CHAPTER 5

Administering Cisco ISE

Use the tasks and reference information in this chapter to specify global settings and configure essential functions in Cisco ISE.

Logging in to Cisco ISE

Log in to Cisco ISE using your administrator username and password.

Step 1 Enter the Cisco ISE URL in the address bar of your browser (for example, *https://<ise hostname or ip address>/admin/*).

Step 2 Enter the username and case-sensitive password, that was specified and configured during the initial Cisco ISE setup.

Step 3 Click **Login** or press **Enter**.

If your login is unsuccessful, click the **Problem logging in?** link in the Login page and follow the instructions in Step 2.

Related Topics

- Administrator Login Browser Support, page 5-2
- Administrator Lockout Following Failed Login Attempts, page 5-2
- If you have to reset the Administrator password, see the "Performing Post-Installation Tasks" chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*.

Administrator Login Browser Support

You can access the Cisco ISE Admin portal using the following browsers:

- Mozilla Firefox Versions 5.*x*, 8.*x*, 9.*x*, 14.*x*, 15.*x*, and 18.*x* (applicable for Windows, Mac OS X, and Linux-based operating systems)
- Windows Internet Explorer 8.*x* and 9.*x* (in Internet Explorer 8 Compatibility Mode)

Note The Admin portal does not support using the Microsoft IE8 browser in its IE7 Compatibility Mode (the Microsoft IE8 is supported in its IE8-only mode).

Adobe Flash Player 11.2.0.0 or above must be installed on the system running your client browser.

The minimum required screen resolution to view the Admin portal and for a better user experience is 1280*800 pixels.

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough times, the Admin portal "locks you out" of the system, adds a log entry in the Server Administrator Logins report, and suspends the credentials for that administrator ID until you have an opportunity to reset the password that is associated with that administrator ID, as described in the "Performing Post-Installation Tasks" chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.2*. The number of failed attempts that is required to disable the administrator account is configurable according to the guidelines that are described in User Account Custom Attributes and Password Policies, page 14-2. After an administrator user account gets locked out, an e-mail is sent to the associated administrator user.

Disabled System administrators' status can be enabled by any Super Admin, including Active Directory users.

Specifying Proxy Settings in Cisco ISE

If your existing network topology requires you to use a proxy for Cisco ISE, to access external resources (like the remote download site where you can find client provisioning and posture-related resources), you can use the Admin portal to specify proxy properties.

Step 1 Choose **Administration > System > Settings > Proxy**.

Step 2 Enter the proxy IP address or DNS-resolvable host name in **Proxy Address**, and specify the port through which proxy traffic travels to and from Cisco ISE in **Proxy Port**.

Step 3 Click **Save**.

What to Do Next

Once you have specified your proxy settings, you can optionally enable the following systemwide client provisioning functions:

- Enabling and Disabling Client Provisioning, page 22-2
- Downloading Client Provisioning Resources Automatically, page 22-4

Related Topics

- Cannot Download Remote Client Provisioning Resources, page G-13

Ports Used by the Admin Portal

The Admin portal is set to use HTTP port 80 and HTTPS port 443, and you cannot change these settings. Cisco ISE also prevents you from assigning any of the end-user portals to use the same ports, which reduces the risk to the Admin portal.

Related Topics

- Port Settings for Web Portals, page A-50
- Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2

Specifying System Time and NTP Server Settings

Cisco ISE allows you to configure up to three Network Time Protocol (NTP) servers. You can use the NTP servers to maintain accurate time and synchronize time across different timezones. You can also specify whether or not Cisco ISE should use only authenticated NTP servers, and you can enter one or more authentication keys for that purpose.

Cisco recommends that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone—especially if your Cisco ISE nodes are installed in a distributed deployment. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

If you have both a primary and a secondary Cisco ISE node, you must log in to the user interface of the secondary node and configure the system time and NTP server settings on each Cisco ISE node in your deployment individually.

Step 1 Choose **Administration > System > Settings > System Time**.

Step 2 Enter unique IP addresses for your NTP servers.

