Administration User Interface Reference

This chapter is a reference for the Cisco Identity Services Engine (ISE) Admin Portal elements, and contains the following Administration related sections:

System Administration

Deployment Settings

The Deployment Nodes page enables you to configure **Cisco** ISE and Inline Posture nodes and to set up a deployment.

- To configure Administration, Policy Service, and Monitoring nodes, see General Node Settings, page A-2 and Profiling Node Settings, page A-5.
- To configure an Inline Posture node, see Inline Posture Node Settings, page A-6.

Deployment Nodes List Page

The following table describes the fields on the Deployment Nodes List page, which you can use to configure Cisco ISE and Inline Posture nodes in a deployment. The navigation path for this page is: Administration > System > Deployment.

Table A-1 Deployment Nodes List Page

Fields	Usage Guidelines
Hostname	Displays the hostname of the node.
Node Type	Displays the node type. It can be one of the following: • Cisco ISE • Inline Posture node

Table A-1 Deployment Nodes List Page (continued)

Fields	Usage Guidelines
Personas	(Only appears if the node type is Cisco ISE) Lists the personas that an Cisco ISE node has assumed. For example, Administration, Policy Service.
Role	Indicates the role (primary, secondary, or standalone) that the Administration and Monitoring personas have assumed, if these personas are enabled on this node. The role can be any one or more of the following: • PRI(A)—Refers to a primary Administration node • SEC(A)—Refers to a secondary Administration node • PRI(M)—Refers to a primary Monitoring node • SEC(M)—Refers to a secondary Monitoring node
Services	(Only appears if the Policy Service persona is enabled) Lists the services that run on this Cisco ISE node. Services can include any one of the following: • Session • Profiling • All
Node Status	Indicates the status of each ISE node in a deployment for data replication. • Green (Connected)—Indicates that an ISE node, which is already registered in the deployment is in sync with the primary Administration node. • Red (Disconnected)—Indicates that an ISE node is not reachable or is down or data replication is not happening. • Orange (In Progress)—Indicates that an ISE node is newly registered with the primary Administration node or you have performed a manual sync operation or the ISE node is not in sync (out of sync) with the primary Administration node. For more details, click the quick view icon for each ISE node in the Node Status column.

General Node Settings

The following table describes the fields on the General Node Settings page, which you can use to set up your deployment and configure services to be run on each of the nodes. The navigation path for this tab is: Administration > System > Deployment > ISE Node > Edit > General Settings.

For Inline Posture Node Settings, see Inline Posture Node Settings, page A-6.

Table A-2 General Node Settings

Fields	Usage Guidelines
Hostname	Displays the hostname of the Cisco ISE node.
FQDN	Displays the fully qualified domain name of the Cisco ISE node. For example, ise1.cisco.com.
IP Address	Displays the IP address of the Cisco ISE node.
Node Type	Displays the node type. Could be any one of the following: • Identity Services Engine (ISE) • Inline Posture Node

Table A-2 General Node Settings (continued)

Fields	Usage Guidelines
Personas	
Administration	Check this check box if you want an Cisco ISE node to assume the Administration persona. **Note** You can enable the Administration persona only on nodes that are licensed to provide the administrative services. For more information, see Chapter 7, "Cisco ISE Licenses" • Role—Displays the role that the Administration persona has assumed in the deployment. Could take on any one of the following values: – Standalone – Primary – Secondary • Make Primary—Click this button to make this node your primary Cisco ISE node. You can have only one primary Cisco ISE node in a deployment. The other options on this page will become active only after you make this node primary. – You can have only two Administration nodes in a deployment. If the node has a Standalone role, a Make Primary button appears next to it. – If the node has a Secondary role, a Promote to Primary button appears next to it. – If the node has a Primary role and there are no other nodes registered with it, a Make Standalone button appears next to it. You can click this button to make your primary node a standalone node.

Table A-2 General Node Settings (continued)

Fields	Usage Guidelines
Monitoring	Check this check box if you want a Cisco ISE node to assume the Monitoring persona and function as your log collector. There must be at least one Monitoring node in a distributed deployment. At the time of configuring your primary Administration node, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the primary Administration node and disable the Monitoring persona, if required. **Note** To configure a Cisco ISE node on a VMware platform as your log collector, use the following guidelines to determine the minimum amount of disk space that you need: – 180 KB per endpoint in your network, per day – 2.5 MB per Cisco ISE node in your network, per day You can calculate the maximum disk space that you need based on how many months of data you want to have in your Monitoring node. If there is only one Monitoring node in your deployment, it assumes the standalone role. If you have two Monitoring nodes in your deployment, Cisco ISE displays the name of the other monitoring node for you to configure the Primary-Secondary roles. To configure these roles, choose one of the following: • **Primary**—For the current node to be the primary Monitoring node. • **Secondary**—For the current node to be the secondary Monitoring node. • **None**—If you do not want the Monitoring nodes to assume the primary-secondary roles. If you configure one of your Monitoring nodes as primary or secondary, the other Monitoring node automatically becomes the secondary or primary node, respectively. Both the primary and secondary Monitoring nodes receive Administration and Policy Service logs. If you change the role for one Monitoring node to None, the role of the other Monitoring node also becomes None, thereby cancelling the high availability pair. After you designate a node as a Monitoring node, you will find this node listed as a syslog target in the following page: Administration > System > Logging > Remote Logging Targets

Table A-2 General Node Settings (continued)

Fields	Usage Guidelines
Policy Service	Check this check box to enable any one or all of the following services: • Check the **Enable Session Services** check box to enable network access, posture, guest, and client provisioning services. – Choose the group to which this Policy Service node belongs from the Include Node in Node Group drop-down list. Choose **<none>** if you do not want this Policy Service node to be part of any group. **Note** All nodes within a node group should be Layer 2 adjacent (should be on the same subnet) and there should be multicast connectivity between the nodes. • Check the **Enable Profiling Service** check box to enable the Profiler service. If you enable the Profiling service, you must click the Profiling Configuration tab and enter the details as required. For more information, see "Configuring Probes per Cisco ISE Node" section on page 21-13. **Note** When you enable or disable any of the services that run on the Policy Service node or make any changes to this node, you will be restarting the application server processes on which these services run. You must expect a delay while these services restart. You can determine when the application server has restarted on a node by using the **show application status ise** command from the CLI.

Profiling Node Settings

The following table describes the fields on the Profiling Configuration page, which you can use to configure the probes for the profiler service. The navigation path for this page is: Administration > System > Deployment > ISE Node > Edit > Profiling Configuration.

Table A-3 Profiling Node Settings

Fields	Usage Guidelines
NetFlow	Check this check box if you want to enable NetFlow per Cisco ISE node that has assumed the Policy Service persona to receive Netflow packets sent from the routers. Choose these options: • Interface—Choose the interface on the ISE node. • Port—Enter the NetFlow listener port number on which NetFlow exports are received from the routers. The default port is 9996.
DHCP	Check this check box if you want to enable DHCP per Cisco ISE node that has assumed the Policy Service persona to listen for DHCP packets from IP helper. Choose these options: • Interface—Choose the interface on the ISE node. • Port—Enter the DHCP server UDP port number. The default port is 67.
DHCP SPAN	Check this check box if you want to enable DHCP SPAN per Cisco ISE node that has assumed the Policy Service persona to collect DHCP packets. • Interface—Choose the interface on the ISE node.

Table A-3 Profiling Node Settings (continued)

Fields	Usage Guidelines
HTTP	Check this check box if you want to enable HTTP per Cisco ISE node that has assumed the Policy Service persona to receive and parse HTTP packets. • Interface—Choose the interface on the ISE node.
RADIUS	Check this check box if you want to enable RADIUS per ISE node that has assumed the Policy Service persona to collect RADIUS session attributes as well as CDP, LLDP attributes from the IOS Sensor enabled devices.
Network Scan (NMAP)	Check this check box if you want to run a manual network scan on a subnet from the ISE node that has assumed the Policy Service persona to scan endpoints for open ports and the operating system. Enter a valid subnet in the **Manual Scan Subnet** field and click Run Scan to start a manual subnet scan. For example, you can enter 10.0.10.10/24.
DNS	Check this check box if you want to enable DNS per ISE node that has assumed the Policy Service persona to perform a DNS lookup for the FQDN. Enter the timeout period in seconds. **Note** For the DNS probe to work on a particular Cisco ISE node in a distributed deployment, you must enable any one of the following probes: DHCP, DHCP SPAN, HTTP, RADIUS, or SNMP. For DNS lookup, one of the probes mentioned above must be started along with the DNS probe.
SNMP Query	Check this check box if you want to enable SNMP Query per ISE node that has assumed the Policy Service persona to poll network devices at specified intervals. Enter values for the following fields: Retries, Timeout, Event Timeout, and an optional Description. **Note** In addition to configuring the SNMP Query probe, you must also configure other SNMP settings in the following location: Administration > Network Resources > Network Devices. When you configure SNMP settings on the network devices, ensure that you enable the Cisco Device Protocol (CDP) and Link Layer Discovery Protocol (LLDP) globally on your network devices.
SNMP Trap	Check this check box if you want to enable SNMP Trap probe per ISE node that has assumed the Policy Service Persona to receive linkUp, linkDown, and MAC notification traps from the network devices. Choose any of the following: • Link Trap Query—Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap. • MAC Trap Query—Check this check box to receive and interpret MAC notifications received through the SNMP Trap. • Interface—Choose an interface on the ISE node. • Port—Enter the UDP port of the host to use. The default port is 162.

Inline Posture Node Settings

The following table describes the fields on the Deployment Nodes List page for an Inline Posture node, which you can use to configure the Inline Posture nodes in your deployment. The navigation path for this page is: Administration > System > Deployment > Inline Posture Node > Edit.

Table A-4 Inline Posture Node Settings

Fields	Usage Guidelines
Basic Information	
Time Sync Server	Enter the IP address of the primary, secondary, and tertiary time sync server.
DNS Server	Enter the IP address of the primary, secondary, and tertiary DNS server.
Trusted Interface (to protected network)	Enter the Management VLAN ID (all the other information is automatically populated for these options)
Untrusted Interface (to management network)	Enter the IP Address, Subnet Mask, Default Gateway, and Management VLAN ID for the untrusted interface.
Deployment Modes	
Routed Mode	Choose this option for this node to provide router (hop in the wire) functionality for Inline Posture.
Bridged Mode	Choose this option for this node to provide VLAN mapping functionality for the subnets to be managed by Inline Posture. After checking the Bridged Mode check box, enter the Untrusted Network and Trusted Network VLAN ID information. For VLAN mapping, you should also do the following: • Add a mapping for management traffic by entering the appropriate VLAN ID for the trusted and untrusted networks. • Add a mapping for client traffic by entering the appropriate VLAN ID for the trusted and untrusted networks.
Filters	
MAC Address	Enter the MAC Address of the device on which to avoid policies. **Note** For security reasons, we recommend that you always include the IP address along with the MAC address in a MAC filter entry. For more information, see the Warning in Deploying an Inline Posture Node, page 4-13.
IP Address	Enter the IP Address of the device on which to avoid policies.
Description	Enter a description of the MAC Filter.
Subnet Address	Enter the subnet Address of the device on which to avoid policies.
Subnet Mask	Enter the subnet Mask of the device on which to avoid policies
Description	Enter a description of the Subnet Filter.
RADIUS Config[1]	
Primary Server	Enter the IP address, shared secret, timeout in seconds, and number of retries for the primary RADIUS server, usually the Policy Service node.
Secondary Server	Enter the IP address, shared secret, timeout in seconds, and number of retries for the secondary RADIUS server.
Client	Enter the IP address, shared secret, timeout in seconds, and number of retries for the device that requests access on behalf of clients, WLC or VPN. **Note** WLC roaming is not supported in Cisco ISE Release 1.1.1.

Table A-4 Inline Posture Node Settings (continued)

Fields	Usage Guidelines
Enable KeyWrap	Check this check box and specify the following Authentication Settings: • Key Encryption Key • Message Authenticator Code Key • Key Input Format: ASCI or Hexidecimal Deployments that utilize wireless LAN technology require secure transmission from a RADIUS server to a network access point. KeyWrap attributes provide stronger protection and more flexibility.
Failover	
Displays only if you have deployed an Inline Posture high availability pair.	
HA Peer Node	Choose the **HA Peer Node** from the drop-down list. A list of eligible standalone Inline Posture nodes appear from which to choose. The secondary node syncs to the primary node. • Replication Status—(Only appears for secondary nodes) Indicates whether incremental replication from the primary node to the secondary node is complete or not. You will see one of the following states: – Failed—Incremental database replication has failed. – In-Progress—Incremental database replication is currently in progress. – Complete—Incremental database replication is complete. – Not Applicable—Displayed if the Cisco ISE node is a standalone or primary node. • Sync Status—(Only appears for secondary Cisco ISE nodes) Indicates whether replication from the primary node to the secondary node is complete or not. A replication happens when a node is registered as secondary or when you click Syncup to force a replication. You will see one of the following states: – Sync Completed—Full database replication is complete. – Sync in Progress—Database replication is currently in progress. – Out of Sync—Database was down when the secondary node was registered with the primary Cisco ISE node. – Not Applicable—Displayed if the Cisco ISE node is a standalone node.
Service IP (Trusted)	Enter the Trusted Service IP address (eth0) for the traffic interface of the primary node.
Service IP (Untrusted)	Enter the Untrusted Service IP address (eth1) for the traffic interface of the primary node. In the bridged mode, the service IP address is the same for both trusted and untrusted networks.

