Troubleshooting Device Communication and Deployment

One of the more likely areas where you can run into problems is with actions where Security Manager must log into a device. These types of actions include policy discovery and deployment using live devices, or actions that involve retrieving information from a device.

The key point to remember is that the communication pathway is from the Security Manager server to the device; the workstation on which you are running the Security Manager client is not involved in device communication (unless the server is installed on the same machine, of course). The Security Manager server must have a network pathway to the device as well as the correct credentials and certificates to authenticate with the device for communication to be successful.

The following topics can help you troubleshoot general device communication and policy deployment problems:

Testing Device Connectivity

Security Manager must be able to connect to and log into a device in order to manage it. You can test whether Security Manager can use the credentials and transport method you have defined within Security Manager for this purpose.

You can test connectivity only for devices that have static IP addresses. You also cannot test connectivity for devices that use Token Management Server (TMS) as the transport protocol.

If you add a device from the network or from an inventory file to the inventory, Security Manager tests connectivity automatically.

You can manually test device connectivity for any device in the inventory or for new devices that you are adding manually. The following procedure describes how to test connectivity for devices that are already in the inventory. When adding devices manually, click **Test Connectivity** on the Device Credentials page of the New Device wizard to perform the test described below. For more information on adding devices manually, see Adding Devices by Manual Definition.

Before You Begin

Security Manager uses the settings on the Device Communication page to determine the connection timeout, how often to retry the connection, the transport protocol, and which credentials to use. To configure these settings, select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents.

Related Topics

- Understanding the Device View
- Viewing or Changing Device Properties
- Device Communication Page

Step 1 In Device view, do one of the following in the Device selector to open the Device Properties dialog box:

- Double-click a device.
- Right-click a device and select **Device Properties**.
- Select a device and select **Tools > Device Properties**.

Step 2 Select **Credentials** from the table of contents.

Step 3 Click **Test Connectivity**.

The Device Connectivity Test dialog box opens and displays the progress of the test, including the protocol being used (see Device Connectivity Test Dialog Box , on page 3). You can abort the test while it is running. When the test is finished, click **Details** to see:

- For successful tests, the output of the **show version** command or the **getVersion** command (for IPS Sensors and Cisco IOS IPS Sensors). You can select the text, press Ctrl+C to copy the text to the clipboard, and then paste it into another file for later analysis.
- For unsuccessful tests, the error information. Some common problems are:
  - The username or password is incorrect.
  - The wrong protocol is selected. For example, the device might not be configured to respond to the selected protocol.
  - The device is not configured to accept connections correctly. Ensure that at least one supported protocol is configured.
  - The wrong operating system is specified for the device (for example, you specified PIX for an ASA device).
  - If you are using ACS authentication and the connection to the device is completed, you can get errors when Security Manager tries to obtain version information if you do not have Control authorization.
  - There might be general network configuration problems. Test connectivity to the device from outside of Security Manager. Look for hardware, media, and booting errors, excessive traffic causing queues to overflow, duplicate MAC or IP addresses on the device, physical discrepancies, such as link, duplex, and speed mismatch, or logical discrepancies, such as VLAN and VTP inconsistencies or ATM network misconfiguration.

Device Connectivity Test Dialog Box

Use the Device Connectivity Test dialog box to view whether Security Manager can contact the device using the configured credentials.

Navigation Path

To start the device connectivity test, click **Test Connectivity** from the Credentials page in one of these areas:

- New Device wizard when adding a device manually. See Adding Devices by Manual Definition.
- Device Properties. To open the page, double-click a device in the Device selector or select **Tools > Device Properties**.

The connectivity test is done automatically when you click **Next** or **Finish** on the Credentials page when adding a device from the network.

Related Topics

- Testing Device Connectivity , on page 1
- Device Credentials Page
- Viewing or Changing Device Properties

Field Reference

Table 1: Device Connectivity Test Dialog Box

Element	Description
Connectivity Protocol	The transport protocol being used to log into the device. Security Manager uses the protocol specified in the device properties for the device, which is usually the default protocol configured on the Device Communications page (see Device Communication Page).
Connectivity Status	Displays the status of the test and the time elapsed since the start of the test.
Details button	Click this button to display detailed information about the result of the test. • Passed tests—The details display the output of the **show version** command for PIX Firewall, Adaptive Security Appliances (ASA), Firewall Service Modules (FWSM), Cisco IOS routers, and VPN Services Modules (VPNSM), or the output of the **getVersion** command for IPS Sensors and Cisco IOS IPS Sensors. You can copy the command output and paste it into a file for analysis. • Failed tests—The detailed error message.
Abort button	Stops the connectivity test before it is completed.

Managing Device Communication Settings and Certificates

If you discover device inventory and policies directly from devices, or deploy configurations to devices rather than to files, you must configure Security Manager to use the transport protocols that your devices use. For some device types, only one transport protocol is supported, so you do not need to make a choice. For other devices, such as Cisco IOS routers, you have options concerning the protocols you use.

Security Manager has default settings for transport protocols that are the most-used protocols for each device type. To change these settings, select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents (see Device Communication Page).

For most users, the communication settings that require management are the certificates used for SSL (HTTPS) connections and the public keys used for SSH connections. You might update the certificates and keys on the device, which would leave Security Manager holding an outdated copy.

