This chapter covers the following topics:

- General CSA components overview
- CSA installation requirements
- Agent kits

CHAPTER 6

Understanding CSA Components and Installation

The Cisco Security Agent (CSA) is a complex architecture that can enforce enterprise security policies by granularly controlling endpoint behavior. Although technical and security expertise is required to configure, control, and monitor the deployment, it takes very little remote user knowledge of such topics to successfully use the product. In most cases, users have very little interaction with the product and typically are completely unaware of the protection the product is providing their system. Occasionally, the local CSA prompts the user for a response regarding an action that might be normal or malicious or even displays temporary balloon messages to the user about actions that are taking place. In general, however, you should keep the interaction between the user and CSA at a minimum, and generally the user will continue unaffected by the dangers lurking on the network.

Other than the installation of the product, which can be scripted through various methods, the user may never need to interact with the product if that is the desired outcome. Through the application of effective tuning mechanisms, discussed in Chapter 12, "Creating and Tuning Policy," you can get the implemented policy to a point where protective mechanisms are enforced and yet users have no interaction with the product at all. Security administrators use the CSA MC to configure all parameter assignments of the agent and its personalized policies. Optionally, as a new feature in version 4.5, the administrator can allow end users to view and use an advanced user interface (UI) that allows the user on the endpoint to control some of the policy enforced on the local workstation, such as personal firewall rules. If that is not desired, you do not need to deploy this interactive capability to all users in the architecture, or any at all.

In this chapter, you continue to gain an understanding of the CSA architecture through an exploration of the agent software components, protocol communication, and installation.

General CSA Agent Components Overview

You have access to several "under-the-hood" components that are built in to CSA. To fully understand how CSA works, it is best to get at least a high-level understanding of a few of the key components and their interaction on the local agent system.

When rules are changed, edited, added, or removed on the CSA MC that pertain to the particular rules and policies running on your agent, you need to update your local policies with the necessary changes. To do this, your local security agent software communicates with the CSA MC via HTTPS (443) to retrieve the new information. If you recall from an earlier discussion in Chapter 2, "Introducing the Cisco Security Agent," the CSA architecture uses a pull model whereby the agent requests information regarding possible policy changes at a set interval, which by default is 10 minutes. CSA version 4.5 includes a signed UDP hint message that can "nudge" the remote agents into polling earlier than the predetermined time so that they will receive the update ahead of schedule. This feature is very convenient, especially in environments where you have changed the default polling interval to a higher time value and you need the ability to push (that is, request a pull) a change quicker than the typical poll cycle.

The *agent policy manager* is the agent component that receives the policies from the CSA MC server and forwards them to another agent component known as the *rule/event correlation engine*. This engine reviews the old and new rules and replaces or updates whatever is necessary to form the new local rule set.

Another component in the CSA is known as *interceptors*. Interceptors proxy actions that are attempted and verify how to proceed against the rules in the rule/event correlation engine. Some of the interceptors are as follows:

- **Network Traffic interceptor**—Use for SYN flood and port scan protection.
- **Network Applications interceptor**—Limit or allow individual applications to access the network via specific protocols and networks addressing parameters.
- **File interceptor**—Limit an application's ability to read and write to specific files and directories.

A final noteworthy component is the *local event manager*. The local event manager locally stores events that are generated by the rules that have been triggered and set to log. Once stored and cached locally, the events that are to be logged are sent to the CSA MC for administrative review and global event correlation capabilities. If the CSA MC is not available, the agent stores the events and transmits the next time the agent can communicate with the CSA MC server with the appropriate time stamps attached.

All of the previously mentioned agent components also reside in the UNIX agents, although they are implemented through different programming methods available to those operating system architectures.

CSA Installation Requirements

In each of the operating systems in which CSA may be installed, you must satisfy minimum hardware and software requirements to ensure the deployment is supported by Cisco Technical Assistance Center (TAC). This section describes the software and hardware requirements and the communication requirements.

Software and Hardware Requirements

CSA has specific minimum requirements to load on an endpoint-protected server or workstation. Because the CSA is a software product, it only runs on appropriate operating systems. In version 4.5, the agent is supported on some Solaris, Linux, and Windows flavors. Future versions might provide you with an expanded operating system support base, but for version 4.5, follow the operating system requirements described in this section or refer to the latest CSA documentation for the most current guidelines, which are available at Cisco.com.

The hardware requirements for Windows, Solaris, and Linux agents differ slightly. Verify the requirements for your system before attempting installation and architecture implementation.

NOTE CSA uses approximately 20–30 MB of disk space on all platforms.

Table 6-1 shows the Windows agent minimum requirements.

Table 6-1 *Windows Agent Requirements*

System Component	Requirement
Processor	Intel Pentium 200 MHz or higher. Note: Uni/dual/quad processors are all supported.
Operating systems	Windows 2003. Windows XP (Professional English 128 bit) with Service Pack 0, 1, or 2. Windows 2000 (Professional, Server, or Advanced Server) with Service Pack 0, 1, 2, or 3 or higher. Windows NT (Workstation, Server, or Enterprise Server) with Service Pack 5 or higher. Note: Citrix MetaFrame and Citrix XP are supported. Terminal Services are supported on XP and Windows 2000. Terminal Services is not supported on Windows NT.
Memory	128 MB minimum.
Hard drive space	15 MB or higher.
Network	Ethernet or dialup. Note: Maximum of 64 IP addresses supported on a single system.

Table 6-2 lists the Solaris agent minimum requirements.

Table 6-2 *Solaris Agent Requirements*

System Component	Requirement
Processor	UltraSPARC 400 MHz or higher. Note: Uni/dual/quad processors are all supported.
Operating systems	Solaris 8, 64-bit 7/01 edition or higher. Note: Solaris minimum core installation is not sufficient. You must also install the SUNWlibCx library.
Memory	256 MB minimum.
Hard drive space	15 MB or higher.
Network	Ethernet. Note: Maximum of 64 IP addresses supported on a single system.

Table 6-3 shows the Linux agent minimum requirements.

Table 6-3 *Linux Agent Requirements*

System Component	Requirement
Processor	500 MHz or higher x86 processor. Note: Uni/dual/quad processors are all supported.
Operating systems	RedHat Enterprise Linux 3.0 ES, AS, or WS.
Memory	256 MB minimum.
Hard drive space	15 MB or higher.
Network	Ethernet. Note: Maximum of 64 IP addresses supported on a single system.

