SOPHOS
Security made simple.

Sophos Endpoint Security and Control

MSP Guide for Single Server

Product Version: 5.5

Contents

1 About this guide

This guide is for managed service providers (MSPs) who offer managed Sophos Endpoint Security and Control to customers. It describes how to set up Sophos Endpoint Security and Control (SESC) in such a way that you can manage it remotely on behalf of a customer (as well as protecting your own computers) using a single server.

Note
If you want to set up a distributed system (where one or more additional servers are used, such as for hosting the clients' updating source in your DMZ) instead of a single server, see the *Sophos Endpoint Security and Control Managed Service Provider guide* for a distributed system instead of this guide.

This guide assumes you are familiar with and already using a remote monitoring and management system (RMM) such as Kaseya, N-able, LevelPlatforms or Zenith to provide remote software installation, management and monitoring services to your customer end-users.

Use this document in partnership with your assigned Sophos Sales Engineer. If you do not have a Sales Engineer, contact your Sophos Account Manager.

Sophos documentation is published at http://www.sophos.com/en-us/support/documentation.aspx.

2 About Sophos software

This section describes the Sophos products for managed endpoint security.

2.1 Sophos Enterprise Console

Sophos Enterprise Console is an administration tool that deploys and manages Sophos endpoint software using groups and policies. It also provides alerts and detailed reports about endpoint status and detected threats.

Sophos Enterprise Console includes and manages Sophos Update Manager.

2.1.1 Sophos Update Manager

Sophos Update Manager downloads software and updates from Sophos automatically to a central location. It makes these updates available in shared update folders. Endpoint computers update themselves from these shares.

Sophos Update Manager is installed as part of Sophos Enterprise Console but can also be installed separately.

2.1.2 Reporting Interface and Log Writer

Sophos Reporting Interface and Sophos Reporting Log Writer are additional tools you can use with Sophos Enterprise Console. They enable you to use third-party reporting and log-monitoring software to generate reports from threat and event data in Sophos Enterprise Console. For more information, see:

- Sophos Reporting Interface documentation page
- Sophos Reporting Log Writer documentation page
- Knowledgebase article 112873

2.2 Sophos Endpoint Security and Control

Sophos Endpoint Security and Control (SESC) refers both to the entire suite of Sophos security software as described in this section, and also the agent which runs on endpoint computers, protecting them and interacting with the administration tools.

Sophos Endpoint Security and Control (for endpoints) includes these components:

- Sophos AutoUpdate. This updates itself and the other components from an Sophos Update Manager.
- Sophos Remote Management System (RMS). This handles communications with Sophos Enterprise Console over TCP on ports 8192 and 8194.
- Sophos Anti-Virus. This includes anti-virus, HIPS, data control, and device control features.

- Web protection (optional) provides enhanced protection against web threats. It includes the following features:
    - Live URL filtering, which blocks access to websites that are known to host malware. This feature works by performing a real-time lookup against Sophos's online database of infected websites.
    - Content scanning, which scans data and files downloaded from the internet (or intranet) and proactively detects malicious content. This feature scans content hosted at any locations, including those not listed in the database of infected websites.
        - With Website control (optional), you can filter the web activity of users, based on the 14 website categories: Adult Sexually Explicit, Alcohol and Tobacco, Anonymizer Proxies, Criminal Activity, Gambling, Hacking, Illegal Drugs, Intolerance and Hate, Phishing and Fraud, Spam URLs, Spyware, Tasteless and Offensive, Violence, and Weapons.
- Sophos Client Firewall (optional). This enables only named applications, or classes of applications, to access a network or the internet.
- Sophos Patch (optional). Sophos Enterprise Console enables you to check that the endpoint computers have the most up-to-date security patches installed. SophosLabs provides ratings that help you determine the most critical security patch issues so that you can resolve them quickly. SophosLabs ratings take the latest exploits into account and therefore may differ from a vendor's severity level.

3 How does Sophos Endpoint Security and Control work for MSPs?

Managed Sophos Endpoint Security and Control works as follows:

You, the Managed Service Provider (MSP) provide managed IT services to remote customers over the internet.

Sophos Enterprise Console (SEC) runs on a server you host (the *SEC Server*). It allows you to manage computer groups and security policies, and displays detailed endpoint status and alerts.

Sophos Update Manager (SUM parent) runs on the SEC server. It publishes software installation files and updates from Sophos on your host to shared folders on your LAN.

Sophos Update Manager (SUM child) runs on a web server in your DMZ (the *Sophos DMZ Server*). It gets and publishes software installation files and updates from the SUM parent to shared folders in your DMZ.

The Sophos DMZ Server also needs to run the Microsoft IIS (Internet Information Services) web server so that it can publish the shared Sophos update folders to the internet using HTTP.

Sophos Endpoint Security and Control (SESC) runs on the SEC Server, the Sophos DMZ Server and the customer's endpoint computers, protecting them from threats and sending reports back to Sophos Enterprise Console.

Sophos Endpoint Security and Control includes Sophos AutoUpdate (SAU) which gets its updates from the shared folders maintained by SUM installed on the Sophos Enterprise Console Server over HTTP (using IIS).

Remote Management System (RMS) runs on all computers (including the Sophos Enterprise Console Server and clients) to provide the bidirectional communication mechanism for policies, client status, and alerts.

