CHAPTER 3

Cisco ISE Task Navigator

This chapter introduces the Cisco Identity Service Engine (ISE) Task Navigators, and contains the following topics:

Navigating Multiple Task Procedures

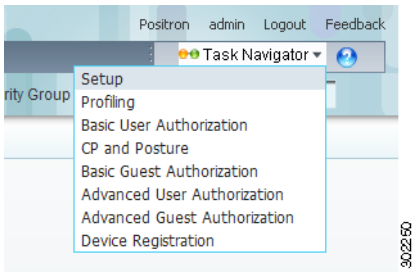
Task Navigators provide a visual path through Cisco ISE administration and configuration processes, which span multiple user interface pages. The linear presentation of the Task Navigator outlines the order in which the tasks should be completed, while also providing direct links to the pages where you perform the tasks.

Note The Task Navigator does not retain information about the tasks you have completed. It is a visual guide that takes you directly to the user interface pages where you perform its related tasks.

Task Navigator Menu

The Task Navigator menu appears in the upper right corner of the Cisco ISE window.

Figure 3-1 Task Navigator Menu



Bringing Up and Using a Task Navigator

Each option on the Task Navigator menu brings up a pop-up dialog that shows a list of tasks arranged along a line. The tasks are arranged in the order in which they should be performed, from left to right.

To bring up and use a task navigator, complete the following steps:

Step 1 Right-click the **Task Navigator** menu, and choose one of the following options from the drop-down menu:

- Setup—Perform the first part of the Cisco ISE setup process.
- Profiling—Profile endpoints.
- Basic User Authorization—Establish basic user authorization.
- Client Provisioning and Posture—Configure client provisioning and posture.
- Basic Guest Authorization—Establish basic guest authorization.
- Advanced User Authorization—Establish user authorization, along with client provisioning and posture.
- Advanced Guest Authorization—Establish guest authorization, along with client provisioning and posture.

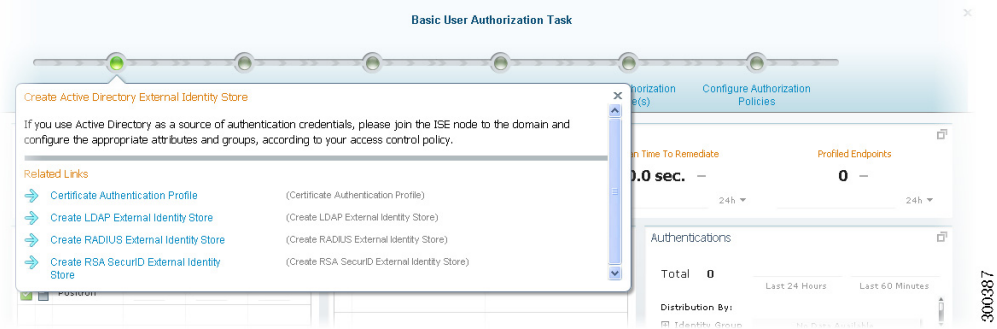
The Task Navigator you selected appears at the top of the window.

Step 2 Complete the tasks in the order in which they appear, starting from left to right.

Note The Task Navigator does not retain information about the tasks you have completed. It is a visual guide that takes you directly to the user interface pages where you perform its related tasks.

Step 3 To display information about the tasks, hover your mouse cursor over the task bullet. A quick view dialog appears.

Figure 3-2 Basic User Authorization Task



Step 4 To begin a task, click the radio button icon. The page changes, taking you directly to the place where you can begin the task.

Step 5 After completing the last task on the navigation path, close the dialog.

Next Steps

See the other sections in this chapter for information on each of the Task Navigator options.

Setup

Table 3-1 lists the initial tasks you perform to set up your Cisco ISE network. Links to detailed information about the tasks are provided for your convenience.

