CHAPTER 8

Administering Cisco ISE

This chapter describes the administrative activities for the Cisco Identity Services Engine (ISE) and how to perform them. The following topics are covered:

Logging In

The Cisco ISE GUI is supported on the following HTTPS-enabled following browsers:

- Mozilla Firefox version 3.6
- Mozilla Firefox version 9
- Microsoft Internet Explorer version 8
- Microsoft Internet Explorer version 9 (in Internet Explorer version 8 compatibility mode).

Note The Cisco ISE GUI is not supported on Internet Explorer version 8 running in Internet Explorer 7 compatibility mode. For a collection of known issues regarding Microsoft Internet Explorer version 8, see the "Known Issues" section of the *Release Notes for Cisco Identity Services Engine, Release 1.1*.

After you have installed Cisco ISE as described in the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*, you can log into Cisco ISE.

To log into the Cisco ISE GUI, complete the following steps:

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

The ISE login window appears.

Step 2 Enter the Username and Password which you would have configured during initial Cisco ISE Setup.

The Password field is case-sensitive.

If you have to reset Administrator password, refer to the "Performing Post-Installation Tasks" chapter of the *Cisco Identity Services Engine Hardware Installation Guide, Release 1.1*.

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

You can now access the menus in the ISE user interface.

Note Any time your login is unsuccessful, click the **Problem logging in?** link in the Login window and follow the instructions in Step 2.

Tip The minimum required screen resolution to view the Cisco ISE GUI and for a better user experience is 1280X800 pixels.

Related Topic

Administrator Lockout Following Failed Login Attempts, page 8-2

Administrator Lockout Following Failed Login Attempts

If you enter an incorrect password for your specified administrator user ID enough times, the Cisco ISE user interface "locks you out" of the system, adds a log entry in the **Operations > Reports > Catalog > Server Instance > 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 1.1*. The number of failed attempts that is required to disable the administrator account is configurable according to the guidelines that are described in Configuring a Password Policy for Administrator Accounts, page 4-62. After an administrator user account gets locked out, an email is sent to the associated administrator user.

Disabled System administrators' status can be enabled by any Super Admin including AD users.

Enabling FIPS Mode in Cisco ISE

Cisco ISE supports Federal Information Processing Standard (FIPS) 140-2, the 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.

In addition, 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 Key Management measures. While in FIPS mode, any attempt to perform functions using a non-FIPS compliant algorithm fails, and, as such, certain authentication functionality is disabled. For more details, including protocol support, see the "Support for FIPS 140-2 Implementation" section on page 1-3 and "Support Common Access Card Functions" section on page 1-3 section in Chapter 1, "Overview of Cisco ISE."

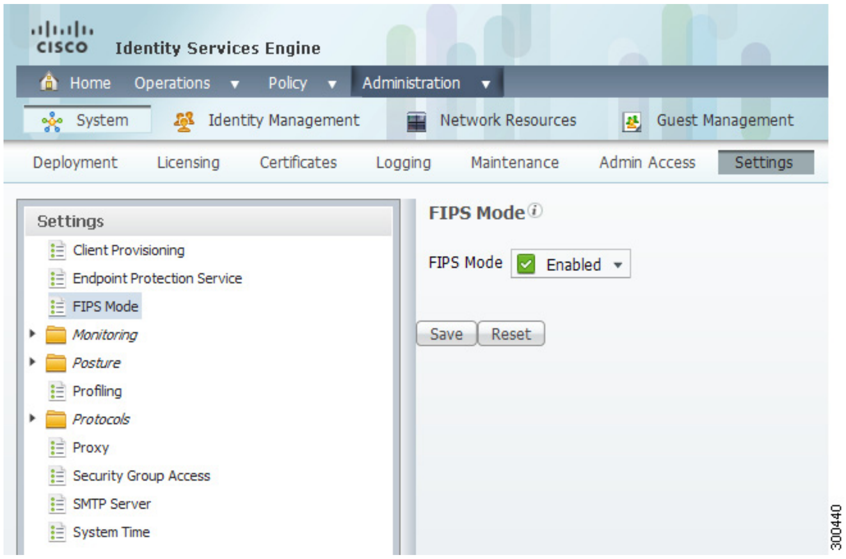
When FIPS mode is enabled, The Cisco ISE administrator interface displays a FIPS mode icon in the upper right portion of the screen, immediately to the left of the node name.

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

To enable FIPS 140-2 compliant operations on Cisco ISE, complete the following steps:

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

Figure 8-1 Administration > System > Settings > FIPS Mode



FIPS Mode: Enabled

Note 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 those protocols have been addressed appropriately.

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

Step 3 Click **Save**. Cisco ISE automatically prompts you to restart your machine.

Once you have enabled FIPS mode, you must also 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 ISE node, and then restarting each secondary node, one node at a time.

To fully enable FIPS 140-2 compliance once you have turned on this setting, be sure to also configure the FIPS-specific functions that are included under "Next Steps" below and then reboot all Cisco ISE nodes in your deployment.

Next Steps

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

- Adding and Editing Devices, page 6-3
- Generating a Self-Signed Certificate, page 13-7
- Generating a Certificate Signing Request, page 13-8
- Creating RADIUS Servers, page 16-23

In addition, you may wish 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 8-4. 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.

Cisco NAC Agent Requirements when FIPS Mode is Enabled

The (temporal) Cisco NAC Web Agent and (persistent) Cisco NAC Agent always look 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 with TLS1.0 enabled to allow for Cisco ISE posture assessment functions to operate on client machines accessing the network. See the following guidelines:

- 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.
- The Cisco NAC Web Agent does not automatically enable the TLS 1.0 settings in Windows Internet Explorer.
- You also need to ensure that TLS 1.0 settings are enabled for end users launching Mozilla Firefox or Google Chrome browsers on client machines going through Cisco ISE posture assessment.

Configuring Cisco ISE for Administrator CAC Authentication

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 of, for example, the U.S Department of Defense (DoD). Access via the CAC requires a card reader into which the user inserts the card and enters 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.

The administrator user interface can be configured so that administrators can only authenticate themselves by using a client certificate (credentials-based authentication—such as a user ID and password—is not required or even permitted). In this setup, an administrator inserts the CAC card, enters the correct PIN, then enters the Cisco ISE administrator user interface URL into the browser address field. The browser forwards the certificate to Cisco ISE, and Cisco ISE authenticates and authorizes the administrator, based on the contents of the certificate. If this process is successful, the user is presented with the Cisco ISE Monitoring and Troubleshooting home page, and is given the appropriate RBAC permissions.

The following sections describe how to set up Cisco ISE to allow certificate-based administrator authentication using a CAC device:

- Preliminary Setup Done by ISE Administrator, page 8-5
- Step 1: Enable FIPS Mode, page 8-6
- Step 2: Configure Active Directory, page 8-6
- Step 3: Create Certificate Authentication Profile, page 8-9
- Step 4: Import CA Certificates into ISE Certificate Trust Store, page 8-9
- Step 5: Configure CA Certificates for Revocation Status Check, page 8-10
- Step 6: Enable Client Certificate-Based Authentication, page 8-12
- Step 7: Configure Admin Group to AD Group Mapping, page 8-13
- Step 8: Configure Admin Authorization Policy, page 8-16

Note 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/.

Preliminary Setup Done by ISE Administrator

Before beginning configuration, ensure that the following is done:

- The DNS server setting in Cisco ISE is set correctly for Active Directory.
- 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

Step 1: Enable FIPS Mode

Note This step is optional in CAC configuration. 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*.

To enable FIPS 140-2 compliant mode on Cisco ISE, see the guidelines and subsequent setup steps as described in Enabling FIPS Mode in Cisco ISE, page 8-2.

Tip You will be prompted to restart all Cisco ISE nodes in your deployment when enabling FIPS mode.

Step 2: Configure Active Directory

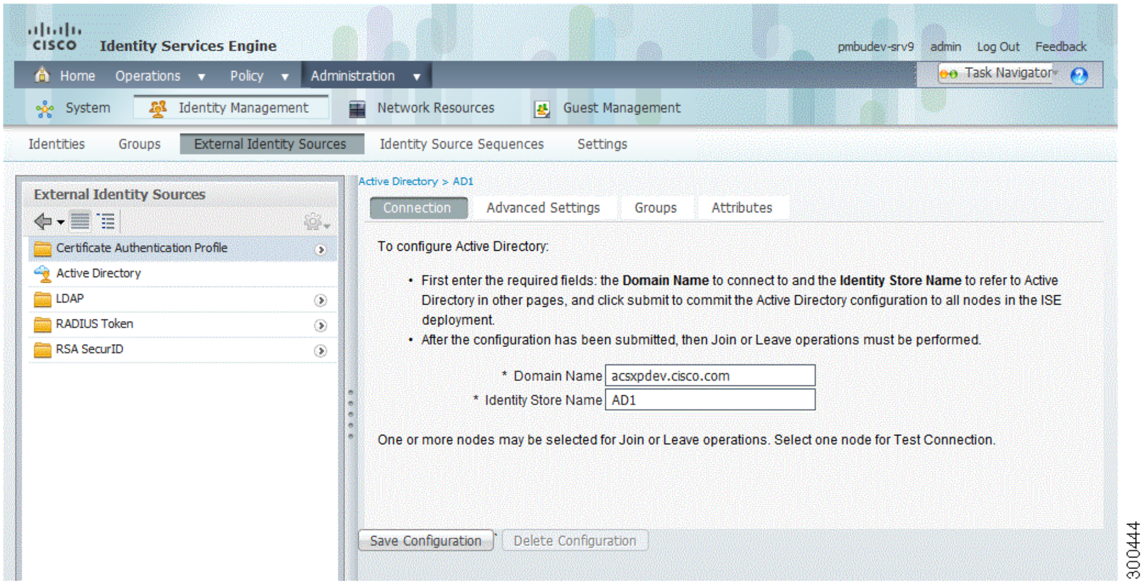
Active Directory is used to authenticate and authorize administrators using CAC cards. See Microsoft Active Directory, page 5-4.

To configure Cisco ISE to use Active Directory in this example, complete the following steps:

Step 1 Navigate to **Administration > Identity Management > External Identity Sources > Active Directory**.

Step 2 Enter the Active Directory Domain Name and an Identity Store Name, then click **Save Configuration**.

