Administration User Interface Reference

System Administration

Deployment Settings

The Deployment Nodes page enables you to configure Cisco ISE (Administration, Policy Service, and Monitoring) nodes and Inline Posture nodes and to set up a deployment.

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**.

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 (Administration, Policy Service, and Monitoring) nodes • Inline Posture node
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.

Fields	Usage Guidelines
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 the Primary Administration Node (PAN) • SEC(A)—Refers to the Secondary Administration Node • PRI(M)—Refers to the Primary Monitoring Node • SEC(M)—Refers to the 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 PAN. • 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 PAN or you have performed a manual sync operation or the ISE node is not in sync (out of sync) with the PAN. 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**.

Table 1: 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.

Fields	Usage Guidelines
Node Type	Displays the node type. Could be any one of the following: Identity Services Engine (ISE), Inline Posture Node
Personas	
Administration	Check this check box if you want a Cisco ISE node to assume the Administration persona. You can enable the Administration persona only on nodes that are licensed to provide the administrative services. 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.
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 PAN, you must enable the Monitoring persona. After you register a secondary Monitoring node in your deployment, you can edit the PAN and disable the Monitoring persona, if required. 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

Fields	Usage Guidelines
Policy Service	Check this check box to enable any one or all of the following services: • Enable Session Services—Check this 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. All the nodes within the same node group should be configured on the network access device (NAD) as RADIUS clients and authorized for CoA, because any one of them can issue a CoA request for the sessions that are established through any node in the node group. If you are not using a load balancer, the nodes in a node group should be the same as, or a subset of the RADIUS servers and clients configured on the NAD. These nodes would also be configured as RADIUS servers. While a single NAD can be configured with many ISE nodes as RADIUS servers and dynamic-authorization clients, it is not necessary for all the nodes to be in the same node group. The members of a node group should be connected to each other using high-speed LAN connection such as Gigabit Ethernet. The node group members need not be L2 adjacent, but L2 adjacency is highly recommended to ensure sufficient bandwidth and reachability. See Create a Policy Service Node Group section for more details. • Enable Profiling Service—Check this 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. 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.
pxGrid	Check this check box to enable the pxGrid services. Cisco pxGrid is used to share the context-sensitive information from Cisco ISE session directory to other policy network systems such as Cisco Adaptive Security Appliance (ASA). The pxGrid framework can also be used to exchange policy and configuration data between nodes like sharing tags and policy objects between ISE and third party vendors, and for non-ISE related information exchanges such as threat information.

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 2: 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:Port—Enter the DHCP server UDP port number. The default port is 67. • 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.
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 box to enable the NMAP probe. You can also do a manual scan of a subnet in this panel.
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.

Fields	Usage Guidelines
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 3: 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	

Fields	Usage Guidelines
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. For security reasons, we recommend that you always include the IP address along with the MAC address in a MAC filter entry. Do not configure the MAC address in a MAC filter for a directly connected ASA VPN device without also entering the IP address. Without the addition of the optional IP address, VPN clients are allowed to bypass policy enforcement. This bypass happens because the VPN is a Layer 3 hop for clients, and the device uses its own MAC address as the source address to send packets along the network toward the Inline Posture node.
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	
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. The timeout and retry values should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: (IPN 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 IPN server (5*1=5) is lesser than the value configured on the client (5*3=15)

Fields	Usage Guidelines
Secondary Server	Enter the IP address, shared secret, timeout in seconds, and number of retries for the secondary RADIUS server. The timeout and retry values should be based on the timeout and retries that you define on the client such as WLC or ASA. We recommend the following: (IPN 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 IPN server (5*1=5) is lesser than the value configured on the client (5*3=15)
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.
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.	

Fields	Usage Guidelines
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. ◦ 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.
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.

Fields	Usage Guidelines
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.

Certificate Store Settings

The Certificate Store page enables you to configure certificates in Cisco ISE that can be used for authentication.

Endpoint Certificate Overview Page

The following table describes the fields on the Certificate Management Overview page. The PSN nodes in your deployment issue certificates to endpoints. This page provides you information about the endpoint certificates issued by each of the PSN nodes in your deployment. The navigation path for this page is: Administration > System > Certificates > Overview.

Fields	Usage Guidelines
Node Name	Name of the Policy Service node (PSN) that issued the certificate.
Endpoint Certificates Issued	Number of endpoint certificates issued by the PSN node.
Endpoint Certificates Revoked	Number of revoked endpoint certificates (certificates that were issued by the PSN node).
Endpoint Certificates Requests	Number of certificate-based authentication requests processed by the PSN node.
Endpoint Certificates Failed	Number of failed authentication requests processed by the PSN node.

Self-Signed Certificate Settings

The following table describes the fields in the Generate Self Signed Certificate page. This page allows you to create system certificates for inter-node communication, EAP-TLS authentication, Cisco ISE web portals, and to communicate with the pxGrid controller. The navigation path for this page is: Administration > System > Certificates > System Certificates > Generate Self Signed Certificate.

Fields	Usage Guidelines
Select Node	(Required) The node for which you want to generate the system certificate.
Common Name (CN)	(Required if you do not specify a SAN) By default, the common name is the Fully Qualified Domain Name of the ISE node for which you are generating the self-signed certificate.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	An IP address or DNS name that is associated with the certificate.
Key Length	Choose 2048 if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.
Digest to Sign With	Choose one of the following hashing algorithm: SHA-1 or SHA-256.
Expiration TTL	Specify the number of days after which the certificate will expire.
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.
Allow Wildcard Certificates	Check this check box if you want to generate a self-signed wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com.