Additional Installation Requirements

For the CSA to become fully functional, you must address a few other points. Beyond the requirement to be loaded on a supported hardware and software platform, the agent must also support the necessary communication to be sure the agent remains current from a policy standpoint. The agent must also be able to resolve the IP address of the CSA MC server by its fully qualified domain name (FQDN) within Domain Name System (DNS).

CSA MC Server and Database

The CSA MC server contains the rules and policies that are required for agent enforcement. The MC is also where configuration changes and updates are maintained and is the focal point

for the agents when they need to update their local policy enforcement rules. In addition, the MC serves as the destination for agent event messages that are transmitted and thus provides a centralized aggregation point for global event correlation and agent troubleshooting.

The default installation of the CSA MC includes the installation of Microsoft Data Engine (MSDE) database. This database is sufficient for smaller installations of 500 agents or fewer. The MSDE database has a database size limitation of 2 GB, which is not sufficient in larger deployments. When the enterprise agent deployment total increases to a number greater than 500 agents, it is recommended that you migrate the MSDE database to MS SQL.

In version 4.5, you can keep the MS SQL database local to the CSA MC server itself or you can use an externally loaded MS SQL server installation. It is important in either case that this database and server be secured from both a network and physical standpoint. You might decide to use an external MS SQL database in your enterprise for a number of reasons, as follows:

- Off-box SQL allows for cold standby CSA MC servers in case of a server failure.
- Fewer enterprise SQL deployments to maintain (regular maintenance and patching) because the SQL database can reside in your current enterprise SQL system.
- The ability to leverage highly effective SQL hardware, including server architectures and disaster recovery mechanisms such as storage-area networks (SANs).

Communication Security

For policy and rule changes created on the CSA MC to take effect on the CSA, the CSA must have the ability to contact and communicate with the CSA MC over the network. This communication path can take any transport necessary between the agent and MC machines as long as there is end-to-end IP reachability for the duration of the connection.

For the agent to request the update or transmit event log messages, the agent attempts to resolve the MC IP address using DNS or any other local resolution means available such as the local hosts file. It is important that this information be correct to facilitate both a successful connection and to verify the certificate used in the Secure Sockets Layer (SSL) communication.

SSL over the standard TCP port 443 is the protocol used for all MC-to-agent interaction. SSL ensures an authenticated and encrypted communication of the updates and event transmissions. Within an enterprise, name resolution is not typically an issue; however, if you have systems that will roam around disparate networks, you need to be certain that the machine resolves the correct address and that the CSA MC server is reachable from those locations.

NOTE The CSA policy information is local upon installation and does not need to be in contact with the CSA MC for the policy to remain active. CSA MC contact is required for policy and software updates and for transmission of the locally stored events for global interrogation and correlation.

Agent Kits

Agents are initially installed on endpoints via an executable install file. You can download and install this file directly from the CSA MC itself from an SSL-protected web page. Other methods of installation include locally executing the EXE file manually or via many other scripted and automated installation procedures such as an enterprise software installation system.

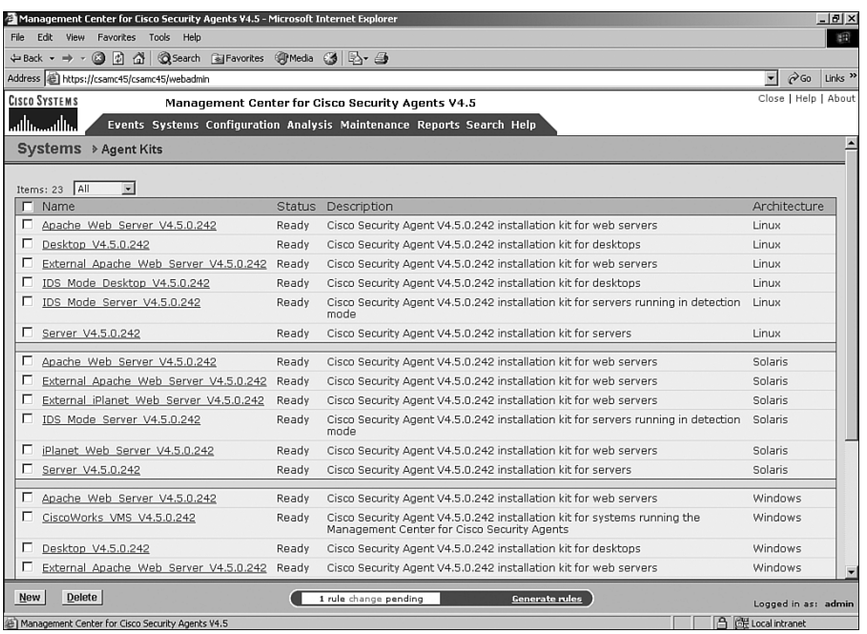
Creating an Agent Kit

Before you can install an agent kit on a workstation, you must accomplish a few tasks. First you must create the appropriate initial modules, policies, and rules that the agent will use. Then you must define the group and attach policies to it. Then you must create the agent kit and define a few installation kit parameters. This section describes these tasks and explains the options along the way.

Step 1 Choose **System > Agent Kits** from the navigation bar. This brings you to a view of all the currently available kits. (There are pre-installed agent kits available.) See Figure 6-1.

Step 2 Click **New**.