Figure 8-2 Using Active Directory for CAC



To configure Active Directory:

- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in other pages, and click submit to commit the Active Directory configuration to all nodes in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

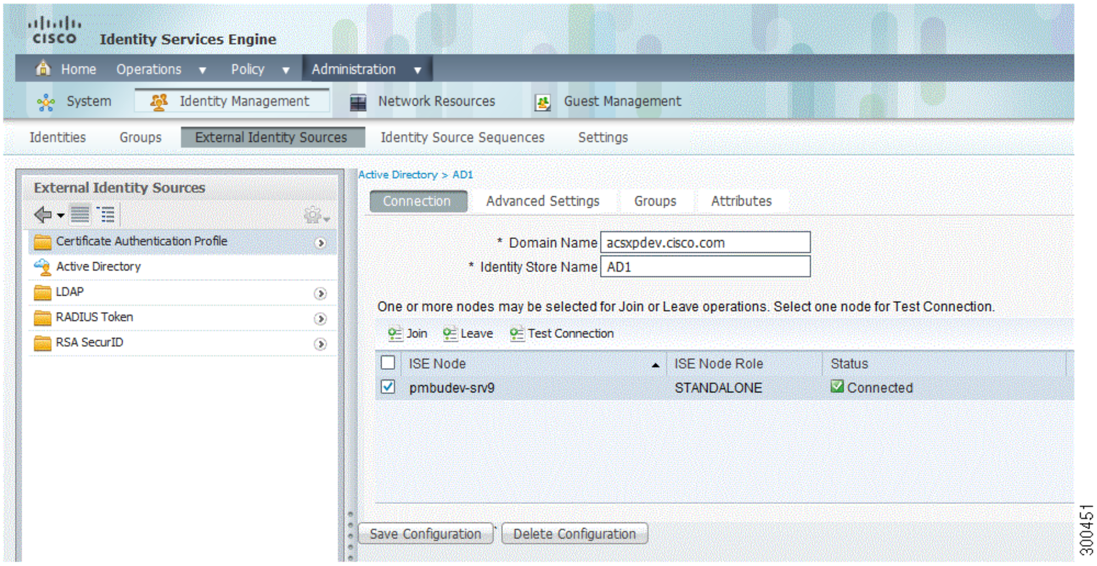
* Domain Name acsxpdev.cisco.com
* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. Select one node for Test Connection.

Step 3 Click **Save Configuration**.

Step 4 Join your Cisco ISE deployment nodes to Active Directory.

Figure 8-3 Join Cisco ISE to Active Directory for CAC



* Domain Name acsxpdev.cisco.com

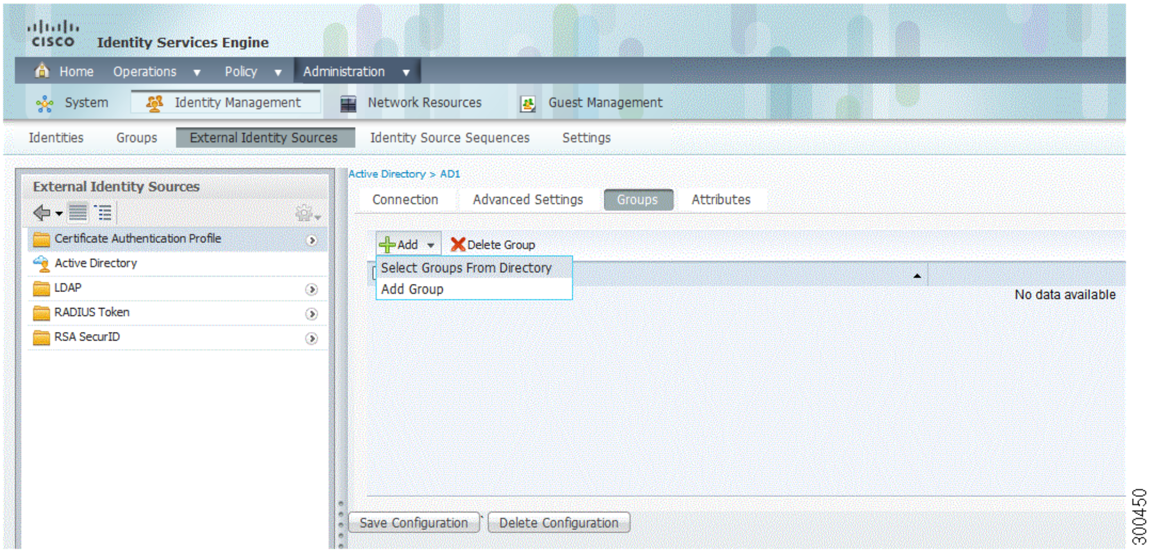
* Identity Store Name AD1

One or more nodes may be selected for Join or Leave operations. Select one node for Test Connection.

□ ISE Node	ISE Node Role	Status
☑ pmbudev-srv9	STANDALONE	☑ Connected

Step 5 You will want to eventually map Administrator Groups to AD Groups; therefore, you need to import some AD Groups to which your administrator belongs. Click the Groups tab, click **Add**, and choose the **Select Groups From Directory** drop-down option.

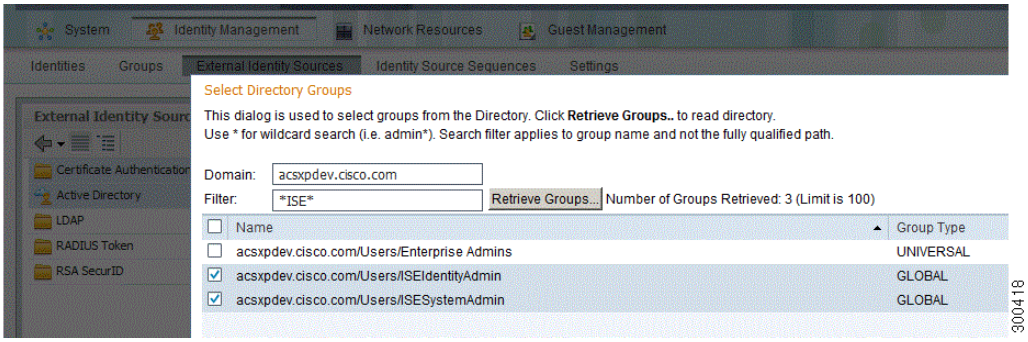
Figure 8-4 Select Groups from Directory for CAC



No data available

Step 6 In the resulting pop-up dialog, select one or more directory groups. In this example, two Cisco ISE administrator groups are defined in AD.

Figure 8-5 Select Directory Groups for CAC



Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory.
Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

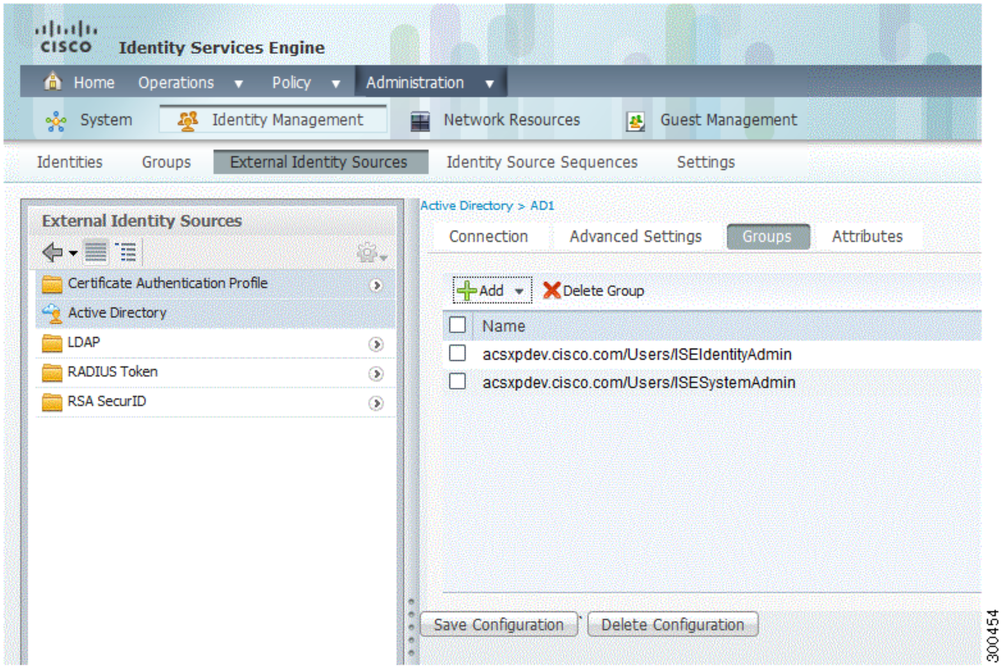
Domain: acsxpdev.cisco.com
Filter: *ISE*

Number of Groups Retrieved: 3 (Limit is 100)

☐	Name	Group Type
☐	acsxpdev.cisco.com/Users/Enterprise Admins	UNIVERSAL
☑	acsxpdev.cisco.com/Users/ISEIdentityAdmin	GLOBAL
☑	acsxpdev.cisco.com/Users/ISESystemAdmin	GLOBAL

Step 7 After selecting the groups, be sure to press the **Save Configuration** button again. Otherwise, your group selections will not be saved.

Figure 8-6 Save CAC Configuration



☐	Name
☐	acsxpdev.cisco.com/Users/ISEIdentityAdmin
☐	acsxpdev.cisco.com/Users/ISESystemAdmin

Step 3: Create Certificate Authentication Profile

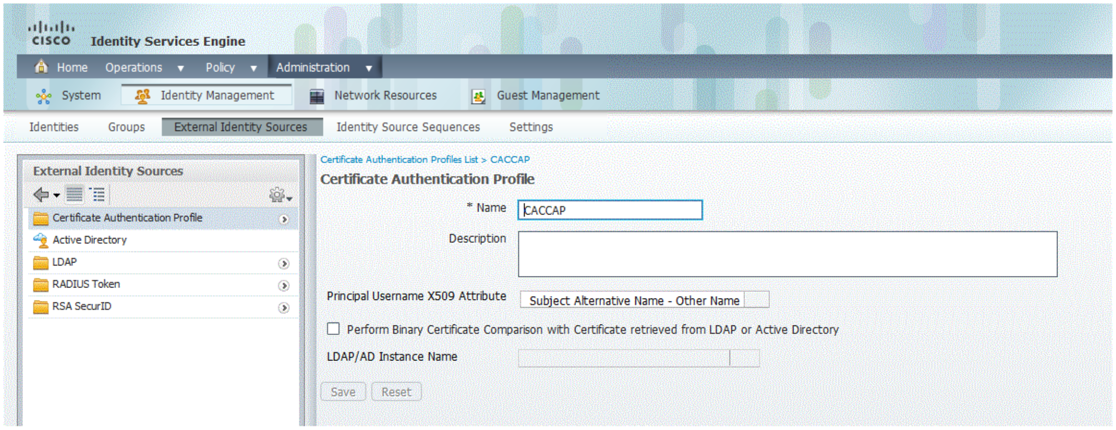
The Certificate Authentication Profile tells ISE where to find the user's identity in the client certificate. See Adding or Editing a Certificate Authentication Profile, page 5-2.