Step 3 Check-the **Only allow authenticated NTP servers** check box if you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time.

Step 4 Click the **NTP Authentication Keys** tab and specify one or more authentication keys if any of the servers that you specify requires authentication via an authentication key, as follows:

a. Click **Add**.

b. Enter the necessary **Key ID** and **Key Value**, specify whether the key in question is trusted by activating or deactivating the **Trusted Key** option, and click **OK**. The **Key ID** field supports numeric values between 1 to 65535 and the **Key Value** .field supports up to 15 alphanumeric characters.

c. Return to the **NTP Server Configuration** tab when you are finished entering the NTP Server Authentication Keys.

Step 5 Click **Save**.

Related Topics

- Role-Based Access Control in Cisco ISE, page 6-8

Changing the System Time Zone

Once set, you cannot edit the time zone from the Admin portal. To change the time zone setting, you must enter the following command in the Cisco ISE CLI:

clock timezone *timezone*

Caution Changing the time zone on a Cisco ISE appliance after installation causes the Cisco ISE application on that node to be unusable. However, the preferred time zone (default UTC) can be configured during the installation when the initial setup wizard prompts you for the time zone.

Changing time zone impacts different Cisco ISE node types in your deployment as follows:

Standalone or Primary ISE Node

Changing the time zone after installation is not supported on a Standalone or Primary ISE node. However, if you inadvertently change the time zone, do the following:

- Revert to the time zone back. (the time zone before it changed).
- Run the application reset-config ise command from the CLI of that node.
- Restore from the last known good backup before the time zone change on that node.

Secondary ISE Node

Changing the time zone on a secondary node renders it unusable on your deployment. If you want to change the time zone on the secondary node to keep it to be the same as the primary node, do the following:

- Deregister the secondary node.
- Correct the time zone to be the same as the primary node.
- Run the application reset-config ise command from the CLI of that node.
- Reregister the node as a secondary node to the primary node.

For more information on the **clock timezone** command, refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*.

Configuring the SMTP Server to Support Notifications

You must set up a Simple Mail Transfer Protocol (SMTP) server to send e-mail notifications for alarms and to enable sponsors to send guests their account credentials using e-mail or Short Message Service (SMS) text messages.

Step 1 Choose **Administration** > **System** > **Settings** > **SMTP Server**.

Step 2 Enter the host name of the outbound SMTP server in the **SMTP server** field. This SMTP host server must be accessible from the Cisco ISE server. The maximum length for this field is 60 characters.

Step 3 Choose one of these options:

- **Use email address from Sponsor** to send guest notification e-mail from the e-mail address of the sponsor and choose **Enable Notifications**.
- **Use Default email address** to specify a specific e-mail address from which to send all guest notifications and enter it in the **Default email address** field.

Step 4 Click **Save**.

The recipient of alarm notifications can be any internal admin users with "Include system alarms in emails" option enabled. The sender's email address for sending alarm notifications is hardcoded as ise@<hostname>.

Related Topic

- Customizing Guest Notifications, page 16-9
- Enabling and Configuring Alarms, page 25-11
- Creating a New Cisco ISE Administrator, page 6-2

Installing a Software Patch

You can install patches on Cisco ISE servers in your deployment from the primary administration node. To install a patch from the Admin portal, you must download the patch from Cisco.com to the system that runs your client browser.

Note Cisco ISE allows you to install a patch on an Inline Posture node only through the CLI.

To install patches from the CLI, refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*.

Before You Begin

You must have the Super Admin or System Admin administrator role assigned.

Step 1 Choose **Administration** > **System** > **Maintenance** > **Patch Management** > **Install**.

Step 2 Click **Browse** and choose the patch that you downloaded from Cisco.com.

Step 3 Click **Install** to install the patch.

After the patch is installed on the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log in again.

Note When patch installation is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

Step 4 Log in and click the **Alarms** link at the bottom of the dashboard page.

Step 5 Choose **Administration > System > Maintenance > Patch Management** to return to the Patch Installation page.

Step 6 Click the radio button next to the patch that you have installed on any secondary nodes and click **Show Node Status** to verify whether installation is complete.