Table 3-1 Setup Task Map

Task	Description	User Interface Navigation Path	Documentation Link
1. Administrator password policy	Verify the password policy for Cisco ISE administrators to make sure it is in accordance with your company security policy.	Administration > System > Admin Access > Settings > Password Policy	Configuring a Password Policy for Administrator Accounts, page 4-63
2. Network access password policy	Verify the password policy for internal users who are requesting network access to make sure it is in accordance with your company security policy.	Administration > Identity Management > Settings > User Password Policy	Configuring a User Password Policy for the Network Access User Account, page 4-68
3. Guest access password policy	Verify the password policy for internal users who are requesting network access to make sure it is in accordance with your company security policy.	Administration > Web Portal Management > Settings > Guest > Password Policy	Configuring Guest Password Policy, page 21-68
4. Licensing	Verify that you have the correct licensing for the products you purchased.	Administration > System > Licensing > Current Licenses	Adding and Upgrading Licenses, page 12-3

Table 3-1 Setup Task Map (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Time	Configure and verify the system time, date, and NTP settings.	Administration > System > Settings > System Time	System Time and NTP Server Settings, page 8-18
6. Proxy	Configure the appropriate proxy server settings so that the Cisco ISE node can communicate externally for updates.	Administration > System > Settings > Proxy	Specifying Proxy Settings in Cisco ISE, page 8-17
7. Certificate signing request	Create a Certificate Signing Request (CSR).	Administration > System > Certificates > Local Certificates	Generating a Certificate Signing Request, page 13-8
8. Export certificate signing request	Export the CSR to be submitted to the appropriate certificate authority (CA) for your company.	Administration > System > Certificates > Certificate Signing Requests	Viewing and Exporting Certificate Signing Requests, page 13-15
9. Certificate authority certificates	Import the necessary CA certificates to establish trusts for internode communication, Cisco ISE administration, and client authentication.	Administration > System > Certificates > Certificate Authority Certificates	Adding a Certificate Authority Certificate, page 13-18
10. Monitoring and troubleshooting e-mail settings	Configure the correct Simple Mail Transfer Protocol (SMTP) server so that alarms can be sent to the appropriate operations team.	Administration > System > Settings > Monitoring > Email Settings	Configuring E-mail Settings, page 8-20
11. Monitoring and troubleshooting system alarm settings	Configure the necessary alarm settings so that they meet your operational requirements.	Administration > System > Settings > Monitoring > System Alarm Settings	Configuring System Alarm Settings, page 8-21
12. System logging settings	Configure logging functions, to ensure proper event management operations for your environment.	Administration > System > Logging > Local Log Settings	Chapter 14, “Logging.”
13. Scheduled backup	Configure an automated backup schedule that is based on your data recovery policy.	Administration > System > Maintenance > Data Management > Administration Node > Scheduled Backup	Scheduling a Backup, page 15-7

Table 3-1 Setup Task Map (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Distributed deployment	Verify the proper number, type, and synchronization status of the Cisco ISE nodes in your installation.	Administration > System > Deployment	• To configure nodes in your deployment, see the following: – Configuring an ISE Node, page 9-7 – Registering and Configuring a Secondary Node, page 9-13 • To verify the synchronization status of the nodes in your deployment, see Synchronizing Primary and Secondary Nodes in a Distributed Environment, page 15-12.

Profiling

Table 3-2 lists the tasks you perform to establish profiling for endpoints. Links to detailed information about the tasks are provided for your convenience.

Table 3-2 Task Navigator: Profiling

Task	Description	User Interface Navigation Path	Documentation Link
1. Node sensor configuration	Review each of the Cisco ISE nodes in your deployment and verify that the profiling sensor probes for all of the nodes are configured properly.	Administration > System > Deployment > [Choose a Node] > Edit > Profiling Configuration	Configuring the Probes, page 18-13
2. Verify/Create profiler conditions	Verify or create new profiler conditions for your profiling requirements.	Policy > Policy Elements > Conditions > Profiling > Conditions	Creating a Profiling Condition, page 18-57
3. Verify/Create profiler policy	Verify or create profiler policies using the profiler conditions.	Policy > Profiling > Profiling Policies > Endpoint Policies	Creating an Endpoint Profiling Policy, page 18-42
4. Create Downloadable ACLs[1]	Create appropriate downloadable ACLs for security enforcement.	Policy > Policy Elements > Results > Authorization > Downloadable ACLs > DACL Management > Add	Configuring DACLs, page 17-35

Table 3-2 Task Navigator: Profiling (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create authorization profiles	Create authorization profiles that are based on the types of privileges that are used for your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles > Add	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-29
6. Create authorization rules for profiled endpoints	Create authorization rules for profiled endpoints that are pertinent to your environment.	Policy > Authorization > Standard	Understanding Authorization Policies, page 17-1

1. Downloadable access control lists (ACLs)

Basic User Authorization

The process for setting up basic user authorization involves the use of multiple pages in the user interface. Table 3-3 lists the tasks you perform. Links to detailed information about the tasks are provided for your convenience.