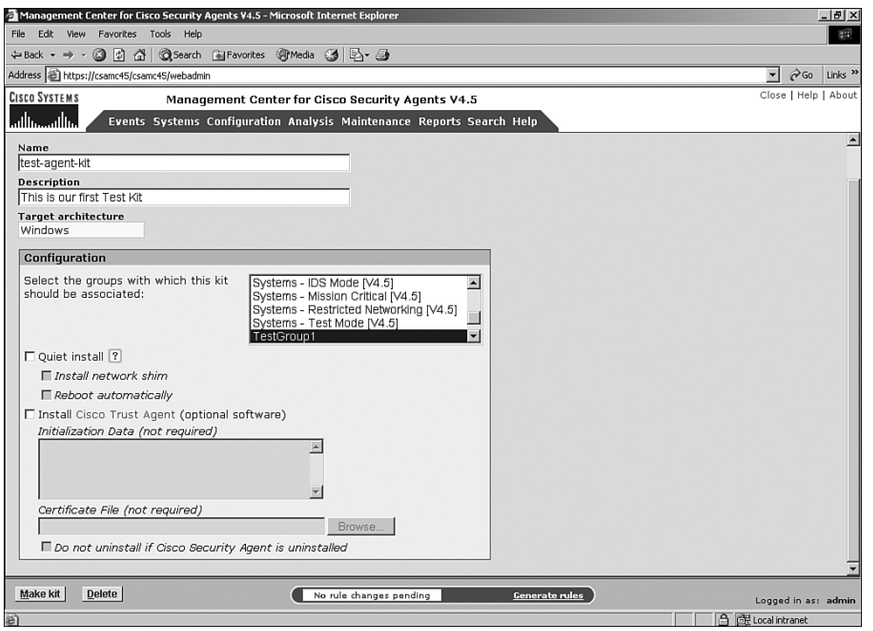
Figure 6-1 *Available Agent Installation Kits*



Step 3 When prompted with the What Is Your Target Architecture? pop-up window, choose the appropriate platform. In this example, choose **Windows**.

Step 4 Create a name and description that is appropriate to this agent kit, as shown in Figure 6-2.

Figure 6-2 *Agent Kit Creation*



Step 5 Choose the appropriate groups that will be associated with this installation kit. You may choose more that one group if necessary.

Step 6 Choose whether this should be a quiet install. Both the quiet and nonquiet installs need to be executed on the local machine either manually or via a scripted or automated method; however, when you choose Quiet Install, the user is not prompted during the installation for options such as installing the network shim or rebooting after installation.

Step 7 (Optional) If you choose Quiet Install, you can then select to install the network shim or reboot automatically after the installation completes.

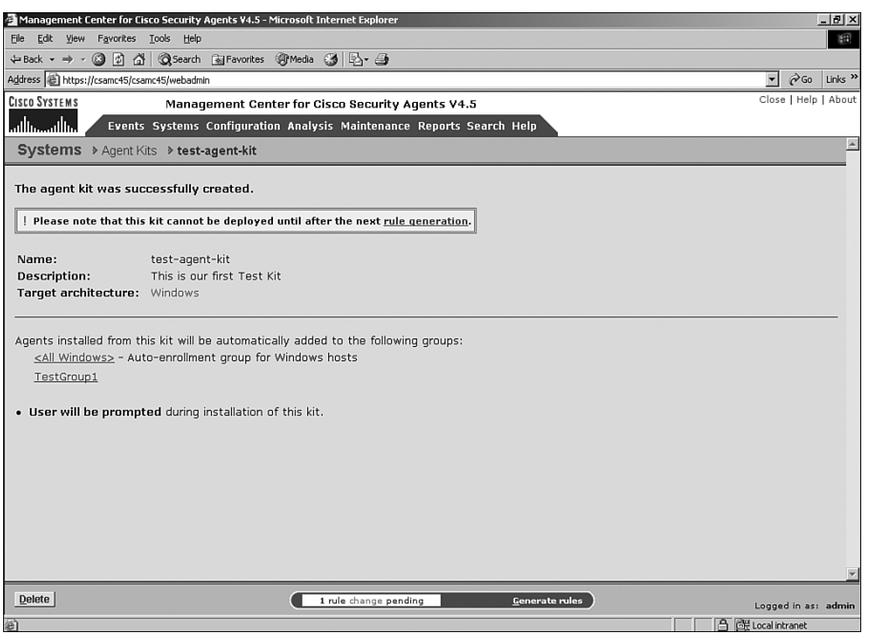
Step 8 (Optional) Choose whether you want to install the Cisco Trust Agent (CTA), which is part of the Cisco Self-Defending Network Initiative. CTA can query the CSA for information about the local workstation, such as installed hotfixes and service patches as well as some state

information about the CSA itself. If you do opt to load CTA, you can include information regarding its initialization as well as CTA certificate information that is used to secure the CTA Extensible Authentication Protocol (EAP) session to the Cisco Secure Access Control Server (ACS). Finally, under CTA, you can opt to state whether the CTA should be uninstalled if the CSA is ever uninstalled.

Step 9 After you have configured the kit to your liking, click **Make Kit**.

Upon completion of your agent kit creation, a confirmation screen displays summarizing the selections you made during the creation process. (See Figure 6-3.) You are also reminded that the kit is not ready for deployment until after the next rule generation has been performed. You can perform a generation at this time if you are ready to proceed.

Figure 6-3 *Agent Kit Confirmation Screen*



To Shim or Not to Shim?

With regard to the CSA operation and ability to protect a host, the network shim provides the following capabilities:

- Port scan detection
- SYN flood protection
- Malformed packet protection

Now, you may say, "I want all of that. Why would I not load the network shim with every agent kit?" Good question! The reason is that other network shims might already be loaded on the workstation. These other network shims typically take the form of VPN or personal firewall software. Quite often, these shims can conflict and cause problems with endpoint operation. The solution is to either not load the CSA network shim or remove the other software that is in conflict.

NOTE The Cisco Secure VPN Client does not conflict with the CSA network shim.

Disabling the network shim does not stop network access control rules from running; it only stops the network hardening features from being active, such as SYN flood protection and port scan detection. As a best practice, it is advisable to continue to use the network shim on Internet-facing servers or systems that might be targeted by such attacks as listed previously. Servers do not tend to use the type of software that conflicts with the network shim provided by the CSA, and you would therefore have few conflicts to resolve in this case. Desktop and laptop systems regularly use applications that could conflict, and you should cautiously test the shim on these systems to prevent unnecessary outages. Because desktop systems are not often targeted for denial-of-service (DoS) attacks, these preventive and alerting mechanisms in the shim can often be better served by well-placed network IDS sensors.

Installing Agent Kits

Agent kits, once created, still need to be installed on the remote systems you are attempting to protect. The installation package created varies according to the intended operating system architecture onto which it will be loaded. The installation procedures vary between the Windows, Linux, and Solaris implementations of the product. The next few sections cover the installation processes and procedures necessary to successfully load the agent on these systems.