Table A-4 Inline Posture Node Settings (continued)

Fields	Usage Guidelines
Link Detect (Trusted)	Enter the IP address (optional, but recommended as a best practice) for the Link-Detect system for the trusted and untrusted sides. This address is usually the IP address of the Policy Service node, because both the active and standby nodes should always be able to reach the Policy Service node.
Link Detect (Untrusted)	Enter the IP address for the Link-Detect system for the untrusted side.
Link Detect Timeout	Enter a Link-Detect Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value. Link-detect ensures that the Inline Posture node maintains communication with the Policy Service node. If the active node does not receive notification (ping) from the Policy Service node at the specified intervals, the active node fails over to the standby node.
Heart Beat Timeout	Enter a Heart Beat Timeout value. The default value of 30 seconds is recommended. However, there is no maximum value. The heartbeat is a message that is sent between the two Inline Posture nodes at specified intervals. The heartbeat happens on eth2 and eth3 interfaces. If the heartbeat stops or does not receive a response in the allotted time, failover occurs.
Syncup Peer Node	If the sync status for any secondary node is out of sync, click **Syncup** Peer Node to force a full database replication. **Note** You must use the Syncup option to force a full replication if the Sync Status is *Out of Sync* or the Replication Status is *Failed*.

1. The timeout and retry values that you specify in the RADIUS config tab for the primary and secondary servers should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: (IPEP RADIUS Config Timeout * No. of Retries) < (Client device's Timeout * No. of Retries). For example, on the primary and secondary servers, you can configure the timeout to be 5 seconds and the number of retries to be 1, and on the client, you can configure the timeout to be 5 seconds and the number of retries to be 3. So the timeout * no. of retries configured on the IPEP server (5*1=5) is lesser than the value configured on the client (5*3=15).

License Page Parameters

The following table describes the fields on the Current Licenses Page, which you can edit to add or upgrade a license. The navigation path for this page is: **Administration > System > Licensing > Current Licenses**.

Table A-5 License Page Parameters

Parameter	Description
Administration Node	Name of the Cisco ISE server instance where the primary node is installed.
ID (PID, VID, SN)	Administration node ID containing PID, VID, and SN, obtained from the licensing information.
Version	Version number of Cisco ISE.

Table A-5 License Page Parameters

Parameter	Description
License Type	• Base—The status or type of any Base License that is currently installed on the Administration node. • Advanced—The status or type of any Advanced License that is currently installed on the Administration node. • Wireless—The status or type of any Wireless License that is currently installed on the Administration node. After the 90-day Evaluation License expires and you install a Wireless License, the Current Licenses page reflects a Wireless License with <*x*> days remaining on the life of the license. • Wireless Upgrade—The status or type of any Wireless Upgrade License that is currently installed on the Administration node. After the 90-day Evaluation License expires and you install a Wireless Upgrade License, the Current Licenses page reflects a Wireless License with <*x*> days remaining on the life of the license.
Licensed To	Name of the organization to which the license has been allotted.
Base (Active/Allowed)	A ratio representing the number of utilized endpoints versus the number of allowed endpoints that are supported under the current Base licensing scheme. For example, if you are using an Evaluation License and have identified only one endpoint, the ratio is 1/100. When you install a Wireless or Wireless Upgrade License, the applicable Active/Allowed user counts are automatically calculated to reflect the capabilities of the specific license(s) and are represented in the same existing Base and Advanced columns.
Advanced (Active/Allowed)	A ratio representing the number of utilized endpoints versus the number of allowed endpoints that are supported under the current Advanced licensing scheme. For example, if you are using an Evaluation License and have identified only one endpoint, the ratio is 1/100. When you install a Wireless or Wireless Upgrade License, the applicable Active/Allowed user counts are automatically calculated to reflect the capabilities of the specific license(s) and are represented in the same existing Base and Advanced columns.

Certificate Store Settings

The Certificate Store page enables you to configure certificates in Cisco ISE that can be used for authentication. This section contains the following topics;

Certificate Store Page

The following table describes the fields on the Certificate Store page, which you can use to view the certificates that are added to the Administration node. The navigation path for this page is: Administration > System > Certificates > Certificate Store.

Table A-6 Certificate Store Page

Fields	Usage Guidelines
Status	Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Friendly Name	Displays the name of the certificate.
Trust for Client Auth	A green checkmark icon indicates that the certificate will be used for establishing trust in all situations, including for client certificates presented to ISE. A yellow dash icon indicates certificate is not used for client authentication, and is only used to verify server certificates (from other ISE nodes or LDAP servers).
Issued To	Common Name (CN) of the certificate subject.
Issued By	Common Name (CN) of the certificate issuer.
Valid From	The “Not Before” certificate attribute.
Expiration	The “Not After” certificate attribute.
Expiration Status	Provides information about the status of the certificate expiration. There are five icons and categories of informational message that appear in this column: • Green—Expiring in more than 90 days • Blue—Expiring in 90 days or less • Yellow—Expiring in 60 days or less • Orange—Expiring in 30 days or less • Red—Expired
Include in Trust Store	Indicates whether the certificate is available for utilization as trust certificate. This is initially set to false. To include the certificate as a trust certificate, set the flag to true from the Certificate Store Edit page.

Certificate Store Import Settings

The following table describes the fields on the Certificate Store Import page, which you can use to add Certificate Authority (CA) certificates to Cisco ISE. The navigation path for this page is: Administration > System > Certificates > Certificate Store > Import.

Table A-7 Certificate Store Import Settings

Fields	Description
Browse	Click Browse to choose the certificate file from the computer that is running the browser.
Friendly Name	Enter a friendly name for the certificate. If you do not specify a name, Cisco ISE automatically creates a name in the format <*common name*>#<*issuer*>#<*nnnnn*>, where <*nnnnn*> is a unique five-digit number.

Table A-7 Certificate Store Import Settings (continued)

Fields	Description
Trust for client authentication	Check the check box if you want this certificate to be used in authenticating client certificates that are presented to ISE. If the box is not checked, the certificate will only be used to verify server certificates (from other ISE nodes or LDAP servers).
Enable Validation of Certificate Extensions	(Only if you check both the Trust for client authentication and Enable Validation of Certificate Extensions options) Ensure that the "keyUsage" extension is present and the "keyCertSign" bit is set, and that the basic constraints extension is present with the CA flag set to true.
Description	Enter an optional description.

Certificate Store Edit Settings

The following table describes the fields on the Certificate Store Edit Certificate page, which you can use to edit the Certificate Authority (CA) certificate attributes. The navigation path for this page is: Administration > System > Certificates > Certificate Store > Certificate > Edit.

Table A-8 Certificate Store Edit Settings

Fields	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate.
Description	Enter an optional description.
Status	Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Include in Trust Store	Check the check box to include the certificate as a trust certificate.
Certificate Usage	
Trust for client authentication	Check the check box if you want this certificate to be used in authenticating client certificates that are presented to ISE. If the box is not checked, the certificate will only be used to verify server certificates (from other ISE nodes or LDAP servers).
Enable Validation of Certificate Extensions	If you check both the Trust for client authentication and Enable Validation of Certificate Extensions options, ensure that the "keyUsage" extension is present and the "keyCertSign" bit is set, and that the basic constraints extension is present with the CA flag set to true.
Certificate Status Validation	ISE supports two ways of checking the revocation status of a client or server certificate that is issued by a particular CA. The first is to validate the certificate using the Online Certificate Status Protocol (OCSP), which makes a request to an OCSP service maintained by the CA. The second is to validate the certificate against a Certificate Revocation List (CRL) which is downloaded from the CA into ISE. Both of these methods can be enabled, in which case OCSP is used first, and only if a status determination cannot be made then the CRL is used.
Validate Against OCSP Service	Check the check box to validate the certificate against OCSP services. You must first create an OCSP Service to be able to check this box. See the "OCSP Services" section on page 8-31 for more information on OCSP services.

Table A-8 Certificate Store Edit Settings (continued)

Fields	Usage Guidelines
Reject the request if certificate status could not be determined by OCSP	Check the check box to reject the request if certificate status is determined by OCSP. If you check this check box, an unknown status value returned by the OCSP service will cause ISE to reject the client or server certificate currently being evaluated. See the "OCSP Services" section on page 8-31 for more information on OCSP services.
Download CRL	Check the check box for the Cisco ISE to download a CRL.
CRL Distribution URL	Enter the URL to download the CRL from a CA. This field will be automatically populated if it is specified in the certificate authority certificate. The URL must begin with "http", "https", or "ldap."
Retrieve CRL	The CRL can be downloaded automatically or periodically. Configure the time interval between downloads.
If download failed, wait	Configure the time interval to wait before Cisco ISE tries to download the CRL again.
Bypass CRL Verification if CRL is not Received	Check this check box, for the client requests to be accepted before the CRL is received. If you uncheck this check box, all client requests that use certificates signed by the selected CA will be rejected until Cisco ISE receives the CRL file.
Ignore that CRL is not yet valid or expired	Check this check box if you want Cisco ISE to ignore the start date and expiration date and continue to use the not yet active or expired CRL and permit or reject the EAP-TLS authentications based on the contents of the CRL. Uncheck this check box if you want Cisco ISE to check the CRL file for the start date in the Effective Date field and the expiration date in the Next Update field. If the CRL is not yet active or has expired, all authentications that use certificates signed by this CA are rejected.

Logging Settings

These pages allow you to configure the severity of debug logs, create an external log target, and enable Cisco ISE to send log messages to these external log targets.

Remote Logging Target Settings

The following table describes the fields on the Remote Logging Targets page, which you can use to create external locations (syslog servers) to store logging messages. The navigation path for this page is: Administration > System > Logging > Remote Logging Targets.

Table A-9 Remote Logging Target Settings

Fields	Usage Guidelines
Name	Enter the name of the new target.
Target Type	Select the target type. By default it is set to UDP Syslog.
Description	Enter a brief description of the new target.
IP Address	Enter the IP address of the destination machine where you want to store the logs.
Port	Enter the port number of the destination machine.
Facility Code	Choose the syslog facility code to be used for logging. Valid options are Local0 through Local7.

Table A-9 Remote Logging Target Settings (continued)

Fields	Usage Guidelines
Maximum Length	Enter the maximum length of the remote log target messages. Valid options are from 200 to 8192 bytes.
Buffer Message When Server Down	Check this check-box if you want Cisco ISE to buffer the syslog messages when TCP syslog targets and secure syslog targets are unavailable. ISE retries sending the messages to the target when the connection resumes. After the connection resumes, messages are sent by the order from oldest to newest and buffered messages are always sent before new messages. If the buffer is full, old messages are discarded.
Buffer Size (MB)	Set the buffer size for each target. By default, it is set to 100 MB. Changing the buffer size clears the buffer and all existing buffered messages for the specific target are lost.
Reconnect Timeout (Sec)	Give in seconds how long will the TCP and secure syslogs be kept before being discarded, when the server is down.
Select CA Certificate	Select a client certificate.
Ignore Server Certificate Validation	Check this check-box if you want ISE to ignore server certificate authentication and accept any syslog server. By default, this option is set to off unless the system is in FIPS mode when this is disabled.

Related Topics

Configuring Remote Syslog Collection Locations, page 11-4

Logging Category Settings

The following table describes the fields on the Logging Categories page, which you can use to configure the log severity level and choose logging targets for the logs of selected categories to be stored. The navigation path for this page is: Administration > System > Logging > Logging Categories.

Table A-10 Logging Category Settings

Fields	Usage Guidelines
Name	Displays the name of the logging category.
Log Severity Level	Allows you to choose the severity level for the diagnostic logging categories from the following options: • **FATAL**—Emergency. This option means that Cisco ISE cannot be used and you must take action immediately. • **ERROR**—This option indicates a critical or error condition. • **WARN**—This option indicates a normal but significant condition. This is the default condition. • **INFO**—This option indicates an informational message. • **DEBUG**—This option indicates a diagnostic bug message.
Local Logging	Check this check box to enable logging event for the category on the local node.
Target	Allows you to change the targets for a category by transferring the targets between the Available and the Selected boxes using the left and right icons. The Available box contains the existing logging targets, both local (predefined) and external (user-defined). The Selected box, which is initially empty, contains the selected targets for the specific category.

Related Topics

Setting Severity Levels for Message Codes, page 11-6

Maintenance Settings

These pages help you to manage data using the backup, restore, and data purge features.

Repository Settings

The following table describes the fields on the Repository List page, which you can use to create repositories to store your backup files. The navigation path for this page is: Administration > System > Maintenance > Repository.

Table A-11 Repository Settings

Fields	Usage Guidelines
Repository	Enter the name of the repository. Alphanumeric characters are allowed and the maximum length is 80 characters.
Protocol	Choose one of the available protocols that you want to use.
Server Name	(Required for TFTP, HTTP, HTTPS, FTP, SFTP, and NFS) Enter the hostname or IPv4 address of the server where you want to create the repository.

Table A-11 Repository Settings (continued)

Fields	Usage Guidelines
Path	Enter the path to your repository. This value must start with a forward slash (/). The path must be valid and must exist at the time you create the repository. The following three fields are required depending on the protocol that you have chosen.
User Name	(Required for FTP, SFTP, and NFS) Enter the username that has write permission to the specified server. Only alphanumeric characters are allowed.
Password	(Required for FTP, SFTP, and NFS) Enter the password that will be used to access the specified server. Passwords can consist of the following characters: 0 through 9, a through z, A through Z, -, ., |, @, #,$, %, ^, &, *, (,), +, and =. Supports up to 15 alphanumeric characters.

Related Topics

Creating Repositories, page 12-2

On-Demand Backup Settings

The following table describes the fields on the On-Demand Backup page, which you can use to obtain a backup at any point of time. The navigation path for this page is: Administration > System > Backup & Restore.

Table A-12 On-Demand Backup Settings

Fields	Usage Guidelines
Backup Name	Enter the name of your backup file.
Type	Select one of the following: • Configuration backup—contains both application-specific and Cisco ADE operating system configuration data. • Operational backup—contains Monitoring and Troubleshooting data.
Repository Name	Repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	This key is used to encrypt and decrypt the backup file.

