Introduction to Centralized Management for the Symantec™ Gateway Security 400 Series
# Table of Contents

Symantec Gateway Security 400 Series appliances .......................................................... 1
Components of Symantec Gateway Security 400 Series centralized management .................. 2
Deployment considerations ................................................................................................. 4
  Direct SSL ....................................................................................................................... 4
  SSL over VPN ................................................................................................................. 5
  Authentication certificates .............................................................................................. 5
  Basic network settings ................................................................................................. 6
SESA installation overview ............................................................................................... 7
SESA administration ......................................................................................................... 7
Connecting the Symantec Gateway Security 400 Series to SESA ........................................ 8
  How to “join” a 400 Series appliance to SESA ............................................................. 9
Monitoring 400 Series appliances from SESA ............................................................... 9
  How to view events ....................................................................................................... 10
Alerts ................................................................................................................................. 10
  Defining alerts ............................................................................................................... 10
  How to configure an alert .............................................................................................. 11
Creating configurations on SESA for the 400 Series ...................................................... 12
  How to create new Policy and Location Settings ......................................................... 12
Best practices .................................................................................................................. 15
Reference ........................................................................................................................ 15
Symantec Gateway Security 400 Series appliances

Available in four models, 420, 440, 460, and 460R, the Symantec Gateway Security 400 Series is composed of integrated security appliances targeting the enterprise remote office/branch office (ROBO) sector. Each appliance includes a Security Gateway Management Interface (SGMI) Web interface, an easy-to-use set of management screens that allow configuration and operation of a powerful feature set for securing a typical small business network.

Feature highlights of all four models include:

- **Stateful inspection firewall**—Simple to configure for small sites, offering high performance. Up to five definable access groups for outbound rules, antivirus policy enforcement, and content filtering.

- **Antivirus policy enforcement for Symantec virus protection products**—Monitors local hosts and remote virtual private network (VPN) clients and will block their traffic and/or log a warning if they don’t have the appropriate antivirus software installed. Note: This feature is not currently compatible with Norton AntiVirus™ for consumers, but Symantec AntiVirus™ for Small Business, Symantec AntiVirus™ Corporate Edition, and Symantec™ Client Security are supported.

- **VPN gateway**—Configurable for site-to-site tunnels on the WAN or client-to-site tunnels (optional) on the LAN, wireless LAN (WLAN), or WAN. Uses hardware-accelerated AES, DES, and 3DES.

- **Optional high-speed 802.11g/b**—VPN-secured wireless access point—Using industry-standard IPsec, the wireless interface features easy-to-configure VPN authentication/encryption for maximum wireless security.

- **Intrusion detection system (IDS)/intrusion prevention system (IPS)**—Configurable to detect and prevent attacks from the wireless interface/LAN in addition to the WAN.

- **URL content filtering**—Static entries for two list types, Allow and Deny, of 100 URLs each.

- **LAN switch VPN authentication enforced on a per–physical port basis**—Turn any LAN port into a secured network port that requires VPN authentication and encryption.

- **Connection failover to backup**—Automatic failover and failback of ISP connections and VPN tunnels to the serial port (or second WAN ports on models 460 and 460R).

- **Unrestricted user licensing**—No user restrictions on six base security functions.

Every 400 Series model includes secure, policy-based, and scalable centralized management capabilities that enable administrators to centrally monitor, alert, report, and easily maintain policy-based configurations for thousands of the appliances. The centralized management capability gives the 400 Series greatly expanded capabilities compared with stand-alone monitoring and management. The 400 Series’ centralized logging and reporting functions also allow similar network events from other Symantec and supported third-party vendor products to be combined, making it easier for administrators to visualize the security status of the entire heterogeneous network.

