

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.

- Change management, on page 1
- Requirements and prerequisites for change management, on page 5
- Guidelines and limitations for change management, on page 6
- Enabling or disabling change management, on page 6
- Manage tickets, on page 7
- History for change management, on page 13

Change management

Change management is a formal process that

- enforces an official approval process before configuration changes can be made to a device,
- requires administrators to open tickets before they can make configuration changes, and
- ensures that the right employees make the final decisions through submission and approval of tickets.

Change management characteristics

When using change management, the system implements these controls:

- Administrators can see their own changes within a ticket, but they cannot see changes anyone else has made within a ticket
- A policy is locked once a user makes a change within a ticket, preventing interfering changes
- Users cannot make changes while another user has made a change that is pending approval

Administrators can create multiple tickets so that a single ticket contains only logically-related policy changes. Tickets with a more limited scope are also easier to evaluate and approve quickly.

Make configuration changes in the change management workflow

This task enables configuration specialists to make configuration changes to supported policies and objects when change management is enabled.

When you enable change management, users who configure devices and shared policies need to change their approach slightly. Configuration specialists need to take the following approach when making configuration changes to supported policies and objects.

Procedure

Step 1 Create a ticket.

Step 2 Open the ticket.

Step 3 Make the configuration changes.

Note that the procedures explained in the online help and user guides assume that change management is not active, and omit any steps for creating, opening, or submitting tickets.

Step 4 Optionally, preview and validate the ticket to ensure the changes are complete and correct.

Step 5 Submit the ticket. At this point, the approver can either approve or reject the ticket.

- If the ticket is approved, deploy the changes.
- If the ticket is rejected, address the issues, and resubmit the ticket.

The configuration changes are successfully implemented through the change management workflow with proper approval and deployment processes.

Create separate approver and configuration roles

Separate approver and configuration roles are system-defined and custom roles that

- have permissions to modify (create/open/discard) and review (approve/reject/take over) tickets,
- provide granular access control to separate ticket approval from configuration changes, and
- ensure that ticket approval is assigned only to users who have organizational authority to approve changes.

System-defined roles and permissions

Some system-defined roles have permissions to modify (create/open/discard) and review (approve/reject) tickets:

- To both modify and review tickets:
  - Admin
  - Network Admin
- To modify tickets only:
  - Access Admin
  - Intrusion Admin
- To review tickets only:

- Security Approver

If you need more granular roles to separate these activities due to your organizational requirements, you can create separate roles to ensure that ticket approval is assigned only to those users who have the organizational authority to approve changes. To create new user roles, go to **System** (⚙) > **Users** > **User Roles**.

These are the permissions, in the **System** (⚙) > **Configuration** > **Change Management** folder, relevant to ticket usage and approval. Note that these permissions are available only after you enable change management.

- Modify Tickets—To create tickets (for yourself), to use tickets for configuration changes, and to discard tickets.
- Review Tickets—To approve or reject tickets.
- Both Modify and Review Tickets—To create tickets for yourself and others, use tickets, and approve/reject tickets. You can also take over tickets assigned to other users.

The approach you take depends on your precise requirements. For example:

- If your approvers should also be allowed to make configuration changes, you can simply assign them the system-defined roles, such as Administrator. Then, create custom configuration-only roles that include the same permissions but not the Review Tickets permission.
- If you need complete separation between approvers and those who make configuration changes, create custom roles for both, limiting the roles to either the Modify Tickets or the Review Tickets permission plus all other needed permissions for viewing or changing the supported policies and objects.

Policies and objects that support change management

If a policy or object supports the change management workflow, then creating, editing, or deleting the policy or object, including assigning a policy to a device, must be done in an open ticket.

Any action, policy, or object that does not support the change management workflow can be created, edited, or deleted, and so forth, without an open ticket. Even if a ticket is open, the changes made to unsupported policies are not included in the ticketed changes and are available for deployment immediately.

This information includes the policies and objects that are supported. Anything not listed is unsupported.