Related Topics

Performing an On-Demand Backup, page 12-4

Scheduled Backup Settings

The following table describes the fields on the Scheduled Backup Page, which you can use to restore a full or incremental backup. The navigation path for this page is: Administration > System > Backup and Restore.

Table A-13 Scheduled Backup Settings

Fields	Usage Guidelines
Name	Enter a name for your backup file. You can enter a descriptive name of your choice. Cisco ISE appends the timestamp to the backup filename and stores it in the repository. You will have unique backup filenames even if you configure a series of backups. On the Scheduled Backup list page, the backup filename will be prepended with "backup_occur" to indicate that the file is a **kron** occurrence job.
Description	Enter a description for the backup.
Repository Name	Select the repository where your backup file should be saved. You cannot enter a repository name here. You can only choose an available repository from the drop-down list. Ensure that you create the repository before you run a backup.
Encryption Key	Enter a key to encrypt and decrypt the backup file.
Schedule Options	Choose the frequency of your scheduled backup and fill in the other options accordingly.

Related Topics

Scheduling a Backup, page 12-5

Admin Access Settings

These pages enable you to configure access settings for administrators.

Administrator Password Policy Settings

The following table describes the fields on the Administrator Password Policy page, which you can use to define a criteria that administrator passwords should meet. The navigation path for this page is: **Administration > System > Admin Access > Authentication**.

Table A-14 Administrator Password Policy Settings

Fields	Usage Guidelines
Minimum Length	Specifies the minimum length of the password (in characters). The default is six characters.
Password should not contain the admin name or its characters in reversed order	Check this check box to restrict the use of the administrator username or its characters in reverse order.
Password should not contain 'cisco' or its characters in reversed order	Check this check box to restrict the use of the word "cisco" or its characters in reverse order.
Password should not contain *variable* or its characters in reversed order	Check this check box to restrict the use of any word that you define or these characters in reverse order.
Password should not contain repeated characters four or more times consecutively	Check this check box to restrict the use of repeated characters four or more times consecutively.

Table A-14 Administrator Password Policy Settings (continued)

Fields	Usage Guidelines
Password must contain at least one character of each of the selected types	Specifies that the administrator password must contain at least one character of the type that you choose from the following choices: • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-alphanumeric characters
Password History	Specifies the number of previous passwords from which the new password must be different to prevent the repeated use of the same password. Also, specifies the number of characters that must be different from the previous password.
Password Lifetime	Specifies the following options to force users to change passwords after a specified time period: • Time (in days) before the administrator account is disabled if the password is not changed. (The allowable range is 0 to 2,147,483,647 days.) • Reminder (in days) before the administrator account is disabled.
Lock or Suspend Account with Incorrect Login Attempts	Specifies the number of times Cisco ISE records incorrect administrator passwords before locking the administrator out of Cisco ISE, and suspending or disabling account credentials. An e-mail is sent to the administrator whose account gets locked out. You can enter a custom e-mail remediation message.

Session Timeout and Session Info Settings

The following table describes the fields on the Session page, which you can use to define session timeout and terminate an active administrative session. The navigation path for this page is: Administration > System > Admin Access > Settings > Session.

Table A-15 Session Timeout and Session Info Settings

Fields	Usage Guidelines
Session Timeout	
Session Idle Timeout	Enter the time in minutes that you want Cisco ISE to wait before it logs out the administrator if there is no activity. The default value is 60 minutes. The valid range is from 6 to 100 minutes.
Session Info	
Invalidate	Check the check box next to the session ID that you want to terminate and click **Invalidate.**

Related Topics

- Configuring Session Timeout for Administrators, page 6-15

- Terminating an Active Administrative Session, page 6-15

Settings

These pages enable you to configure general settings for the various services.

Posture General Settings

The following table describes the fields on the Posture General Settings page, which you can use to configure general posture settings such as remediation time and posture status. The navigation path for this page is: Administration > System > Settings > Posture > General Settings.

Table A-16 Posture General Settings

Fields	Usage Guidelines
Remediation Timer	Enter a time value in minutes. The default value is 4 minutes. The valid range is 1 to 300 minutes.
Network Transition Delay	Enter a time value in seconds. The default value is 3 seconds. The valid range is 2 to 30 seconds.
Default Posture Status	Choose Compliant or Noncompliant. The non-agent devices like Linux assumes this status while connecting to the network.
Automatically Close Login Success Screen After	Check the check box to close the login success screen automatically after the specified time. Enter a time value in seconds, in the field next to the check box. You can configure the timer to close the login screen automatically between 0 to 300 seconds. If the time is set to zero, then the NAC Agents and Web Agents do not display the login success screen.

Posture Reassessment Configuration Settings

The following table describes the fields in the Posture Reassessment Configurations Page, which you can use to configure posture reassessment. The navigation path for this page is: Administration > System > Settings > Posture > Reassessments.

Table A-17 Posture Reassessment Configuration Settings

Fields	Usage Guidelines
Configuration Name	Enter the name of PRA configuration.
Configuration Description	Enter a description for PRA configuration.
Use Reassessment Enforcement?	Check the check box to apply the PRA configurations for the user identity groups.

Table A-17 Posture Reassessment Configuration Settings (continued)

Fields	Usage Guidelines
Enforcement Type	Choose the action to be enforced: • **Continue** — The user continues to have the privileged access without any user intervention to remediate the client irrespective of the posture requirement. • **Logoff** — If the client is not compliant, the user is forced to logoff from the network. When the client logs in again, the compliance status is unknown. • **Remediate** — If the client is not compliant, the agent waits for a specified time for the remediation to happen. Once the client has remediated, the agent sends the PRA report to the policy service node. If the remediation is ignored on the client, then the agent sends a logoff request to the policy service node to force the client to logoff from the network. If the posture requirement is set to mandatory, then the RADIUS session will be cleared as a result of the PRA failure action and a new RADIUS session has to start for the client to be postured again. If the posture requirement is set to optional, then the NAC Agent allows the user to click the continue option from the agent. The user can continue to stay in the current network without any restriction.
Interval	Enter a time interval in minutes to initiate PRA on the clients after the first successful login. The default value is 240 minutes. Minimum value is 60 minutes and maximum is 1440 minutes.
Grace time	Enter a time interval in minutes to allow the client to complete remediation. The grace time cannot be zero, and should be greater than the PRA interval. It can range between the default minimum interval (5 minutes) and the minimum PRA interval. The minimum value is 5 minutes and the maximum value is 60 minutes. **Note** The grace time is enabled only when the enforcement type is set to remediate action after the client fails the posture reassessment.
Select User Identity Groups	Choose a unique group or a unique combination of groups for your PRA configuration.
PRA configurations	Displays existing PRA configurations and user identity groups associated to PRA configurations.

Posture Acceptable Use Policy Configuration Settings

The following table describes the fields in the Posture Acceptable Use Policy Configurations Page, which you can use to configure an acceptable use policy for posture. The navigation path for this page is: Administration > System > Settings > Posture > Acceptable Use Policy.

Table A-18 Posture AUP Configurations Settings

Fields	Usage Guidelines
Configuration Name	Enter the name of the AUP configuration that you want to create.
Configuration Description	Enter the description of the AUP configuration that you want to create.

Table A-18 Posture AUP Configurations Settings (continued)

Fields	Usage Guidelines
Show AUP to Agent users (for NAC Agent and Web Agent on Windows only)	If checked, the Show AUP to Agent users check box displays users (for NAC Agents, and Web Agents on Windows only) the link to network usage terms and conditions for your network and click it to view the AUP upon successful authentication and posture assessment.
Use URL for AUP message radio button	When selected, you must enter the URL to the AUP message in the AUP URL, which clients must access upon successful authentication and posture assessment.
Use file for AUP message radio button	When selected, you must browse to the location and upload a file in a zipped format in the AUP File, which contains the index.html at the top level. The .zip file can include other files and subdirectories in addition to the index.html file. These files can reference each other using HTML tags.
AUP URL	Enter the URL to the AUP, which clients must access upon successful authentication and posture assessment.
AUP File	In the AUP File, browse to the file and upload it to the Cisco ISE server. It should be a zipped file and the zipped file should contain the index.html file at the top level.
Select User Identity Groups	In the Select User Identity Groups drop-down list, choose a unique user identity group, or a unique combination of user identity groups, for your AUP configuration. Note the following while creating an AUP configuration: • Posture AUP is not applicable for a guest flow • Each configuration must have a unique user identity group, or a unique combination of user identity groups • No two configurations have any user identity group in common • If you want to create a AUP configuration with a user identity group “Any”, then delete all other AUP configurations first • If you create a AUP configuration with a user identity group “Any”, then you cannot create other AUP configurations with a unique user identity group, or user identity groups. To create an AUP configuration with a user identity group other than Any, either delete an existing AUP configuration with a user identity group “Any” first, or update an existing AUP configuration with a user identity group “Any” with a unique user identity group, or user identity groups.
Acceptable use policy configurations—Configurations list	Lists existing AUP configurations and end user identity groups associated with AUP configurations.

EAP-FAST Settings

The following table describes the fields on the Protocol Settings page, which you can use to configure the EAP-FAST, EAP-TLS, and PEAP protocols. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > EAP FAST Settings.

Table A-19 Configuring EAP-FAST Settings

Fields	Usage Guidelines
Authority Identity Info Description	Enter a user-friendly string that describes the Cisco ISE node that sends credentials to a client. The client can discover this string in the Protected Access Credentials (PAC) information for type, length, and value (TLV). The default value is Identity Services Engine.
Master Key Generation Period	Specifies the master key generation period in seconds, minutes, hours, days, or weeks. The value must be a positive integer in the range 1 to 2147040000 seconds. The default is 604800 seconds, which is equivalent to one week.

Related Topics

Configuring EAP-FAST Settings, page 19-11

Generate PAC for EAP-FAST Settings

The following table describes the fields on the Generate PAC page, which you can use to configure protected access credentials for EAP-FAST authentication. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-FAST > Generate PAC.

Table A-20 Generating PAC for EAP-FAST Settings

Fields	Usage Guidelines
Tunnel PAC	Click this radio button to generate a tunnel PAC.
Machine PAC	Click this radio button to generate a machine PAC.
SGA PAC	Click this radio button to generate an SGA PAC.
Identity	(For the Tunnel and Machine PAC identity field) Specifies the username or machine name that is presented as the “inner username” by the EAP-FAST protocol. If the identity string does not match that username, authentication fails. This is the hostname as defined on the Adaptive Security Appliance (ASA). The identity string must match the ASA hostname otherwise, ASA cannot import the PAC file that is generated. If you are generating an SGA PAC, the Identity field specifies the Device ID of an SGA network device and is provided with an initiator ID by the EAP-FAST protocol. If the Identity string entered here does not match that Device ID, authentication fails. See the “OOB SGA PAC” section on page 24-18for more information on SGA PAC.
PAC Time to Live	(For the Tunnel and Machine PAC) Enter a value in seconds that specifies the expiration time for the PAC. The default is 604800 seconds, which is equivalent to one week. This value must be a positive integer between 1 and 157680000 seconds. For the SGA PAC, enter a value in days, weeks, months, or years. By default, the value is one year. The minimum value is one day and the maximum is 10 years.

Table A-20 Generating PAC for EAP-FAST Settings (continued)

Fields	Usage Guidelines
Encryption Key	Enter an encryption key. The length of the key must be between 8 and 256 characters. The key can contain uppercase or lowercase letters, or numbers, or a combination of alphanumeric characters.
Expiration Data	(For SGA PAC only) The expiration date is calculated based on the PAC Time to Live.

Related Topics

Generating the PAC for EAP-FAST, page 19-12

EAP-TLS Settings

The following table describes the fields on the EAP-TLS Settings page, which you can use to configure the EAP-TLS protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > EAP-TLS.

Table A-21 EAP-TLS Settings

Fields	Usage Guidelines
Enable EAP-TLS Session Resume	Check this check box to support an abbreviated reauthentication of a user who has passed full EAP-TLS authentication. This feature provides reauthentication of the user with only a Secure Sockets Layer (SSL) handshake and without applying the certificates. EAP-TLS session resume works only if the EAP-TLS session has not timed out.
EAP-TLS Session Timeout	Specifies the time in seconds after which the EAP-TLS session times out. The default value is 7200 seconds.

Related Topics

Configuring EAP-TLS Settings, page 19-12

PEAP Settings

The following table describes the fields on the PEAP Settings page, which you can use to configure the PEAP protocol settings. The navigation path for this page is: Administration > System > Settings > Protocols > PEAP.

Table A-22 PEAP Settings

Fields	Usage Guidelines
Enable PEAP Session Resume	Check this check box for the Cisco ISE to cache the TLS session that is created during phase one of PEAP authentication, provided the user successfully authenticates in phase two of PEAP. If a user needs to reconnect and the original PEAP session has not timed out, the Cisco ISE uses the cached TLS session, resulting in faster PEAP performance and a reduced AAA server load. You must specify a PEAP session timeout value for the PEAP session resume features to work.

Table A-22 PEAP Settings (continued)

Fields	Usage Guidelines
PEAP Session Timeout	Specifies the time in seconds after which the PEAP session times out. The default value is 7200 seconds.
Enable Fast Reconnect	Check this check box to allow a PEAP session to resume in the Cisco ISE without checking user credentials when the session resume feature is enabled.

Related Topics

Configuring PEAP Settings, page 19-13

RADIUS Settings

The following table describes the fields on the RADIUS Settings page, which you can use to detect the clients that fail to authenticate and to suppress the repeated reporting of successful authentications. The navigation path for this page is: Administration > System > Settings > Protocols > RADIUS.

