CHAPTER 2

Understanding the User Interface

This chapter introduces the Cisco Identity Service Engine (ISE) user interface in the following topics:

Cisco ISE Internationalization and Localization

Cisco ISE internationalization adapts the user interface for supported languages. Localization of the user interface incorporates locale-specific components and translated text.

In Cisco ISE, Release 1.1 internalization and localization support is focused on the text and information that is presented to the end user (connecting to Cisco ISE). This includes support for non-English text in UTF-8 encoding to the end-user facing portals and on selective fields on the Cisco ISE Admin user interface.

This section covers the following topics:

Supported Languages

Cisco ISE, Release 1.1 provides localization and internalization support for the following languages and browser locales:

Table 2-1 Supported Languages and Browser Locales

Language	Browser Locale
Chinese traditional	zh-tw
Chinese simplified	zh-cn
English	en
French	fr-fr
German	de-de
Italian	it-it
Japanese	ja-jp
Korean	ko-kr
Portuguese	pt-br (Brazilian)
Russian	ru-ru
Spanish	es-es

Internationalization and localization applies to all supported internet browsers. For more information, see the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

UTF-8 Character Data Entry

Cisco ISE administrative user interface fields that are exposed to the end user through the Cisco NAC agent, supplicants, or the sponsor portal, guest portal, and client provisioning portals, support UTF-8 character sets for all languages. Character values are stored in UTF-8 in the administration configuration database, and are then viewed in UTF-8 as entered.

UTF-8 is a multibyte character encoding for the unicode character set, which includes many different language character sets, including Hebrew, Sanskrit, Arabic, and many more. The ISE user interface supports UTF-8 characters in a number of input fields. When the user-entered UTF-8 characters appear in reports and user interface components, they are displayed correctly.

Note Many more character sets are supported in ISE user interface input fields (UTF-8) than are currently supported for localizations (for translated text) in portals and end-user messages.

For a complete list of UTF-8 character data entry fields, see UTF-8 Character Support in the User Interface, page 21-36.

Portal Localization

Internationalizing includes input that is configured by the end user, or Cisco ISE administrator configurations that are displayed in any of the following user portals:

- Sponsor Portal, page 2-3
- Guest Portal, page 2-3
- Client Provisioning Portal, page 2-4

Sponsor Portal

The Sponsor portal user interface is localized into all supported languages and locales. This includes text, labels, messages, field names, and button labels. The predefined text per language is configurable on the Cisco ISE Admin user interface, and you can add additional languages. For more information, see Configuring Sponsor Language Templates, page 21-37.

Note If an undefined locale is requested by a client browser, the English locale default portal is displayed. This means that if the browser requests a locale that is not mapped to a template in ISE, the English template is presented. See Table 2-1 for a list of supported Languages and Browser Locales

Sponsor portal fields support UTF-8 char sets. UTF-8 values are stored in the administrative configuration database and viewed in UTF-8 in the Sponsor portal as entered. Guest accounts accept plain text and .csv files with UTF-8 values. The following table lists the UTF-8 Sponsor portal fields.

Guest account list	• Filter value edit box
Create guest account	• First name • Last name • Email address • Company • Optional data
Create random guest accounts	• User name prefix
Settings customizations	• Email

Guest Portal

The Guest portal can be localized to present user interface elements in all left-to right language locales. This includes text, field names, button labels, and messages. You can configure supported language templates on the administrative portal. For more information, see Configuring Sponsor Language Templates, page 21-37.

Note Currently, ISE does not support right-to-left languages, such as Hebrew or Arabic, even though the character sets themselves are supported.

You can 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. ISE provides the ability to upload, store, and render custom internationalized HTML pages.

Default templates for supported languages are included in a standard Cisco ISE installation. If an undefined locale is requested by the client browser, the English locale default portal is displayed.

The following are the Guest portal input fields to support UTF-8:

- Login user name
- All fields on the self-registration page

Client Provisioning Portal

The Client Provisioning portal interface has been localized for all supported language locales. This includes text, labels, messages, field names, and button labels. If an undefined locale is requested by a client browser, the English locale default portal is displayed.

Currently, language templates are not supported for the Client Provisioning portal, as they are for the Admin, Guest, and Sponsor portals.

Note NAC and MAC agent installers are not localized, nor are WebAgent pages.

For more information on client provisioning, see Chapter 19, "Configuring Client Provisioning Policies."