To create the authentication profile in this example, complete the following steps:

Step 1 Navigate to **Administration > Identity Management > External Identity Sources > Certificate Authentication Profile**.

Step 2 Click **Add** to bring up the profile configuration pane.

Figure 8-7 Create Authentication Profile for CAC



Certificate Authentication Profile

* Name: CACCAP

Description:

Principal Username X509 Attribute: Subject Alternative Name - Other Name

☐ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory

LDAP/AD Instance Name:

Save Reset

Step 3 Enter the profile name and an optional description.

Step 4 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.")

Step 5 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 (which was specified this earlier in Step 2: Configure Active Directory, page 8-6).

Step 4: Import CA Certificates into ISE Certificate Trust Store

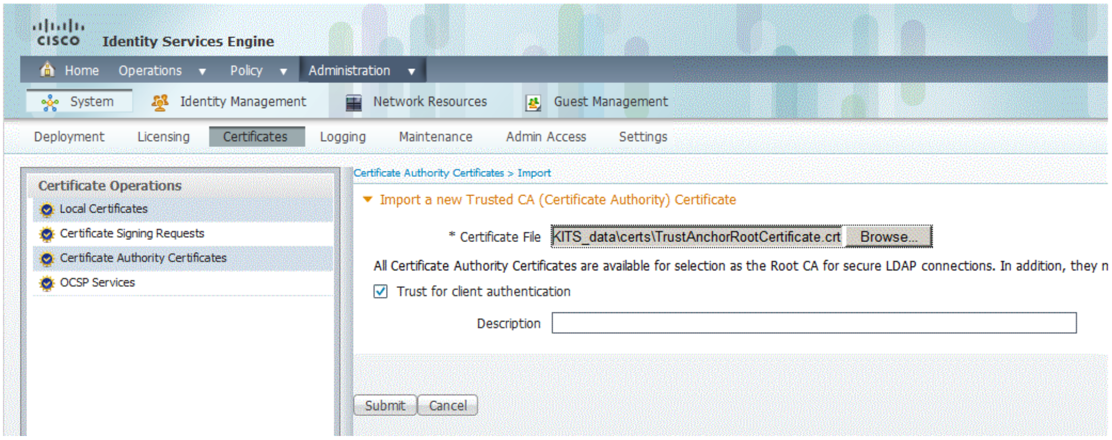
The ISE application server will not accept a client certificate unless the CA certificates in the client certificate's trust chain are placed in the ISE trust store. This means you will need to import the appropriate CA certificate into the ISE trust store. See Importing Root and CA Certificates into the CTL of the Primary Node, page 13-23.

Step 1 Navigate to **Administration > System > Certificates > CA Certificates**.

Step 2 On the list page, click **Add**.

Step 3 Select the file containing the CA certificates you want to import, and check the **Trust for client authentication** check box.

Figure 8-8 Specify CA Certificates for CAC



* Certificate File KITS_data\certs\TrustAnchorRootCertificate.crt

All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they n

☑ Trust for client authentication

Description

Step 4 Click **Submit**.

Tip Cisco recommends that you import the CA certificates that are needed to trust client certificates *before* you enable client certificate-based authentication. Importing CA certificates after enabling client certificate-based authentication requires an application server restart on all ISE nodes in your deployment.

If you must import a CA certificate after enabling client certificate-based authentication, you have the option to defer the restart. This is convenient if you are going to import multiple CA certificates, and you wish to avoid having to restart each time. If you defer the restart, a Deferred Restart notification appears on the Notifications tab, which is accessible at the bottom right portion of the page. You must access this tab and enable the restart for your CA certificate changes to take effect.

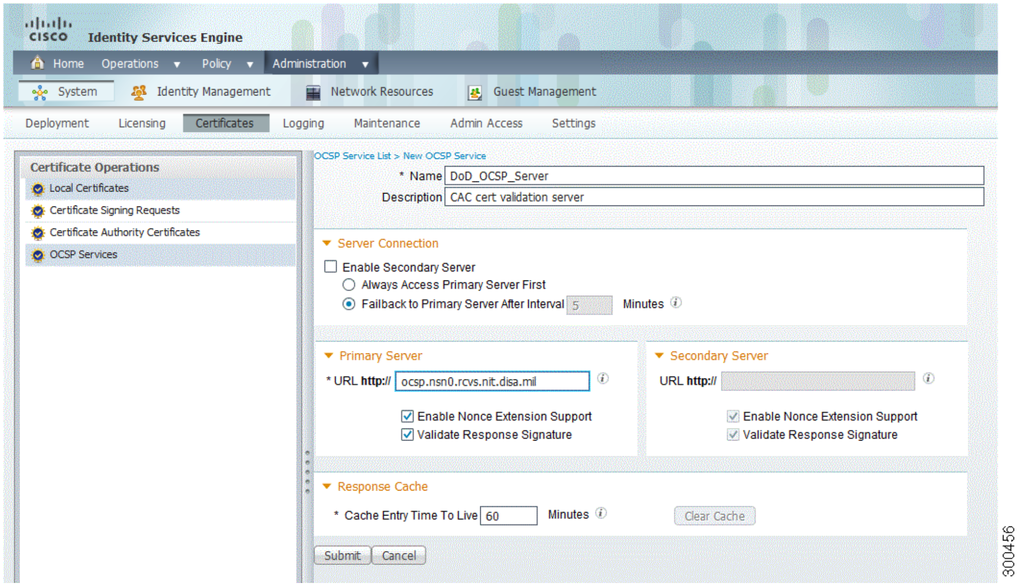
Step 5: Configure CA Certificates for Revocation Status Check

A certificate authority may revoke or declare a certificate "unusable" prior to its expiration date. You can use Cisco ISE to query the certificate authority to verify the revocation status of a certificate via the Online Certificate Status Protocol (OCSP) server or the Certificate Revocation Lists (CRLs). You can perform this check when a client certificate is authenticated. See OCSP Services, page 13-25 and Editing a Certificate Authority Certificate, page 13-19.

Step 1 If you are going to use OCSP, first navigate to **Administration > System > Certificates > OCSP Services**. Otherwise, skip to Step 3.

Step 2 Enter a name for the OCSP server, an optional description, and the URL of the server.

Figure 8-9 Specify CA Certificates for Revocation Using OCSP



OCSP Service List > New OCSP Service

* Name DoD_OCSP_Server

Description CAC cert validation server

Server Connection

□ Enable Secondary Server

○ Always Access Primary Server First

● Failback to Primary Server After Interval 5 Minutes

Primary Server

* URL http:// ocsp.nsn0.rcvs.nit.disa.mil

☑ Enable Nonce Extension Support

☑ Validate Response Signature

Secondary Server

URL http://

☑ Enable Nonce Extension Support

☑ Validate Response Signature

Response Cache

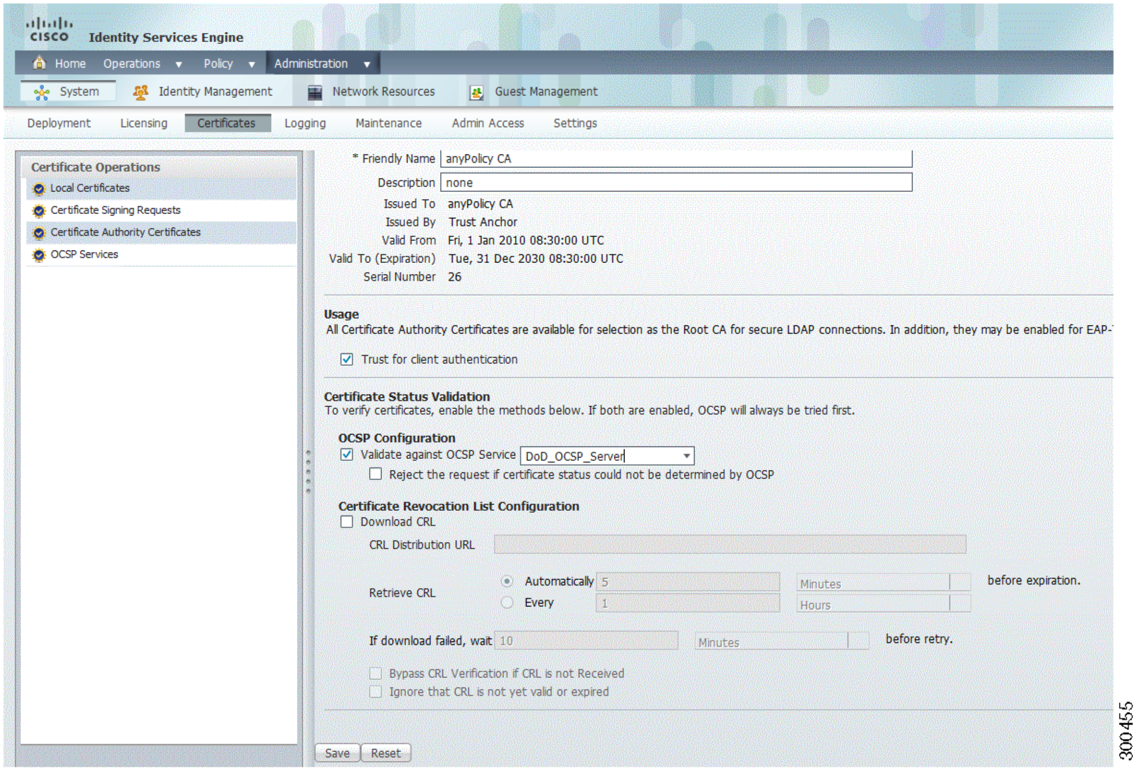
* Cache Entry Time To Live 60 Minutes

Step 3 Navigate to **Administration > System > Certificates > CA Certificates**.

Step 4 For each CA certificate that can sign a client certificate, you must specify how to do the revocation status check for that CA. Select a CA certificate from the list and click **Edit**.

Step 5 On the edit page that appears, you can select OCSP or the CRL validation. If you select OCSP, you must select an OCSP service to use for that CA. If you select CRL, you must specify the CRL Distribution URL and other applicable configuration parameters.

Figure 8-10 Specify CA Certificates for Revocation Using CRL



* Friendly Name: anyPolicy CA
Description: none
Issued To: anyPolicy CA
Issued By: Trust Anchor
Valid From: Fri, 1 Jan 2010 08:30:00 UTC
Valid To (Expiration): Tue, 31 Dec 2030 08:30:00 UTC
Serial Number: 26

Usage
All Certificate Authority Certificates are available for selection as the Root CA for secure LDAP connections. In addition, they may be enabled for EAP-

☑ Trust for client authentication

Certificate Status Validation
To verify certificates, enable the methods below. If both are enabled, OCSP will always be tried first.