Installing a Windows Agent Kit

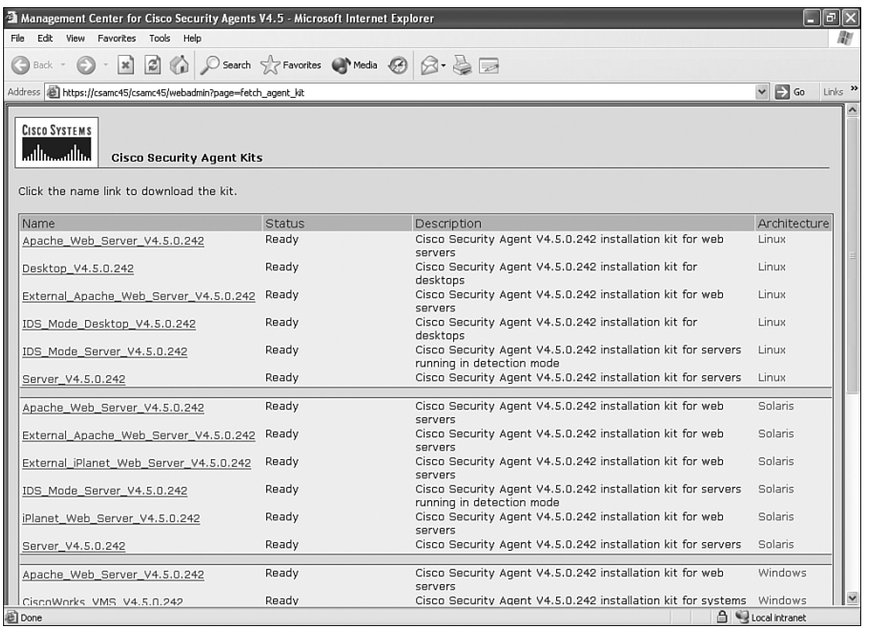
After you have created the Windows agent kits, they are ready for installation. First look at how the remote endpoints can install the software directly from an SSL-protected web page on the CSA MC. Perform the following tasks on the endpoint:

Step 1 Open a web browser and go to the following URL:

https://*ciscoworks_system_name*/csamc45/kits

The web page that displays, as seen in Figure 6-4, provides a listing of all agent kits on this CSA MC server.

Figure 6-4 *Available Agent Kits Page*



To view this URL and register with this particular CSA MC server, you must be allowed to do so as defined in the Registration Control settings on the CSA MC, as shown in Figure 6-5. To access this page, choose **Systems > Registration Control**.

Step 2 From the Cisco Security Agent Kits page, choose the kit you want to install by clicking the link. You must have local administrator rights to install the kit.

Step 3 You are prompted to save the installation file. Click **Save** and find a location that is appropriate for the file.

Step 4 Close your browser and double-click the executable file you downloaded. The EXE is a self-extracting file.

If the agent is performing a quiet install, no interaction occurs with the user, and all installation occurs without any input required from the user. If the agent is performing a nonquiet install, proceed with the following steps to complete the installation.

Before the installation can continue, the agent installation kit verifies the user has local administrator rights; otherwise, a pop-up notification displays.

Step 5 After clicking **Next** to proceed with the installation, read the license agreement, as shown in Figure 6-6. You are required to accept the license agreement to continue.

Figure 6-5 *Registration Control Page*

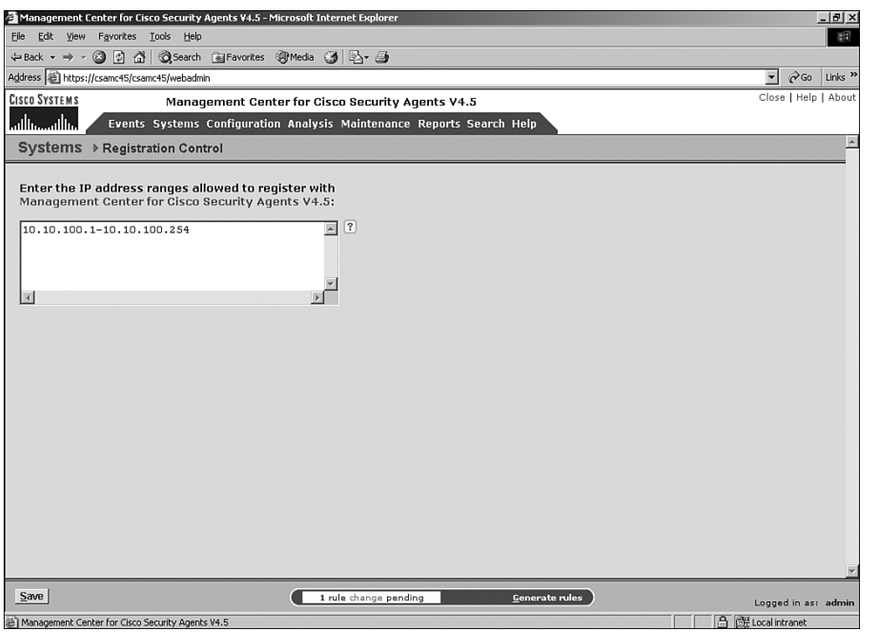
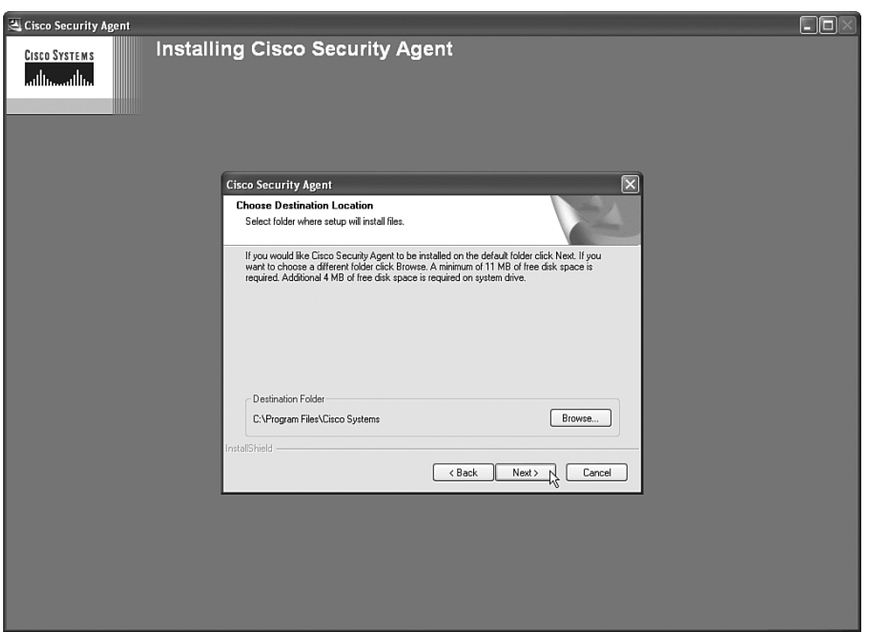