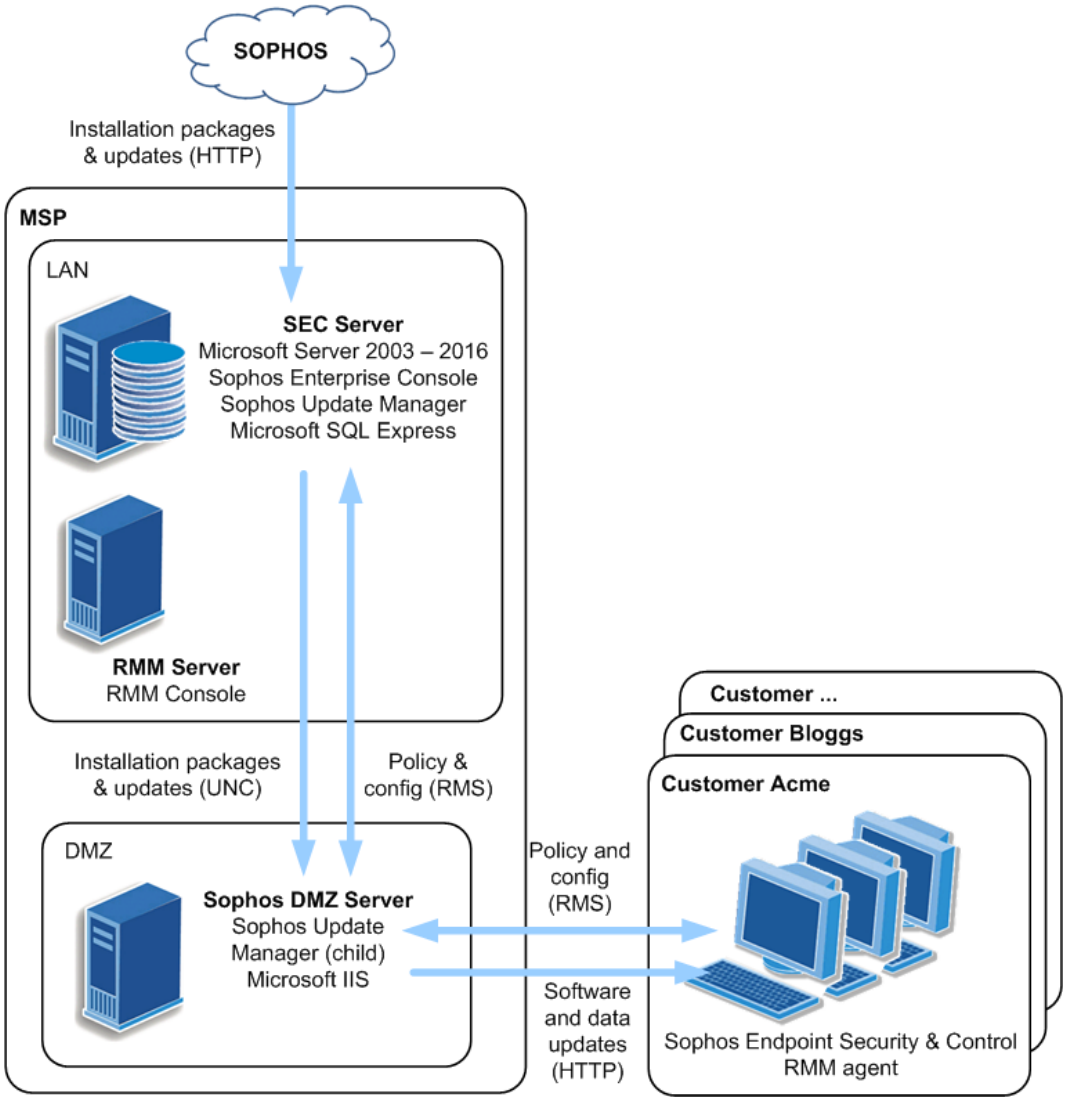
The Remote Monitoring and Management system (RMM) (for example Kaseya) consists of a console at the MSP, together with agents installed on each managed endpoint.

The RMM system:

- deploys a custom Sophos Endpoint Security and Control installer package on each endpoint,
- runs the package, installing Sophos Endpoint Security and Control on each endpoint,
- regularly runs a script on each endpoint which queries Sophos Endpoint Security and Control, enabling the RMM console to display basic status and alerts,
- manages other third-party endpoint software in a similar way.

There are many RMM products from various vendors for different situations and applications.

The configuration and methods of communication between RMM components are proprietary and beyond the scope of this guide.



Note

Other computers within the MSP's LAN may also optionally be protected as described in Protect your Sophos Enterprise Console Server (page 17); for clarity, this is not shown. Likewise, RMM network communications will vary according to the system used and are not shown.