UTF-8 Credential Authentication

Network access authentication supports UTF-8 username and password credentials. This includes RADIUS, EAP, RADIUS proxy, RADIUS token, web authentication from the Guest and Administrative portal login authentications. This provides end users network access with a UTF-8 user name and password, as well as administrators with UTF-8 credentials. UTF-8 support for user name and password applies to authentication against the local identity store as well as 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. If you are experiencing difficulties with a Windows native supplicant, the following Windows hotfixes may be helpful:

- http://support.microsoft.com/default.aspx?scid=kb;EN-US;957218
- http://support.microsoft.com/default.aspx?scid=kb;EN-US;957424

Note RSA (Rivest, Shamir, and Adleman) does not support UTF-8 users, hence UTF-8 authentication with RSA is not supported. Likewise, RSA servers, which are compatible with ISE 1.1, 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. In addition, you can configure conditions with UTF-8 values through the Administrative portal.

Posture requirements can be modified as File, Application, and Service conditions based on a UTF-8 character set. This includes sending UTF-8 requirement values to the NAC agent. The NAC agent then assesses the endpoint accordingly, and reports UTF-8 values, when applicable.

Cisco NAC and MAC Agent UTF-8 Support

The Cisco NAC agent supports internationalization of text, messages, and any UTF-8 data that is exchanged with ISE. This includes requirement messages, requirement names, and file and process names that are used in conditions.

The following limitations apply:

- UTF-8 support applies to Windows-based NAC agents only.
- Cisco NAC and MAC agent interfaces currently do not support localization.

Note WebAgent does not support UTF-8 based rules and requirements. For Cisco NAC agent versions supported by Cisco ISE, Release 1.1, see *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

If an acceptable use policy (AUP) is configured, the policy pages are provided on the client side, based on the browser locale and the set of languages that are specified in the configuration. The administrator is responsible for providing a localized AUP bundle or site URL.

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.

Note Cisco ISE prompts and messages may not be in sync with the locale of the client operating system on which the supplicant is running. It is the responsibility of the administrator to 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 Cisco ISE supported languages, in the following ways:

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

UTF-8 Support Outside the User Interface

This section covers the areas outside the 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; therefore, all debug logs accept UTF-8 values. Downloading debug logs provides raw UTF-8 data that can be viewed by the administrator with a UTF-8 supported viewer.

Note Microsoft Office Excel is not a supported viewer.

ACS Migration UTF-8 Support

Cisco ISE, Release 1.1 allows for the migration of ACS UTF-8 configuration objects and values. Migration of some UTF-8 objects may not be supported by ISE UTF-8 languages, which might render some of the UTF-8 data that is provided during migration as unreadable using Administrative portal or report methods.

For a complete list of ACS migration issues, see the *Cisco Identity Services Engine Migration Guide for Cisco Secure ACS 5.1 and 5.2, Release 1.1.*

Note It is the responsibility of the administrator to convert unreadable UTF-8 values (that are migrated from ACS) into ASCII text.

Support for Importing and Exporting UTF-8 Values

You can import or export users to a file and have the UTF-8 values for the fields retained. You can import plain text csv files. The user information is stored as UTF-8 and is presented accordingly in the user list of the Administrative portal. Exported files are provided as csv files.

Note A csv file must be saved in UTF-8 format using an application that supports the UTF-8 format.

UTF-8 Support on REST

UTF-8 values are supported on external REST communication. This applies to configurable items that have UTF-8 support in the Cisco ISE user interface, with the exception of admin authentication. Admin authentication on REST requires ASCII text credentials for login.

For information on supported REST APIs, see the *Cisco Identity Services Engine API Reference Guide, Release 1.1.*

Inherent Usability

The Cisco ISE user interface centralizes network identity management, while providing drill-down access to granular data across the network. The Cisco ISE user interface makes it easier for you to get the information you need to make critical decisions in a timely fashion by providing the following:

- Data based on user roles and their respective tasks
- A centralized administration workspace

- At-a-glance statistics for monitoring network-wide health and security
- Simplified visualizations of complex data

Functional User Interface

The Cisco ISE user interface is role-based and tailored to your job function. Elements that are associated with tasks that are outside of your job description are deactivated or not shown at all.

Menu structures within the user interface link roles to job functions, thereby determining the available permissions. It is possible to be assigned to multiple roles, depending on the nature of your job. For more information, see Understanding the Impact of Roles and Admin Groups, page 2-19.

Centralizing the Administration

The Cisco ISE user interface allows you to perform all necessary network administration tasks from one window. The Cisco ISE home page, also known as the dashboard, is the landing page, displaying real-time monitoring and troubleshooting data. The navigation tabs and menus at the top of the window provide point-and-click access to all other administration features. For more information, see Primary Navigation Tabs and Menus, page 2-8.

At-a-Glance Monitoring

The dashboard consists of dashlets and meters that provide a visual overview of network health and security. These tools allow you to act on issues as they arise. Similar to the warning light on an automobile dashboard, you must go directly to the problem area to resolve an issue that appears on the ISE dashboard. For information on the individual dashboard elements, see Introducing the Dashboard, page 2-12.