What To Do Next

If you need to install the patch on one or more secondary nodes, ensure that the nodes are up and repeat the process from Step 1 to install the patch on the remaining nodes.

Related Topics

- Cisco ISE Software Patches, page 5-6
- Software Patch Installation Guidelines, page 5-6
- Rolling Back Software Patches, page 5-7
- Viewing Patch Install and Rollback Changes, page 5-8
- Role-Based Access Control in Cisco ISE, page 6-8

Cisco ISE Software Patches

Cisco ISE software patches are usually cumulative. However, any restrictions on the patch installation are described in the *README* file included with the patch. Cisco ISE allows you to perform patch installation and rollback from CLI or GUI.

Software Patch Installation Guidelines

When you install or roll back a patch from a standalone or primary administration node, Cisco ISE restarts the application. You might have to wait for a few minutes before you can log in again.

Ensure that you install patches that are applicable for the Cisco ISE version that is deployed in your network. Cisco ISE reports any mismatch in versions as well as any errors in the patch file.

You cannot install a patch with a version that is lower than the patch that is currently installed on Cisco ISE. Similarly, you cannot roll back changes of a lower-version patch if a higher version is currently installed on Cisco ISE. For example, if patch 3 is installed on your Cisco ISE servers, you cannot install or roll back patch 1 or 2.

When you install a patch from a primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment. If the patch installation is successful on the primary node, Cisco ISE then continues patch installation on the secondary nodes. If it fails on the primary node, the installation does not proceed to the secondary nodes. However, if the installation fails on any of the secondary nodes for any reason, it still continues with the next secondary node in your deployment. Secondary Cisco ISE nodes are restarted consecutively after the patch is installed on those nodes. While installing a patch on secondary nodes, you can continue to perform tasks on the primary administration node.

Rolling Back Software Patches

When you roll back a patch from a primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary node and then all the secondary nodes in the deployment.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

Step 1 Choose **Administration > System > Maintenance > Patch Management**.

Step 2 Click the radio button for the patch version whose changes you want to roll back and click **Rollback**.

> **Note** When a patch rollback is in progress, **Show Node Status** is the only function that is accessible on the Patch Management page.

After the patch is rolled back from the primary administration node, Cisco ISE logs you out and you have to wait a few minutes before you can log in again.

Step 3 After you log in, click the **Alarms** link at the bottom of the page to view the status of the rollback operation.

Step 4 Choose **Administration > System > Maintenance > Patch Management**

Step 5 To view the progress of the patch rollback, choose the patch in the Patch Management page and click **Show Node Status**.

Step 6 Click the radio button for the patch and click **Show Node Status** on any secondary nodes to ensure that the patch is rolled back from all the nodes in your deployment.

If the patch is not rolled back from any of the secondary nodes, ensure that the node is up and repeat the process from Step 1 to roll back the changes from the remaining nodes. Cisco ISE only rolls back the patch from the nodes that still have this version of the patch installed.

Related Topics

- Software Patch Rollback Guidelines, page 5-8
- To roll back patches from the CLI, refer to *Cisco Identity Services Engine CLI Reference Guide, Release 1.2*
- Installing a Software Patch, page 5-5
- Viewing Patch Install and Rollback Changes, page 5-8
- Role-Based Access Control in Cisco ISE, page 6-8

Software Patch Rollback Guidelines

To roll back a patch from Cisco ISE nodes in a deployment, you must first roll back the change from the primary node. If this is successful, the patch is then rolled back from the secondary nodes. If the rollback process fails on the primary node, the patches are not rolled back from the secondary nodes. However, if the patch fails on any of the secondary nodes, it still continues to roll back the patch from the next secondary node in your deployment.

While Cisco ISE rolls back the patch from the secondary nodes, you can continue to perform other tasks from your primary administration node GUI. The secondary nodes will be restarted after the rollback.

Viewing Patch Install and Rollback Changes

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your Cisco ISE nodes according to a time period that you specify.

Before You Begin

You must have either the Super Admin or System Admin administrator role assigned.