The following topics provide more information about managing certificates and keys, and how to troubleshooting device communications:

- SSL certificates—You can configure Security Manager to automatically replace certificates using the ones obtained from the device on the Device Communication page. If you decide to manually manage the SSL certificate store, see Manually Adding SSL Certificates for Devices that Use HTTPS Communications , on page 5. The following topics provide more information about certificate errors:
  - Security Certificate Rejected When Discovering Device , on page 6
  - Invalid Certificate Error During Device Discovery , on page 7
  - Managing IPS Certificates

Tip Ensure that all PIX Firewalls and Adaptive Security Appliances that you intend to manage with Security Manager have a 3DES/AES license. See Understanding Device Communication Requirements.

- SSH Public Keys—By default, Security Manager replaces public keys with the new ones obtained during SSH connections. If you have problems with SSH communications, see Troubleshooting SSH Connection Problems , on page 7.
- General Device Communication Troubleshooting—For other problems you might encounter, see Troubleshooting Device Communication Failures , on page 8.

Multiple Certificate Authentication Support

Beginning from version 4.13, the Cisco Security Manager supports ASA 9.7.1 feature of multiple certificate authentication for VPN connectivity. ASA, in its release 9.7.1, has introduced multiple certificate authentication support to its VPN client customers. Thus, the client can authenticate remote VPN users with two client certificates. The two client certificate could be a combination of one user certificate and one machine certificate, or two user certificates. Two machine certificate authentication is not supported for security considerations. The multiple certificate authentication works for both SSL VPN and IPsec VPN.

In Cisco Security Manager 4.13, to enable the multiple certificate authentication support, you are required to appropriately specify the AAA authentication method (see AAA Tab (Connection Profiles)) and configure the DAP policy (see Add/Edit DAP Entry Dialog Box Multiple Certificate Authentication).

Manually Adding SSL Certificates for Devices that Use HTTPS Communications

Note In addition to the techniques described in this topic, for IPS devices you can use the IPS Certificates utility to manage the certificates in Security Manager's certificate data store. For more information, see Managing IPS Certificates.

When you use SSL (HTTPS) as the transport protocol for communicating with IPS, PIX, ASA, or FWSM devices, or Cisco IOS routers, you can configure Security Manager to automatically retrieve the device authentication certificate when adding the device (see Device Communication Page).

Tip Having an accurate certificate is required for successful HTTPS communications; Security Manager cannot communicate with the device without the correct certificate, which prevents configuration deployment. When using self-signed certificates, the device might create a new certificate if Security Manager attempts to access it using the wrong certificate. Thus, it is best to configure Security Manager to always retrieve the certificate from the device.

Instead of having Security Manager automatically retrieve the certificates, you can manually add them to increase the level of network security. On the Device Communication page, you would configure the device authentication setting for the device type as **Manually add certificates**.

The easiest way to manually update the certificate for a device is to retrieve it from the device. Right-click the device and select **Device Properties**. Click **Credentials** to open the Credentials page, and then click **Retrieve From Device** to the right of the **Authentication Certificate Thumbprint** field. Security Manager retrieves the certificate and prompts you to accept it. You might need to do this if you encounter certificate problems during configuration deployment. (You can also type or paste the certificate into this field.)

You can also manually type in, or copy and paste, the certificate thumbprint without having Security Manager log into the device. Use the following procedure to manually enter the SSL certificate thumbprint for a device if you configured that device type to require manually added certificates.

Tip Security Manager allows you to generate a 2048-bit self-signed certificate under **Megamenu > Server Administration > Server > Security > Single Server Management > Certificate Setup.**

Tip To reach the Megamenu, double-click the Cisco Security Manager icon on your server desktop and log on. Another way to reach the Megamenu is as follows: Windows > Start > All Programs > Cisco Security Manager > Cisco Security Manager > [log on]. This second navigation path may differ slightly, depending upon how you have personalized your Windows Server installation.

Before You Begin

Obtain the certificate thumbprint (a hexadecimal string) for the device.

Tip If the thumbprint is not readily available, you can copy it from the error message that is displayed when you add the device from the network or from an export file.

Step 1 Select **Tools > Security Manager Administration** and select **Device Communication** from the table of contents to open the Device Communication page (see Device Communication Page).

Step 2 Click **Add Certificate** to open the Add Certificate dialog box (see Add Certificate Dialog Box).

Step 3 Enter the DNS hostname or IP Address of the device, the certificate thumbprint in hexadecimal format, and click **OK**. The thumbprint is added to the certificate store.

Tip To erase an existing thumbprint, leave the Certificate Thumbprint field empty.

Security Certificate Rejected When Discovering Device

If an error occurs when you attempt to discover a device, and the error message states that the security certificate received from the device was rejected, you need to update the certificate. You can do this using one of the following methods:

- For IPS devices only, select **Manage > IPS > IPS Certificates** and synchronize the certificates. You might also need to regenerate the certificate. For more information, see Managing IPS Certificates.
- Manually enter the thumbprint required by the certificate by doing one of the following:
  - Select **Tools > Security Manager Administration > Device Communication**. Click **Add Certificate**, enter the IP address of the device, then copy and paste the thumbprint displayed in the error message into the Certificate Thumbprint field.
  - Right-click the device and select **Device Properties > Credentials**. Copy and paste the thumbprint displayed in the error message into the Authentication Certificate Thumbprint field.

You must manually enter the thumbprint whenever you add a new device using the Add New Device or Add From Configuration File options and when you perform rediscovery. It is not required when you add a new device using the Add New Device From Network or Add Device From File options.

- Configure the SSL certificate settings to automatically retrieve the certificate when adding devices. You can select different settings for IPS, router, and ASA/PIX/FWSM devices. To configure these settings, select **Tools > Security Manager Administration > Device Communication**, and look at the **SSL Certificate Parameters** group.