Fields	Usage Guidelines
Usage	Choose the service for which this system certificate should be used: • Admin—Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment • EAP Authentication—Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling • pxGrid—Client and server certificate to secure communication between the pxGrid client and server • Portal—Server certificate used to secure communication with all Cisco ISE web portals

Certificate Signing Request Settings

Cisco ISE allows you to generate CSRs for all the nodes in your deployment from the Admin portal in a single request. Also, you can choose to generate the CSR for a single node or multiple nodes in the deployment. If you choose to generate a CSR for a single node, ISE automatically substitutes the Fully Qualified Domain Name (FQDN) of the particular node in the CN= field of the certificate subject. If you choose to include an entry in the Subject Alternative Name (SAN) field of the certificate, you must enter the FQDN of the ISE node in addition to other SAN attributes. If you choose to generate CSRs for all the nodes in your deployment, check the Allow Wildcard Certificates check box and enter the wildcard FQDN notation in the SAN field (DNS name), for example, *.amer.example.com. If you plan to use the certificate for EAP Authentication, do not enter the wildcard value in the CN= field.

With the use of wildcard certificates, you no longer have to generate a unique certificate for each Cisco ISE node. Also, you no longer have to populate the SAN field with multiple FQDN values to prevent certificate warnings. Using an asterisk (*) in the SAN field allows you to share a single certificate across multiple nodes in a deployment and helps prevent certificate name mismatch warnings. However, use of wildcard certificates is considered less secure than assigning a unique server certificate for each Cisco ISE node.

The following table describes the fields in the Certificate Signing Request (CSR) page, which you can use to generate a CSR that can be signed by a Certificate Authority (CA). The navigation path for this page is: **Administration** > **System** > **Certificates** > **Certificate Management** > **Certificate Signing Request**.

Field	Usage Guidelines
Certificate(s) will be used for	

Field	Usage Guidelines
	Choose the service for which you are going to use the certificate: **Cisco ISE Identity Certificates** • Multi-Use—Used for multiple services (Admin, EAP-TLS Authentication, pxGrid, and Portal). Multi-use certificates use both client and server key usages. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: ◦ Key Usage: Digital Signature (Signing) ◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) • Admin—Used for server authentication (to secure communication with the Admin portal and between ISE nodes in a deployment). The certificate template on the signing CA is often called a Web Server certificate template. This template has the following properties: ◦ Key Usage: Digital Signature (Signing) ◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) • EAP Authentication—Used for server authentication. The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: ◦ Key Usage: Digital Signature (Signing) ◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) • Portal—Used for server authentication (to secure communication with all ISE web portals). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: ◦ Key Usage: Digital Signature (Signing) ◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) • pxGrid—Used for both client and server authentication (to secure communication between the pxGrid client and server). The certificate template on the signing CA is often called a Computer or Machine certificate template. This template has the following properties: ◦ Key Usage: Digital Signature (Signing) ◦ Extended Key Usage: TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS Web Client Authentication (1.3.6.1.5.5.7.3.2) **Cisco ISE Certificate Authority Certificates** • ISE Root CA—(Applicable only for the internal CA service) Used for regenerating the entire internal CA certificate chain including the root CA on

Field	Usage Guidelines
	the PAN and subordinate CAs on the PSNs. • ISE Intermediate CA—(Applicable only for the internal CA service when ISE acts as an intermediate CA of an external PKI) Used to generate an intermediate CA certificate on the PAN and subordinate CA certificates on the PSNs. The certificate template on the signing CA is often called a Subordinate Certificate Authority. This template has the following properties: ◦ Basic Constraints: Critical, Is a Certificate Authority ◦ Key Usage: Certificate Signing, Digital Signature ◦ Extended Key Usage: OCSP Signing (1.3.6.1.5.5.7.3.9) • Renew ISE OCSP Responder Certificates—(Applicable only for the internal CA service) Used to renew the ISE OCSP responder certificate for the entire deployment (and is not a certificate signing request). For security reasons, we recommend that you renew the ISE OCSP responder certificates every six months.
Allow Wildcard Certificates	Check this check box to use a wildcard character (*) in the CN and/or the DNS name in the SAN field of the certificate. If you check this check box, all the nodes in the deployment are selected automatically. You must use the asterisk (*) wildcard character in the left-most label position. If you use wildcard certificates, we recommend that you partition your domain space for greater security. For example, instead of *.example.com, you can partition it as *.amer.example.com. If you do not partition your domain, it can lead to security issues.
Generate CSRs for these Nodes	Check the check boxes next to the nodes for which you want to generate the certificate. To generate a CSR for select nodes in the deployment, you must uncheck the Allow Wildcard Certificates option.
Common Name (CN)	By default, the common name is the FQDN of the ISE node for which you are generating the CSR. $FQDN$ denotes the FQDN of the ISE node. When you generate CSRs for multiple nodes in the deployment, the Common Name field in the CSRs is replaced with the FQDN of the respective ISE nodes.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.

Field	Usage Guidelines
Subject Alternative Name (SAN)	Available options for SAN include: • DNS Name—If you choose the DNS name, enter the fully qualified domain name of the ISE node. If you have enabled the Allow Wildcard Certificates option, specify the wildcard notation (an asterisk and a period before the domain name). For example, *.amer.example.com. • IP Address—IP address of the ISE node to be associated with the certificate. An IP address or DNS name that is associated with the certificate.
Key Length	Choose 2048 or greater if you plan to get a public CA-signed certificate or deploy Cisco ISE as a FIPS-compliant policy management system.
Digest to Sign With	Choose one of the following hashing algorithm: SHA-1 or SHA-256.

System Certificate Import Settings

The following table describes the fields in the Import System Certificate page that you can use to import a server certificate. The navigation path for this page is: Administration > System > Certificates > System Certificates > Import.

Fields	Description
Select Node	(Required) Choose the Cisco ISE node on which you want to import the system certificate.
Certificate File	(Required) Click **Browse** to select the certificate file from your local system.
Private Key File	(Required) Click **Browse** to select the private key file.
Password	(Required) Enter the password to decrypt the private key file.
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.
Allow Wildcard Certificates	Check this check box if you want to import a wildcard certificate (a certificate that contains an asterisk (*) in any Common Name in the Subject and/or the DNS name in the Subject Alternative Name. For example, DNS name assigned to the SAN can be *.amer.cisco.com. If you check this check box, Cisco ISE imports this certificate to all the other nodes in the deployment.