Scope of this document

This document offers administrators a high-level overview of how to centrally manage 400 Series appliances; also included are deployment considerations and installation requirements. For more detailed information about deployment considerations, installation requirements, scenarios, and feature descriptions, see the reference section at the end of this document.
Components of Symantec Gateway Security 400 Series
centralized management

Symantec™ Enterprise Security Architecture (SESA™) version 2.0 consists of a set of core server applications that enable centralized management of the Symantec Gateway Security 400 Series. SESA uses XML over encrypted SSL links (with certificates) to allow scalable management and monitoring of thousands of appliances from a single administration console. As an open architecture, SESA can manage and monitor many different security devices and computer applications, both from Symantec and from third-party vendors that have incorporated support for SESA into their devices and software.

The SESA server application that performs the centralized management function is made up of three main components: SESA Manager, SESA Directory, and SESA DataStore.

- The SESA Manager contains the Java™ based administrator console (HTTPS human interface) and the SSL/XML network suite that allows SESA to communicate with the products that it manages.
- The SESA Directory handles the system and configuration policy management, as well as LDAP communication.
- The SESA DataStore is the database component used to store the property/value pairs that make up product configurations.

Figure 1. SESA architecture

Both the SESA Manager and SESA Directory are included in the SESA Foundation Pack version 2.0 software media (CD-ROM). Note that the 400 Series requires the IBM DB2 DataStore.

Depending on the scale of the management deployment, the three main SESA server components can be installed on a single server platform. For medium and large deployments, organizations typically install the SESA DataStore on separate server platforms or all three components on their own server platform. Symantec's sales team can help determine an organization's hardware requirements.
A fourth component that completes the architecture on the device side is the SESA Agent. Each device or computer communicating to the SESA Manager must have a SESA Agent installed. This agent handles the SSL/XML link to the SESA Manager and may perform one or more functions, including:

- Send product events (logs) to SESA
- Send regular state information (product statistical data) at predefined intervals
- Accept and parse configuration updates that are distributed to the product from the SESA Manager

The SESA Agent for the 400 Series is contained in the unit’s firmware and can be configured in two ways (see figure 2):

1. For monitoring (sending log events and state information)
2. To accept configuration updates from the SESA Manager

![Figure 2. Configuring a Symantec Gateway Security 460 for full centralized monitoring and policy management](image)

Since SESA can manage many types of products from different vendors, a plug-in, called a SESA Integration Package (SIP), is needed for each type of product to be managed or monitored from the SESA application. This SIP adds product-specific configuration tabs, product IDs, event schemas, and predefined event reports to the SESA Manager.

The SIP for the 400 Series appliances is called the Symantec Event Manager and Advanced Manager for Security Gateways (Group 2). (Group 1 is for Symantec™ Gateway Security 5400 Series appliances and Symantec™ Enterprise Firewall 8.0 products.) Once the media pack containing the SIP is purchased (the SIP license is included with the purchase of each 400 Series appliance), the SIP can be installed into the SESA Manager and used to manage or monitor any number of 400 Series appliances.

To summarize, the following components enable centralized management of the Symantec Gateway Security 400 Series:

- **SESA Foundation Pack version 2.0 software media**—Contains the SESA Directory and SESA Manager components to be installed on server hardware.

- **Separate SESA 2.0 compatible database component, called the SESA DataStore**—SESA 2.0 is compatible with IBM DB2 (for Windows) or Oracle9i (for Solaris). Only IBM DB2 is supported for the Symantec Gateway Security 400 Series.

- **Symantec Event Manager and Advanced Manager for Security Gateways (Group 2)**—The plug-in, or SIP, for the SESA Manager that enables monitoring and policy management of the Symantec Gateway Security 400 Series appliances. The SIP is delivered on a CD-ROM in the media kit for this product.

- **A Symantec Gateway Security 400 Series appliance**—The appliance firmware contains a SESA Agent that sends event logs and statistical information, and accepts and parses configuration updates from a SESA Manager.

For more information about these components and requirements, contact a Symantec sales representative.
Deployment considerations

Before deploying 400 Series appliances that will be managed by SESA, administrators must first determine how their network resources will communicate and in what network scenarios they will manage the gateways. This will allow administrators to plan basic network configurations at the remote sites. It will also allow administrators to plan the network path that connects the SESA Agent in the 400 Series appliance to the SESA Manager. For example, administrators must decide whether to use direct SSL (the simplest method) or VPN tunnels with nested SSL communication to connect to SESA.

