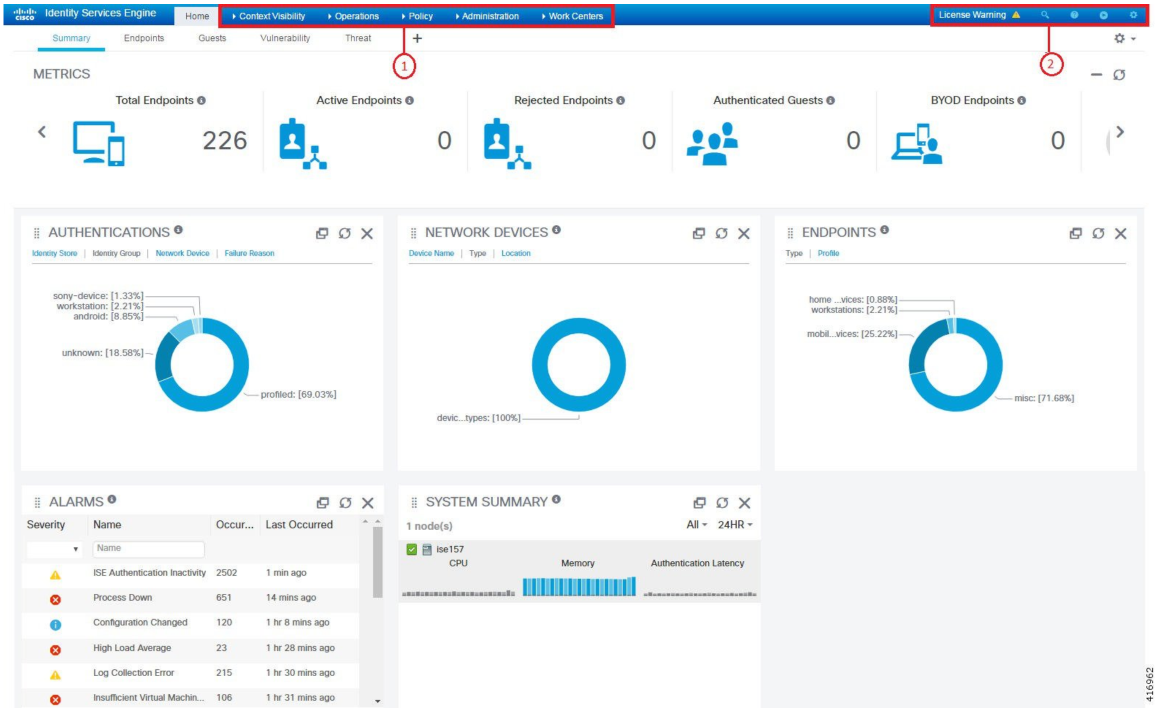
Administration Portal

The administration portal provides access to Cisco ISE configuration and reporting. The following figure shows the main elements of the menu bar of the administration portal.

Figure 1: Cisco ISE Administration Portal



Severity	Name	Occur...	Last Occurred
⚠	ISE Authentication Inactivity	2502	1 min ago
⊗	Process Down	651	14 mins ago
ⓘ	Configuration Changed	120	1 hr 8 mins ago
⊗	High Load Average	23	1 hr 28 mins ago
⚠	Log Collection Error	215	1 hr 30 mins ago
⊗	Insufficient Virtual Machin...	106	1 hr 31 mins ago

Table 1: Components of the Cisco ISE Administration Portal

1	Menu Drop-downs	The menu options on the left pane are: • **Context Visibility**: The context visibility windows display information about endpoints, users, and network access devices (NAD). The context visibility information is grouped by features, applications, Bring Your Own Device (BYOD), and other categories, depending on the licenses you have registered. The context visibility windows use a central database and gather information from database tables, caches, and buffers. As a result, the content in the context visibility dashlets and lists gets updated quickly. The context visibility windows consist of dashlets at the top, and a list of information at the bottom. When you filter data by modifying the column attributes in the list, the dashlets get refreshed and display the modified content. • **Operations**: Operations windows include tools to view RADIUS, TACACS+, and TC-NAC Live Logs, the Adaptive Network Control (ANC) policy, and troubleshooting options to diagnose and debug issues related to Cisco ISE deployments. • **Policy**: Policy windows include tools for managing network security in the areas of authentication, authorization, profiling, posture, and client provisioning. • **Administration**: Administration windows include tools for managing Cisco ISE nodes, licenses, certificates, network devices, users, endpoints, and guest services. • **Work Centers**: Work Centers list the following expandable submenus. These submenus act as a single starting point for Cisco ISE administrators, to configure relevant features within a Cisco ISE deployment. • **Network Access** • **Guest Access** • **TrustSec** • **BYOD** • **Profiler** • **Posture** • **Device Administration** • **PassiveID**

2	Top-Right Menu Icons	

- 🔍

  Use this icon to search for endpoints and display their distribution by profiles, failures, identity stores, location, device type, and so on.

- ?

  Click this icon for a drop-down list that allows you to access the online help for the currently displayed page, and links to the Cisco ISE Community, Portal Builder, and more.

- Click this icon to access the following options:

  - **PassiveID Setup**: The **PassiveID Setup** option launches the **PassiveID Setup** wizard to set up passive identity using Active Directory. Configure the server to gather user identities and IP addresses from external authentication servers and deliver the authenticated IP addresses to the corresponding subscriber.

  - **Visibility Setup**: **Visibility Setup** is a Proof of Value (PoV) service that collects endpoint data such as applications, hardware inventory, USB status, firewall status, and the overall compliance state of Windows endpoints. The collected data is then sent to Cisco ISE. When you launch the **ISE Visibility Setup** wizard, it allows you to specify an IP address range to run endpoint discovery for a preferred segment of the network or a group of endpoints.

    The PoV service uses the Cisco Stealth Temporal agent to collect endpoint posture data. Cisco ISE pushes the Cisco Stealth Temporal agent to computers running Windows with an Administrator account type, which automatically runs a temporary executable file to collect context. The agent then removes itself. To experience the optional debug capabilities of Cisco Stealth Temporal agent, check the **Endpoint Logging** check box (**Visibility Setup** > **Posture**) to save the debug logs in an endpoint or multiple endpoints. You can view the logs in either of the following locations:

    - C:\WINDOWS\syswow64\config\systemprofile\ (64-bit operating system)

    - C:\WINDOWS\system32\config\systemprofile\ (32-bit operating system)

  - **Wireless Setup (BETA)**: The **Wireless Setup (BETA)** option provides an easy way to set up wireless flows for 802.1X, Guest services, and BYOD. This option also provides workflows to configure and customize each portal for Guest services and BYOD.

