

CiscoWorks VPN/Security Management Solution FAQs

Document ID: 42861

Questions

Introduction

CiscoWorks Management Center for VPN Routers (Router MC)

CiscoWorks Auto Update Server (AUS)

CiscoWorks Management Center for Firewalls (Firewall MC)

CiscoWorks Management Center for IDS Sensors (IDS MC)

CiscoWorks Monitoring Center for Security (Security Monitor)

CiscoWorks Management Center for Cisco Security Agents (CSA MC)

CiscoWorks Monitoring Center for Performance (Performance Monitor)

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document contains frequently asked questions (FAQs) about VPN / Security Management Solution (VMS), which includes these components:

- CiscoWorks Management Center for VPN Routers (Router MC)
- CiscoWorks Auto Update Server (AUS)
- CiscoWorks Management Center for Firewalls (Firewall MC). [This component was known as Management Center for PIX Firewalls in earlier versions.]
- CiscoWorks Management Center for IDS Sensors (IDS MC)
- CiscoWorks Monitoring Center for Security (Security Monitor)
- CiscoWorks Management Center for Cisco Security Agents (CSA MC)
- CiscoWorks Monitoring Center for Performance (Performance Monitor)

Refer to CiscoWorks VPN / Security Management Solution Installation FAQs for additional information on VMS installation.

Note: This document is written specifically for the VPN / Security Management Solution for Windows, but the concepts are also relevant for Solaris versions.

Refer to the Conventions Used in Cisco Technical Tips for more information on document conventions.

CiscoWorks Management Center for VPN Routers (Router MC)

Q. Where can I find Router MC documentation and product support information?

A. Refer to the Router MC technical documentation and Router MC support page.

Q. Where can I download the latest versions and patches for Router MC?

A. Refer to Router MC software downloads (registered customers only) .

Q. Where can I find information on existing bugs for Router MC?

A. Details on existing bugs can be found in the Bug Toolkit for Router MC (registered customers only) .

Q. I cannot import my router into Router MC using the "Single device import" option. How can I fix this?

A. Use this checklist to troubleshoot this issue:

- ◆ Ensure that Secure Shell (SSH) is configured and that the VMS server can access the router via SSH. Refer to Configuring Secure Shell on Routers and Switches Running Cisco IOS in order to configure SSH.

Note: Router MC communicates with the router via SSH only. Telnet is not supported.

- ◆ Ensure that the router hardware and software are supported. Refer to Router MC Device Support Tables for compatibility information.

Refer to the Router MC User Guide for more information.

Q. How do I configure NAT on the VPN hub router using Router MC?

A. Use beginning and ending commands in order to configure Network Address Translation (NAT) on the VPN hub router. NAT translation rules are used only for spoke routers and are not supported for the VPN hub router. Refer to Configuring Translation Rules for more information.

CiscoWorks Auto Update Server (AUS)

Q. Where can I find AUS documentation and product support information?

A. Refer to the AUS technical documentation and AUS support page.

Q. Where can I download the latest versions and patches for AUS?

A. Refer to AUS software downloads (registered customers only) .

Q. Where can I find information on existing bugs for AUS?

A. Details on existing bugs can be found in the the Bug Toolkit for AUS (registered customers only) .

Q. I have a PIX firewall configured to communicate with AUS and traffic has stopped passing through. How can I fix this?

A. The PIX stops all new connections if it is configured to communicate with AUS and it has not been contacted for a period of time. An administrator can change the value of the timeout period with the command **auto-update timeout**. The Auto Update specification provides the infrastructure necessary for remote management applications to download PIX Firewall configurations, software images, and to perform basic monitoring from a centralized location. Failure to communicate with the server causes the PIX to stop passing all traffic.

CiscoWorks Management Center for Firewalls (Firewall MC)

Q. Where can I find Firewall MC documentation and product support information?

A. Refer to the Firewall MC technical documentation and Firewall MC support page.

Q. Where can I download the latest versions and patches for Firewall MC?

A. Refer to Firewall MC software downloads (registered customers only) .

Q. Where can I find information on existing bugs for Firewall MC?

A. Details on existing bugs can be found in the Bug Toolkit for Firewall MC (registered customers only) .

Q. I get the message "The MC is not fully initialized yet. Please click refresh (F5) to try again in a few seconds". What does this message mean?

A. This message can be seen both at startup and during runtime. The system is initialized successfully, but at some point a service that Firewall MC is dependent on went down temporarily, and then came back up. When this happens, the MC must re-initialize in order for the application to begin to work again.

The system can take some time to get all its services started and then initialize all its applications correctly. If you attempt to connect to the application too early, you can get this message. You can wait a few seconds and then refresh the page. You can also close the window and attempt to connect again via the link or shortcut you used previously. If the screen persists, check to make sure all the services run. If they are, reboot the system and try again. If they are not, try to restart the service from the Services control panel. If it does not successfully start there, try to cycle the system by stopping the CiscoWorks 2000 Daemon Manager service. Allow it to stop completely before you attempt to re-start the Daemon Manager. If the service still fails to start, the one option that remains is to attempt a hard reboot. If that fails, run the MDCSupport utility, save the zip file, and contact Cisco Technical Support. If the message persists, run the MDCSupport utility, save the zip file, and contact Cisco Technical Support.

Q. What are the different ways in which I can log in and access Firewall MC?

A. There are several ways to access the Firewall MC application. The standard way is to go through the main Common Management Foundation (CMF) desktop. Login, open the

VPN/Security Management Solution drawer and open the Management Center folder. You should see a PIX Firewalls link. Since you have already logged in through the CMF desktop login applet, you do not need to login again. The Firewall MC application opens for you.

Alternatively, some reports that the MC e-mails out contains a URL that allows you to login directly to Common Service and Firewall MC without the use of the CMF desktop. You can generate a URL of your own to bookmark if you wish. This URL takes you to a plain HTML based login page with no applets involved. Once you log in, it takes you to the URL that you originally attempted to go to. The form of this URL is '

`https://<hostname>/MDC/servlet/direct?url=<url that you want to go to>'. This is how a URL appears in order for it to take you to the main page of the Firewall MC:`

◆ `https://<hostname>/MDC/servlet/direct?url=/pixmdc/pixmdcServlet?locId=0`

Q. What are the ramifications if the IP address of the machine changes for Firewall MC?

A. Neither the Common Services framework, nor the Firewall MC application is designed to deal with the IP if it changes on the fly. If the IP of the system changes, restart the CiscoWorks 2000 Daemon Manager. This can be accomplished via the Services control panel. You can also reboot the system. When the Daemon Manager comes back up, the system works as it did before.

Q. What are Dependency Holds?

A. Each application is dependent on some set of the services provided by the Common Services component of VMS. Common Services has a framework in place for applications to register their dependencies and receive notification of the status of those services. When the application receives notification of a dependent service changing its operational status, the application can take whatever actions it determines are necessary. When a service that the application is dependent on is in a state where the application itself cannot proceed, then a hold is put on the application based on this dependency. The application holds the user at the current location and does not allow them to proceed until the dependent service provides notification that it is in a condition where the application may continue.