OCSP Configuration
☑ Validate against OCSP Service: DoD_OCSP_Server
□ Reject the request if certificate status could not be determined by OCSP

Certificate Revocation List Configuration
□ Download CRL
CRL Distribution URL:
Retrieve CRL: ● Automatically 5 Minutes before expiration.
○ Every 1 Hours
If download failed, wait 10 Minutes before retry.
□ Bypass CRL Verification if CRL is not Received
□ Ignore that CRL is not yet valid or expired

Step 6 Click **Save**.

Step 6: Enable Client Certificate-Based Authentication

Switch from the default password-based authentication to certificate-based authentication.

The method you use to authenticate the administrator certificate is specified by a Certificate Authentication Profile. User authorization is done through an external identity store, which in this case is Active Directory. Note that the Principal Name attribute from the Certificate Authentication Profile is used to look up the user in Active Directory. See Configuring the Simple Authentication Policy, page 16-26.

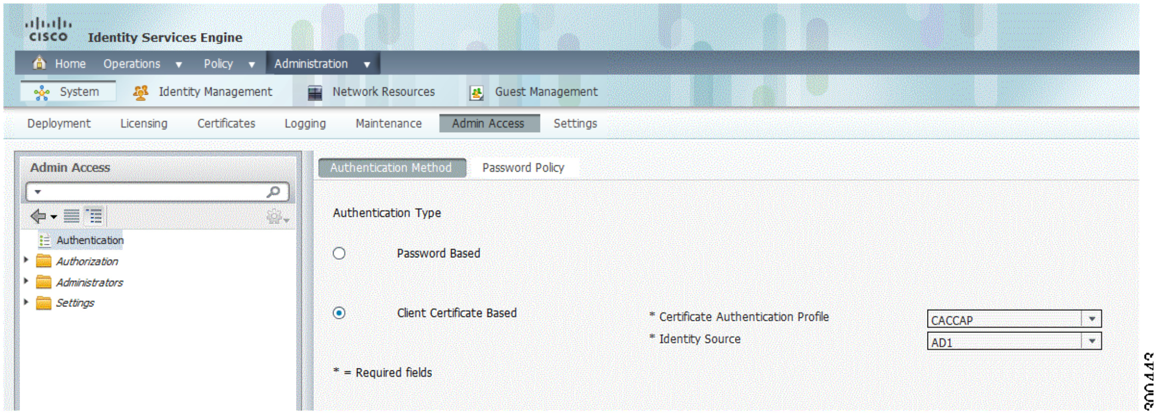
To enable client certificate-based authentication in this example, complete the following steps:

Step 1 Navigate to **Administration > System > Admin Access > Authentication**.

Step 2 On the Authentication Method tab, select the **Client Certificate Based** option.

Step 3 Select the Certificate Authentication Profile that you created earlier. For Identity Source, select the Active Directory instance name.

Figure 8-11 Enable Certificate-Based Authentication for CAC



Authentication Type

○ Password Based

● Client Certificate Based

* Certificate Authentication Profile: CACCAP

* Identity Source: AD1

* = Required fields

Note You will be prompted to restart the application server on all Cisco ISE nodes in your deployment, when enabling client certificate-based authentication.

Step 7: Configure Admin Group to AD Group Mapping

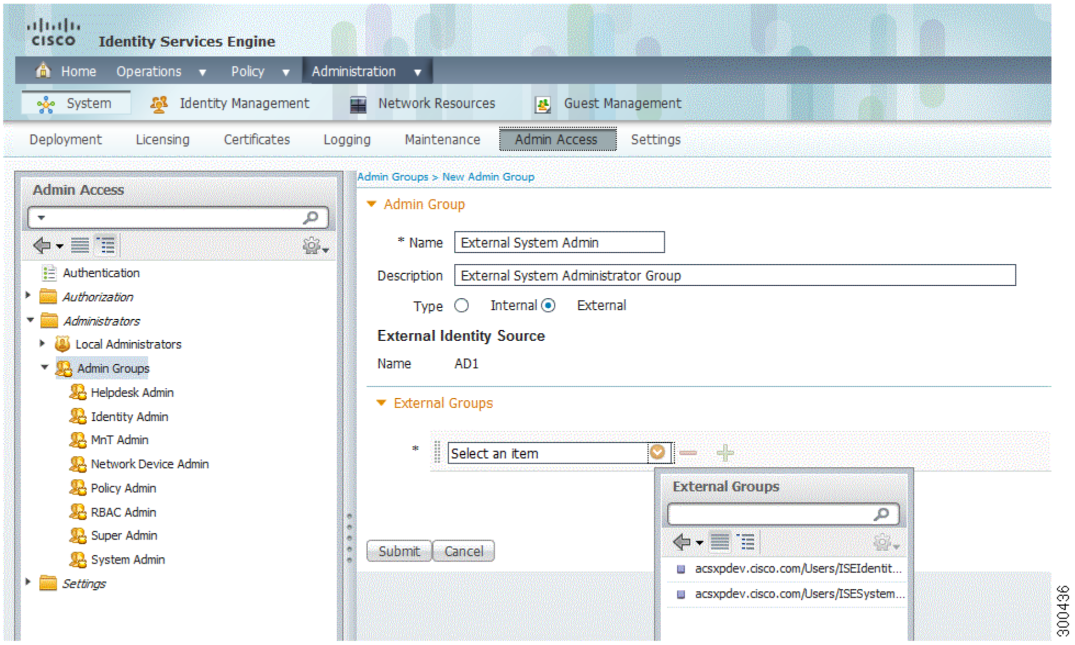
Define one or more Cisco ISE Admin Groups, and map each one to Active Directory groups. This allows user authorization to determine the RBAC permissions for the administrator, based on group membership in Active Directory. See Managing Admin Access (RBAC) Policies, page 4-49.

Note You cannot map predefined Admin Groups to AD groups; you must create new Admin Groups, and you *must* do this step after you have enabled client certificated-based authentication (Step 6: Enable Client Certificate-Based Authentication, page 8-12). Otherwise, you will not see any available AD Groups to which you can map.

Step 1 Navigate to **Administration** > **System** > **Admin Access** > **Administrators** > **Admin Groups**.

Step 2 Click **Add** in the table header to bring up the new Admin Group configuration pane.

Figure 8-12 Configure Admin Group to AD Group Mapping for CAC



* Name: External System Admin

Description: External System Administrator Group

Type: ○ Internal ● External

External Identity Source

Name: AD1

External Groups

* Select an item

External Groups

- acsxpdev.cisco.com/Users/ISEIdentit...
- acsxpdev.cisco.com/Users/ISESystem...

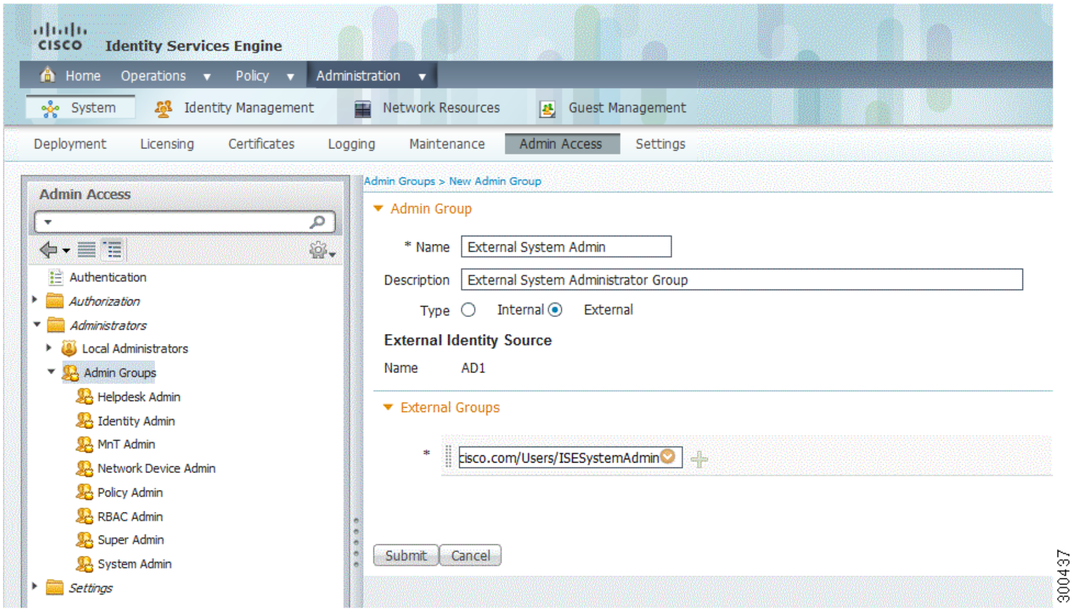
Step 3 Enter a name and optional description for the new Admin Group.

Step 4 For the group Type, select **External**. The instance name for Active Directory appears.

Step 5 Under External Groups, where it says "Select an item," click the down arrow to display a list of the AD Groups that you imported when setting up Active Directory.

Step 6 Select the AD Group to which you want this Admin Group to map. If you require a one-to-many mapping, click the "+" (plus) icon and select another AD Group.

Figure 8-13 Configure Additional Admin Group to AD Group Mapping for CAC



Admin Group

* Name: External System Admin

Description: External System Administrator Group

Type: ○ Internal ● External

External Identity Source

Name: AD1

External Groups

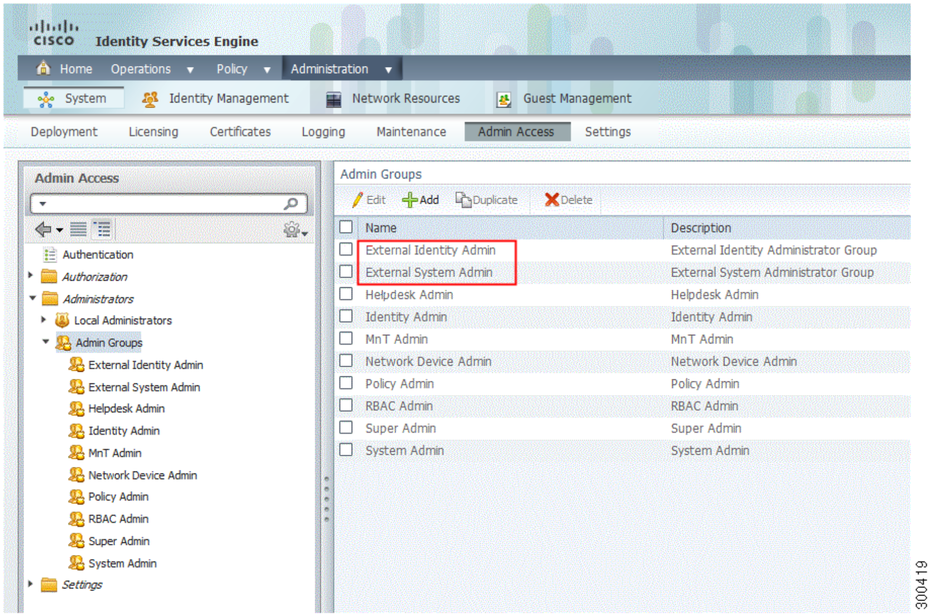
* cisco.com/Users/ISESystemAdmin

In this example, you have created an Admin Group called External System Admin and mapped it to an AD Group called ISESystemAdmin.