Table A-23 RADIUS Settings

Fields	Usage Guidelines
Suppress Anomalous Clients	Check this check box to detect the clients for which the authentications fail repeatedly. A summary of the failures will be reported every Reporting Interval.
Detection Interval	Enter the time interval in minutes for the clients to be detected.
Reporting Interval	Enter the time interval in minutes for the failed authentications to be reported.
Reject Requests After Detection	Check this check box to reject the requests after the detection. The requests for anomalous clients will be rejected every Request Rejection Interval
Request Rejection Interval	Enter the time interval in minutes for which the requests to be rejected. This option is available only when you have checked Reject Requests After Detection.
Suppress Repeated Successful Authentications	Check this check box to prevent repeated reporting of successful authentication requests in last 24 hours that have no change in identity context, network device, and authorization.
Accounting Suppression Interval	Enter the time interval in seconds for which the reporting of accounting requests to be suppressed.
Long Processing Step Threshold Interval	Enter the time interval in milliseconds. The steps are displayed in authentication details reports. If execution of a single step exceeds the specified threshold, then it will be highlighted in the authentication details report.

Related Topics

Configuring RADIUS Settings, page 19-13

Security Group Access Settings

For Cisco ISE to function as an Security Group Access (SGA) server and provide SGA services, you must define some global SGA settings. The following table describes fields in Security Group Access page. The navigation path for this page is: Administration > System > Settings > Security Group Access.

Table A-24 Configuring Security Group Access Settings

Fields	Usage Guidelines
Tunnel PAC Time to Live	Specify the expiry time for the PAC. The tunnel PAC generates a tunnel for the EAP-FAST protocol. You can specify the time in seconds, minutes, hours, days, or weeks. The default value is 90 days. The valid ranges follow: • 1 to 157680000 seconds • 1 to 2628000 minutes • 1 to 43800 hours • 1 to 1825 days • 1 to 260 weeks
Proactive PAC Update Will Occur After	Cisco ISE proactively provides a new PAC to the client after successful authentication when a configured percentage of the Tunnel PAC TTL remains. The tunnel PAC update is initiated by the server after the first successful authentication that is performed before the PAC expiration. This mechanism allows the client to be always updated with a valid PAC. The default value is 10%.
All Tags Automatically Generated by System	Choose this option if you want all the SGTs to be automatically generated by Cisco ISE. Use this option only if you plan to manually configure specific security groups and policies on the SGA device.
Reserve a Range	Choose this option if you want to reserve a range of security group tags (SGTs) to be configured on the device manually. Cisco ISE creates an SGT by default: Unknown, which takes the value as 0. If you configure a range of SGTs, Cisco ISE will not use the values in this range while generating SGT values.
All tags are manually defined	Choose this option to define the SGTs manually.

Identity Management

These pages enable you to configure and manage identities in Cisco ISE.

Endpoints

These pages enable you to configure and manage endpoints that connect to your network.

Endpoint Settings

The following table describes the fields on the Endpoints page, which you can use to create endpoints and assign policies for endpoints. The navigation path for this page is: Administration > Identity Management > Identities > Endpoints.

Table A-25 Endpoint Settings

Fields	Usage Guidelines
MAC Address	Enter the MAC address in hexadecimal format to create an endpoint statically. The MAC address is the device identifier for the interface that is connected to the Cisco ISE enabled network
Static Assignment	Check this check box when you want to create an endpoint statically in the Endpoints page and the status of static assignment is set to static. You can toggle the status of static assignment of an endpoint from static to dynamic or from dynamic to static.
Policy Assignment	(Disabled by default unless the Static Assignment is checked) Choose a matching endpoint policy from the Policy Assignment drop-down list. You can do one of the following: • If you do not choose a matching endpoint policy, but use the default endpoint policy Unknown, then the static assignment status is set to dynamic for the endpoint that allows dynamic profiling of an endpoint. • If you choose a matching endpoint policy other than Unknown, then the static assignment status is set to static for that endpoint and the Static Assignment check box is automatically checked.
Static Group Assignment	(Disabled by default unless the Static group Assignment is checked) Check this check box when you want to assign an endpoint to an identity group statically. In you check this check box, the profiling service does not change the endpoint identity group the next time during evaluation of the endpoint policy for these endpoints, which were previously assigned dynamically to other endpoint identity groups. If you uncheck this check box, then the endpoint identity group is dynamic as assigned by the ISE profiler based on policy configuration. If you do not choose the Static Group Assignment option, then the endpoint is automatically assigned to the matching identity group the next time during evaluation of the endpoint policy.
Identity Group Assignment	Choose an endpoint identity group to which you want to assign the endpoint. You can assign an endpoint to an identity group when you create an endpoint statically, or when you do not want to use the Create Matching Identity Group option during evaluation of the endpoint policy for an endpoint. Cisco ISE includes the following system created endpoint identity groups: • Blacklist • GuestEndpoints • Profiled – Cisco IP-Phone – Workstation • RegisteredDevices • Unknown

Endpoint Import from LDAP Settings

The following table describes the fields on the Import from LDAP page, which you can use to import endpoints from an LDAP server. The navigation path for this page is: Administration > Identity Management > Identities > Endpoints.

Table A-26 Endpoint Import from LDAP Settings

Fields	Usage Guidelines
Connection Settings	
Host	Enter the hostname, or the IP address of the LDAP server.
Port	Enter the port number of the LDAP server. You can use the default port 389 to import from an LDAP server, and the default port 636 to import from an LDAP server over SSL. **Note** Cisco ISE supports any configured port number. The configured value should match the LDAP server connection details.
Enable Secure Connection	Check the Enable Secure Connection check box to import from an LDAP server over SSL.
Root CA Certificate Name	Click the drop-down arrow to view the trusted CA certificates. The Root CA Certificate Name refers to the trusted CA certificate that is required to connect to an LDAP server. You can add (import), edit, delete, and export trusted CA certificates in Cisco ISE.
Anonymous Bind	Check the Anonymous Bind check box to enable the anonymous bind. You must enable either the Anonymous Bind check box, or enter the LDAP administrator credentials from the slapd.conf configuration file.
Admin DN	Enter the distinguished name (DN) configured for the LDAP administrator in the slapd.conf configuration file. Admin DN format example: cn=Admin, dc=cisco.com, dc=com
Password	Enter the password configured for the LDAP administrator in the slapd.conf configuration file.
Base DN	Enter the distinguished name of the parent entry. Base DN format example: dc=cisco.com, dc=com.
Query Settings	
MAC Address objectClass	Enter the query filter, which is used for importing the MAC address. For example, ieee802Device.
MAC Address Attribute Name	Enter the returned attribute name for import. For example, macAddress.

Table A-26 Endpoint Import from LDAP Settings (continued)

Fields	Usage Guidelines
Profile Attribute Name	Enter the name of the LDAP attribute. This attribute holds the policy name for each endpoint entry that is defined in the LDAP server. When you configure the Profile Attribute Name field, consider the following: • If you do not specify this LDAP attribute in the Profile Attribute Name field or configure this attribute incorrectly, then endpoints are marked "Unknown" during an import operation, and these endpoints are profiled separately to the matching endpoint profiling policies. • If you configure this LDAP attribute in the Profile Attribute Name field, the attribute values are validated to ensure that the endpoint policy matches with an existing policy in Cisco ISE, and endpoints are imported. If the endpoint policy does not match with an existing policy, then those endpoints will not be imported.
Time Out [seconds]	Enter the time in seconds between 1 and 60 seconds.

Groups

These pages enable you to configure and manage endpoint identity groups.

Endpoint Identity Group Settings

The following table describes the fields on the Endpoint Identity Groups page, which you can use to create an endpoint group. The navigation path for this page is: Administration > Identity Management > Groups > Endpoint Identity Groups.

Table A-27 Endpoint Identity Group Settings

Fields	Usage Guidelines
Name	Enter the name of the endpoint identity group that you want to create.
Description	Enter a description for the endpoint identity group that you want to create.
Parent Group	Choose an endpoint identity group from the Parent Group drop-down list to which you want to associate the newly created endpoint identity group. Cisco ISE includes the following five endpoint identity groups: • Blacklist • GuestEndpoints • Profiled • RegisteredDevices • Unknown In addition, it creates two more identity groups, Cisco-IP-Phone and Workstation, which are associated to the Profiled (parent) identity group.

External Identity Sources

These pages enable you to configure and manage external identity sources that contain user data that Cisco ISE uses for authentication and authorization.

LDAP Identity Source Settings

The following table describes the fields on the LDAP Identity Sources page, which you can use to create an LDAP instance and connect to it. The navigation path for this page is: Administration > Identity Management > External Identity Sources > LDAP.

LDAP General Settings

The following table describes the fields in the General tab.

Table A-28 LDAP General Settings

Fields	Usage Guidelines
Name	Enter a name for the LDAP instance. This value is used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 64 characters.
Description	Enter a description for the LDAP instance. This value is of type string, and has a maximum length of 1024 characters.
Schema	Choose any one of the following built-in schema types and the schema details are prepopulated and are hidden: • Active Directory • Sun Directory Server • Novell eDirectory **Note** You can edit the details from the predefined schema, but Cisco ISE detects the change and creates a Custom schema. You can click the arrow next to Schema to view the schema details.
Note The following fields contain schema details are displayed only when you choose the Custom schema.	
Subject Objectclass	Enter a value to be used in searches to obtain the subject DN and attributes. The value is of type string and the maximum length is 256 characters.
Subject Name Attribute	Enter the name of the attribute containing the username in the request. The value is of type string and the maximum length is 256 characters.
Certificate Attribute	Enter the attribute that contains the certificate definitions. For certificate-based authentication, these definitions are used to validate certificates that are presented by clients.
Group Objectclass	Enter a value to be used in searches to specify the objects that are recognized as groups. The value is of type string and the maximum length is 256 characters.
Group Map Attribute	Specifies the attribute that contains the mapping information. This attribute can be a user or group attribute based on the reference direction that is chosen.
Subject Objects Contain Reference To Groups	Click this radio button if the subject objects contain an attribute that specifies the group to which they belong.

Table A-28 LDAP General Settings (continued)

Fields	Usage Guidelines
Group Objects Contain Reference To Subjects	Click this radio button if the group objects contain an attribute that specifies the subject. This value is the default value.
Subjects in Groups Are Stored in Member Attribute As	(Only available when you select the Group Objects Contain Reference To Subjects radio button) Specifies how members are sourced in the group member attribute and defaults to the DN.

LDAP Connection Settings

The following table describes the fields in the Connection Settings tab.

Table A-29 LDAP Connection Settings

Fields	Usage Guidelines
Enable Secondary Server	Check this option to enable the secondary LDAP server to be used as a backup if the primary LDAP server fails. If you check this check box, you must enter configuration parameters for the secondary LDAP server.
Primary and Secondary Servers	
Hostname/IP	Enter the IP address or DNS name of the machine that is running the LDAP software. The hostname can contain from 1 to 256 characters or a valid IP address expressed as a string. The only valid characters for hostnames are alphanumeric characters (a to z, A to Z, 0 to 9), the dot (.), and the hyphen (-).
Port	Enter the TCP/IP port number on which the LDAP server is listening. Valid values are from 1 to 65,535. The default is 389, as stated in the LDAP specification. If you do not know the port number, you can find this information from the LDAP server administrator.
Access	Anonymous Access—Click to ensure that searches on the LDAP directory occur anonymously. The server does not distinguish who the client is and will allow the client read access to any data that is configured as accessible to any unauthenticated client. In the absence of a specific policy permitting authentication information to be sent to a server, a client should use an anonymous connection. Authenticated Access—Click to ensure that searches on the LDAP directory occur with administrative credentials. If so, enter information for the Admin DN and Password fields.
Admin DN	Enter the DN of the administrator. The Admin DN is the LDAP account that has permission to search all required users under the User Directory Subtree and to search groups. If the administrator specified does not have permission to see the group name attribute in searches, group mapping fails for users who are authenticated by that LDAP server.
Password	Enter the LDAP administrator account password.
Secure Authentication	Click to use SSL to encrypt communication between Cisco ISE and the primary LDAP server. Verify that the Port field contains the port number used for SSL on the LDAP server. If you enable this option, you must choose a root CA.
Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate. See the "Certificate Store" section on page 8-24 and "Adding a Certificate to Certificate Store" section on page 8-27 for information on CA certificates.
Server Timeout	Enter the number of seconds that Cisco ISE waits for a response from the primary LDAP server before determining that the connection or authentication with that server has failed. Valid values are 1 to 300. The default is 10.

Table A-29 LDAP Connection Settings (continued)

Fields	Usage Guidelines
Max. Admin Connections	Enter the maximum number of concurrent connections (greater than 0) with LDAP administrator account permissions that can run for a specific LDAP configuration. These connections are used to search the directory for users and groups under the User Directory Subtree and the Group Directory Subtree. Valid values are 1 to 99. The default is 20.
Test Bind to Server	Click to test and ensure that the LDAP server details and credentials can successfully bind. If the test fails, edit your LDAP server details and retest.

LDAP Directory Organization Settings

The following table describes the fields in the Directory Organization tab.

Table A-30 LDAP Directory Organization Settings

Fields	Usage Guidelines
Subject Search Base	Enter the DN for the subtree that contains all subjects. For example: o=corporation.com If the tree containing subjects is the base DN, enter: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.
Group Search Base	Enter the DN for the subtree that contains all groups. For example: ou=organizational unit, ou=next organizational unit, o=corporation.com If the tree containing groups is the base DN, type: o=corporation.com or dc=corporation,dc=com as applicable to your LDAP configuration. For more information, refer to your LDAP database documentation.