Q. Why does my system startup and have Dependency Holds in place right away?

A. If you launch Firewall MC and there are dependency holds in place right away, this is typically an error condition. If it is a case of the system still initializing for some reason, you receive a different error. The first thing to do in this case is to check the error message on the page to see what dependencies place holds. The message itself can point you in the correct direction. If not, check the Services control panel for the relevant services and check their status. If they all run correctly, you might want to wait and see if the system eventually comes up. If some or all of them do not run, stop the CiscoWorks 2000 Daemon Manager, and then restart it. If the error persists, run the MDCSupport utility, save the file somewhere else, and reboot the system.

If the reboot fails to resolve the situation, collect the logs from CSCOPx/logs, run (from the CiscoWorks Desktop) the **Server Configuration > Diagnostics > Collect Server Info** and retrieve the file it generates, run MDCSupport, and run **netstat a** with and without Daemon Manager running. Package all of this data and contact Cisco Technical Support.

Q. What does it mean when I receive a "File not found", "Cannot find server", or "Page cannot be displayed" error when I try to use Firewall MC?

A. This typically means that you connect to the server correctly, but for some reason the resource that you attempt to reach cannot be found. Check the URL or the link that you use. In order to do this, look in the address bar of the window that you use. If it is not displayed, use the **View > Toolbars > Address Bar** menu to display it. If this appears correct, ensure that a larger error is not the cause. Check to make sure all the services are up and running. Also, check to ensure the hostname and IP address of the server system are correct. Finally, attempt to determine if a port conflict is affecting the Common Management Foundation (CMF) or Common Services web servers. This case is especially likely if you have IIS or other servers running, and if you receive the "Page cannot be displayed" message in the main window. If all of this looks correct, run the MDCSupport utility and save the file somewhere else try to reboot the system.

If a reboot fails to resolve the situation, collect the logs from CSCOpX/logs, run (from the CiscoWorks Desktop) the **Server Configuration > Diagnostics > Collect Server Info** and retrieve the file it generates, run MDCSupport, and run **netstat a** with and without Daemon Manager running. Package all of this data and contact Cisco Technical Support.

Q. What does it mean when I receive a blank page when I attempt to use Firewall MC?

A. This typically means that something has failed in the actual operation of the application. If the blank page immediately happens in the initial launch of the Firewall MC, check to see if the system was installed correctly and that the Administrator level user and password for the services are all still valid.

Note: The password is only a concern for versions before 1.1.2.

If the blank page comes up during operation, check to see if all the services still run. If they are not, attempt to restart the stopped services. If this fails, or if they are all running, run MDCSupport, save the zip file somewhere else, and try to cycle the system by stopping and restarting the CiscoWorks 2000 Daemon Manager service. If this fails, attempt a reboot of the system.

If a reboot fails to resolve the situation, collect the logs from CSCOpX/logs, run (from the CiscoWorks Desktop) the **Server Configuration > Diagnostics > Collect Server Info** and retrieve the file it generates, run MDCSupport, and run **netstat a** with and without Daemon Manager running. Package this data and contact Cisco Technical Support.

Q. What does it mean if I can see the Object Selector applet but all of my groups and devices are missing?

A. This question deals with cases where any applet has loaded but the data has not initialized correctly. For example, with the Object Selector, you would see the standard background of the applet (greenish color) but no devices or groups.

This is the result of a known problem with SSL support for applets that use the JRE within the Cisco Management Foundation (CMF) framework. What happens is that if the CMF web server is in SSL mode when a client browses to the server using the normal URL

(http://<hostname>:1741), an SSLPluginInitializer is run on the JRE. This causes connections from the applets to the Core web server to break.

Note: A CMF web server is in SSL mode with standard VMS 2.2 installations.

This problem will be fixed in VMS Service Pack 2. The current workaround is to use the **https://<hostname>:1742/login.html** URL to browse to the desktop instead of the normal one.

This URL bypasses the SSL initialization and allows applet connections to work correctly through the JRE. An alternative approach is to install JRE 1.4.1_02 on the client machines. This JRE is more robust and can handle the situation that the SSL initialization causes.

Cisco bug ID CSCeb45521 (registered customers only) is used to track this for Firewall MC.

Q. How do I run MDCSupport?

A. Within the Firewall MC, under the Admin tab, there is a Support link. This link takes you to a page that displays a path, a Browse button, and an Execute button. You can set the location for the support file to be built using the textfield or the **Browse** button. You can also hit the **Execute** button to create the support file.

If your system is in a state where you cannot launch Firewall MC, or you would rather not disturb the state of the system any further, the MDCSupport executable is on the system path for your convenience. From any command prompt or shell, you can enter **MDCSupport** to generate the file. In this command line case, the file is written to the CSCOpX/MDC/etc directory. In either case, the file is generated with the name MDCSupportInformation.zip and it overwrites any existing file that is at that location. Be sure to save your file elsewhere and with a unique name so that you can identify it later.

Q. What does the MDCSupport package gather?

A. The MDCSupport executable gathers several log and configuration files that are related to the operation of the Common Services infrastructure, and the Firewall MC itself. These files include:

- ◆ The configuration and log files for the Apache web server located at CSCOpX/MDC/Apache/conf and CSCOpX/MDC/Apache/logs.
- ◆ The configuration and log files for the Tomcat servlet engine located at CSCOpX/MDC/Tomcat/conf and CSCOpX/MDC/Tomcat/logs. The important ones here are the stdout.log and stderr.log for the Tomcat process.
- ◆ A full copy of the KRS database.
- ◆ A full copy of the Sybase database.
- ◆ All the operations and audit logs for applications using Common Services which are located at CSCOpX/MDC/log and CSCOpX/MDC/log/audit.
- ◆ The Core Client Registry (CCR) stored at CSCOpX/MDC/etc/regdaemon.xml.
- ◆ Diagnostic information collected about your system.
- ◆ Installation logs for all CiscoWorks 2000 related install activity on this system.

Q. Are these any other useful log files and why are they not packaged up with the MDCSupport?

A. When an attempt is made to troubleshoot a problem on the system, other useful information exists that Cisco can use which is not currently collected by the MDCSupport utility. This information includes:

- ◆ Any log file of the form `hs_err_pid*.log` located in the `CSCOpX/MDC/tomcat` directory. An example of one of these files look like `hs_err_pid1396.log`. These log files are normally a result of hard crashes to the tomcat process and should not be that common to see. (These are now included in the support file in 1.2.)
- ◆ The `CoreTib.log` file located under the `CSCOpX/logs` provides information about the Core tibco process.
- ◆ The CiscoWorks desktop also provides a diagnostic tool to gather some extra information that can be useful. Under the Server Configuration drawer, there is a Diagnostics folder. This folder contains a link called 'Collect Server Info'. This link generates an HTML page that concatenates and formats several useful pieces of information into one file for easier access.
- ◆ The log files for the JRun servlet engine can provide some insight as well. These are located at `CSCOpX/lib/jrun/<finish log path> MMF`.