Step 1 Choose **Operations > Reports > Catalog > Server Instance**.

Step 2 Click the **Server Operations Audit** radio button, click **Run**, and choose the time period for which you want to generate the report.

Step 3 Click the **Launch Interactive Viewer** link in the upper right corner of the page to view, sort, and filter the data in this report.

Related Topics

- Cisco ISE Software Patches
- Installing a Software Patch
- Rolling Back Software Patches
- Role-Based Access Control in Cisco ISE, page 6-8
- “Running and Viewing Reports” section on page 26-2

Enabling FIPS Mode in Cisco ISE

You can provide Federal Information Processing Standard (FIPS) 140-2 compliant encryption and decryption in your Cisco ISE network.

Step 1 Choose **Administration > System > Settings > FIPS Mode**.

Step 2 Choose the **Enabled** option from the FIPS Mode drop-down list.

Step 3 Click **Save** and restart your machine.

What to Do Next

Once you have enabled FIPS mode, enable and configure the following FIPS 140-2 compliant functions:

- Importing Network Devices into Cisco ISE, page 9-4
- Generating a Self-Signed Certificate, page 8-18
- Generating a Certificate Signing Request, page 8-19
- RADIUS Authentication Settings, page A-37

In addition, you may want to enable administrator account authorization using a Common Access Card (CAC) function according to the guidelines in Configuring Cisco ISE for Administrator CAC Authentication, page 5-10. Although using CAC functions for authorization is not strictly a FIPS 140-2 requirement, it is a well-known secure-access measure that is used in a number of environments to bolster FIPS 140-2 compliance.

FIPS Mode Support

Cisco ISE supports Federal Information Processing Standard (FIPS) 140-2 Common Criteria EAL2 compliance. FIPS 140-2 is a United States government computer security standard that is used to accredit cryptographic modules. Cisco ISE uses an embedded FIPS 140-2 implementation using validated C3M and Cisco ACS NSS modules, per FIPS 140-2 Implementation Guidance section G.5 guidelines.

When FIPS mode is enabled, the Cisco ISE administrator interface displays a FIPS mode icon to the left of the node name in the upper-right of the page.

If Cisco ISE detects at least one protocol or certificate that is not supported by the FIPS 140-2 level 1 standard, Cisco ISE displays a warning with the names of the protocols and FIPS mode is not enabled until the protocols have been addressed appropriately.

After you enable FIPS mode, you must reboot all other nodes in the deployment. To minimize disruption to your network, Cisco ISE automatically performs a rolling restart by first restarting the primary Administration node and then restarting each secondary node, one at a time.

Tip Cisco recommends that you do not enable FIPS mode before completing any database migration process.

FIPS Mode Operational Parameters

The FIPS standard places limitations on the use of certain algorithms. In order to enforce this standard, you must enable FIPS operation in Cisco ISE. Cisco ISE enables FIPS 140-2 compliance via RADIUS shared secret and key management measures. While in FIPS mode, any functions using non-FIPS-compliant algorithms fail, and certain authentication functionality is disabled. For more details, including protocol support, see FIPS 140-2 Implementation, page 1-4 and Support for Common Access Card Functions, page 1-5.

Enabling FIPS mode also automatically disables Password Authentication Protocol (PAP) and Challenge Handshake Authentication Protocol (CHAP) protocols, which the guest login function of Cisco ISE requires. For information on addressing this issue with Layer-3 guest login implementation, see Chapter 16, “Supporting Authorized Network Access for Guests.”

Cisco NAC Agent Requirements when FIPS Mode is Enabled

The Cisco NAC Agent always looks for the Windows Internet Explorer TLS 1.0 settings to discover the Cisco ISE network. (These TLS 1.0 settings should be enabled in Internet Explorer.) Therefore, client machines must have Windows Internet Explorer Version 7, 8, or 9 installed and TLS1.0 enabled to allow for Cisco ISE posture assessment functions to operate on client machines accessing the network. The Cisco NAC Agent can automatically enable the TLS 1.0 setting in Windows Internet Explorer if FIPS mode has been enabled in Cisco ISE.