- ⚙

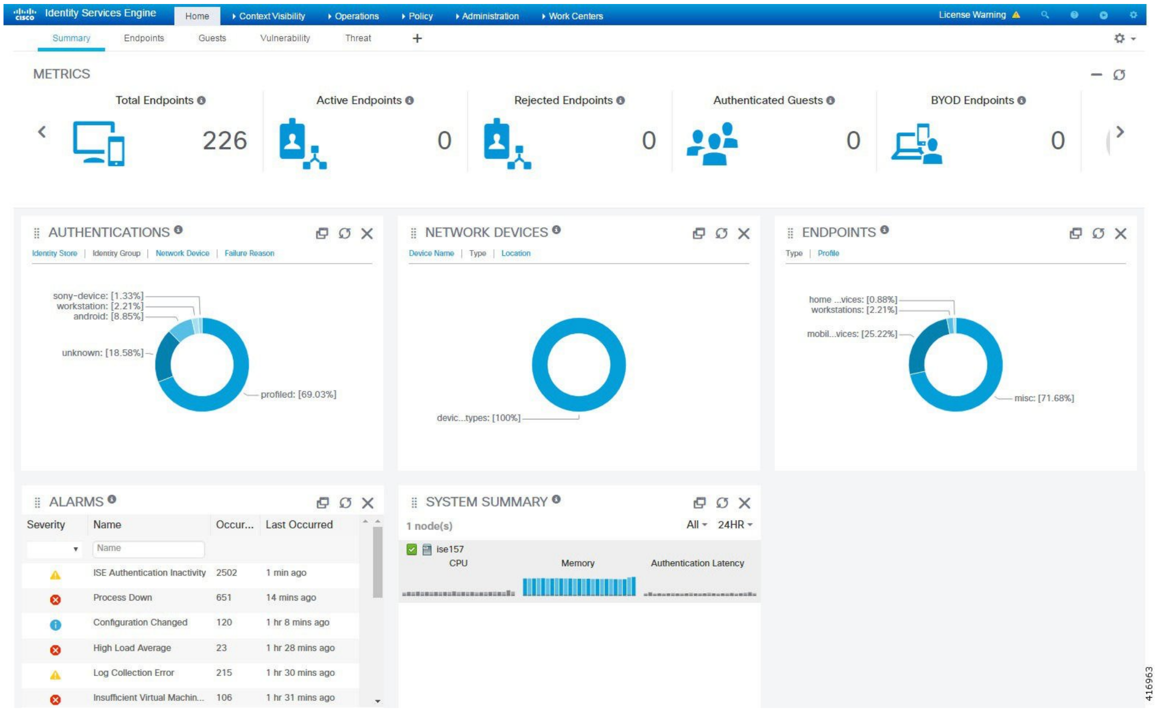
		Click this icon for a menu of system activities, including launching online help, and configuring account settings.

- Cisco ISE Home Dashboards, on page 5
- Configuring Home Dashboards, on page 6
- Context Visibility Views, on page 7
- Dashlets, on page 13
- Filtering Displayed Data in a View, on page 14
- Create Custom Filters, on page 17
- Filter Data by Conditions Using the Advanced Filter, on page 17
- Filter Data by Field Attributes Using the Quick Filter, on page 17
- Endpoint Actions in Dashlet Views, on page 18
- Cisco ISE Dashboard, on page 18
- Cisco ISE Internationalization and Localization, on page 21
- MAC Address Normalization, on page 27
- Cisco ISE Deployment Upgrade, on page 27

Cisco ISE Home Dashboards

The Cisco ISE Home dashboard displays live consolidated and correlated statistical data that is essential for effective monitoring and troubleshooting. Dashboard elements typically display activity over 24 hours. The following figure is an example of the information available in a Cisco ISE dashboard. You can view the Cisco ISE dashboard data only in the primary Policy Administration node (PAN) portal.

Figure 2: Cisco ISE Home Dashboard



Severity	Name	Occur...	Last Occurred
	Name		
⚠	ISE Authentication Inactivity	2502	1 min ago
⊗	Process Down	651	14 mins ago
ⓘ	Configuration Changed	120	1 hr 8 mins ago
⊗	High Load Average	23	1 hr 28 mins ago
⚠	Log Collection Error	215	1 hr 30 mins ago
⊗	Insufficient Virtual Machin...	106	1 hr 31 mins ago

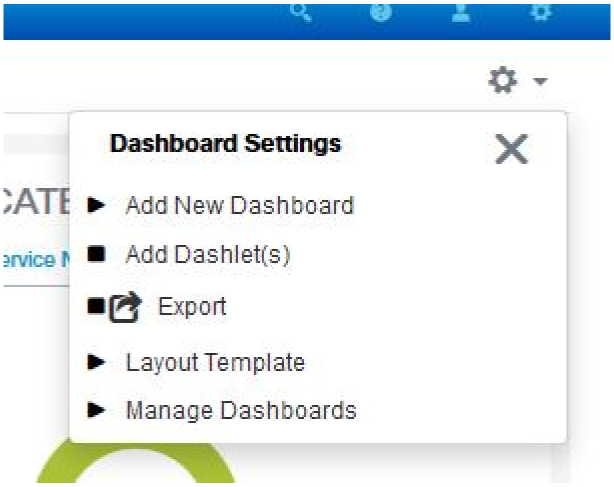
The home page has five default dashboards that display your Cisco ISE data. Each of these dashboards has several predefined dashlets.

- **Summary**: This dashboard contains a linear metrics dashlet, pie chart dashlets, and list dashlets. The metrics dashlet is not configurable. By default this dashboard contains the dashlets **Status Endpoints**, **Endpoint Categories**, and **Network Devices**.
- **Endpoints**: By default, this dashboard contains the dashlets **Status**, **Endpoints**, **Endpoint Categories**, and **Network Devices**.
- **Guests**: This dashboard contains dashlets that provide information on guest user type, log in failures, and location of acitivity.
- **Vulnerability**: This dashboard displays the information that vulnerability servers report to Cisco ISE.
- **Threat**: This dashboard displays information from the threat servers reports sent to Cisco ISE.

Configuring Home Dashboards

You can customize a home page dashboard by clicking the **Gear** icon in the top right corner of the window:

Figure 3: Customize A Dashboard



The following options are displayed in the drop-down list:

- **Add New Dashboard** allows you to add a new dashboard. Enter a value in the field that is displayed and click **Apply**.
- **Add Dashlet(s)** displays a dialog box with a list of dashlets available. Click **Add** or **Remove** next to the dashlet name to add or remove a dashlet from the dashboard.
- **Export** saves the selected home page view to a PDF.
- **Layout Template** configures the number of columns that are displayed in this view.
- **Manage Dashboards** contains two options:
  - **Mark As Default Dashboard**: Choose this option to make the current dashboard the default view when you choose Home.

- **Reset All Dashboards**: Use this option to also reset all the dashboards and remove your configurations on all the Home dashboards.

Context Visibility Views

The structure of a **Context Visibility** window is similar to the home page, except that the Context Visibility windows:

- Retain your current context (browser window) when you filter the displayed data
- Are more customizable
- Focus on endpoint data

You can view the context visibility data only from the primary PAN.

Dashlets on the **Context Visibility** windows show information about endpoints, and endpoint connections to NADs. The information currently displayed is based on the content in the list of data below the dashlets on each window. Each window displays endpoint data, based on the name of the tab. As you filter the data, both the list and dashlets update. You can filter the data by clicking on parts of one or more of the circular graphs, by filtering rows on the table, or any combination those actions. As you select filters, the effects are additive, also referred to as cascading filter, which allows you to drill down to find the particular data you are looking for. You can also click an endpoint in the list, and get a detailed view of that endpoint.

We recommend that you enable the accounting settings on the network access devices (NADs) to ensure that the accounting start and update information is sent to Cisco ISE.

Cisco ISE can collect accounting information, such as the latest IP address, status of the session (Connected, Disconnected, or Rejected), the number of days an endpoint has been inactive, only if accounting is enabled. This information is displayed in the **Live Logs**, **Live Sessions** and **Context Visibility** windows in the Cisco ISE administration portal. When accounting is disabled on a NAD, there might be a missing, incorrect, or mismatched accounting information between the **Live Sessions**, **Live Logs** and **Context Visibility** windows.