Q. What commands are supported or explicitly not supported on this version of Firewall MC?

A. Refer to the CiscoWorks Management Center for Firewalls Device Support Tables documentation specific to your version of Firewall MC.

Q. What users are allowed to install Firewall MC, and why?

A. The same user who installs Common Services must install Firewall MC. The reason for this is that Firewall MC makes use of the FMS and LM services which are tied to the user and their password. If another user installs Firewall MC, or the original user's password changes in between the installation of Common Services and Firewall MC, then the database fails to initialize correctly. The user also receives this error message when an attempt is made to use Firewall MC:

```
Error: The scope is set back to Global
```

The original user must run a re-install of Firewall MC, and elect to re-initialize the database in order to fix this. This error is resolved in version 1.1.2.

Q. I cannot import my firewall into Firewall MC using the "Import configuration from a device" option. How can I fix this?

A. Use this checklist to troubleshoot this issue:

- ◆ Ensure that HTTPS (Secure Socket Layer [SSL]) is configured on your firewall and that the VMS server is permitted to access your firewall via HTTPS. Use the **http server enable** command and the **http vms_server_ip_address 255.255.255.255 fw_interface** command.
- ◆ Test HTTPS access from Firewall MC to the firewall. Use Internet Explorer and go to **https://ip_address/exec/show%20config** where *ip_address* is the IP address of the firewall. If authentication, authorization, and accounting (AAA) is not configured for HTTPS, type the **enable** password when prompted. You do not need to type a username. If AAA is configured for HTTPS, type the username and password when prompted.

- ◆ Ensure that your firewall, software version, and commands are supported by Firewall MC. For compatibility information, refer to Firewall MC Device Support Tables.

Q. I currently manage my firewall using CSPM. How can I migrate to Firewall MC?

A. You must import the firewall configuration directly into Firewall MC in order to migrate from Cisco Secure Policy Manager (CSPM) to Firewall MC. There is no tool to convert the CSPM database to the Firewall MC format.

Q. I have a large configuration, which takes a long time to deploy to my firewall. How can I fix this?

A. PIX versions earlier than 6.2(2) and Firewall Services Module (FWSM) versions earlier than 2.2 support a single command for each HTTPS connection. Firewall MC issues approximately four commands per second because of this limitation. This limitation does not apply to PIX versions 6.2(2) and later or FWSM versions 2.2 and later. These software versions support a bulk deploy capacity that allows Firewall MC to issue all commands through one HTTPS connection.

Note: Firewall MC contacts the firewall, downloads the current configuration, compares it to the current generated configuration, and issues only the new or changed commands.

Q. Connections through the firewall are dropped after I deploy a configuration through Firewall MC. How can I fix this?

A. When a configuration is deployed through Firewall MC, the **clear xlate** command is issued and connections on the firewall are dropped. Select **Configuration > MC Settings > Management** and uncheck the **Clear XLATE on Deployment** check box in order to disable this feature.

Note: Cisco does *not* recommend that you disable the Clear XLATE on Deployments feature. Translation information needs to be cleared using the **clear xlate** command after you add, change, or remove the **aaa-server** , **access-list** , **alias** , **global** , **nat** , **route** , or **static** commands in your configuration.

CiscoWorks Management Center for IDS Sensors (IDS MC)

Q. Where can I find IDS MC documentation and product support information?

A. Refer to the IDS MC technical documentation and IDS MC support page.

Q. Where can I download the latest versions and patches for IDS MC?

A. Refer to IDS MC software downloads (registered customers only) .

Q. Where can I find information on existing bugs for IDS MC?

A. Details on existing bugs can be found in the Bug Toolkit for IDS MC (registered customers only) .

Q. Where can I download the latest IDS Sensor updates?

A. Updates are available for IDS version 4.x and IDS version 3.x.

These updates are used for several purposes:

- ◆ Update IDS Sensors using IDS MC.
- ◆ Update IDS MC.
- ◆ Update Security Monitor.

Note: IDS MC updates Security Monitor automatically if it resides on the same server.

Q. Can I receive e-mail notifications when a new IDS Sensor update is available?

A. You can receive e-mail notifications for new updates and the latest product news when you subscribe to the IDS Active Update Bulletin.

Q. Can IDS MC support version 3 and 4 Sensors simultaneously?

A. Yes, IDS MC versions 1.1 and later can monitor legacy (Version 3) PostOffice protocol Sensors as well as newer generation (Version 4) Remote Data Exchange Protocol (RDEP) Sensors. Refer to IDS MC Device Support Tables for compatibility information.

Q. What IDS Sensor hardware and software versions does IDS MC support?

A. For compatibility information, refer to IDS MC Device Support Tables. IDS Sensors running software versions earlier than version 3.0 are not supported.

Q. Can I import into IDS MC my Cisco router that runs Cisco IOS® software with the IDS feature set?

A. A Cisco IOS router that runs the IDS feature set can be configured to send alarms to a syslog server or IDS Director via the PostOffice protocol. IDS MC does not support the Cisco IOS router PostOffice configuration, but Security Monitor can support syslogs from a Cisco IOS router.

Q. I currently manage my firewall with the use of CSPM. How can I migrate to IDS MC?

A. You must import the IDS Sensor configuration directly into IDS MC in order to migrate from Cisco Secure Policy Manager (CSPM) to IDS MC. There is no tool to convert the CSPM database to the IDS MC format.

Q. I cannot import my IDS Sensor into IDS MC. How can I fix this?

A. Use this checklist to troubleshoot an IDS Sensor that runs version 4:

- ◆ Record the current version that runs on your Sensor with the **show version** IDS command.

- ◆ Ensure that your IDS Sensor is supported by the IDS MC version that you are running. Refer to IDS MC Device Support Tables for compatibility information.
- ◆ Ensure that the VMS server is included in the list of allowed hosts. In order to check, type the **show config | i accessList** IDS command. If your VMS server is not listed, refer to Adding Trusted Hosts. You can also use the **setup** command, which allows you to modify the access list. For more information on the **setup** command, refer to "Initializing the Sensor" in Cisco Intrusion Detection System Appliance and Module Installation and Configuration Guide Version 4.1.
- ◆ Ensure that you can use Secure Shell (SSH) to connect to the Sensor from IDS MC using the **plink -ssh username@ip_address_of_sensor** DOS command.
- ◆ Ensure that the exact version is installed in IDS MC. Select **Devices > Sensor** and add a Sensor without checking the box for Discover Settings in order to check your version. Click **Next** and view the drop-down list for the Version field. If the exact version is not installed, you should receive an error message that instructs you to update the signature and try again. Refer to Updating IDS Sensor Software Versions and Signature Release Levels in order to update IDS MC.

Note: Software versions must match exactly between the IDS Sensor and the IDS MC applied signature update in order to successfully import the IDS Sensor. For example, if you run version 4.1(4)S105 on the IDS Sensor, you need to ensure that you apply IDS-sig-4.1-4-S105.zip to IDS MC.

