Managing Cisco Trust and Identity Management Solutions

Cisco TrustSec Identity, earlier known as Cisco Identity-based Networking Services (IBNS), a part of the Cisco Trust and Identity Management Solution, is the foundation for providing access control to corporate networks. The Cisco TrustSec Identity solution is a set of Cisco IOS Software services designed to enable secure user and host access to enterprise networks powered by Cisco Catalyst switches and Wireless LANs (WLANs).

Cisco TrustSec Identity offers authentication, access control, and user policies to secure network resources and connectivity. With Cisco TrustSec Identity you can ensure greater security for your network and manage network changes throughout your organization in a cost-effective manner. Having a secure Identity framework in place helps enterprises manage employee mobility, and reduce network access expenses.

Cisco TrustSec Identity enables you to grant customized access to the network based on the identity of a user or device, and the corporate security policy. An Identity is an indicator of a client in a trusted domain; it is used as a pointer to a set of rights or permissions that is allowed for a client.

Cisco TrustSec Identity improves the network’s ability to identify, prevent, and adapt to threats. It also provides automated AAA services for switch-based network access; automates security policy enforcement and provides dynamic VLAN provisioning.

This chapter contains:

- Identity in LMS
- Features and Benefits of Identity in LMS
- Terms and Definitions in Identity
- Understanding the Identity Dashboard
- Supported Devices and Images for Identity
- Getting Started with Identity
- Assessing Identity Readiness of Your Network
- Configuring RADIUS
- Provisioning Identity
- Scheduling Identity Configuration Jobs
- Identity Readiness Assessment
- Managing Identity Devices
- Monitoring Identity
Identity in LMS

In LMS, IBNS or Identity provides a set of management functions to simplify and automate the Identity management lifecycle. The Identity dashboard organizes all the Identity functions into a single portal for quick navigation and real-time Identity updates.

Identity management in LMS consists of:

- Assessing the Identity readiness of your network using the Identity Readiness Assessment. See Assessing Identity Readiness of Your Network for more information.
- Identifying Identity-capable devices, Identity-software-incapable devices, Identity-hardware-incapable devices, and RADIUS-capable devices through a readiness report.
- Preparing the network for Identity provisioning
  - Configuring RADIUS Settings
    See Configuring RADIUS for more information.
- Provisioning Identity on Identity-capable devices
  - Configuring security modes, authentication profile, and host mode
  - Configuring MACsec on capable devices.
  - Dynamically assigning resources
    See Provisioning Identity for more information.
- Monitoring and reporting on user activity
- Troubleshooting authentication and authorization issues

The sections describes the following:

- Features and Benefits of Identity in LMS
- Terms and Definitions in Identity
- Understanding the Identity Dashboard
- Supported Devices and Images for Identity
- Getting Started with Identity
- Provisioning Identity
- Identity Readiness Assessment
- Monitoring Identity
- Managing Identity Jobs
Features and Benefits of Identity in LMS

Identity in LMS provides comprehensive support for automating the provisioning of Identity in the network, and for monitoring various authentication and authorization details. Table 2-1 lists the features and benefits of Identity in LMS.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>View identity enabled devices</td>
<td>You can quickly identify Identity enabled devices in the Getting Started page. For more information, see Identity Readiness Assessment.</td>
</tr>
<tr>
<td>Enable Identity on devices</td>
<td>You can easily upgrade images on Identity-software-incapable devices and configure Identity.</td>
</tr>
</tbody>
</table>
| Enable phased deployment of Cisco IBNS services using various modes | You can  
• Gain visibility to your network  
• Strengthen access security  
• Provide differentiated services  
• Minimize impact to end users.  
• Assign resources dynamically to the correct VLAN.  
• Automate security policy enforcement.  
For more information, see Provisioning Identity.                                                                 |
| Configure MACsec                             | You can  
• Enable MACsec on supported devices  
• Select the policy to be applied for the session after the supplicant passes 802.1x authentication.  
• Specify the MKA policy.  
For more information on:  
• Understanding MACsec, see Understanding Media Access Control Security (MACsec).  
• Configuring MACsec using LMS, see Configuring Identity. |
| Monitor user activity                        | • You can identify the authentication and authorization trends through charts and graphs; provides real-time status for quickly isolating potential issues. For more information, see Understanding the Identity Dashboard. |
This section explains certain terms and definitions used in Identity:

- Understanding the Security Modes
- Understanding Authentication Profiles
- Understanding Host Modes
- Understanding MAC Move and MAC Replace
- Understanding Change of Authorization (CoA)
- Understanding Media Access Control Security (MACsec)

### Understanding the Security Modes

LMS allows you to deploy Identity in phases with minimal impact to end users. You can deploy Identity in three security modes. They are:

- Monitor Mode
- Low Impact Mode
- High Security Mode

### Monitor Mode

In Monitor Mode, you can enable authentication (802.1X and MAB) without enforcing any type of authorization. There will be no interruption to the existing network services. In the background, however, the network queries each endpoint as it connects, and validates its credentials.

This mode enables you to create an inventory of the MAC addresses and determine any 802.1X devices before enforcing any access control. It provides visibility into the end-user network access activities, assessment, and policy evaluation information.

**Note**

MACSec is not supported in monitor mode.

### Terms and Definitions in Identity Dashboard

You can have fast and easy access to Identity-related data. Provides a snapshot of the effect of provisioning Identity in the network; you can monitor, and reduce the time required to isolate, and troubleshoot problems.

For more information, see Understanding the Identity Dashboard.

### Troubleshooting

You can quickly isolate and troubleshoot Identity related issues through the Identity dashboard.

For more information, see Understanding the Identity Dashboard.

---

**Table 2-1  Features and Benefits of Identity in LMS**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefits</th>
<th>For more information, see Understanding the Identity Dashboard.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity dashboard</td>
<td>- You can have fast and easy access to Identity-related data.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Provides a snapshot of the effect of provisioning Identity in the network; you can monitor, and reduce the time required to isolate, and troubleshoot problems.</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>You can quickly isolate and troubleshoot Identity related issues through the Identity dashboard.</td>
<td></td>
</tr>
</tbody>
</table>
Low Impact Mode

In Low Impact Mode, you can incrementally increase the level of port-based access control without affecting the existing network infrastructure. This mode neither requires the addition of any new VLANs nor does it impact your existing network addressing scheme. With the Low Impact Mode, you can add as little or as much access control as you want.

Low Impact Mode builds on top of Monitor Mode. In Monitor Mode, the Pre-Authentication authorization level is completely open, whereas in Low Impact Mode, the Pre-Authentication level is selectively open. This mode enables differentiated access through policy-driven downloadable access control lists (dACLs), based on user identity information.

High Security Mode

The High Security Mode ensures the highest security level using 802.1X, where access is not granted unless authentication succeeds.

In High Security Mode, the port is kept completely closed until a successful authentication takes place. There is no concept of Pre-Authentication access. After a successful authentication, network access will change the authorization from completely closed to completely open. To add more granular access control, this mode uses dynamic VLAN assignment to isolate different classes of users into different broadcast domains.

Understanding Authentication Profiles

The different types of authentication profiles available in Identity in LMS are:

- 802.1x Port-Based Authentication
- MAC Authentication Bypass (MAB)
- Web-Based Authentication (WebAuth)
- Flexible Authentication (FlexAuth)
- Local WebAuth

802.1x Port-Based Authentication

IEEE 802.1X protocol allows Cisco Catalyst switches to offer network access control at the port level. Every port on the switch is individually enabled or disabled based on the identity of the user or device connecting to it.

