Cisco Secure Workload and Secure Firewall Management Center Integration Guide

First Published: 2021-02-25

Last Modified: 2023-12-22

Secure Workload Integration with Secure Firewall Management Center

Feature History

Table 1: Feature History

Feature Name	Release	Feature Description	Where to Find
Segmentation Workflow Simplification	3.9.1.1	Simplified workflow for the mapping of Scope to Access Control Policies for Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD) enforcement. The enhanced API integration marks the decoupling of Segmentation and Virtual Patching workflows.	Segmentation in 3.9.1.1
Virtual Patching Workflow Simplification	3.8.1.36	Simplified workflow for workload or Common Vulnerability and Exposure (CVE) filtering.	Virtual Patching in 3.8.1.36

About this Integration

Integrate the capabilities of Cisco Secure Workload (previously Cisco Tetration) with the robust features of Cisco's Secure Firewall (formerly Cisco Firepower) to establish an agentless security solution specifically designed for:

- Segmenting workloads where software agents cannot be installed.

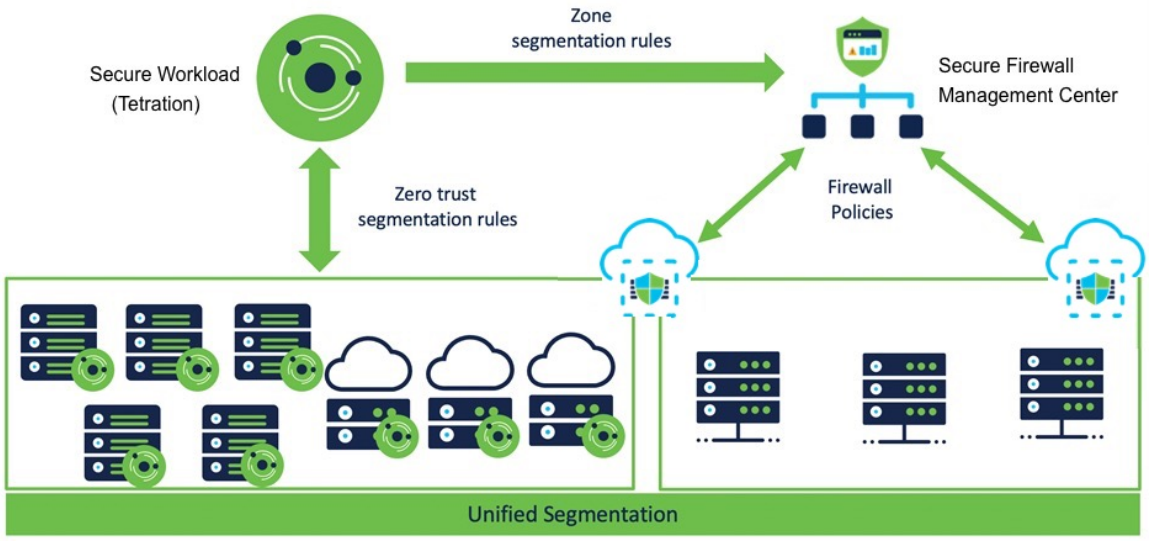
  For example, use this integration if you do not have control over workload operating systems (appliance-based software), or if workloads are running on legacy operating systems that are not supported by the agents.

- Segmenting traffic for different zones within your datacenter and cloud.

  For example, you can easily and broadly apply different sets of policies for traffic entering your network, for traffic exiting your network, and for traffic between workloads within your network.

With this integration, Secure Workload automatically enforces and manages segmentation policies on the Secure Firewall Threat Defense (formerly known as Firepower Threat Defense) firewalls managed by the Secure Firewall Management Center instance. Policies are updated dynamically, and the set of workloads to which policies apply is refreshed continually as the application environment changes.

Figure 1: Integration of Secure Workload with Secure Firewall Management Center



In Secure Workload versions 3.7 and 3.6: Secure Workload enforced segmentation policies are converted to access control policies based on IP address sets from scopes, inventory filters, and clusters converted to dynamic objects in Secure Firewall Management Center. For details, see Important Information for Secure Workload Versions 3.7 and 3.6, on page 5.