There are four main views under **Context Visibility**:

- **Endpoints**: Filter the endpoints you want to view based on types of devices, compliance status, authentication type, hardware inventory, and more. See The Hardware Dashboard, on page 11 for additional information.

Note The **Visibility Setup** workflow that is available on the Cisco ISE administration portal home page allows you to add a list of IP address ranges for endpoints discovery. After this workflow is configured, Cisco ISE authenticates the endpoints, but the endpoints that are not included in the configured IP address ranges are not displayed in the **Context Visibility** > **Endpoints** window and the **Endpoints** listing page (**Work Centers** > **Network Access** > **Identities** > **Endpoints**).

- **Users**: Displays user-based information from user identity sources.

  If there is a change in the username or password attribute, it reflects in the **Users** window when there is a change in the authentication status.

If the username is changed in the Microsoft Active Directory, the updated change is displayed in the **Users** window immediately after re-authentication.

If any other attributes such as Email, Phone, Department, etc are changed in the Microsoft Active Directory, the updated attributes are displayed in the **Users** window 24 hours after re-authentication.

Note Updating User Attributes from AD depends on the interval configured under Active Directory Probe. For more information, see Active Directory Probe.

- **Network Devices**: This window displays the list of NADs that have endpoints connected to them. For any NAD, click the number of endpoints that is displayed in the corresponding **# of endpoints** column. A window that lists all the devices filtered by that NAD is displayed.

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 Cisco ISE 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.

- **Application**: Use this window to identify the number of endpoints that have a specific application installed. The results are displayed in graphical and table formats. The graphical representation helps you make a comparative analysis. For example, you can find out the number of endpoints with the Google Chrome software along with their Version, Vendor, and Category (Anti-phishing, Browser, and so on) in a table as well as a bar chart. For more information, see The Application Dashboard.

You can create a new tab in the **Context Visibility** windows and create a custom list for additional filtering. Dashlets are not supported in custom views.

Click a section of a circular graph in a dashlet to view a new window with filtered data from that dashlet in. From this new window, you can continue to filter the displayed data, as described in Filtering Displayed Data in a View, on page 14.

For more information about using Context Visibility windows to find endpoint data, see the following Cisco YouTube video https://www.youtube.com/watch?v=HvonGhrydfg.

Related Topics

The Hardware Dashboard, on page 11

Attributes in Context Visibility

The systems and services that provide attributes for Context Visibility sometimes have different values for the same attribute name. The following are a few examples:

For Operating System

- *OperatingSystem*: Posture operating system.
- *operating-system*: NMAP operating system.

- *operating-system-result*: Profiler consolidated operating system.

Note There might be some discrepancies in the endpoint operating system data that is displayed in the Context Visibility window when you enable multiple probes in Cisco ISE for an endpoint.

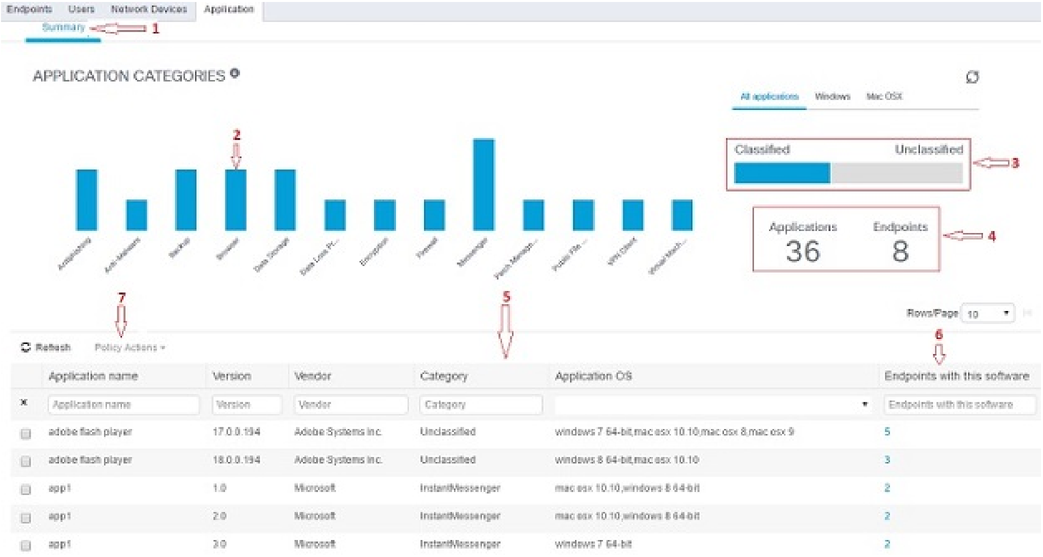
For Portal Name

- *Portal.Name*: Guest portal name when device registration is turned on.
- *PortalName*: Guest portal name when device registration is not turned on.

For Portal User

- *User-Name*: Username from RADIUS authentication.
- *GuestUserName*: Guest username.
- *PortalUser*: Portal username.

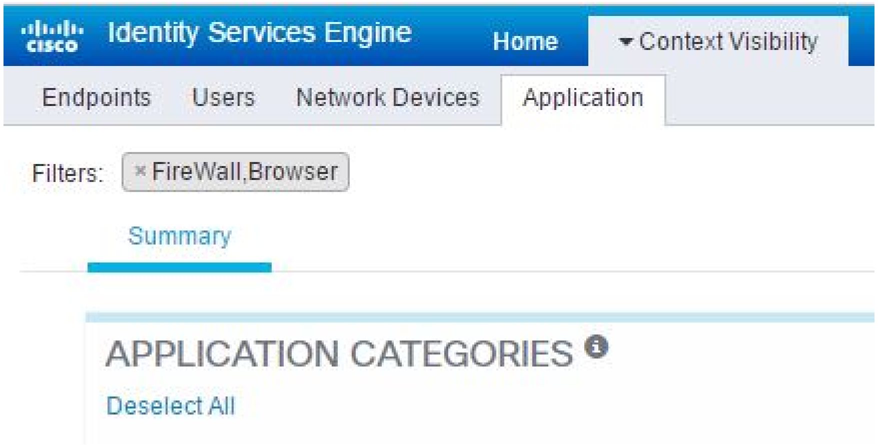
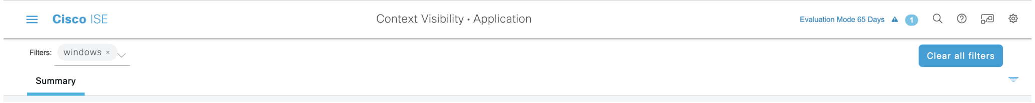
The Application Dashboard



	Application name	Version	Vendor	Category	Application OS	Endpoints with this software
×	Application name	Version	Vendor	Category		Endpoints with this software
□	adobe flash player	17.0.0.194	Adobe Systems Inc.	Unclassified	windows 7 64-bit,mac osx 10.10,mac osx 8,mac osx 9	5
□	adobe flash player	18.0.0.194	Adobe Systems Inc.	Unclassified	windows 8 64-bit,mac osx 10.10	3
□	app1	1.0	Microsoft	InstantMessenger	mac osx 10.10,windows 8 64-bit	2
□	app1	2.0	Microsoft	InstantMessenger	mac osx 10.10,windows 8 64-bit	2
□	app1	3.0	Microsoft	InstantMessenger	windows 7 64-bit	2

Table 2: Description of the Application Dashboard

Label	Description
1	The **Summary** tab is displayed by default on the home page. It displays the **Application Categories** dashlet, which contains a bar chart. Applications are classified into 13 categories. Applications that do not fall into any of these categories are grouped as **Unclassified**. The available categories are Anti-Malware, Antiphishing, Backup, Browser, Data Loss Prevention, Data Storage, Encryption, Firewall, Messenger, Patch Management, Public File Sharing, Virtual Machine, and VPN Client.