Step 7 Click **Submit** to save the new Admin Group.

To further illustrate the different RBAC permissions that you can assign to Admin Groups, you have created a second group called External Identity Admin, which is mapped to the AD Group ISEIdentityAdmin.

Figure 8-14 Display New Admin Group for CAC



Admin Groups

□	Name	Description
□	External Identity Admin	External Identity Administrator Group
□	External System Admin	External System Administrator Group
□	Helpdesk Admin	Helpdesk Admin
□	Identity Admin	Identity Admin
□	MnT Admin	MnT Admin
□	Network Device Admin	Network Device Admin
□	Policy Admin	Policy Admin
□	RBAC Admin	RBAC Admin
□	Super Admin	Super Admin
□	System Admin	System Admin

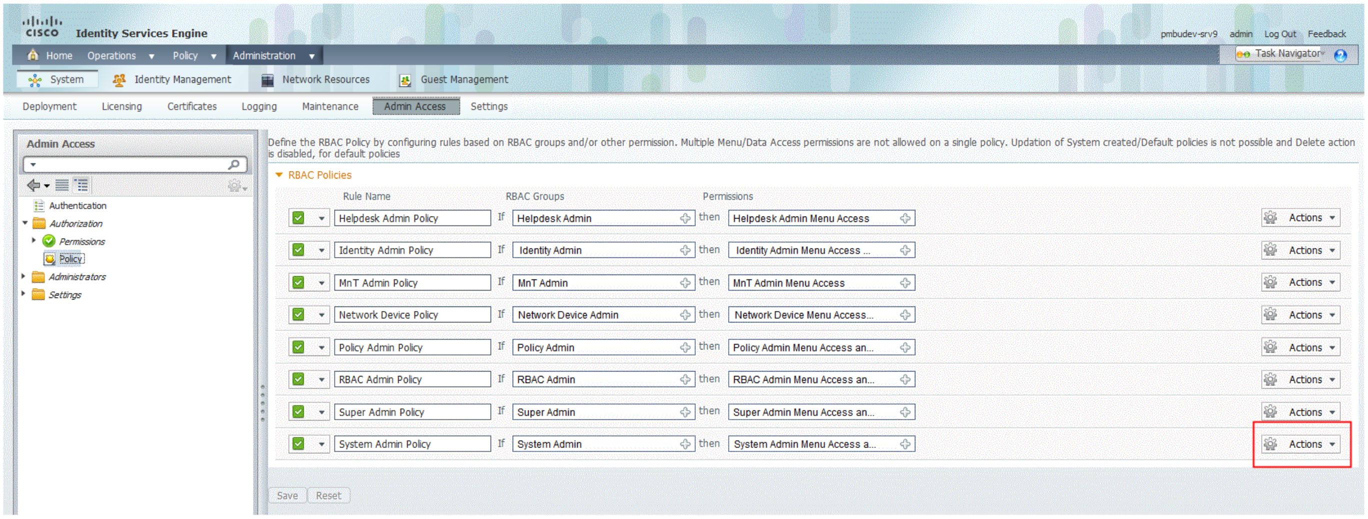
Step 8: Configure Admin Authorization Policy

Assign RBAC permissions to each of the Admin Groups created in Step 7: Configure Admin Group to AD Group Mapping, page 8-13. See Configuring Authorization Policies, page 17-14.

Step 1 Navigate to **Administration > System > Admin Access > Authorization > Policy**.

This page shows the RBAC polices that are in effect for administrative access. You can add a new by clicking the Actions drop-down list on the right and selecting **Insert new policy below**.

Figure 8-15 Insert New Admin Policy for CAC

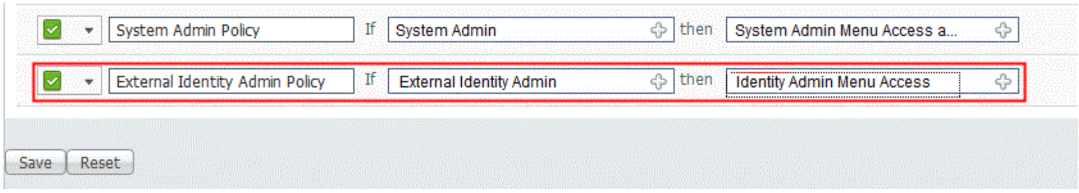

Cisco Identity Services Engine
pmbudev-srv9 admin Log Out Feedback
Home Operations Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Admin Access
Authentication
Authorization
Permissions
Policy
Administrators
Settings
RBAC Policies
Save Reset
300441

Define the RBAC Policy by configuring rules based on RBAC groups and/or other permission. Multiple Menu/Data Access permissions are not allowed on a single policy. Updation of System created/Default policies is not possible and Delete action is disabled, for default policies

	Rule Name		RBAC Groups		Permissions	
☑	Helpdesk Admin Policy	If	Helpdesk Admin	then	Helpdesk Admin Menu Access	Actions
☑	Identity Admin Policy	If	Identity Admin	then	Identity Admin Menu Access ...	Actions
☑	MnT Admin Policy	If	MnT Admin	then	MnT Admin Menu Access	Actions
☑	Network Device Policy	If	Network Device Admin	then	Network Device Menu Access...	Actions
☑	Policy Admin Policy	If	Policy Admin	then	Policy Admin Menu Access an...	Actions
☑	RBAC Admin Policy	If	RBAC Admin	then	RBAC Admin Menu Access an...	Actions
☑	Super Admin Policy	If	Super Admin	then	Super Admin Menu Access an...	Actions
☑	System Admin Policy	If	System Admin	then	System Admin Menu Access a...	Actions

Step 2 Create a new policy called External Identity Admin Policy, which specifies the new External Identity Admin group and assigns it Identity Admin Menu Access permissions.

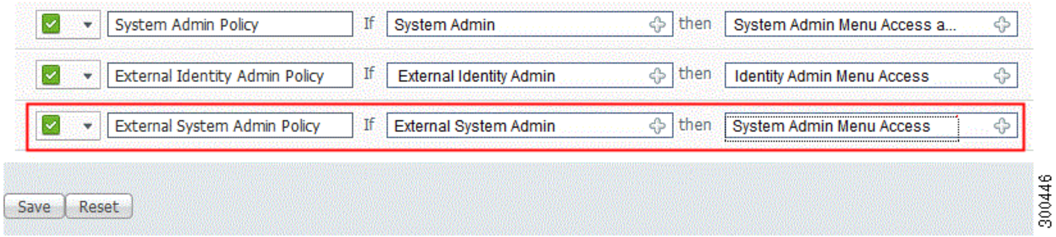
Figure 8-16 Specify the New Admin Policy Attributes for CAC



☑	System Admin Policy	If	System Admin	then	System Admin Menu Access a...
☑	External Identity Admin Policy	If	External Identity Admin	then	Identity Admin Menu Access

Step 3 Create another policy for your other new Admin Group, External System Admin.

Figure 8-17 Create Additional Admin Policy for CAC



☑ System Admin Policy If System Admin then System Admin Menu Access a...

☑ External Identity Admin Policy If External Identity Admin then Identity Admin Menu Access

☑ External System Admin Policy If External System Admin then System Admin Menu Access

Step 4 Click **Save** after adding the policies.

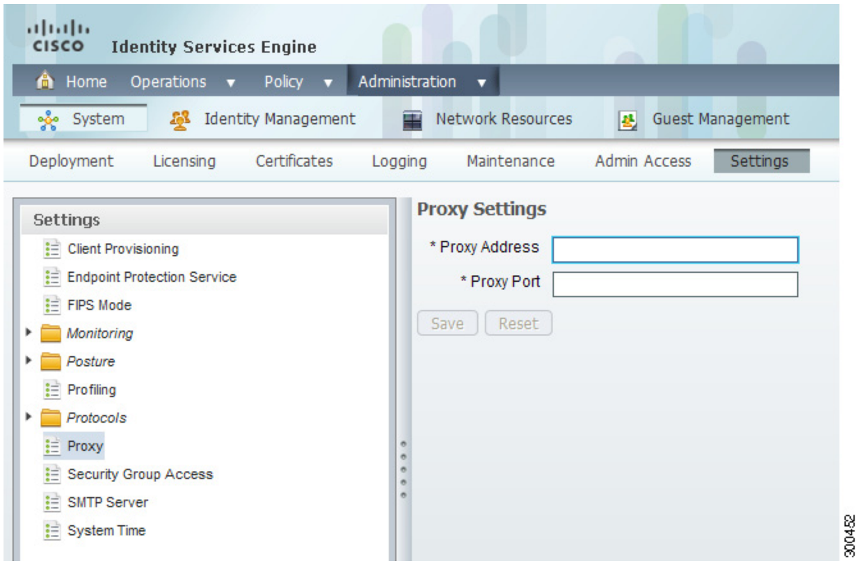
Specifying Proxy Settings in Cisco ISE

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 Cisco ISE user interface to specify proxy properties.

To specify proxy settings for Cisco ISE, complete the following steps:

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

Figure 8-18 Administration > System > Settings > Proxy



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

Step 3 Click **Save**.

Next Steps

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

- Enabling and Disabling the Client Provisioning Service, page 19-25
- Downloading Client Provisioning Resources Automatically, page 19-26

Troubleshooting Topics

- Cannot Download Remote Client Provisioning Resources, page D-10

System Time and NTP Server Settings

Cisco ISE allows you to view the system time settings through the administrator user interface. The Cisco Application Deployment Engine (ADE) operating system, which is the operating system in the 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. This procedure ensures that your logs are always reliable. 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.

Note You must configure the system time and NTP server settings on each ISE node in your deployment individually.