The SESA Manager can directly face the Internet, but Symantec recommends placing it behind a firewall gateway (such as the Symantec Gateway Security 5400 Series appliances). This enables security and deployment flexibility by allowing the addition of VPN-based management scenarios.

![Figure 3. Direct SSL management scenario](image)

**Direct SSL**

For 400 Series appliances used in simple gateway scenarios at home or in branch offices with only a few host PCs on the LAN/wireless LAN (WLAN) side, a direct SSL connection over the Internet to the SESA Manager can be used (see figure 3). Since SSL is capable of strong encryption and authentication methods, SESA management sessions over the Internet are secure and have robust security.

For each 400 Series appliance to be managed via direct SSL, a static IP address ISP account is needed. Since the 400 Series uses Network Address Translation (NAT), the direct SSL method cannot be used if there are other products managed by SESA behind the 400 Series branch gateway. Because these products would use private IP addresses, they would not be directly accessible by the SESA Manager over the Internet.

![Figure 4. SSL over VPN management scenario](image)
SSL over VPN

For offices with other products managed by SESA behind the branch office gateway, a VPN tunnel from the SESA Manager site to the branch site is required (see figure 4). An example is an office using multiple 400 Series appliances with the wireless access point (WAP) option used in a secure wireless infrastructure. A VPN tunnel enables “direct” access to these private IP addresses from the SESA Manager network.

The SSL over VPN method provides the following advantages for certain deployments:

- The more expensive static IP addresses are not required at branch sites since the 400 Series supports VPN tunnels using dynamic Domain Name System (DNS) (i.e., the branch site VPN endpoint is a domain name that is updated automatically with every IP address change from the ISP).

- With a Symantec Gateway Security 460 appliance with dual WAN ports, failover of VPN tunnels is supported (using dynamic DNS) to the working broadband connection. If the ISP link supporting the original session goes down, failover allows the management session to be maintained. Note: All 400 Series appliances support VPN tunnel failover to the serial backup port (analog or ISDN). The reduced bandwidth of this connection type limits management and event collection, but the connection type can be used for emergency uptime.

- VPN tunnels may already be required to enable other business requirements, such as resource sharing or main site firewall filtering of branch office traffic. Therefore, sending management traffic over the VPN can be complementary to this deployment topology.

A disadvantage of SSL over VPN is that the resource requirements on the main site gateway are extensive for large deployments. Administrators have the option of mixing and matching direct SSL and VPN over SSL links to remote sites on a gateway-by-gateway basis to limit the resource impact of hundreds or thousands of VPN tunnels terminating at the main site. Symantec also provides clustering options with their line of enterprise-class 5400 Series gateways that can easily scale to handle any size deployment.

Authentication certificates

By default, SESA uses a self-signed SSL certificate to encrypt communications; this requires no further configuration on the SESA Manager or the 400 Series appliances. If a deployment requires a custom-trusted certificate, administrators have two options:

1. Load the custom-trusted certificate into SESA and the certificate authority’s (CA’s) root certificate.

2. Load the same SESA certificate onto each 400 Series appliance intended for SESA management.

Using the CA root on the 400 Series appliances offers two advantages:

1. The CA root certificate has a long life; it will not expire after one or two years (expiration requires import of new certificates).

2. When using the CA root, the 400 Series will trust any “child” certificates provided by that “parent.”

The second point above is important because the 400 Series supports the use of secondary SESA Managers should the primary become unavailable. A secondary SESA Manager would use a different certificate but one likely issued by the same CA; primary and secondary SESA Managers using the same root certificate will be trusted by the 400 Series appliance. In any case, to offer flexibility in any deployment scenario, the 400 Series supports the import of up to three certificates.
Basic network settings

Administrators must determine the basic network settings that will be used at all remote sites. All remote sites should be configured with different LAN subnet IP addressing. For example, 100 offices should not be configured on the same 192.168.0.0/255.255.255.0 subnet. Although this is technically possible to implement with the direct SSL scenario, it can cause issues; for instance, if sites need access to servers that are placed at remote sites. Configuring each remote site with a different subnet address will:

- Enable future VPN meshes (one remote site creating a tunnel directly to another remote site)
- Simplify common hub and spoke VPN deployments
- Increase the scalability of the remote sites

Note that VPN over SSL management scenarios require different subnets at each branch location.