A. Use this checklist to troubleshoot an IDS Sensor that runs version 3:

- ◆ Record the current version running on your Sensor using the **nrvers** or **idsvers** command.
- ◆ Ensure that your IDS Sensor is supported by the IDS MC version that you run. Refer to IDS MC Device Support Tables for compatibility information.
- ◆ Ensure that the VMS server is included in the hosts.allow file. Type the **more /etc/hosts.allow** UNIX command in order to check this. If your VMS server is not listed, log in as root and type the **sysconfig-sensor** command, and then type **5** to choose the option for **Access Control List**. Refer to "Initializing the Sensor" in Cisco Intrusion Detection System Sensor Configuration Note Version 3.1 for further information.
- ◆ Use the command **nrconns** on the IDS Sensor to ensure that the PostOffice information is correct and to verify that the Sensor communicates with IDS MC. Compare the contents of the hosts, destination, organizations and routes files between the IDS Sensor (located in directory /usr/nr/etc) and IDS MC (located in directory *install-dir*\Program Files\CSCOpX\PostOffice\etc).
- ◆ Ensure that the exact version is installed in IDS MC. In order to check your version, select **Devices > Sensor** and add a Sensor without checking the box for Discover Settings. Click **Next** and view the drop-down list for the Version field. If the exact version is not installed, you receive an error message that instructs you to update the signature and try again. Refer to Updating IDS Sensor Software Versions and Signature Release Levels in order to update IDS MC.

Note: Software versions must match exactly between the IDS Sensor and the IDS MC applied signature update in order to successfully import the IDS Sensor. For example, if you run version 3.1(5)S82 on the IDS Sensor, you need to ensure that you apply IDS-sig-3.1-5-S82.zip to IDS MC.

If you continue to experience problems, contact Cisco Technical Support. Provide the Technical Support engineer with details of the information in the checklists in this document in order to aid in a prompt resolution.

Q. How can I upgrade my IDS Sensor using IDS MC, IDS MC and Security Monitor?

A. Refer to Updating IDS Sensor Software Versions and Signature Release Levels.

Q. How can I determine if the IDS Sensor update was applied?

A. There are multiple ways to determine if the IDS Sensor update was applied, and include:

- ◆ For a Version 4 IDS Sensor, type the **show version** command. For a Version 3 IDS Sensor, type the **nrvers** or **idsvers** command.
- ◆ Run an Audit Log Report in IDS MC. For additional information on how to run an Audit Log Report, refer to **step 15** in the Updating IDS Sensor Software Other than from 3.x to 4.x section of the *Task List for Configuring Sensors and Signature Settings* documentation.

Q. IDS MC reports the Sensor version incorrectly. How can I fix this?

A. In order to ensure that there is no mismatch between the reported IDS Sensor version and the actual IDS Sensor version, use IDS MC version 1.2(3) or later with the latest patch. Earlier IDS MC versions ignore errors that are returned from the IDS Sensor and do not re-query the IDS Sensor to ensure that the update is applied. These issues are consolidated under Cisco bug ID CSCec42665 (registered customers only) . Remove the IDS Sensor, and then re-import the Sensor using the option for Discover Settings in order to resolve the issue.

Q. I cannot upgrade my IDS Sensor using IDS MC. How can I fix this?

A. Use this checklist to troubleshoot this issue:

- ◆ Refer to the readme file for the Sensor to ensure that the current Sensor version is supported for the update.

Note: The readme file can be downloaded with the updates for IDS version 4.x and IDS version 3.x.
- ◆ Ensure that IDS 4210 and 4220–E Sensors have a minimum of 512 MB of RAM if you are upgrading to version 4.1. Refer to Intrusion Detection System 4.1 Software Memory Requirements for more information.
- ◆ Ensure that you download and use a ZIP file to upgrade the Sensor. If you do not use a ZIP file, IDS MC displays an error message that the update package may be corrupt. Refer to the updates for IDS version 4.x and IDS version 3.x to download the ZIP files.
- ◆ Ensure that the Sensor can contact IDS MC via HTTPS (TCP port 443).
- ◆ Ensure that the time setting on the VMS server is close to that on the IDS Sensor. If the time difference is greater than 24 hours, problems are encountered.
- ◆ Issue the **show version** command to ensure that all daemons are running on the IDS Sensor for version 4 Sensors or **nrconns** for version 3 Sensors.
- ◆ Ensure that the Apache Certificate is valid. For more information, see How can I validate the Apache Certificate and generate a new certificate on the VMS Server?. If a new Apache certificate is generated, ensure that the old certificate is removed and the new certificate is imported on the IDS Sensor by issuing the commands **no tls trusted-host <ip address of MC>** and **tls trusted-host <ip address of MC>**. Refer to Cisco bug ID CSCed75423 (registered customers only) for more information.

- ◆ If the link between IDS MC and the IDS Sensor is slow, ensure that IDS MC is running version 1.2 or later. In earlier versions of IDS MC, an update to an IDS Sensor must be transferred within 30 minutes or the update fails. This issue is logged as Cisco bug ID CSCea55080. For more information, refer to Release Notes for Management Center for IDS Sensors 1.2 and Monitoring Center for Security 1.2.
- ◆ If you experience issues with database connection, you may be unable to upgrade the IDS Sensor or the IDS MC itself, and you may be unable to access many components within IDS MC. Ensure that IDS MC version 1.2.3 or later is installed with the latest patch. This issue is logged as Cisco bug ID CSCsa08592 (registered customers only) .
- ◆ If you are running Network Address Translation (NAT) between the IDS MC and the IDS Sensor, ensure that IDS MC Version 1.2.3 or later is installed with the latest patch. This feature is logged as Cisco bug ID CSCsa04030 (registered customers only) .
- ◆ Ensure that the IP address of the VMS server running IDS MC has not changed since it was installed. IDS MC issues the **upgrade** command to the Sensor and indicates where the update package exists. The old IP address is issued unless IDS MC is modified with the new IP address information. For information on how to make the changes, see Can I change the IP address of the VMS Server running IDS MC?.
- ◆ Enable debugs by following the steps to debug sensor upgrade and configuration deployments in IDS MC.

If you continue to experience problems, contact Cisco Technical Support for further troubleshooting. Provide the Technical Support engineer with details of the information in these checklists to aid in prompt resolution.

Q. I cannot deploy the configuration to the IDS Sensor using IDS MC. How can I fix this?

A. Use this checklist to troubleshoot this issue:

- ◆ Ensure that you have deployed the IDS Sensor configurations made in IDS MC. Refer to Generating, Approving, and Deploying Sensor Configurations for information on how to deploy Sensor configurations.
- ◆ Ensure that there is no mismatch between the Sensor version reported by IDS MC and the actual Sensor version.
- ◆ Ensure that IDS MC version 1.2.3 or later is installed. Configuration deployments may not be completed in earlier versions of IDS MC. This issue is logged as Cisco bug ID CSCsa02920 (registered customers only) .
- ◆ Complete the steps in debug sensor upgrade and configuration deployments in IDS MC to enable debugs.

If you continue to experience problems, contact Cisco Technical Support for further troubleshooting. Provide the Technical Support engineer with details of the information in these checklists to aid in prompt resolution.