Supported policies

- Access control, including rules, references to other policies, and inheritance settings. Cloning access control policies is not included within a ticket. The clone is immediately accepted and available to all users.
- Device configuration policies:
  - Interfaces
  - Inline sets
  - DHCP
  - VTEP
  - All routing

- Decryption policy
- DNS policy
- FlexConfig
- Intrusion policy and network analysis policy (NAP), Snort 3 only.
- Malware and file policy
- Network address translation (NAT)
- Network discovery policy
- Platform settings
- Prefilter policy
- QoS
- Umbrella SASE topology
- VPN policies, both site-to-site and remote access
- Zero trust access

Supported objects

- AAA server
- Access list
- Address pools
- AS path
- Cipher suit lists
- Community list
- Distinguished name objects
- DHCP IPv6 pools
- DNS server group
- FlexConfig objects
- Group policy
- Interface
- Key chain
- Network
- PKI certificates, all objects
- Policy list
- Port

- Prefix list
- PKI certificates, all objects
- Route map
- Sinkhole
- SLA monitor
- Time range
- Time zone
- Tunnel zone
- URL
- Variable set
- VLAN tag
- VPN objects (IKEv1, IKEv2 IPSec and policy, PKI enrollment, certificate map)

Requirements and prerequisites for change management

This reference provides the requirements and prerequisites necessary to configure change management functionality.

Model support

Management center

Supported domains

Any

User roles

- To enable or disable change management: Admin.
- To both modify and review tickets:
  - Admin
  - Network Admin
- To modify tickets only:
  - Access Admin
  - Intrusion Admin
- To review tickets only:
  - Security Approver

Guidelines and limitations for change management

When operating in change management mode, users can make changes to supported policies, but they cannot save the changes. For example, you could go through the dialog box to create a new platform settings policy without an open ticket, but when you click OK to actually create the policy, you will get an error and the policy will not be created.

The following activities require that all tickets be in a terminal state, that is, approved or discarded: backup/restore, moving a device between domains, upgrading Firewall Management Center.

Deleting a device from the inventory requires that all tickets involving that device be approved or discarded.

Some system processes prevent you from enabling or disabling change management. Wait until the following processes complete before you enable or disable change management:

- critical management center processes, including SRU updates, LSP updates, VDB updates, and management center upgrades
- pending or running background activities, including device registration; cluster auto-registration; Firewall Threat Defense high availability operations; high availability auto-registration; FlexConfig migration; cluster creation, break, edit, reconcile, or node changes; device-template creation or application; device-model migration; and EPM join or breakout
- system jobs, including backup or restore, device import or export, general import, and domain movement.

Your ability to create objects while configuring a feature is constrained based on whether the feature and objects are all supported by change management. For example, importing a configuration is not supported by change management. Therefore, you cannot create security zone objects, which are supported, during the import. On the other hand, you can create new objects while configuring access control rules, because both are supported.

When using Cloud-Delivered Firewall Management Center, a user defined in Security Cloud Control is available to be assigned tickets only after the user cross-launches cdFMC at least once. Until the first cross-launch, the user does not exist in cdFMC.

Enabling or disabling change management

Enable or disable change management to control whether users must open tickets and get approval when making configuration changes to the system.

The default is that the change management workflow is disabled. Users do not need to open tickets and get approval when making configuration changes. If you want to enforce the change management workflow, you must enable it globally for the system.

Before you begin

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.

Follow these steps to enable or disable change management:

Procedure

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

Step 2 Click **Change Management**.

Step 3 Select **Enable 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.

Step 4 Select the **Number of approvals required**, which is 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.

Step 5 Select the **Ticket Purge Duration**, which is the number of days to keep approved tickets, from 1-100 days. The default is 5 days.

Step 6 (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.

Step 7 Click **Save**.

The system adds the **Ticket** (▣) shortcut to the menu bar, and the **System** (⚙) > **Change Management Workflow** command. Users can manage tickets using these methods.