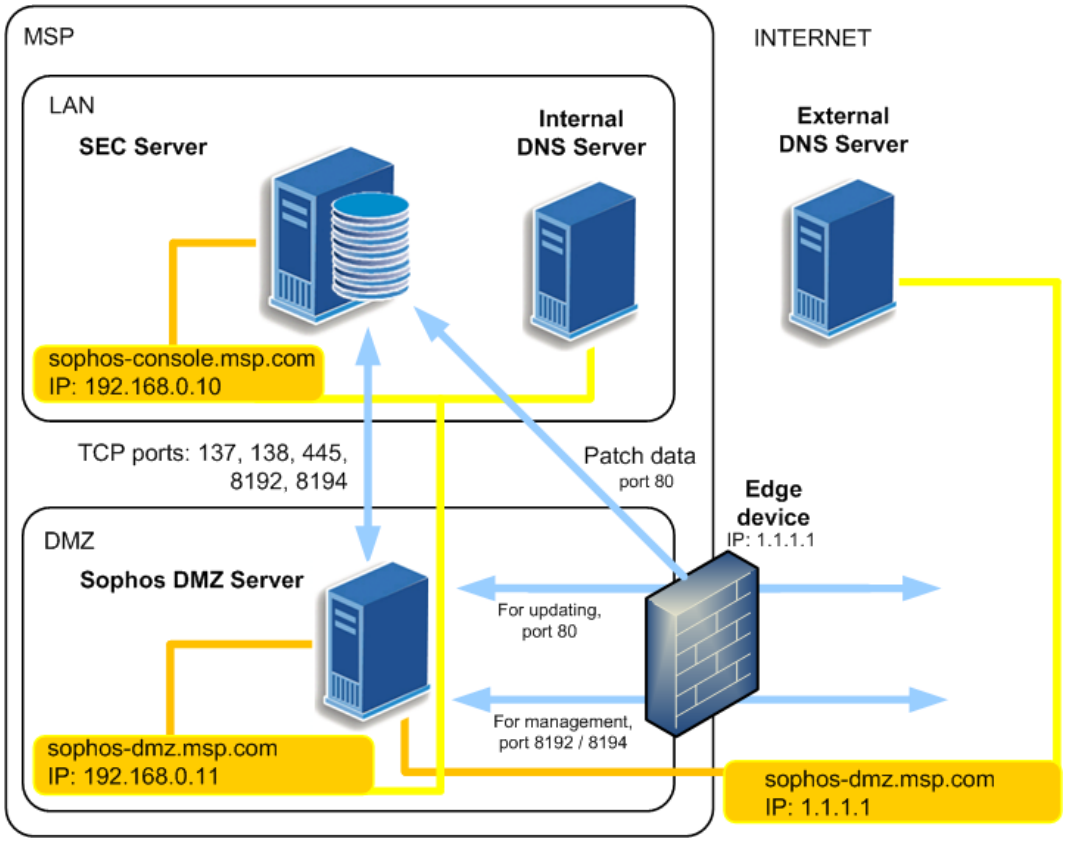
Note

Starting with version 5.4.0, Sophos Enterprise Console (including the remote management console component) is no longer supported on Windows Server 2003, Windows Server 2003 R2, Windows XP, and Windows Vista.

4 How does your Sophos Enterprise Console Server manage its clients

This section explains how to configure the various network components to enable communications between the Sophos Enterprise Console Server, the Sophos DMZ Server and the customers' managed endpoints.

The diagram below shows how the various servers, domains, ports, internal and external IP addresses interact. The IP addresses shown are examples and should be replaced with actual IP addresses.



The Sophos DMZ Server is addressed both internally and externally by the same domain name, sophos-dmz.msp.com. The internal and external DNS servers however map sophos-dmz.msp.com to different IP addresses, as shown above.

We assume that the virtual directory website uses port 80 for inbound connections. All ports shown in the above example are TCP ports.

In the example shown, the edge device has an IP address 1.1.1.1, which is the external interface of the firewall. Ports 80, 8192, and 8194 are translated with NAT through this interface.

If you plan to use Sophos Patch, you must configure the reverse proxy on the edge device so it redirects the traffic that matches the address http://<1.1.1.1>/Sophos/Management/Patch/EndpointCommunicator/ directly to the Sophos Enterprise Console Server.

We recommend you use a transparent caching proxy on the customer's location to reduce traffic used by patch and endpoint updates.

Note
Alternative ports can be used if necessary, for example if another application is already using port 80. When configuring client updating, the location should be specified in the standard manner. For example, if port 8085 is to be used, the update location should be http://sophos-dmz.msp.com:8085/sophos.

4.1 Network requirements

All machines, including the Sophos Enterprise Console server, should be able to resolve the fully qualified domain name (FQDN) appropriately. If your server is using a private IP (RFC 1918) and is publically reached using NAT, this would mean that sophos-dmz.msp.com would resolve to the Sophos DMZ Server's internal IP address (e.g. 192.168.0.2). For remote machines, the FQDN would resolve to your Sophos DMZ Server's external IP address (e.g 1.1.1.1).

1. Create a DNS A record called sophos-dmz.msp.com for BOTH internal and external DNS systems as follows:
    a) Create an internal address record that resolves to the internal IP address of the Sophos DMZ Server (e.g. 192.168.0.11).
    b) Create an external (Internet) DNS A record that resolves to the public interface of the Sophos DMZ Server (e.g. 1.1.1.1).
2. Configure the Sophos DMZ Server Internet firewall to port-forward (with NAT) ports TCP 8192 and 8194.

5 What are the key steps?

The key steps are as follows:

- Install Sophos Enterprise Console on a server you host (your Sophos Enterprise Console Server). This includes the Sophos Update Manager.
- Modify the configuration and registry values.
- Download the security software you need.
- Publish a shared folder from which customers' computers can update.
- Configure your Sophos Enterprise Console Server by creating groups for each customer and editing the updating policy.
- Verify your Sophos Enterprise Console Server configuration
- Protect the Sophos Enterprise Console Server with Sophos security software, and optionally other computers on your LAN.
- Create an installer package.
- Verify your installation package.
- Distribute the installer package to the customer's computers (using the RMM system).
- Manage the endpoint security software.

6 Installing Sophos Enterprise Console on your Sophos Enterprise Console server

The following instructions explain how to install Sophos Enterprise Console on your Sophos Enterprise Console Server.

6.1 Prepare to install Sophos Enterprise Console

On the server that meets the system requirements for a Sophos Enterprise Console Server (see knowledgebase article 118635), you must:

1. Ensure it is connected to the internet.
2. Ensure you have access to the Windows operating system installation and Service Pack CDs. You may be prompted for them during installation.
3. If the Sophos Enterprise Console Server has Microsoft SQL Server version earlier than 2005 SP4, upgrade it. If not, SQL Server Express is included with Sophos Enterprise Console (SQL Server Express 2012 SP4 is included with Sophos Enterprise Console 5.5.1).
4. If the server is running Windows Server 2008 or later, turn off User Account Control (UAC) and restart the server.
   You can turn UAC on again after you have completed the installation and downloaded your security software.

6.2 Install Sophos Enterprise Console

To install Sophos Enterprise Console:

1. Log on as an administrator:
   a) If the computer is in a domain, log on as a domain administrator.
   b) If the computer is in a workgroup, log on as a local administrator.
2. Go to the download web page that is specified in your registration/download e-mail.
3. Download the Sophos Enterprise Console installer package.
4. Double-click the downloaded package.
5. In the **Sophos Enterprise Console** dialog box, click Next. A wizard guides you through installation. You should do as follows:
   a) Accept the defaults wherever possible.
   b) In the **Components selection** dialog box, select all three components: Management Server, Management Console, and Database.
6. When installation is complete, you may be prompted to restart. Click Yes or Finish.

Important
When you log back on (or restart) for the first time after installation, cancel the Download Security Software Wizard that appears as you need to modify configuration and registry values before downloading the security software.

If you used Remote Desktop to install Sophos Enterprise Console, the console does not open automatically.

For more information on installation and setting up policies, see the *Sophos Enterprise Console Quick Startup Guide* and *Sophos Enterprise Console Policy Setup Guide*.