Simplifying Complex Data

Dashboard elements visually convey complex information in a simplified format. This display allows you to quickly analyze data and drill down for in-depth information if needed. Dashlets utilize a variety of elements to display data, including sparklines, stack bars, and metric meters. For more information, see Dashboard Elements, page 2-13.

Elements of the User Interface

The ISE user interface provides an integrated network administration console from which you can manage various identity services. These services include authentication, authorization, posture, guest, profiler, as well as monitoring, troubleshooting, and reporting. All of these services can be managed from a single console window called the Cisco ISE dashboard.

This section is an introduction to navigation elements that are incorporated into the Cisco ISE user interface, and covers the following topics:

Primary Navigation Tabs and Menus

This section introduces the Cisco ISE primary navigation tabs and the associated menus.

Primary Navigation Tabs

The primary navigation tabs span the top of the Cisco ISE window. Administrators can perform various tasks from the Cisco ISE dashboard depending on their assigned access roles. The major tasks are performed from the following high-level tabs in the user interface:

- Home—This tab is the landing page when you first log into the Cisco ISE console. This page provides a real-time view of all the services running on the Cisco ISE network. You can view more detailed information by double-clicking elements on the page.
- Operations—This tab provides access to tools for monitoring live authentications, querying historical data through reports, and troubleshooting network services. It also provides information on real-time alarms as they occur on the network.
- Policy—This tab provides access to tools for managing network security in the areas of authentication, authorization, profiling, posture, client provisioning. Secure Group Access and select policy elements have direct links for ease of use.
- Administration—This tab provides access to tools for administering the ISE network in these functional areas: System, Identity Management, Network Resources, and Guest Management.

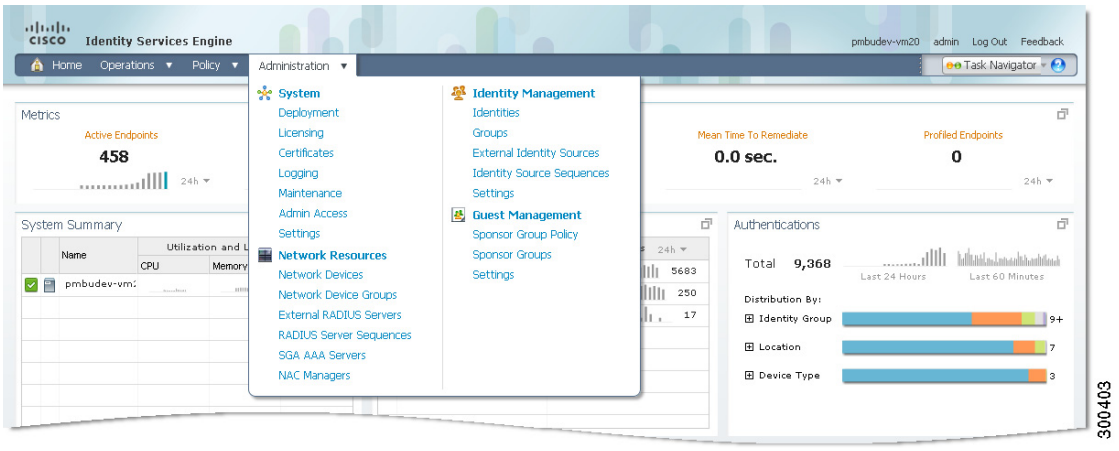
The following illustration shows the Operations primary navigation tab, and its related subtabs. A quicker way to access the navigation tab functionality is through the navigation tab menus, as described in Easy-Access Menus, page 2-8.

Figure 2-1 Primary Navigation Tabs

Easy-Access Menus

An easy-access menu is a pop-up menu that provides quick access to the features that are associated with a primary navigation tab. Mouse over the title of a navigation tab to bring up the associated menu. Clicking the name links on the menu takes you directly to the feature page. The following illustration is an example of the Administration menu.

Figure 2-2 Navigation Tab Menu



The Global Toolbar

The Global Toolbar is always available at the bottom of the Cisco ISE window, providing instantaneous access to the complete Cisco ISE online Help system and a summary of alarm notifications. Mouse over the Help icon to access the available online Help.

Mouse over the Alarms icon to display the summarized Alarms page, with a list of recent system alarms and the ability to filter for alarms of a specific nature. You can also drill down for detailed information on individual alarms.

Figure 2-3 Global Toolbar

For more information:

- Getting Help, page 2-11.
- Managing Alarms, page 23-11.