Change management is enabled or disabled according to your configuration. If enabled, the system adds ticket management shortcuts to the interface, and users must follow the change management workflow when making configuration changes.

Manage tickets

This task enables you to manage change management tickets for configuration changes to supported policies that require approval workflow.

When you enable change management, configuration changes for supported policies must be done within the context of a ticket. You open a ticket, make your changes, then submit the ticket for approval.

You can see a list of tickets, and create new ones, either on the change management page or through the ticket quick-access menu. All ticket changes are synchronized in each menu, so you can switch back and forth at your convenience and use whichever method you prefer.



Note When you open a ticket and make a change to a supported policy, that policy is locked from changes by other users or through other tickets. The policy remains locked until the ticket is approved or discarded.

Procedure

Step 1 Do any of these actions:

- Choose **System** (⚙) > **Change Management Workflow** to open a page showing existing tickets.
- Click the **Ticket** (🎫) quick-access menu. The icon can either be named Select a Ticket (if no ticket is opened), the ticket name if a ticket is opened, or unnamed if no tickets exist.

Both pages are organized the same. The **Ticket** tab lists all tickets, whereas the **Review** tab lists tickets that have been submitted for approval. The default view shows your tickets only.

Step 2 On the **Ticket** tab, take any of these actions:

- To create a new ticket, click **Add Ticket**.
- To view the details of a ticket, click the > next to the ticket name. The Details page includes UUID, name, description, user, last modified date, and comments. The History page includes the status changes for the ticket. The image at the top shows where the ticket stands in the overall workflow.
- To preview the configuration changes for an open ticket, click **Preview** (🔍).
- To validate the configuration changes in an open ticket, click **Validate** (✓) or **More** (⋮) > **Validate**. A dialog box opens showing error, warning, and informational messages, if there are any validation errors.
- To open a ticket, click **Open** (📂) or **More** (⋮) > **Open**. To close an open ticket, click **Put Ticket on Hold (X)** or **More** (⋮) > **Put Ticket on Hold**. Closing a ticket does not submit it for review, nor does it release any locks placed on edited policies.
- To submit an open ticket for review and approval, click **Submit for Approval** (📝) or **More** (⋮) > **Submit for Approval**. The ticket must be open to be submitted.
- To discard a ticket, click **Discard** (🗑) or **More** (⋮) > **Discard**.
- To take over or reassign a ticket, click **More** (⋮) > **Take Over Ticket** when viewing all tickets in the system.
- To search for a ticket, type a string in the search box. The search looks at ticket name, description, and responsible user. To filter the list by ticket status (on the change management workflow page), click the status above the list: **New**, **Open**, **On Hold** (ticket was closed), **Rejected**, **Pending Approval**, **Approved**. Each status has a count of the number of tickets in that state. Click **All** under **My Tickets** to return to the default of showing all of your tickets, or **All** under **Tickets in System** to see everyone's tickets.

Step 3 On the **Reviews** tab, take any of these actions on submitted tickets.

The list is empty if there are no submitted tickets. In addition, only users with Review Ticket permissions can see this tab.

- To preview the configuration changes for a ticket, click **Preview** (🔍).
- To validate the configuration changes in an open ticket, click **Validate** (✓) or **More** (⋮) > **Validate**.
- To approve the ticket, click **Approve** (✓) or **More** (⋮) > **Approve**.

- To disapprove the ticket, click **Reject** (✕) or **More** (⋮) > **Reject**.

You have successfully managed your change management tickets. Approved tickets can proceed with configuration changes, while rejected tickets require revision before resubmission.

Create change management tickets

Create change management tickets to ensure all configuration changes are performed within the context of an approved workflow ticket.

When using the change management workflow, you must do all configuration changes within the context of an open ticket. If you do not already have a ticket, you must create a new one.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (🎫) shortcut menu.

Step 2 Click **Add Ticket**.