Figure 6-6 *Installation License Agreement*

Step 6 Choose the installation path, as shown in Figure 6-7. The default installation directory is Program Files\Cisco Systems. The folder selected here becomes the location in which a CSAgent folder is created. All agent executables and other supporting files are placed in a directory hierarchy within the newly created CSAgent folder in the directory you select.

Figure 6-7 *Installation Directory Path*



Step 7 After you select the path, choose whether to install the network shim, as shown in Figure 6-8.

Upon completing Step 7, a summary screen displays before final installation continues, as shown in Figure 6-9. After you verify that the summary information regarding the installation to be performed is correct, the actual agent installation begins, as shown in Figure 6-10.

After completing the installation, the system presents you with a reboot request. A reboot is not required for most agent functionality to become active; however, for a more detailed look at the functions available after a successful reboot, see the "Immediately Rebooting the System After Installation" section later in this chapter. Figure 6-11 shows a sample reboot request.

Figure 6-8 *Choose Whether to Shim*

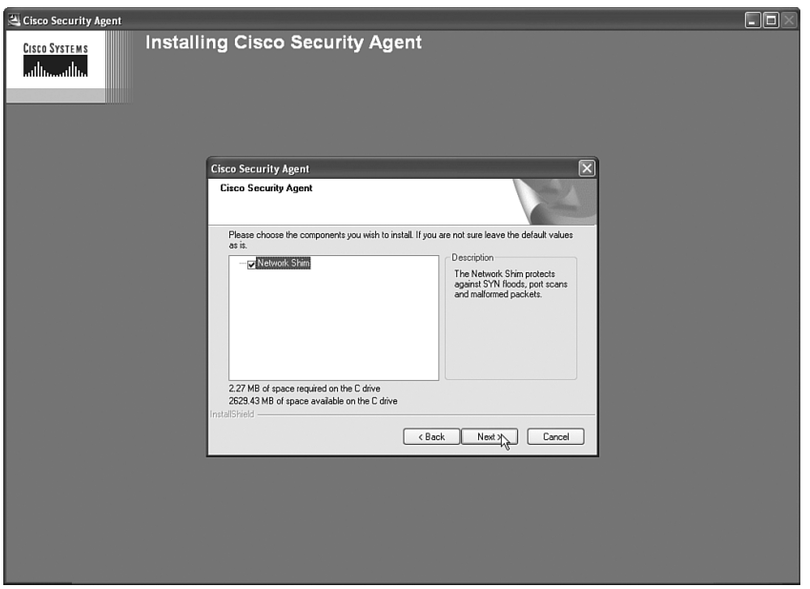


Figure 6-9 *Pre-Installation Summary Screen*

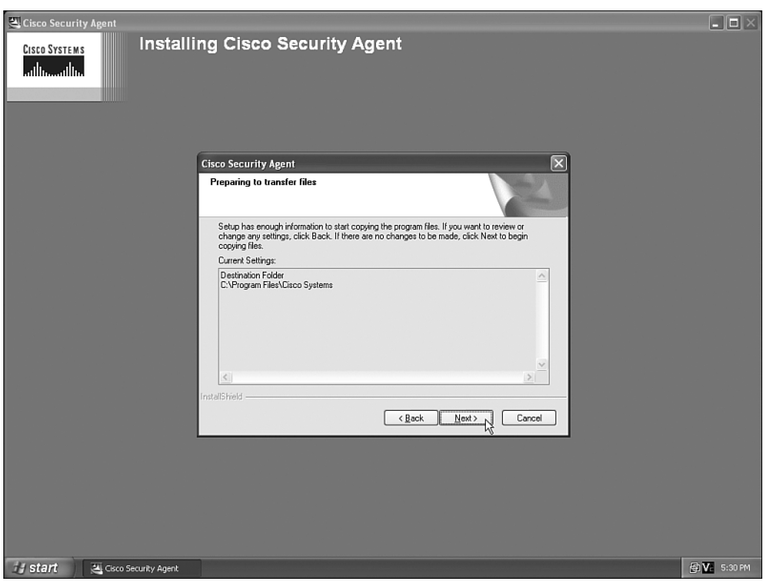


Figure 6-10 *Installation Begins*

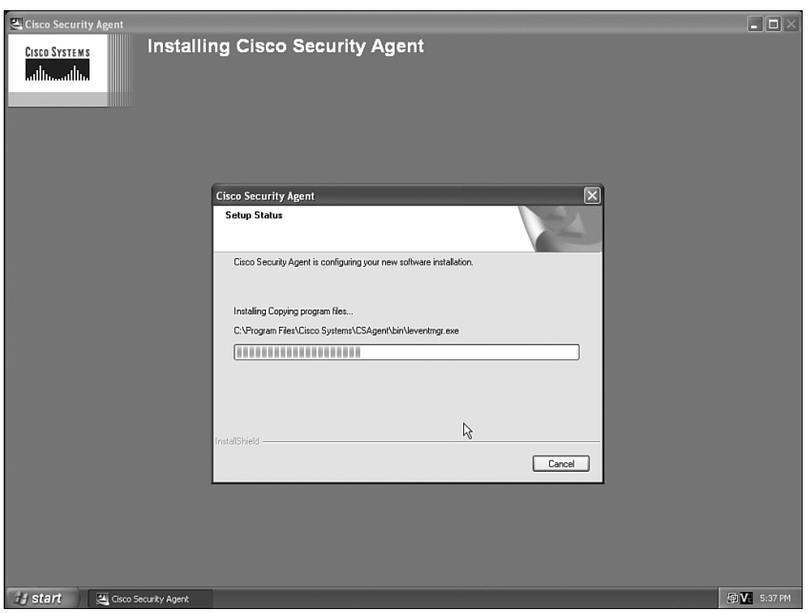
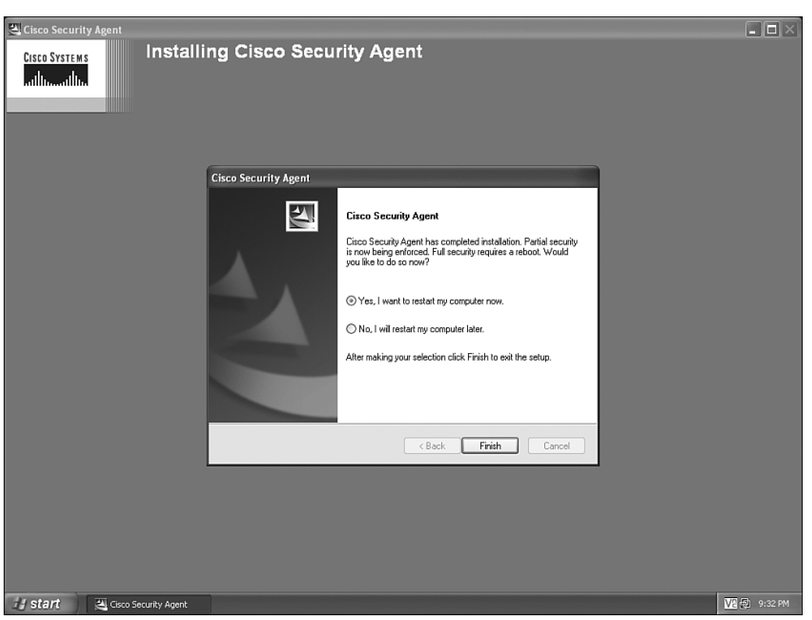


Figure 6-11 *Reboot Request*



As an alternative to sending the user to the URL that includes every possible agent kit, you can go back to the Cisco Security Agent Kits page and choose the specific kit you want the user to install. When this page opens, you will see a specific link that you can send to the user via e-mail or another method. This link is to the direct download for that kit and enables the user to install that specific agent kit when clicked. You are also given the Copy to Clipboard option, which places the specific link in your Windows clipboard so that you can craft an e-mail and then just paste the link into the message from your clipboard.

Installing a Solaris Agent Kit

The installation of a Solaris agent kit is a command-line process that requires the installer to be a super user on the system. To install a Solaris agent kit, retrieve the agent installation kit as per the Windows agent kit retrieval process described earlier or manually copy the kit from the CSA MC. Continue the installation process by unpacking the archive and installing the package to the default directory, which is /opt/CSCOcsa, using the following two commands on the Solaris system:

