



Sophos Endpoint Security and Control: Best Practice Guide for Planning Your Installation

CURRENT FOR VERSION 9.0

In this Guide

What to expect from this document	2
What software is installed as part of Endpoint Security and Control?	2
What features require planning?	2
General installation planning considerations.....	3
Main installation scenarios	4
Single site network.....	4
WAN	6
No server	8
No suitable Windows computer.....	9
No Enterprise Console.....	10
Additional configurations	11
Roaming users connecting via VPN	11
Air gapped network.....	12
Remote workers, no VPN access.....	13
Home users (extended licence).....	14

What to expect from this document

You're a network administrator who will be installing Endpoint Security and Control on your company network. This document is designed to answer your preliminary questions and suggest the ways that Endpoint Security and Control can be best adapted for your network.

It begins with a few general questions to set the context and then describes more specific network scenarios.

What software is installed as part of Endpoint Security and Control?

When we say installation of Endpoint Security and Control, we mean that you will be installing:

- One or two admin/management consoles: Enterprise Console and NAC Manager
- Anti-virus and other software on your endpoint computers: Endpoint Security and Control (Sophos Anti-Virus, Client Firewall and NAC/Compliance Agent) and some extra software to handle updates, messaging, etc.
- A management database that stores information about the configuration of your endpoint computers
- A management server (and management service) that handle communications between the console, the database, and the endpoint computers

What features require planning?

Installation locations and methods

The location of the management database, management server and management consoles can be customized to suit your needs. For instance you could install:

- all components on the same server – this is referred to a 'standard' or 'default' installation throughout our documentation
- each component on a separate server
- only the database(s) on a separate server, possibly on a dedicated SQL cluster
- Enterprise Console on your local computer and the other components on a separate server
- the whole product on VMWare to be managed from within a virtual machine
- all components on a server in a server room and you use Remote Desktop sessions to use Enterprise Console from your local computer

We don't describe each of these installation configurations in this document, but we do explain generally how to install the management software and the software on your endpoint computers in each of the network configuration scenarios that follow.

Other features

Some features in the management console require a little foreplanning as well. The considerations that go into each are described in this document for each network configuration scenario:

- **Update Manager.** This component creates a structure for updating the anti-virus (and other) software on your endpoint computers. It will automatically create a central location for your network to update from, but you can choose to create more update locations as you see fit. Update locations can either be set up as a UNC path or a web folder.
- **Role-based Administration.** This is an optional feature that allows you to subdivide the management of your network so that other users can monitor the network's health and perform actions.

General installation planning considerations

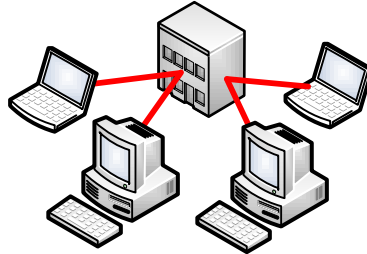
In general, if you consider the following items before you read this document, you'll get the most out of this guide:

1. Think about the numbers. The number of end users you have will determine how many sub-estates and update locations you should set up.
2. Think about your network configuration. Your network configuration will determine how you should install the software on your client computers, how you will distribute updates, and how many sub-estates you should set up.
3. Think about who will manage your network. The number of IT staff who will monitor and respond to malware alerts and firewall events will determine the number of sub-estates you should set up.
4. Think about how you would like to deploy updates. There are countless ways of doing this. Think about whether you would want everyone on the network downloading from one shared folder, or whether you want every department to have their own update location with a failover location as well.

The rest of this document describes various deployment scenarios (like WANs, remote users, or networks with no servers) that we have anticipated.

Main installation scenarios

Single site network



Installation

Management software

Install the Enterprise Console/NAC Manager on one server (to be used to manage the network) or install the database(s) on a separate server if you have a large network. For more information on installing the Enterprise Console database on a SQL cluster, please see [Installing the Enterprise Console version 4 database in a clustered SQL Server environment](#).

If you use Active Directory, use it to import containers (OUs) at first. Then, once you've adjusted your groups and created the subgroups that you need, synchronize with Active Directory to import the computers.