Q. How can I delete pending jobs in IDS MC?

A. Select the Admin tab, click on **System Configuration** and then **View Current Locks** to get a list of pending jobs in IDS MC. Select the Configuration tab and click **Pending** to delete the pending job. Check the relevant job and click **Delete**.

Q. How do I debug Sensor upgrade and configuration deployments in IDS MC?

A. Complete these steps to collect debugs on IDS Sensor version 4:

1. Use Notepad to open *install-dir\MDC\etc\ids\xml\DeploymentConfig.xml*. Keep a backup of this file.
2. Set `DebugEnabled` and `CliLog` to **true**. The default value is "false."
3. Save and close the file.
4. Select **Server Configuration > Administration > Process Management**, stop the **IDS_DeployDaemon** process, and then start the process again.
5. Perform the intended function on the IDS Sensor (for instance, deploy the configuration or upgrade).
6. Check the debug logs to see the commands that the IDS MC sends to the IDS device.

Note: The location of the CLI log files are referenced in the debug logs.

◇ Debug information for Sensor configuration deployments is stored in *install-dir\log\IDS_DeploymentDebug.log*.

◇ Debug information for Sensor upgrades is stored in *install-dir\log\IDS_SensorInterfaceDebug.log*.

A. Complete these steps to collect debugs on IDS Sensor version 3:

1. Use Notepad to open *install-dir\MDC\etc\ids\xml\DeploymentConfig.xml*. Keep a backup of this file.
2. Set `DebugEnabled` to **true**. The default value is "false."
3. Set `CleanupTempFiles` to **false**. The default value is "true."
4. Save and close the file.
5. Select **Server Configuration > Administration > Process Management**, stop the **IDS_DeployDaemon** process, and then start the process again.
6. Deploy a configuration to the IDS Sensor.
7. Check the debug logs to see the commands that the IDS MC sends to the IDS device.
 - ◇ Debug information for Sensor configuration deployments is stored in *install-dir\log\IDS_DeploymentDebug.log*.
 - ◇ Debug information for Sensor upgrades is stored in *install-dir\log\IDS_SensorInterfaceDebug.log*.

Note: When you are finishing debugging, reset the value for `DebugEnabled` and `CliLog` back to **false** and the value for `CleanupTempFiles` to **true**. These settings ensure that the log files do not get too large or consume large amounts of disk space.

A. Contact Cisco Technical Support for further troubleshooting if you continue to experience problems. Provide the Technical Support engineer with details of the information in these checklists to aid prompt resolution.

Q. Can I change the IP address of the VMS server running IDS MC?

A. Cisco does not recommend that you change the IP address of the VMS server after installation. If you must change the IP address of the VMS server, complete these steps to ensure that IDS MC operates properly:

1. Stop the service daemon manager.
2. Use Notepad to open *install-dir\MDC\etc\ids\xml\SystemConfig.xml*.
3. Change the `<HostIP>` value to the new IP address.
4. Save the modified file.
5. Copy the modified file to *install-dir\MDC\Tomcat\vms\ids-config\web-inf\classes\com\cisco\nm\mdc\ids\common\SystemCo* and *install-dir\MDC\Tomcat\vms\ids-monitor\web-inf\classes\com\cisco\nm\mdc\ids\common\SystemC*
6. Use Notepad to open *install-dir\PostOffice\etc\routes*.
7. Change the host name and IP address to the new values.

8. Save the modified file.
9. Start the service daemon manager.

Note: If you have any Sensors in the system, you must modify every Sensor individually. In addition, you must select **Configuration > Settings > Communications > Remote Hosts** and change the IP address to your new address.

Q. How can I validate the Apache Certificate and generate a new certificate on the VMS Server?

A. Complete these steps to validate the Apache Certificate on the VMS Server:

1. Open a DOS command prompt
2. Type the command **cd install-dir/CSCOpX/MDC/apache/conf/ssl**.
3. Type the command **keytool printcert file server.cert**. This command provides the Apache Certificate details including when it will expire.

Note: Part of the VMS Installation creates an Apache certificate that expires in one year.

A. Complete these steps if the certificate is no longer valid and a new certificate needs to be generated:

1. Stop the CiscoWorks Daemon Manager.
2. Open a DOS command prompt.
3. Type the command **cd install-dir/CSCOpX/MDC/apache**.
4. If you want to generate a certificate that has a longer validity period than one year, edit the file `gencert.bat` and change the value 365 located at the end of the file to a larger value. For example, 3650 is about 10 years.
5. Type the command **gencert**. This command creates a new certificate.
6. Start the CiscoWorks Daemon Manager.

Q. Where can I find a complete list of IDS Signatures on Cisco.com?

A. Refer to the Cisco Secure Encyclopedia (registered customers only) for a complete list of IDS Signatures. This resource is also known as the Network Security Database.

CiscoWorks Monitoring Center for Security (Security Monitor)

Q. Where can I find Security Monitor documentation and product support information?

A. Refer to the Security Monitor technical documentation and Security Monitor support page.

Q. Where can I download the latest versions and patches for Security Monitor?

A. Refer to Security Monitor software downloads (registered customers only).

Q. Where can I find information on existing bugs for Security Monitor?

A. Details on existing bugs can be found in the Bug Toolkit for Security Monitor (registered customers only) .

Q. How do I add my IDS Sensor to Security Monitor?

A. Follow these steps to add your IDS Sensor:

- ◆ If you imported the Sensor into IDS MC, click the Devices tab and select **Import**. Type your login information for the IDS MC server (not the Sensor). Security Monitor connects to the IDS MC server (usually the same machine) and imports the list of Sensors.
- ◆ If you did not import the Sensor into IDS MC, click the **Devices** tab and select **Add**. Choose the appropriate device type, and then type the device information. Select **Monitor > Connections** to verify connectivity between the IDS Sensor and Security Monitor.

Note: Cisco recommends that you import the IDS Sensor into IDS MC before you import the Sensor into Security Monitor.

Q. My Sensor shows connection status as Not Connected . How do I fix this?

A. Use this checklist to troubleshoot IDS Sensor version 4:

- ◆ Verify TCP ports 22 and 443 have connectivity between the VMS server and the Sensor.
- ◆ Type the **show version** command to verify that all processes are running on the IDS Sensor. Reboot the Sensor if any process does not run.

Use this checklist to troubleshoot IDS Sensor version 3:

- ◆ Verify UDP port 45000 connectivity between the VMS server and the Sensor.
- ◆ Type the **nrconns** command to verify that the IDS Sensor can communicate with the VMS Server.
- ◆ Verify that the IDS PostOffice settings on Security Monitor match the settings on the IDS Sensor. The "orgname" setting is case sensitive and must be exactly the same on both devices. Follow these steps to change the PostOffice settings:

- ◇ On Security Monitor, select **System Configuration > PostOffice Settings**.
- ◇ On the the IDS Sensor, log in as root and type the **sysconfig-sensor** command.

Q. My Sensor shows connection status as Indeterminate . How do I fix this?

A. Select **Server Configuration > Administration > Process Management > Process Status** to check the status of the IDS_Receiver process on the VMS server. Restart the process if it has stopped. Try these suggestions if the process continues to stop automatically:

- ◆ Check the *install-dir/CSCOpX/log/IDS_Receiver.log* file.
- ◆ Run an audit log report that shows the IDS_Receiver subsystem messages.