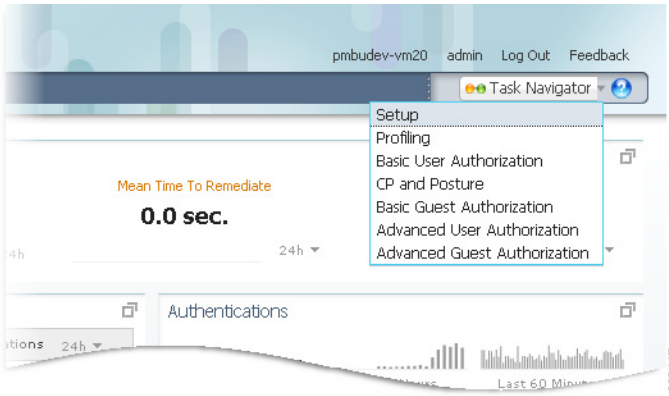
Task Navigators

Task Navigators are visual guides for navigating through procedures whose tasks span multiple screens, such as ISE system setup and profiling. The linear presentation visually outlines the order in which the tasks should be completed, while also providing direct links to the screens where the tasks are performed.

You access Task Navigators from the drop-down menu in the upper right corner of the ISE window. You can choose from the following Task Navigators:

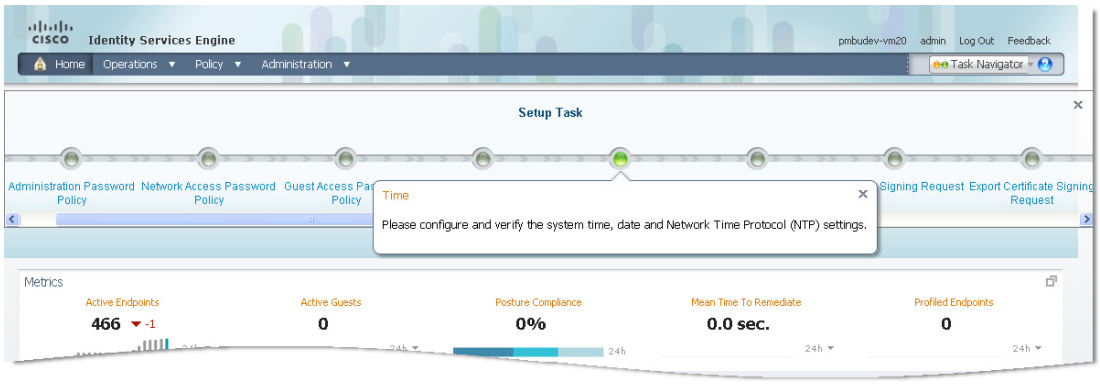
- Infrastructure—Process for fine tuning your ISE network with advanced configuration tasks
- Profiling—Process for profiling endpoints
- Setup—Process for setting up your ISE network after an initial installation

Figure 2-4 Task Navigator Menu



The task navigator displays a series of tasks along a line in the order in which they should be performed, from left to right. Hovering over a task bullet displays a quick view dialog with information on the task. You can close the task navigator at any time by clicking the X icon in the upper right corner.

Figure 2-5 Task Navigator Dialog



Clicking a bullet icon takes you directly to the page where you can begin the associated task.

Task Navigators are a quick reference that you may need to rely on at first. As you complete the tasks and become familiar with the processes, you will quickly outgrow that necessity. For this reason, you can show and hide Task Navigators as needed.

For information on the individual Task Navigators and how to use them, see Chapter 3, “Cisco ISE Task Navigator.”

Getting Help

It is easy to get answers to your questions and find information on topics related to Cisco ISE with the following Help tools:

- Global Help, page 2-11
- Page-Level Help, page 2-11

Note You can be a part of improving Cisco ISE by voicing your opinion on specific features or requesting future enhancements by going to Providing Feedback to Cisco, page 2-12.

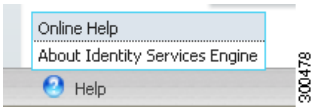
Global Help

The Global Help icon is located in the bottom left corner of the Global Toolbar in the Cisco ISE window. Global Help provides quick access to Cisco ISE comprehensive online Help.

To launch Global Help, complete the following steps:

Step 1 On the global toolbar, move your cursor over the Help icon.

Step 2 Choose **Online Help** from the pop-up menu.



A new browser window appears displaying the Cisco ISE Online Help.

Page-Level Help

You can access contextual (page-level) Help by clicking the Help icon that appears in the upper right corner of the Cisco ISE window. Page-level help provides information on the features, functions, and tasks associated with the current selected page in the Cisco ISE user interface.

To access Help for a current page, complete the following steps:

Step 1 Navigate to a page in the Cisco ISE user interface.

Step 2 In the upper right corner of the Cisco ISE window, click the blue **Help** icon. A browser window appears with links to the Help topics relating to that page.

Providing Feedback to Cisco

You can help improve Cisco ISE by providing feedback to Cisco directly from the Cisco ISE user interface.