Fields	Description
Enable Validation of Certificate	Check this check box if you want Cisco ISE to validate the certificate extensions. If you check this check box and the certificate that you are importing contains a basic constraints extension with the CA flag set to true, ensure that the key usage extension is present, and that the keyEncipherment bit or the keyAgreement bit, or both, are also set.
Usage	Choose the service for which this system certificate should be used: • Admin—Server certificate used to secure communication with the Admin portal and between ISE nodes in a deployment • EAP Authentication—Server certificate used for authentications that use the EAP protocol for SSL/TLS tunneling • pxGrid—Client and server certificate to secure communication between the pxGrid client and server • Portal—Server certificate used to secure communication with all Cisco ISE web portals

Trusted Certificate Store Page

The following table describes the fields on the Trusted Certificates 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 > Trusted Certificates.

Table 4: Certificate Store Page

Fields	Usage Guidelines
Friendly Name	Displays the name of the certificate.
Status	Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Trusted for	Displays the service for which the certificate is used.
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 Date	The “Not After” certificate attribute.

Fields	Usage Guidelines
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

Trusted Certificate 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 5: Certificate Store Edit Settings

Fields	Usage Guidelines
Certificate Issuer	
Friendly Name	Enter a friendly name for the certificate.
Status	Choose Enabled or Disabled. If Disabled, ISE will not use the certificate for establishing trust.
Description	Enter an optional description.
Usage	
Trust for authentication within ISE	Check the check box if you want this certificate to verify server certificates (from other ISE nodes or LDAP servers).
Trust for client authentication and Syslog	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to ISE using the EAP protocol • Trust a Syslog server
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.

Fields	Usage Guidelines
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.
Reject the request if OCSP returns UNKNOWN status	Check the check box to reject the request if certificate status is not 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.
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.

Trusted Certificate Import Settings

The following table describes the fields on the Trusted Certificate 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 > Trusted Certificates > Import.

Table 6: Trusted Certificate 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.
Trust for authentication within ISE	Check the check box if you want this certificate to be used to verify server certificates (from other ISE nodes or LDAP servers).
Trust for client authentication and Syslog	(Applicable only if you check the Trust for authentication within ISE check box) Check the check box if you want this certificate to be used to: • Authenticate endpoints that connect to ISE using the EAP protocol • Trust a Syslog server
Trust for authentication of Cisco Services	Check this check box if you want this certificate to be used to trust external Cisco services such as the feed service.
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.

OCSP Client Profile Settings

The following table describes the fields on the OCSP Client Profile page, which you can use to configure OCSP client profiles. The navigation path for this page is **Administration** > **Certificates** > **Certificate Management** > **OCSP Profile**.

Field	Usage Guidelines
Name	Name of the OCSP Client Profile.

Field	Usage Guidelines
Description	Enter an optional description.
Enable Secondary Server	Check this check box to enable a secondary OCSP server for high availability.
Always Access Primary Server First	Use this option to check the primary server before trying to move to the secondary server. Even if the primary was checked earlier and found to be unresponsive, Cisco ISE will try to send a request to the primary server before moving to the secondary server.
Fallback to Primary Server After Interval *n* Minutes	Use this option when you want Cisco ISE to move to the secondary server and then fall back to the primary server again. In this case, all other requests are skipped, and the secondary server is used for the amount of time that is configured in the text box. The allowed time range is 1 to 999 minutes.
URL	Enter the URL of the primary and/or secondary OCSP server.
Enable Nonce Extension Support	You can configure a nonce to be sent as part of the OCSP request. The Nonce includes a pseudo-random number in the OCSP request. It is verified that the number that is received in the response is the same as the number that is included in the request. This option ensures that old communications cannot be reused in replay attacks.
Validate Response Signature	The OCSP responder signs the response with one of the following certificates: • The CA certificate • A certificate different from the CA certificate In order for Cisco ISE to validate the response signature, the OCSP responder needs to send the response along with the certificate, otherwise the response verification fails, and the status of the certificate cannot be relied on. According to the RFC, OCSP can sign the response using different certificates. This is true as long as OCSP sends the certificate that signed the response for Cisco ISE to validate it. If OCSP signs the response with a different certificate that is not configured in Cisco ISE, the response verification will fail.

Field	Usage Guidelines
Cache Entry Time To Live *n* Minutes	Enter the time in minutes after which the cache entry expires. Each response from the OCSP server holds a nextUpdate value. This value shows when the status of the certificate will be updated next on the server. When the OCSP response is cached, the two values (one from the configuration and another from response) are compared, and the response is cached for the period of time that is the lowest value of these two. If the nextUpdate value is 0, the response is not cached at all. Cisco ISE will cache OCSP responses for the configured time. The cache is not replicated or persistent, so when Cisco ISE restarts, the cache is cleared. The OCSP cache is used in order to maintain the OCSP responses and for the following reasons: • To reduce network traffic and load from the OCSP servers on an already-known certificate • To increase the performance of Cisco ISE by caching already-known certificate statuses
Clear Cache	Click **Clear Cache** to clear entries of all the certificate authorities that are connected to the OCSP service. In a deployment, **Clear Cache** interacts with all the nodes and performs the operation. This mechanism updates every node in the deployment.

Internal CA Settings

The following table describes the fields in the internal CA settings page. You can view the internal CA settings and disable the internal CA service from this page. The navigation path for this page is: Administration > System > Certificates > Internal CA Settings.