Label	Description
2	Each bar corresponds to a classified category. Hover over each bar to view the total number of applications and endpoints that correspond to the selected application category.
3	The applications and endpoints that fall under the Classified category are displayed in blue. Unclassified applications and endpoints are displayed in gray. Hover over the classified or unclassified category bars to view the total number of applications and endpoints that belong to that category. You can click **Classified** and view the results in the bar chart and table in the window. When you click **Unclassified**, the bar chart is disabled and the results are displayed in the table in the window.
4	The applications and endpoints are displayed based on the selected filter. You can view the breadcrumb trail as you click different filters. You can click **Deselect All** to remove all the applied filters.  Identity Services Engine Home Context Visibility Endpoints Users Network Devices Application Filters: × FireWall,Browser Summary APPLICATION CATEGORIES Deselect All  Cisco ISE Context Visibility • Application Evaluation Mode 65 Days 1 Filters: windows × Clear all filters Summary

<table>
<tr><th>Label</th><th colspan="6">Description</th></tr>
<tr><td rowspan="5">5</td><td colspan="6">When you click multiple bars, the corresponding classified applications and endpoints are displayed in the table. For example, if you select the Antimalware and Patch Management categories, the following results are displayed:</td></tr>
<tr><td><b>Application Name</b></td><td><b>Version</b></td><td><b>Vendor</b></td><td><b>Category</b></td><td><b>Application OS</b></td><td><b>Endpoints With This Software</b></td></tr>
<tr><td>Gatekeeper</td><td>9.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>windows 7 64-bit,mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
<tr><td>Gatekeeper</td><td>10.9.5</td><td>Apple Inc.</td><td>Antimalware</td><td>Windows 8 64-bit, mac osx 10.10</td><td>3</td></tr>
<tr><td>Software Update</td><td>2.3</td><td>Apple Inc.</td><td>Patch Management</td><td>Windows 7 64 bit, mac osx 10.10,mac osx 8,mac osx 9</td><td>5</td></tr>
<tr><td>6</td><td colspan="6">Click an endpoint in the <b>Endpoints With This Software</b> column in the table to view the endpoint details, such as Mac address, NAD IP address, NAD port ID/SSID, IPv4 address, and so on.</td></tr>
<tr><td>7</td><td colspan="6">You can select an application name and choose the <b>Create App Compliance</b> option from the <b>Policy Actions</b> drop-down list to create application compliance condition and remediation.</td></tr>
</table>

The Hardware Dashboard

The endpoint hardware tab under context visibility helps you collect, analyze, and report endpoint hardware inventory information within a short time. You can gather information, such as finding endpoints with low memory capacity or finding the BIOS model/version in an endpoint. You can increase the memory capacity or upgrade the BIOS version based on these findings. You can assess the requirements before you plan the purchase of an asset. You can ensure timely replacement of resources. You can collect this information without installing any modules or interacting with the endpoint. In summary, you can effectively manage the asset lifecycle.

Note The hardware inventory data takes 120 seconds to be displayed in the ISE GUI. The hardware inventory data is collected for posture compliant and non-compliant states.

The **Context Visibility** > **Endpoints** > **Hardware** page displays the **Manufacturers** and **Endpoint Utilizations** dashlets. These dashlets reflect the changes based on the selected filter. The **Manufacturers** dashlet displays hardware inventory details for endpoints with Windows and Mac OS. The **Endpoint Utilizations** dashlet displays the CPU, Memory, and Disk utilization for endpoints. You can select any of the three options to view the utilization in percentage.

- Devices With Over n% CPU Usage.

- Devices With Over n% Memory Usage.
- Devices With Over n% Disk Usage.

The hardware attributes of an endpoint and their connected external devices are displayed in a table format. The following hardware attributes are displayed:

- MAC Address
- BIOS Manufacturer
- BIOS Serial Number
- BIOS Model
- Attached Devices
- CPU Name
- CPU Speed (GHz)
- CPU Usage (%)
- Number of Cores
- Number of Processors
- Memory Size (GB)
- Memory Usage (%)
- Total Internal Disk(s) Size (GB)
- Total Internal Disk(s) Free Size (GB)
- Total Internal Disk(s) Usage (%)
- Number of Internal Disks
- NAD Port ID
- Status
- Network Device Name
- Location
- UDID
- IPv4 Address
- Username
- Hostname
- OS Types
- Anomalous Behavior
- Endpoint Profile
- Description

- Endpoint Type
- Identity Group
- Registration Date
- Identity Store
- Authorization Profile

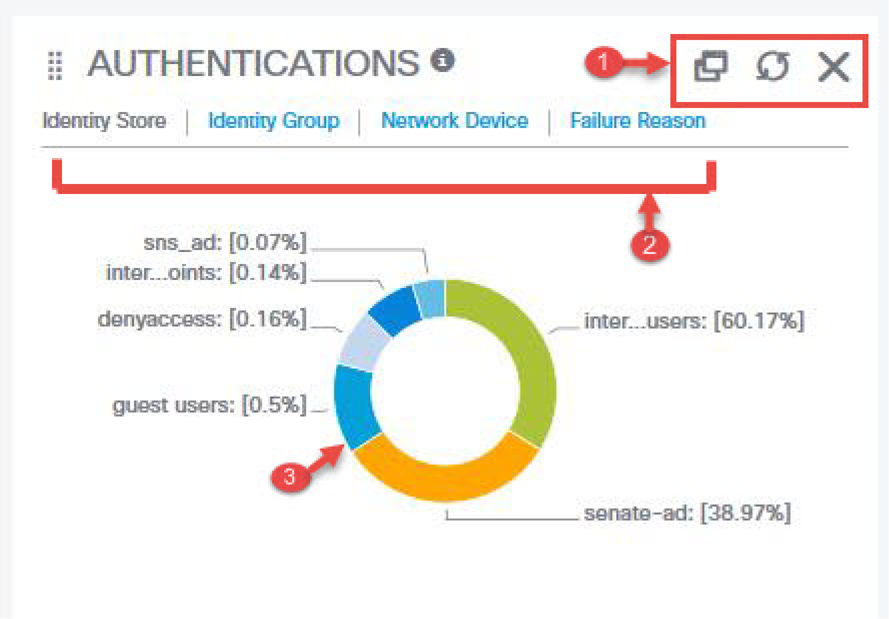
You can click the number in the **Attached Devices** column that corresponds to an endpoint to view the Name, Category, Manufacturer, Type, Product ID, and Vendor ID of the USB devices that are currently attached to the endpoint.