Contact Cisco Technical Support for further troubleshooting if you continue to experience problems. Provide the Technical Support engineer with details of the information in these checklists to aid in a prompt resolution.

Q. I cannot see alerts from my IDS Sensors in Security Monitor. How do I fix this?

A. Use this checklist to troubleshoot IDS Sensor version 4:

- ◆ Verify that Security Monitor shows the IDS Sensor connection status as "Connected."
- ◆ Type the **show interface** command to verify that the sensing interface is up on the IDS Sensor. If the interface is not up, select **Configuration > Settings > Interfaces** to enable the interface in IDS MC, and then deploy the configuration to the Sensor.
- ◆ Type the **show interface** command to verify that the sensing interface can see traffic. Check the statistics under the Virtual Sensor section, and look specifically at these counters:

```
Alarm Statistics for this Virtual Sensor
Number of alarms triggered by events = 2543
Number of alarms excluded by filters = 0
Number of alarms removed by summarizer = 1654
Number of alarms sent to the Event Store = 320
```

Use this checklist to troubleshoot IDS Sensor version 3:

- ◆ Type the **nrconns** IDS Sensor command to verify that the Sensor can communicate with the Security Monitor.
- ◆ Verify that Security Monitor shows the IDS Sensor connection status as "Connected."
- ◆ Type the **nrstatus** command to verify that the packetd daemon is running on the IDS Sensor. If the packetd daemon is not running, push a configuration from IDS MC to the Sensor, which should start the daemon. If the daemon still does not start, edit the `/usr/nr/etc/daemons` file, and then add `nr.packetd`. To restart the Sensor, type the **nrstop** command, and then type the **nrstart** command.
- ◆ Verify that the sniffing interface can see monitored traffic correctly. Log in as root and type the **snoop** command.

Q. I cannot see any syslog events from my PIX or IOS router in Security Monitor. How can I fix this?

A. Use this checklist to troubleshoot this issue:

- ◆ Ensure that your PIX or IOS router is set up correctly to send syslog messages to Security Monitor. Select **Admin > System Configuration > SYSLOG Settings** to check that the setting matches the UDP port number that the device uses. Refer to *Configuring Devices to Monitor* for information on how to configure devices to send syslog data.

Note: You do not need to check the Forward Syslog Messages box unless you want to forward the events to another syslog server.

- ◆ Add the device into Security Monitor from the Devices tab to ensure that the device name appears in the Event Viewer. When you start the Event Viewer, ensure the Event Type is set to one of the syslog types. The "PIX Security Summary" should show you all syslog data received. In order to access the PIX Security Summary, in Security Monitor go to the tab Monitor, select **Events** (this is where the Event Viewer can be launched from). Select **PIX Security Summaries** in the drop down menu for

the Event Type field before launching the Event Viewer.

- ◆ Ensure that the **CWCS syslog** service on the VMS server has started correctly. If this service fails to start correctly, check the size of the *install-dir*\Program Files\CSCOpX\log\syslog.log file. If this file is quite large, clear the file or move it to an alternate location, and then restart the service.

Q. I see thousands of "ICMP Unreachable" syslog messages between my PIX and VMS server. What is happening?

A. In this case, the PIX is set to send syslog messages to Security Monitor, but the syslog service on the VMS server that accepts these messages is down. The VMS server sends back an "ICMP Unreachable" message to the PIX. The PIX receives the error message and sends another syslog message to Security Monitor to report the error. The two devices get stuck in an endless loop.

Use this checklist to determine why the syslog service on the VMS server is down:

- ◆ Check for available disk space.
 - ◆ Ensure that the PIX sends the syslog messages to the same UDP port that Security Monitor uses to receive messages. See I cannot see any syslog events from my PIX or IOS router in Security Monitor. How can I fix this? for more information
- If you have **ip audit** configured on the PIX, type the **no logging message 40011** command so that the PIX does not report the ICMP error messages to Security Monitor.

Q. I have e-mail alerts set up, but I want to see things like the Signature name and Signature ID within the alert? How do I do this?

A. Refer to Configure E-mail Notifications with Scripts for IDS Alerts Using CiscoWorks Monitoring Center for Security.

Q. When I go into the Event Rules screen, I get an error and / or my event rules are not there. How can I fix this?

A. In older versions, event rules can get corrupted under certain circumstances, such as when you change the name of a device that has an existing event rule. This issue is recorded as Cisco bug ID CSCea55080 (registered customers only) .

Use one of these options (listed in order of preference) to resolve this issue:

- ◆ If you modified or removed a device that had an existing event rule, add back the device that the event rule references.
- ◆ Remove the database rules with SQL commands, and then add back the rules with the GUI. Type the DOS command (all on one line)**dbisql-c "uid=idsmdc;pwd=password;dbf=path to db file\idsmdc.db;eng=sqlcoredbserver" delete top 10 from eventrule** to remove the rules.

◇ *password* is your database password as defined during installation. Contact Cisco Technical Support if you do not know your password.

◇ *path to db file* is the full path name to the idsmdc.db file.

Q. How can I back up my alert database?

A. Select **VPN/Security Management Solutions > Administration > Common Services > Back up Database** to back up the alert database. This option backs up the `idsmdc.db` and `idsmdc.log` files, which include your device and signature settings and all the received alerts.

Q. Why is the time on my alerts in Security Monitor different from my local time?

- ◆ Type the **show clock** command to verify the time settings on the Sensor.
- ◆ Type these commands to ensure that the UTC offset is correct:

```
sensor# configure terminal
sensor(config)# service host
sensor(config-Host)# timeParams
sensor(config-Host-tim)# show settings
```

- ◆ Use the **setup** command in order to configure the Sensors to use Network Time Protocol (NTP) to synchronize their clocks with an NTP server.

Note: The IDS Sensor only supports authenticated NTP.

- ◆ Verify that the time and time zone settings on the VMS server are correct.

Q. Security Monitor takes a long time to open. How do I maintain my database to prevent this?

A. The Security Monitor database is the file `install-dir\CSCOpX\MDC\Sybase\Db\IDS\idsmdc.db`. The `idsmdc.log` file in the same directory is used to keep track of database changes. It is important to maintain these files so that they do not become too large or consume all available disk space. Refer to *Maintaining the Database* for information on how to maintain database size.

VMS comes with a number of executables to help manage your database size.

- ◆ By default, Security Monitor is configured to perform a database prune when 2 million alerts are stored in the database. You can go to **Admin > Database Rules** to modify this setting so that a database prune is performed daily at a specified time, or when a certain amount of disk space is left, or according to other parameters.

Note: Under normal circumstances, this rule keeps your database file at a manageable size, but a database prune does not reduce the overall database file size. Database records are removed from the database, but the database retains the allocated space to write new records.