Table A-30 LDAP Directory Organization Settings (continued)

Fields	Usage Guidelines
Search for MAC Address in Format	Enter a MAC Address format for Cisco ISE to use for search in the LDAP database. MAC addresses in internal identity sources are sourced in the format xx-xx-xx-xx-xx-xx. MAC addresses in LDAP databases can be sourced in different formats. However, when Cisco ISE receives a host lookup request, Cisco ISE converts the MAC address from the internal format to the format that is specified in this field. Use the drop-down list to enable searching for MAC addresses in a specific format, where <*format*> can be any one of the following: • xxxx.xxxx.xxxx • xxxxxxxxxxxx • xx-xx-xx-xx-xx-xx • xx:xx:xx:xx:xx:xx The format you choose must match the format of the MAC address sourced in the LDAP server.
Strip Start of Subject Name Up To the Last Occurrence of the Separator	Enter the appropriate text to remove domain prefixes from usernames. If, in the username, Cisco ISE finds the delimiter character that is specified in this field, it strips all characters from the beginning of the username through the delimiter character. If the username contains more than one of the characters that are specified in the <start_string> box, Cisco ISE strips characters through the last occurrence of the delimiter character. For example, if the delimiter character is the backslash (\) and the username is DOMAIN\user1, Cisco ISE submits user1 to an LDAP server. **Note** The <start_string> cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark (“), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.
Strip End of Subject Name from the First Occurrence of the Separator	Enter the appropriate text to remove domain suffixes from usernames. If, in the username, Cisco ISE finds the delimiter character that is specified in this field, it strips all characters from the delimiter character through the end of the username. If the username contains more than one of the characters that are specified in this field, Cisco ISE strips characters starting with the first occurrence of the delimiter character. For example, if the delimiter character is @ and the username is *user1@domain*, then Cisco ISE submits *user1* to the LDAP server. **Note** The <*end_string*> box cannot contain the following special characters: the pound sign (#), the question mark (?), the quotation mark ("), the asterisk (*), the right angle bracket (>), and the left angle bracket (<). Cisco ISE does not allow these characters in usernames.

Related Topics

- LDAP, page 14-19
- Adding LDAP Identity Sources, page 14-24
- Configuring Primary and Secondary LDAP Servers, page 14-25

RADIUS Token Identity Sources Settings

The following table describes the fields on the RADIUS Token Identity Sources page, which you can use to configure and connect to an external RADIUS identity source. The navigation path for this page is: Administration > Identity Management > External Identity Sources > RADIUS Token.

Table A-31 RADIUS Token Identity Source Settings

Fields	Usage Guidelines
Name	Enter a name for the RADIUS token server. The maximum number of characters allowed is 64.
Description	Enter a description for the RADIUS token server. The maximum number of characters is 1024.
SafeWord Server	Check this check box if your RADIUS identity source is a SafeWord server.
Enable Secondary Server	Check this check box to enable the secondary RADIUS token server for Cisco ISE to use as a backup in case the primary fails. If you check this check box, you must configure a secondary RADIUS token server.
Always Access Primary Server First	Click this radio button if you want Cisco ISE to always access the primary server first.
Fallback to Primary Server after	Click this radio button to specify the amount of time in minutes that Cisco ISE can authenticate using the secondary RADIUS token server if the primary server cannot be reached. After this time elapses, Cisco ISE reattempts to authenticate against the primary server.
Primary Server	
Host IP	Enter the IP address of the primary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret that is configured on the primary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the primary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the primary RADIUS token server before it determines that the primary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the primary server before moving on to the secondary server (if defined) or dropping the request if a secondary server is not defined. Valid values are 1 to 9. The default is 3.
Secondary Server	
Host IP	Enter the IP address of the secondary RADIUS token server. This field can take as input a valid IP address that is expressed as a string. Valid characters that are allowed in this field are numbers and dot (.).
Shared Secret	Enter the shared secret configured on the secondary RADIUS token server for this connection.
Authentication Port	Enter the port number on which the secondary RADIUS token server is listening. Valid values are from 1 to 65,535. The default is 1812.
Server Timeout	Specify the time in seconds that Cisco ISE should wait for a response from the secondary RADIUS token server before it determines that the secondary server is down. Valid values are 1 to 300. The default is 5.
Connection Attempts	Specify the number of attempts that Cisco ISE should make to reconnect to the secondary server before dropping the request. Valid values are 1 to 9. The default is 3.

Related Topics

- RADIUS Token Identity Sources, page 14-27
- Adding a RADIUS Token Server, page 14-31

RSA SecurID Identity Source Settings

The following table describes the fields on the RSA SecurID Identity Sources page, which you can use to create and connect to an RSA SecurID identity source. The navigation path for this page is: Administration > Identity Management > External Identity Sources > RSA SecurID.

RSA Prompt Settings

The following table describes the fields in the RSA Prompts tab.

Table A-32 RSA Prompt Settings

Fields	Usage Guidelines
Enter Passcode Prompt	Enter a text string to obtain the passcode.
Enter Next Token Code	Enter a text string to request the next token.
Choose PIN Type	Enter a text string to request the PIN type.
Accept System PIN	Enter a text string to accept the system-generated PIN.
Enter Alphanumeric PIN	Enter a text string to request an alphanumeric PIN.
Enter Numeric PIN	Enter a text string to request a numeric PIN.
Re-enter PIN	Enter a text string to request the user to re-enter the PIN.

RSA Message Settings

The following table describes the fields in the RSA Messages tab.

Table A-33 RSA Messages Settings

Fields	Usage Guidelines
Display System PIN Message	Enter a text string to label the system PIN message.
Display System PIN Reminder	Enter a text string to inform the user to remember the new PIN.
Must Enter Numeric Error	Enter a message that instructs users to enter only numbers for the PIN.
Must Enter Alpha Error	Enter a message that instructs users to enter only alphanumeric characters for PINs.
PIN Accepted Message	Enter a message that the users see when their PIN is accepted by the system.
PIN Rejected Message	Enter a message that the users see when the system rejects their PIN.
User Pins Differ Error	Enter a message that the users see when they enter an incorrect PIN.
System PIN Accepted Message	Enter a message that the users see when the system accepts their PIN.
Bad Password Length Error	Enter a message that the users see when the PIN that they specify does not fall within the range specified in the PIN length policy.

Related Topics

- RSA Identity Sources, page 14-32
- Adding RSA Identity Sources, page 14-35

Identity Management Settings

User Password Policy Settings

The following table describes the fields on the User Password Policy page, which you can use to define a criteria for user passwords. The navigation path for this page is: Administration > Identity Management > Settings > Password Policy.

Table A-34 User Password Policy Settings

Option	Description
Minimum Length	Sets the minimum length of password (in characters)
Username	Restricts the use of the username or its characters in reversed order
Cisco	Restricts the use of “cisco” or its characters in reversed order
Special characters	Restricts the use of special characters that you define in reverse order
Repeated characters	Restricts the use of characters repeated four or more times consecutively
Required characters	Requires that the password include at least one of each of the following types: • Lowercase alphabetic characters • Uppercase alphabetic characters • Numeric characters • Non-alphanumeric characters
Password History	Enter the number of previous versions from which the password must be different to prevent the repeated use of the same password You can also enter the number of characters that must be different from the previous password
Password Lifetime	Sets the following options to force users to change passwords after a specified time period: • Time (in days) before the user account is disabled if the password is not changed • Reminder (in days) before the user account is disabled
Lock or Suspend Account with Incorrect Login Attempts	Specifies the number of times Cisco ISE records incorrect user passwords before locking the user out of Cisco ISE, and suspending or disabling account credentials. An e-mail is sent to the user whose account gets locked out. You can enter a custom e-mail remediation message.

Network Resources

Network Devices

These pages enable you to add and manage network devices.

Network Device Definition Settings

The following table describes the fields on the Network Devices page, which you can use to a network access device in Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

This section covers the Admin portal elements for the following configuration:

- RADIUS Authentication Settings, page A-37
- SNMP Settings, page A-38
- SGA Device Attribute Settings, page A-39

Table A-35 Network Device Definition Settings

Fields	Description
Name	Enter the name for the network device. You can provide a descriptive name to the network device that can be different from the hostname of the device. The device name is a logical identifier. **Note** You cannot edit the name of a device once configured.
Description	Enter the description for the device.
IP Address/Mask	Enter a single IP address and a subnet mask. The following are the guidelines that must be followed while defining the IP addresses and subnet masks: • You can define a specific IP address, or a range with a subnet mask. If device A has an IP address range defined, you can configure another device B with an individual address from the range that is defined in device A. • You cannot define two devices with the same specific IP addresses. • You cannot define two devices with the same IP range. The IP ranges must not overlap either partially or completely.
Model Name	Click the drop-down list to choose the device model, for example, the Cisco Catalyst 6K, the Cisco Nexus 7K, and so on. You can use the model name as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Software Version	Click the drop-down list d to choose the version of the software running on the network device, for example, Cisco IOS Release 12.3, 12.3 (2), and so on. You can use the software version as one of the parameters while checking for conditions in rule-based policies. This attribute is present in the device dictionary.
Network Device Group	Click the Location and Device Type drop-down lists to choose a location and device type that can be associated with the network device. If you do not specifically assign a device to a group when you configure it, it becomes a part of the default device groups (root NDGs), which is All Locations by location and All Device Types by device type and the default device groups (root NDGs) are assigned. For example, All Locations and All Device Groups.

RADIUS Authentication Settings

The following table describes the fields on the New Network Device page, which you can use to configure RADIUS authentication settings for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-36 RADIUS Authentication Settings

Fields	Usage Guidelines
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter a shared secret, which can be up to 128 characters in length. The shared secret is the key that you have configured on the network device using the **radius-hos**t command with the **pac** option.
Enable KeyWrap	Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm. **Note** When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.
Key Encryption Key	(Only appears when you enable KeyWrap) Enter an encryption key that is used for session encryption (secrecy).
Message Authenticator Code Key	(Only appears when you enable KeyWrap) Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages.
Key Input Format	Choose one of the following formats: • **ASCII**—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long. • **Hexadecimal**—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long. You can specify the key input format that you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLC. (The value that you specify must be the correct [full] length for the key, and shorter values are not permitted.)

SNMP Settings

The following table describes the fields on the New Network Device page, which you can use to configure SNMP settings for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-37 SNMP Settings

Fields	Usage Guidelines
SNMP Version	Choose an SNMP version from the Version drop-down list to be used for requests. Version includes the following: • 1—SNMPv1 does not support informs. • 2c • 3—SNMPv3 is the most secure model because it allows packet encryption when you choose the Priv security level. **Note** If you have configured your network device with SNMPv3 parameters, you cannot generate the Network Device Session Status Summary report that is provided by the Monitoring service (Operations > Reports > Catalog > Network Device > Session Status Summary). You can generate this report successfully if your network device is configured with SNMPv1 or SNMPv2c parameters.
SNMP RO Community	(Only for SNMP Versions 1 and 2c when selected) Enter the Read Only Community string that provides Cisco ISE with a particular type of access to the device.
SNMP Username	(Only for SNMP Version 3) Enter SNMP username.
Security Level	(Only for SNMP Version 3) Choose the security level from the following: • Auth—Enables Message Digest 5 or Secure Hash Algorithm (SHA) packet authentication • No Auth—No authentication and no privacy security level • Priv—Enables Data Encryption Standard (DES) packet encryption
Auth Protocol	(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Choose the authentication protocol that you want the network device to use. Authentication Protocol includes one of the following for security levels of Auth and Priv: • MD5 • SHA
Auth Password	(Only for SNMP Version 3 when the security levels Auth and Priv are selected) Enter the authentication key that must be at least 8 characters in length. Click **Show** to display the Auth Password that is already configured for the device.
Privacy Protocol	(Only for SNMP Version 3 when the security level Priv is selected) Choose the privacy protocol that you want the network device to use. Privacy Protocols are one of the following: • DES • AES128 • AES192 • AES256 • 3DES

Table A-37 SNMP Settings (continued)

Fields	Usage Guidelines
Privacy Password	(Only for SNMP Version 3 when the security level Priv is selected) Enter the privacy key. Click **Show** to display the Privacy Password that is already configured for the device.
Polling Interval	Enter the polling interval in seconds. The default is 3600 seconds.
Link Trap Query	Check this check box to receive and interpret linkup and linkdown notifications received through the SNMP Trap.
Mac Trap Query	Check this check box to receive and interpret MAC notifications received through the SNMP Trap
Originating Policy Service Node	Indicates which ISE server to be used to poll for SNMP data. By default, it is automatic, but you can overwrite the setting by assigning different values.

SGA Device Attribute Settings

The following table describes the fields on the New Network Device page, which you can use to configure SGA Attributes for the device. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-38 SGA Device Attribute Settings

Fields	Usage Guidelines
SGA Device Notification and Updates Settings	
Use Device ID for SGA Identification	Check this check box if you want the Device Name to be listed as the device identifier in the Device ID field. If you check this check box, then the Device Name appears in the Device Id field. You can also change this Device Id to a descriptive name of your choice.
Device Id	(Only when the Use Device ID for SGA Identification check box is not checked). You can use the Device Name as the logical identifier when populated in this field.
Password	Enter the password to authenticate the SGA device (the same password that you have configured on the SGA device command-line interface [CLI]). Click **Show** to display the password that is used to authenticate the SGA device.
Download Environment Data Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the SGA device environment information from Cisco ISE. For example, if you enter 60 in seconds, the device would download its environment data from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Download Peer Authorization Policy Every	Specify the expiry time that allows you to configure the time interval in seconds, minutes, hours, weeks, or days between to download the peer authorization policy from Cisco ISE. For example, if you enter 60 in seconds, the device would download its peer authorization policy from Cisco ISE every minute. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.