To provide feedback on Cisco ISE, complete the following steps:

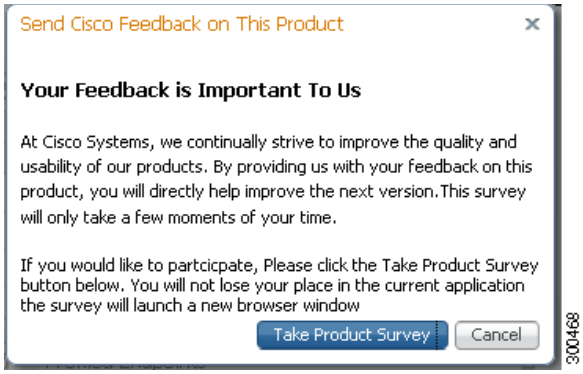
Step 1 Click the **Feedback** link in the upper right corner of the Cisco ISE window to bring up the Send Cisco Feedback on this Product dialog.

Step 2 Click **Take the Product Survey** in the lower right corner of the dialog to launch the survey wizard.

Step 3 Choose the answers that relate to your experience, enter personal comments as desired, and then submit your response.

Your answers and comments are reviewed by the Cisco ISE product team, and are taken into serious consideration.

Figure 2-6 Cisco ISE Feedback Survey



Introducing the Dashboard

The Cisco ISE dashboard is a centralized management window that displays live consolidated and correlated statistical data. The dashboard provides an at-a-glance status of the devices that are accessing your network, and its real-time data is essential for effective monitoring and troubleshooting.

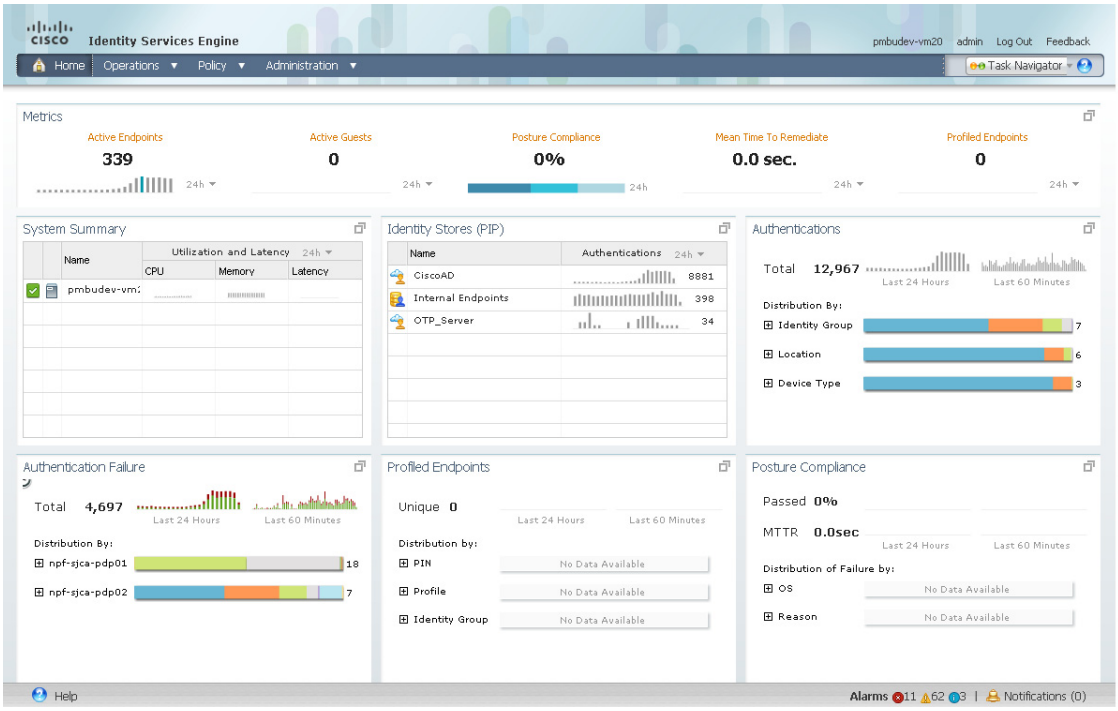
The dashboard uses a variety of elements to convey complex data in simplified formats. Dashboard elements show activity over 24 hours, unless otherwise noted. However, you can mouse over elements to view data for the last 60 minutes in the tooltip display.

Note You must have Adobe Flash Player installed on the Cisco ISE administration node to view the dashlets and meters on the Cisco ISE dashboard. For information on the current recommended version, see the *Cisco Identity Services Engine Network Component Compatibility, Release 1.1*.

This section introduces the elements that comprise the dashboard, explains how to interpret the different visual representations of data, and covers the following topics:

- Dashboard Elements, page 2-13
- Drilling Down for Details, page 2-15

Figure 2-7 Cisco ISE Dashboard Example



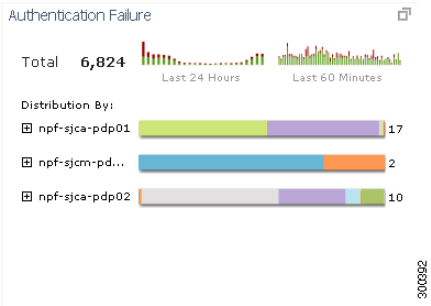
Dashboard Elements

This section introduces dashboard elements, and explains how to interpret the visual data.