- **tar xf CSA-Server_4.5.0.15-setup.tar**
- **pkgadd -a CSCOcsa/reloc/cfg/admin –d**

To complete the Solaris installation process, verify the package to install is the intended package as per the system response that displays as a result of your command entry above and acknowledge that you want to continue the installation. Press **q** when the installation completes. Finally, reboot the system by typing **shutdown -y i6 g0**.

Installing a Linux Agent Kit

The installation of a Linux agent kit is a command-line process. To begin the process, you must first obtain the Linux agent kit file from the CSA MC. After retrieving the installation kit, you unpack the compressed agent kit using the following command entered at a command prompt:

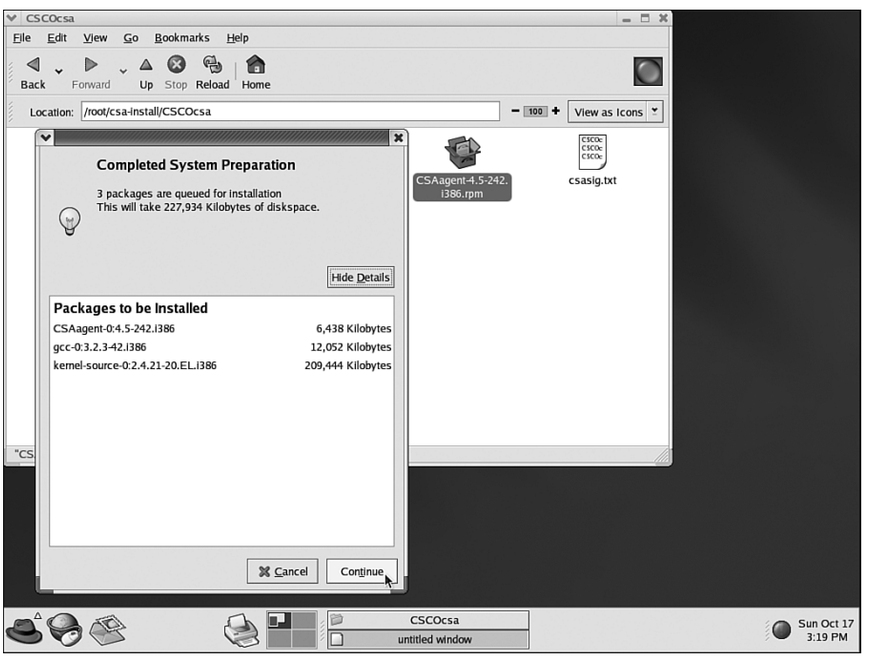
tar xvf CSAagent-4.5-51.i386.tar

You should now change directories to the CSCOcsa directory that was created during the unpacking process. This directory is the location from which you install the Red Hat Packet Manager (RPM). When in the correct directory, type the following to install the Linux RPM: **./install_rpm**.

NOTE Because of the access required to various system and file resources, you must be a root user to install the Linux agent.

As an alternative to using the command-line installation procedure, you can use the graphical interface of Red Hat to download, extract, and install the CSA. (See Figure 6-12.)

Figure 6-12 *Linux Agent Installation*



Immediately Rebooting the System After Installation

Most CSA protective mechanisms take effect immediately after installation, even before a reboot. CSA is not fully functional, however, until a reboot has occurred. Here is a list of functionality that does not take effect until after a reboot:

- **Network shield rules**—Network shield rules are not applied until after a reboot. Network shield rules provide protective mechanisms that relate to the network shim.
- **Buffer-overflow protection**—Buffer-overflow protection is only enforced for processes that start after the installation is complete. The agent does not monitor any processes that were already running; however, it does monitor any new processes that are spawned by the already running process. For Linux/Solaris agents, buffer overflow protection is only in effect for new processes.