Table A-38 SGA Device Attribute Settings (continued)

Fields	Usage Guidelines
Reauthentication Every	Specify the 802.1X reauthentication period that allows you to configure the time interval in seconds, minutes, hours, weeks or days between for reauthentication. In a network that is configured with the SGA solution, after initial authentication, the SGA device re authenticates itself against Cisco ISE. For example, if you enter 1000 seconds, the device would authenticate itself against Cisco ISE every 1000 seconds. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Download SGACL Lists Every	Specify the expiry time for SGACL lists that allow you to configure the time interval in seconds, minutes, hours, weeks or days between to download SGACLs from Cisco ISE. For example, if you enter 3600 seconds, the network device obtains the SGACL lists from Cisco ISE every 3600 seconds. The default value is 86,400 seconds or one day. The valid range is from 1 to 24850.
Other SGA Devices to Trust This Device (SGA Trusted)	Check this check box if you want all the peer devices to trust this SGA device. If you uncheck this check box, the peer devices do not trust this device, and all packets that arrive from this device will be colored or tagged accordingly.
Notify this device about SGA configuration changes	Check this check box if you want Cisco ISE to send SGA CoA notifications to this SGA device.
Device Configuration Deployment Settings	
Include this device when deploying Security Group Tag Mapping Updates	Check this check box if you want this SGA device to obtain the IP-SGT mappings using device interface credentials.
Exec Mode Username	Enter the username that has privileges to edit the device configuration in the Exec mode.
Exec Mode Password	Enter the password of the user having privileges to edit the device configuration in the Exec mode.
Enable Mode Password	Enter the password to enable Exec mode password for the device that would allow you to edit its configuration. Click **Show** to display the Exec mode password that is already configured for this device.
Out Of Band (OOB) SGA PAC Display	
Issue Date	Displays the issuing date of the last SGA PAC that has been generated by Cisco ISE for this SGA device.
Expiration Date	Displays the expiration date of the last SGA PAC that has been generated by Cisco ISE for this SGA device.
Issued By	Displays the name of the issuer (an SGA administrator) of the last SGA PAC that has been generated by Cisco ISE for this device.
Generate PAC	Click Generate PAC to create SGA Protected Access Credentials (PAC). By default, Out Of Band SGA Protected Access Credentials (PAC) information is empty, but appears disabled when populated. SGA PAC information can be automatically populated when you generate SGA PAC for any SGA enabled device.

Default Network Device Definition Settings

The following table describes the fields on the Default Network device page, which allows you to configure a default network device that Cisco ISE can use for RADIUS authentications. The navigation path for this page is: Administration > Network Resources > Network Devices > Default Device.

Table A-39 Default Network Device Definition Settings

Fields	Usage Guidelines
Default Network Device Status	Choose **Enable** from the Default Network Device Status drop-down list to enable the default network device definition.
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter the shared secret that can be up to 128 characters in length. The shared secret is the key that you have configured on the network device using the **radius-hos**t command with the **pac** option.
Enable KeyWrap	Check this check box only when supported on the network device, which increases RADIUS security via an AES KeyWrap algorithm. When you run Cisco ISE in FIPS mode, you must enable KeyWrap on the network device.
Key Encryption Key	Enter an encryption key that is used for session encryption (secrecy) when you enable KeyWrap.
Message Authenticator Code Key	Enter the key that is used for keyed Hashed Message Authentication Code (HMAC) calculation over RADIUS messages when you enable KeyWrap.
Key Input Format	Choose one of the following formats: • **ASCII**—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long. • **Hexadecimal**—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long. You can specify the key input format that you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLC. (The value that you specify must be the correct [full] length for the key, and shorter values are not permitted.)

Network Device Import Settings

The following table describes the fields on the Network Device Import Page, which you can use to import network device details into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Devices.

Table A-40 Network Devices Import Settings

Fields	Usage Guidelines
Generate a Template	Click this link to create a comma-separated value (.csv) template file. You must update the template with network devices information in the same format, and save it locally to import those network devices into any Cisco ISE deployment.
File	Click **Browse** to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment. You can import network devices in another Cisco ISE deployment with new and updated network devices information using import.
Overwrite Existing Data with New Data	Check this check box if you want Cisco ISE to replace existing network devices with the devices in your import file. If you do not check this check box, new network device definitions that are available in the import file are added to the network device repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network devices until that time of an error. If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import devices.

Network Device Groups

These pages enable you to configure and manage network device groups.

Network Device Group Settings

The following table describes the fields on the Network Device Groups Page, which you can use to create network device groups. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

Table A-41 Network Device Group Settings

Fields	Usage Guidelines
Name	Enter the name for the root Network Device Group (NDG). For all subsequent child network device groups under the root NDG, enter the name of the new network device group. The full name of the Network Device Group that can have a maximum of 100 characters. For example, if you are creating a subgroup India under the parent groups Global > Asia, then the full name of the NDG that you are creating would be Global#Asia#India and this full name should not exceed 100 characters. If the full name of the NDG exceeds 100 characters, the NDG creation fails.

Table A-41 Network Device Group Settings (continued)

Fields	Usage Guidelines
Description	Enter the description for the root or the child Network Device Group.
Type	Enter the type for the root Network Device Group. For all subsequent child network device groups under the root NDG, the type is inherited from the parent NDG and therefore all the child NDGs under a root NDG will be of the same type. If this NDG is a root NDG, then the type will be available as an attribute in the device dictionary. You can define conditions based on this attribute. The name of the NDG is one of the values that this attribute can take.

Network Device Group Import Settings

The following table describes the fields on the Network Device Group Import Page, which you can use to import network device groups into Cisco ISE. The navigation path for this page is: Administration > Network Resources > Network Device Groups > Groups.

Table A-42 Network Device Groups Import Settings

Fields	Usage Guidelines
Generate a Template	Click this link to create a comma-separated value (.csv) template file. You must update the template with network device groups information in the same format, and save it locally to import those network device groups into any Cisco ISE deployment.
File	Click **Browse** to the location of the comma-separated value file that you might have created or previously exported from any Cisco ISE deployment. You can import network device groups in another Cisco ISE deployment with new and updated network device groups information using import.
Overwrite Existing Data with New Data	Check this check box if you want Cisco ISE to replace existing network device groups with the device groups in your import file. If you do not check this check box, new network device group that are available in the import file are added to the network device group repository. Duplicate entries are ignored.
Stop Import on First Error	Check this check box if you want Cisco ISE to discontinue import when it encounters an error during import, but Cisco ISE imports network device groups until that time of an error. If this check box is not checked and an error is encountered, the error is reported, and Cisco ISE continues to import device groups.

External RADIUS Server Settings

The following table describes the fields on the External RADIUS Server page, which you can use to configure a RADIUS server. For Cisco ISE to act as a RADIUS server, you must configure it in this page. The navigation path for this page is: Administration > Network Resources > External RADIUS Servers.

Table A-43 External RADIUS Server Settings

Fields	Usage Guidelines
Name	Enter the name of the external RADIUS server.
Description	Enter a description of the external RADIUS server.
Host IP	Enter the IP address of the external RADIUS server.
Shared Secret	Enter the shared secret between Cisco ISE and the external RADIUS server that is used for authenticating the external RADIUS server. A shared secret is an expected string of text that a user must provide to enable the network device to authenticate a username and password. The connection is rejected until the user supplies the shared secret. The shared secret can be up to 128 characters in length.
Enable KeyWrap	Enable this option to increase the RADIUS protocol security via an AES KeyWrap algorithm, to help enable FIPS 140-2 compliance in Cisco ISE.
Key Encryption Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for session encryption (secrecy).
Message Authenticator Code Key	(Only if you check the Enable Key Wrap check box) Enter a key to be used for keyed HMAC calculation over RADIUS messages.
Key Input Format	Specify the format you want to use to enter the Cisco ISE FIPS encryption key, so that it matches the configuration that is available on the WLAN controller. (The value you specify must be the correct [full] length for the key as defined below—shorter values are not permitted.) • ASCII—The Key Encryption Key must be 16 characters (bytes) long, and the Message Authenticator Code Key must be 20 characters (bytes) long. • Hexadecimal—The Key Encryption Key must be 32 bytes long, and the Message Authenticator Code Key must be 40 bytes long.
Authentication Port	Enter the RADIUS authentication port number. The valid range is from 1 to 65535. The default is 1812.
Accounting Port	Enter the RADIUS accounting port number. The valid range is from 1 to 65535. The default is 1813.
Server Timeout	Enter the number of seconds that the Cisco ISE waits for a response from the external RADIUS server. The default is 5 seconds. Valid values are from 5 to 120.
Connection Attempts	Enter the number of times that the Cisco ISE attempts to connect to the external RADIUS server. The default is 3 attempts. Valid values are from 1 to 9.

RADIUS Server Sequences

The following table describes the fields on the RADIUS Server Sequences page, which you can use to create a RADIUS server sequence. The navigation path for this page is: Administration > Network Resources > RADIUS Server Sequences.

Table A-44 RADIUS Server Sequences

Fields	Usage Guidelines
Name	Enter the name of the RADIUS server sequence.
Description	Enter an optional description.

Table A-44 RADIUS Server Sequences (continued)

Fields	Usage Guidelines
Host IP	Enter the IP address of the external RADIUS server.
User Selected Service Type	Choose the external RADIUS servers that you want to use as policy servers from the Available list box and move them to the Selected list box.
Remote Accounting	Check this check box to enable accounting in the remote policy server.
Local Accounting	Check this check box to enable accounting in Cisco ISE.
Advanced Attribute Settings	
Strip Start of Subject Name up to the First Occurrence of the Separator	Check this check box to strip the username from the prefix. For example, if the subject name is acme\userA and the separator is \, the username becomes userA.
Strip End of Subject Name from the Last Occurrence of the Separator	Check this check box to strip the username from the suffix. For example, if the subject name is userA@abc.com and the separator is @, the username becomes userA. • You must enable the strip options to extract the username from NetBIOS or User Principle Name (UPN) format usernames (user@domain.com or /domain/user), because only usernames are passed to the RADIUS server for authenticating the user. • If you activate *both* the \ and @ stripping functions, and you are using Cisco AnyConnect, Cisco ISE does not accurately trim the first \ from the string. However, each stripping function that is used individually, however, works as it is designed with Cisco AnyConnect.
Modify Attributes in the Request to the External RADIUS Server	Check this check box to allow Cisco ISE to manipulate attributes that come from or go to the authenticated RADIUS server. The attribute manipulation operations include these: • **Add**—Add additional attributes to the overall RADIUS request/response. • **Update**—Change the attribute value (fixed or static) or substitute an attribute by another attribute value (dynamic). • **Remove**—Remove an attribute or an attribute-value pair. • **RemoveAny**—Remove any occurrences of the attribute.
Continue to Authorization Policy	Check this check box to divert the proxy flow to run the authorization policy for further decision making, based on identity store group and attribute retrieval. If you enable this option, attributes from the response of the external RADIUS server will be applicable for the authentication policy selection. Attributes that are already in the context will be updated with the appropriate value from the AAA server accept response attribute.
Modify Attributes before send an Access-Accept	Check this check box to modify the attribute just before sending a response back to the device.

NAC Manager Settings

The following table describes the fields on the New NAC Managers page, which you can use to add a NAC Manager. The navigation path for this page is: Administration > Network Resources > NAC Managers.

Table A-45 NAC Manager Settings

Fields	Usage Guidelines
Name	Enter the name of the Cisco Access Manager (CAM).
Status	Click the Status check box to enable REST API communication from the Cisco ISE profiler that authenticates connectivity to the CAM.
Description	Enter the description of the CAM.
IP Address	Enter the IP address of the CAM. Once you have created and saved a CAM in Cisco ISE, the IP address of the CAM cannot be edited. You cannot use 0.0.0.0 and 255.255.255.255, as they are excluded when validating the IP addresses of the CAMs in Cisco ISE, and so, they are not valid IP addresses that you can use in the IP Address field for the CAM. **Note** You can use the virtual service IP address that a pair of CAMs share in a high-availability configuration. This allows a failover support of CAMs in a high-availability configuration. For more information on how to set up a pair of CAMs for high availability, see the compatible link for Cisco NAC Appliance, Release 4.9. http://www.cisco.com/en/US/docs/security/nac/appliance/installation_guide/hardware/49/hi_ha.html#wp1084663.
Username	Enter the username of the CAM administrator that allows you to log on to the user interface of the CAM.
Password	Enter the password of the CAM administrator that allows you to log on to the user interface of the CAM.

Web Portal Management

Sponsor Group Policy Settings

The following table describes the fields on the Sponsor Group Policy page, which you can use to define sponsor group policies. The navigation path for this page is: Administration > Web Portal Management > Sponsor Group Policy.

You are not allowed to delete sponsor groups that are in use in a sponsor group policy

Table A-46 Sponsor Group Policy Settings

Fields	Usage Guidelines
Status	Choose to enable or disable the policy.
Policy Name	Enter a descriptive name for the new policy.
Identity Groups	Choose the identity group to associate with the defined sponsor group. For example, the default Manage All Accounts policy includes the SponsorAllAccount identity group.
Other Conditions	Choose or create additional conditions.
Sponsor Groups	Choose the sponsor group to which you want to apply these settings. For example, the default Manage All Accounts policy defines the sponsor group as SponsorAllAccounts.