In Tetration version 3.5: Tetration segmentation policies are converted to Prefilter policies in Firepower Management Center.

All versions:

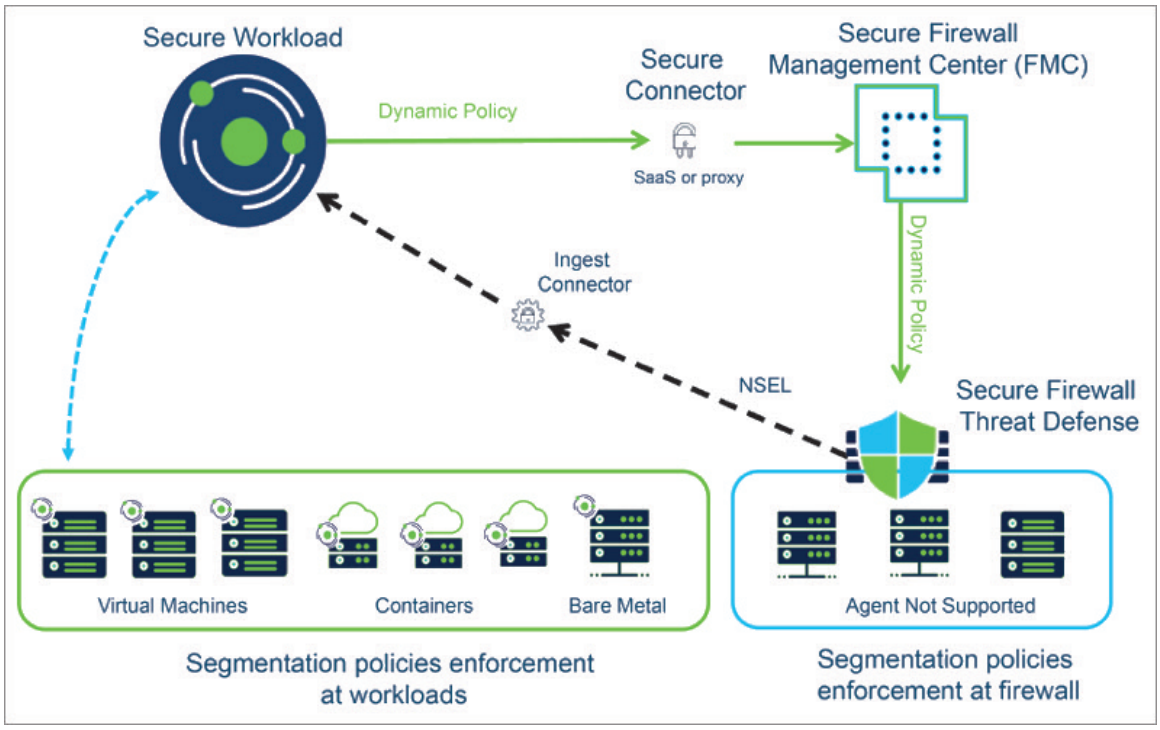
The Secure Firewall Management Center external orchestrator does not generate any user annotations.

Use this guide to deploy the applicable solution for your product versions.