First, a client, such as a laptop equipped with an 802.1X supplicant, connects to an IEEE 802.1X-enabled network and sends a start message to the LAN switch (the authenticator). Once the start message is received, the LAN switch sends a login request to the client and the client replies with a login response. The switch forwards the response to the policy database (the authentication server), which authenticates the user. After the user identity is confirmed, the policy database authorizes network access for the user and informs the LAN switch. The LAN switch then enables the port connected to the client. User or device credentials are processed by AAA server.
MAC Authentication Bypass (MAB)

Devices that cannot authenticate themselves using 802.1X can use MAB to get network access. MAB enables differentiated access control for devices and not for users. With this method the MAC address of the connected devices is used, as user name and password, to grant or deny network access. This method requires a database of pre-defined MAC addresses.

Web-Based Authentication (WebAuth)

WebAuth is an alternate or fallback method for 802.1X and MAB to authenticate end users or client connecting to the network. In wired networks, WebAuth begins after IEEE 802.1X has timed out or failed, or MAB has failed. WebAuth is only for users and not for devices because it requires a browser and manual entry of user name and password.

On a wired port, network access is restricted by a pre-authentication port access control list (ACL). This ACL must be configured and applied to the WebAuth fallback profile. The contents of the pre-authentication ACL are arbitrary and can be defined to allow or limit as much access as the network security policy allows. At a minimum, however, the ACL should allow access for DHCP and DNS, so that a host can acquire an IP address and resolve host names in URLs. In addition, the pre-authentication ACL should allow redirected traffic to the Cisco Network Admission Control (NAC) Guest Server (NGS).

Flexible Authentication (FlexAuth)

Flexible authentication (FlexAuth) is a set of features that allows IT administrators to configure the sequence and priority of IEEE 802.1X, MAB, and Local WebAuth.

The Cisco IOS Flex-Auth feature allows you to create a flexible, adaptable deployment in the high security mode. It allows secondary authentication methods to 802.1X, such as MAB or WebAuth for guest access authorization.

Local WebAuth

WebAuth authenticates the user at the access edge by providing a web-based login page on which you can enter your credentials. After the user is identified, the user's identity can be used by mapping identities to policies that grant or deny granular network access.

Integrated local WebAuth enables network administrators to use webpages that are centrally managed and hosted on the Cisco NAC Guest Server (NGS). Centralized management greatly reduces the operating expenses associated with maintaining a WebAuth solution because webpage updates and changes can be made in a single place.

Understanding Host Modes

You can select a host mode in a switch to determine the number of hosts that can be authenticated on a given port. The different types of host modes are:

- Single Host Mode
- Multiple Host Mode
- Multiple Domain Authentication
- Multiple Authentication Mode
**Single Host Mode**

In this mode, only one user is allowed per port with only one MAC address. When you add a second MAC address to the network, a security violation will be generated and the port will shutdown or change to the error-disable state based on the security violation behavior.

**Multiple Host Mode**

Multiple host mode supports multiple hosts on the same port in a single domain. In this mode, multiple users can get connected to the switch through a hub; however, among all hosts on this port only one of the hosts will be authorized to have access to the network.

**Multiple Domain Authentication**

Multiple Domain Authentication (Multi-domain) mode, an IP phone (Cisco or a third-party IP phone) and a host behind the IP phone can authenticate independently, using one of the three authentication mechanisms: 802.1X, MAC authentication bypass (MAB), or web-based authentication (webauth) for the host only. Only two MAC addresses are allowed per port, one in the data domain and one in the voice domain. Multi-domain refers to two domains — data and voice — and only two MAC addresses are allowed per port.

**Multiple Authentication Mode**

Multiple Authentication Mode (Multi-auth) allows only one client on the voice VLAN and multiple authenticated clients on the data VLAN. If there are multiple users behind a hub connected to a phone, all the users behind the hub have to be authenticated individually. Multi-auth mode provides enhanced security over multiple hosts mode by requiring authentication of each connected client. It also allows you to detect virtualized endpoints or unauthorized hubs.

---

**Note**

You cannot use MACsec and the MKA Protocol in High Security Mode with Multiple authentication mode.

**Understanding MAC Move and MAC Replace**

Host Movement of mobile hosts that are indirectly connected (for example, hosts connected behind an IP phone or a hub) to the switch can be problematic. A switch may trigger a security violation, not knowing that an indirectly connected host has disconnected, when a new host plugs into the same port or when the original host plugs into a different port on the same switch.

Cisco IP phones can work in conjunction with Cisco switches to facilitate host movement using the Cisco Discovery Protocol (CDP), but, for non-Cisco phones or other intermediary devices that cannot signal a link down event, Cisco switches support two additional features to enable host movement such as:

- MAC Move
- MAC Replace
MAC Move

MAC Move allows a host to move to another port on the switch, even if an authenticated session already exists on a different port. For example, you unplug your laptop from behind a non-Cisco phone in your cube and plug directly into a port in a nearby conference room that is connected to the same switch as the phone. Not knowing that the laptop had unplugged, the switch would detect the same MAC address on two ports and, by default, trigger a security violation. Although this default behavior helps prevent MAC spoofing, it also impedes host movement. If MAC Move is enabled, however, the switch will delete the session on the first port and authenticate the laptop on the second port.

MAC Replace

MAC Replace allows one host to replace a previously authenticated host on the same port. For example, you temporarily plug your laptop into a phone. After you leave the room, another user tries to plug into the phone. Not knowing that the original laptop had disconnected, the switch detects a second MAC on the port and, by default, triggers a security violation that can cause packets from the second MAC to be dropped, or even shuts down the port.

Although this mitigates against port piggybacking, it also impedes host movement. If MAC Replace is enabled, however, the switch will still trigger a security violation but instead of shutting down the port or dropping packets from the second host, the switch will delete the first session on the port and authenticate the second device, effectively replacing the first authenticated session with the second authenticated session.

Understanding Change of Authorization (CoA)

CoA provides a mechanism for changing the attributes of a session after it has been authenticated. When a change in authentication, authorization, and accounting (AAA) policy occurs for a user or user group, administrators can send the RADIUS CoA packets from the AAA server, such as the Cisco Secure Access Control Server (ACS), to re-initialize authentication and apply the new policies.

In LMS, you can use the CoA system-defined template to generate and deploy the configuration commands on devices in your network. You can deploy the template by selecting Configuration > Tools > Template Center > Deploy from the LMS home page.

LMS provides you with a list of system-defined templates. These templates generate configuration commands that can be deployed on devices in your network. These templates are deployed using Deploy Template job in LMS.

You can modify the system-defined templates and save them as user-defined templates. You can also import templates from a server repository or a client machine and these templates are stored as system-defined templates in LMS.

Understanding Media Access Control Security (MACsec)

MACsec, defined in IEEE 802.1AE, provides secure, encrypted communication on wired LANs. MACsec is capable of identifying and preventing threats from denial of service, intrusion attacks, and other attacks launched from behind the firewall.

This protocol allows unauthorized LAN connections to be identified and excluded from communication within the network. MACsec defines a security infrastructure to provide data confidentiality and data integrity. MACsec can mitigate attacks on Layer 2 protocols and works with any type of traffic carried over Ethernet links.
Each packet on the wire is encrypted using symmetric key cryptography. This encryption ensures that communication is not monitored or altered on the wire.

The MACsec Key Agreement (MKA) Protocol provides the required session keys and manages the required encryption keys. MKA discovers MACsec peers and negotiates the keys used by MACsec. MKA is defined in IEEE 802.1X-2010.

---

**Note**

You cannot use MACsec and the MKA Protocol in High Security Mode with Multiple authentication mode.

---

When a device connects to a MACSec-capable switch and authentication is successful, the switch has three options:

- **Optionally secure sessions**
  - The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only.
  - If MKA times out or fails, the switch will permit unencrypted traffic. This policy is the default security policy.

