System Configuration

This chapter explains how to configure system configuration settings on the Secure Firewall Management Center.

Requirements and Prerequisites for the System Configuration

Model Support

Management Center

Supported Domains

Global

User Roles

Admin

Manage the Secure Firewall Management Center System Configuration

The system configuration identifies basic settings for the management center.

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Use the navigation panel to choose configurations to change.

Access Control Preferences

Configure access control preferences on **System** (⚙) > **Configuration** > **Access Control Preferences**.

Requiring Comments on Rule Changes

You can track changes to access control rules by allowing (or requiring) users to comment when they save. This allows you to quickly assess why critical policies in a deployment were modified. By default, this feature is disabled.

Object Optimization

When you deploy rule policies to a firewall device, you can configure the management center to evaluate and optimize the network/host policy objects that you use in the rules when it creates the associated network object groups on the device. Optimization merges adjacent networks and removes redundant network entries. This reduces the runtime access list data structures and the size of the configuration, which can be beneficial to some firewall devices that are memory-constrained.

For example, consider a network/host object that contains the following entries and that is used in an access rule:

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

When optimization is enabled, when you deploy the policy, the resulting object group configuration is generated:

```
object-group network test
description (Optimized by management center)
network-object 10.1.1.0 255.255.255.252
network-object 192.168.1.0 255.255.255.0
```

When optimization is disabled, the group configuration would be as follows:

```
object-group network test
network-object 192.168.1.0 255.255.255.0
network-object 192.168.1.23 255.255.255.255
network-object 10.1.1.0 255.255.255.255
network-object 10.1.1.1 255.255.255.255
network-object 10.1.1.2 255.255.255.254
```

This optimization does not change the definition of the network/host object, nor does it create a new network/host policy object. If a network object-group contains another network, host object, or object-groups, the objects are not combined. Instead, each network object-group is optimized separately. Also, only inline values of network object-groups are being modified as part of the optimization process during a deployment.

Important The optimizations occur on the *managed device* on the *first deploy* after the feature is enabled on the management center. If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled. After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time.

This feature is enabled by default. To disable it, contact Cisco TAC.

Change Reconciliation

To monitor the changes that users make and ensure that they follow your organization's preferred standard, you can configure the system to send, via email, a detailed report of changes made over the past 24 hours. Whenever a user saves changes to the system configuration, a snapshot is taken of the changes. The change reconciliation report combines information from these snapshots to present a clear summary of recent system changes.

The following sample graphic displays a User section of an example change reconciliation report and lists both the previous value for each configuration and the value after changes. When users make multiple changes to the same configuration, the report lists summaries of each distinct change in chronological order, beginning with the most recent.

You can view changes made during the previous 24 hours.

Configuring Change Reconciliation

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Click **Change Reconciliation**.

Step 3 Check the **Enable** check box.

Step 4 Choose the time of day you want the system to send out the change reconciliation report from the **Time to Run** drop-down lists.

Step 5 Enter email addresses in the **Email to** field.

Tip
Once you have added email addresses, click **Resend Last Report** to send recipients another copy of the most recent change reconciliation report.

Step 6 If you want to include policy changes, check the **Include Policy Configuration** check box.

Step 7 If you want to include all changes over the past 24 hours, check the **Show Full Change History** check box.

Step 8 Click **Save**.

Related Topics

Using the Audit Log to Examine Changes

Change Reconciliation Options

The **Include Policy Configuration** option controls whether the system includes records of policy changes in the change reconciliation report. This includes changes to access control, intrusion, system, health, and network discovery policies. If you do not select this option, the report will not show changes to any policies. This option is available on management centers only.

The **Show Full Change History** option controls whether the system includes records of all changes over the past 24 hours in the change reconciliation report. If you do not select this option, the report includes only a consolidated view of changes for each category.

Note The change reconciliation report does not include changes to threat defense interfaces and routing settings.

Change Management

You can enable Change Management if your organization needs to implement more formal processes for configuration changes, including audit tracking and official approval before changes are deployed.

When you enable Change Management, the system adds the **Ticket** ( ) shortcut to the menu bar, and **Change Management Workflow** to the **System** ( ) menu. Users can manage tickets using these methods.

For details about how to use Change Management, see Change ManagementFor details, see the Change Management chapter in Cisco Secure Firewall Management Center Device Configuration Guide.

On the **System** ( ) > **Configuration** page, you can configure the following settings. Click **Save** to save your changes.

- **Enable Change Management**—Turn on ticketing and the Change Management workflow. Once enabled, you must approve or discard all tickets to turn off Change Management.

  To disable the feature, deselect the option. All tickets must be approved or discarded to disable Change Management. You cannot disable Change Management if any ticket is in the In Progress, On Hold, Rejected, or Pending Approval state.

- **Number of approvals required**—How many administrators must approve the change for the ticket to be approved and deployable. The default is 1, but you can require up to 5 approvers per ticket. Users can override this number when creating tickets.