If your network has more than 10,000 computers (5,000 if you use Windows 2008), you should set up at least one message relay to reduce the load of communications to and from the management server. See [Enterprise Console: configuring message relay computers](#) for more information.

Another way of offsetting the communications load on the server running Enterprise Console is by using two separate NIC cards on the server running Enterprise Console – one for update traffic and the other for agent traffic. See [Using a separate network interface card \(NIC\) for updating and other communications between Enterprise Console and the endpoints](#).

Client software

You have many options for deploying Endpoint Security and Control to your client computers:

- Deploy directly from Enterprise Console, as described in the [Quick Startup Guide](#) (for smaller networks) or the [Advanced Startup Guide](#) (for larger networks)
- Use SMS/SCCM (Microsoft recommends that you use SCCM to distribute software when you have 250 or more client computers in your network). For detailed instructions, please see [Using SCCM 2007 \(SMS\) to deploy Endpoint Security and Control \(Sophos Anti-Virus\)](#).
- Create a script to invoke special features when running the installation with setup.exe. You can then use a Group Policy Object to deploy the script and installation file.

Role-based administration

Consider whether you would like to use sub-estates to divide up the day-to-day management of your network. Consider who will have what roles and install Enterprise Console on their computers when you are ready.

We recommend that you have at least one sub-estate at each of your locations, with more than one IT person assigned to each one. That way, they can manage two networks when one person is off sick or on vacation.

Updating structure

There are many considerations that go into planning an update structure. When planning, remember that the update manager pushes the files to each share in turn, so the number of shares should be tailored to fit your network bandwidth. Also remember that you shouldn't put a share on a computer that may go into standby or otherwise be unavailable for long periods of time.

How big is your network?

On a network with fewer than 1,000 computers, you can install a single update manager and create one or more update locations for your client computers to download updates from.

On a network of 1,000 or more computers, you'll want to design your update structure to take advantage of the best network architecture and the most effective servers. If you use a UNC path for your update location, it should be used by a maximum of 1,000 computers, unless it is on a dedicated file server. If you set up a web location for updating, it can handle somewhere between 5,000 and 10,000 computers updating from it.

You could also set up additional update managers to spread the load. They could either update from the primary update manager or directly from Sophos. This kind of scenario could also be used for designing failovers. For detailed instructions about installing an additional update manager, please see section 6 of the [Advanced Startup Guide](#).

As a general rule, you should install an additional update manager for each 25,000 client computers on your network.

What computers are on your network?

Your update shares can publish software for all the different supported operating systems.

Consider whether you may want more than one update location for a specific operating system. For example, you might want half your Windows 2000+ operating systems to use one update location and the other half to use another, and use a separate server for Mac OS X and Linux updates.

You can also download software for UNIX and Netware and set up a share on any server for these computers to update from. This is described in sections 13-16 of the [Advanced Startup Guide](#).

Do you have roaming or remote users connecting to your network?

We've tried to illustrate the most common 'additional network configuration' scenarios in the rest of this document. Refer to the type of installation that applies to your situation to learn how to install Endpoint Security and Control on the client computers and how to structure your updating structure to support them.

WAN



Please note: The following points apply to both single-domain and multiple-domain (or workgroup) networks.

Choose the scenario that best applies to your situation.

There is an administrator at each site who will administer their own site independently.

Installation

Install Endpoint Security and Control (Enterprise Console and NAC Manager) at each site and use Active Directory to sync with the local domain only.

Role-based administration

If there is only one person responsible for checking the network at each site, set up the other site administrator with the right to monitor alerts and events to ensure that there is coverage to deal with malware outbreaks and other security events in the event that the local admin is not present.

If there are several people at each site who can check the network, set them up with roles and sub-estates as required.

Updating structure

If you desire, you could configure the update manager on site B to download its updates from site A, but you could also have it download its updates directly from Sophos.

Read the advice for the 'Standard' scenario described above to see what other issues you should consider before installing Endpoint Security and Control at each site.