7 Modify the configuration file

In the Sophos Enterprise Console Server:

1. Browse to the SUMInstaller folder.

Windows version	Default location
32-bit	C:\Program Files\Sophos\Enterprise Console\SUMInstaller
64-bit	C:\Program Files (x86)\Sophos\Enterprise Console\SUMInstaller

2. Locate the file MRinit.conf and edit the values for MRParentAddress and ParentRouterAddress.

   The MRParentAddress is used by the Sophos DMZ Server to connect to the Sophos Enterprise Console Server, and the ParentRouterAddress is used by the client computers to connect to the Sophos DMZ Server.

   Default value example:

```
"MRParentAddress"="sophos-console.abc.sophos,sophos-console"
"ParentRouterAddress"="sophos-console.abc.sophos,sophos-console"
```

   Modified content example:

   Include an externally accessible IP address and the local NetBIOS name for the Sophos Enterprise Console Server and the Sophos DMZ Server.

```
"MRParentAddress"="192.168.0.10, sophos-console.msp.com, sophos-
console"
"ParentRouterAddress"="sophos-dmz,sophos-dmz.msp.com"
```

   Save the file and close it. For an example of the modified MRinit.conf file, see Appendix: MRinit.conf file contents (page 29).

8 Download security software from Sophos

When you log back on (or restart) for the first time after installation, Sophos Enterprise Console opens automatically and runs a wizard to select and download endpoint security software.

If you used Remote Desktop to install Sophos Enterprise Console, the console does not open automatically; open it from the Start menu.

As the wizard runs:

1. On the Sophos Download Account Details page, enter your Sophos license schedule user name and password. If you access the Internet via a proxy server, select the Access Sophos via a proxy server checkbox and enter your proxy settings.
2. On the Platform selection page, select only the platforms you need to protect now.

   When you click Next, Sophos Enterprise Console begins downloading your software.

   Note
   You can add other platforms later by modifying your software subscription in Update Manager view.

3. On the **Downloading Software** page, downloading progress is displayed. Click **Next** at any time.
4. On the **Import computers from Active Directory** page, if you wish to protect your own computers on your LAN with Sophos security software and have the appropriate license, you may select **Set up groups for your computers**.

This creates a shared installation folder on your Sophos Enterprise Console Server, which contains installable versions of Sophos endpoint software for each operating system you choose to protect. It is shared as `\\<SEC-Server>\SophosUpdate\CIDs`. The share root is located at the following location:

Windows Server	Default location
2003	C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager \Update Manager\CIDs\
2008, 2008 R2, 2012, 2012 R2, 2016	C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

The installation and update files for Sophos Endpoint Security and Control for Windows are located in the subdirectory `\S000\SAVSCFXP\`.

Note
You can view the CID path for each platform from Sophos Enterprise Console: On the **View** menu, click **Bootstrap Locations**.

If you turned off User Account Control before installation, you can now turn it on again.

9 Publish customer update folders

When you install the Update Manager a shared 'SophosUpdate' folder is automatically created at the following location on the Sophos DMZ Server `\\<sophos-dmz.msp.com>\SophosUpdate`. This shared folder must be accessible by http so customers' computers can update from it.

1. Go to the Sophos Enterprise Console Server and open Sophos Enterprise Console.
2. In Sophos Enterprise Console, select the Update Managers view. Find and right-click the child Sophos Update Manager on your Sophos DMZ Server.
3. From **View/Edit configuration** select **Subscriptions** and ensure that the recommended package is subscribed to `\\<sophos-dmz.msp.com>\SophosUpdate`
   The Sophos Enterprise Console Server will communicate with the Sophos DMZ Server and build a new shared folder in `SophosUpdate`. This may take up to 15 minutes.
4. On the Sophos DMZ Server create an account, *sophosupd* with a complex password and read-only access to `SophosUpdate`.
5. Install and configure Microsoft IIS on the Sophos DMZ Server and secure it appropriately.
6. In IIS, create a virtual directory called `SophosUpdate`, which shares `\\<sophos-dmz.msp.com>\SophosUpdate`, assigning the new account *sophosupd* rights.

   If you use a localpath instead of a UNC, the default path to the CID is:

Windows Server	Default location
2003	C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\
2008, 2008 R2, 2012, 2012 R2, 2016	C:\ProgramData\Sophos\Update Manager\Update Manager\

7. Configure MIME types. For testing purposes, you can add .* as a MIME type.

   For more information on how to create a Web CID and configure MIME types, see knowledgebase article 38238.

Note
HTTPS is not supported for client updating. We recommend that you use NTLM (Integrated Windows authentication) or Digest authentication to ensure credentials are secure. These settings can be configured in IIS, and the clients will automatically use the most secure option available to them.

10 Configuring your Sophos Enterprise Console Server to manage customers

After you download the security software you must configure your Sophos Enterprise Console Server to manage the customers and their computers.

10.1 Create groups

You organise computers by creating groups in Sophos Enterprise Console. We recommend you create at least one group for yourself, the MSP, and at least one group for each customer. If your customers have systems that require distinct policies, sub groups can be created inside customer groups, for example "Servers" and "Desktops". Each group may be set to comply with a distinct set of policies, although in practice many groups will likely use the same policies. Dividing managed endpoints into groups like this enables you to change a particular security policy for one customer without affecting other customers', or your own endpoints.

To create a new group for computers:

1. In the **Endpoints** view, in the **Groups** pane (on the left-hand side of the console), select where you want to create the group.
   Click the computer name at the top if you want to create a new top-level group. Click an existing group if you want to create a subgroup.
2. On the toolbar, click the **Create group** icon.
   A “New Group” is added to the list, with its name highlighted.
3. Type a name for the group.
   Policies are applied to the new group automatically. You can edit these policies, or apply different policies.

   If the new group is a subgroup, it initially uses the same settings as the group it is within.

For your own computers, you can import groups from Microsoft Active Directory.

For more information on setting up groups, see the *Sophos Enterprise Console Help* and knowledgebase article 63155.