Once the deployment and addressing plan is complete, administrators can begin to develop security policies and determine the resource-sharing requirements for each site. SESA’s powerful policy distribution model allows quick setup of hub and spoke VPN deployments (see figure 5) of hundreds of 400 Series appliances with a single configuration policy. This easily enables main site access to branch office network resources throughout a deployment’s topology.

Figure 5. Hub and spoke VPN topology
SESA installation overview

To install the SESA Foundation Pack version 2.0, administrators should follow the installation quickstart card. The installation wizard guides administrators through the installation of all three main SESA components. A few tips:

- The SESA software must be installed onto a clean system (i.e., one with a fresh OS install); services that may interfere with the application should not be running.
- The system requirements for the SESA installation are included with its documentation.
- The scale of the deployment will determine whether each SESA component is installed on its own server hardware or whether components can be combined onto a single hardware platform.
- Deployment scale will also determine the minimum bandwidth of the Internet or local network connection needed by the SESA server.
- To access the management console remotely, T1 bandwidth (at a minimum) should be available to support administrator console traffic. If an administrator intends to access the SESA Manager locally or from the server itself, bandwidth is not an issue.

Once SESA is installed, the SIP for the 400 Series appliances is installed.

SESA administration

SESA is administered using a standard Web browser. To log in to the SESA Manager:

- From the server itself: Click on the hyperlink icon installed on the Start Menu (Windows). If administering remotely, enter the following into the Web browser address field: https://<IP of SESA Manager>/sesa/ssmc.
- Enter the user/pass/domain that was configured during the SESA installation.

The SESA Manager console (see figure 6) will now display in the administrator’s browser window.

Figure 6. SESA Manager console overview
The SESA console consists of several sections that allow administrators to easily view events and reports, manage multiple products and groups within a product type, and manage specific policies and events within product groups. Toolbar buttons and menus change depending on the current SESA control tab. The following four control tabs correlate to the main SESA functions:

- **Alerts**—Here administrators configure notifications for particular events.
- **Events**—Event logs and reports from products managed by SESA are displayed here.
- **Configurations**—This section is used to create configuration policies for all products managed by the SESA Manager.
- **System**—This is where the SESA Manager, SESA Agent parameters, and state information can be viewed or changed.

The following sections provide a high-level overview of the SESA console features and usage. For in-depth coverage of each feature, see the reference section at the end of this document.

### Connecting the Symantec Gateway Security 400 Series to SESA

Once SESA is installed, the administrator can activate the 400 Series appliances for centralized management and to connect to (or “join”) the SESA Manager. The appliance joins by querying the SESA Manager for available Organizational Units, or groups, defined for products. Each Organizational Unit has associated configuration parameters defined for units that join that group. The administrator selects the appropriate Organizational Unit from those sent to the 400 Series appliance (for example, the “Accounting” Organizational Unit) and proceeds to join (see figure 7).

Once joined to SESA, the 400 Series will start sending events (logs) and state information (statistics) at regular intervals to the SESA server. If the administrator joined in full Centralized Monitoring and Policy Management mode, the policy intended for the 400 Series appliance (the parameters associated with that Organizational Unit) will immediately be applied by the SESA Manager. Changes made to the Organizational Unit configurations will automatically be applied to the 400 Series appliance, or new configuration parameters can be created from the SESA Manager for each appliance individually.

![Figure 7. View of a Symantec Gateway Security 460 joining SESA](image)
How to join a 400 Series appliance to SESA

1. On the 400 Series Administration > Advanced Management screen, select the Centralized Monitoring and Policy Management radio button.