Related Topics

- Manually Adding SSL Certificates for Devices that Use HTTPS Communications , on page 5
- Adding Devices to the Device Inventory
- Preparing Devices for Management
- Device Communication Page

- Device Credentials Page

Invalid Certificate Error During Device Discovery

If the time settings on the device and Security Manager are not in synchronization, when you try to discover policies on a device (adding it to the inventory or rediscovering policies on a device already in the inventory), an error message might state that the certificate is not yet valid.

When the time set on the Security Manager server is lagging behind the time set on the device, Security Manager cannot validate the device certificate if the start time of the validity period is ahead of the Security Manager time setting. Even if the time zones configured on the device and Security Manager are the same, the invalid certificate error occurs if the daylight saving time (summertime) settings are different. To resolve this problem, make sure that the daylight saving time settings are the same on the device and Security Manager, regardless of whether the time zone is the same. After setting the daylight saving time, synchronize the clock on the device with Security Manager so that both of them display the same time.

To obtain best results, we recommend that you set the same time zone on the device and Security Manager, and modify the time zone after you discover the certificates at a later time, if necessary.

Related Topics

- Manually Adding SSL Certificates for Devices that Use HTTPS Communications , on page 5
- Managing IPS Certificates
- Adding Devices to the Device Inventory
- Preparing Devices for Management

Troubleshooting SSH Connection Problems

For devices that use SSH as the transport protocol, Security Manager automatically detects the appropriate SSH version (1.5 or 2) to use with each device. During SSH version 2 connections, Security Manager automatically negotiates encryption algorithms or ciphers with the device. Security Manager also automatically overwrites the SSH public key for the device if the key changes. Thus, you typically will not run into SSH connection problems.

If you do have SSH connection problems, consider these fixes:

- If the public key on the device changed, and SSH connections are failing due to a key problem, remove the key for the device from the Program Files/CSCOpx/MDC/be/tmp/.shh/known_hosts file on the Security Manager server and retry the operation.
- Security Manager uses 3DES (Data Encryption Standard) as the default encryption algorithm. If this is not the correct algorithm for your devices, either change the configuration of your devices, or update the Program Files/MDC/athena/config/DCS.properties file to indicate the correct algorithm on the DCS.ssh.encipher property. (Contact Cisco TAC if you need more help). You must restart the Security Manager daemon manager if you change this file.

Related Topics

- Preparing Devices for Management

- Device Communication Page
- Device Credentials Page

Troubleshooting Device Communication Failures

If Security Manager fails to communicate with a device, for example, by failing to log into it, during discovery, deployment, or other actions, look at these areas to identify and resolve the problem:

- Ensure the device is operational.
- Check which transport protocol is selected. You must select a protocol that the device is configured to accept. For most devices, the protocol is selected on the Device Properties General page (select **Tools > Device Properties > General**). For IPS devices, the IPS RDEP mode is selected on the device properties Credentials page.

For IOS devices that do not have a K8 or K9 crypto image, ensure that you select Telnet as the protocol.

Some methods of adding devices also allow you to select a non-default transport protocol. To configure the default transport protocols for classes of devices, select **Tools > Security Manager Administration > Device Communications**.

- On the Device Properties General page, ensure that the hostname, domain name, and IP address are correct. Keep in mind that the Hostname and Accounts and Credentials policies for the device define the actual names and credentials that get configured on the device. However, the policies are not used for device communication. If you make changes to the policies that affect the credentials you are using for device communication, you must also manually update the device properties.
- Make sure DNS names can be resolved from the Security Manager server. You might need to fix the DNS settings on the server.
- Check the credentials for the device in Security Manager and ensure that they are correct and that there is a route between the server and device. Right-click the device, select **Device Properties**, select the Credentials tab, and click the **Test Connectivity** button. If the connection fails, check error messages to determine whether the problem is connectivity or credentials. Update the credentials in the device properties if necessary.

When adding new devices the credentials are defined within the New Device wizard if your method of adding the device requires credentials. Keep the following in mind:

- The primary credentials are used for SSH and Telnet connections.
- The HTTP/HTTPS credentials are used for HTTP and SSL connections unless you select **Use Primary Credentials**, in which case the primary credentials are also used for these connections.
- Beginning with version 4.11, Security Manager does not support the device SSL Certificates using MD5 algorithms. If the device SSL uses MD5 algorithms, Security Manager throws up an error when you try to add the device to Security Manager. This happens because JRE, by default, disables the MD5 algorithms due to security vulnerability. To resolve this, you must use higher encryption algorithm for device SSL certificate.
- Beginning with version 4.19, Cisco Security Manager does not support the device SSL Certificates using DES algorithms. If the device SSL uses DES algorithms, Security Manager throws up an error when you try to add the device to Security Manager. This happens because the JRE, by default, disables the DES

algorithms due to security vulnerability. To resolve this, you must use higher encryption algorithm for device SSL certificate, or follow the steps below:

- Stop Security Manager server services.
- Ensure you take a backup of MDC\vms\jre\lib\security\java.security properties.
- In properties, find "jdk.tls.disabledAlgorithms=SSLv3, DES, MD5withRSA, DH keySize <1024, \ EC keySize < 224, RC4_40, 3DES_EDE_CBC" and remove "DES" from the list.
- Start Security Manager server services again.