Step 3 Configure the ticket options:

- **Name**—The name of the ticket. The name can include letters, numbers, spaces, and the following special characters: #-_!
- **Description**—An optional description of what you intend to configure using this ticket. For example, if you have a case number related to what you intend to fix using this ticket, that would be useful information in a description.
- **Number of Approvers**—How many administrators must approve the change for the ticket to be approved and deployable. You can specify 1-5.
- **Assign to**—Select the user who will own the ticket and be responsible for implementing the changes. Choose **self** to assign it to yourself.

Step 4 Click one of the following:

- **Create**—The ticket is added to the list of tickets, but it is not opened. You need to open it before you can work within the context of the ticket.
- **Create and Open**—The ticket is added to the list of tickets and also opened.

The change management ticket is created and available for use in the workflow. If you selected Create and Open, the ticket is immediately opened for configuration changes.

Opening a ticket for configuration changes

Open a ticket to enable configuration changes within the ticket management system.

Before you can make changes within a ticket, you must open the ticket.

If you have another ticket open, the system puts it on hold (closes it) for you before opening the new one.

Procedure

Step 1 Choose **System** ( ) > **Change Management Workflow**, or click the **Ticket** ( ) shortcut menu.

Step 2 On the **Tickets** tab, click **Open** ( ) or **More** ( ) > **Open** for the ticket.

Step 3 Optionally, enter a comment for the action.

Step 4 Click **Open**.

You can now start your configuration changes. The name of the ticket icon changes to the name of the open ticket.

The ticket is now open and ready for configuration changes. The ticket icon displays the name of the open ticket.

Preview a ticket

Preview a ticket to view all configuration changes made within the context of the ticket.

You can preview a ticket while making your configuration changes, or before approving it. The preview shows all configuration changes made within the context of the ticket.

Procedure

Step 1 Choose **System** ( ) > **Change Management Workflow**, or click the **Ticket** ( ) shortcut menu.

Step 2 Click **Preview** ( ) for the ticket.

The Preview dialog box opens. Changes are color coded according to the legend at the top of the dialog box.

Step 3 Select the policy whose changes you want to view in the Changed Policies list.

You are shown both the current version of the policy as it is defined in Secure Firewall Management Center (on the left) and the proposed changes defined within the ticket.

For policies that contain pages, such as platform settings, you can select the overall policy to see all changes, or specific pages within the policy, in the Changed Policies list.

You cannot alter the changes from within the preview. If you need to change something, you must close the preview and return to the policy you want to change.

Step 4 Optionally, click **Download as PDF** to save the preview to a PDF file for offline viewing or archival purposes.

Step 5 Click **OK**.

The ticket preview displays all configuration changes, allowing you to review them before approval or while making modifications.

Submit a ticket

Submit a ticket to apply changes made within the ticket after validation and review.

After you have completed the changes needed for a ticket, you can preview and validate the changes. Then, when you are satisfied with the changes, submit the ticket for review and approval.

Changes made within the ticket are not applied until you submit the ticket and the ticket is approved. Until approval happens, all policies modified within a ticket are locked to that ticket and cannot be changed by anyone else.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (▣) shortcut menu.

Step 2 Click **Submit for Approval** (✎) or **More** (⋮) > **Submit for Approval** for the open ticket.

Step 3 Optionally, enter a comment for your action.

Step 4 Click **Submit**.

The ticket is submitted for review and approval. Once approved, the changes made within the ticket are applied and the policies are unlocked.

Discard a ticket

Discard a ticket to remove any changes that were made within the ticket when you no longer need to proceed with those changes.

You cannot undo this action and retrieve a ticket with its changes. If you need them, you must create a new ticket and start over.

You cannot discard a ticket after you submit it. However, if the approver rejects the ticket, you can then discard it.



Note If you have permission to modify tickets, you can discard tickets that belong to another user. This makes it possible to deal with situations where an admin is on vacation or otherwise unavailable to manage an in-process ticket. If you have Review Ticket permission, you can alternatively reassign or take over the ticket rather than discard it.