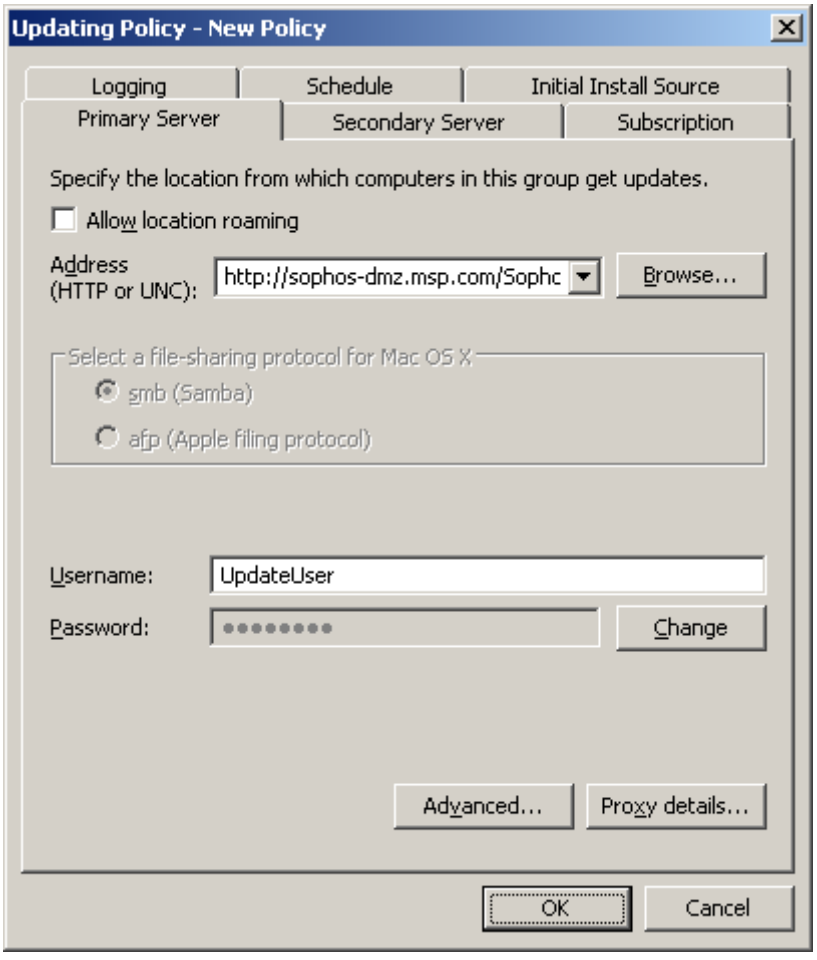
10.2 Create updating policy

You must create a new updating policy and configure it to use the HTTP address you set up in IIS earlier (Publish customer update folders (page 13)).

To create a new updating policy:

1. In the **Policies** pane, right-click on **Updating** and select **Create Policy**.
   Enter a policy name.
2. Double-click the policy name. In the **Updating Policy** dialog box, on the **Primary Server** tab, enter the address and credentials that will be used to access the server. The **Address** should be a fully qualified domain name or IP address (e.g. http://sophos-dmz.msp.com/SophosUpdate or http://1.1.1.1/SophosUpdate)

For **Username** and **Password**, enter the account credentials that will be used by clients to download updates. We recommend using a unique account per customer and having read-only permission.



Change other details, if appropriate and click **OK** to close the Updating Policy dialog box.

3. In the **Groups** pane, select a group to use the updating policy you configured by dragging the policy onto the group, or right-click the group, click on **View/Edit Group Policy Details** and then select the new policy from the drop-down list for Updating.
   Repeat this step for each group that you want the updating policy to be applied.

11 Verify your Sophos Enterprise Console Server configuration

Your Sophos Enterprise Console server configuration is now complete. To verify if the settings are appropriate, we recommend that you perform the tests below:

1. From the Sophos Enterprise Console Server, ensure you can connect to port 8192 using the fully qualified domain name (FQDN) of the server itself. You should receive a response that starts with "IOR".

   You can do this using a tool such as Telnet. For example, in the command prompt window, type `telnet sec-server.msp.com 8192`.

   If it does not work, then try using “localhost” in place of the FQDN to determine if it is a DNS/IP routing issue.
2. From an external client, repeat the above step to verify if the server is externally accessible.
3. Verify if the management system is configured with the FQDN. To do this:

   a) On your Sophos Enterprise Console Server, open the Registry Editor.
   To open click Start, Run, type `regedit` and then click OK.

   b) Navigate to the registry key `HKEY_LOCAL_MACHINE\SOFTWARE`.

   c) Right-click `SOFTWARE` and click Find.

   d) In Find what enter the FQDN of the SEC Server.

   e) After you find an instance, press F3 on your keyboard to search again to find another instance.

   Note
   You should have two instances of the FQDN name.

   Once you ensure you have two instances, close the **Registry Editor** window.
4. From an external client, check if you can connect to IIS on port 80 using the FQDN through a web browser. Navigate through the folder structure (or if directory listing is disabled, then specify paths derived from browsing the local directory) to ensure you can download files.
   For example, download a .pem file as it is not in the default list of IIS MIME types. With default initial settings, the path to download .pem file will be:

   http://<sec-console.msp.com>/SophosUpdate/CIDs/s000/SAVSCFXP/cac.pem

After you verify the above steps, you can continue to protect your Sophos Enterprise Console Server.

12 Protect your Sophos Enterprise Console Server

As a test, we recommend you protect your SEC server.

1. Install Sophos Endpoint Security and Control. To do this, from the computer to be protected, run setup from the CID path listed above at the end of Download security software from Sophos (page 12).
2. Confirm the installation is successful.
   To verify this, open Enterprise Console. In the Status tab, the Up to date column displays yes.

For more information on installing Sophos Endpoint Security and Control, see the *Sophos Endpoint Security and Control upgrade guide*.

13 Creating an installation package

13.1 About the Deployment Packager tool

You can install Sophos Endpoint Security and Control (SESC) on client endpoints by using the Deployment Packager tool, available on the Sophos website. The Deployment Packager creates a single self-extracting archive file from a set of Sophos endpoint setup files, for installing Sophos Endpoint Security and Control on Windows endpoints. The packaged file includes configuration options such as silent/interactive installation, installation package choices and setup parameters, update path/credentials and endpoint group membership.

