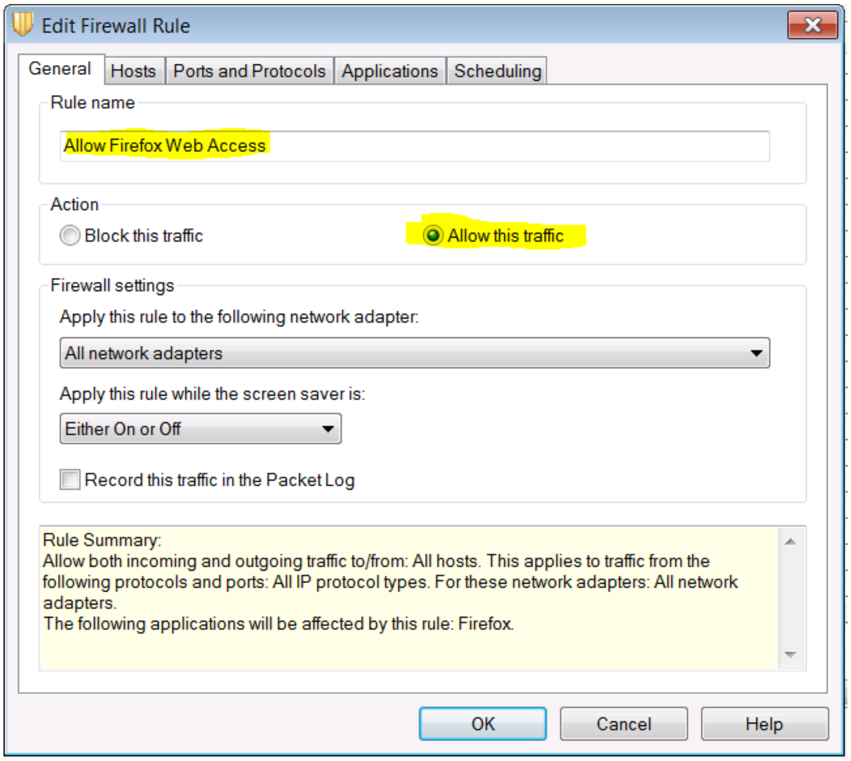
Rule Name	Hosts	Ports and Protocols	Action	Network Adapt...	Scheduling	Screen Saver Mo...	Applications
☐ Block IPv6 (Ethernet type 0x86dd)	All hosts	ethernet type 34525; both inco...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block IPv6 over IPv4 (Teredo) Remote UDP port 3544	All hosts	UDP remote port(s) 3544; both...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block IPv6 over IPv4 (ISATAP)	All hosts	IP protocol type 41; both inco...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block ICMPv6	All hosts	IP protocol type 58; both inco...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow EAPOL wireless traffic	All hosts	ethernet type 0x888E; both inc...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow BOOTP protocol	All hosts	UDP local port(s) 68,67; both i...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow UPnP Discovery from private IP addresses	10.0.0.0-10.25...	UDP local port(s) 1900; both in...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block UPnP Discovery	All hosts	UDP local port(s) 1900; both in...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow Web Service requests from private IP address...	10.0.0.0-10.25...	TCP local port(s) 5357,5358; b...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow Web Service requests from private IP address...	10.0.0.0-10.25...	UDP local port(s) 5357,5358; b...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block Web Service requests part A	All hosts	TCP local port(s) 5357,5358; b...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block Web Service requests part B	All hosts	UDP local port(s) 5357,5358; b...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow Ipv4 LLMNR from private IP addresses	10.0.0.0-10.25...	UDP local port(s) 5355; both in...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block Ipv4 LLMNR	0.0.0.1-255.25...	UDP local port(s) 5355; both in...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow Ipv6 LLMNR	All hosts	UDP local port(s) 5355; both in...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow Web Services Discovery from private IP addre...	10.0.0.0-10.25...	UDP local port(s) 3702; both in...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block Web Services Discovery	All hosts	UDP local port(s) 3702; both in...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow SSDP from private IP addresses	10.0.0.0-10.25...	TCP local port(s) 2869; both in...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Block SSDP	All hosts	TCP local port(s) 2869; both in...	Block	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow IGMP traffic	All hosts	IP protocol type 2; both incomi...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications
☑ Allow USB over IEEE802 (Ethernet type 0x892e)	All hosts	ethernet type 0x892E; both inc...	Allow	All network ad...	Scheduling is disa...	Either On or Off	All applications

Most of these rules may be difficult to interpret unless you have some technical networking background. If you suspect that a particular rule is problematic, simply uncheck the box next to it under the "Rule Name" column to disable it. You must also click the "OK" button to activate the changes.