Table 3-3 Task Navigator: Basic User Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory External Identity Store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating Cisco ISE with Active Directory, page 5-6
2. Create Identity Source Sequences	Create identity source sequences that are based on the external identity stores you created in the previous task.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Verify Authentication Policy	Create or modify the authentication policy to include any new identity source sequences that were created in Task 2.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-27. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-30.
4. Create Downloadable ACLs	Create the appropriate downloadable ACLs for security enforcement, as necessary.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-35

Table 3-3 Task Navigator: Basic User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create Authorization Profile(s)	Create authorization profiles that are based on the types of privileges that are used for your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-29
6. Create Authorization Policy	Create an authorization policy to grant the appropriate access privileges for your implementation.	Policy > Authorization	Creating a New Authorization Policy, page 17-15

Client Provisioning and Posture

Table 3-4 lists the tasks you perform to establish client provisioning and posture. After login and successful posture, you may also have to perform additional tasks in posture on Acceptable Use Policy and Reassessments, which are not part of this flow. Links to detailed information about the tasks are provided for your convenience.

Table 3-4 Task Navigator: Client Provisioning and Posture

Task	Description	User Interface Navigation Path	Documentation Link
1. Configure Posture updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
2. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-28
3. Manual client provisioning resources download and create agent profiles	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.
4. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-31

Table 3-4 Task Navigator: Client Provisioning and Posture (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create the posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-56 • Application Conditions, page 20-68 • Service Conditions, page 20-74
6. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
7. Create remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-114.
8. Verify/Create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-151
9. Verify/Create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33

Basic Guest Authorization

Table 3-5 lists the tasks you perform to establish basic authorization for guests. Links to detailed information about the tasks are provided for your convenience.

Table 3-5 Task Navigator: Basic Guest Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory External Identity Store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups according to your access control policy. In this task, the Active Directory configuration permits employees to use the Guest portal to achieve network access in situations where their endpoint is not working properly, or is not supported.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating Cisco ISE with Active Directory, page 5-6
2. Create Identity Source Sequences	Create identity source sequences that are based on the external identity stores you created in the previous task, as necessary.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Configure guest settings	Configure guest settings, as per guest requirements.	Administration > Web Portal Management > Settings > Guest > Multi-portal Configurations	Multi-Portal Configurations, page 21-47
4. Configure self-service guest settings	Configure self-service guest settings, if “allow for self-service” is selected in the Task 3 configuration.	Administration > Web Portal Management > Settings > Guest > Portal policy	Configuring Guest Portal Policy, page 21-67
5. Create time profile	Create a guest time profile.	Administration > Web Portal Management > Settings > Guest > Time profiles	Time Profiles, page 21-69
6. Configure sponsor authentication identity sequence	Provide a sponsor authentication source.	Administration > Web Portal Management > Settings > Sponsor > Authentication source	Specifying an Authentication Source, page 21-28
7. Create guest sponsor group	Create a guest sponsor group for sponsor login.	Administration > Web Portal Management > Sponsor Groups	Sponsor Groups, page 21-20
8. Create sponsor policy	Create a guest sponsor login policy.	Administration > Web Portal Management > Sponsor Group Policy	Sponsor Group Policy, page 21-16

Advanced User Authorization

Table 3-6 lists the tasks you perform for more advanced authorization for users. Links to detailed information about the tasks are provided for your convenience.

Table 3-6 Task Navigator: Advanced User Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory external identity store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy. Internal guest users do not require an Active Directory Identity Store setup.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating Cisco ISE with Active Directory, page 5-6
2. Create identity source sequences	Create identity source sequences that are based on the external identity stores you created in the previous task, as necessary.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Verify authentication policy	Create or modify the authentication policy to include any new identity source sequences that you created in the previous task.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-27. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-30.
4. Configure Posture Updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
5. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-28
6. Manual client provisioning resources	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.