- **Always secure sessions**
  - The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only.
  - If MKA times out or fails, the switch will treat this as an authorization failure by terminating the IEEE 802.1X-authenticated session, and retrying authentication after a period of time. No traffic will be allowed from the endpoint unless you configure a MACsec failure policy. The policy can be set to try the next authentication method or authorize into a special VLAN.

- **Never secure sessions**
  - The switch will not perform MKA. If the supplicant sends MKA protocol frames, they will be ignored. The switch will send and receive unencrypted traffic.

- **No Change**
  - If you select this option, the default policy will occur. The default policy, Optionally secure sessions, will be used.

**Advantages of MACsec**

MACsec offers the following benefits on wired networks:

- **Confidentiality**
  - MACsec ensures data confidentiality by providing strong encryption at Layer 2.

- **Integrity**
  - MACsec provides integrity checking to ensure that data cannot be modified in transit.

- **Flexibility**
  - You can selectively enable MACsec using a centralized policy. You can enforce MACSec on supported devices and also allow non-MACSec-capable components to access the network.

- **Network Intelligence**
  - MACsec encrypts packets on a hop-by-hop at Layer 2, allowing the network to inspect, monitor, mark and forward traffic according to the existing policies.
Understanding the Identity Dashboard

You can access the Identity dashboard using:

- Work Centers > Identity > Dashboard
- My Menu > Default Dashboards > Identity
- Monitor > Dashboards > Identity

The Identity Dashboard displays all the Identity portlets. The various Identity portlets are:

- Identity - Authentication Trend
- Identity - Authorization Trend
- Identity - Security Modes Distribution
- Identity - 802.1x Agentless Portlet
- Identity - Authenticated Users Portlet
- User Tracking Summary

---

**Note**

You need Adobe flash player 9 or later to view some Identity portlets. You can install the flash player from the portlet. Reload the page after installing the flash player.

Identity - Authentication Trend

The Authentication Trend Portlet displays a line graph of successful or failed authentications for a selected time period. You can generate separate reports for successful and failed authentications.

When you select a time period, the graph will show the data only for the last accessed time of the users. For example, in the following scenario, the selected time period is one week.

For the selected week if you have four users, A, B, C, and D, who have successfully authenticated on Monday, on Wednesday, only A and B are authenticated, and on Friday only C and D are successfully authenticated. Here, the graph will show only two users for Wednesday, and two for Friday.

To configure this portlet, see Configuring Identity Portlets for more information. Click Show Grid to view the details in a tabular format.

Identity - Authorization Trend

The Authorization Trend Portlet displays a line graph of successful or failed authorization for a selected time period. You can generate separate reports for successful and failed authorizations.

When you select a time period, the graph will show the data only for the last accessed time of the users. For example, in the following scenario, the selected time period is one week.

For the selected week if you have four users, A, B, C, and D, who are successfully authorized on Monday, on Wednesday, only A and B are authorized, and on Friday only C and D are successfully authorized. In the above case, the graph will show only two users for Wednesday, and two for Friday.

You can also see the details of the graph in a tabular format. To configure this portlet, see Configuring Identity Portlets for more information.
Configuring Identity Portlets

To configure the portlet:

- **Step 1** Move the mouse over the title bar of the Identity portlet to view the icons.
- **Step 2** Click the Configuration icon.
- **Step 3** Select the Auto refresh check box to set the refresh time.
- **Step 4** Select the minute or hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed according to the specified refresh time.
- **Step 5** Select the number of rows to be displayed from the drop-down list.
- **Step 6** Click **Select Devices** to launch the device selector.
- **Step 7** Select an Identity-enabled switches from the device selector.
- **Step 8** Click **Save** to save your settings for this portlet.

Identity - Security Modes Distribution

You can view this portlet in the Identity dashboard using:

- **Work Centers > Identity > Dashboard**
- **My Menu > Default Dashboards > Identity**
- **Monitor > Dashboards > Identity**

The Identity Modes Portlet displays a pie chart of the different types of security modes that are deployed in your network and also the devices that are not in any security mode. The security modes are:

- Monitor Mode
- Low Impact Mode
- High Security Mode
- Unsecured Mode

When you click a slice of the pie chart, the Manage Identity Devices page appears. You can change the security mode or disable Identity of an Identity-enabled device. For more information, see Managing Identity Devices.

You can also click the View as Grid icon at the bottom of the portlet and see the same information in a tabular format.

To set the refresh time of this portlet:

- **Step 1** Move the mouse over the title bar of the Identity Modes portlet to view the icons.
- **Step 2** Click the Configuration icon.
- **Step 3** Select the Auto refresh check box to set the refresh time.
- **Step 4** Select the minute or hour from the Refresh Every drop-down list to change the Refresh time. The items in the portlet get refreshed according to the specified refresh time.
Understanding the Identity Dashboard

Identity - 802.1x Agentless Portlet

You can view this portlet in the Identity dashboard using:

- Work Centers > Identity > Dashboard
- My Menu > Default Dashboards > Identity
- Monitor > Dashboards > Identity

The 802.1x Agentless Portlet displays a pie chart of the current number of successful or failed authentications through MAC Authentication Bypass (MAB), or Web-Based Authentication (WebAuth). When you click a slice of the pie chart, the corresponding report appears.

You can select a time interval to view the details for that time period.

To configure this portlet, see Configuring Identity Portlets for more information.

Identity - Authenticated Users Portlet

You can view this portlet in the Identity dashboard using:

- Work Centers > Identity > Dashboard
- My Menu > Default Dashboards > Identity
- Monitor > Dashboards > Identity

The Authenticated Users Portlet displays a pie chart of the current number of users authenticated using one of the following authentication profiles:

- 802.1x Port-Based Authentication
- MAB
- WebAuth

You can select a time interval to view the users authenticated during that time period.

To configure this portlet, see Configuring Identity Portlets for more information.

User Tracking Summary

You can view this portlet in the Identity dashboard using:

- Work Centers > Identity > Dashboard
- My Menu > Default Dashboards > Identity
- Monitor > Dashboards > Identity

The User Tracking Summary portlet displays the number of MACs. These are:

- Rogue MAC—MAC addresses that are not authorized to exist in your network. MAC addresses that are configured as Rogue in the User Tracking setting will be displayed here.
- New MAC—MAC addresses that are newly added to your network.
- Dormant MAC—MAC addresses that are inactive for a specified number of days.

This portlet also gives the summary about the last User Tracking information such as the number of end hosts, active, connected, dormant, new and rogue end hosts.
End hosts are hosts that are currently connected to the network. The regular end hosts report shows both active end hosts and end hosts that were previously connected to the network but are disconnected now. You can also view details of the Connected End Hosts. These hosts have MAC entries that are not available in the CAM table but are in active state.

Table 2-2 lists the User Tracking Summary portlet details.

### Table 2-2  User Tracking Summary

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of End hosts</td>
<td>Displays the number of end hosts. You can click the number to navigate to the End Hosts Immediate Reports page.</td>
</tr>
<tr>
<td>Number of Active End hosts</td>
<td>Displays the number of active end hosts. You can click the number link to navigate to the Active End Hosts Immediate Report page.</td>
</tr>
<tr>
<td>Number of Connected End Hosts</td>
<td>Displays the number of connected end hosts. These hosts have MAC entries that are not available in the CAM table but are in active state. You can click the number link to navigate to the Connected End Hosts Immediate Report page.</td>
</tr>
<tr>
<td>Number of Dormant hosts in last 7 days</td>
<td>Displays the number of hosts that are inactive for 7 days. The number of days depends on the days configured in the configuration screen. You can click the number link to navigate to the Dormant MAC Report page.</td>
</tr>
<tr>
<td>Number of New hosts in last 7 days</td>
<td>Displays the number of new hosts in the last 7 days. The number of days depends on the days configured in the configuration screen. You can click the number link to navigate to the New MAC Report page.</td>
</tr>
<tr>
<td>Number of Rogue hosts in last 7 days</td>
<td>Displays the number of rogue hosts in the last 7 days. The number of days depends on the days configured in the configuration screen. You can click the number link to navigate to the Rogue MAC Report page.</td>
</tr>
</tbody>
</table>

You can configure the User Tracking Summary portlet.