Fields	Usage Guidelines
Disable Certificate Authority	Click this button to disable the internal CA service.
Host Name	Host name of the Cisco ISE node that is running the CA service.
Personas	Cisco ISE node personas that are enabled on the node running the CA service. For example, Administration, Policy Service, etc.
Role(s)	The role(s) assumed by the Cisco ISE node running the CA service. For example, Standalone or Primary or Secondary.
CA & OCSP Responder Status	Enabled or disabled

Fields	Usage Guidelines
OCSP Responder URL	URL for Cisco ISE node to access the OCSP server.

Certificate Template Settings

The following table describes the fields in the CA Certificate Template page, which you can use to define a SCEP RA profile that will be used by the client provisioning policy. The navigation path for this page is: Administration > System > Certificates > Certificate Templates > Add.

Note We do not support UTF-8 characters in the certificate template fields (Organizational Unit, Organization, City, State, and Country). Certificate provisioning fails if UTF-8 characters are used in the certificate template.

Fields	Usage Guidelines
Name	(Required) Enter a name for the certificate template. For example, Internal_CA_Template.
Description	(Optional) Enter a description.
Common Name (CN)	(Display only) Common name is autopopulated with the username.
Organizational Unit (OU)	Organizational Unit name. For example, Engineering.
Organization (O)	Organization name. For example, Cisco.
City (L)	(Do not abbreviate) City name. For example, San Jose.
State (ST)	(Do not abbreviate) State name. For example, California.
Country (C)	Country name. You must enter the two-letter ISO country code. For example, US.
Subject Alternative Name (SAN)	(Display only) MAC address of the endpoint.
Key Size	Specify a key size of 1024 or higher.
SCEP RA Profile	Choose the ISE Internal CA or an external SCEP RA profile that you have created.
Valid Period	Enter the number of days after which the certificate expires.

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 7: 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.
Maximum Length	Enter the maximum length of the remote log target messages. Valid options are from 200 to 1024 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.

Fields	Usage Guidelines
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.

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 8: 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.

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 9: 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.
Path	Enter the path to your repository. The path must be valid and must exist at the time you create the repository. This value can start with two forward slashes (//) or a single forward slash (/) denoting the root directory of the server. However, for the FTP protocol, a single forward slash (/) denotes the FTP user's home directory and not the root directory.
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 =.

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 10: 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.

Fields	Usage Guidelines
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.

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 11: 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.

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** > **Password Policy**.

Table 12: 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.
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. Enter the number of days before which you cannot reuse a 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.

Fields	Usage Guidelines
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 13: 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.**

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 14: 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.

Fields	Usage Guidelines
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 Lease	
Perform posture assessment every time a user connects to the network	Select this option to initiate posture assessment every time the user connects to network
Perform posture assessment every *n* days	Select this option to initiate posture assessment after the specified number of days although the client is already postured Compliant.

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 15: 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.

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 16: 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.
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.

Fields	Usage Guidelines
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 17: 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.
Revoke all master keys and PACs	Click Revoke to revoke all master keys and PACs.

Fields	Usage Guidelines
Enable PAC-less Session Resume	Check this check box if you want to use EAP-FAST without the PAC files.
PAC-less Session Timeout	Specifies the time in seconds after which the PAC-less session resume times out. The default is 7200 seconds.

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 18: 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.
Trustsec PAC	Click this radio button to generate a Trustsec 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 a Trustsec PAC, the Identity field specifies the Device ID of a Trustsec 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.
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 Trustsec 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.
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 Trustsec PAC only) The expiration date is calculated based on the PAC Time to Live.

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 19: 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.

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 20: 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.
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.

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**.

When you enable anomalous client suppression and an endpoint authentication fails twice within the configured detection interval, Cisco ISE marks the supplicant as misconfigured and suppresses additional failed authentications with the same failure reason. You can find more details about the suppression by clicking the Misconfigured Supplicant Counter link on the Live Authentications page. A successful authentication from a suppressed endpoint clears the suppression, and results in a decrease in the Misconfigured Supplicant Counter value on the Live Authentications page. Also, if there is no authentication activity from the suppressed endpoint for a period of six hours, the suppression is cleared automatically.

Cisco ISE allows you to enable strong suppression by enabling the Reject Requests After Detection option. If you check the Reject Requests After Detection check box, and an endpoint authentication fails five times with the same failure reason, Cisco ISE activates strong suppression. All subsequent authentications, whether successful or not, are suppressed, and authentication does not occur. This “strong” suppression is cleared after the configured Request Rejection Interval elapses or after six hours of authentication inactivity from the endpoint.

Table 21: 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 from a client that is identified as anomalous or misconfigured. The requests from anomalous clients will be rejected during the Request Rejection Interval.
Request Rejection Interval	Enter the time interval in minutes for which the requests are to be rejected. This option is available only when you have checked Reject Requests After Detection check box.
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.

TrustSec Settings

For Cisco ISE to function as a TrustSec server and provide TrustSec services, you must define the global TrustSec settings. The following table describes the fields on the TrustSec Settings page. The navigation path for this page is: **Administration** > **System** > **Settings** > **TrustSec Settings**.

Table 22: Configuring TrustSec 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 following are the valid ranges: • 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 server initiates the tunnel PAC update if the first successful authentication happens before the PAC expiration. This mechanism allows the client to be always updated with a valid PAC. The default value is 10%.

SMS Gateway Settings

The navigation path for these settings is **Guest Access** > **Settings** > **SMS Gateway**.
Use these settings to configure sending SMS messages to guests and sponsors via an email server.

Table 23: SMS Gateway Settings for SMS Email Gateway

Field	Usage Guidelines
SMS Gateway Provider Domain	Enter the provider domain, which is used as the host portion and the guest account's mobile number as the user portion of the email address to send the message to the provider's SMS/MMS gateway.
Provider account address	(Optional) Enter the account address, which is used as the FROM address (typically the account address) for the email and overrides the **Default Email Address** global setting in **Guest Access** > **Settings**.