Table 3-6 Task Navigator: Advanced User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
7. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-31
8. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-56 • Application Conditions, page 20-68 • Service Conditions, page 20-74
9. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
10. Create Remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-114.
11. Verify/create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-151
12. Verify/create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33
13. Create downloadable ACLs	Create the appropriate downloadable ACLs for enforced security, as necessary.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-35

Table 3-6 Task Navigator: Advanced User Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Create authorization profiles	Create authorization profiles that are based on the types of privileges that apply to your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-29
15. Authorization policies	Create an authorization policy to grant the appropriate access privileges. Choose the conditions and/or attributes in each rule to define an overall network access policy. Create pre-posture and post-posture authorization policies.	Policy > Authorization	Creating a New Authorization Policy, page 17-15

Advanced Guest Authorization

Table 3-7 lists the tasks you perform for more advanced authorization for guests. Links to detailed information about the tasks are provided for your convenience.

Table 3-7 Task Navigator: Advanced Guest Authorization

Task	Description	User Interface Navigation Path	Documentation Link
1. Create Active Directory external identity store	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating Cisco ISE with Active Directory, page 5-6
2. Create identity source sequences	Create identity source sequences that are based on the external identity stores you created in Task 1, as per requirements.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
3. Configure guest settings	Configure guest settings, as per guest requirements.	Administration > Web Portal Management > Settings > Guest > Multi-portal Configuration	Multi-Portal Configurations, page 21-47
4. Configure for self-service guest settings	Configure self-service guest settings, if “allow for self-service” was selected in Task 3.	Administration > Web Portal Management > Settings > Guest > Portal Policy	Configuring Guest Portal Policy, page 21-67

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
5. Create time profile	Create a guest time profile.	Administration > Web Portal Management > Settings > Guest > Time Profiles	Time Profiles, page 21-69
6. Configure sponsor authentication identity sequence	Provide a sponsor authentication source.	Administration > Web Portal Management > Settings > Sponsor > Authentication Source	Specifying an Authentication Source, page 21-28
7. Create guest sponsor group	Create a guest sponsor group for sponsor login.	Administration > Web Portal Management > Sponsor Groups	Sponsor Groups, page 21-20
8. Create sponsor policy	Create a guest sponsor login policy.	Administration > Web Portal Management > Sponsor Group Policy	Sponsor Group Policy, page 21-16
9. Verify authentication policy	Create or modify the authentication policy to include any new identity source sequences that you created in the Task 8.	Policy > Authentication	• For simple authentication policy, see Configuring the Simple Authentication Policy, page 16-27. • For rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-30.
10. Configure Posture Updates URL	Initial compliance module download (posture updates) takes 15 to 20 minutes for the first time.	Administration > System > Settings > Posture > Updates	For posture updates through web and offline, see Posture Updates, page 20-22.
11. Configure client provisioning settings	Configure the client provisioning update feed URL.	Administration > System > Settings > Client Provisioning	Setting Up Global Client Provisioning Functions, page 19-28
12. Manual client provisioning resources	Download client provisioning resources which you can add from local and remote resources. Create client provisioning agent profiles which you can add from local and remote resources.	Policy > Policy Elements> Results > Client Provisioning > Resources > Add	• For downloading client provisioning resources, see Adding Client Provisioning Resources to Cisco ISE, page 19-5. • For creating client provisioning agent profiles, see Creating Agent Profiles, page 19-12.
13. Create client provisioning policy	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-31

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
14. Verify/create posture conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined simple conditions are downloaded to Cisco ISE. Create simple conditions for posture as needed.	Policy > Policy Elements > Conditions > Posture	To create posture simple conditions, see the following: • File Conditions, page 20-44 • Registry Conditions, page 20-56 • Application Conditions, page 20-68 • Service Conditions, page 20-74
15. Verify/create posture compound conditions	Verify that the compliance module update (posture updates) is fully downloaded and installed where predefined compound conditions and antivirus and antispyware support chart updates are downloaded to Cisco ISE. Create posture compound conditions using posture simple conditions that are already created.	Policy > Policy Elements > Conditions > Posture	To create posture compound conditions, see the following: • Compound Conditions, page 20-80 • Antivirus Compound Conditions, page 20-88 • Antispyware Compound Conditions, page 20-94
16. Create remediation actions	Create remediation actions, which are listed in alphabetical order.	Policy > Policy Elements > Results > Posture > Remediation Actions	To create remediation actions, see Configuring Custom Posture Remediation Actions, page 20-114.
17. Verify/create posture requirements	Create posture requirements using posture simple conditions, or compound conditions.	Policy > Policy Elements > Results > Posture > Requirements	Client Posture Assessment Requirements, page 20-151
18. Verify/create posture policy	Create posture policies using posture requirements.	Policy > Posture	Client Posture Assessment Policies, page 20-33
19. Create downloadable ACLs	Create the appropriate downloadable ACLs, as needed for enforced security.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-35
20. Create authorization profiles	Create authorization profiles that are based on the types of privileges that apply to your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-29