Related Topics

- Sponsor Group Policies, page 16-6
- Creating a Sponsor Group Policy, page 16-6

Sponsor Group Settings

The following table describes the fields on the Guest Sponsor Group page, which you can use to define sponsor groups. The navigation path for this page is: Administration > Web Portal Management > Sponsor Groups. You are not allowed to delete sponsor groups that are in use in a sponsor group policy

Table A-47 Sponsor Group Settings

Fields	Usage Guidelines
General	
Name	Enter a name for the sponsor group. When choosing a name, you might want to consider which identity groups with which you will be associating the sponsor group. For example, the default sponsor groups have names similar to the default user identity groups to assist you in associating the correct identity group and sponsor group when creating the sponsor policies.
Description	Enter a description for the sponsor group.
Authorization Levels	
Allow Login	Indicate whether or not to allow sponsors to sign into the Sponsor portal.
Create Single Account	Indicate whether sponsors can create individual guest accounts.
Create Random Accounts	Indicate whether sponsors can create random guest accounts.
Import CSV	Indicate whether sponsors can import guest accounts.
Send Email	Indicate whether sponsors can email the account details to guest users.
Send SMS	Indicate whether sponsors to send text messages with the account details to guest users.
View Guest Password	Indicate whether sponsors can view guest passwords when creating accounts.
Allow Printing Guest Details	Indicate whether sponsors can print the account details for guest users.
View/Edit Accounts	Choose one of these settings: • No—Sponsors are not allowed to edit any guest accounts. • All Accounts—Sponsors are allowed to edit/view all guest accounts. • Group Accounts—Sponsors are allowed to edit guest accounts created by anyone in the same sponsor user group. • Own Account—Sponsors are allowed to edit only the guest accounts they created.

Table A-47 Sponsor Group Settings (continued)

Fields	Usage Guidelines
Suspend/Reinstate Accounts	Choose one of these settings: • No—Sponsors are not allowed to suspend any guest accounts. • All Accounts—Sponsors are allowed to suspend or reinstate all guest accounts. • Group Accounts—Sponsors are allowed to suspend guest accounts created by anyone in the same sponsor user group. • Own Account—Sponsors are allowed to suspend only the guest accounts they created.
Account Start Time	Restrict the number of days the sponsor can specify for starting the guest account. This is applicable only for the Start End type of time profile.
Maximum Duration of Account	Specify the maximum duration for which a guest account can be active. The expiration date is based on the maximum duration of the account or the time profile duration, whichever is minimum. This value overrides the maximum duration value set by the sponsor when creating a guest account when this value is less than the one specified in the time profile.
Guest Roles	
Guest Roles	Choose the guest roles that a sponsor in this group can use to assign different levels of access to a guest account. These roles are used in the authorization policies to associate guest user accounts to identity groups. Guest roles with a yellow icon indicate that they are an ActivatedGuest role.
Time Profiles	
Available Currently Selected	Choose any available default or custom time profiles: • DefaultEightHours—The guest user can login within eight hours of the account creation, after which the account expires. The account start time is equal to the user creation time, and the end time is eight hours from the start time. • DefaultFirstLoginEight—The account start time starts when the guest user first logs in to the guest portal, and the end time is eight hours later. • DefaultStartEnd—The sponsor can set the account start and end time.

Related Topics

- Sponsor Groups, page 16-5
- Creating Sponsor Groups, page 16-5

Web Portal Management Settings

These pages enable you to apply changes to all Cisco ISE web portals.

General Portal Theme Settings

The following table describes the fields on the Portal Theme Page, which you can use to determine the look and feel of all the Cisco ISE web portals. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Portal Theme.

Table A-48 General Portal Theme Settings

Fields	Usage Guidelines
Style Settings	
Login Page Logo	Upload a jpeg, gif, or png image file to use as the logo on the portal Login page for the Guest, Sponsor, and My Devices portals. When you upload the image, it is automatically resized to fit an image size of 86 pixels (width) by 46 pixels (height). To avoid distortion, resize your image to fit these dimensions.
Login Page Background Image	Change the background image on the portal login page for the Guest, Sponsor, and My Devices portals. Supported image formats include jpeg, gif, and png. The supported size image size is 533 pixels (width) by 314 pixels (height).
Banner Logo	Upload a jpeg, gif, or png image file to use as the banner logo on the Guest, Sponsor, and My Devices portals. When you upload the image, it is automatically resized to fit an image size of 86 pixels (width) by 45 pixels (height). To avoid distortion, resize your image to fit these dimensions.
Banner Background Image	Upload a jpeg, gif, or png image file to use as the background image for the Guest, Sponsor, or My Devices portals. Change the portal banner background image. The supported size image size is 1724 pixels (width) x 133 pixels (height), but the banner background color displays to fill the remaining area.
Login Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format to change the background color of the portal login page for the Guest, Sponsor, and My Devices portals. The logic background color displays only if the logic page background image is not set or is too small to fill the designated area.
Banner Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format to change the banner background color of the portal. The banner background color displays only if the banner background image is not set or is too small to fill the designated area.
Banner Text Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Banner Link Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Mobile Device Style Settings	
Logo Image	Upload a jpeg, gif, or png image file to use as the banner logo on the mobile-optimized Guest portal. The recommended image size is 100 pixels (width) x 61 pixels (height).

Table A-48 General Portal Theme Settings

Fields	Usage Guidelines
Banner Image	Upload a jpeg, gif, or png image file to use as the banner image on the mobile-optimized Guest portal. The recommended image size is 754 pixels (width) x 47 pixels (height), but it resizes appropriately when switching between portrait and landscape orientation on mobile devices.
Banner Background Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Banner Text Color	Enter the color value as a RGB (Red Green Blue) hexadecimal value in HTML color format.
Display Settings	
Display pre-login banner	Check to display messages to users before they log into the Sponsor, My Devices, or Guest portals. The pre-login banner displays on the login page for each portal.
Display post-login banner	Check to briefly display messages to users after they log into the Sponsor or My Devices portals. The post-login banner displays for 15 seconds on the Sponsor and My Devices portal and does not apply to the Guest portal.

Related Topics

- Customizing the Web Portal Images and Color Scheme, page 15-5
- Displaying Banner Messages to Users When Logging In or Out of Portals, page 15-6

Port Settings for Web Portals

The following table describes the fields on the Web Portal Settings page, which you can use to define ports and interfaces for the different Cisco ISE web portals. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Ports.

Table A-49 Port Settings for Web Portals

Fields	Usage Guidelines
Admin Portal Settings	
HTTP Port	The default value is 80, and you cannot change this setting.
HTTPS Port	The default value is 443, and you cannot change this setting.
Blacklist Portal Settings	
HTTPS Port	Enter the port value betwen 8000-8999; the default value is 8444. You cannot set this value to be the same as the Guest, Sponsor, or My Devices portals. If you upgraded to Cisco ISE 1.2 with port 8444 already assigned to another portal, the Blacklist portal will be set to an unused port in 8000 to 8999 range instead.

Table A-49 Port Settings for Web Portals (continued)

Fields	Usage Guidelines
Allowed Interfaces	Check to partition portal traffic to specific Gigabit Ethernet interfaces. You must configure the Ethernet interfaces using IP addresses on different subnets. Any portals assigned to the same HTTPS port also use the same Ethernet interfaces. For example, if you assign both the Sponsor and My Devices portals to port 8443, and you disable GigabitEthernet 0 on the Sponsor portal, that interface is also automatically disabled for the My Devices portal.
Guest Portal, Client Provisioning, My Devices, and Sponsor Portal Settings	
HTTPS Port	Enter the port value between 8000-8999; the default value is 8443. The port range restriction is new in Cisco ISE 1.2. If you upgraded with port values outside this range, they are honored until you make any change to this page. If you make any change to this page, you must update the port setting to comply with this restriction. For posture assessments and remediation only, the Client Provisioning portal uses ports 8905 and 8909. Otherwise, it uses the same ports assigned to the Guest portal.
Allowed Interfaces	Check to partition portal traffic to specific Gigabit Ethernet interfaces. You must configure the Ethernet interfaces using IP addresses on different subnets. Any portals assigned to the same HTTPS port also use the same Ethernet interfaces. For example, if you assign both the Sponsor and My Devices portals to port 8443, and you disable GigabitEthernet 0 on the Sponsor portal, that interface is also automatically disabled for the My Devices portal.
Portal FQDNs	
Default Sponsor Portal FQDN Default My Devices Portal FQDN	Check these options if you want to change the URLs from the default settings. You must enter a fully-qualified domain name (such as mydevices.yourcompany.com). The default settings are: • My Devices portal: https://*ip_address*:8443/mydevices/, where *ip_address* is the IP address of the Cisco ISE server. • Sponsor portal: https://*ip_address*:8443/sponsorportal/, where *ip_address* is the IP address of the Cisco ISE server. You must also update DNS to ensure the FQDN of the new URL resolves to a valid policy service node IP address. Additionally, to avoid certificate warning messages due to name mismatches, you should also include the FQDN of the customized URL in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE policy service node. This requires that you specify the SAN attribute outside of Cisco ISE, such as from the certificate authority (CA) server when submitting the Certificate Signing Request (CSR) or by using a utility like openssl to create a custom CSR.

Related Topics

- Specifying Ports and Ethernet Interfaces for End-User Portals, page 15-2
- Specifying the Fully Qualified Domain Name for Sponsor and My Devices Portals, page 15-3

Guest Purge Settings

The following table describes the fields on the Purge Settings page, which you can use to remove expired guest accounts. The navigation path for this page is: Administration > Web Portal Management > Settings > General > Purge.

Table A-50 Guest Purge Settings

Fields	Usage Guidelines
Enable purge settings for expired guest accounts	Check this option to schedule a purge of expired guest accounts.
Purge occurs every	Enter the purge interval from 1-365 days. Default setting is 15 days.
Hour of the day when the last purge should occur	Specify the hour of the day when the purge should occur. Default setting is at 23:00 hours.
Date of last purge	Displays the date of the most recent purge.
Date of next purge	Displays the date of the next scheduled purge.
Purge Now	Click to immediately purge the expired guest user records.

Related Topics

Purging Expired Guest Accounts, page 16-24

Sponsor Language Template Settings

The following table describes the fields on the Sponsor Language Template page, which you can use to customize the Sponsor Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > Sponsor > Language Template.

Keep these guidelines in mind when editing these fields:

- You should copy and rename a default template to a unique name before making modifications. This ensures that you have the original template to go back to in case of an error.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-51 Sponsor Portal Language Template Settings

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.
Configure Home Page	Customize the fields displayed on the main page in the Sponsor portal.
Configure Login Page	Customize the information displayed when users log into the Sponsor portal.
Configure Change Password	Customize the fields that display when sponsors change their passwords.

Table A-51 Sponsor Portal Language Template Settings (continued)

Fields	Usage Guidelines
Configure Common Table Headers	Specify the fields that appear as column headings in tables.
Configure Create Single Guest Account	Specify the fields that display when sponsors create a single guest account.
Configure Create Random Guest Accounts	Specify the fields that display when sponsors create random accounts.
Configure Import Guest Accounts	Specify the fields that display when sponsors import accounts.
Configure Bulk Create Status Display	Specify the fields that display when sponsors create multiple accounts.
Configure Print Tabular Display	Specify the fields that display when sponsors print account details.
Configure Sponsor Settings Customizations	Specify the fields that display in My Settings page in the Sponsor portal.
Configure Email Notification	Customize the fields and content of the e-mail that will be sent to guests with their account details.
Configure SMS Text Message Notification	Customize the fields and content of the SMS text message that will be sent to guests with their account details.
Configure Print Notification	Customize the fields and content of the message to be printed for guests with their account details.
Configure Date/Time Formats	Choose the format in which to display the date and time.
Configure Info/Error Messages	Customize the error messages display to users while using the Sponsor portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Popup Dialog Messages	Customize the information that displays to users while using the Sponsor portal.
Configure Common Items	Customize the fields common across the pages in the Sponsor portal.

My Devices Portal Language Template Settings

The following table describes the fields on the My Devices Language Template Page, which you can use to select a language and to customize the My Devices Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > My Devices > Language Template.

Keep these guidelines in mind when editing these fields:

- You should copy and rename a default template to a unique name before making modifications. This ensures that you have the original template to go back to in case of an error.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-52 My Devices Portal Language Template Settings

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.
Configure Login Page	Customize the information displayed when users log into the My Devices portal.
Configure Device Management Page	Customize the field names and labels for the options available to users when manage their devices. Users can enter only a maximum of 256 characters in the Page Description text box when they add devices.
Configure Acceptable Use Policy Page	Customize the acceptable use policy for your company, which appears on the login page and the device registration page of the My Devices portal.
Configure Info/Error Messages	Customize the error messages and information that display to users while using the My Devices portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Miscellaneous Items	Indicate the field names and labels for remaining UI elements.
Configure Blackhole Portal Items	Indicate portal name and error message that displays when a user attempts to access the My Devices portal using a blacklisted device.

Related Topics

Customizing the Portal Language, Text, and Error Messages, page 15-4

My Devices Portal Settings

The following table describes the fields on the My Devices Portal Settings page, which you can use to configure the My Devices Portal. The navigation path for this page is: **Administration > Web Portal Management > Settings > My Devices > Portal Configuration**.

Table A-53 My Devices Portal Settings

Fields	Usage Guidelines
Enable My Devices Portal	Check to allow employees to register and manage their devices using the My Devices portal.
Enable the Acceptable Use Policy link	Check to require an acceptable use policy for employees. You must also update the language template to reflect your company's policy.
The maximum number of devices to register	Enter the maximum number of devices that an employee can register. The default value is set to 5 devices.

Table A-53 My Devices Portal Settings (continued)

Fields	Usage Guidelines
Email Address	Customize the e-mail address associated with the Contact link on the login and main page of the My Devices Portal.
Phone Number	Customize the phone number associated with the Contact link on the login and main page of the My Devices Portal.

Related Topics

- Customizing the Portal Language, Text, and Error Messages, page 15-4

Guest Portal Language Template Settings

The following table describes the fields on the Guest Language Template page, which you can use to select a language for the Guest Portal and to customize it. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Language Template.