To configure the User Tracking Summary:

**Step 1** Configure the refresh time.

**Step 2** Enter the number of days to view the list of Dormant, New, and Rogue hosts in the corresponding text fields for the specified number of days.
Step 3  Click **Save** to save all the settings.
Supported Devices and Images for Identity

Table 2-3 lists the devices and images, that support Identity.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>Minimum Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catalyst 2960</td>
<td>12.2(52)SE</td>
</tr>
<tr>
<td>Catalyst 2975</td>
<td>12.2(52)SE</td>
</tr>
<tr>
<td>Catalyst 3560</td>
<td>12.2(52)SE</td>
</tr>
<tr>
<td>Catalyst 3750</td>
<td>12.2(52)SE</td>
</tr>
<tr>
<td>Catalyst 3750 (Stack Mode)</td>
<td>12.2(52)SE</td>
</tr>
<tr>
<td>Catalyst 4500</td>
<td>12.2(50)SG</td>
</tr>
<tr>
<td>Catalyst 6500</td>
<td>12.2(33)SXI</td>
</tr>
</tbody>
</table>

Note
The minimum supported version for MACsec is 12.2(53)SE2 Software image for Cisco Catalyst 3750-X and 3560-X switches. Table 2-4 lists the devices and images, that support MACsec.

<table>
<thead>
<tr>
<th>Device Type</th>
<th>sysObjectID</th>
<th>Minimum Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Catalyst 3750X-24T-L,S</td>
<td>1.3.6.1.4.1.9.1.1222</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750X-48T-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1223</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750X-24P-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1224</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3750X-48PF-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1225</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560X-24T-L,S</td>
<td>1.3.6.1.4.1.9.1.1226</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560X-48T-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1227</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560X-24P-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1228</td>
<td>12.2(53)SE2</td>
</tr>
<tr>
<td>Cisco Catalyst 3560X-48PF-L,S Switch</td>
<td>1.3.6.1.4.1.9.1.1229</td>
<td>12.2(53)SE2</td>
</tr>
</tbody>
</table>

Getting Started with Identity

The Getting Started workflow guides you on provisioning Identity for Day 1 operations. For advanced configurations you can choose the corresponding link in the Identity TOC.

The Getting Started workflow for Identity is:

1. Assessing Identity Readiness of Your Network
2. Configuring RADIUS
3. Provisioning Identity
Assessing Identity Readiness of Your Network

**Note**
Config collection and inventory collection must be successful to assess the Identity readiness of your network.

The Identity readiness assessment in the Getting Started Assistant displays Identity based device details after assessing the network. A pie chart appears with the following types of devices:

- Identity-capable Devices
- Identity-software-incapable Devices
- RADIUS-capable Devices
- Identity-hardware-incapable Devices

Click on any of the pie chart slices to view the details of the devices. Config collection and inventory collection must be successful to assess the Identity readiness of your network.

**Note**
You need Adobe flash player 9 or later to display the readiness assessment pie chart. You can install the flash player from LMS. Reload the page after installing the flash player.

**Identity-capable Devices**

Click the **Identity-capable devices** slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices have the supported Identity-capable IOS image. However, Identity is not configured on these devices. RADIUS is enabled on these devices.

Select one or more devices and click **Enable Identity** to configure Identity on the selected devices. See, **Configuring Identity** for more details.

**Identity-software-incapable Devices**

Click the **Identity-software-incapable devices** slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices do not have the Identity-capable IOS images. You can upgrade to the Identity-capable image version. See **Supported Devices and Images for Identity** for more information. Select one or more devices and click **Upgrade Software Image** to upgrade to the Identity-capable IOS image.

**RADIUS-capable Devices**

Click the **RADIUS-capable devices** slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices have RADIUS-capable IOS images, but RADIUS is not configured on these devices.

Select one or more devices and click **Configure RADIUS** to configure RADIUS and AAA settings on the selected devices. See, **Configuring RADIUS** for more details.

**Note**
If a device has the Identity-capable IOS image, and RADIUS is not configured on it, the device will appear as a RADIUS-capable and not an Identity-capable device.
Identity-hardware-incapable Devices

Click the **Identity-hardware-incapable devices** slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices do not have the provision for Identity technology. You can upgrade the devices with the latest Identity-supported hardware from Cisco.com.

See **Supported Devices and Images for Identity** for more information.

See **Known List of Hardware-incapable Devices** for more information.

**Note**

After you enable Identity, configure RADIUS, or upgrade the software image on a device, LMS performs a config archive on the affected devices. The device state updates appear in the Readiness Assessment pie chart after a while.

Configuring RADIUS

You can configure the RADIUS server for authentication, authorization, and accounting.

You can configure the RADIUS server in the Getting Started workflow and also from the Identity TOC. The following users alone can perform this configuration:

- Network Operator
- Network Administrator
- Super Admin

To configure the RADIUS server settings:

**Step 1** Select **Work Centers > Identity > Configure > Configure RADIUS**.
The Configure RADIUS page appears.

**Step 2** Click the **Select Devices** tab and select the devices for which you want to configure the RADIUS server.

**Step 3** Click **Next**. The Configure RADIUS server page appears.

**Step 4** Select one of the following:

- **Single RADIUS Host** radio button to specify a RADIUS server host. The following information appears:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP</td>
<td>DNS name or IP address of the RADIUS server host.</td>
</tr>
<tr>
<td>Authentication port</td>
<td>Specify the port number for authentication requests.</td>
</tr>
</tbody>
</table>

**Note**

Authentication and Accounting port numbers cannot be the same. Do not enter the port numbers used by LMS server.

The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.
### Configuring RADIUS

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting port</td>
<td>Specify the port number for accounting requests.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Authentication and Accounting port numbers cannot be the same. Do not enter the port numbers used by LMS server.</td>
</tr>
<tr>
<td></td>
<td>The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.</td>
</tr>
<tr>
<td>Shared key</td>
<td>Specify the authentication and encryption key to the RADIUS server.</td>
</tr>
<tr>
<td></td>
<td>The key is a text string that must match the encryption key used on the RADIUS server. The leading spaces are ignored, but spaces within and at the end of the key are used. If you use spaces in the key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.</td>
</tr>
<tr>
<td>Verify Shared key</td>
<td>Specify the key for verification.</td>
</tr>
</tbody>
</table>

**AAA Configuration**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable AAA for 802.1X/MAB</td>
<td>Select this check box to enable AAA for 802.1X and MAB authentication. In LMS 4.0 and LMS 4.0.1, AAA was automatically enabled for 802.1X and MAB authentication.</td>
</tr>
<tr>
<td>Enable AAA for Web Authentication</td>
<td>Select this check box to enable AAA for Web-Based Authentication (WebAuth). In LMS 4.0 and LMS 4.0.1, AAA was automatically enabled for WebAuth.</td>
</tr>
</tbody>
</table>

Or

- **RADIUS Group** radio button to specify a RADIUS server group. The RADIUS settings page appears. You can create only single RADIUS group, that can contain multiple RADIUS servers.

**Note** The order of addition is important as the first entry acts as the primary RADIUS, the second acts as the secondary, and so on.