Packages created with the Deployment Packager always attempt to remove other potentially-clashing protection software when installed.

It may be necessary for you to produce several packages, each meeting the requirements of different endpoint types.

You can run the Deployment Packager tool through either its graphical user interface (GUI) or command-line interface (CLI).

- The GUI is easier for one-off deployments.
- The CLI is more versatile for repeated deployments.

  A string to invoke the command line version with options can be stored in a text file, or regularly run from a scheduled batch file, ensuring that the installation packages are always up-to-date. So, if you are managing large numbers of computers where there is a need for frequent installation on endpoints, then the CLI is preferable.

Instructions for using the Deployment Packager via the command line can be found in Create a protection package using the CLI (page 27).

System requirements

The minimum requirements to run the Deployment Packager tool are as follows:

- Windows operating systems: see knowledgebase article 118635
- Disk space: 1 GB
- Memory: 1 GB
- Processor: 2 GHz Pentium or equivalent

You should also be aware of system requirements for the packaged endpoint components. See knowledgebase article 118620.

13.2 Create a protection package using the GUI

1. To create a protection package, run `DeploymentPackager.exe`.
   The **Sophos Deployment Packager** dialog box is displayed.

2. In **Source folder**, specify the location of the central installation directory containing the endpoint software installation files. This may be a UNC path or a local folder.

3. Select from the following:
   - **Remote Management System (RMS)**

     This installs and enables the Sophos Remote Management System, which allows Sophos Enterprise Console to control Sophos Endpoint Security and Control. For Managed systems you must enable this component.

     Note
     When you select this option, endpoints obtain their updating path and credentials from Enterprise Console through RMS.

   - **Exploit Prevention**

     This installs Sophos Exploit Prevention.

   - **Firewall**

     This installs the Sophos Client Firewall.

     Note
     If you want to install this option, check endpoint system requirements at www.sophos.com/en-us/products/all-system-requirements.aspx.

   - **Patch**

     This installs Sophos Patch Agent. You must also enter the address where the Management server is installed under **Management Server URL**. The address must be a fully qualified domain name. Example: http://<server name>.

     If you select this option, you can choose the **Operating system type**.

   - **NTP**

     This installs and enables Sophos Network Threat Protection (NTP).

   - In **Include selected components** do one of the following:

     To include the selected components in the deployment package, click **In the package**.

     To download selected components from the update source, click **Configure AutoUpdate to download components**.

     The endpoint installer is unable to use a proxy server. If the update location is accessed through a proxy server, then the required endpoint components must be included in the package.

   If you select **Remote Management System (RMS)** and then click **In the package** in **Include selected components**, the updating details are obtained from Sophos Enterprise Console.

   Sophos System Protection and Sophos Endpoint Defense packages will be automatically added to the generated package (if they are part of the licensed packages) as they are not optional components.
4. In **Operating system type**, choose which operating system type to package. This option is only applicable if Patch is being installed from the deployment package. If you choose either **32-bit** or **64-bit**, the package can be installed only on specific 32-bit or 64-bit operating systems. If you choose **32-bit and 64-bit**, the package can be installed on both 32 and 64-bit operating systems, but the package size will be large.
5. In **Installation type**, select how the installation program will run on endpoint computers.

- Select Silent: the program runs without any user interaction. The installation progress is not displayed on the endpoint computer.
- Select Non-interactive: the program runs without any user interaction. The installation progress is displayed on the endpoint computer.
- Select Interactive: the program runs with user interaction. The user can control the installation.

6. In **Additional setup parameters**, specify endpoint setup installation options. Always specify group membership using the -g option so that each installer is specific to and sets up endpoints to be members of existing groups.

   The packager does not check these options for errors.

   For further information, see www.sophos.com/en-us/support/knowledgebase/12570.aspx.
7. In Output package, specify the destination path for the output installer package. You can also specify an optional filename; if this is not supplied, the Deployment Packager will use a default filename.
8. In the Updating panel, for indirectly-managed endpoint packages or where remote management is enabled but not included in the package, enter the update path and credentials. You may set ":<port number>" after an HTTP URL; if unset, this defaults to 80.

   Note
   - Ensure all the components that are selected can be updated from the update location you specify (for example, Patch). If a different location is used for components, you can configure it as a secondary update location.
   - Credentials are obfuscated in the package; however, accounts set up for endpoints to read update server locations should always be as restrictive as possible, allowing only read-only access.
   - Endpoints will attempt to use their system proxy settings only if set using the environmental variables http_proxy or all_proxy. Proxy settings in Windows Control Panel Internet Options or Internet Explorer are ignored. _proxy variable values take the format _proxy=[protocol://][user:password@]host[:port], for example http_proxy=http://user:password@proxy:8080

9. Click Build Package to build the self-extracting archive.

14 Verify your installation package

After the installation package has been created, we recommend you verify if you are able to install, update, and manage computers using the package that has been created.

To do this:

1. Identify a standalone computer that is part of your local network to be used as an endpoint computer.
2. Deploy the installation package to the endpoint computer.
3. Ensure the installation is successful and check the following functionalities:
    - Updating: To verify if the endpoint computer is downloading updates from Sophos Enterprise Console, in the endpoint computer, right-click the Sophos protection system tray icon and click **Update now**. The endpoint computer should be able to download updates from Sophos Enterprise Console.
    - Management: To verify if Sophos Enterprise Console is managing the endpoint. In Sophos Enterprise Console window, ensure the Sophos protection icon besides the endpoint is not grayed out, and it does not have a red cross or a yellow exclamation mark.

    After verifying the installation package, you can deploy it to the customers' computers.

15 Distribute package to customer's computers

Use your RMM system to distribute and run the installer package(s) on the customer's computers. The details of how to do this will depend on which system you use, and are beyond the scope of this guide.