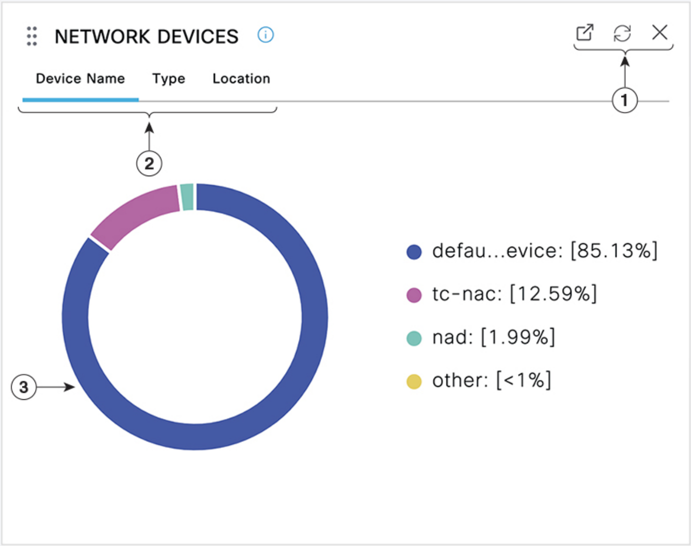
Note Cisco ISE profiles the hardware attributes of a client's system, however, there may be a few hardware attributes Cisco ISE does not profile. These hardware attributes may not appear in the Hardware Context Visibility page.

The hardware inventory data collection interval can be controlled in the **Administration** > **System** > **Settings** > **Posture** > **General Settings** page. The default interval is 5 minutes.

Dashlets

The following image is an example of a dashlet:





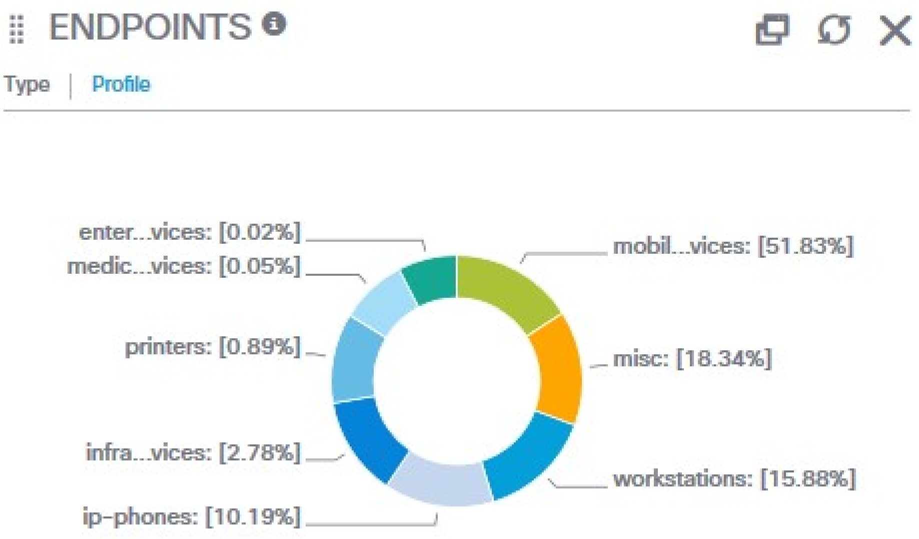
1. The stacked window symbol “detaches”,Open New Window icon opens this dashlet in a new browser window. The pie chart refreshes. Click the **X** to delete this dashlet. This option is only available on the home page. You delete dashlets in Context Visibility windows using the gear symbol in the top-right corner of the screen.
2. Some dashlets have different categories of data. Click the category to see a pie chart with that set of data.
3. The pie chart shows the data that you have selected. Click one of the pie segments to open a new tab in with the filtered data, based on that pie segment.

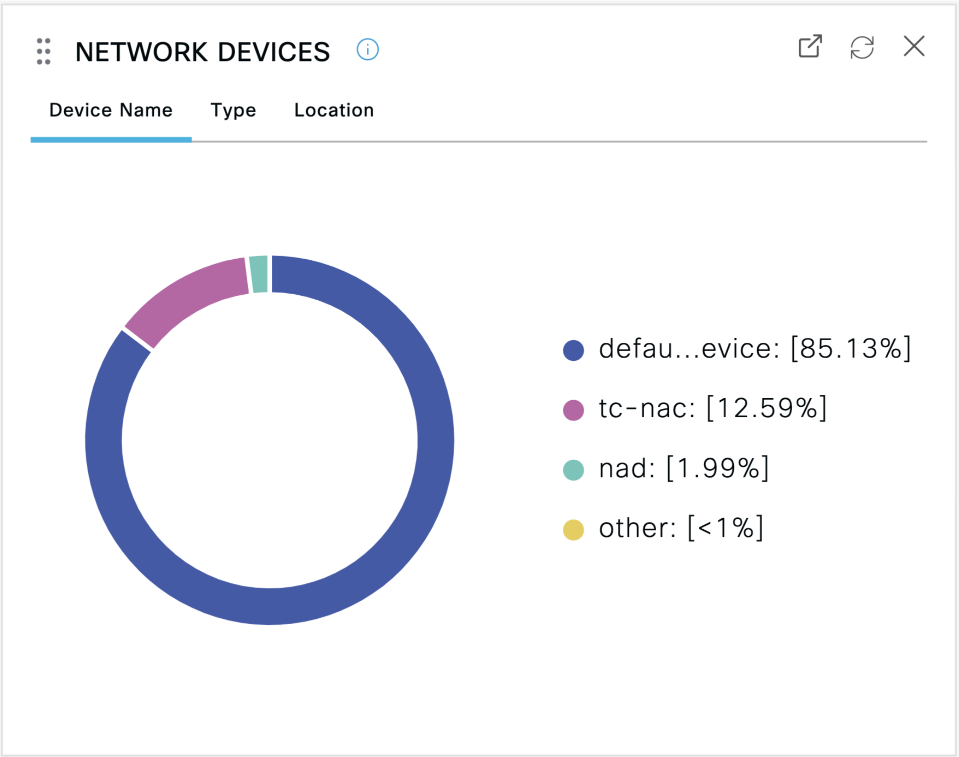
Click a section of the pie chart in a home page dashboard to open the chart in a new browser window. The new window displays data that is filtered by the section of the pie chart that you clicked on.

When you click a section of the pie chart in a Context Visibility window, the displayed data is filtered but context does not change. You view the filtered data in the same browser window.

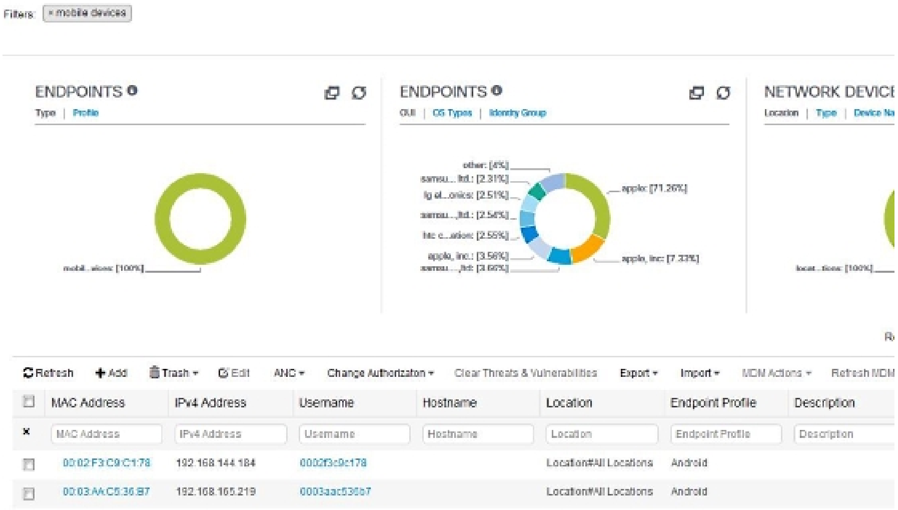
Filtering Displayed Data in a View

When you click a dashlet in a Context Visibility window, the corresponding data is filtered by the item you click and displayed. For example, when you click a section of a pie chart, the data for the chosen section is filtered and displayed.