Dashlets

Dashlets are individual panels on the dashboard that summarize important statistics about the devices and users that are accessing the network, and the overall health and security of the network. Each dashlet contains an independent function, and can display the statistical data that is related its function in a variety of ways.

Figure 2-8 Dashlet Example



Sparklines

Sparklines are a method of visualizing data with vertical lines that depict trends over time. A sparkline is a small version of a bar chart that portrays utilization or relative load on the system. Taller bars mean there was a higher load at a particular time.

Most sparklines are grouped in time increments. A 24-hour time increment shows 24 sparklines. A 60-minute time increment displays 60 sparklines. For data represented in 24-hour increments only, you can mouse over a sparkline to view data for the last 60 minutes in the tooltip display.

Hover your cursor over a sparkline to bring up a quick view display that explains the data. Click a sparkline to bring up a visual report for the function. For more information, see Viewing Deep-Drill Reports, page 2-16.

Percentages are absolute, but numbers are relative, such as the display “Total: 154” shown in the following example.

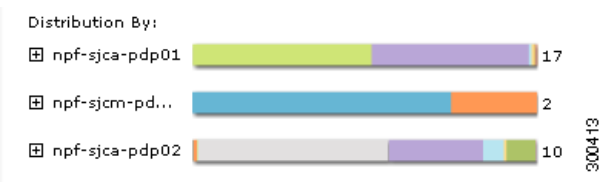
Figure 2-9 Sparklines

Stack Bars

Stack bars are a method of visualizing data with horizontal blocks of color that depict the distribution of parameters. Color is used as a dividing element, so you can easily see where one parameter ends and another begins. The number of distributions within a stack bar are limited to 10. For this reason, only top 10 distributions are shown.

Hover your cursor over a color area to bring up a quick view display that explains the data.

Figure 2-10 Stack Bars

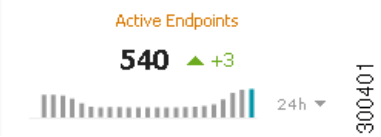


Metric Meters

Metric meters are the small panels that line the top of the dashboard, and summarize the most important statistics regarding the devices that are accessing the network. Metric meters provide an at-a-glance view of network health and performance.

The number display depicts change, similar to a stock market index. Sparklines convey trending and provide the time range selector, which lets you toggle the time interval between 60 minutes or 24 hours. Stack bars represent the distribution of a parameter.

Figure 2-11 Metric Meter

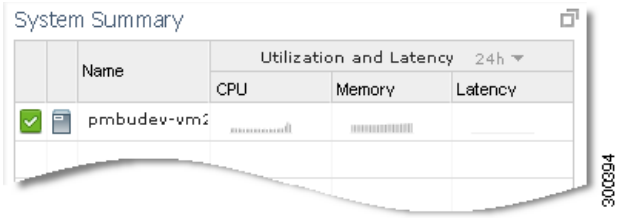


Color and Meaning

In some dashlets, color is used to convey meaning. In general, stack bars use color to mark the boundary points between one data measurement and another. In other dashlets, colors convey a different meaning, such as system health classifications:

- Healthy = Green
- Warning = Yellow
- Critical = Red
- No information = Gray

Figure 2-12 Dashboard Color Significance



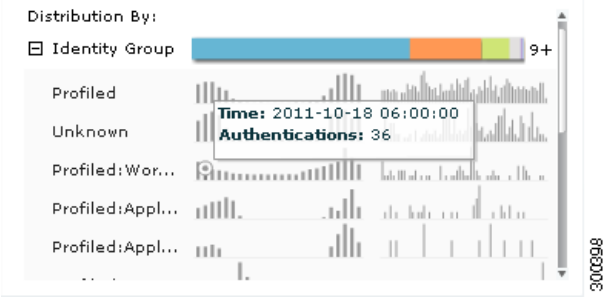
Drilling Down for Details

You can expand some dashlets to see a granular view of the data. Click sparklines to access a deep-drill report.

Expanding Dashlets

If data is available, a plus sign (+) appears next to an item in a dashlet. To view the data, click the plus sign (+). In the following illustration, an Identity Group stack bar is expanded to show a breakdown of authentication identity group data. Place your cursor over a sparkline to display granular authentication details.

