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](http://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.

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

Select the “Unmanaged Client” radio button.

Select “Typical” for the installation type. A “Typical” installation will require approximately 624 Mb of hard drive space.
Click “Install” to begin the installation process.

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

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

Select the “Finish” button.

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.

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.
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”.

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

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.

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.

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.

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.

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.
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.

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 were enabled by choosing the corresponding “Options” button and selecting “Disable...”

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

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.

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.

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.
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.
SEP Interaction: Network Based Threat Detected

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....”
The Network Activity applet will launch...

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!
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.

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

The firewall rules interface will launch and will list a set of firewall rules.
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.
Under the “Action” header, select the radio button.

Now select the tabby near the top of the interface.

Your application list will be blank at this time. Select the 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 button.

Firefox should now be listed along with its’ version number and path in the application list.
Click the **OK** button.

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

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 through the SEP’s firewall.