

Specifying User Preferences

The following topics describe how to specify user preferences:

- User Preferences Introduction, on page 1
- Changing Your Password, on page 1
- Changing an Expired Password, on page 2
- Specifying Your Home Page, on page 2
- Configuring Event View Settings, on page 3
- Setting Your Default Time Zone, on page 7
- Specifying Your Default Dashboard, on page 7

User Preferences Introduction

Depending on your user role, you can specify certain preferences for your user account.

In a multidomain deployment, user preferences apply to all domains where your account has access. When specifying home page and dashboard preferences, keep in mind that certain pages and dashboard widgets are constrained by domain.

Changing Your Password

All user accounts are protected with a password. You can change your password at any time, and depending on the settings for your user account, you may have to change your password periodically.

If password strength checking is enabled, passwords must be at least eight alphanumeric characters of mixed case and must include at least one numeric character. Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.

If you are an LDAP or a RADIUS user, you cannot change your password through the web interface.

Procedure

Step 1 From the drop-down list under your user name, choose **User Preferences**.

Step 2 Enter your **Current Password**, and click **Change**.

Step 3 In the **New Password** and **Confirm** fields, enter your new password.

Step 4 Click **Change**.

Changing an Expired Password

Depending on the settings for your user account, your password may expire. The password expiration time period is set when your account is created. If your password has expired, the Password Expiration Warning page appears.

Procedure

On the Password Expiration Warning page, you have two choices:

- Click **Change Password** to change your password now. If you have zero warning days left, you **must** change your password.

  Tip If password strength checking is enabled, passwords must be at least eight alphanumeric characters of mixed case and must include at least one numeric character. Passwords cannot be a word that appears in a dictionary or include consecutive repeating characters.

- Click **Skip** to change your password later.

Specifying Your Home Page

You can specify the page within the web interface to use as your home page for the appliance. The default home page is the default dashboard (**Overview** > **Dashboards**), except for user accounts with no dashboard access, such as External Database users. (See Specifying Your Default Dashboard, on page 7 to set the default dashboard.)

In a multidomain deployment, the home page you choose applies to all domains where your user account has access. When choosing a home page for an account that frequently accesses multiple domains, keep in mind that certain pages are constrained to the Global domain.

Procedure

Step 1 From the drop-down list under your user name, choose **User Preferences**.

Step 2 Click **Home Page**.

Step 3 Choose the page you want to use as your home page from the drop-down list.

The options in the drop-down list are based on the access privileges for your user account. For more information, see User Account Privileges.

Step 4 Click **Save**.

Configuring Event View Settings

Use the Event View Settings page to configure characteristics of event views on the Firepower Management Center. Note that some event view configurations are available only for specific user roles. Users with the External Database User role can view parts of the event view settings user interface, but changing those settings has no meaningful result.

Procedure

Step 1 From the drop-down list under your user name, choose **User Preferences**.

Step 2 Click **Event View Settings**.

Step 3 In the **Event Preferences** section, configure the basic characteristics of event views; see Event View Preferences, on page 3.

Step 4 In the **File Preferences** section, configure file download preferences; see File Download Preferences, on page 4.

Step 5 In the **Default Time Windows** section, configure the default time window or windows; see Default Time Windows, on page 5.

Step 6 In the **Default Workflow** sections, configure default workflows; see Default Workflows, on page 7.

Step 7 Click **Save**.

Event View Preferences

Use the Event Preferences section of the Event View Settings page to configure basic characteristics of event views in the Firepower System. This section is available for all user roles, although it has little to no significance for users who cannot view events.

The following fields appear in the Event Preferences section:

- The **Confirm "All" Actions** field controls whether the appliance forces you to confirm actions that affect all events in an event view.

  For example, if this setting is enabled and you click **Delete All** on an event view, you must confirm that you want to delete all the events that meet the current constraints (including events not displayed on the current page) before the appliance will delete them from the database.

- The **Resolve IP Addresses** field allows the appliance, whenever possible, to display host names instead of IP addresses in event views.

  Note that an event view may be slow to display if it contains a large number of IP addresses and you have enabled this option. Note also that for this setting to take effect, you must use management interfaces configuration to establish a DNS server in the system settings.