Related Topics

- Adding Devices to the Device Inventory
- Understanding Device Communication Requirements
- Preparing Devices for Management
- Device Credentials Page

Resolving Red X Marks in the Device Selector

If a device is marked with a red X in the device selector in Device view, it means that the Auto Update Server (AUS) or Configuration Engine server assignment for the device was lost during an upgrade from a Security Manager release prior to 3.2.0. AUS and Configuration Engines are not migrated during an upgrade from 3.1.x, and devices managed by them need to be reassigned to them after the upgrade using the following procedure.

Step 1 Do one of the following in Device view:

- From the Device selector, right-click a device with a red X icon, then select **Update Server Info**.
- Click any red X icon in the device selection tree. A warning message is displayed stating that AUS and Configuration Engine information was not migrated after the upgrade process. Click **Yes** to add these servers manually.

The Device Server Assignment dialog box opens.

Step 2 From the Available Devices list, select all the devices that use the same AUS or Configuration Engine server and click >> to move them to the selected list. The Available Devices list includes all devices that are managed by AUS or Configuration Engine that are marked with a red X.

Step 3 Select the AUS or Configuration Engine that manages the selected devices from the Server list. If the correct server is not listed, select **+ Add Server...** to add it to the inventory using the Server Properties Dialog Box.

For more information on adding AUS or Configuration Engine servers to the inventory, see Adding, Editing, or Deleting Auto Update Servers or Configuration Engines.

Step 4 Repeat the process until no device is marked with a red X.

Troubleshooting Deployment

The deployment process is one of the most likely areas in which you will encounter problems when using Security Manager. There are many different processes involved in deployment that influence whether the deployment job is successful:

- Security Manager itself.
- The stability and availability of your network, including links to remotely-managed devices.
- Any bugs inherent in the versions of the operating systems that you are using on your network devices that affect the commands Security Manager is trying to deploy (Security Manager is not immune to these bugs).
- The licenses you have enabled on the device, because many security commands require specific device licenses.
- The specific features supported by your devices, which Security Manager cannot always determine ahead of time. For example, some platforms support features only if the device has a certain minimum RAM, and some interface settings are available for specific interface cards only.
- The correct functioning of interim applications such as AUS, Configuration Engine, or your TMS server.

If you encounter deployment failures, examine the messages in the deployment status window carefully. In addition, the following topics address some of the problems you might encounter:

- Changing How Security Manager Responds to Device Messages , on page 10
- Memory Violation Deployment Errors for ASA 8.3+ Devices , on page 12
- Security Manager Unable to Communicate With Device After Deployment , on page 12
- Updating VPNs That Include Routing Processes , on page 13
- Mixing Deployment Methods with Router and VPN Policies , on page 14
- Deployment Failures for Routers , on page 15
- Deployment Failures for Catalyst Switches and Service Modules , on page 16
- Deployment Failures to Devices Managed by AUS , on page 18
- Troubleshooting the Setup of Configuration Engine-Managed Devices , on page 19

Changing How Security Manager Responds to Device Messages

Security Manager has built-in responses to many of the response messages that can be encountered when configuring a device. You might find that messages Security Manager treats as errors are messages that you want to ignore or treat as informational. Although you can configure your deployment jobs to ignore errors, you might instead want to update Security Manager to treat specific messages differently using a properties file.

It is important to understand that setting the properties file to ignore the error is not always sufficient. Deployment can fail because the **Allow Download on Error** check box (located on the **Tools > Security Manager Administration > Deployment** page) is deselected by default. The following table provides details

about how Security Manager behaves when an error occurs during deployment, the **Allow Download on Error** option is either selected or deselected, and the **Save Changes Permanently on Device** option is selected or deselected.

Table 2: Deployment Device Error Handling for SSL and SSH on PIX Firewall, ASA, and Cisco IOS Routers

Allow Download on Error	Error Occurred	Error Ignored Using Warning Expression	Deployment Status	Write Memory Done
Selected	Yes	No	Failed	Based on whether **Save Changes Permanently on Device** is selected.
Selected	Yes	Yes	Success	Based on whether **Save Changes Permanently on Device** is selected.
Selected	No	Not applicable	Success	Based on whether **Save Changes Permanently on Device** is selected.
Deselected	Yes	No	Failed (Deploy not Completed message)	No.
Deselected	Yes	Yes	SSL (ASA, PIX, IOS devices)—Failed SSH (IOS devices—Success	SSL—No. SSH (IOS devices)—Based on whether **Save Changes Permanently on Device** is selected.
Deselected	No	Not applicable	Success	Based on whether **Save Changes Permanently on Device** is selected.

Note On Cisco IOS routers using the SSL protocol, deployment on devices stops on command syntax errors. It does not stop when configuration-related errors occur.

To change how Security Manager treats a message, you need to update the DCS.properties file in \CSCOpx\MDC\athena\config folder in the installation directory (usually c:\Program Files). Use a text editor such as NotePad to update the file.

It is easiest to determine the message you want to ignore by looking at the transcript of a deployment job that encountered the error using the following procedure.

Related Topics

- Viewing Deployment Status and History for Jobs and Schedules

Step 1 Click the **Deployment Manager** button in the Main toolbar.

The Deployment Manager window appears. Click the **Deployment Jobs** tab if it is not active.

Step 2 Select the job with the error message.

Step 3 Click the **Transcript** button in the Deployment Details tab to open the transcript.

Step 4 Identify the error text that you want to ignore.

Step 5 Locate the appropriate warning expressions property in the DCS.properties file. For example, for PIX devices the property is called **dev.pix.warningExpressions**, whereas for IOS devices the property is called **dev.ios.warningExpressions**.