Configuring Cisco ISE for Administrator CAC Authentication

Before You Begin

Before beginning configuration, do the following:

- (Optional) Turn on FIPS mode according to the instructions in Enabling FIPS Mode in Cisco ISE, page 5-8. FIPS mode is not required for certificate-based authentication, but the two security measures often go hand-in-hand. If you do plan to deploy Cisco ISE in a FIPS 140-2 compliant deployment and to use CAC certificate-based authorization as well, be sure to turn FIPS mode on and specify the appropriate private keys and encryption/decryption settings first.
- Ensure that the domain name server (DNS) in Cisco ISE is set for Active Directory.
- Ensure that Active Directory user and user group membership has been defined for each administrator certificate.

To ensure that Cisco ISE can authenticate and authorize an administrator based on the CAC-based client certificate that is submitted from the browser, be sure that you have configured the following:

- The external identity source (Active Directory in the following example)
- The user groups in Active Directory to which the administrator belongs
- How to find the user's identity in the certificate
- Active Directory user groups to Cisco ISE RBAC permissions mapping
- The Certificate Authority (trust) certificates that sign the client certificates
- A method to determine if a client certificate has been revoked by the CA

You can use a Common Access Card (CAC) to authenticate credentials when logging into Cisco ISE.

Step 1 Enable FIPS mode as described in Enabling FIPS Mode in Cisco ISE, page 5-8. You will be prompted to restart your system after you enable the FIPS mode. You can defer the restart if you are going to import CA certificates as well.

Step 2 Configure an Active Directory identity source in Cisco ISE and join all Cisco ISE nodes to Active Directory as described in Configuring Active Directory as an External Identity Source, page 14-12.

Step 3 Configure a certificate authentication profile according to the guidelines in Adding a Certificate Authentication Profile, page 14-8.

Be sure to select the attribute in the certificate that contains the administrator user name in the Principal Name X.509 Attribute field. (For CAC cards, the Signature Certificate on the card is normally used to look up the user in Active Directory. The Principal Name is found in this certificate in the "Subject Alternative Name" extension, specifically in a field in that extension that is called "Other Name." So the attribute selection here should be "Subject Alternative Name - Other Name.")

If the AD record for the user contains the user's certificate, and you want to compare the certificate that is received from the browser against the certificate in AD, check the Binary Certificate Comparison check box, and select the Active Directory instance name that was specified earlier.

Step 4 Enable Active Directory for Password-Based Admin Authentication as described in Configuring a Password-Based Authentication Using an External Identity Store, page 6-17. Choose the Active Directory instance name that you connected and joined to Cisco ISE earlier.

Note You must use password-based authentication until you complete other configurations. Then, you can change the authentication type to client certificate based at the end of this procedure.

Step 5 Create an External Administrator Group and map it to an Active Directory Group. Choose **Administration > System > Admin Access > Administrators > Admin Groups**. Create an external system administrator group as described in Creating an External Administrator Group, page 6-18.

Step 6 Configure an admin authorization policy to assign RBAC permissions to the external admin groups as described in Creating an RBAC Policy for External Administrator Authentication, page 6-19.

Warning **We strongly recommend that you create an external Super Admin group, map it to an Active Directory group, and configure an admin authorization policy with Super Admin permissions (menu access and data access), and create at least one user in that Active Directory Group. This mapping ensures that at least one external administrator has Super Admin permissions once Client Certificate-Based Authentication is enabled. Failure to do this may lead to situations where the Cisco ISE administrator is locked out of critical functionality in the Admin Portal.**

Step 7 Choose **Administration > System > Certificates > Certificate Store** to import certificate authority certificates into the Cisco ISE certificate trust store.

Cisco ISE does not accept a client certificate unless the CA certificates in the client certificate's trust chain are placed in the Cisco ISE Certificate Store. You must import the appropriate CA certificates in to the Cisco ISE Certificate Store.

a. Click **Browse** to choose the certificate.

b. Check the Trust for client authentication check box.

c. Click **Submit**.