Field	Usage Guidelines
SMTP API destination address	(Optional) Enter the SMTP API Destination Address, if you are using an SMTP SMS API that requires a specific account recipient address, such as Clickatell SMTP API. This is used as the TO address for the email and the guest account's mobile number is substituted into the message's body template.
SMTP API body template	(Optional) Enter the SMTP API Body Template, if you are using an SMTP SMS API that requires a specific email body template for sending the SMS, such as Clicketell SMTP API. The supported dynamic substitutions are $mobilenumber$ and $message$.

The navigation path for these settings is **Guest Access** > **Settings** > **SMS Gateway**.
Use these settings to configure sending SMS messages to guests and sponsors via an HTTP API (GET or POST method).

Table 24: SMS Gateway Settings for SMS HTTP API

Field	Usage Guidelines
URL	Enter the URL for the API. This field is not URL encoded. The guest account's mobile number is substituted into the URL. The supported dynamic substitutions are $mobilenumber$ and $message$. If you are using HTTPS with the HTTP API, include HTTPS in the URL string and upload your provider's trusted certificates into Cisco ISE. Choose **Administration** > **System** > **Certificates** > **Trusted Certificates**.
Data (Url encoded portion)	Enter the Data (Url encoded portion) for the GET or POST request. This field is URL encoded. If using the default GET method, the data is appended to the URL specified above.

Field	Usage Guidelines
Use HTTP POST method for data portion	If using the POST method, check this option. The data specified above is used as the content of the POST request.
HTTP POST data content type	If using the POST method, specify the content type such as "plain/text" or "application/xml".
HTTPS Username HTTPS Password HTTPS Host name HTTPS Port number	Enter this information.

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 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.

Fields	Usage Guidelines
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 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.

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 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.

Fields	Usage Guidelines
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 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.

Fields	Usage Guidelines
Schema	You can choose any one of the following built-in schema types or create a custom schema: • Active Directory • Sun Directory Server • Novell eDirectory You can click the arrow next to Schema to view the schema details. If you edit the attributes of the predefined schema, Cisco ISE automatically creates a Custom schema.
Note The following fields can be edited 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.
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 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.
LDAP Server Root CA	Choose a trusted root certificate authority from the drop-down list to enable secure authentication with a certificate.
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 99. The default is 10.

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.
Failover	
Always Access Primary Server First	Click this option if you want Cisco ISE to always access the primary LDAP server first for authentications and authorizations.
Failback to Primary Server After	If the primary LDAP server that Cisco ISE attempts to contact cannot be reached, Cisco ISE attempts to contact the secondary LDAP server. If you want Cisco ISE to use the primary LDAP server again, click this option and enter a value in the text box.

LDAP Directory Organization Settings

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

Table 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.

Fields	Usage Guidelines
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.
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.

Fields	Usage Guidelines
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.

LDAP Group Settings

Table 31: LDAP Group Settings

Fields	Usage Guidelines
Add	Choose **Add > Add Group** to add a new group or choose **Add > Select Groups From Directory** to select the groups from the LDAP directory. If you choose to add a group, enter a name for the new group. If you are selecting from the directory, enter the filter criteria, and click **Retrieve Groups**. Check the check boxes next to the groups that you want to select and click OK. The groups that you have selected will appear in the Groups page.

LDAP Attribute Settings

Table 32: LDAP Attribute Settings

Fields	Usage Guidelines
Add	Choose **Add > Add Attribute** to add a new attribute or choose **Add > Select Attributes From Directory** to select attributes from the LDAP server. If you choose to add an attribute, enter a name for the new attribute. If you are selecting from the directory, enter the username and click **Retrieve Attributes** to retrieve the user's attributes. Check the check boxes next to the attributes that you want to select, and then click OK.

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 33: 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.

Fields	Usage Guidelines
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.

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 34: 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.

Fields	Usage Guidelines
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 35: 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.

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 36: 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 Enter the number of days before which you cannot reuse a 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 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.

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 configure a network access device in Cisco ISE. The navigation path for this page is: **Administration** > **Network Resources** > **Network Devices**.

Network Device Settings

The following table describes the fields in the Network Device section.

Table 37: Network Device 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. 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.

Fields	Description
Software Version	Click the drop-down list d to choose the version of the software running on the network device. 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 in the RADIUS Authentication Settings section.

Table 38: RADIUS Authentication Settings

Fields	Usage Guidelines
Protocol	Displays RADIUS as the selected protocol.
Shared Secret	Enter a shared secret, which can be up to 127 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.

Fields	Usage Guidelines
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 in the SNMP Settings section.

Table 39: 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.

Fields	Usage Guidelines
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
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

Fields	Usage Guidelines
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.

Advanced Trustsec Settings

The following table describes the fields in the Advanced Trustsec Settings section.

Table 40: Advanced Trustsec Settings

Fields	Usage Guidelines
Trustsec Device Notification and Updates Settings	
Use Device ID for Trustsec 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 Trustsec 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 Trustsec device (the same password that you have configured on the Trustsec device command-line interface [CLI]). Click **Show** to display the password that is used to authenticate the Trustsec 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 Trustsec 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.

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 Trustsec solution, after initial authentication, the Trustsec 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 Trustsec Devices to Trust This Device (Trustsec Trusted)	Check this check box if you want all the peer devices to trust this Trustsec 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 Trustsec configuration changes	Check this check box if you want Cisco ISE to send Trustsec CoA notifications to this Trustsec device.
Device Configuration Deployment Settings	
Include this device when deploying Security Group Tag Mapping Updates	Check this check box if you want this Trustsec 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) Trustsec PAC Display	
Issue Date	Displays the issuing date of the last Trustsec PAC that has been generated by Cisco ISE for this Trustsec device.