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**, or click the **Ticket** (▣) shortcut menu.

Step 2 Click **Discard** (🗑) or **More** (⋮) > **Discard** for the ticket.

Step 3 Optionally, enter a comment for your action.

Step 4 Click **Discard**.

The ticket is discarded and any changes made within the ticket are removed.

Approving or rejecting a ticket

Approve or reject tickets to control which configuration changes become active and available for deployment in your network.

When a user submits a ticket, it must be approved for the changes made within the ticket to become active and available for deployment.

Whether you can approve your own tickets, or there is a separate approver, depends on your workplace policies and how user roles are assigned, not on the management software.

The Details view includes a summary of how many approvers are required for the ticket, and who has approved the ticket.

If the changes are inadequate or undesirable, you can reject the ticket. Rejected tickets go back to the submitter, who can then make additional changes and resubmit the ticket, or simply discard the ticket and the configuration changes it contains.

Procedure

Step 1 Choose **System** ( ) > **Change Management Workflow**, or click the **Ticket** ( ) shortcut menu.

Step 2 On the **Review** tab, click **Preview** ( ) for the ticket and evaluate the proposed changes.

You can also click **Validate** ( ) or **More** ( ) > **Validate** to check for errors.

Step 3 After completing your evaluation, do one of the following:

- To approve the ticket, click **Approve** ( ) or **More** ( ) > **Approve**.
- To disapprove the ticket, click **Reject** ( ) or **More** ( ) > **Reject**.

Step 4 Optionally, enter a comment for your action.

Step 5 Click **Approve** or **Reject**, as appropriate.

The ticket is approved or rejected based on your selection. Approved tickets become active and available for deployment. Rejected tickets return to the submitter for revision or disposal.

Take over or reassign tickets

Take over or reassign tickets to ensure continuous workflow management when the original ticket owner is unavailable or when ticket ownership needs to be transferred for deployment purposes.

Sometimes it might be necessary to take over a ticket that someone else created. For example, the ticket owner might be on vacation or is otherwise unavailable, and the ticket is blocking updates that need to be deployed.

You can also use this procedure to reassign your own ticket to another person.

Before you begin

Following are the permissions required to take over tickets:

- Admin user—You can assign tickets to yourself or other users.
- Modify or Review ticket + System > User Management > Users (custom role)—You can assign tickets to yourself or other users.

However, you can assign a user only if the user has the same role as the current ticket owner, or the Admin role. This ensures that the new user has the permissions required to configure the features currently modified within the ticket.

You cannot reassign a ticket that has been submitted for approval.

Follow these steps to take over or reassign tickets:

Procedure

Step 1 Choose **System** (⚙) > **Change Management Workflow**.

Step 2 Click on **All** under **Tickets in System**.

Step 3 Click **More** (⋮) > **Take Over Ticket**.

Step 4 Select the user who should now own the ticket.

The list of users is restricted to those who have the permissions required to edit the policies already changed within the ticket. For example, if a ticket contains changes to the access control policy, the list of users contains only those users who are allowed to modify the access control policy.

Step 5 Enter an optional comment and click **Takeover**.

The ticket ownership is transferred to the selected user, and the new owner can now manage and modify the ticket according to their permissions.

History for change management

The following table summarizes the feature changes by release for change management functionality.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Taking over tickets and additional support for change management.	7.6.0	Any	You can take over another user's ticket. This is useful if a ticket is blocking other updates to a policy and the user is unavailable. In addition, these features are now included in the change management approval workflow: decryption policies, DNS policies, file and malware policies, network discovery, certificates and certificate groups, cipher suite lists, distinguished name objects, sinkhole objects.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Change management.	7.4.1	Any	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. We added the **System**( ) > **Configuration** > **Change Management** page to enable the feature. When enabled, there is a **System**( ) > **Change Management Workflow** page, and a new **Ticket**( ) quick access icon in the menu.