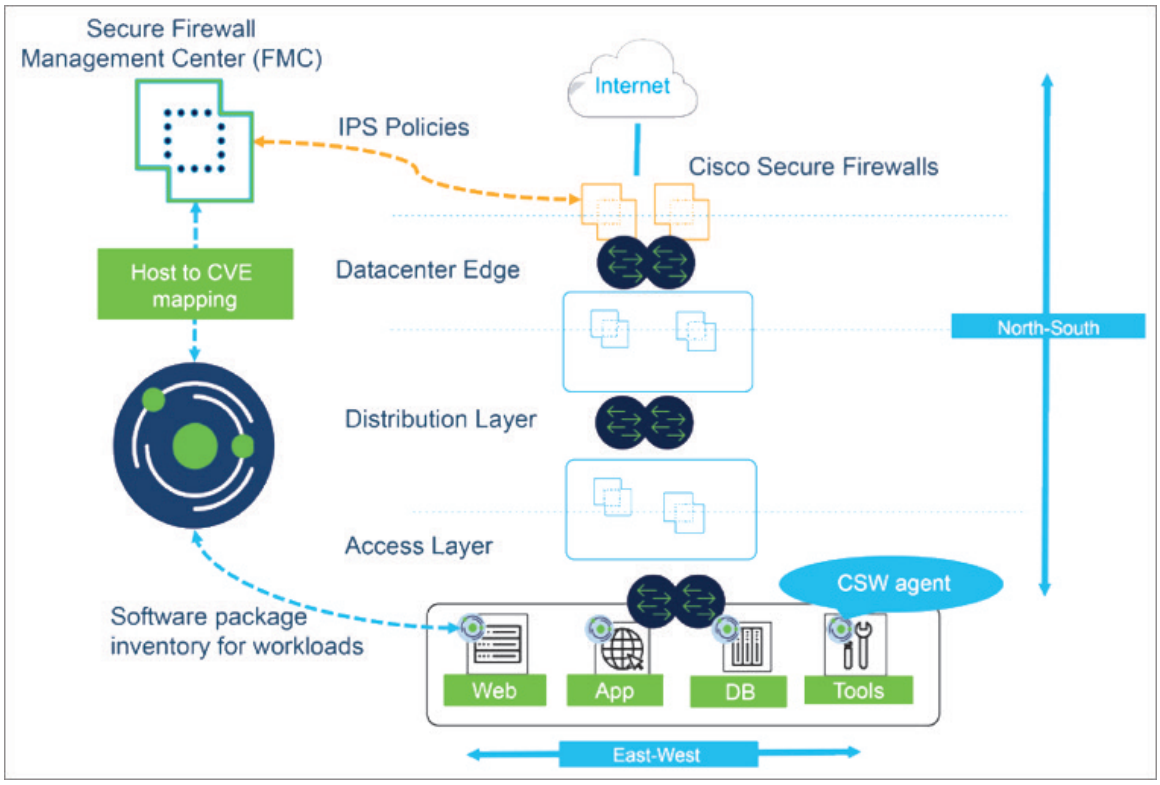
Important Information for Secure Workload Version 3.8

This integration offers the following features and benefits:

- Full visibility and enforcement for agentless workloads.
- Secure Workload is capable of ingesting NSEL records from Secure Firewall Management Center and automatically creating segmentation policies for agentless workloads.
- Secure Workload automatically pushes the enforced policies to Firewall Management Center.



- Secure Workload pushes the CVE information from agent-based workloads to Secure Firewall Management Center to augment the visibility of vulnerable workloads. This enables FMC to run firewall recommendations to adjust the Intrusion Prevention Policies with the relevant snort signatures to protect against exploits.



Network inventory is dynamically updated by the Secure Workload scopes, inventory filters, and clusters on which your segmentation policies are based; when workloads are added, changed, or removed from your network, Secure Workload automatically updates the Dynamic Objects in Secure Firewall Management Center on which the corresponding access control rules are based.

Overview of the process:

1. Deploy Secure Workload, Secure Firewall Management Center, and Secure Firewall Threat Defense products.
2. Create the FMC connector Secure Workload and establish communication with your Secure Firewall Management Center.
3. Create scopes, inventory filters, and clusters in Secure Workload that define the consumers and providers that you will use in your segmentation policies.

   ("Consumer "and "provider" in Secure Workload correspond roughly to "source" and "destination" of traffic in Secure Firewall Management Center.)
4. Discover policies automatically using application dependency mapping or manually create segmentation policies in the application workspace in Secure Workload.
5. When you enforce policy in an application workspace, Secure Workload pushes the segmentation policies to the Secure Firewall Management Center as access control rules. The consumers and providers in these rules are converted from scopes, inventory filters, and clusters to dynamic objects in Secure Firewall Management Center.
6. The changes are automatically deployed on Secure Firewall Threat Defense devices managed by Secure Firewall Management Center.