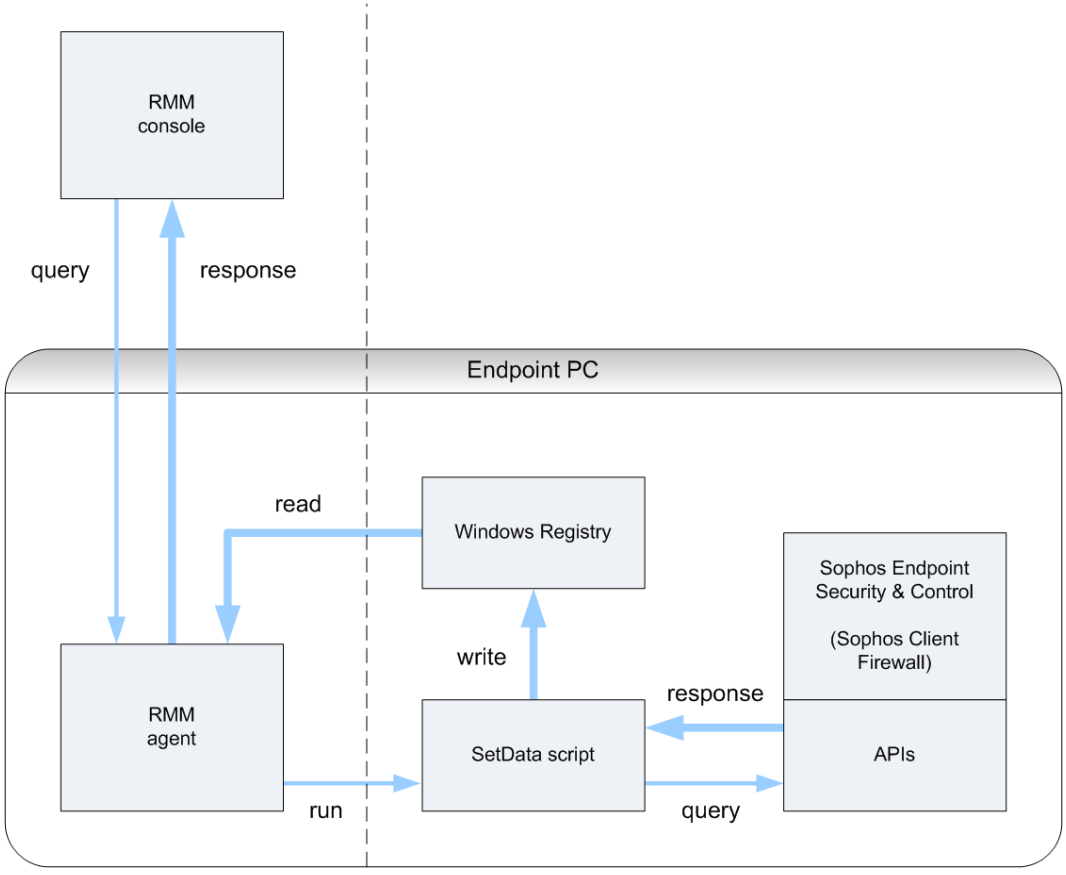
16 Monitoring endpoint security

Once Sophos Endpoint Security and Control is installed on endpoints, you manage groups, policies and other settings via Sophos Enterprise Console, which provides complete status reporting of endpoints. For more details, see the Sophos Enterprise Console *Help* and *Policy Setup guide*.

Most MSPs will use their existing RMM system for routine status monitoring, and only use Sophos Enterprise Console for group/policy configuration, and in the event of a security problem, for detailed endpoint status analysis. Your RMM system is used as the primary method for management and monitoring of all endpoint software (not just Sophos Endpoint Security and Control).

This section explains how to use the SetData script to provide the most important endpoint status information to your RMM system.

The diagram below shows how the RMM system uses the SetData script to know endpoint status.



16.1 About the SetData script

The SetData script, `MSPSetData.vbs`, may be run from Windows or called from the command line or a batch file. MSPSetData:

- reads parameters from Sophos Endpoint Security and Control,
- writes the Sophos Endpoint Security and Control parameters to the endpoint Windows registry,
- must be run with LOCAL_SYSTEM administrator privileges,

- must be run in a 32-bit environment. For 64-bit versions of Windows, the 32-bit version of the command prompt is available at `%WINDIR%\SysWOW64\cmd.exe`.

To run the SetData script in command line mode, use the following format:

```
MSPSetData <base_key> [logFileName]
```

Where `<base_key>` is the base key within HKEY_LOCAL_MACHINE to write the endpoint parameters and `[logFileName]` is an optional path to a log file.

Note
If you call SetData with the logFileName parameter, it appends log data to any existing log file. If you call SetData frequently, this can result in a very large log file.

Example:

```
MSPSetData "SOFTWARE\Sophos\ESCStatus" "c:\MSPSetDataLog.txt"
```

This will write all parameters within `HKEY_LOCAL_MACHINE\SOFTWARE\Sophos\ESCStatus` and log to `c:\MSPSetDataLog.txt`.

16.2 About the endpoint parameters

The SetData script reads parameters from Sophos Endpoint Security and Control and Sophos Client Firewall, and writes them to the endpoint Windows registry as detailed below, under a configurable hive path root within `HKEY_LOCAL_MACHINE`.

If Sophos Endpoint Security and Control or Sophos Client Firewall are not present or not running, their REG_DWORD parameters are set to -1 and REG_SZ parameters to null.

If Sophos Endpoint Security and Control or Sophos Client Firewall are updating, all their REG_DWORD parameters except UpdateInProgress are set to -1 and all their REG_SZ parameters to null.