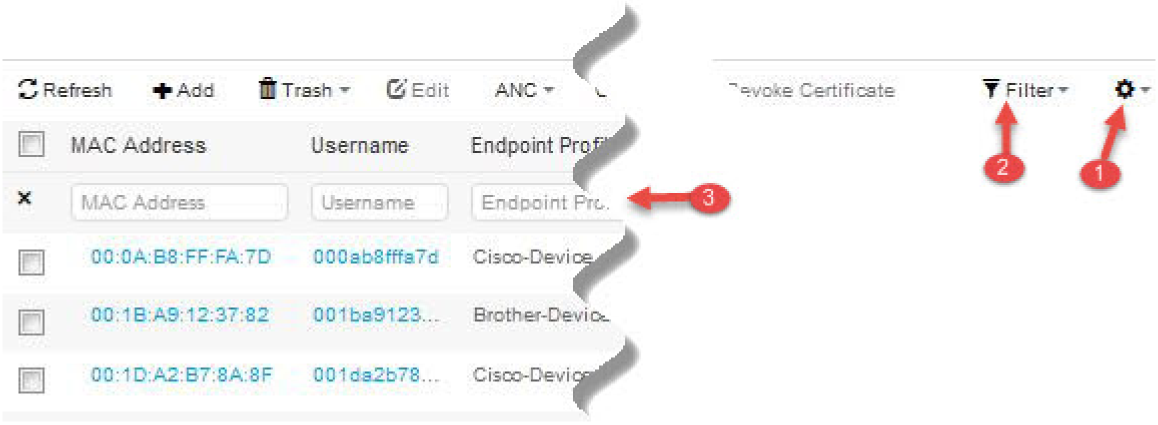


If you click **mobil…vices** in the **Endpoints** dashlet, the window refreshes to disaplay two **Endpoints** dashlets, a **Network Devices** dashlet, and a list of data. The dashlets and list show data for mobile devices, as shown in the following examplea new window displays the data, as shown in the following image:



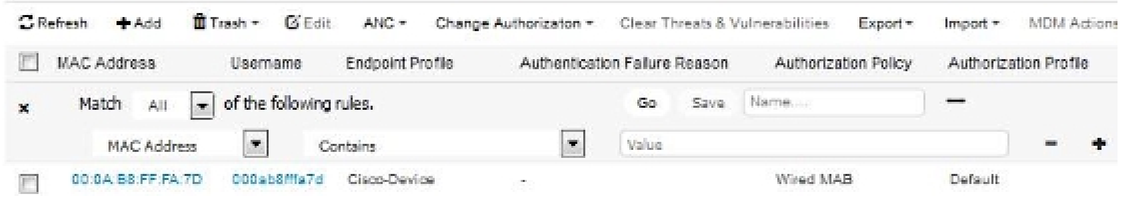
☐	MAC Address	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description
×	MAC Address	IPv4 Address	Username	Hostname	Location	Endpoint Profile	Description
☐	00:02:F3:C9:C1:78	192.168.144.184	0002f3c9c178		Location#All Locations	Android	
☐	00:03:AA:C5:36:B7	192.168.165.219	0003aac536b7		Location#All Locations	Android	

You can continue to filter data by clicking more sections of the pie charts, or by using the controls on the list of data.



☐	MAC Address	Username	Endpoint Profi
×	MAC Address	Username	Endpoint Pro...
☐	00:0A:B8:FF:FA:7D	000ab8fffa7d	Cisco-Device
☐	00:1B:A9:12:37:82	001ba9123...	Brother-Devic
☐	00:1D:A2:B7:8A:8F	001da2b78...	Cisco-Devic

1. The gear icon filters the displayed columns. From the drop-down list, choose the columns that you want to view in this dashboard's list.
2. The Quick Filter is displayed by default. Enter characters into the box (label number 3) to filter the list based on the result. The Custom Filter provides a more granular filter, as shown in the following image:



☐	MAC Address	Username	Endpoint Profile	Authentication Failure Reason	Authorization Policy	Authorization Profile
☐	00:0A:B8:FF:FA:7D	000ab8fffa7d	Cisco-Device	-	Wired MAB	Default

Save your custom filters.

Create Custom Filters

Create and save user-specific custom filters that are accessible only to you. Other users logging in to Cisco ISE cannot view the custom filters that you create. These custom filters are saved in the Cisco ISE database. You can access them from any computer or browser with which you log in to Cisco ISE.

Step 1 Click **Filter** and choose **Advanced Filter** from the drop-down list.

Step 2 Specify the search attributes, such as fields, operators, and values from the Filter menus.

Step 3 Click **+** to add more conditions.

Step 4 Click **Go** to display the entries that match the specified attributes.

Step 5 Click **Save** to save the filter.

Step 6 Enter a name and click **Save**. The filter now appears in the **Filter** drop-down list.

Filter Data by Conditions Using the Advanced Filter

The Advanced Filter allows you to filter information based on specified conditions, such as, First Name = Mike and User Group = Employee. You can specify more than one condition.

Step 1 Click **Filter** and choose **Advanced Filter** drop-down list.

Step 2 Specify search the search attributes, such as fields, operators, and values from the filter menus.

Step 3 Click **+** to add more conditions.

Step 4 Click **Go** to view the entries that match the specified attributes.

Filter Data by Field Attributes Using the Quick Filter

The Quick Filter allows you to enter a value for any of the field attributes displayed in the listing page, refreshes the page, and lists only those records that match your filter criteria.

Step 1 Click **Filter** and choose **Quick Filter** from the drop-down list.

Step 2 Enter search criteria in one or more of the attribute fields, and the entries that match the specified attributes display automatically.

Endpoint Actions in Dashlet Views

The toolbar at the top of the list allows you to act on endpoints in the list that you select. Not all actions are enabled for every list. Some actions depend on the feature that is enabled for use. The following list shows two endpoint actions that must be enabled in Cisco ISE before you can use them.

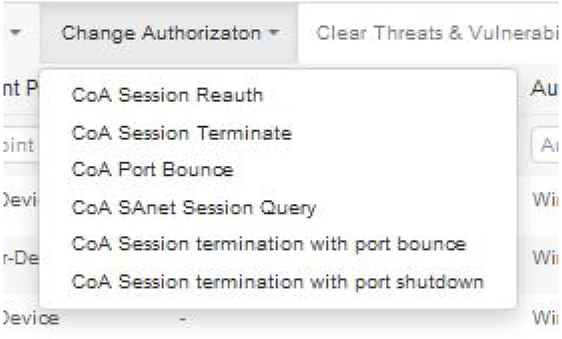
- **Adaptive Network Control Actions**

  If you enable the Adaptive Network Control service, you can select endpoints in the list and assign or revoke network access. You can also issue a change of authorization.