- ◆ The `idsmdc.log` file records database changes. A database prune increases the size of this log file, which can exacerbate the problem of low available disk space. Select **VPN/Security Management Solutions > Administration > Common Services > Back up Database** to perform a database backup in order to reset the log file size back to 0. The backup is stored in the `install-dir\CSCOpX\MDC\backup` directory and can be deleted to reclaim disk space.
- ◆ If you have already run out of usable space, you can back up the database to a different drive. Run the `IdsPruning` utility and then the `IdsDbCompact.exe` utility to shrink the actual database size and reclaim maximum disk space produced by a database prune. The `IdsDbCompact` utility writes a new copy of the database to another file. Before you remove the old database and copy the new one in its place,

you must specify that the new database is created on a separate drive with available space if there is not sufficient space on the current drive (use the **c** and **u** options).

Q. How can I keep the customization of my columns in Security Monitor?

A. This feature was introduced in Security Monitor 1.2, which is part of VMS 2.2. When you have modified the columns, select **Edit > Save Column Set**. Then select **Monitor > Events** to ensure that the Event Viewer option for Column Set is set to **Last Saved**.

Q. How do I view the Network Security Database (NSDB) from Security Monitor?

A. Click in any cell in the row to highlight the signature you are interested in from within the Event Viewer. Then Select **View > Network Security Database**, or right-click on the cell and select **View NSDB**.

Q. I cannot see Low and Informational severity alerts. How can I fix this?

A. By default, Medium is the lowest severity level for alerts sent from a Sensor to Security Monitor. This means that only Medium and High severity alerts are seen in the Event Viewer. Go to the Devices tab and edit the Sensor so that the Minimum Event Level reflects the desired severity in order to see Low and/or Informational alerts.

Note: When the Sensor is configured to display these additional severity alerts, the number of events sent to the VMS server increases dramatically. This can cause database issues if you do not perform regular database maintenance.

Q. How can I remove specific alarms from the database?

A. Go to Event Viewer and right-click in any cell in a column that shows the alerts you want to delete to delete alerts for a specific signature. Select **Delete From Database** to mark the events for removal from the database. The alerts are no longer visible within Security Monitor, but you must run the PruneMarkedForDeletion utility to remove the marked alerts from the database permanently.

Use the IdsPruning utility to delete alerts based on other criteria, such as alerts received before a certain time, alerts older than a certain number of days, or alerts of a specific severity.

Q. How can I limit the number of alarms I see for a particular signature?

A. Use IDS MC to filter and tune your signatures and alarms.

- ◆ Choose the appropriate Sensor, select **Configuration > Settings > Filters**, and then add a new filter in order to filter a signature. Filters can be based on signature and subsignature number and on source and destination addresses. When you want to filter a specific signature, verify that it is a false positive. Create the filter to be as specific as possible so that you do not filter out other potentially positive alerts.
- ◆ Choose the appropriate Sensor, select **Configuration > Settings > Signatures**, and then look for the signature that generates the large number of alarms in order to tune a signature. Click on the link in the Engine column to see the parameters for the signature. Refer to Working with Signature Engines for information on parameter

definitions.

You can tune signatures in several different ways. For example, if the AlarmThrottle parameter is set to FireAll or FireOnce, you may see a large number of alerts for the same attack. If you change this parameter to Summarize, you see an initial alert and then a summary alert delivered at a time specified by the ThrottleInterval parameter. Ensure that you fully understand the parameters you want to modify. Contact Cisco Technical Support if you need assistance.

Q. How can I reduce false positives?

A. Create a filter based on the signature and the source and destination address pair when an alert is verified to be a false positive. Choose the appropriate Sensor, select **Configuration > Settings > Filters**, and then add a new filter in order to filter the signature in IDS MC.

Q. Is there a limit to the number of events I can receive through Security Monitor?

A. There is no configured limit to the number of events Security Monitor can receive. The maximum suggested rate for received events, such as syslog and IDS, is 45 per second, with a burst rate of 500 per second for 5 minutes.

Q. I am having trouble receiving e-mail notifications of reports. How can I fix this?

A. If your version of Security Monitor is earlier than version 1.2, you should upgrade to Security Monitor version 1.2 or later. This issue is logged as Cisco bug ID CSCin33516 (registered customers only).

If your version of Security Monitor is version 1.2 and later, use this checklist to troubleshoot this issue:

- ◆ Select **Admin > System Configuration > E-mail Server** to verify that the mail server has been added.
- ◆ Launch a command prompt on the VMS server and verify that you can use Telnet to port 25 on the mail server. If this attempt is unsuccessful, check for any firewall devices between the VMS server and the e-mail servers that could block this traffic.
- ◆ Run an audit log report, and check for any Notifier errors that indicate there is a problem with the e-mail server.

Q. My standard and / or scheduled reports remain in Waiting state and do not run. How can I fix this?

A. Select **Server Configuration > Administration > Process Management > Process Status** on the VMS GUI to verify that the IDS_ReportScheduler process is running. If the process is not running, start it, and then monitor the process to ensure that it stays running.

If the process stops again, check the *install-dir*\Program Files\CSCOpX\log\IDS_ReportScheduler.log file for indications of why the service stopped.

Q. How do I get Security Monitor to send me a daily report at a specified time?

A. Complete these steps to schedule a daily alarm report:

1. Select the Reports tab.
2. Select **Generate**.
3. Choose the report that you want to run, such as IDS Summary Report.
4. Select the **Schedule for Later** radio button and **Repeat Every Day** options for the report.
5. Select the time that you want the report to generate.
6. Check the **Email Report To:** checkbox and enter the destination e-mail address for the report.
7. Click **Finish**.

Tip: If you want to schedule multiple reports, separate the reports by at least 30 minutes to avoid conflicts.

CiscoWorks Management Center for Cisco Security Agents (CSA MC)

Q. Where can I find Cisco Security Agent Frequently Asked Questions?

A. Refer to the Cisco Security Agent FAQ.

Q. Where can I find CSA MC documentation and product support information?

A. Refer to the CSA MC technical documentation and CSA MC support page.

Q. Where can I download the latest versions and patches for CSA MC?

A. Refer to CSA MC software downloads (registered customers only) .

Q. Where can I find information on existing bugs for CSA MC?

A. Details on existing bugs can be found in the Bug Toolkit for CSA MC (registered customers only) .

Q. How do I add or remove licenses in CSA MC?

◆ Use one of these options to add licenses to CSA MC:

◇ Copy the licenses to the CSA MC directory when the installation process prompts you.

or

◇ In CSA MC, select **Maintenance > License Information**, and then add the license file.

◆ Browse to *install-dir\CSCOPx\CSAMC\cfg*, and then remove or rename the .lic file(s) to remove licenses in CSA MC. Close any browsers relating to CiscoWorks.

Q. When I go to Monitor > Event Log in CSA MC, I see a critical error message that says, "Product license for profiler is invalid or has expired." CSA is working as expected. How do I keep the error events out of the log?

A. The standard CSA license does not include the profiler license. The profiler is an option that you can purchase. This issue is logged as Cisco bug ID CSCin33516 (registered customers only) .