There is admin or helpdesk staff who will administer groups across the two domains/sites

OR

There is one administrator who will administer both domains/sites from site A

Installation

Install Endpoint Security and Control (Enterprise Console/NAC Manager) at site A and use RDP or TS to manage the computers at site B. If you have staff at site B who should be allowed to perform certain tasks, install Enterprise Console only at site B.

If the sites are on different domains, remember that once you install Enterprise Console, you will need to [set it up for multiple domains](#).

Ensure that your web filtering equipment allows the following ports for Sophos communications:

Network: allow ports 137-139 and 445

Weblink: allow port 80

Role-based administration

This all depends on how the IT department is structured. If all the IT staff is on one site, you'd probably want to break down the network into sub-estates based on location. If there is IT staff at each site, you could divide each site into sub-estates as well. It's up to you.

Updating

Wherever possible, we recommend that you install an additional update manager in a remote location. There are a few reasons, but most important is the amount of bandwidth needed to update the shared folders on site B and the danger that the shares would be incomplete if the link went down.

If there is a server or other suitable Windows computer¹ on site B which could be used to distribute updates

Install an Update Manager at site B to update the local computers. This update manager could either download its updates from site A or directly from Sophos.

If you have a firewall between your sites, you'll have to update via HTTP. Set up a web folder at site A so that the site B computers can get their updates.

If there is no server or suitable Windows computer¹ on site B

Use the update manager at site A to create a share for site B. This shared folder could be located at site A, or at site B if bandwidth is a concern. If the link would be too slow to download updates from site A once an hour, consider creating a web folder for the site B computers to update from.

No matter what you choose as the primary source for updates, ensure that the secondary updating source in the updating policy for Site B computers point to Sophos in case the link between the two sites goes down or the web location is unavailable.

¹ Suitable computers are those running Windows NT4 SP6a/2000/XP/2003/Vista/ Windows 7/2008

No server



Installation

If you have a small network with no server (ten or fewer computers), you can still download and use Enterprise Console to manage your network as long as you have a computer running Windows 2000, XP or Vista.

Follow the advice for the 'Single site network' scenario, described above.

Alternatively, if all of your computers are connected to the Internet, you could install the standalone version of Endpoint Security and Control on those computers and they would all update directly from Sophos.

Role-based administration

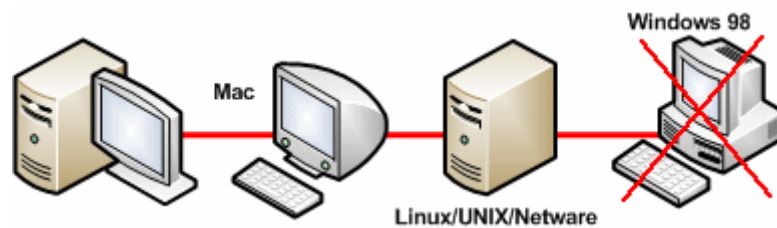
If you install Enterprise Console on one of your computers, you could set up another user to monitor your network when you are away from the office.

Updating

If you install Enterprise Console on one of your computers, use the update manager to set up an update system with a single share.

If you install the standalone version of Endpoint Security and Control on all of your computers, they will update directly from Sophos.

No suitable Windows computer



If you don't have a Windows Server, or a suitable Windows computer running Windows 2000, XP or Vista, you will have to download Sophos Anti-Virus for your non-Windows computers and they will update separately.

Due to recent changes to the Sophos databanks, Windows 95/98/NT computers are no longer supported in this scenario, as they cannot download updates directly from the Sophos databanks. For more information, please see our [software lifecycle pages](#).

Installation

Download and install:

- [Sophos Anti-Virus for Mac OS X](#)
- [Sophos Anti-Virus for Linux](#)

Role-based Administration

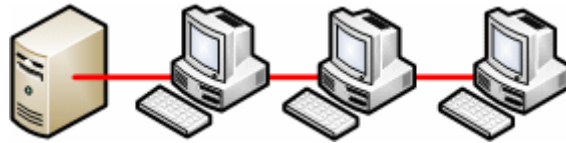
Does not apply as Enterprise Console can only be run on a Windows server or suitable workstation.