Tip Conversely, you can make device responses that are not tagged with the Error prefix to appear as error messages. To do this, add the message to the Error Expressions list (for example, **dev.pix.ErrorExpressions**).

Step 6 Add the error text to the warning expressions list. The warning message should be a generic regular expression string. Except for the last expression, you must delimit all expressions with "$\". For example, if the message you want to ignore is "Enter a public key as a hexadecimal number," enter the following string:

.*Enter a public key as a hexadecimal number .*$

Step 7 Restart the CiscoWorks Daemon Manager.

Memory Violation Deployment Errors for ASA 8.3+ Devices

ASA Software release 8.3+ requires significantly more device memory than previous versions of the ASA software. If you upgrade an ASA device that does not meet the minimum memory requirements, the upgrade process notifies you of the problem and the device regularly sends syslog messages until the minimum memory requirement is met.

Because an ASA device that does not meet the minimum memory requirements can function poorly, Security Manager does not deploy configurations to these devices, although you are allowed to add the device to the inventory and discover policies from it. However, if you try to deploy policies to the device before you add memory, you get a deployment error stating that the device does not meet the minimum memory requirements and deployment fails.

The best way to resolve the error is to add memory to the device. For information about ASA devices and memory upgrade possibilities, see http://www.cisco.com/go/asa .

Alternatively, you can downgrade the ASA software version, in which case you should delete the device from the inventory, then add it back to the inventory and discover policies.

Error While Attempting to Remove Unreferenced Object

If you enable the Remove Unreferenced Object Groups from Device option on the **Tools > Security Manager Administration > Deployment** page, Security Manager will remove objects during deployment that are not used in any policies managed or discovered by Security Manager. If any policy that is NOT discovered or managed by Security Manager is using such an object, Security Manager will still attempt to delete that object during deployment. In such cases, deployment will fail with a transcript error indicating that it was unable to delete the object as the object is being used. To successfully deploy, disable the Remove Unreferenced Object Groups from Device option.

Security Manager Unable to Communicate With Device After Deployment

There are a number of policies that you can configure in Security Manager that prevent access to a device. That is the point of security, ensuring that unwanted hosts cannot enter your network or network devices.

However, you can inadvertently lock the Security Manager server out of a device, making it impossible for Security Manager to deploy configurations to it or manage it. If you find that after a deployment, Security

Manager can no longer contact a device, and you have already checked that the device is up and running and otherwise functioning normally, look into the following policies to see if they are causing the lock-out:

- **Firewall > Access Rules, or Firewall > Zone Based Firewall Rules** —If you use these policies, the rules must allow management traffic from the Security Manager server. Consider allowing at least HTTP, HTTPS, SSH, and Telnet. Consider creating a shared policy that defines the required access for Security Manager and applying it to all devices. Keep in mind that if you create any rules in these policies, an implicit rule is added to the end of the policy that denies any traffic that is not explicitly allowed.
- **NAT policies**—Make sure that you are not using a local address on the device as the original address to be translated. Translating this address might result in translating the management traffic sent between Security Manager and the device, causing the interruption.
- **Device Access policies on routers**—Security Manager might loose contact with a device after you unassign a device access policy from the device and redeploy it. Device access policies can be used to define the enable password for accessing the device. If you unassign this policy and redeploy, the password is removed from the device. In such cases, the device typically reverts to the default password. However, in some cases, the device might contain an additional password that is unknown to Security Manager, such as a line console password. If this additional password exists, the device reverts to that password instead of the default password. If that happens, Security Manager cannot configure this device. Therefore, if you use a device access policy to configure the enable password or enable secret password on a device, make sure that you do not unassign the policy without assigning a new policy before the next deployment.
- **Site-to-Site VPNs**—If you lose communication with a spoke in a VPN, the problem can occur when the Security Manager server communicates with an external interface on the spoke from within the hub's protected network. We recommend that when you add the hub device to Security Manager that you define a management IP address that is located outside of the hub's protected network.
- **Platform > Device Admin > Device Access > Allowed Hosts**—For IPS devices, the Allowed Hosts policy identifies the hosts that can connect to the sensor. The Security Manager server must be included in this policy.

Related Topics

- Troubleshooting Device Communication Failures , on page 8
- Managing Device Communication Settings and Certificates , on page 4
- Managing IPS Certificates
- Understanding Device Communication Requirements

Updating VPNs That Include Routing Processes

Problem: When you define and deploy changes to a routing process that is being used by a VPN topology (using either the Site-to-Site VPN Manager or the routing policies), the changes that you make are not reflected in the CLI commands configured on the device.

Solution: When you discover a VPN topology that includes routing processes, such as GRE full mesh, Security Manager populates the GRE Modes policy in the Site-to-Site VPN Manager, as well as the relevant routing policies. However, changes made to one of these policies in Security Manager are not automatically reflected in the other policy, which can lead to unexpected results after deployment. Therefore, if you make changes to the secured IGP in the Site-to-Site VPN Manager, be sure to go to Platform > Routing in Device view to

make the necessary changes in the device's routing policies. Likewise, if you make changes directly to the routing policy, be sure to make the necessary changes in the Site-to-Site VPN Manager as well.

Related Topics

- Managing Site-to-Site VPNs: The Basics
- Managing Routers
- Managing Firewall Devices

Mixing Deployment Methods with Router and VPN Policies

You might receive unpredictable results when you deploy router platform and VPN policies to a live device after previously deploying to a configuration file.