  Enable the Adaptive Network Services or Endpoint Protection Services in Cisco ISE in the **Adaptive Network Service** window. In the Cisco ISE GUI, click the **Menu** icon (☰) and choose**Administration** > **System** > **Settings** > **Endpoint Protection Service** > **Adaptive Network Control**. For more information, see the "Enable Adaptive Network Control in Cisco ISE" section in *Cisco ISE Admin Guide: Maintain and Monitor* .

  When you click the pie chart on a home page dashlet, the new window that is displayed contains the options **ANC** and **Change Authorization**. Check the check box for the endpoint you want to perform an action on, and choose the necessary action from the drop-down lists of**ANC** and **Change Authorization**.

  Figure 4: Endpoint Actions in Dashlet Views



- **MDM Actions**

  If you connect an MDM server to Cisco ISE, you can perform MDM actions on selected endpoints. Choose the necessary action from the **MDM Actions** drop-down list.

Cisco ISE Dashboard

The Cisco ISE dashboard or home page (**Home** > **Summary**) is the landing page that you view after you log in to the Cisco ISE administration portal. The dashboard is a centralized management console consisting of metric meters along the top of the window, with dashlets below. The default dashboards are **Summary**, **Endpoints**, **Guests**, **Vulnerability**, and **Threat**. See Cisco ISE Home Dashboards, on page 5.

Note You can view this dashboard data only in the Cisco ISE primary PAN portal.

The dashboard's real-time data provides an at-a-glance status of the devices and users accessing your network, and an overview of the system's health.

Click the gear icon in the second level menu bar for a drop-down list of dashboard settings. The following table contains descriptions for the dashboard settings options available in the drop-down list:

Drop-Down List Option	Description
Add New Dashboard	You can have a maximum of 20 dashboards, including the five default dashboards.
Rename Dashboard	(This option is available only for custom dashboards) To rename a dashboard: **1.** Click **Rename Dashboard**. **2.** Specify a new name. **3.** Click **Apply**.
Add Dashlet	To add a dashlet to the home page dashboard: **1.** Click **Add Dashlet(s)**. **2.** In the **Add Dashlets** window, click **Add** next to the dashlets that you want to add. **3.** Click **Save**. **Note** You can add a maximum of nine dashlets per dashboard.

Drop-Down List Option	Description
Export	You can export the dashboard data as a PDF or a CSV file. 1. Click **Export**. 2. In the **Export** dialog box, click the radio button next to one of the following file formats: • **PDF**: Choose the PDF format for a snapshot view of the selected dashlets. • **CSV**: Choose the CSV format to download the selected dashboard data as a zip file. 3. In the **Export** dialog box, check the check boxes next to the dashlets you want to export. 4. Click **Export**. The zip file contains individual dashlet CSV files for the selected dashboard. Data related to each tab in a dashlet is displayed as separate sections in the corresponding dashlet CSV file. When you export a custom dashboard, the zip file is exported with the same name. For example, if you export a custom dashboard that is named MyDashboard, then the exported file's name is MyDashboard.zip.
Layout Template	You can change the layout of the template in which the dashlets are displayed. To change the layout: 1. Click **Layout Template**. 2. Select the required layout from the options available.
Manage Dashboards	Click **Manage Dashboards** and choose one of the following options: • **Mark as Default Dashboard**: Use this option to set a dashboard as your default dashboard (the home page). • **Reset all Dashboards**: Use this option to reset all the dashboards to their original settings.

You can delete a dashboard that you have created by clicking the close (**x**) icon next to the corresponding custom dashboard.

Note You cannot rename or delete a default dashboard.

Each dashlet has a toolbar at the top-right corner where you can perform the following operations:

- Detach: To view a dashlet in a separate window.
- Refresh: To refresh a dashlet.
- Remove: To remove a dashlet from the dashboard.

You can drag and drop the dashlet using the gripper icon that is present at the top-left corner of the dashlet.

The Alarms dashlet contains a quick filter for the **Severity** column. You can filter alarms by their severity by choosing **Critical**, **Warning**, or **Info** from the **Severity** drop-down list.

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface to the supported languages. Localization of the user interface incorporates location-specific components and translated text. In Windows, MAC OSX, and Android devices, the native supplicant provisioning wizard can be used in any of the following supported languages.

In Cisco ISE, internalization and localization support focuses on support for non-English text in UTF-8 encoding to the end user-facing portals and on selective fields in the administration portal.

Supported Languages

Cisco ISE provides localization and internalization support for the following languages and browser locales.

Table 3: Supported Languages and Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
Czech	cs-cz
Dutch	nl-nl
English	en
French	fr-fr
German	de-de
Hungarian	hu-hu
Italian	it-it
Japanese	ja-jp

Language	Browser Locale
Korean	ko-kr
Polish	pl-pl
Portuguese (Brazil)	pt-br
Russian	ru-ru
Spanish	es-es

End-User Web Portal Localization

The Guest, Sponsor, My Devices, and Client Provisioning portals are localized into all the supported languages and locales. This includes text, labels, messages, field names, and button labels. If a client browser requests a locale that is not mapped to a template in Cisco ISE, the portal displays content using the English template.

Using the administration portal, you can modify the fields that are used in the Guest, Sponsor, and My Devices portals for each language. You can also add other languages. Currently, you cannot customize these fields for the Client Provisioning portal.

You can further customize the Guest portal by uploading HTML pages to Cisco ISE. When you upload customized pages, you are responsible for the appropriate localization support for your deployment. Cisco ISE provides a localization support example with sample HTML pages, which you can use as a guide. Cisco ISE allows you to upload, store, and render custom internationalized HTML pages.

Note NAC and MAC agent installers, and WebAgent pages are not localized.

Support for UTF-8 Character Data Entry

Cisco ISE fields that are exposed to the end user (through the Cisco client agent or supplicants, or the Sponsor, Guest, My Devices, and Client Provisioning portals) support UTF-8 character sets for all languages. UTF-8 is a multibyte character encoding for the Unicode character set, which includes many different language character sets including Hebrew, Sanskrit, and Arabic.

Character values are stored in UTF-8 in the administration configuration database, and the UTF-8 characters display correctly in reports and user interface components.

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, Extensible Authentication Protocol (EAP), RADIUS proxy, RADIUS token, and web authentication from the Guest and administration portal login authentications. UTF-8 support for username and password applies to authentication against the local identity store and external identity stores.

UTF-8 authentication depends on the client supplicant that is used for network login. Some Windows native supplicants do not support UTF-8 credentials.

Note UTF-8 authentication with RSA is not supported as RSA does not support UTF-8 users. RSA servers, which are compatible with Cisco ISE, also do not support UTF-8.

UTF-8 Policies and Posture Assessment

Policy rules in Cisco ISE that are conditioned on attribute values may include UTF-8 text. Rule evaluation supports UTF-8 attribute values. You can also configure conditions with UTF-8 values through the administration portal.

Posture requirements are modified as File, Application, and Service conditions based on a UTF-8 character set.

UTF-8 Support for Messages Sent to Supplicant

RSA prompts and messages are forwarded to the supplicant using a RADIUS attribute REPLY-MESSAGE, or within EAP data. If the text contains UTF-8 data, it is displayed by the supplicant, based on the client's local operating system language support. Some Windows-native supplicants do not support UTF-8 credentials.