Keep these guidelines in mind when editing these fields:

- You should copy and rename a default template to a unique name before making modifications. This ensures that you have the original template to go back to in case of an error.
- You can only delete custom language templates. You are not allowed to delete any of the standard default language templates.

Table A-54 Guest Portal Language Template Settings

Fields	Usage Guidelines
Configure Template Definition	Enter a unique name and description and a valid locale to associate with the language. If you create a custom language template with a name that conflicts with a default template name, your template is automatically renamed after an upgrade and restore. After an upgrade and restore, default templates revert back to their default settings, and any templates with names that conflict with defaults are renamed as follows: user_{LANG_TEMP_NAME}.
Configure Login Page	Customize the information displayed when users log into the Guest portal.
Configure Acceptable Use Policy Page	Customize the acceptable use policy for your company, which appears on the login page and the device registration page of the Guest portal.
Configure Change Password	Customize the fields that display when guests change their passwords.
Configure Self Registration	Customize the fields that display when guests register independently.
Configure Device Registration	Customize the fields that display when guests register their devices.
Configure VLAN/Install Release	Customize the fields that display when forcing a VLAN reconfiguration.
Configure Error Messages	Customize the error messages displayed to users when using the Guest portal.
Configure JavaScript Enable Instructions	Customize the instructions for enabling JavaScript in supported web browsers.
Configure Popup Dialog Messages	Customize the information that displays to users while using the Guest portal.

Table A-54 Guest Portal Language Template Settings (continued)

Fields	Usage Guidelines
Configure Miscellaneous Items	Customize the field names and labels for remaining items.
Configure Self-Provisioning Portal (Registration)	Customize the registration page for the Self-Provisioning portal.
Configure Self-Provisioning Portal (Install)	Customize the installation page for the Self-Provisioning portal.
Configure Mobile Device Management (MDM)	Customize the field names for the MDM enrollment and compliance pages.

Related Topics

- Customizing Portal UI Fields and Error Messages, page 15-5
- Requiring an Acceptable Use Policy for Guests, page 16-19

Multi-Portal Configuration Settings

The following table describes the fields on the Multi-Portal Configurations page, which you can use to.

The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Multi-Portal Configurations.

Table A-55 Multi-Portal Configurations Settings

Fields	Usage Guidelines
General	
Name	Enter the name of the portal to use to access the portal. This name also will appear in the captive portal URL specified in the network access device (NAD) for wireless LAN controller (WLC) setups. For example, a portal with the name *ClientPortal* will have the following access URL: https://*ip address:port number*/guestportal/portals/ClientPortal/portal.jsp
Description	Enter an optional description.
Portal type	Choose a portal type: • Default Portal (Choose customization template and theme) • Device Web Authentication Portal (Choose customization template and theme), and then specify an Endpoint Identity Group • Custom Default Portal (Upload files) • Custom Device Web Authentication Portal (Upload files), and then specify an Endpoint Identity Group
EndPoint Identity Group	(Only for DRW portals) Choose an endpoint identity group. Cisco ISE provides the GuestEndpoints default identity group to use for the DRW portal.
Operations	

Table A-55 Multi-Portal Configurations Settings (continued)

Fields	Usage Guidelines
Acceptable use policy	Choose whether guests must accept an acceptable use policy to fully enable their account. If guests do not accept the policy, they will not obtain network access. Default setting for the DefaultGuestPortal is First Login. For new portals, the default is Not Used.
Enable Self-Provisioning Flow	Check to allow employees to directly connect their personal devices to the network. This option enables them to provision these devices using the native supplicant, which is available for Windows, Mac, iPhone, iPad, and Android devices. If you do not want to enable self-provisioning from the devices directly, you do not need to enable this feature. Employees can still add personal devices using the My Devices Portal. This feature requires an advanced license and is off by default when upgrading and on by default for new installations.
Enable Mobile Portal	Check to allow guests using mobile devices to access a mobile-optimized version of the Guest portal.
Allow guest users to change password	Check to allow guest users to change their password after the sponsor creates their initial account credentials. If guest users change their passwords, sponsors cannot provide guests with their login credentials if lost. The sponsor must create a new guest account.
Require guest users to change password at expiration and first login	Check to require guest users to change their password both at first login and after expiration. Sponsors cannot provide guests with their login credentials if lost. The sponsor must create a new guest account.
Guest users should download the posture client	Check to redirect the guest user to the Client Provisioning portal. Guests will be required to download a client provisioning agent for controlling posture before obtaining full network access. If you choose this option, the guest login flow performs a central web authorization (CWA), and the guest portal is redirected to the Client Provisioning portal after performing AUP and change password checks. In this case, the posture subsystem performs a CoA to the NAD to reauthenticate the client connection once the posture has been assessed. If you choose Vlan Dhcp Release, posture will perform the client side IP release and renew operation. Client Provisioning does not occur in Local Web Authentication scenarios.

Table A-55 Multi-Portal Configurations Settings (continued)

Fields	Usage Guidelines
Guest users should be allowed to do self service	Check to allow guest users to complete their personal information and create a new user account. When enabled, the Self Registration screen appears as a link on the guest user login page. User accounts are created with a random generated password. This password follows the password policy that is set for the guest users. To use this feature, you must also configure the default guest roles and time profiles in the Guest Portal Policy page.
Guest users should be allowed to do device registration	Check to allow guests to add devices to the network. When enabled, the Device Registration screen appears as a link on the guest user login page. You can configure the maximum number of devices per user from the Guest Portal Policy page. You can also add the device registration page for your custom portal. But, this page will only have the ability to add new devices. There will be no list of existing devices nor can you delete devices.
Vlan Dhcp Release	Check the VLAN DHCP Release option to refresh the IP address for Windows, Mac OS, Unix, or LINUX devices after a VLAN change in both wired or wireless environments for Guest with no posture. This affects the Central WebAuth (CWA) flow during final authorization when the network access changes the guest VLAN to a new VLAN. The guest's old IP address must be released before the VLAN change and a new guest IP must be requested through DHCP once the new VLAN access is in place. An applet downloads to perform the IP release renew operation. The VLAN DHCP Release option does not work on mobile devices. Instead, guests must manually reset the IP address. This method varies by devices. For example, on Apple iOS devices, users can select the Wi-Fi network and click the **Renew Lease** button.
Delay to Release	Enter the delay to release time. Enter a brief time because it must occur immediately after the applet is downloaded and before the Cisco ISE server directs the NAD to re-authenticate with a CoA request. The default release value is 1 second.
Delay to COA	Enter the time to delay Cisco ISE from executing the CoA. Enough time should be given to allow the applet to download and perform the IP release on the client. The default value is 8 seconds.\
Delay to Renew	Enter the delay to renew value. This time is added to the IP release value and does not begin timing until the control is downloaded. The renew should be given enough time so that the CoA is allowed to process and the new VLAN access granted. The default value is 12 seconds.
Customization	
Language template	Choose the display language to use for the Guest portal. You cannot change this setting if the User browser locale option is checked.
Use browser locale	Check this option to allow the Guest portal to use the browser locale as the display language.

Table A-55 Multi-Portal Configurations Settings (continued)

Fields	Usage Guidelines
Authentication	
Identity Store Sequence	Specify the identity store sequence to apply for the guest flow. This sequence defines the order in which Cisco ISE will look for user credentials in the different databases. You can use one of the default sequences or first define a new one to use from **Identity Management > Identity Source Sequences**.
File Uploads (Available only when creating a custom portal)	
Upload File	Upload the HTML files you have created for the Login, AUP, Change Password, and Self Registration pages. These pages can include images and other links to the upload files. All uploaded files are held in a single directory with no subdirectories. Add "portals/<*portalname*>" to indicate the path to the files in the HTML code. You cannot run any back end scripts in the Cisco ISE server. Only HTML, HTM, JPEG, GIF, PNG, and CSS files are allowed.
Delete File	Select the uploaded files you want to delete.
File Mapping	
Login file	Indicate the uploaded HTML files to associate with each guest page. Based on the selections you made on the General tab, some fields might be grayed out. Required files are based on the selections made in the General tab. To ensure that the guest flow redirects and displays the appropriate portal pages, you must be sure to associate all required files.
AUP file	
Change Password file	
Self Registration file	
Self Registration Results file	
Device Registration file	
Guest Success file	
Error Page file	

Guest Portal Policy Settings

The following table describes the fields on the Guest Portal Policy page, which you can use to configure the Guest Portal. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Portal Policy.

Table A-56 Guest Portal Policy Settings

Fields	Usage Guidelines
Self-Registration	
Guest Role	Choose the default guest role to assign to the guest user after self-registration. This role associates the guest user to an identity group based on the policies defined in the system. Guest roles with a yellow icon indicate that they are an ActivatedGuest role.
Time Profile	Choose the default time profile to assign to the guest user after self-registration.
Login Restrictions	

Table A-56 Guest Portal Policy Settings (continued)

Fields	Usage Guidelines
Allow only one guest session per user	Check to restrict guest users to connecting to the network with only one device at a time. If a guest user attempts to connect another device, the currently-connected device is disconnected from the network.
Maximum Login Failures	Enter the maximum number of failed logins that can occur before a guest account is suspended. The default value is five.
Device Registration Portal Limit	Enter the maximum number of devices that can be registered for each guest. The device registration portal will not allow the guest user to add more devices if the maximum number has been reached. You can limit this setting below the maximum number of devices currently registered to a guest account, but this change will not affect the existing registered devices.
Guest Password Expiration (Days)	Enter the number of days after which the guest password will expire and the guest will have to reset their password. You must also require guests to change their passwords at expiration from: Administration > Web Portal Management > Settings > Guest > Multi-Portal Configuration > Operations.

Guest Time Profile Settings

The following table describes the fields on the Guest Time Profiles page, which you can use to create new time profiles to specify how long guests' have network access. These changes are global and affect all Guest portals. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Time Profiles.

Table A-57 Guest Time Profile Settings

Fields	Usage Guidelines
Name	Enter a name for the time profile using alphanumeric characters only; do not include spaces or any special characters. Keep this name brief yet descriptive enough for sponsors to be able to interpret it when creating guest accounts.
Description	Enter an optional description.
Time Zone for Restrictions	Choose a time zone to be used for the time restrictions.
Account Type	Choose one of these options: • FromCreation—The guest user can login within the specified duration time from the account creation, after which the account expires. • FromFirstLogin—The account start time starts when the guest user first logs in to the guest portal, and the end time equals the specified duration time. If the guest user never logs in, the account remains in the Awaiting first login state and never expires. • StartEnd—The sponsor can set the account start and end time.

Table A-57 Guest Time Profile Settings (continued)

Fields	Usage Guidelines
Duration	Enter the time for which the account will be active. The account expires after the duration set here has expired. This option is available only if you select the Account Type as FromCreation or FromFirstLogin.
Restrictions	Enter the day of the week and a start and end clock time. The Time Zone for Restrictions value affects these time settings. For example, a time restriction that specifies Monday 12:00 am to 8:00 am and Monday 6:00 pm to 11:59 pm would only grant system access between 8:00 am and 6:00 pm on Mondays within the time zone of the time profile. Any other day of the week would have no time restriction. The time profile can have restrictions that fall outside the start and end time specified in a Guest account during creation. Only those restrictions that cover the start end time of the account will be applied to the account. For a wired network the Termination-Action must be set to 0 “Default” so that the Session-Timeout is treated as a terminate session. This value must be set on the Authorization Profile as a RADIUS value. For a WLC the Allow AAA Override must be turned on in the WLAN configuration. The RADIUS access-accept will contain a Session-Timeout value in seconds, remaining for the account. When this time has elapsed, NAD will close the connection. At the time of Guest login the Network Access system will return the remaining time left in the guest account to the NAD that is making the access request. This is so that the NAD can enforce account expiration. For the DefaultEightHours and DefaultFirstLoginEight time profiles, the expiration date will be calculated based on the sponsor group duration or time profile duration, whichever is the minimum.

Guest Username Policy Settings

The following table describes the fields on the Guest Username Policy page, which you use to specify requirements and guidelines for guest usernames. These changes are global and affect all Guest portals. The navigation path for this page is: Administration > Web Portal Management > Settings > Guest > Username Policy.

Table A-58 Guest Username Policy Settings

Fields	Usage Guidelines
General	
Create username from email address	Select this option if you want the guest username to be formed from the guest’s e-mail address.
Create username from first name and last name	Select this option if you want the guest username to be formed from the first initial of the first name combined with the last name of the guest user.

Table A-58 Guest Username Policy Settings (continued)

Fields	Usage Guidelines
Minimum Username Length	Enter the minimum number of characters required for usernames. If the guest usernames formed by the e-mail address or by the combination of first and last name are shorter than the minimum length, the username will be appended with *0* (zero) characters and a *1* at the end. If the username is not unique, numeric characters are appended to the name to make it unique. For example, if there are two guest users named *Firstname Lastname,* the first username would be *flastname* and the second username would be *flastname1*. Similarly, if the Minimum Username length is set to eleven, then the two usernames would be generated as *flastname01* and *flastname02.*
Random	
Username may include the alphabetic characters	Enter all allowable uppercase and lowercase letters from A-Z.
Minimum number to include	Enter the minimum number of required alphabetic characters. Random username length is determined by combining this value with that of the numeric and special character minimum values. The length of the username defines the total number of unique names that can be created. For example, if you need to create 10,000 users, you cannot create enough unique values with usernames of only two characters in length.
Username may include the numeric characters	Enter all allowable numeric characters from 0-9.
Minimum number to include	Enter the minimum number of required numeric characters. Random username length is determined by combining this value with that of the alphabetic and special character minimum values.
Username may include the special characters	Enter any of the following special characters: $ ( ) < > ~ ` / * - _ @
Minimum number to include	Enter the minimum number of required special characters. Random username length is determined by combining this value with that of the alphabetic and numeric character minimum values.