Prerequisite:

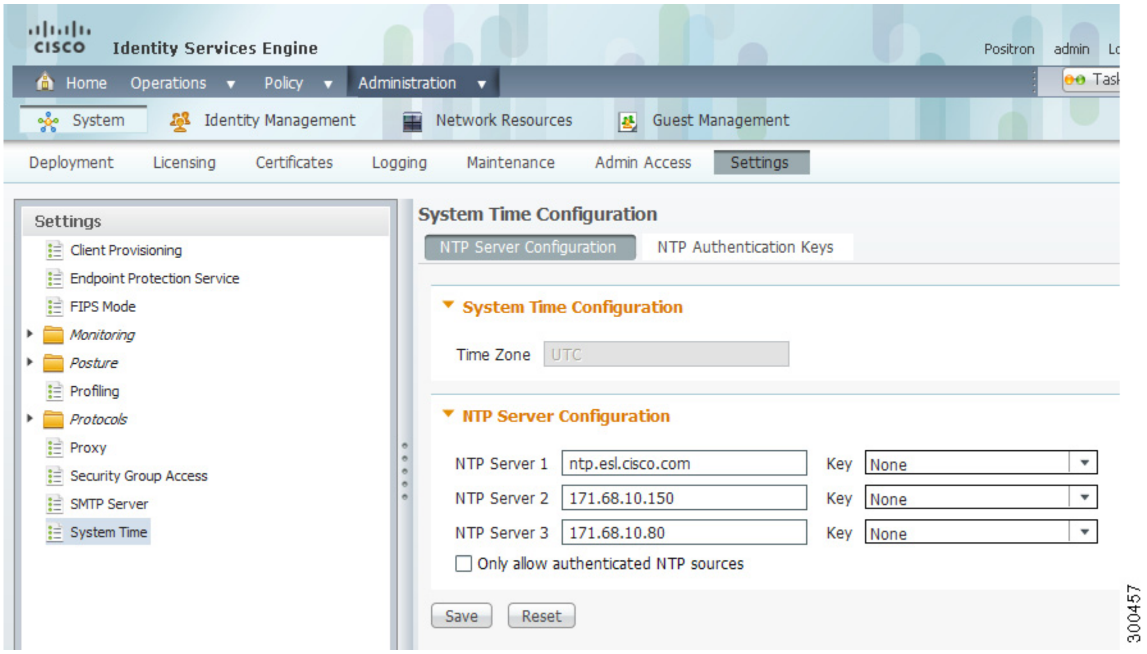
Every ISE administrator account is assigned one or more administrative roles. To perform the operations that are described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See “Cisco ISE Admin Group Roles and Responsibilities” for more information on the various administrative roles and the privileges that are associated with each of them.

To view the system time settings and configure NTP server settings, complete the following steps:

Step 1 From your primary ISE node, choose **Administration > System > Settings**.

Step 2 From the Settings navigation pane on the left, click **System Time**.

Figure 8-19 Administration > System > Settings > System Time



System Time Configuration

System Time Configuration

Time Zone: UTC

NTP Server Configuration

NTP Server 1: ntp.esl.cisco.com Key: None
NTP Server 2: 171.68.10.150 Key: None
NTP Server 3: 171.68.10.80 Key: None

□ Only allow authenticated NTP sources

Note If you want to view the system time settings and configure NTP server settings on a secondary Cisco ISE node, you must log into the user interface of the secondary node and choose **Administration > System > Settings > System Time**.

The timezone that you have configured appears in the Time Zone field. You cannot edit this value from the ISE user interface. To configure the timezone, you must enter the following command from the ISE CLI:

clock timezone *timezone*

For more information on the **clock timezone** command, see the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

Step 3 In the NTP Server Configuration area, enter the IP address of your NTP servers.

If you have only one NTP server in your network, enter the IP address in the Primary Server text box. If you have two NTP servers, enter the IP address in the **NTP Server 1** and **NTP Server 2** text boxes, respectively.

Note If you enter the same IP address for NTP server 1 and 2, then when NTP server 1 is down, Cisco ISE cannot access any other NTP server, because you have specified the same identity as the "other" NTP server. Cisco recommends that you verify the IP address of NTP server 2 and ensure that it is different than NTP server 1.

Step 4 If you want to restrict Cisco ISE to use only authenticated NTP servers to keep system and network time, check (enable) the **Only allow authenticated NTP servers** check box.

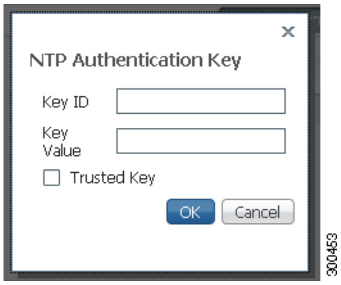
Step 5 If any of the servers that you specify requires authentication via an authentication key, be sure to also click the **NTP Authentication Keys** tab and specify one or more authentication keys, as follows:

a. Click **Add**.

b. Enter the necessary **Key ID** and **Key Value**, and specify whether the key in question is trusted by activating or deactivating the **Trusted Key** option.

c. Click **OK**.

Figure 8-20 Administration > System > Settings > System Time



NTP Authentication Key

Key ID

Key Value

□ Trusted Key

d. When you are finished entering the NTP Server Authentication Keys, return to the **NTP Server Configuration** tab.

Step 6 Click **Save** to save the NTP server settings.

The saved NTP Authentication Keys are displayed in the NTP Server Configuration page, and when you place your cursor over to the hostname in the top right corner of the Cisco ISE dashboard window, the current server role and server system time appear in the Server Information quick-view pop-up.

Note We recommend that you set all Cisco ISE nodes to the Coordinated Universal Time (UTC) timezone. This procedure ensures that the reports and logs from the various nodes in your deployment are always in sync with regard to the timestamps.

Configuring Email Settings

This section shows you how to specify the address of the email server and the name that is displayed for this address. This address is used for sending and receiving log messages.

Note Depending upon the roles assigned to your account, you may or may not be able to perform the operations or see the options described in the following procedure. For more information, see Understanding the Impact of Roles and Admin Groups.

To specify email settings for the mail server, complete the following steps:

Step 1 Select **Administration > System > Settings**

Step 2 In the left-hand Settings panel, expand **Monitoring** and then choose **Email Settings**.

Step 3 In the Mail Server field, enter the hostname or IPV4 address of the outgoing SMTP mail server. This information is required to send email notifications for alarms.

Note A hostname requires a format such as mailman.cisco.com. An IPv4 address requires a format such as, 192.168.1.1.

Step 4 Enter a name or email address (such as admin@somedomain.com) in the Mail From field. This name or email address is what users see when they receive a message from the mail server.

Step 5 Click **Submit.**

Configuring System Alarm Settings

System alarms notify you of critical conditions that are encountered. System alarms are standard and cannot be created or deleted.

This section describes the available system alarms, shows you how to enable and disable the alarms, and how to configure to receive notification. Cisco ISE provides the following system alarms:

- Distributed Management—This alarm is sent during the following operations:
  - Registering a node (Success or Failure)
  - Deleting a node
  - Unregistering a node (Success or Failure)
  - Updating a node (Success or Failure)
- License Enforcement—This alarm is sent when the number of concurrent endpoints or users exceed the total amount allowed for a particular license.
- Software Management—This alarm is sent during the following operations:
  - Patch Installation (Success or Failure) on a node
  - Patch Rollback (Success or Failure) on a node
- Purging Failed—This alarm is sent whenever a purge fails.
- Collector—This alarm is sent whenever collection failures occur.
- Alarm Manager—This alarm is sent when the **Alarm** manager cannot complete monitoring of all thresholds.
- Backup Failed—This alarm is sent whenever there is backup failure.
- DNS Resolution Failed—This alarm indicates that you are not using a proper DNS server, or your host is not defined in the DNS server that you are using. Both of these lead to DNS resolution failure. For Cisco ISE to work properly, you should use DNS servers and have your host resolvable from DNS.

You can choose to send alarm notifications through email and as syslog messages. To send syslog messages successfully, you must configure Alarm Syslog Targets, which are syslog message destinations. For more information, see Configuring Alarm Syslog Targets.

Enabling and Configuring System Alarms

The following task shows you how to activate and configure notification for system alarms.

To enable and configure a system alarm, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.

Step 3 Check the **Notify System Alarms** check box. A green check mark appears to show that the option has been activated.

Step 4 Designate the number of hours to suppress duplicate system alarms from being sent to the Email Notification User List.

Step 5 To request Email Notification, enter a valid email address in the text field. Then, check the **Email in HTML Format** check box, as desired.

When a system alarm occurs, an email is sent to all the recipients in the Email Notification User List.

Step 6 To request Syslog Notification, check the **Send Syslog Message** check box.

Step 7 Click **Submit** to apply the settings.

For more information:

See the System Alarm Settings section of Appendix A, "User Interface Reference."

Disabling System Alarms

The following task shows you how to deactivate system alarms.

To disable system alarms, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **System Alarm Settings**.

Step 3 Uncheck the **Notify System Alarms** check box. The green check mark disappears to show that the option has been deactivated.

For more information:

See the System Alarm Settings section of Appendix A, "User Interface Reference."

Configuring Alarm Syslog Targets

This section shows you how to create, edit, and delete alarm syslog targets.

If you configure system alarm notifications to be sent as syslog messages, then you need a syslog target to receive the notification. Alarm syslog targets are the destinations to which alarm syslog messages are sent. A system that is configured as a syslog server is also required to receive syslog messages.

Creating and Editing Alarm Syslog Targets

When you create or edit an alarm syslog target, you establish or modify the destination to which syslog messages are sent.

To create and edit an alarm syslog target, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.

Step 3 To create an alarm syslog target, do the following:

- **a.** Click **Create**.
- **b.** Enter a unique name in the Name field and a meaningful description in the Description field.
- **c.** Enter a valid IP address in the IP Address field and click **Submit**.

  The newly created alarm syslog target appears in the list.

Step 4 To edit an alarm syslog target, do the following:

- **a.** Click the alarm syslog target Name link from the list.
- **b.** Modify the Name and Description, as necessary.
- **c.** Change the IP Address as needed, and click **Submit.**

  Your changes are applied to the alarm syslog target.

For more information:

See the Alarm Syslog Targets section of Appendix A, "User Interface Reference."

Deleting Alarm Syslog Targets

You can delete an alarm syslog target at any time.

To delete an alarm syslog target, complete the following steps:

Step 1 Select **Administration > System > Settings**.

Step 2 In the left Settings panel, expand **Monitoring** and then choose **Alarm Syslog Targets**.

Step 3 Check the check box next to the alarm syslog target that you want to delete. A green check mark appears to show that it is selected.

Step 4 Click **Delete**, and then click **Yes** in the dialog prompt to confirm the deletion.