This problem can occur when you use a mix of deployment methods (deploy to device and deploy to file) with router platform policies and VPN policies. Because Security Manager does not manage all the available CLI commands for these policy types, it maintains a snapshot of the commands it has configured and leaves all other commands (which includes unsupported commands as well as supported commands in policies that have not been configured in Security Manager) intact on the device.

After each deployment, Security Manager creates a snapshot of the policies that were deployed to each device. This snapshot is used during the next deployment to generate the list of configuration changes that will be deployed to the device. Only one snapshot is maintained at a time per device.

Mixing deployment methods with router platform policies and VPN policies can lead to unpredictable results, as shown in this example:

1. Configure router platform policy A to a live device. When deployment completes, Security Manager creates a snapshot for that device with policy A.
2. Next, configure policy B to replace policy A, but instead of deploying policy B to the device, deploy it to a file instead. When this deployment completes, Security Manager creates a snapshot with policy B that replaces the previous snapshot with policy A. However, because you did not deploy policy B to the device, the CLI commands that are required to negate policy A have not been deployed. Policy A is still deployed on the device.
3. Deploy again to the device without first copying the changes in the configuration file to the device. Security Manager cannot generate the commands that are required to negate policy A from the device because the snapshot with policy A no longer exists.

Because policy A is a router platform policy, any of the following results might occur:

- The policy in the latest deployment overrides policy A.
- Both policies end up defined on the device.
- Deployment fails because the two policies cannot coexist.

Therefore, if you deploy to a file when working on a live device, we strongly recommend that you copy your configuration changes from the file to the device before performing additional deployments to the device.

Related Topics

- Managing Site-to-Site VPNs: The Basics
- Managing Routers

Deployment Failures for Routers

Following are some potential problems you might encounter when deploying configurations to Cisco IOS routers.

Deployment Fails for Interface Settings

Problem: Deployment fails for interface settings on a router.

Solution: Security Manager cannot validate whether you have the appropriate types of interface cards or shared port adapters (SPAs) installed on the router, or the appropriate licenses configured, to support your interface policies. If you add or remove an interface card without changing your interface policies, you can encounter deployment errors. The best practice is to ensure that you discover inventory from the router whenever you change interface modules or SPAs so that Security Manager can discover the appropriate interface features.

Deploying Layer 2 Interface Definitions

Problem: Deployment fails if the interface policy includes a definition for a Layer 2 interface.

Solution: Layer 2 interfaces do not support Layer 3 interface definitions, such as IP addresses. Make sure that you did not define a Layer 3 definition on the Layer 2 interface.

VPN Traffic Sent Unencrypted

Problem: Traffic that should be sent encrypted over a VPN is instead being sent unencrypted.

Solution: Ensure that you are not performing NAT on VPN traffic. Performing address translation on VPN traffic prevents the traffic from being encrypted and sent through the VPN tunnel. When defining dynamic NAT rules, make sure that the Do Not Translate VPN Traffic check box is selected, even when you perform NAT into IPSec. (This option does not interfere with the translation of addresses arriving from overlapping networks.)

This option can be used only on site-to-site VPNs. For remote access VPNs, you need to create an ACL object that explicitly denies the flow containing VPN traffic and define this ACL as part of a dynamic rule in the NAT policy. For more information, see NAT Page: Dynamic Rules.

Unable to Deploy ADSL or PVC Policy

Problem: Deployment fails for your ADSL or PVC policy.

Solution: Make sure that you have selected the correct ATM interface card type in the policy definition. Security Manager cannot properly validate the policy definition without knowing the correct card type, which can lead to deployment failures.

DHCP Traffic Not Being Transmitted

Problem: DHCP traffic is not being transmitted even after you deploy a DHCP policy to the device.

Solution: Check whether an access rule on the device blocks Bootstrap Protocol (BootP) traffic. Having such a rule prevents DHCP traffic from being transmitted.

NAC Not Implemented on Router

Problem: Network admission control is not being implemented on the router, even though a NAC policy was deployed to it.

Solution: Ensure that the default ACL on the router permits UDP traffic over the port defined in the NAC policy for EAP over UDP traffic. This is the protocol that NAC uses for communication between the Cisco Trust Agent (CTA), which is the NAC client that provides posture credentials for the endpoint device on which it is installed and the network access device (NAD; in this case, the router) that relays the posture credentials to the AAA server for validation. The default port used for EAP over UDP traffic is 21862, but you can change this port as part of the NAC policy. If the default ACL blocks UDP traffic, EAP over UDP traffic is likewise blocked, which prevents NAC from taking place.

Deployment Fails with Error Writing to Server or HTTP Response Code 500 Messages

Problem: Deployment to a Cisco IOS router fails and an "Error Writing to Server" or "Http Response Code 500" error message occurs.

Solution: When you use SSL as the transport protocol for deploying configurations to a Cisco IOS router, the configuration is split into multiple configuration bulks. The size of this configuration bulk varies from platform to platform. If Security Manager tries to deploy a configuration bulk that exceeds the size of the SSL chunk configured on that device, the deployment fails and you get an "Error Writing to Server" or "Http Response Code 500" error message.

To resolve this, do the following:

1. On the Security Manager server, open the DCS.properties file in the \CSCOpx\MDC\athena\config folder in the installation directory (usually C:\Program Files).
2. Locate **DCS.IOS.ssl.maxChunkSize=**<*value of the configuration bulk* >.
3. Reduce the value of the configuration bulk.
4. Restart the CiscoWorks Daemon Manager.