Table 3-7 Task Navigator: Advanced Guest Authorization (continued)

Task	Description	User Interface Navigation Path	Documentation Link
21. Authorization policies	Create an authorization policy to grant the appropriate access privileges. Choose the conditions and attributes in each rule to define the overall network access policy. Create pre-posture and post-posture authorization policies.	Policy > Authorization	Creating a New Authorization Policy, page 17-15

Device Registration

Table 3-8 lists the tasks that you perform for user device registration. Links to detailed information about the tasks are provided for your convenience.

Table 3-8 Task Navigator: Device Registration

Task	Description	User Interface Navigation Path	Documentation Link
1. Add or import required network devices.	Ensure that Cisco ISE knows of other network devices in your environment that are required to provide appropriate network provisioning.	Administration > Network Resources > Network Devices	Adding and Editing Devices, page 6-3
2. Create Active Directory External Identity Store.	If you use Active Directory as a source of authentication credentials, join the Cisco ISE node to the domain and configure the appropriate attributes and groups, according to your access control policy.	Administration > Identity Management > External Identity Sources > Active Directory	Integrating Cisco ISE with Active Directory, page 5-6
3. Create identity source sequences.	Create identity source sequences that are based on the external identity stores that you created in Task 2, as per requirements.	Administration > Identity Management > Identity Source Sequences	Creating Identity Source Sequences, page 5-52
4. Create downloadable ACLs.	Create the appropriate downloadable ACLs, as needed for enforced security.	Policy Elements > Results > Authorization > Downloadable ACLs	Creating and Configuring Permissions for a New DACL, page 17-35
5. Create authorization profiles.	Create authorization profiles that are based on the types of privileges that apply to your deployment and security policy.	Policy > Policy Elements > Results > Authorization > Authorization Profiles > Standard Authorization Profiles	Creating and Configuring Permissions for a New Standard Authorization Profile, page 17-29

Table 3-8 Task Navigator: Device Registration (continued)

Task	Description	User Interface Navigation Path	Documentation Link
6. Download the supplicant provisioning wizard and create a supplicant provisioning profile.	Set up Cisco ISE so that remote users accessing the network are able to use their own access devices.	Policy > Policy Elements > Results > Client Provisioning > Resources	• Adding Client Provisioning Resources from a Remote Source, page 19-5 • Creating Native Supplicant Profiles, page 19-24
7. Create client provisioning policies.	Create client provisioning policies that are based on identity groups and operating systems.	Policy > Client Provisioning	Configuring Client Provisioning Resource Policies, page 19-31
8. Verify the authentication policy.	Create or modify the authentication policy to include any new identity source sequences that you created in Task 2.	Policy > Authentication	• For the simple authentication policy, see Configuring the Simple Authentication Policy, page 16-27. • For the rule-based authentication policy, see Configuring the Rule-Based Authentication Policy, page 16-30.
9. Create an authorization policy.	Create an authorization policy to grant the appropriate access privileges. Choose the conditions and attributes in each rule to define the overall network access policy. Create pre-posture and post-posture authorization policies.	Policy > Authorization	Creating a New Authorization Policy, page 17-15
10. Configure self-service guest settings (for guests and employees).	Configure self-service guest settings for user login with personal devices.	Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations > Default Guest Portal > Operations > Enable Self-Provisioning Flow	Hosting Multiple Portals, page 21-48
11. Configure Simple Certificate Enrollment Protocol (SCEP) Certificate Authority (CA) profiles.	Create one or more SCEP request profiles.	Administration > System > Certificates > SCEP CA Profile	Adding and Modifying Simple Certificate Enrollment Protocol Profiles, page 13-25