Cisco ISE prompts you to restart all the nodes in the deployment after you import a certificate. You can defer the restart until you import all the certificates. However, after importing all the certificates, you must restart Cisco ISE before you proceed.

Step 8 Configure the certificate authority certificates for revocation status verification.

a. Choose **Administration > System > Certificates > OSCP Services**.

b. Enter the name of an OSCP server, an optional description, and the URL of the server.

c. Choose **Administration > System > Certificates > Certificate Store**.

d. For each CA certificate that can sign a client certificate, specify how to do the revocation status check for that CA. Choose a CA certificate from the list and click Edit. On the edit page, choose OCSP and/or CRL validation. If you choose OCSP, choose an OCSP service to use for that CA. If you choose CRL, specify the CRL Distribution URL and other configuration parameters. See OCSP Services, page 8-31 and Editing a Certificate Store Certificate, page 8-28 for more information.

Step 9 Enable client certificate-based authentication. Choose **Administration > System > Admin Access > Authentication**.

a. Choose Client Certificate Based authentication type on the Authentication Method tab.

b. Choose the certificate authentication profile that you configured earlier.

c. Select the Active Directory instance name.

d. Click **Save**.

Here, you switch from password-based authentication to client certificate-based authentication. The certificate authentication profile that you configured earlier determines how the administrator's certificate is authenticated. The administrator is authorized using the external identity source, which in this example is Active Directory.

The Principal Name attribute from the certificate authentication profile is used to look up the administrator in Active Directory.

You have now configured Cisco ISE for administrator CAC authentication.

Related Topics

- Supported Common Access Card Standards, page 5-12
- Common Access Card Operation in Cisco ISE, page 5-12

Supported Common Access Card Standards

Cisco ISE supports U.S. government users who authenticate themselves using Common Access Card (CAC) authentication devices. A CAC is an identification badge with an electronic chip containing a set of X.509 client certificates that identify a particular employee. Access via the CAC requires a card reader into which you insert the card and enter a PIN. The certificates from the card are then transferred into the Windows certificate store, where they are available to applications such as the local browser running Cisco ISE.

Windows Internet Explorer Version 8 and 9 users running the Windows 7 operating system must install the ActiveIdentity ActivClient Version 6.2.0.133 third-party middleware software product for Cisco ISE to interoperate with CAC. For more information on ActiveIdentity security client products, please refer to http://www.actividentity.com/products/securityclients/ActivClient/.

Common Access Card Operation in Cisco ISE

The Admin portal can be configured so that you authentication with Cisco ISE is permitted only by using a client certificate. Credentials-based authentication—such as providing a user ID and password—is not permitted. In client certificate authentication, you insert a Common Access Card (CAC) card, enter a PIN and then enter the Cisco ISE Admin portal URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes your login session, based on the contents of the certificate. If this process is successful, you are presented with the Cisco ISE Monitoring and Troubleshooting home page and given the appropriate RBAC permissions.

Securing SSH Key Exchange Using Diffie-Hellman Algorithm

You can configure Cisco ISE to only allow Diffie-Hellman-Group14-SHA1 SSH key exchanges. To do this, you must enter the following commands from the Cisco ISE Command-Line Interface (CLI) Configuration Mode:

service sshd key-exchange-algorithm diffie-hellman-group14-sha1

Here's an example:

```
ise/admin# conf t
ise/admin (config)# service sshd key-exchange-algorithm diffie-hellman-group14-sha1
```

Configuring Cisco ISE to Send Secure Syslog for Common Criteria Compliance

The Common Criteria (CC) Compliance Certification requires Cisco ISE to send only TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring nodes.

Before You Begin

- Ensure that all the Cisco ISE nodes in your deployment are configured with appropriate server certificates. If you want your setup to be FIPS 140-2 compliant, the certificate keys must have a key size of 2048 bits or greater. See Chapter 8, "Managing Certificates" for more information.
- Enable the FIPS mode in the Admin portal. See Enabling FIPS Mode in Cisco ISE, page 5-8 for details.
- Ensure that the default network access authentication policy does not allow any version of the SSL protocol. Use the TLS protocol in the FIPS mode along with FIPS-approved algorithms. See Chapter 19, "Managing Authentication Policies" for more information.
- Ensure that all the nodes in your deployment are registered with the primary Administration node. Also, ensure that at least one node in your deployment has the Monitoring persona enabled to function as the secure syslog receiver (TLS server). See Chapter 3, "Setting Up Cisco ISE in a Distributed Environment" for more information.