You must enter the RADIUS Group name, Shared key, and Verify Shared key of the group. The RADIUS Server details table appears with the following fields:

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name or IP Address</td>
<td>DNS name or IP address of the RADIUS server host.</td>
</tr>
</tbody>
</table>
Chapter 2  Managing Cisco Trust and Identity Management Solutions

Configuring RADIUS

In the RADIUS Server details table, you can:

a. Click Add to add a RADIUS server.

b. Select a RADIUS server and click Edit to change its IP Address, Authentication port, or Accounting port.

c. Select a RADIUS server and click Delete to remove the RADIUS server from the RADIUS group.

d. Click Filter to view RADIUS servers based on their Server Name or IP Address, Authentication port, or Accounting port.

Step 5  Click Next. The Schedule Deployment page appears.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication port</td>
<td>Specify the port number for authentication requests.</td>
</tr>
<tr>
<td>Note</td>
<td>Authentication and Accounting port numbers cannot be the same. Do not enter the port numbers used by LMS server.</td>
</tr>
<tr>
<td></td>
<td>The host is not used for authentication if port number is set to 0. The default authorization port number is 1645.</td>
</tr>
<tr>
<td>Accounting port</td>
<td>Specify the port number for accounting requests.</td>
</tr>
<tr>
<td>Note</td>
<td>Authentication and Accounting port numbers cannot be the same. Do not enter the port numbers used by LMS server.</td>
</tr>
<tr>
<td></td>
<td>The host is not used for accounting if the port number is set to 0. The default accounting port number is 1646.</td>
</tr>
</tbody>
</table>
Provisioning Identity

Before you configure Identity using LMS, you must read the prerequisites, see Prerequisites for Configuring Identity Using LMS.

Prerequisites for Configuring Identity Using LMS

1. You must manually configure the device and user policies in the RADIUS server.
2. Config collection and inventory collection must be successful to assess the Identity readiness of your network.

Workflow for Configuring Identity

The workflow for configuring Identity on the required devices is:

1. Select devices from the list of Identity-capable devices. These devices are also RADIUS-enabled.
2. Select access port groups from the Port Selector.
3. Verify the selected devices and their ports. Unselect the ports that you want to exclude from Identity configuration.
   Using the Configuration pane, you can configure the security mode, authentication profile, related VLANs, MACsec, and enable SNMP MAC notifications. See, Configuring Identity for more information.
5. Schedule deployment. See, Scheduling Identity Configuration Jobs for more information.
Configuring Identity

To configure Identity on the devices:

**Step 1** Select **Work Centers > Identity > Configure > Enable Interfaces**. The Enable Interfaces for Identity page appears.

**Step 2** In the Select Devices and Port Groups tab, select devices from the list of Identity-capable devices, and ports groups from the Port Selector.

If you select a MACsec-capable and a MACsec-software-incapable device, a warning message appears. Table 2-4 lists the devices and images, that support MACsec.

**Step 3** Click Next. Verify the selected devices and ports.

**Step 4** Click Next. The Configuring Identity page has the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Security mode       | Select the security mode based on the level of security you wish to implement in your network. The three types of security modes are:  
• Monitor Mode  
• Low Impact Mode  
• High Security Mode  
See, **Understanding the Security Modes** for more information. |
| Associated ACL      | Enter the Associated ACL. The ACL allows selective access control, and introduces a high level of access security in the Low Impact mode.  
**Note** This ACL should be configured on the device.  
This feature allows you to restrict access, while enabling network connectivity for devices that need basic network service to function. |
| Authentication profile | Select the authentication profile from the drop-down list. The authentication profile selects the method of authentication to be used. Multi-method profiles provide a fallback order, if the first method fails, the second method will take over.  
See, **Understanding Authentication Profiles** for more information.  
**Note** You cannot configure MACsec if you select an Authentication profile that does not contain 802.1x. |
| Host Mode           | Select the host mode. It determines the number of hosts that can be authenticated on a given port. You can choose one of the following:  
• Single Host  
• Multiple Host Mode  
• Multiple Authentication  
• Multiple Domain Authentication  
See, **Understanding Host Modes** for more information. |
### Provisioning Identity

#### Chapter 2      Managing Cisco Trust and Identity Management Solutions

### Action to be taken on security violation
Select the action to be taken when a port security violation is detected due to the following reasons:
- An unauthorized device connects to a port.
- If traffic with a secure MAC address is configured on one secure port, and attempts to access another secure port in the same VLAN.
- If the maximum number of secure MAC addresses have been added to the address table and the port receives traffic from a MAC address that is not in the address table.

You can choose from the following:
- **Restrict** – When the number of secure MAC addresses reaches the maximum limit allowed on the port, packets from any new device that sends traffic to the port are dropped. When this security violation occurs a syslog message is logged.
- **Protect** – When the number of secure MAC addresses reaches the maximum limit allowed on the port, packets from any new device that sends traffic to the port are dropped. When this security violation occurs you are not notified.
- **Shutdown** – The port becomes error-disabled and shuts down immediately.
- **No Change** – No configurations will be deployed on the device.

### Local WebAuth Settings
This is an optional field.
This grid appears when you choose WebAuth as the main or fallback authentication profile. For more information, see Configuring Local WebAuth Settings.

### VLAN configuration
Specify the VLAN for dynamic VLAN provisioning.
This field appears only when you select the high security mode.

### Auth Fail VLAN
After a failed authentication, this VLAN will be applied to the port, and it is configured to grant limited access based on the type of failed authentication method.
This field appears only when you select the high security mode.

### Access VLAN
After a successful authentication, the client connecting to the port will be placed in this VLAN.
This field appears only when you select the high security mode.

### Critical VLAN
The port will be moved to this VLAN when the switch determines that the AAA server has failed during an IEEE 802.1X or MAB authentication. The range is from 1 to 4094.
This field appears only when you select the high security mode.

### Voice VLAN
After a successful authentication, the client IP phone connecting to the port will be placed in this voice VLAN.
This field appears only when you select the high security mode.

### MAC Configuration

#### MAC Move/Replace
This feature allows movement of non-Cisco phones or other intermediary devices that cannot signal a link-down event.
MAC Replace is a corrective action for the security violation that is triggered when one host replaces another authenticated host. MAC Replace takes precedence over other actions like Restrict, Protect, and Shutdown, which might be configured in this page.
For more information, see Understanding MAC Move and MAC Replace.

#### Enable MAC Move
Select this check box to allow a host to move to another port on the switch, even if an authenticated session already exists in the current port.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MAC Replace</td>
<td>Select this check box to allow a host to replace a previously authenticated host on the same port.</td>
</tr>
<tr>
<td>SNMP MAC notification</td>
<td>MAC address notification enables you to track users on a network by storing the MAC address activity on the switch. Whenever the switch learns about or removes a MAC address, an SNMP notification can be generated and sent.</td>
</tr>
<tr>
<td>Notify MAC addition</td>
<td>Select this check box to enable notification whenever a MAC address is connected to an interface.</td>
</tr>
<tr>
<td>Notify MAC removal</td>
<td>Select this check box to enable the MAC address notification whenever a MAC address is disconnected from an interface.</td>
</tr>
<tr>
<td>MACsec Configuration</td>
<td></td>
</tr>
<tr>
<td>Enable MACsec</td>
<td>Select this check box to enable MACsec on the interface. MACsec provides secure, encrypted communication on wired LANs. For more information on MACsec, see Understanding Media Access Control Security (MACsec).</td>
</tr>
<tr>
<td>Security Policy</td>
<td>Select the policy to be applied for the session after the supplicant passes 802.1x authentication. You can choose one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Optionally secure sessions</td>
</tr>
<tr>
<td></td>
<td>The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only. If MKA times out or fails, the switch will permit unencrypted traffic. This policy is the default security policy.</td>
</tr>
<tr>
<td></td>
<td>• Always secure sessions</td>
</tr>
<tr>
<td></td>
<td>The switch will attempt MKA. If MKA succeeds, the switch will send and receive encrypted traffic only. If MKA times out or fails, the switch will treat this as an authorization failure. No traffic will be allowed from the endpoint unless you configure a MACsec failure policy.</td>
</tr>
<tr>
<td></td>
<td>• Never secure sessions</td>
</tr>
<tr>
<td></td>
<td>The switch will not perform MKA. If the supplicant sends MKA protocol frames, they will be ignored. The switch will send and receive in unsecure sessions.</td>
</tr>
<tr>
<td></td>
<td>• No Change</td>
</tr>
<tr>
<td></td>
<td>If you select this option, the default policy will occur. The default policy, Optionally secure sessions, will be used.</td>
</tr>
</tbody>
</table>
### Provisioning Identity

#### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Failure Policy       | This field appears when you select Always secure sessions as the security policy. You can specify a MACsec failure policy after a failed authentication attempt. The switch will not fallback to a particular policy unless you specify it. You can choose one of the following:  
  - Re-authenticate with MAB or WebAuth  
    - After the failed authentication attempt, the switch will re-authenticate with MAB or WebAuth. This option will enabled only if the Authentication profiles are:  
      - 802.1x, then MAB, then WebAuth  
      - 802.1x, then MAB  
      - 802.1x, then WebAuth  
  - Authorize into a VLAN  
    - You can authorize a restricted VLAN on the port. When you select this option, a text box, **VLAN into which the supplicant is to be placed** appears. You can specify the VLAN ID to use when the security authentication fails.  
  - No Change  
    - If you select this option, the default action will occur. By default, denies access to the network.  

**Note** MACSec fallback policies are not the same as authentication fallback policies that you choose from the Authentication profile drop-down list.

| MKA Policy           | You must apply a defined MKA policy to the interface to enable MKA on the interface. You can choose one of the following:  
  - Default Policy  
    - Select this radio button to apply the default MKA policy that is configured on the device, to the interface.  
  - Other Policy  
    - Select this radio button to specify the MKA policy. Enter the MKA policy in the **Provide MKA Policy Name** text box. Ensure that this policy is configured on the device. If the policy is not configured on the device, you can add use the Additional configuration section to deploy the required commands on the device.  

| Advanced Options     | Select this option to enter any global commands that you want to deploy on the selected Identity-capable device, in the Adhoc Commands text box. For example, If you have selected Low Impact or High Security mode and if ACL is not configured on the device, you can enter the ACL configuration here.  

**Note** Ensure that the ACL name you enter here is the same as the one you specified earlier in the associated ACL text box. Apart from ACL, you can use this text area for any additional global commands.
Step 5 Click Next. The Schedule Deployment page appears.

The Identity configurations will be deployed on the Identity-enabled devices only when you schedule a job. See Scheduling Identity Configuration Jobs for more details.

Step 6 Click Finish. A notification message appears along with the Job ID.

The newly created job appears in the Identity Job Browser (Work Centers > Identity > Jobs). See Managing Identity Jobs for more details.

This section contains Configuring Local WebAuth Settings.

Configuring Local WebAuth Settings

The Local WebAuth Settings grid appears in the Configure Identity pane when you choose WebAuth as the main or fallback authentication profile.

This is an optional setting.

Note When you configure Local WebAuth settings in a device, you must select the Config transport setting protocol as TELNET or SSH. The Local WebAuth configurations will fail when you deploy them on the device using protocols like RCP, TFTP, and SCP.

To configure the Config transport setting protocol, select Admin > Collection Settings > Config > Config Transport Settings.

You can:

- Click Add to configure the local WebAuth settings. The Local WebAuth Settings page appears with the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Type</td>
<td>Select the type of file for centralized webpage management from the drop-down list. You can choose from the following:</td>
</tr>
<tr>
<td></td>
<td>• Login</td>
</tr>
<tr>
<td></td>
<td>• Success</td>
</tr>
<tr>
<td></td>
<td>• Failure</td>
</tr>
<tr>
<td></td>
<td>• LoginExpired</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>File Name in NGS</th>
<th>Specify a name for the type of file that you chose from the File Type list. The file in the NAC Guest Server (NGS) should have the same name. For example, if you have chosen the file type as Login, then enter Login.html as the file name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Storage Location</td>
<td>Specify the location where the files pointing to the customized web pages will be stored on the switch. For example, it can be disk1, disk0, or flash of the switch.</td>
</tr>
</tbody>
</table>
Scheduling Identity Configuration Jobs

Every configuration is deployed as a job. In many workflows, the Schedule Deployment pane appears at the end. You can schedule a job and set the job options. By default, parallel job execution order will run on the devices.

Note

Identity in LMS uses NetConfig protocol order to communicate with the device. See Defining the NetConfig Protocol Order, for more information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGS IP Address</td>
<td>Enter the IP address of the NGS server.</td>
</tr>
<tr>
<td>NGS Hotspot Name</td>
<td>Enter the name of the directory where the customized web pages will be stored on the Cisco NGS. The directory should be available in the NGS at /guest/www/html/sites/&lt;name of hotspot&gt;. For example, if you enter LWA as the NGS Hotspot Name, the files will be stored in /guest/www/html/sites/LWA.</td>
</tr>
</tbody>
</table>

Click Save, the customized web pages will be created in the specified location of the switch.

Note

LMS can create the customized web pages only on the Identity-capable switch and not on the NGS server.

You have to manually load the NGS server with these customized web pages. You have to configure some ACL commands on the switch to get the customized web pages from the NGS server.

Permit udp any any eq domain
Permit TCP any host [IP address of NAC Guest Server] eq 8443

You can enter these commands in the Adhoc Commands text box, after you enable the Advanced Options check box.

- Click Edit to edit the local WebAuth settings.
- Click Delete to delete the local WebAuth settings.
Table 2-5 describes the fields and options in the Schedule Deployment page.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Scheduler                     | Specifies when you want to run the job. Select one of the following:  
  • Immediate—Runs the job immediately.  
  • Once—Runs the job once at the specified date and time.  
  • Daily—Runs daily at the specified date and time.  
  • Weekly—Runs weekly at the specified days of the week and at the specified time.  
  • Monthly—Runs monthly at the days of the month and at the specified time. |
| Job Description               | Enter a description for the job. This is mandatory. You can enter only alphanumeric characters.                                                                                                         |
| E-mail                        | Enter e-mail addresses to which the job sends messages. You can enter multiple e-mail addresses separated by commas.                                                                                   |
| Job Options                   |                                                                                                                                                                                                             |
| Fail on Mismatch of Config Versions | Select this check box to cause the job to be considered a failure when the most recent configuration version in the configuration archive is not identical to the most recent configuration version that was in the configuration archive when you created the job. |
| Sync Archive before Job Execution | Select this check box to cause the job to archive running configuration before making configuration changes.                                                                                       |
| Copy Running Config to Startup | Select this check box to cause the job to write the running configuration to the startup configuration on each device after configuration changes are made.                                                   |
| Enable Job Password           |                                                                                                                                                                                                             |
| Login User name               | Enter the login user name to access the device. This option is available to you if you have set the appropriate job password policy in Admin > Network > Configuration Job Settings > Config Job Policies.  
  These credentials override the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module. |
| Login Password                | Enter the login password to access the device. This option is available to you if you have set the appropriate job password policy in Admin > Network > Configuration Job Settings > Config Job Policies.  
  These credentials override the credentials that you have entered at the time of adding the device in the Device and Credentials Administration module. |
Scheduling Identity Configuration Jobs