- The **Expand Packet View** field allows you to configure how the packet view for intrusion events appears. By default, the appliance displays a collapsed version of the packet view:
  - **None** - collapse all subsections of the Packet Information section of the packet view
  - **Packet Text** - expand only the Packet Text subsection

- **Packet Bytes** - expand only the Packet Bytes subsection
- **All** - expand all sections

Regardless of the default setting, you can always manually expand the sections in the packet view to view detailed information about a captured packet.

- The **Rows Per Page** field controls how many rows of events per page you want to appear in drill-down pages and table views.
- The **Refresh Interval** field sets the refresh interval for event views in minutes. Entering `0` disables the refresh option. Note that this interval does not apply to dashboards.
- The **Statistics Refresh Interval** controls the refresh interval for event summary pages such as the Intrusion Event Statistics and Discovery Statistics pages. Entering `0` disables the refresh option. Note that this interval does not apply to dashboards.
- The **Deactivate Rules** field controls which links appear on the packet view of intrusion events generated by standard text rules:
  - **All Policies** - a single link that deactivates the standard text rule in all the locally defined custom intrusion policies
  - **Current Policy** - a single link that deactivates the standard text rule in only the currently deployed intrusion policy. Note that you cannot deactivate rules in the default policies.
  - **Ask** - links for each of these options

To see these links on the packet view, your user account must have either Administrator or Intrusion Admin access.

Related Topics

Management Interfaces

File Download Preferences

Use the File Preferences section of the Event View Settings page to configure basic characteristics of local file downloads. This section is only available to users with the Administrator, Security Analyst, or Security Analyst (Read Only) user roles.

Note that if your appliance does not support downloading captured files, these options are disabled.

The following fields appear in the File Preferences section:

- The **Confirm 'Download File' Actions** check box controls whether a File Download pop-up window appears each time you download a file, displaying a warning and prompting you to continue or cancel.



Caution Cisco strongly recommends you do **not** download malware, as it can cause adverse consequences. Exercise caution when downloading any file, as it may contain malware. Ensure you have taken any necessary precautions to secure the download destination before downloading files.

Note that you can disable this option any time you download a file.

- When you download a captured file, the system creates a password-protected .zip archive containing the file. The **Zip File Password** field defines the password you want to use to restrict access to the .zip file. If you leave this field blank, the system creates archive files without passwords.
- The **Show Zip File Password** check box toggles displaying plain text or obfuscated characters in the **Zip File Password** field. When this field is cleared, the **Zip File Password** displays obfuscated characters.

Default Time Windows

The time window, sometimes called the time range, imposes a time constraint on the events in any event view. Use the Default Time Windows section of the Event View Settings page to control the default behavior of the time window.

User role access to this section is as follows:

- Administrators and Maintenance Users can access the full section.
- Security Analysts and Security Analysts (Read Only) can access all options except **Audit Log Time Window**.
- Access Admins, Discovery Admins, External Database Users, Intrusion Admins, Network Admins, and Security Approvers can access only the **Events Time Window** option.

Note that, regardless of the default time window setting, you can always manually change the time window for individual event views during your event analysis. Also, keep in mind that time window settings are valid for only the current session. When you log out and then log back in, time windows are reset to the defaults you configured on this page.

There are three types of events for which you can set the default time window:

- The **Events Time Window** sets a single default time window for most events that can be constrained by time.
- The **Audit Log Time Window** sets the default time window for the audit log.
- The **Health Monitoring Time Window** sets the default time window for health events.

You can only set time windows for event types your user account can access. All user types can set event time windows. Administrators, Maintenance Users, and Security Analysts can set health monitoring time windows. Administrators and Maintenance Users can set audit log time windows.

Note that because not all event views can be constrained by time, time window settings have no effect on event views that display hosts, host attributes, applications, clients, vulnerabilities, user identity, or compliance white list violations.

You can either use **Multiple** time windows, one for each of these types of events, or you can use a **Single** time window that applies to all events. If you use a single time window, the settings for the three types of time window disappear and a new **Global Time Window** setting appears.