To configure Cisco ISE to send TLS-protected secure syslog between the Cisco ISE nodes and to the Monitoring node, you must perform the following tasks:

1. Configure secure syslog remote logging target. See Configuring Secure Syslog Remote Logging Target, page 5-13 for more information.
2. Enable Logging Categories to send auditable events to the secure syslog remote logging target. See Enabling Logging Categories to Send Auditable Events to the Secure Syslog Target, page 5-14 for more information.
3. Disable TCP Syslog and UDP syslog collectors. Only TLS-protected syslog collectors should be enabled. See Disabling the TCP Syslog and UDP Syslog Collectors, page 5-15 for more information.

Configuring Secure Syslog Remote Logging Target

Cisco ISE system logs are collected and stored by log collectors for various purposes. You must choose the Cisco ISE Monitoring node as your log collector for configuring a secure syslog target.

Step 1 Log in to the Admin portal.

Step 2 Choose **Administration > System > Logging > Remote Logging Targets**.

Step 3 Click **Add**.

Step 4 Enter a name for the secure syslog server.

Step 5 Choose Secure Syslog from the Target Type drop-down list.

Step 6 Choose Enabled from the Status drop-down list.

Step 7 Enter the IP address of the Cisco ISE Monitoring node in your deployment.

Step 8 Enter 6514 as the port number. The secure syslog receiver listens on TCP port 6514.

Step 9 Choose the syslog facility code. The default is LOCAL6.

Step 10 Enter the maximum length. The default is 8192.

Step 11 Check the **Include Alarms for this Target** check box for alarms to be sent to the syslog server if your remote secure syslog logging target is not a Cisco ISE node.

If you are configuring your Cisco ISE node (Monitoring) as your secure syslog logging target, uncheck the **Include Alarms for this Target** check box.

Step 12 Check the **Buffer Messages When Server is Down** check box. If this option is checked, Cisco ISE stores the logs if the secure syslog receiver is unreachable, periodically checks the secure syslog receiver, and forwards them when the secure syslog receiver comes up.

a. Enter the buffer size.

b. Enter the Reconnect Timeout in seconds for Cisco ISE to periodically check the secure syslog receiver.

Step 13 Select a CA certificate that you want Cisco ISE to present to the secure syslog server.

Step 14 Uncheck the **Ignore Server Certificate validation** check box. You must not check this option.

Step 15 Click **Submit**.

Enabling Logging Categories to Send Auditable Events to the Secure Syslog Target

You must enable logging categories for Cisco ISE to send auditable events to the secure syslog target.

Step 1 Log in to the Admin portal.

Step 2 Choose **Administration > System > Logging > Logging Categories**.

Step 3 Click the radio button next to the AAA Audit logging category, then click **Edit**.

Step 4 Choose WARN from the Log Severity Level drop-down list.

Step 5 Move the secure syslog remote logging target that you created earlier to the Selected box.

Step 6 Click **Save**.

Step 7 Repeat this procedure to enable the following logging categories:

- Administrative and Operational Audit

- Posture and Client Provisioning Audit

Disabling the TCP Syslog and UDP Syslog Collectors

For Common Criteria compliance, you must disable the TCP and UDP syslog collectors, and only the secure syslog collector must be enabled.

Step 1 Log in to the Admin portal.

Step 2 Choose **Administration > System > Logging > Remote Logging Targets**.

Step 3 Click the radio button next to the TCP or UDP syslog collector.

Step 4 Click **Edit**.

Step 5 Choose Disabled from the Status drop-down list.

Step 6 Click **Save**.

Step 7 Repeat this process until you disable all the TCP or UDP syslog collectors.