2. Enter the IP/domain name of the SESA server, the administrator username, and password (from the SESA install).

3. Click the Query SESA button to retrieve the Organizational Units (groups) that your 400 Series appliance can join. Note: Only “Default” will show unless you’ve configured groups within SESA. Select the appropriate Organizational Unit.

4. Click the Join SESA button.

5. After a few moments, click the Refresh button. You’ll see the status at the bottom of the screen change to reflect your SESA ID and that management is Active.

Monitoring 400 Series appliances from SESA

The powerful monitoring features of SESA provide a wealth of data from various products and product types that can be combined and distilled into a simple pie chart if needed. Administrators can view all 400 Series events (see figure 8). SESA maintains a common event schema for firewall events that enables the 400 Series events to be used in reports containing other firewall events managed by SESA (see “All firewall network events” in the navigation pane of figure 8).

With a simple right click of the mouse, the administrator can filter events according to any parameter, including event type, severity, and individual appliances (referred to as “machines” within the SESA console).

The 400 Series SIP (SESA plug-in) comes with predefined reports for the 400 Series events. New custom reports can be created with easy-to-use report wizards.

Figure 8. Displaying events for 400 Series appliances
How to view events
1. Log in to SESA and click on the Events tab.
2. Expand the Firewall Events tree.
3. Expand the Symantec Gateway Security 400 Series tree.
4. Click on Symantec Gateway Security Network Events. Alternatively, you can click on All firewall network events in the previous branch, which will include events received from the 400 Series appliances.
5. Scroll through the events in the right pane. Right click on Events for Filtering for more options.

Alerts
Since SESA can gather a multitude of events from hundreds or thousands of appliances, the Alert feature provides a flexible method to automatically single out important events or event trends and notify an administrator. Alert notifications can be delivered to the administrator via pager, email, or SNMP traps, or by logging on to local OS facilities.

Defining alerts
Because alerts are not predefined in SESA, administrators need to create alert definitions. Administrators can create alert definitions containing:

- Product type
- Event class, category, type, or severity
- Repeated threshold events within a period of time

When defining alerts, administrators should take into account the Internet connection type and ISP to which that the gateway is connected. Broadband cable is typically “noisier” than DSL and more prone to attacks. Some ISPs carry more broadcast traffic than others. An ISP may experience traffic variances from one locale to another. These factors can result in a large number of notifications if the alert parameters are defined too strictly. On the other hand, administrators may wish to be notified of all attacks on a gateway connected to a T1 connection. A few tips:

- Tailor alerts for the ISP type or down to the specific “machine.”
- Do not create alerts that will trigger excessive notifications, as this may result in dismissal of an actual network attack.
- Use vulnerability assessment tools to test alerts in “real-world” scenarios, if possible.
In figure 9, an alert was configured to notify the administrator any time 99 Firewall Connection Denied events are received within a one-minute period (termed the Alert “threshold”).

How to configure an alert

1. Click on the Alerts tab.
2. Click the Alert Configuration icon.
3. The wizard will guide you through the following selections:
   - Product
   - Type of event
   - Parameters that will cause the alert
   - Users to notify
Creating configurations on SESA for the 400 Series

Two types of configuration policies are available for all products managed by the SESA Manager:

- **Policy Settings**—These can be easily applied to multiple gateways in a group, for example, IDS settings.

- **Location Settings**—These are more appliance-specific settings that can also be applied to groups of appliances handling similar tasks (such as all secondary roaming access points in a wireless deployment).

Combined, these two groups of configuration settings make up the configuration package sent to the 400 Series appliances from SESA. Both groups can be associated with an Organizational Unit or with an individual appliance. Each Location Setting has an associated Policy Setting configuration and vice versa.

When the 400 Series appliance joins SESA, it is automatically associated and configured with the Policy and Location Settings related to its Organizational Unit. This enables the appliance to conform to the administrator’s defined security policy for that product type. For this reason, it’s best to pre-define Organizational Units and their related Location Settings and Policy before joining appliances to SESA. SESA also uses logical names for certain configuration parameters, such as an inbound firewall rule. For example, the SESA administrator can create an inbound firewall rule to TCP Port 80 called “WebServer” in the Policy associated with the “Marketing” Organizational Unit. All 400 Series appliances in the Marketing Organizational Unit with a computer defined on the LAN as WebServer will automatically activate that inbound firewall rule. This logical configuration definition capability allows SESA to apply a set policy to hundreds of appliances (see figure 10).