For more information:

See the Alarm Syslog Targets section of Appendix A, "User Interface Reference."

Managing Software Patches

You can install patches on ISE servers in your deployment from the primary administration node. ISE patches are usually cumulative, however, any restrictions on the patch installation will be described in the *README* file that will be included with the patch. Cisco ISE allows you to perform patch installation and rollback from either the command-line interface (CLI) or GUI.

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

Note When you install or roll back a patch from the primary administration node that is part of a distributed deployment, Cisco ISE installs the patch on the primary and all the secondary nodes in the deployment. If the patch installation is successful on the primary node, Cisco ISE then proceeds to the secondary nodes. If it fails on the primary node, the installation is aborted. 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.

To roll back a patch from ISE nodes in a deployment, you must roll back the change from the primary node and if successful, the patch is rolled back from the secondary nodes. If it fails on the primary node, the rollback process is aborted. However, if it fails on any of the secondary nodes, it still continues to roll back the patch from the next secondary node in your deployment.

Note You cannot install a patch whose version is lower than the patch that is currently installed on 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 ISE servers, you cannot install patch 1 or 2, or roll back patch 1 or 2.

To install and roll back patches from the CLI, refer to the *Cisco Identity Services Engine CLI Reference Guide, Release 1.1*.

This section contains:

- Installing a Software Patch, page 8-24
- Rolling Back Software Patches, page 8-28
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Installing a Software Patch

To install a patch from the GUI, you must download the patch from the following location 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.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To install a patch on Cisco ISE nodes in a deployment, complete the following steps:

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

The Patch Management page appears, which lists the patches that are installed on your ISE node.

Step 2 Click **Install**.

The Install Patch Bundle page appears.

Step 3 Click **Browse** to choose the patch that you downloaded earlier.

Step 4 Click **Install** to install the patch.

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 and also any errors in the patch file.

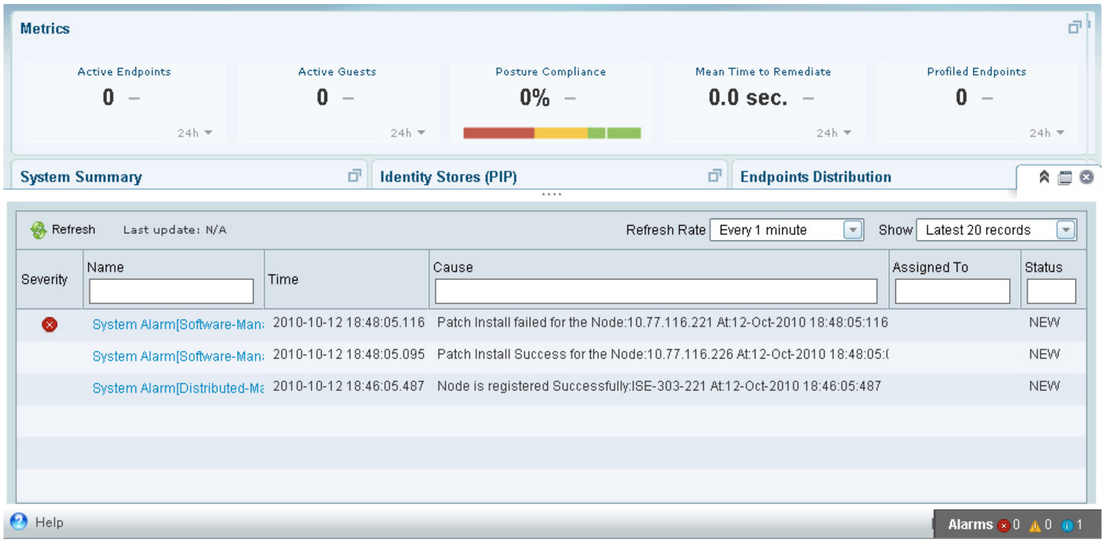
After the patch is installed on the primary administration node, Cisco ISE logs you out and you have to wait for a few minutes before you can log back in.

Note When patch installation is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

Step 5 After you log back in, from the dashboard, click the **Alarms** link at the bottom of your screen as shown in Figure 8-21.

Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by Downloading Support Bundles.

Figure 8-21 Patch Installation Status in the Dashboard



Last update: N/A

Refresh Rate: Every 1 minute

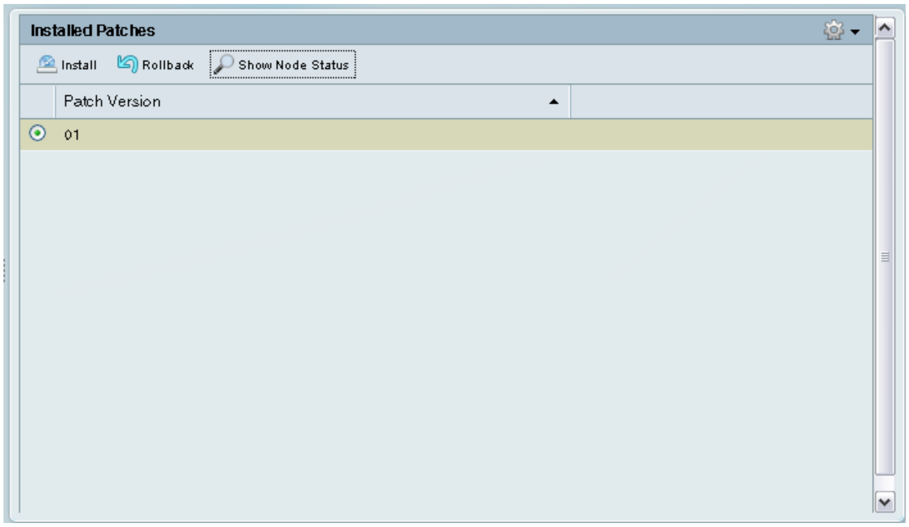
Show: Latest 20 records

Severity	Name	Time	Cause	Assigned To	Status
✖	System Alarm[Software-Man:	2010-10-12 18:48:05.116	Patch Install failed for the Node:10.77.116.221 At:12-Oct-2010 18:48:05:116		NEW
	System Alarm[Software-Man:	2010-10-12 18:48:05.095	Patch Install Success for the Node:10.77.116.226 At:12-Oct-2010 18:48:05:(		NEW
	System Alarm[Distributed-Ma	2010-10-12 18:46:05.487	Node is registered Successfully:ISE-303-221 At:12-Oct-2010 18:46:05:487		NEW

Step 6 You can go back to the Patch Installation page (choose **Administration > System > Maintenance > Patch Management**).

Step 7 The Installed Patches page appears as shown in Figure 8-22.

Figure 8-22 Patch Listing Page



Installed Patches

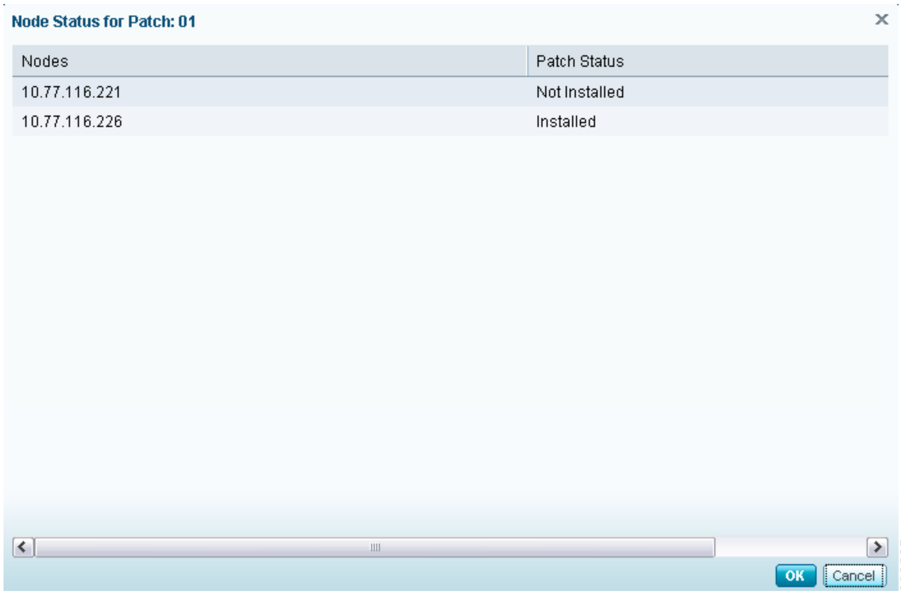
	Patch Version
●	01

This page lists all the patches that you have installed so far.

Step 8 Click the radio button next to the patch whose status you want to view and click **Show Node Status**.

A pop-up appears that shows the status of this patch (Installed, Not Installed, or Node is Down) on the various nodes in your deployment as shown in Figure 8-23.

Figure 8-23 Node Status Pop-Up



Node Status for Patch: 01

Nodes	Patch Status
10.77.116.221	Not Installed
10.77.116.226	Installed

Step 9 After the patch is installed on the primary node, ISE will install it on your secondary nodes consecutively.

While installing a patch on the secondary nodes, the primary administration node is not restarted and you can continue to perform your tasks on the primary administration node. During this time, the secondary ISE nodes are restarted consecutively after the patch is installed on those nodes. At any point during the installation process, you can click the **Show Node Status** button to see the status of patch installation.

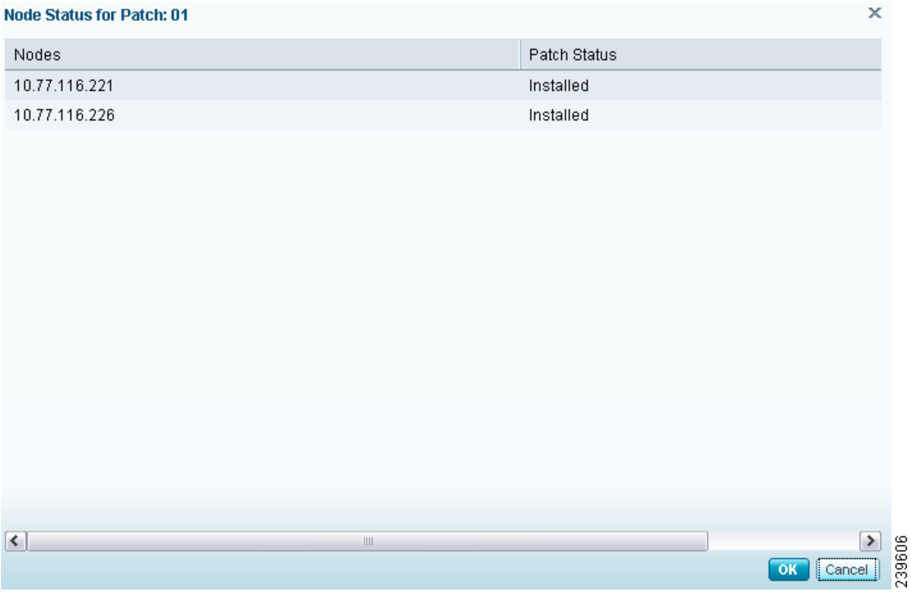
If for some reason, the patch installation fails on the primary administration node, the installation does not proceed to the secondary nodes.