Launch a command prompt and type these commands in order to prevent these messages:

```
net stop csagent
report_install.exe u
net start csagent
```

You can also download to CSA MC 4.0.1 or later from the Software Center (registered customers only) . This issue is resolved in these later software releases.

Q. I receive license errors in CSA MC. How can I fix this?

A. License errors in CSA MC refer specifically to the license for the MC itself. Select **Maintenance > License Information** to ensure that a valid Management Center for Cisco Security Agents license is installed.

If the license is invalid, send an e-mail to licensing@cisco.com with your company name, e-mail address, CSA product number(s) (for example, CSA-B25-DTOP-K9) and the purchase or sales order number.

Q. The Cisco Security Agent cannot register with the CSA MC. How can I fix this?

A. Refer to this checklist to troubleshoot issues with agent registration:

- ◆ Ensure that the CSAgent service is running.
- ◆ Ensure that the agent can resolve the DNS name of the CSA MC.
- ◆ Ensure that you have connectivity on TCP port 5401 or 443 between the agent and the CSA MC. Type the **icpping webadmin number** command to test connectivity from the agent.
- ◆ Ensure that the licenses for the agent are correct and valid.
- ◆ View the csalog.txt file from the agent. If an entry for "Error Code = 2035" appears in the log, then the license is invalid, has reached its limit, or is corrupted.

Contact Cisco Technical Support if you need additional assistance.

Q. How do I get my Windows Agent to register against my new CSA MC?

A. Reinstall the Cisco Security Agent using the new CSA MC. You do not need to uninstall the Cisco Security Agent that uses the old CSA MC.

Q. What ports do I need to open in my firewall to allow my agents to communicate with CSA MC?

A. These agent components and relevant ports are needed for communication to the CSA MC:

- ◆ **Registration** By default, the agents communicate to the CSA MC on TCP port 5401. If that port is not available, the agents try TCP port 443 instead.
- ◆ **Browsing** If you use a web browser to communicate to the CSA MC, open TCP ports 1741, 1742, and 443.
- ◆ **Profiler** The Profiler communicates with CSA MC on TCP port 5402.

Q. I have disabled logging for a particular rule. However, I still receive logs for this rule. Is this normal?

A. In CSA MC Version 4.0.2, these rule types are logged regardless of the configuration when the group is in test mode:

- ◆ Application Control
- ◆ COM component access control
- ◆ File access control
- ◆ File version control
- ◆ Registry access control

For all other rules types, logging is enabled or disabled as configured. In CSA MC Version 4.5 and later, the logging configuration is utilized for all rules types regardless of whether the group is in test or production mode.

Q. How do I switch an agent from test mode to production?

A. To place an agent in production mode, use the CSA management console to place the agent's group into production mode:

1. Select **Systems > Groups** from CSA.
2. Select the group that the agent is in.
3. Uncheck the **Test mode** check box in the group properties.
4. Click on **Generate rules**. The next time the agent polls the CSA MC and downloads the new setup, it is placed in production mode.

Q. Where can I get information about each policy and a description for the rules?

A. In CSA MC, select **Configuration > Policies** and select the policy you want to view. Then click the **Explain rules** link for a detailed description of each rule in the policy. This link is also available for a group where multiple policies are applied and for an individual host that may belong to multiple groups.

Q. What are the run levels for the CSA Agent on UNIX?

A. These are the run levels for the CSA Agent on UNIX:

- ◆ /etc/rc0.d/K40csa
- ◆ /etc/rc1.d/K40csa
- ◆ /etc/rc2.d/S32csatdi
- ◆ /etc/rc2.d/S77csa
- ◆ /etc/rcS.d/K40csa

◆ /etc/rcS.d/S22csanet

For information about run levels, type the **main init** command to refer to the manual for init on UNIX.

Q. In version 4.5, can the CSA MC database reside on a shared version of the SQL Server?

A. Yes, the SQLServer for the CSA MC can be a part of a SQLServer cluster.

Q. In version 4.5, is it possible to change the times that backups occur?

A. While a mechanism used to backup the local database at will has always been provided, if the SQL server is on a remote system, Cisco does not provide the capability to do backups from the MC GUI. Cisco assumes that the admin of the SQL server (which can be shared by other databases and the CSA) is responsible for the arrangement of backups.

Q. What port is required for database communication if the database is separate from the CSA MC?

A. The database communication is over ODBC to the SQL server. Therefore, the database listener port of 1433 needs to be available for connections.

Q. Do the 4.0.x license keys work with the 4.5 system?

A. Yes, the 4.0.x license keys work with the 4.5 system.

Q. What is Application Analysis?

A. In version 4.5, the former "Profiler" is replaced with the Application Analysis component. Application analysis constantly collects data and places it in a file in the directory \Cisco systems\csagent\log. This file is uploaded to the CSA MC at a minimum of once every 24 hours.

Q. I reinstalled the agent on the exact same machine but it does not register. Why is this?

A. Once you un-install your CSA agent, the Hostname of your machine remains in the host page of the CSA MC for at least one hour before it is marked as Inactive. If you need to install the CSA agent again, you need to delete the Hostname from the Host page in the CSA MC before you can re-install. If you do not wait, the CSA agent is not able to register to the CSA MC and you see an `error = 2037` (backoff registration) in the csalog file. This is in order to prevent an attack where someone tries to register unauthorized agents over and over again.

Q. Where do I get the installed applications inventory?

A. Registry values are used in order to obtain the installed applications inventory. These are the same values that the Add/Remove Programs dialog reads to populate its list. Refer to Chapter 11 of the CSA 4.5 User's Guide for more information on the functionality.

Q. How are the default groups best used?

A. In version 4.5, policy groups are cumulative, or combined in layers. All Desktop computers need to be in the "Desktop – All types" policy group.

Remote and/or laptop computers also need to be in the "Desktop – Remote or mobile" policy group. This group only has policies vital to VPN access, and therefore still need the protection of the policies in the "Desktop – All types" group.

This is the same for Servers. All servers need to be in the "Servers – All types" policy group as well as in any necessary individual groups (such as "Servers – DHCP servers").

CiscoWorks Monitoring Center for Performance (Performance Monitor)

Q. Where can I find Performance Monitor documentation and product support information?

A. Refer to the Performance Monitor technical documentation and Performance Monitor support page.

Q. Where can I download the latest versions and patches for Performance Monitor?

A. Refer to Performance Monitor software downloads (registered customers only) .

Q. Where can I find information on existing bugs for Performance Monitor?

A. Details on existing bugs can be found in the Bug Toolkit for Performance Monitor (registered customers only) .

Q. Where can I find further FAQs and a troubleshooting guide for Performance Monitor?

A. Refer to FAQs and Troubleshooting Guide for Monitoring Center for Performance 2.x.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for VPN
Service Providers: VPN Service Architectures
Service Providers: Network Management
Virtual Private Networks: General

Related Information

- [CiscoWorks VPN / Security Management Solution Installation FAQ](#)
 - [Cisco Secure Intrusion Detection System \(Versions 3.1 and Earlier\) FAQ](#)
 - [FAQs and Troubleshooting Guide for Monitoring Center for Performance 2.x](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 30, 2008

Document ID: 42861