- **Data access control rules**—These rules are not applied to Uniform Resource Identifiers (URIs) until the web server is restarted. This pertains to Windows, Solaris, and Linux agents.
- **COM component access control rules**—COM rules, which are discussed in Chapter 4, "Understanding CSA Policies, Modules, and Rules," are not functional until the system restarts.
- **Network access control rules (Solaris/Linux restriction only)**—On Solaris and Linux, these rules only apply to new socket connections.
- **File access control rules (Solaris/Linux restriction only)**—Only newly opened files have these rules enforced.

Scripted Installation

As an alternative to the manual installation processes described previously for each operating system, you can install the CSA agent automatically via a script when the user logs in to the network. The CSA agent self-extracting EXE is located in %Program Files%\CSCOpx\CSAMC45\bin\webserver\htdocs\deploy_kits on the CSA MC server. You can move this file to an appropriate location and use it in scripts or other automated installation mechanisms. For a script to install the executable successfully, be sure to create the kit as a quiet install and with the appropriate options, such as network shim and automatic reboot.

Installing Software Updates

As with any software product, various software updates will become available for the CSA product over time. You should install these updates to add new functionality or provide fixes to CSA components. When you receive a new update to the CSA product, read the release and installation notes provided with the software update. When you are familiar with the reason for the update and the procedures necessary to complete the update, proceed with updating the CSA MC application. This update will also update the agent software that is available to the agents in the form of future agent kits or updates to currently deployed agent installations. To see a listing of the available software updates on the CSA MC, as shown in Figure 6-13, choose **Systems > Software Updates** from the navigation bar.

You can obtain the information regarding each update by following the link in the Name column. Figure 6-14 shows an example of the information that displays.

Currently, two different types of scheduled updates are available to CSA: automatic and manual. With automatic updates, an agent polls as expected, and as part of the transaction it receives and installs the updated software silently. Figure 6-15 shows a typical screen that displays in a CSA MC regarding scheduled software updates that have been configured for deployment.

Figure 6-13 *Available Software Updates Page*

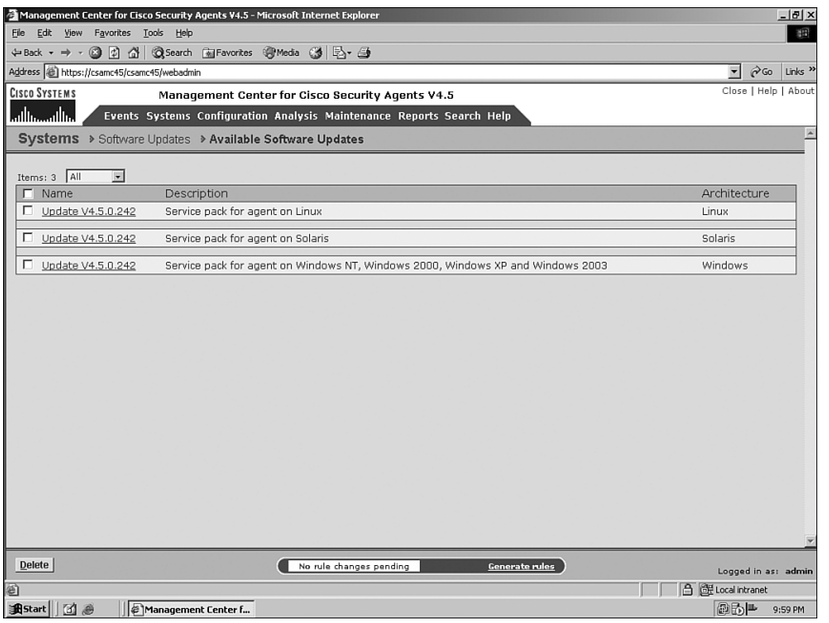


Figure 6-14 *Specific Available Update Information*

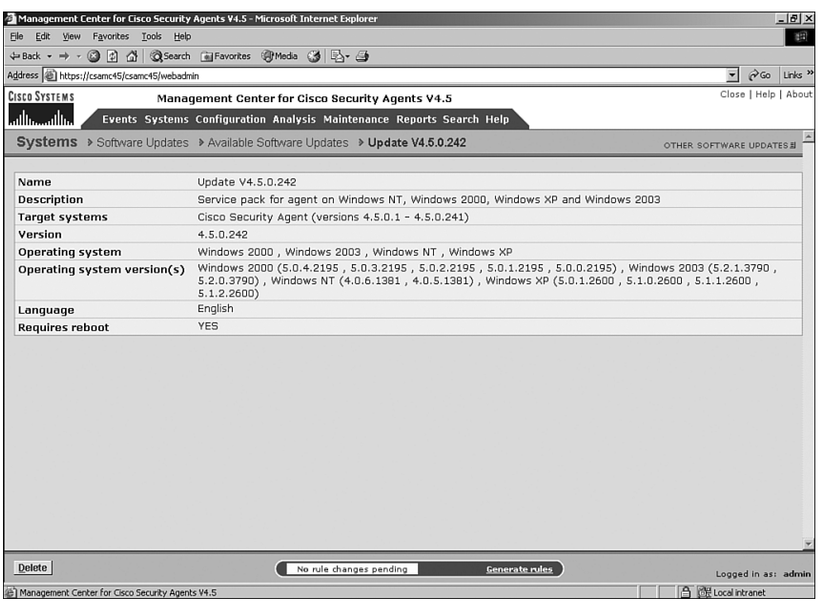
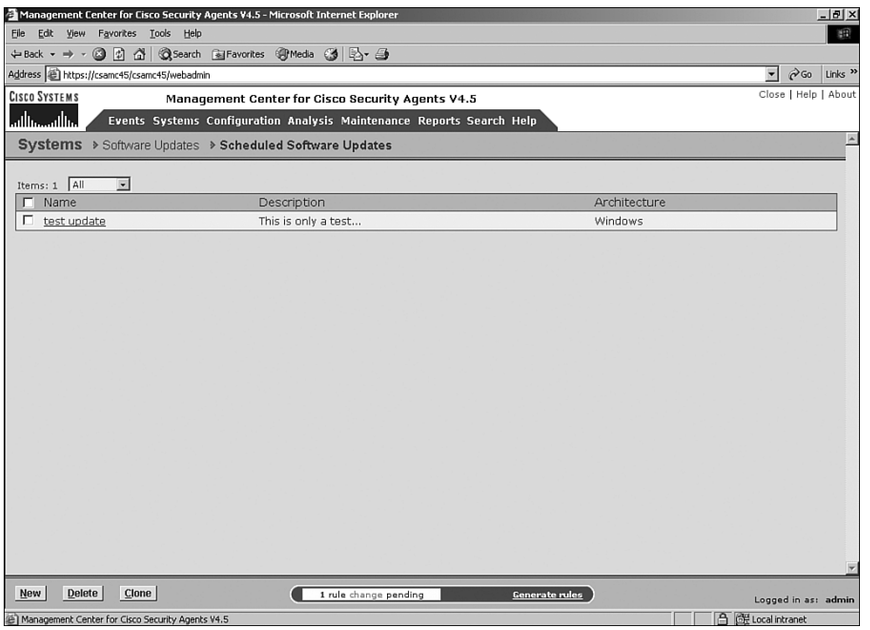