For most users (and technicians for that matter) it will be easier to add a rule to grant access through the SEP firewall. The following steps will guide you through the process.

At the bottom of the interface click the Add... button.

An "Add Firewall Rule" template will launch. In the "Rule name" field enter a meaningful name. In this case we'll call it "Allow Firefox Web Access". Our intent with this example rule is to grant the Firefox browser complete network access.



Rule name

Allow Firefox Web Access

Action

○ Block this traffic ● Allow this traffic

Firewall settings

Apply this rule to the following network adapter:

All network adapters

Apply this rule while the screen saver is:

Either On or Off

□ Record this traffic in the Packet Log

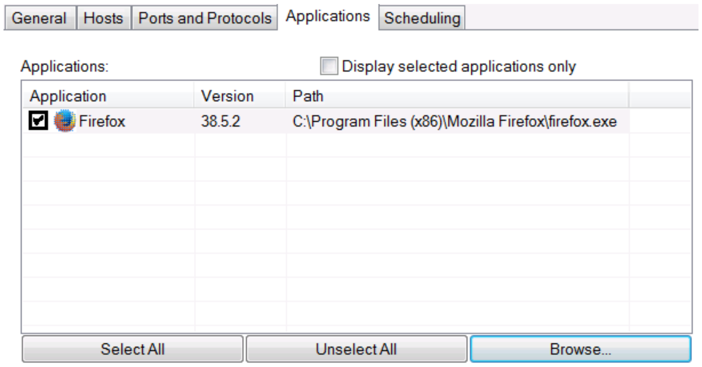
Rule Summary:
Allow both incoming and outgoing traffic to/from: All hosts. This applies to traffic from the following protocols and ports: All IP protocol types. For these network adapters: All network adapters.
The following applications will be affected by this rule: Firefox.

Under the "Action" header, select the ● Allow this traffic radio button.

Now select the Applications tabby near the top of the interface.

Your application list will be blank at this time. Select the Browse... button to launch a file navigator. We are looking for the executable firefox.exe which is usually located in the "C:\Program Files (X86)\Mozilla Firefox" directory. Navigate to that location and select firefox.exe and then select the Open button.

Firefox should now be listed along with its' version number and path in the application list.

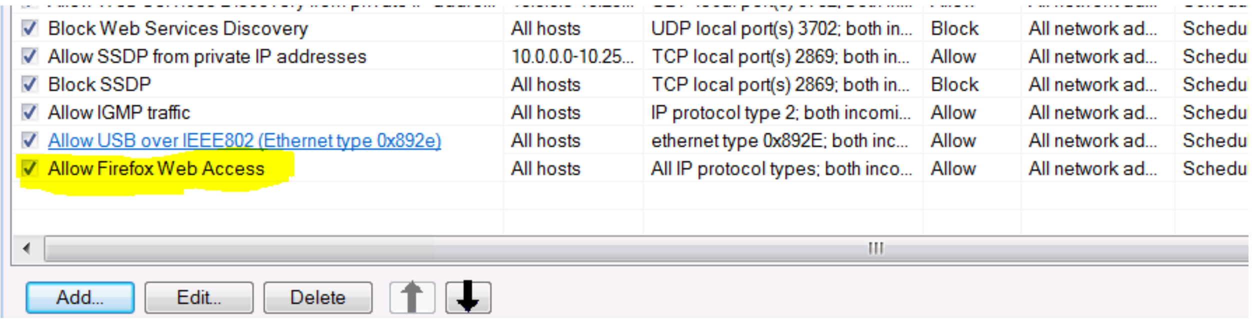


Applications: □ Display selected applications only

Application	Version	Path
☑ Firefox	38.5.2	C:\Program Files (x86)\Mozilla Firefox\firefox.exe

Click the OK button.

You should now see the “Allow Firefox Web Access” at the bottom of the rule lists.



☑ Block Web Services Discovery	All hosts	UDP local port(s) 3702; both in...	Block	All network ad...	Schedu
☑ Allow SSDP from private IP addresses	10.0.0.0-10.25...	TCP local port(s) 2869; both in...	Allow	All network ad...	Schedu
☑ Block SSDP	All hosts	TCP local port(s) 2869; both in...	Block	All network ad...	Schedu
☑ Allow IGMP traffic	All hosts	IP protocol type 2; both incomi...	Allow	All network ad...	Schedu
☑ Allow USB over IEEE802 (Ethernet type 0x892e)	All hosts	ethernet type 0x892E; both inc...	Allow	All network ad...	Schedu
☑ Allow Firefox Web Access	All hosts	All IP protocol types; both inco...	Allow	All network ad...	Schedu

Finally, click the OK button. The rule should now be active and Firefox will have access to the network.

You can do the same thing for any other browser or application that you wish to allow network access though the SEP’s firewall.