Chapter 2  Managing Cisco Trust and Identity Management Solutions

Table 2-5  Fields in the Schedule Deployment Page Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Password</td>
<td>Enter the Enable password to access the device. This option is available to</td>
</tr>
<tr>
<td></td>
<td>you if you have set the appropriate job password policy in Admin &gt; Network &gt;</td>
</tr>
<tr>
<td></td>
<td>Configuration Job Settings &gt; Config Job Policies. These credentials override</td>
</tr>
<tr>
<td></td>
<td>the credentials that you have entered at the time of adding the device in the</td>
</tr>
<tr>
<td></td>
<td>Device and Credentials Administration module.</td>
</tr>
<tr>
<td>Failure Policy</td>
<td>Select one of these options to specify what the job should do if it fails to</td>
</tr>
<tr>
<td></td>
<td>run on a device.</td>
</tr>
<tr>
<td></td>
<td>• Stop on failure—If the job fails to execute on a device, the job is</td>
</tr>
<tr>
<td></td>
<td>stopped. The database is updated only for the devices on which the job</td>
</tr>
<tr>
<td></td>
<td>was executed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Ignore failure and continue—If the job fails on a device, the job skips</td>
</tr>
<tr>
<td></td>
<td>the device and continues with the remaining devices. The database is</td>
</tr>
<tr>
<td></td>
<td>updated only for the devices on which the job was executed successfully.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and stop—Rolls back the changes on the failed device</td>
</tr>
<tr>
<td></td>
<td>and stops the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback device and continue—Rolls back the changes on the failed device</td>
</tr>
<tr>
<td></td>
<td>and continues the job.</td>
</tr>
<tr>
<td></td>
<td>• Rollback job on failure—Rolls back the changes on all devices and</td>
</tr>
<tr>
<td></td>
<td>stops the job.</td>
</tr>
</tbody>
</table>

- Click Preview CLI to see the CLI commands that will be applied to the Identity devices. You can select a device from the Preview CLI pop-up and see the CLI commands.
  You can modify an instance of a configuration task (and its configuration commands) at any time before the job is scheduled.
- Click Finish after you review the CLI commands.
  A notification message appears along with the Job ID. The newly created job appears in the Identity Job Browser (Work Centers > Identity > Jobs). See Managing Identity Jobs for more details.
Defining the NetConfig Protocol Order

To define or modify the NetConfig protocol order:

**Step 1** Select Admin > Collection Settings > Config > Config Transport Settings. The Transport Settings page appears.

**Step 2** Select NetConfig from the Application drop-down list.

**Step 3** Select a protocol from the Available Protocols pane and click Add.

If you want to remove a protocol or change the protocol order, you must remove the protocol using the Remove button and add the protocol again.

The list of protocols that you have selected appears in the Selected Protocol Order pane.

**Step 4** Click Apply.

A message appears, New settings saved successfully.

**Step 5** Click OK.

Identity Readiness Assessment

The Identity Readiness Assessment (Work Centers > Identity > Readiness Assessment) displays Identity based device details after assessing the network. A pie chart appears with the following types of devices:

- Identity-capable Devices
- Identity-software-incapable Devices
- Radius-capable Devices
- Identity-hardware-incapable Devices

Click any section of the pie chart to view the details of the devices.

Config collection and inventory collection must be successful to assess the Identity readiness of your network.

**Note** You need Adobe flash player 9 or later to display the readiness assessment pie chart. You can install the flash player from LMS. Reload the page after installing the flash player.

Identity-capable Devices

Click the Identity-capable devices slice in the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices have Identity-capable IOS images, but Identity is not yet configured on these devices. RADIUS is enabled on these devices.

Select one or more devices and click Enable Identity to configure Identity on the selected devices. See, Configuring Identity for more details.
Identity-software-incapable Devices

Click the Identity-software-incapable devices slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices do not have the Identity-capable IOS images. You can upgrade to the Identity-capable image version. See Supported Devices and Images for Identity for more information.

Select one or more devices and click Upgrade Software Image to upgrade to the Identity-capable IOS image.

Radius-capable Devices

Click the Radius-capable devices slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices have RADIUS-capable IOS images, but RADIUS is not configured on these devices.

Select one or more devices and click Configure RADIUS to configure RADIUS and AAA settings on the selected devices. See Configuring RADIUS for more details.

Note
If a device has the Identity-capable IOS image, and RADIUS is not configured on it, the device will appear as a RADIUS-capable and not an Identity-capable device.

Identity-hardware-incapable Devices

Click the Identity-hardware-incapable devices slice of the pie chart. The details of the corresponding devices appear at the bottom of the page. These devices do not have the provision for Identity technology. You can upgrade the devices with the latest Identity-supported hardware from Cisco.com.

See Supported Devices and Images for Identity for more information.

See Known List of Hardware-incapable Devices for more information.
Managing Identity Devices

You can view the Identity security mode distribution in your network as a pie chart. You can select a section of the pie to view the ports of devices configured in the respective security mode. The corresponding table appears at the bottom of the page.

**Step 1** Select Work Centers > Identity > Configure > Manage Identity Devices.

The Identity security mode pie chart appears. Select a section of the pie to view the devices and the ports configured in the respective security mode. For more information on security modes, see Understanding the Security Modes.

**Step 2** Select the device from the table and:

- Change the security mode of any device. See, Configuring Identity for more details.
  
  Or

- Disable Identity for any device. See, Disabling Identity for more details.

You can click the count to view details of the ports configured in the chosen security mode.

Disabling Identity

You can select a device and disable Identity, RADIUS, or a specific RADIUS group. Identity cannot be disabled for the ports that are in unsecured mode.

To do this:

**Step 1** Select Work Centers > Identity > Configure > Manage Identity Devices. The Identity security mode pie chart appears. Select a slice of the pie to view the devices configured in the respective security mode.

**Step 2** Select the device from the table and click Disable Identity. The Disable Identity page appears.

**Step 3** Select the check box next to the feature you want to disable. The different options are:

- Disable Identity
- Disable security mode
- Disable authentication
- Disable host modes
- Disable security violation
- Fallback policies (Critical and AuthFail VLAN)
- Disable SNMP MAC Notification
- Disable MACsec
- Disable RADIUS
- Disable RADIUS Hosts
- Disable RADIUS Groups

If you select Disable RADIUS hosts, you must enter the name of the RADIUS host that you want to remove. If you select Disable RADIUS Groups, you must enter the name of the RADIUS group that you want to remove.
Step 4  Click Next. The Schedule Deployment page appears.

The Identity configurations will be deployed on the Identity-enabled devices only when you schedule a job. See Scheduling Identity Configuration Jobs for more details.

Step 5  Click Finish. A notification message appears along with the Job ID.

The newly created job appears in the Identity Job Browser (Work Centers > Identity > Jobs). See Managing Identity Jobs for more details.

---

**Monitoring Identity**

For LMS to monitor Identity, User Tracking acquisition should be successful. After a successful UT, Identity collection occurs and the data is available through Identity portlets and reports. The data is not be dynamically updated, and depends on the User Tracking acquisition schedule. For more details on User Tracking, see User Tracking and Dynamic Updates in Administration Online Help.

If you want dynamic updates in the Identity portlets and reports, you should configure Dynamic UT. LMS will query the CISCO-AUTH-FRAMEWORK-MIB on Identity-enabled device and get details for generating Identity reports.

You can monitor Identity using the following reports:

- Authenticated Users
- Authentication Failure
- Authorized Users
- Authorization Failure
- User-specific

For more information see Technology Report in Reports Management with Cisco Prime LAN Management Solution 4.1 User Guide.

You can also use Identity portlets to monitor the Identity-related information, in your network. For more information, see Understanding the Identity Dashboard.
Managing Identity Jobs

You can browse the Identity jobs that are deployed on the system. Using the Identity Job Browser you can manage Identity jobs; you can stop, refresh, or delete jobs using this job browser.