Updating

Sophos Anti-Virus for Mac OS X has its own updating mechanism, called [Sophos Update Manager](#), that can be used to update your Mac computers.

Sophos Anti-Virus for Linux can be updated by one computer and the cache folder can be shared with the other Linux computers in your network.

No Enterprise Console



Please note that this scenario is not supported. You should make all efforts to use Enterprise Console on your network. Of course, you could always use one of our Small Business suites if you have a small network and no dedicated server.

Installation

Download the standalone installer and install Endpoint Security and Control on each computer individually. Each computer would then update directly from Sophos.

Role-based administration

Not applicable, as these computers are not managed and Enterprise Console is not being used.

Updating

The computers would update directly from Sophos.

Additional configurations

Roaming users connecting via VPN



Installation

Follow the advice for the 'Standard' scenario for recommendations for installing Enterprise Console on the management server.

For your roaming users, because the computers will connect to the network via VPN, you should deploy Endpoint Security and Control software to these computers from Enterprise Console. When they next connect, they will download and install the security software.

Role-based administration

Your roaming users can be a bit of a concern. What are they doing online? There might be some merit in setting up one sub-estate for roaming users so that one person can keep tabs on them.

Updating

Ensure that the updating policies for these computers have Sophos set up as a secondary source for updates, in case the user can't connect to your network while they're away from the office. Alternatively, you may also consider creating a web location for them to update from, so that they can update their security software even if they can't connect to your network.

Air gapped network



Installation

Follow the advice for 'Standard' scenario for recommendations for installing Enterprise Console on the management server on the outside network.

For your air-gapped network, you have two options:

1. Install Enterprise Console and an update manager and deploy to the client computers from the management server in the air-gapped network.
2. Install Endpoint Security and Control on each of the computers individually and have them update from a shared folder copied from the outside network. You won't be able to manage the computers on the air-gapped network, nor would you be able to take advantage of all the features of Endpoint Security and Control, because Application Control, Device Control and Data Control are all configured using Enterprise Console.

Role-based administration

You will have separate installations of Enterprise Console on the two networks, so you won't be able to monitor both networks from one Enterprise Console. You could break your air-gapped network into sub-estates, if it's big enough. As with any network, you'd probably want to define at least one extra role to monitor the network when the admin is busy.

Updating

When you configure the update manager in the air-gapped network, ensure that it uses a folder on the management server, or a removable device that you manually update with data from the outside network as its update source.

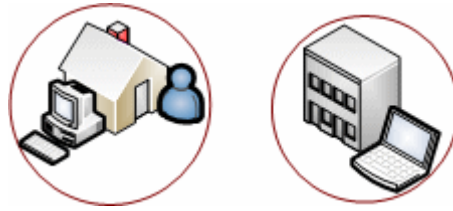
For detailed instructions on setting up an air gapped network, please see:

[EM Library: installing and updating on a secure network with an air gap](#) (for Enterprise Console 3.x)

[Installing and configuring an air gap using Enterprise Console 4's Update Manager](#) (for Enterprise Console 4)

[Sophos Update Manager: Air Gap Networks on a MAC Environment](#) (for Mac OS X environments)

Remote workers, no VPN access



Installation

First, you could download the standalone installer and install Endpoint Security and Control on each computer individually. The users would then update directly from Sophos.

Or, you could create a self-extracting .exe for your users to install themselves. These users would update from a Web location that you configure and update.

Role-based administration

Not applicable, as these computers are not managed.

Updating

Either the computers would update directly from Sophos or they would update from a web location that you configure.

Home users (extended licence)



Installation

The only supported installation for home users is a self-extracting .exe that you build for them. We do not permit home users to update from the Sophos databanks directly. You will have to create a web folder where your home users can download their updates.

Role-based Administration

Does not apply.

Updating

Create a web folder that will copy the updates from your update manager and allow you to distribute them to your employees' personal computers at home.

Please see our [Best Practice article about setting up home users](#) for more information.