![Figure 10. Configuring a setting to disable radios on all 400 Series appliances associated with the Policy “Jack”](attachment:image.png)
How to create new Policy and Location Settings
1. Click the Configurations tab.
2. Expand the Symantec Gateway Security 400 Series tree.
3. Right click on the Policies tree and select New.
4. Right click on the Location Settings tree and select New.

To associate the new Policy and Location Settings with an Organizational Unit or an individual 400 Series appliance (see figure 11):
1. Click the Find All Gateways icon button.
2. Select the Organizational Units or expand the Organizational Units and select the individual 400 Series appliance and click Associate.
3. In the Associate window:
   • Select the Policy name from the Policy drop-down menu
   • Select the Location Settings name from the Location Settings drop-down menu
4. Click OK.
5. Close the window.

Figure 11. Associating new Policy and Location Settings with an Organizational Unit
The Organizational Unit or the individual 400 Series appliance is now associated with the new Policy and Location Setting names. The administrator can now configure settings and “activate” them for the associated appliance(s). Note that changes “applied” on each right-pane tab are not actually sent to the appliance(s) until the Activate button on the toolbar is clicked.

There are other methods to apply settings and define groups (Organizational Units) of gateways to associate with different policies (see figure 12). These are further described in the Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) Administrator’s Guide and Integration Guide.

Figure 12. Editing the VPN configuration under Location Settings
Best practices

After administrators develop a clear and concise security policy that can be realistically followed by various departments, SESA can be used to enforce that security policy on gateways and to monitor events that may indicate security policy violations.

Administrators should run reports regularly to create a history of data. Although the predefined reports included with the 400 Series SIP installation provide a solid foundation, administrators are best served by tailoring the reports for an organization’s specific product deployment. Alerts should also be defined and refined to ensure that notifications are delivered to the individuals who can appropriately deal with pressing security issues.

If there are multiple administrators using the SESA Manager, user privileges should be defined that will delineate policy management access. SESA allows flexible user-defined privileges that can limit access to specific Organizational Units or product types, for example.

It is best to install the SESA Manager behind a high-performance firewall such as the Symantec Gateway Security 5400 Series. This will prevent system intrusions and denial-of-service-type attacks on the SESA Manager.

Only applications that relate to SESA should be installed on the SESA server hardware (with the possible exception of a local host firewall). Unrelated applications can interfere with SESA operation and open potential security vulnerabilities that otherwise would not be available as an attack vector.

Reference

For more information about SESA 2.0 in general or managing the Symantec Gateway Security 400 Series specifically, refer to the following documents:


- **Symantec Event Manager and Advanced Manager for Security Gateways (Group 2) Administrator’s Guide and Integration Guide**—available from the Symantec Gateway Security 400 Series support page

- For further information on pricing and requirements, call Symantec Corporate Sales at 1 800 745 6054
SYMANTEC IS THE GLOBAL LEADER IN INFORMATION SECURITY PROVIDING A BROAD RANGE OF SOFTWARE, APPLI-
ANCES AND SERVICES DESIGNED TO HELP INDIVIDUALS, SMALL AND MID-SIZED BUSINESSES, AND LARGE ENTER-
PRISES SECURE AND MANAGE THEIR IT INFRASTRUCTURE. SYMANTEC’S NORTON BRAND OF PRODUCTS IS THE
WORLDWIDE LEADER IN CONSUMER SECURITY AND PROBLEM-SOLVING SOLUTIONS. HEADQUARTERED IN
CUPERTINO, CALIF., SYMANTEC HAS OPERATIONS IN MORE THAN 35 COUNTRIES. MORE INFORMATION IS AVAILABLE
AT WWW.SYMANTEC.COM.