Parameters list

Registry hive path	Parameter/Key	Description	Type REG_
\SAVService\Status \Infected	ControlledAppDetected	0: No controlled application detected 1: Controlled application detected (& quarantined)	DWORD
	MalwareDetected	0: No malware detected 1: Malware detected & quarantined	
	PUADetected	0: No PUA detected 1: PUA detected	

Registry hive path	Parameter/Key	Description	Type REG_
	SuspiciousBehaviorDetected	0: No suspicious behavior detected 1: Endpoint exhibiting suspicious behavior	
	SuspiciousFileDetected	0: No suspicious files detected 1: Suspicious file detected	
\SAVService\Status \LastScan	SystemScan	Time/date of last scan(s) (epoch value) e.g. 1268337010	
	NormalScan		
	EnterpriseScan		
\SAVService\Status \Policy	AppControlComplies	0: Non-compliant with SEC policy 1: Compliant with SEC policy	
	SAVComplies		
	DataControlComplies		
	DevControlComplies		
\SAVService\Application	Managed	0: Independent 1: Managed by SEC	
\SAVService\Version	Data	SAV Virus data version e.g. 4.50G	SZ
	Major	SAV major version # e.g. 9	DWORD
	Minor	SAV minor version # e.g. 5	
	Extra	SAV version supplementary information e.g. beta	SZ
\SAVService\Status \Policy	OnAccessEnabled	0: On-access scanning disabled 1: On-access scanning enabled	DWORD
\SAVService\Update	UpdateInProgress	0: Not updating 1: Updating	
	IDECount	Number of Sophos virus identity files present	
	LastUpdated	Time/date of last update dd.mm.yyyy hh:mm:ss e.g. 02.03.2010 18:56:30	SZ

Registry hive path	Parameter/Key	Description	Type REG_
\Sophos Client Firewall \Config	ActiveLocation	1: Primary location 2: Secondary location	DWORD
	DetectedLocation		
	Disabled	0: Operational 1: Passing all traffic	
	Mode	0: Interactive 1: Block unknown 2: Pass unknown	
\Sophos Client Firewall \Update	UpdateInProgress	0: Not updating 1: Updating	
\Sophos Client Firewall \Version	FirewallVersion	Firewall version # e.g. 2.0	SZ

16.3 Using your RMM to read endpoint parameters

These instructions are generic, since it depends on your specific implementation of remote management.

1. Copy the SetData script to managed endpoint computers.
2. Configure your RMM console to run the script periodically (for example once every four hours), read the endpoint parameter registry values and display them as required with alerts for critical conditions.

You can run the script manually to check that it is working properly and check the values written to the endpoint Windows registry using regedit.

17 Create a protection package using the CLI

Before using this section, read Create a protection package using the GUI (page 18).

To run the Deployment Packager in command line mode, use the following format as a minimum:

```
DeploymentPackager.exe -cli -mng yes -cidpath <CIDpath> -sfxpath <SFXpath>
-crt R
```

where <CIDpath> is the path to the relevant central installation directory and <SFXpath> is the path of the output package. **-crt R** automatically removes third-party protection software.

The packager returns a value of zero when run successfully and non-zero for an error condition, together with a message to standard error method (stderr).

Command-line options

You can also use other command line qualifiers, as listed below.

-mng yes

Enable Remote Management.

-mngcfg

Specify path to custom Remote Management configuration files.

-scf

Install Sophos Client Firewall.

-ntp

Install Sophos Network Threat Protection.

-hmpa

Install Sophos Exploit Prevention.

-patch <Management Server URL>

Install Sophos Patch Agent with the Management Server address. The address should be a fullyqualified domain name. Example: http://<server name>.

-sauonly

Include Create a protection package using the GUI (page 18) only (chosen remote management, firewall, NTP and SSP components are downloaded from the update source). If this option is not selected, chosen components are included in the package.

-arch <32bit, 64bit>

Specify the architecture of the package you want to create, either 32-bit or 64-bit.

Note
This option is only applicable if Patch is being installed from packaged CID. If you choose **32-bit** or **64-bit** the package can be installed only on specific 32-bit or 64-bit operating systems. If you do not specify any architecture, a single package is created which can be installed on both 32 and 64-bit operating systems, but the package size will be large.

-updp <update_path>

Updating path.

-user <username>

-pwd <password>

Username and password. The packager obfuscates these in the package. However, if you are saving a Deployment Packager command line with clear username and password in a text or batch file, ensure that it is secure.

-opwd <obfuscated_password>

Obfuscated password. For information on how to obfuscate passwords, see Knowledge Base article *Obfuscating the username and password* at www.sophos.com/en-us/support/knowledgebase/13094.aspx.

-s

Silent installation.

-ni

Non-interactive installation.

Other options

Any other options are packaged to be run with the installer setup file.

18 Appendix: MRinit.conf file contents

Following is an example of the MRinit.conf file after modification:

```
[Config]
"NotifyRouterUpdate"="EM"
"ClientIIOPPort"=dword:00002001
"ClientSSLPort"=dword:00002002
"ClientIORPort"=dword:00002000
"IORSenderPort"=dword:00002000
"DelegatedManagerCertIdentityKey"="NOChhZvtx8i59YN4OVkvtaOYHsA="
"ManagedAppCertIdentityKey"="KeDbiqpDTPaiKSPwXhiS/FxPMaE="
"RouterCertIdentityKey"="+Z3KILDInN7HZn0jbZu4zsLSyfg="
"ServiceArgs"=""
"MRParentAddress"="192.168.0.10, sophos-console.msp.com, sophos-console"
"ParentRouterAddress"="sophos-dmz,sophos-dmz.msp.com"
```

19 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the Sophos Community at community.sophos.com/ and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at www.sophos.com/en-us/support.aspx.
- Download the product documentation at www.sophos.com/en-us/support/documentation.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

20 Legal notices

ACE™, TAO™, CIAO™, DAnCE™, and CoSMIC™

Since DOC software obtains time/date and calendaring information from operating systems users will not be affected by the new DST rules as long as they upgrade their operating systems accordingly.

The names ACE™, TAO™, CIAO™, DAnCE™, CoSMIC™, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington University, UC Irvine, or Vanderbilt University. This license grants no permission to call products or services derived from this source ACE™, TAO™, CIAO™, DAnCE™, or CoSMIC™, nor does it grant permission for the name Washington University, UC Irvine, or Vanderbilt University to appear in their names.

If you have any suggestions, additions, comments, or questions, please let me know.

Douglas C. Schmidt

Apache

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Apache License. A copy of the license agreement for any such included software can be found at http://www.apache.org/licenses/LICENSE-2.0

Boost Software License

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software, unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at https://www.sophos.com/en-us/support/contact-support.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

ConvertUTF

Loki

OpenSSL Cryptography and SSL/TLS Toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape’s SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

WilsonORMapper

Copyright © 2007, Paul Wilson

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.