There are three types of time window:

- *static*, which displays all the events generated from a specific start time to a specific end time
- *expanding*, which displays all the events generated from a specific start time to the present; as time moves forward, the time window expands and new events are added to the event view

- *sliding*, which displays all the events generated from a specific start time (for example, one day ago) to the present; as time moves forward, the time window "slides" so that you see only the events for the range you configured (in this example, for the last day)

The maximum time range for all time windows is from midnight on January 1, 1970 (UTC) to 3:14:07 AM on January 19, 2038 (UTC).

The following options appear in the **Time Window Settings** drop-down list:

- The **Show the Last - Sliding** option allows you configure a sliding default time window of the length you specify.

  The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the present. As you change event views, the time window "slides" so that you always see events from the last hour.

- The **Show the Last - Static/Expanding** option allows you to configure either a static or expanding default time window of the length you specify.

  For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

  For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from a specific start time (for example, 1 hour ago) to the present. As you change event views, the time window expands to the present time.

- The **Current Day - Static/Expanding** option allows you to configure either a static or expanding default time window for the current day. The current day begins at midnight, based on the time zone setting for your current session.

  For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from midnight to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

  For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from midnight to the present. As you change event views, the time window expands to the present time. Note that if your analysis continues for over 24 hours before you log out, this time window can be more than 24 hours.

- The **Current Week - Static/Expanding** option allows you to configure either a static or expanding default time window for the current week. The current week begins at midnight on the previous Sunday, based on the time zone setting for your current session.

  For **static** time windows, enable the **Use End Time** check box. The appliance displays all the events generated from midnight to the time when you first viewed the events. As you change event views, the time window stays fixed so that you see only the events that occurred during the static time window.

  For **expanding** time windows, disable the **Use End Time** check box. The appliance displays all the events generated from midnight Sunday to the present. As you change event views, the time window expands to the present time. Note that if your analysis continues for over 1 week before you log out, this time window can be more than 1 week.

Default Workflows

A workflow is a series of pages displaying data that analysts use to evaluate events. For each event type, the appliance ships with at least one predefined workflow. For example, as a Security Analyst, depending on the type of analysis you are performing, you can choose among ten different intrusion event workflows, each of which presents intrusion event data in a different way.

The appliance is configured with a default workflow for each event type. For example, the Events by Priority and Classification workflow is the default for intrusion events. This means whenever you view intrusion events (including reviewed intrusion events), the appliance displays the Events by Priority and Classification workflow.

You can, however, change the default workflow for each event type. The default workflows you are able to configure depend on your user role. For example, intrusion event analysts cannot set default discovery event workflows.

Setting Your Default Time Zone

This setting determines the times displayed in the web interface for your user account only, for things like task scheduling and viewing dashboards. This setting does not change the system time or affect any other user, and does not affect data stored in the system, which generally uses UTC.

Warning The Time Zone function (in User Preferences) assumes that the system clock is set to UTC time. DO NOT ATTEMPT TO CHANGE THE SYSTEM TIME. Changing the system time from UTC is NOT supported, and doing so will require you to reimage the device to recover from an unsupported state.

Procedure

Step 1 From the drop-down list under your user name, choose **User Preferences**.

Step 2 Click **Time Zone**.

Step 3 Choose the continent or area that contains the time zone you want to use.

Step 4 Choose the country and state name that corresponds with the time zone you want to use.

Specifying Your Default Dashboard

The default dashboard appears when you choose **Overview** > **Dashboards**. Unless changed, the default dashboard for all users is the Summary dashboard. You can change the default dashboard if your user role is Administrator, Maintenance, or Security Analyst.

In a multidomain deployment, the default dashboard you choose applies to all domains where your user account has access. When choosing a dashboard for an account that frequently accesses multiple domains, keep in mind that certain dashboard widgets are constrained by domain.

Procedure

Step 1 From the drop-down list under your user name, choose **User Preferences**.

Step 2 Click **Dashboard Settings**.

Step 3 Choose the dashboard you want to use as your default from the drop-down list. If you choose **None**, when you select **Overview** > **Dashboards**, you can then choose a dashboard to view.

Step 4 Click **Save**.

Related Topics

Viewing Dashboards