Cisco ISE prompts and messages may not be in synchrony with the locale of the client operating system on which the supplicant is running. You must align the end-user supplicant locale with the languages that are supported by Cisco ISE.

Reports and Alerts UTF-8 Support

Monitoring and troubleshooting reports and alerts support UTF-8 values for relevant attributes for the languages that are supported in Cisco ISE. The following activities are supported:

- Viewing live authentications.
- Viewing detailed pages of report records.
- Exporting and saving reports.
- Viewing the Cisco ISE dashboard.
- Viewing alert information.
- Viewing tcpdump data.

UTF-8 Character Support in the Portals

More character sets are supported in Cisco ISE fields (UTF-8) than are currently supported for localizations in portals and end-user messages. For example, Cisco ISE does not support right-to-left languages, such as Hebrew or Arabic, although the character sets themselves are supported.

The following table lists the fields in the Admin and end-user portals that support UTF-8 characters for data entry and viewing, with the following limitations:

- Cisco ISE does not support guest usernames and passwords with UTF-8 characters.
- Cisco ISE does not support UTF-8 characters in certificates.

Table 4: Administration Portal UTF-8 Character Fields

Administration Portal Element	UTF-8 Fields
Network access user configuration	• **Username** The usernames can contain any combination of upper and lowercase letters, numbers, space, and special characters (except `, %, ^, ;, :, [, {, |, },], \, ‘, “, =, <, >, ?, !, and control characters). You cannot submit usernames with only spaces. • **First Name** • **Last Name** • **Email**
User list	• All filter fields. • Values displayed in the User List window. • Values displayed in the left navigation quick view.
User password policy	The passwords can contain any combination of upper and lowercase letters, numbers, and special characters (including !, @, #, $, ^, &, *, (, and). The password field accepts any characters including UTF-8 characters, but it does not accept control characters. Some languages do not have uppercase or lowercase alphabets. If your user password policy requires the user to enter a password with uppercase or lowercase characters and the user’s language does not support these characters, the user cannot set a password. For the user password field to support UTF-8 characters, uncheck the following check boxes in the user password policy page (**Administration** > **Identity Management** > **Settings** > **User Authentication Settings** > **Password Policy**): • **Lowercase alphabetic characters** • **Uppercase alphabetic characters** You cannot use dictionary words, their characters in reverse order, or their letters replaced with other characters.
Administrator list	• All filter fields. • Values that aredisplayed in the administrator list window. • Values that are displayed in the left navigation quick view.
Admin login page	• **Username**
RSA	• Messages • Prompts
RADIUS token	• Authentication tab > Prompt

Administration Portal Element	UTF-8 Fields
Posture Requirement	• Name • Remediation action > Message shown to Agent User • Requirement list display
Posture conditions	The following fields in the **Policy** > **Policy Elements** > **Conditions** > **Posture** windows: • **File Condition** > **Add** > **File Path**. • **Application Condition** > **Add** > **Process Name**. • **Service Condition** > **Add** > **Service Name**. • Conditions list displays.
Guest and My Devices settings	• Sponsor > Language Template: all supported languages, all fields. • Guest > Language Template: all supported languages, all fields. • My Devices >Language Template: all supported languages, all fields.
System settings	• SMTP Server > Default email address
Operations > Alarms > Rule	• Criteria > User • Notification > email notification user list
Operations > Reports	• Operations > Live Authentications > Filter fields • Operations > Reports > Catalog > Report filter fields
Operations > Troubleshoot	• General Tools > RADIUS Authentication Troubleshooting > Username
Policies	• Authentication > value for the antivirus expression within policy conditions • Authorization or posture or client provisioning > other conditions > value for the antivirus expression within policy conditions

Administration Portal Element	UTF-8 Fields
Attribute value in policy library conditions	• Authentication > simple condition or compound condition > value for the antivirus expression • Authentication > simple condition list display • Authentication > simple condition list > left navigation quick view display • Authorization > simple condition or compound condition > value for the antivirus expression • Authorization > simple condition list > left navigation quick view display • Posture > Dictionary simple condition or dictionary compound condition > value for the antivirus expression • Guest > simple condition or compound condition > value for the antivirus expression

UTF-8 Support Outside the Cisco ISE User Interface

This section contains the areas outside the Cisco ISE user interface that provide UTF-8 support.

Debug Log and CLI-Related UTF-8 Support

Attribute values and posture condition details appear in some debug logs. All debug logs accept UTF-8 values. You can download debug logs containing raw UTF-8 data that can be viewed with a UTF-8-supported viewer.

Cisco Secure ACS Migration UTF-8 Support

Cisco ISE allows the migration of Cisco Secure Access Control Server (ACS) UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by Cisco ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration unreadable using the administration portal or report methods. Convert the unreadable UTF-8 values (that are migrated from Cisco Secure ACS) into ASCII text. For more information about migrating from Cisco Secure ACS to Cisco ISE, see the Cisco Secure ACS to Cisco ISE Migration Tool for your version of Cisco ISE.

Support for Importing and Exporting UTF-8 Values

The administration and Sponsor portals support plaintext and CSV files with the UTF-8 values to use when importing user account details. Exported files are provided as CSV files.

UTF-8 Support on REST

External Representational State Transfer (REST) communication supports UTF-8 values. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, except for administrator authentication. Administrator authentication in REST requires ASCII text credentials for login.

UTF-8 Support for Identity Stores Authorization Data

Cisco ISE allows Microsoft Active Directory and Lightweight Directory Access Protocol (LDAP) to use UTF-8 data in authorization policies for policy processing.

MAC Address Normalization

Cisco ISE supports normalization of the MAC address that you enter in any of the following formats:

- 00-11-22-33-44-55
- 0011.2233.4455
- 00:11:22:33:44:55
- 001122334455
- 001122-334455

Provide full or partial MAC addresses in the following Cisco ISE windows:

- **Policy** > **Policy Sets**
- **Policy** > **Policy Elements** > **Conditions** > Authorization
- Authentications > Filters (Endpoint and Identity columns)
- Global search
- **Operations** > **Reports** > Report Filters
- **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **Endpoint Debug**

Provide full MAC addresses (six octets separated by ':' or '-' or '.') in the following Cisco ISE windows:

- Operations > Endpoint Protection Services Adaptive Network Control
- **Operations** > **Troubleshoot** > **Diagnostic Tools** > **General Tools** > **RADIUS Authentication Troubleshooting**
- **Operations** > **Troubleshooting** > **Diagnostic Tools** > **General Tools** > **Posture Troubleshooting**
- Administration > Identities > Endpoints
- **Administration** > **System** > **Deployment**
- **Administration** > **Logging** > **Collection Filters**

REST APIs also support normalization of full MAC address.

The valid ranges for an octet are 0 to 9, a to f, or A to F.

Cisco ISE Deployment Upgrade

Cisco ISE offers a GUI-based centralized upgrade from the administration portal. The progress of the upgrade and the status of the nodes are displayed in the Cisco ISE GUI. For information on the preupgrade and postupgrade tasks you must carry out, see the *Cisco Identity Services Engine Upgrade Guide* for the Cisco ISE release that you want to upgrade to.

The upgrade **Overview** window (**Administration** > **System** > **Upgrade** > **Overview** lists all the nodes in your deployment, the personas that are enabled on them, the Cisco ISE version that is currently in use, and the status (whether a node is active or inactive) of each node. You can begin upgrade only if all the nodes are in the **Active** state.