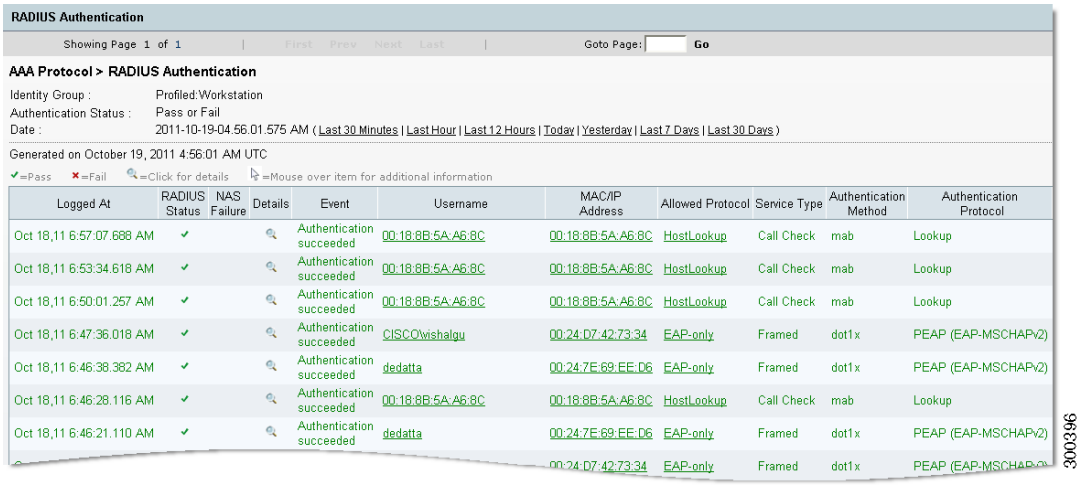
Figure 2-13 Expanded Dashlet



Viewing Deep-Drill Reports

Double-click a sparkline to view an in-depth report of the information. Double-clicking a sparkline in the dashlet that is shown in Figure 2-13 generated and displayed the RADIUS Authentications report that is shown in Figure 2-14.

Figure 2-14 Deep-Drill Report



Common User Interface Patterns

There are several types of cross-functional user interface patterns that enhance usability:

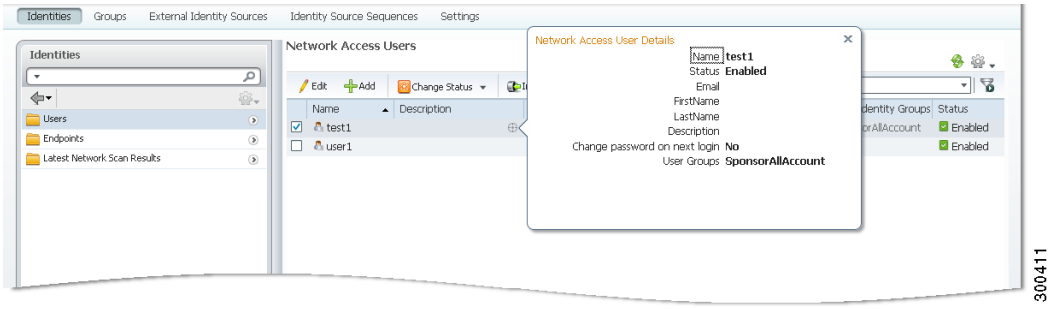
- Quick Views, page 2-17
- Anchored Overlays, page 2-17
- Object Selectors, Navigation Paths, and Object Buttons, page 2-17
- Format Selectors, page 2-18
- Expression Builders, page 2-18

This section covers patterns that occur throughout the Cisco ISE user interface, although the examples shown are associated with Policy tab functions.

Quick Views

A Quick View dialog appears when you place your cursor over a Quick View arrow icon, showing the details of the associated object. In Figure 2-15, the Quick View dialog shows the information for the selected user. To close a Quick View, click the X icon in the upper right corner of the dialog.

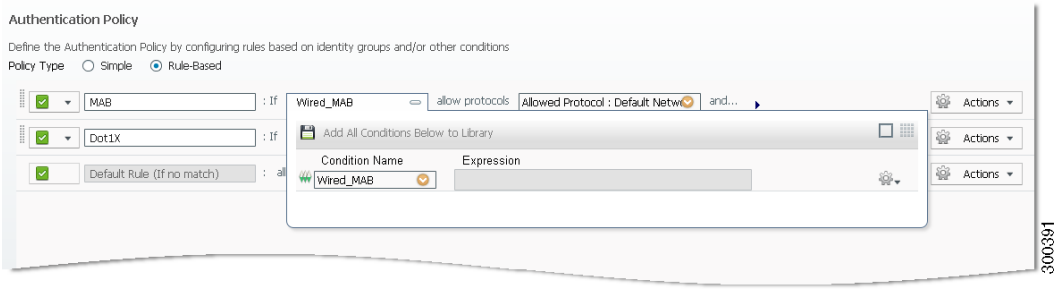
Figure 2-15 Quick View Dialog



Anchored Overlays

An anchored overlay is a stationary pop-up panel that allows you to choose options for a function without having to leave the screen. An anchored overlay is linked to a specific functional element, such as the one that is shown in Figure 2-16. After completing your selections on the anchored overlay, click outside the dialog to close the overlay.