Deployment Failures for Catalyst Switches and Service Modules

Note From version 4.17, though Cisco Security Manager continues to support Cisco Catalyst switches features/functionality, it does not support any enhancements.

Following are some potential problems you might encounter when deploying configurations to Catalyst switches and Catalyst 6500/7600 service modules.

Deployment Fails for Interface Settings

Problem: Deployment fails for interface settings on a Catalyst 6500/7600 device.

Solution: Certain interface settings (such as speed, duplex, and MTU settings) are specific to particular card types and are not validated prior to deployment. Make sure to enter the correct values for your specific card type to ensure successful deployment.

Deployment Failures to FWSM Security Contexts After Changing Interface Policies

Problem: You add an FWSM with security contexts and discover its policies. The configuration includes interface aliases (the allocate interface command). After changing the interfaces policy for a context, deployment fails.

Solution: Connect directly to the FWSM and remove all mapped interface names from the system execution space configuration and in all other contexts, replace interface references to mapped names with the VLAN ID of the interface. You can then delete the FWSM from the Security Manager inventory and rediscover it.

Deployment Failures for FWSMs That Have Multiple Contexts

Problem: Deployment to an FWSM that has multiple security contexts sometimes fails or results in a temporary performance impact to the FWSM.

Solution: The problem is that Security Manager is trying to deploy configurations to more than one security context on a device at the same time. Depending on the configuration changes, this can result in errors on the device that prevent successful deployment. If you use FWSM in multiple-context mode, configure Security Manager to deploy configurations serially to the device so that one context at a time is configured, as described in Changing How Security Manager Deploys Configurations to Multiple-Context FWSM , on page 18.

Deployment Fails for Internal VLANs

Problem: Deployment fails when Security Manager tries to create a VLAN with an ID that is within the range of the device's internal VLAN list.

Solution: Security Manager cannot detect internal VLANs. Therefore, you must define a VLAN ID that falls outside of the device's internal VLAN list. Use the **show vlan internal usage** command on the device to view the list of internal VLANs.

Deployment Fails When Changing the Running Mode of an IDSM Data Port VLAN

Problem: Deployment fails when you attempt to change the running mode of the data port VLAN from Trunk (IPS) to Capture (IDS) and the following error message is displayed:

Command Rejected: Remove trunk allowed vlan configuration from data port 2 before configuring capture allowed-vlans

Solution: On some software releases such as 12.2(18)SFX4, there is a bug that prevents the change from occurring correctly. Reload the device to overcome the problem.

Deployment Fails for FWSM Configuration With Large Numbers of ACLs

Problem: Deployment to FWSM devices fail when the configuration contains a large number of ACLs.

Solution: This could occur because the CPU utilization is high during ACL compilation. To resolve this, reconfigure the CPU utilization threshold limit by doing the following:

1. On the Security Manager server, open the DCS.properties file in the \CSCOpx\MDC\athena\config folder in the installation directory (usually C:\Program Files).
2. Locate the **DCS.FWSM.checkThreshold=False** property.
3. Change the value to true: **DCS.FWSM.checkThreshold=True**.
4. Restart the CiscoWorks Daemon Manager.
5. Deploy the configuration to the device again.

After you set the value to true, discovery and deployment checks the CPU utilization and generates error messages if the CPU utilization is not within the configured value set in the DCS.FWSM.minThresholdLimit property. The default value is 85.

Changing How Security Manager Deploys Configurations to Multiple-Context FWSM

Note From version 4.17, though Cisco Security Manager continues to support FWSM features/functionality, it does not support any enhancements.

If you configure a Firewall Services Module (FWSM) to run in multiple context mode, so that you host more than one security context on the FWSM, you need to configure Security Manager to deploy configurations serially to the FWSM. The FWSM has some limitations that can prevent successful deployments if more than one context is updated at the same time, so you might run into deployment failures if you do not use serial deployment. There can also be an impact on FWSM performance during deployment if you do not use serial deployment.

To change how Security Manager deploys configurations to multiple-context FWSM, you need to update the DCS.properties file. You also need to add the FWSM contexts to the inventory using the FWSM admin context, rather than adding the individual security contexts.

The following procedure explains the end-to-end process for ensuring that FWSM deployments are done serially.

Step 1 Make it a standard practice to add FWSM security contexts using the admin context management IP address. Manage the contexts through the admin context.

Although it is possible to add security contexts for an FWSM individually, using each context's management IP address, Security Manager cannot recognize these individually-added contexts as being hosted on the same physical device. This prevents Security Manager from doing serial deployments to the contexts.

If you have any FWSM security contexts that you added using the security context management IP, delete the contexts and FWSM from the inventory, then add them using the admin context (discover all policies). See Adding Devices to the Device Inventory.

Tip If you have any undeployed changes to these contexts that you want to keep, first deploy the changes to ensure that the configurations on the device are complete. Do the deployments one context at a time.

Step 2 Log into Windows on the Security Manager server and edit the **DCS.properties** file in the \CSCOpx\MDC\athena\config folder in the installation directory (usually c:\Program Files). Use a text editor such as NotePad to update the file.

Step 3 Locate the DCS.doSerialAccessForFWSMVCs property in the DCS.properties file and set it to true:

DCS.doSerialAccessForFWSMVCs=true

Step 4 Restart the CiscoWorks Daemon Manager.

Deployment Failures to Devices Managed by AUS

Deployment might fail when deploying to multiple AUS-managed devices after starting the AUS if you perform deployment before the Auto Update Server (AUS) is fully operational. The AUS requires time to start up after the following operations:

- New installation or upgrade.
- Manual restart (including after a power outage).