Fields	Usage Guidelines
Expiration Date	Displays the expiration date of the last Trustsec PAC that has been generated by Cisco ISE for this Trustsec device.
Issued By	Displays the name of the issuer (a Trustsec administrator) of the last Trustsec PAC that has been generated by Cisco ISE for this device.
Generate PAC	Click Generate PAC to create Trustsec Protected Access Credentials (PAC). By default, Out Of Band Trustsec Protected Access Credentials (PAC) information is empty, but appears disabled when populated. Trustsec PAC information can be automatically populated when you generate Trustsec PAC for any Trustsec 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 41: 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-host** 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.

Fields	Usage Guidelines
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 42: 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 43: 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.
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 44: 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 45: 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.

Fields	Usage Guidelines
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 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 > Add**.

Table 46: RADIUS Server Sequences

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

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.

Fields	Usage Guidelines
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 47: 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.
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.

Device Portal Management

Configure Device Portal Settings

Global Settings for Device Portals

Choose **Administration** > **Device Portal Management** > **Settings**.

You can configure the following general settings for the BYOD and My Devices portals:

- The maximum number of personal devices that an employee can register at any time using either portal.
- An IP address or URL that will reconnect an employee device to the BYOD registration process if a problem is encountered during the process.

Once you configure these general settings, they apply to all BYOD and My Devices portals that you set up for your company.

Portal Identification Settings for Device Portals

The navigation path for these settings is **Administration** > **Device Portal Managment** > **Blacklist Portal, Client Provisioning Portals, BYOD Portals, MDM Portals, or My Device Portals** > **Create, Edit or Duplicate** > **Portals Settings and Customization**.
Use these settings to identify the portal and select the language files to be used for all the portal pages.

Field	Usage Guidelines
Portal Name	Enter a unique portal name to access this portal. Do not use this portal name for any other Sponsor and Guest portals and non-guest portals, such as Blacklist, Bring Your Own Device (BYOD), Client Provisioning, Mobile Device Management (MDM), or My Devices portals. This name appears in the authorization profile portal selection for redirection choices, and is used in the list of portals for easy identification among other portals.
Description	Optional.
Portal test URL	A system-generated URL displays as a link after you click **Save**. Use it to test the portal. Click the link to open a new browser tab that displays the URL for this portal that is being served by a Policy Services Node (PSN) with Policy Services turned on. If Policy Services are not turned on, the PSN will not serve web pages for any portals other than the Admin portal. **Note** The test portal does not support RADIUS sessions, so you won't see the entire portal flow for all portals. BYOD and Client Provisioning are examples of portals that depend on RADIUS sessions. For example, a redirect to an external URL will not work.

Field	Usage Guidelines
Language File	Each portal type supports 15 languages by default, which are available as individual properties files bundled together in a single zipped language file. Export or import the zipped language file to use with the portal. The zipped language file contains all the individual language files that you can use to display text for the portal. The language file contains the mapping to the particular browser locale setting (for example, for French: fr, fr-fr, fr-ca) along with all of the string settings for the entire portal in that language. A single language file contains all the supported languages, so that it can easily be used for translation and localization purposes. If you change the browser locale setting for one language, the change is applied to all the other end-user web portals. For example, if you change the French.properties browser locale from fr,fr-fr,fr-ca to fr,fr-fr in the Hotspot Guest portal, the change is applied to the My Devices portal also.

Portal Settings for the Blacklist Portal

The navigation path for these settings is **Administration** > **Device Portal Management** > **Blacklist Portal** > **Edit** > **Portal Behavior and Flow Settings** > **Portal Settings**

Use these settings to specify values or define behavior that applies to the overall portal; not just to specific portal pages that display to the user (guests, sponsors, or employees as applicable).

- **HTTPS Port—**Enter a Port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded ISE and were using Port values outside this range, they are honored until you make any change to this page. If you do change this page, you must update the Port setting to comply with this restriction.

  If you assign Ports used by a non-guest (such as My Devices) portal to a guest portal, an error message displays.

- **Allowed interfaces—**Select the PSN interfaces where this portal can run. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical and bonded interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - The Ethernet interfaces must use IP addresses on different subnets.

  - The interfaces you enable here must be available on all the PSNs that are running portals, including VM-based ones (when Policy Services turned on). This is required because any of these PSNs can be used for a redirect at the start of the guest session.

- The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP. If the interface IP is not the same as the domain, then configure **ip host x.x.x.x yyy.domain.com** in the ISE CLI to map your interface IP to FQDN in the certificate.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

Portal Settings for BYOD Device Registration and MDM Portals

The navigation path for these settings is **Administration** > **Device Portal Management** > **BYOD Portals or MDM Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

Configure these settings to define portal page operations.

- **HTTPS Port—**Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you change this page. If you do change this page, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message will display.

- **Allowed interfaces—**Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  - Configure **ip host x.x.x.x yyy.domain.com** in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- Endpoint Identity Group— Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create additional endpoint identity groups if you choose to not use the default.

- Use Browser Locale—Specify that the user's browser locale setting is used for the display language of the portal. This assumes that the language file has a language that is mapped to the browser locale. If not, the Fallback Language will be used for the text displayed in the portal.
- Fallback Language—Choose the language to use if a language file is not available for the browser locale.

- Always Use—Choose the display language to use for the portal. This setting overrides the User browser locale option.

BYOD Settings for BYOD Portals

The navigation path for these settings is **Administration** > **Device Portal Management** > **BYOD Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **BYOD Settings**.
Use these settings to enable Bring Your Own Device (BYOD) functionality for employees who want to use their personal devices to access your corporate network.

Field	Usage Guidelines
Include an AUP (on page/as link)	Display your company’s network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
Display Device ID field during registration	Display the device ID to the user during the registration process, even though the device ID is pre-configured and cannot be changed while using the BYOD portal .
Originating URL	After successfully authenticating to the network, redirect the user’s browser to the original website that the user is trying to access, if available. If not available, the Authentication Success page displays. Make sure that the redirect URL is allowed to work on port 8443 of the PSN by the access-control list on the NAD and by authorization profiles configured in ISE for that NAD. For Windows, MAC and Android devices, control is given to the Self-Provisioning Wizard app, which performs the provisioning. Therefore, these devices are not redirected to the originating URL. However, iOS (dot1X) and unsupported devices (that are allowed network access) will be redirected to this URL.