To invoke the Identity job browser:

Select **Work Centers > Identity > Identity Jobs.**

The Identity job browser appears with a detailed list of all scheduled Identity jobs. The browser has the following information:

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Unique number assigned to job when it is created. For periodic</td>
</tr>
<tr>
<td></td>
<td>jobs such as Daily, and Weekly, the job IDs are in the number.x</td>
</tr>
<tr>
<td></td>
<td>format. The x represents the number of instances of the job. For</td>
</tr>
<tr>
<td></td>
<td>example, 1001.3 indicates that this is the third instance of the</td>
</tr>
<tr>
<td></td>
<td>job ID 1001.</td>
</tr>
<tr>
<td></td>
<td>Click on the hyperlink to view the Job details (see Viewing Job</td>
</tr>
<tr>
<td></td>
<td>Details).</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the job:</td>
</tr>
<tr>
<td></td>
<td>• Successful—When the job is successful.</td>
</tr>
<tr>
<td></td>
<td>• Failed—When the job has failed.</td>
</tr>
<tr>
<td></td>
<td>The number, within brackets, next to Failed status indicates the</td>
</tr>
<tr>
<td></td>
<td>count of the devices that had failed for that job. This count is</td>
</tr>
<tr>
<td></td>
<td>displayed only if the status is Failed.</td>
</tr>
<tr>
<td></td>
<td>For example, If the status displays Failed(5), then the count of</td>
</tr>
<tr>
<td></td>
<td>devices that had failed amounts to 5.</td>
</tr>
<tr>
<td></td>
<td>• Stopped—When the job has been stopped.</td>
</tr>
<tr>
<td></td>
<td>• Running—When the job is in progress.</td>
</tr>
<tr>
<td></td>
<td>• Waiting—When the job is awaiting approval (if job approval has</td>
</tr>
<tr>
<td></td>
<td>been enabled).</td>
</tr>
<tr>
<td></td>
<td>• Rejected—When the job has been rejected (if job approval has</td>
</tr>
<tr>
<td></td>
<td>been enabled).</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the job, entered at the time of job creation.</td>
</tr>
<tr>
<td>Owner</td>
<td>Username of the job creator.</td>
</tr>
<tr>
<td>Scheduled at</td>
<td>Date and time at which the job was scheduled.</td>
</tr>
<tr>
<td>Completed at</td>
<td>Date and time at which the job was completed.</td>
</tr>
<tr>
<td>Schedule Type</td>
<td>Type of job schedule—Immediate, Once, Daily, Weekly, Monthly.</td>
</tr>
<tr>
<td></td>
<td>For periodic jobs, the subsequent instances of periodic jobs will</td>
</tr>
<tr>
<td></td>
<td>run only after the earlier instance of the job is complete.</td>
</tr>
<tr>
<td></td>
<td>For example: If you have scheduled a daily job at 10:00 a.m. on</td>
</tr>
<tr>
<td></td>
<td>November 1, the next instance of this job will run at 10:00 a.m.</td>
</tr>
<tr>
<td></td>
<td>on November 2 only if the earlier instance of the November 1 job</td>
</tr>
<tr>
<td></td>
<td>has completed. If the 10:00 a.m. November 1 job has not been</td>
</tr>
<tr>
<td></td>
<td>completed before 10:00 a.m. November 2, then the next job will</td>
</tr>
<tr>
<td></td>
<td>start only at 10:00 a.m. on November 3.</td>
</tr>
</tbody>
</table>

You can filter the jobs displayed in the Identity Job Browser using any of the following criteria and clicking **Filter.** When you click **Filter,** you can select any of the following criteria from the Filter by drop-down list; enter the details in the text box; and click **Go.**
### Managing Identity Jobs

You can click Refresh icon to refresh the Identity job browser, and Refresh Job icon to refresh the selected Identity job.

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job ID</td>
<td>Select Job ID and enter the Job IDs that you want to display. For a non-periodic job, the specified Job ID appears in the browser. For periodic jobs, all the instances of the selected Job ID will also be displayed in the browser.</td>
</tr>
</tbody>
</table>
| Status          | Select Status and then enter any one of these:  
  - Successful  
  - Failed  
  - Stopped  
  - Running  
  - Scheduled  
  - Approved  
  - Waiting  
  - Rejected |
| Description     | Select Description and enter the complete description. |
| Owner           | Select Owner and enter the full name. |
| Scheduled at    | Select Scheduled at and enter the date and time at which the job was scheduled. |
| Completed at    | Select Completed at and enter the date and time at which the job was completed. |
| Schedule Type   | Select the schedule type and enter any one of these:  
  - Immediate  
  - Once  
  - Daily  
  - Weekly  
  - Monthly |
You can perform the following operations using the Identity job browser. (See Table 2-6):

**Table 2-6 Operations Using the Identity Job Browser**

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stop</td>
<td>Stops or cancels a running job. You can stop or cancel a running job. You will be asked to confirm the cancellation of the job. However, the job will be stopped only after the devices currently being processed are successfully completed. This is to ensure that no device is left in an inconsistent state. If the job that you want to stop is a periodic job, you will also be asked whether you want to cancel all the instances of the job. Click OK to cancel all instances. If you click Cancel, only the selected instance of the job is cancelled. The next instance of the job will appear in the Job browser with the status Scheduled. Unless you own the job, your login determines whether you can use this option. You cannot restart the stopped job.</td>
</tr>
<tr>
<td>Delete</td>
<td>Deletes the selected job from the job browser. You can select more than one job to delete. You will be asked to confirm the deletion. If the job that you have selected for deletion is a periodic job, this message appears: If you delete periodic jobs, or instances of a periodic job, that are yet to be run, the jobs will no longer run, nor will they be scheduled to be run again. You must then recreate the deleted jobs. Do you want to continue? Click OK to confirm the deletion. The job, and its instances will be deleted. You can delete a job that has been successful, failed, or stopped, but you cannot delete a running job. Unless you own the job, your login determines whether you can use this option. You must stop a running job before you can delete it.</td>
</tr>
<tr>
<td>Refresh</td>
<td>Refreshes the Identity job browser.</td>
</tr>
<tr>
<td>Refresh Job</td>
<td>Refreshes the job and you can see the current status of the job.</td>
</tr>
</tbody>
</table>

**Viewing Job Details**

From the Job Browser dialog box, you can learn more about any job by viewing its details. Select a job to view its details.

The Job Details appears below the list of Identity jobs. The details are grouped into three parts:

- Work Order
- Device Details
- Job Summary
### Page/Folder Description

#### Work Order
Displays general information about the job:
- Job policies
- Job approval details (if you have enabled job approval)
- Device details
- Task
- CLI commands that will be executed on the selected devices as part of this job

#### Device Details
Contains detailed job results for each device in a table:
- Device—List of devices on which the job ran.
- Status—Status of job (success, failure, etc.)
- Message—A message about the status of a job.
  - If the job failed on the device, the reason for failure is displayed.
  - If the job was a success on that device, the message *Deploy Successful* is displayed.

You can filter the devices by selecting a status and clicking **Filter**.

You can navigate among the pages of the report using the navigation icons at the right bottom of this table.

Click on a device to view the details such as protocol, status and reason when applicable, task used, and the CLI output for that device. These details appear in a pop-up window.

Double-click to display status folders that correspond to possible device status.

#### Job Summary
Click to display summary of completed job:
- Job Summary:
  - Status
  - Start Time
  - End Time
- Job Messages:
  - Pre-job Execution
  - Post-job Execution
- Device Update:
  - Successful
  - Failed
  - Not attempted
  - Pending