Figure 6-15 *Scheduled Updates Screen*



With a manual update, the installation is not silent. The user is prompted to either install the update immediately or postpone the update for up to 10 days.

NOTE Regarding Solaris updates, because there is no GUI for the Solaris client, you need to manually check for updates using the *csactl* client interface.

To configure a new update with parameters specific to your environment, follow these steps and refer to Figure 6-16:

Step 1 Choose **Systems > Software Updates > Schedule Software Updates > New**.

Step 2 Provide a name and description for the update.

Step 3 Choose the architecture the update will be targeting.

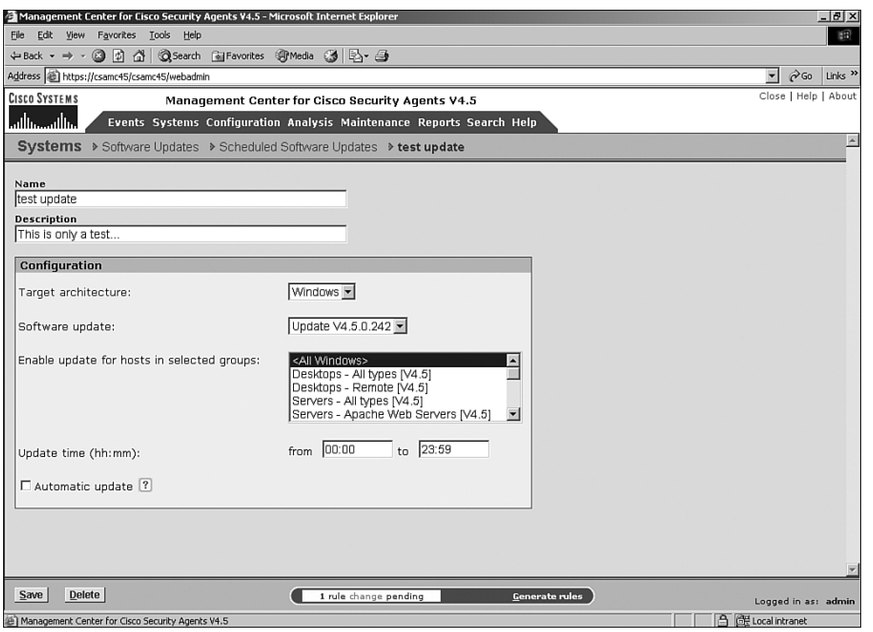
Step 4 Choose the group or groups that will be required to install the update.

Step 5 Choose a timeframe in which the updates will be available. By default, this is set to the entire day. If you edit this timeframe, the update will only be available during that window and no users can update outside of that timeframe even if they select **Postpone** at an earlier time and are now attempting to install via the button on the local GUI.

Step 6 The last configurable option is choosing whether to make the update automatic. If you make the update automatic, users do not have the option to postpone the installation.

NOTE If the update requires a reboot, a reboot occurs 2 minutes after installation completes and cannot be stopped. This is true for both automatic and manual updates.

Figure 6-16 *Update Configuration Screen*



NOTE If users decide to postpone the update, they can wait to be prompted again to install or they can click the Update Available button that appears on the first page of the CSA agent GUI.

Uninstalling an Agent Kit

If you want to script an uninstallation of a security agent, you can use a pre-installed Cisco-provided BAT file to aid in the process. On Windows systems, the script is csa_uninstall.bat and is located in the system32 directory. If you want to script the uninstall as a quiet uninstall, you should add a parameter to the BAT file. For an automated scripted quiet uninstallation, execute csa_uninstall.bat 3 in the agent's local

system32 directory. You might need to disable any rules that relate to service control prior to attempting to uninstall the agent. A query rule could easily foil your attempt to script an uninstallation of the agent.

The process to uninstall an agent running on Solaris is also very simple. From the Solaris server, enter **pkgrm CSCOcsa**. This process can be stopped by agent control rules that might be active. Disable any of these preventive rules before attempting uninstallation.

Uninstalling the agent in Linux is also a command-line feature. Before you can proceed, you must make sure you have the correct version number and then type the following from a command line:

rpm -qf /opt/CSCOcsa/bin/csamanagerd CSAagent-4.5-56

When that completes, type the following:

rpm -ev CSAagent-4.5-56.i386

As always, if any rules would prevent agent installation, you must disable those first before proceeding.

Summary

The CSA agent kit creation and installation process is fairly straightforward, or at least it can be. For larger organizations, you might find that the installation process can be automated quite effectively using scripts and other mechanisms. It is very important that you fully understand the types of machines you will be installing the agent on with regard to hardware and software specifications as well as other possible software that might conflict with the installation process. As always, a pilot, documentation of the scripts and processes, and user training of the new product are recommended for making the installation of your newest security tool a success.

In the next chapter, you continue to explore CSA. The next chapter covers the local GUI itself, its options, and its interaction with the user. You will also discover some local agent files that prove useful when troubleshooting a local policy interaction with the system as well as the agent interaction with the remote CSA MC server.