- Manual restart of the Cisco Security Manager Daemon Manager service.

You can verify whether the AUS is fully operational by verifying the status of its Windows services. To do this, select **Start > Control Panel > Administrative Services > Services**, then check the status of the CiscoWorks AUS Database Engine service. If this service has started, try again to deploy.

Troubleshooting the Setup of Configuration Engine-Managed Devices

The following questions and answers describe issues that might arise when you set up a device managed by a Cisco Configuration Engine (also known as CNS) and how to solve them:

Question: Why does Configuration Engine deployment fail?

Answer: Not all versions of Configuration Engine function in a compatible manner. Because Security Manager does not verify the software version running on a Configuration Engine when you add it to the device inventory, you can add unsupported versions to the inventory. Then, when you try to deploy, you can run into unpredictable errors. Ensure that you are running a supported version of Configuration Engine (for version information, see the release notes for this version of Security Manager at http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html).

Question: Why do I receive an InvalidParameterException when I click on an IOS device on the Configuration Engine web page?

Answer: This is the expected behavior. For IOS devices, Security Manager uses deployment jobs to deploy configurations to Configuration Engine instead of associating a configuration to the IOS device in Configuration Engine. Therefore, you do not see an associated configuration when you click the device name on the Configuration Engine web page. For ASA/PIX devices, Security Manager associates the configuration to the device in Configuration Engine. Therefore, clicking the device name displays the associated configuration.

Question: Why am I getting the following error: com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: [002-01003]]deviceName does not exists?

Answer: This error indicates that the device has not been added to Configuration Engine. It appears if you have not performed rollback or deployment in Security Manager (both of which add the device automatically), and have not manually added the device to Configuration Engine.

Question: Why am I getting the following error: com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: [002-01003]]Device device id is not connected

Answer: The answer depends on the type of setup you are performing:

- Event mode setup—Make sure that the Configuration Engine device ID defined in the Device Properties window in Security Manager matches the device ID configured on the router (using the **cns id string** command).
- Call home mode setup—The device is not connected to Configuration Engine in this mode; therefore, all Security Manager operations that require the retrieval of the device configuration using Configuration Engine are not supported. This includes discovery, preview configuration, display running configuration, and connectivity tests (and rollback, for IOS devices).

Question: Why is deployment to my Configuration Engine-managed ASA/PIX device not working?

Answer: There are several possibilities:

- The configuration contains invalid commands. You can test this by copying the configuration associated with the ASA/PIX device in Configuration Engine and pasting it directly into the device.

- The **auto-update server** command contains an invalid username and password.
- You did not wait long enough for the configuration to be polled into the ASA/PIX device. Use the **show auto** command to verify when the next polling cycle will occur.
- If you previously used the Configuration Engine server for the same ASA/PIX device and did not delete the device from the Configuration Engine server before you started the current task, it is possible that the device received the previous configuration from the server before you deployed the new configuration to it.
- If none of the suggestions above solves the problem, turn on Configuration Engine debug mode on the ASA/PIX device and check the log for errors after the next polling cycle.

Question: Why was I able to deploy successfully to a Configuration Engine-managed ASA/PIX device the first time, but subsequent deployments were unsuccessful?

Answer: This can happen if the configuration pushed during the first deployment contains incorrect CLI commands for the auto-update feature. Check the following:

- Make sure the username and password of the Configuration Engine server is defined correctly in the **auto-update** command.
- If you used **name** commands when configuring the auto-update server using the device CLI, make sure that you have defined a FlexConfig that contains the necessary **name** commands. A FlexConfig is necessary because Security Manager does not support this command directly. As a result, even though the command was discovered, it does not appear in the full configuration. If you use Security Manager to configure the AUS policy, **name** commands are not necessary.

Question: How do I debug Configuration Engine on an ASA/PIX device?

Answer: Enter the following CLI commands:

```
logging monitor debug
terminal monitor
logging on
```

You can also find relevant information in the PIX log on the Configuration Engine server.

Question: How do I debug Configuration Engine on an IOS device?

Answer: Enter the following CLI commands:

```
debug cns all
debug kron exec-cli
terminal monitor
```

When working in event mode, you can also find relevant information in the event log on the Configuration Engine server. When working in call home mode, check the config server log on the Configuration Engine server.

Question: Why did I fail to discover an IOS device and acquire its configuration through Configuration Engine?

Answer: If you see the following errors in debug mode:

*Feb 23 21:42:15.677: CNS exec decode: Unknown hostname cnsServer-lnx.cisco.com ... 474F6860: 72726F72 2D6D6573 73616765 3E584D4C error-message>XML 474F6870: 5F504152 53455F45 52524F52 3C2F6572 _PARSE_ERROR

Verify the following:

- The CNS commands use a fully-qualified host name (host name and domain name).
- The device contains the **ip domain name** command.
- The device contains the **ip host** command with the fully qualified hostname of the Configuration Engine with its IP address.

Question: Why does the event mode router not appear on the Configuration Engine Discover Device page or appear in green on the Configuration Engine web page?

Answer: Check the following:

- Make sure that the router and the Configuration Engine server can ping each other.
- Make sure that the event gateway on the Configuration Engine server is up and running by using one of the following commands:

Status for plain text mode: **/etc/init.d/EvtGateway**

Status for SSL encrypted mode: **/etc/init.d/EvtGatewayCrypto**

- Clear the **cns event** command, then re-enter it without specifying a port number.