Field	Usage Guidelines
Success page	Display a page indicating that the device registration was successful.
URL	After successfully authenticating to the network, redirect the user's browser to the specified URL, such as your company's website.

Note If you redirect a Guest to an external URL after authentication, there may be a delay while the URL address is resolved and the session is redirected.

Portal Settings for Client Provisioning Portals

The navigation path for these settings is **Administration** > **Device Portal Management** > **Client Provisioning Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

- **HTTPS Port—**Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you change this page. If you do change this page, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message will display.

- **Allowed interfaces—**Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.

  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.
  - The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
  - Configure **ip host x.x.x.x yyy.domain.com** in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.

- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.

Employee Mobile Device Management Settings for MDM Portals

The navigation path for these settings is **Administration** > **Device Portal Management** > **MDM Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Employee Mobile Device Management Settings**.

Use these settings to enable Mobile Device Management (MDM) functionality for employees using the MDM portals and define their AUP experience.

Field	Usage Guidelines
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before their account is fully enabled. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not obtain network access.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Portal Settings for My Devices Portals

The navigation path for these settings is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Portal Settings**.

-
- **HTTPS Port—**Enter a port value between 8000 to 8999; the default value is 8443 for all the default portals, except the Blacklist Portal, which is 8444. If you upgraded with port values outside this range, they are honored until you change this page. If you do change this page, update the port setting to comply with this restriction.

  If you assign ports used by a non-guest (such as My Devices) portal to a guest portal, an error message will display.

- **Allowed interfaces—**Select the PSN interfaces which can run a portal. Only a PSN with an available allowed interface on a PSN can create a portal. You can configure any combination of physical interfaces. This is a PSN-wide configuration; all portals can only run on these interfaces, this interface configuration is pushed to all the PSNs.
  - You must configure the Ethernet interfaces using IP addresses on different subnets.
  - The interfaces you enable here must be available on all your PSNs, including VM-based ones when Policy Services turned on. This is required because any of these PSNs can be used for a redirect at the start of the guest session.

- The portal certificate Subject Name / Alternate Subject Name must resolve to the interface IP.
- Configure **ip host x.x.x.x yyy.domain.com** in ISE CLI to map secondary interface IP to FQDN, which is used to match Certificate Subject Name / Alternate Subject Name.

- **Certificate group tag—**Select the group tag of the certificate group to use for the portal's HTTPS traffic.
- **Fully Qualified Domain Name (FQDN)—**Enter at least one unique FQDN or hostname for your Sponsor or MyDevices portal. For example, you can entersponsorportal.yourcompany.com,sponsor, so that when the user enters either of those into a browser, they reach the sponsor portal. Separate names with commas, but do not include spaces between entries. Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.
    - Update DNS to ensure that the FQDN of the new URL resolves to a valid Policy Services Node (PSN) IP address. Optionally, this address could point to a load balancer virtual IP address that serves a pool of PSNs.
    - To avoid certificate warning messages due to name mismatches, include the FQDN of the customized URL, or a wildcard, in the subject alternative name (SAN) attribute of the local server certificate of the Cisco ISE PSN.

  If you choose to update the default FQDN, also do the following:

- **Authentication Method —**Choose which identity source sequence (ISS) or Identity Provider (IdP) to use for user authentication. The ISS is a list of Identity Stores that are searched in sequence to verify user credentials. Some examples include: Internal Guest Users, Internal Users, Active Directory, LDAP Directory.

  Cisco ISE includes a default sponsor Identity Source Sequence for sponsor portals, Sponsor_Portal_Sequence.

- **Endpoint identity group—**Choose an endpoint identity group to track guest devices. Cisco ISE provides the **GuestEndpoints** endpoint identity group to use as a default. You can also create more endpoint identity groups if you choose to not use the default.

  Choose an endpoint identity group to track employee devices. Cisco ISE provides the **RegisteredDevices** endpoint identity group to use as a default. You can also create more endpoint identity groups, if you choose to not use the default.

- **Purge endpoints in this identity group when they reach __ days—**Change the number of days since the registration of a user's device before it is purged from the Cisco ISE database. Purging is done on a daily basis and the purge activity is synchronized with the overall purge timing. The change is applied globally for this endpoint identity group. If changes are made to the Endpoint Purge Policy based on other policy conditions, this setting is no longer available for use.
- **Idle timeout—** Enter the time in minutes that you want Cisco ISE to wait before it logs out the user if there is no activity in the portal. The valid range is from 1 to 30 minutes.
- **Display Language—**Specify which language is used in the portal: the user's browser locale setting, with a fallback to another language if a browser locale is not available. Or force the portal to always use one language.
-

Login Page Settings for My Devices Portals

The navigation path for this page is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Login Page Settings**.
Use these settings to define the login experience for users (guests, sponsors or employees as applicable), the parameters for failed login attempts, and AUP information for this page.

Field	Usage Guidelines
Maximum failed login attempts before rate limiting	Specify the number of failed login attempts from a single browser session before Cisco ISE starts to throttle that account. This does not cause an account lockout. You can specify the time between attempts after this number of failed logins is reached in **Time between login attempts when rate limiting**.
Time between login attempts when rate limiting	Set the length of time in minutes that a user must wait before attempting to log in again, after failing to log in the number of times defined in **Maximum failed login attempts before rate limiting**.
Include an AUP (on page/as link)	Display your company's network-usage terms and conditions, either as text on the page currently being displayed for the user or as a link that opens a new tab or window with AUP text.
Require acceptance	Require users to accept an AUP before they can access the portal. The **Login** button is not enabled unless the user accepts the AUP. If users do not accept the AUP, they will not be able to access the portal.
Require scrolling to end of AUP	This option displays only if **Include an AUP on page** is enabled. Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.