Note When Change Management is enabled and in use, you cannot change the number of approvers if at least one ticket is in the In Progress, On Hold, Rejected, or Pending Approval state. All tickets must be approved or discarded to change the required number of approvers.

- **Ticket Purge Duration**—The number of days to keep approved tickets, from 1-100 days. The default is 5 days.
- **Email Notification** (Optional)—Enter the **Reply to Address** and the email addresses for the **List of Approver Addresses**. You must also configure the Email Notification system settings for email to work.

  For Cloud-delivered Firewall Management Center, the reply to address does not appear. Instead, configure this address in the Email Notification system settings.

Notes

There are several system processes that prevent you from enabling/disabling change management. If any of the following are in process, you need to wait for them to complete before changing these settings: backup/restore; import/export; domain movement; upgrade; Flexconfig migration; device registration; high-availability registration, creation, break, or switch; cluster create, registration, break, edit, add or remove nodes; EPM break out or join.

An access control policy cannot be locked when you change these settings. If a policy is locked, you must wait for the lock to be released before enabling/disabling this feature.

Email Notification

You cannot configure a mail host. The mail relay host is hardcoded to be used from a static host. It is set to email-smtp.us-west-2.amazonaws.com with authorization. For notifications, the email sender is set to cdo-alert@cisco.com

Intrusion Policy Preferences

Configure various intrusion policy preferences to monitor and track changes to the critical policies in your deployment.

Set Intrusion Policy Preferences

Configure the intrusion policy preferences.

Procedure

Step 1 Choose **System** (⚙) > **Configuration**.

Step 2 Click **Intrusion Policy Preferences**.

Step 3 You have the following options:

- **Comments on policy change**: Check this check box to track policy-related changes using the comment functionality when users modify intrusion policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

  If you enable comments on policy changes, you can make the comment optional or mandatory. The management center prompts the user for a comment when each new change to a policy is saved.

- **Write changes in Intrusion Policy to audit log**: Check this check box to record the changes to the intrusion policies to the audit logs. This option is enabled by default.
- **Retain user overrides for deleted Snort 3 rules**: Check this check box to get notifications for changes to any *overridden* system-defined rules during LSP updates. When enabled, the system retains the rule overrides in the new replacement rules that are added as part of the LSP update. On the management center menu bar, click **Notifications** > **Tasks** to view the notifications. This option is enabled by default.
- **Talos Threat Hunting Telemetry**: Check this check box to allow Cisco Talos to conduct threat hunting and to gather critical security intelligence. When enabled, a special set of threat-hunting rules is added to the global intrusion policy. Although the threat-hunting rules are processed like regular IPS rules, the events that the Talos threat hunting rules generate do not appear in the management center's event tables. Instead, the events are sent to Talos as telemetry for analysis. This option is enabled by default.

Note

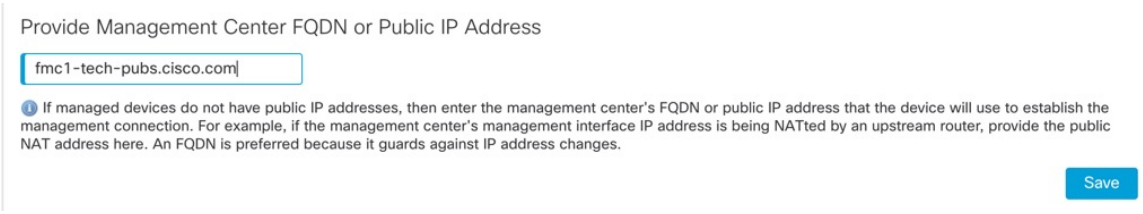
- If you send firewall events to the Cisco Security Cloud via a direct connection by registering your management center to the cloud tenancy using your Security Cloud Control account, your Security Cloud Control account must have a Security Analytics and Logging license in order to forward threat-hunting rule events to Talos.

Manager Remote Access

If managed devices do not have public IP addresses, then enter the management center's FQDN or public IP address that the device will use to establish the management connection. For example, if the management center's management interface IP address is being NATted by an upstream router, provide the *public* NAT address here. An FQDN is preferred because it guards against IP address changes.

If you use the serial number (zero-touch provisioning) method to register a device, then this field is used automatically for the initial configuration of the manager IP address/hostname. If you use the manual method, you can refer to the value on this screen when you perform the device's initial configuration to identify the public management center IP address/hostname.

Figure 1: Manager Remote Access



Network Analysis Policy Preferences

You can configure the system to track policy-related changes using the comment functionality when users modify network analysis policies. With policy change comments enabled, administrators can quickly assess why critical policies in a deployment were modified.

If you enable comments on policy changes, you can make the comment optional or mandatory. The system prompts the user for a comment when each new change to a policy is saved.

Optionally, you can have changes to network analysis policies written to the audit log.