Figure 2-16 Anchored Overlay



Object Selectors, Navigation Paths, and Object Buttons

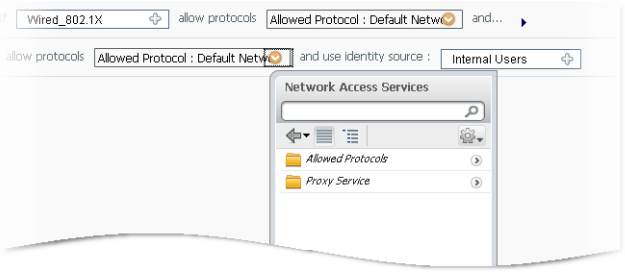
An object selector is a pop-up dialog that displays options for a selected function, as shown in Figure 2-17. An object selector is often linked to another dialog, such as an anchored overlay. Other user interface elements are incorporated into the object selector, such as a search dialog, navigation path, action button, and format selector.

The search dialog is self-explanatory, but these elements may not be familiar to you:

- Navigation path: Click the arrow to display navigation options.
- Action icon: Click the gear-shaped icon to display the drop-down menu from which you can choose an action.

After you make a selection, the dialog closes automatically. For more information, see Format Selectors, page 2-18.

Figure 2-17 Object Selector Dialog



Note When you create nested child objects under **Administration > Identity Management > Groups** (Guest, SponsorAllAccount, SponsorGroupAccounts, SponsorOwnAccount, and so on), you can view and access child objects up to the 15th level in the Object Selector tree view. You must use the pane on the right to view and access child objects that exist beyond the 15th level.

Format Selectors

A format selector is an icon or set of icons in a window, screen, or dialog that allows you to change the display of the data. In many cases, you can choose to view the data in rows or in a tabbed display.

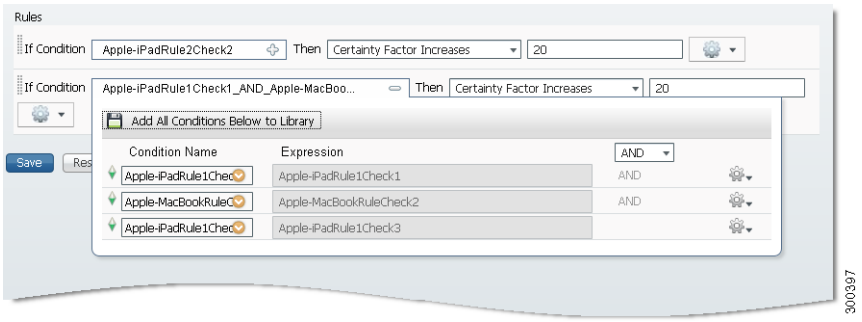
Figure 2-18 Format Selectors

Expression Builders

An expression builder is a pop-up dialog that makes it easier to create expressions, such as those used for authorization policies. You can make your selections interactively to quickly create an expression, such as the one shown in Figure 2-19. Click outside the expression builder to automatically close the dialog.

For information on how to use expression builders to create policies, see Chapter 16, “Managing Authentication Policies.”

Figure 2-19 Expression Builder



Understanding the Impact of Roles and Admin Groups

Cisco ISE provides role-based access control (RBAC) policies that ensure security by restricting administrative privileges. RBAC policies are associated with default admin groups to define roles and permissions. A standard set of permissions (for menu as well as data access) is paired with each of the predefined admin groups, and is thereby aligned with the associated role and job function.

RBAC restricts system access to authorized users through the use of roles that are then associated with admin groups. Each admin group has the ability to perform certain tasks with permissions that are defined by an RBAC policy. Policies restrict or allow a person to perform tasks that are based on the admin group (or groups) to which that person is assigned. You can be assigned to multiple roles, which provides you with privileges for each role to which you are assigned.

Warning **Read-only functionality is unavailable for any administrative access in Cisco ISE, Release 1.1. Regardless of the level of access, any administrator account can modify or delete objects for which it has permission, on any screen that it can access.**

A specialized administrator role has the ability to customize permissions and admin groups and to create custom policies. The default Cisco ISE RBAC policies cannot be modified, however. For information on the default groups and their assigned permissions, see Chapter 4, “Managing Identities and Admin Access.”

Note Some features in the user interface require certain permissions for their use. If a feature is unavailable, or you are not allowed to perform a specific task, your admin group may not have the necessary permissions to perform the task that utilizes the feature. Resources are accessed based on permission, which can be tracked via ise-rbac.log. For more information, see Chapter 4, “Managing Identities and Admin Access.”