Step 10 To check if the installation is complete, click the radio button next to the patch that you have installed and click **Show Node Status**.

Note The Node Status pop-up only provides information about patch installation on ISE nodes. Patch installation and rollback on Inline Posture nodes can only be done through the Cisco ISE CLI and this status will not be displayed in the Node Status pop-up.

A pop-up similar to the one shown in Figure 8-24 appears.

Figure 8-24 Node Status Pop Up: Installation Complete



Node Status for Patch: 01

Nodes	Patch Status
10.77.116.221	Installed
10.77.116.226	Installed

Patch installation is now complete on all the ISE nodes.

If for some reason the patch is not installed on one or more secondary nodes, ensure that the node is up and repeat the process from Step 2 to install it on the remaining nodes. Cisco ISE installs the patch on those nodes that do not have this version of the patch.

Related Topics:

- Managing Software Patches, page 8-24
- Rolling Back Software Patches, page 8-28
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Rolling Back Software Patches

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or System Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

To roll back a patch from Cisco ISE nodes in your deployment, complete the following steps:

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

The Installed Patches page appears.

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

Note When patch rollback is in progress, Show Node Status is the only option that is enabled in the Patch Management page.

After the patch has been rolled back on the primary administration node, Cisco ISE will roll back the patch from the secondary nodes. If for some reason the patch rollback fails on the primary node, the patches are not rolled back from the secondary nodes.

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

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

Note The alarms are generated only for patch install or rollback operations performed from the GUI. To view the status of patch installation from the CLI, you must check the *ade.log* file, which you can access by Downloading Support Bundles.

Step 4 Go back to the Installed Patches page (choose **Administration > System > Maintenance > Patch Management**) to check the status of this rollback on the other nodes in your deployment.

Step 5 If the patch rollback is in progress, this status will be visible in the Installed Patches page. To view the status of the patch rollback, you can choose the patch and click **Show Node Status**.

A pop-up appears that shows the status of the patch on the various ISE nodes 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.

Step 6 Click the radio button for the patch and click **Show Node Status** 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 2 to roll back the changes from the remaining nodes. Cisco ISE rolls back the patch only from those nodes that still have this version of the patch installed.

Related Topics:

- Managing Software Patches, page 8-24
- Installing a Software Patch, page 8-24
- Viewing Patch Install and Rollback Changes in the Audit Report, page 8-29

Viewing Patch Install and Rollback Changes in the Audit Report

The monitoring and troubleshooting component of Cisco ISE provides information on the patch installation and rollback operations that are performed on your ISE nodes.

Prerequisite:

Every ISE administrator account is assigned one or more administrative roles. To perform the operations described in the following procedure, you must have one of the following roles assigned: Super Admin or Monitoring Admin or Helpdesk Admin. See Cisco ISE Admin Group Roles and Responsibilities for more information on the various administrative roles and the privileges associated with each of them.

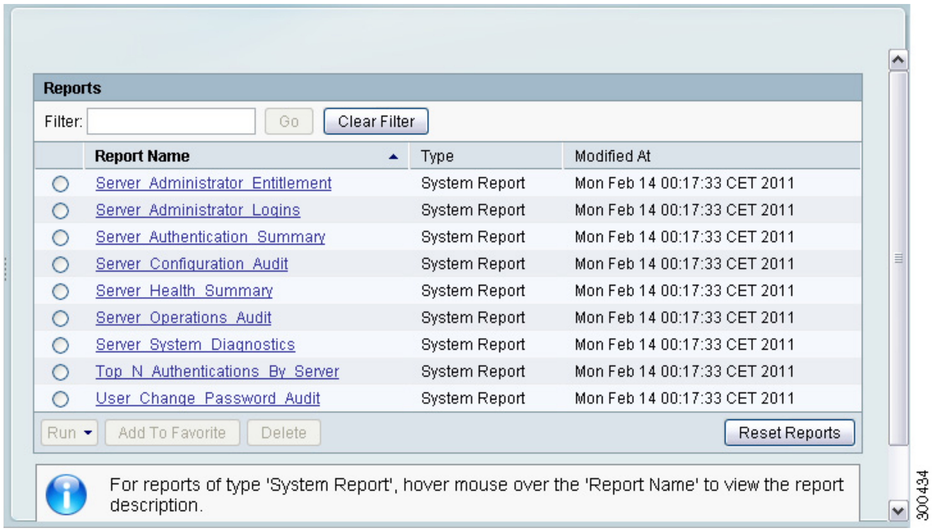
To view these reports, complete the following steps:

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

Step 2 From the Reports navigation pane on the left, click **Server Instance**.

A page similar to the one shown in Figure 8-25 appears.

Figure 8-25 Server Instance Reports Page



	Report Name	Type	Modified At
○	Server_Administrator_Entitlement	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_Administrator_Logins	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_Authentication_Summary	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_Configuration_Audit	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_Health_Summary	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_Operations_Audit	System Report	Mon Feb 14 00:17:33 CET 2011
○	Server_System_Diagnostics	System Report	Mon Feb 14 00:17:33 CET 2011
○	Top_N_Authentications_By_Server	System Report	Mon Feb 14 00:17:33 CET 2011
○	User_Change_Password_Audit	System Report	Mon Feb 14 00:17:33 CET 2011

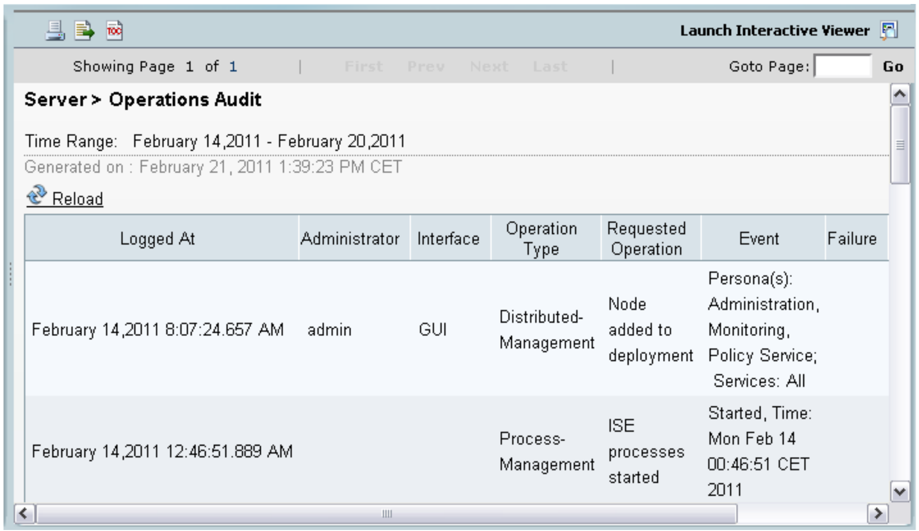
For reports of type 'System Report', hover mouse over the 'Report Name' to view the report description.

Step 3 Click the **Server Operations Audit** radio button, then click **Run** and choose the time period for which you want to generate the report.

Step 4 A report similar to the one shown in Figure 8-26 appears.

This report provides information on the patch installation and rollback operations that were performed within the time period that you have chosen.

Figure 8-26 ISE Operations Audit Report



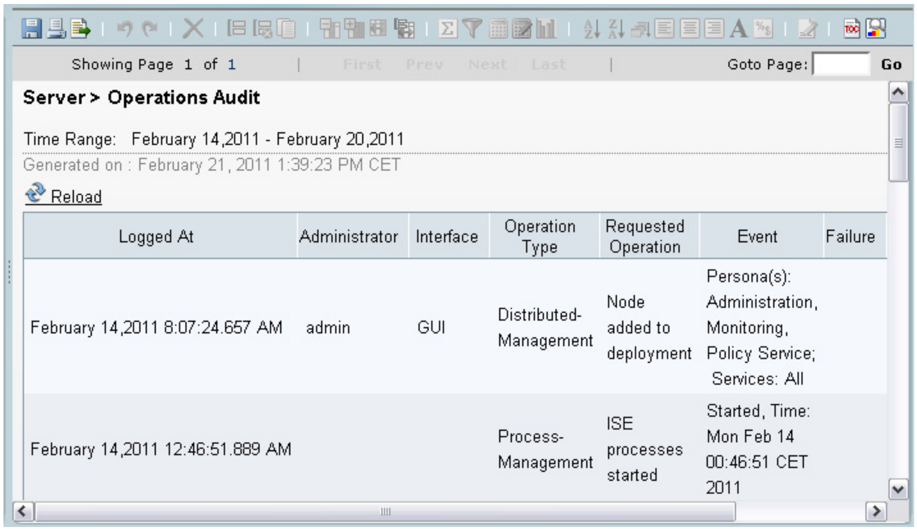
Server > Operations Audit

Time Range: February 14,2011 - February 20,2011
Generated on : February 21, 2011 1:39:23 PM CET

Logged At	Administrator	Interface	Operation Type	Requested Operation	Event	Failure
February 14,2011 8:07:24.657 AM	admin	GUI	Distributed-Management	Node added to deployment	Persona(s): Administration, Monitoring, Policy Service; Services: All	
February 14,2011 12:46:51.889 AM			Process-Management	ISE processes started	Started, Time: Mon Feb 14 00:46:51 CET 2011	

Step 5 Click the Launch Interactive Viewer link in the upper right corner of the screen to view, sort, and filter the data in this report. A screen similar to the one that is shown in Figure 8-27 appears.

Figure 8-27 ISE Operations Report: Interactive View



Server > Operations Audit

Time Range: February 14,2011 - February 20,2011
Generated on : February 21, 2011 1:39:23 PM CET

Logged At	Administrator	Interface	Operation Type	Requested Operation	Event	Failure
February 14,2011 8:07:24.657 AM	admin	GUI	Distributed-Management	Node added to deployment	Persona(s): Administration, Monitoring, Policy Service; Services: All	
February 14,2011 12:46:51.889 AM			Process-Management	ISE processes started	Started, Time: Mon Feb 14 00:46:51 CET 2011	

For information on how to use the interactive viewer features, see the "Working with the Interactive Viewer Toolbar" section on page 24-12.

Related Topics:

- Managing Software Patches
- Installing a Software Patch
- Rolling Back Software Patches