Acceptable Use Policy (AUP) Page Settings for My Devices Portals

The navigation path for this page is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Acceptable Use Policy (AUP) Page Settings**.
Use these settings to define the AUP experience for the users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include an AUP page	Display your company's network-usage terms and conditions on a separate page to the user.

Field	Usage Guidelines
Require scrolling to end of AUP	Ensure that the user has read the AUP completely. The **Accept** button activates only after the user has scrolled to the end of the AUP.
On first login only	Display an AUP when the user logs into the network or portal for the first time only.
On every login	Display an AUP each time the user logs into the network or portal.
Every __ days (starting at first login)	Display an AUP periodically after the user first logs into the network or portal.

Post-Login Banner Page Settings for My Devices Portals

The navigation path for this page is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Post-Login Banner Page Settings**. Use this setting to notify users (guests, sponsors or employees as applicable) of additional information after they log in successfully.

Field	Usage Guidelines
Include a Post-Login Banner page	Display additional information after the users successfully log in and before they are granted network access.

Employee Change Password Settings for My Devices Portals

The navigation path for this page is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Employee Change Password Settings**. Use these settings to define the password requirements for employees using the My Devices portal.

To set the employee password policy, choose **Administration** > **Identity Management** > **Settings** > **Username Password Policy**.

Field	Usage Guidelines
Allow internal users to change password	Allow employees to change their passwords after they log into the My Devices portal. This only applies to employees whose accounts are stored in the Cisco ISE database and not to those stored in external databases, such as Active Directory or LDAP.

Manage Device Settings for My Devices Portal

The navigation path for these settings is **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Manage Devices**.
Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Manage Accounts tab of the My Devices portal.

Under **Settings**, you can specify the actions that employees using this My Devices portal can perform on their registered personal devices.

Table 48: Manage Device Settings for My Devices Portals

Field	Usage Guidelines
Lost	For all devices. Enable employees to indicate that their device is lost. This action updates the device status in the My Devices portal to Lost and adds the device to the Blacklist endpoint identity group.
Reinstate	For all devices. This action reinstates a blacklisted, lost or stolen device and resets it status to its last known value. This action resets the status of a stolen device to Not Registered, since it has to undergo additional provisioning before it can connect to the network. If you want to prevent employees reinstating devices that you have blacklisted, do not enable this option in the My Devices portal.
Delete	For all devices. Enable employees to delete a registered device from the My Devices portal or to delete unused and add new devices, once the maximum number of registered devices is reached. This action removes the device from the list of devices displayed in the My Devices portal, but the device remains in the Cisco ISE database and continues to be listed in the Endpoints list. To define the maximum number of personal devices that employees can register using either the BYOD or My Devices portals, choose **Administration** > **Device Portal Management** > **Settings** > **Employee Registered Devices**. To permanently delete the device from the Cisco ISE database, choose **Administration** > **Identity Management** > **Identities** > **Endpoints**.

Field	Usage Guidelines
Stolen	For all devices. Enable employees to indicate that their device is stolen. This action updates the device status in the My Devices portal to Stolen, adds the device to the Blacklist endpoint identity group, and removes its certificate.
Device lock	For MDM enrolled devices only. Enable employees to immediately lock their device remotely from the My Devices portal, in the event it is lost or stolen. This action prevents unauthorized use of the device. However, the PIN cannot be set in the My Devices portal and should have already been configured by the employee on their mobile device in advance.
Unenroll	For MDM enrolled devices only. Enable employees to choose this option if they no longer need to use their device at work. This action removes only those applications and settings installed by your company, while retaining other apps and data on the employee's mobile device.
Full wipe	For MDM enrolled devices only. Enable employees to choose this option if they have lost their device or are replacing it with a new one. This action resets the employee's mobile device to its default factory settings, removing installed apps and data.

Add, Edit, and Locate Device Customization for My Devices Portals

The navigation path for these settings are **Administration** > **Device Portal Management** > **My Devices Portals** > **Create, Edit or Duplicate** > **Portal Page Customization** > **Add Devices, Edit Devices or Locate Devices**.

Under **Page Customizations**, you can customize the messages, titles, content, instructions, and field and button labels that appear on the Add, Edit and Locate tabs of the My Devices portal.

Support Information Page Settings for Device Portals

The navigation path for this page is **Administration** > **Device Portal Management** > **BYOD Portals, Client Provisioning Portals, MDM Portals, or My Devices Portals** > **Create, Edit or Duplicate** > **Portal Behavior and Flow Settings** > **Support Information Page Settings**.
Use these settings to display the information that your Help Desk can use to troubleshoot access issues experienced by users (guests, sponsors or employees as applicable).

Field	Usage Guidelines
Include a Support Information Page	Display a link to an information page, such as **Contact Us**, on all enabled pages for the portal.
MAC address	Include the MAC address of the device on the Support Information page.
IP address	Include the IP address of the device on the Support Information page.
Browser user agent	Include the browser details such as the product name and version, layout engine and version of the user agent originating the request on the Support Information page.
Policy server	Include the IP address of the ISE Policy Service Node (PSN) that is serving this portal on the Support Information page.
Failure code	If available, include the corresponding number from the log message catalog. You can access and view the message catalog by navigating to **Administration** > **System** > **Logging** > **Message Catalog**.
Hide field	Do not display any field labels on the Support Information page if the information that they would contain is non-existent. For example, if the failure code is unknown, and therefore blank, do not display **Failure code**, even if it is selected.
Display label with no value	Display all selected field labels on the Support Information page, even if the information that they would contain is non-existent. For example, if the failure code is unknown, display **Failure code**, even if it is blank.
Display label with default value	Display this text in any selected field on the Support Information page, if the information that they would contain is non-existent. For example, if you enter Not Available in this field, and the failure code is unknown, the **Failure code** will display as **Not Available**.