7. Secure Workload continuously checks for changes and automatically pushes updates every five seconds.

   The dynamic objects, like the scopes, inventory filters, and clusters that are their source, automatically update to reflect additions, deletions, and changes to the workload inventory on your network. These changes, and policy changes that you enforce in application workspaces, including policy order, are automatically updated on Secure Firewall Threat Defense managed devices.

Converted Access Control Policy Rules

The following types of access control rules are added:

- Rules with prefix: *Workload_golden_*

  These rules, called golden rules, ensure that Secure Workload can communicate with any Secure Workload agents that are installed on workloads behind the Secure Firewalls.

- Rules with prefix: *Workload_*

  These are the rules converted from segmentation policies in application workspaces for which enforcement is enabled.

- Rules with prefix: *Workload_ca_*

  These are the converted catch-all rules for each enforced application workspace. From Secure Workload version 3.7, you can use the catch-all rules of Secure Workload only if you have selected the **Use Secure Workload Catch All** option while configuring the FMC connector.

- Dynamic objects are created with prefix: *WorkloadObj_*

Rule order matches the standard policy enforcement order for Secure Workload policies and workspaces.

If you delete or modify these rules in FMC, your changes will be overwritten the next time Secure Workload pushes updates to the FMC.

If you create additional access control rules in the FMC that are independent of this integration, and you configure the integration to merge rather than overwrite existing rules, this integration does not change your independent rules, as long as they are not named using one of the prefixes described above.

Important Information for Secure Workload Versions 3.7 and 3.6

With this integration, you create segmentation policies in Secure Workload application workspaces, and Secure Workload converts enforced policies into access control rules in Secure Firewall Management Center.

Network inventory is dynamically managed by the Secure Workload scopes, inventory filters, and clusters on which your segmentation policies are based; when workloads are added, changed, or removed from your network, Secure Workload automatically updates the Dynamic Objects in Secure Firewall Management Center on which the corresponding access control rules are based.

Overview of the process:

1. You deploy your Secure Workload, Secure Firewall Management Center, and Secure Firewall Threat Defense products.
2. You create the FMC external orchestrator in Secure Workload and establish communication with your Secure Firewall Management Center.

3. You create scopes, inventory filters, and clusters in Secure Workload that define the consumers and providers that you will use in your segmentation policies.

   ("Consumer "and "provider" in Secure Workload correspond roughly to "source" and "destination" in Secure Firewall Management Center.)

4. You manually create segmentation policies in application workspaces in Secure Workload.
5. When you enforce policy in an application workspace, Secure Workload pushes the segmentation policies to the Secure Firewall Management Center as access control rules. The consumers and providers in these rules are converted from scopes, inventory filters, and clusters to dynamic objects in Secure Firewall Management Center.
6. The changes are automatically deployed on Secure Firewall Threat Defense devices managed by Secure Firewall Management Center.
7. Secure Workload continuously checks for changes and automatically pushes updates every five seconds.

   The dynamic objects, like the scopes, inventory filters, and clusters that are their source, automatically update to reflect additions, deletions, and changes to the workload inventory on your network. These changes, and policy changes that you enforce in application workspaces, including policy order, are automatically updated on Secure Firewall Threat Defense managed devices.

Converted Access Control Policy Rules: Details

- In Secure Workload version 3.7, converted segmentation policies from Secure Workload are added to the Secure Firewall Management Center as rules in the respective sections of the access control policy. The absolute policies are added in the Mandatory rules section and the default policies in the Default section.
- In Secure Workload version 3.6, converted segmentation policies from Secure Workload are added as rules in the Default section of the access control policy.

The following types of access control rules are added:

- Rules with prefix: *Workload_golden_*

  These rules, called golden rules, ensure that Secure Workload can communicate with any Secure Workload agents that are installed on workloads behind the Secure Firewalls.

- Rules with prefix: *Workload_*

  These are the rules converted from segmentation policies in application workspaces for which enforcement is enabled.

- Rules with prefix: *Workload_ca_*

  These are the converted catch-all rules for each enforced application workspace. From Secure Workload version 3.7, you can use the catch-all rules of Secure Workload only if you have selected the **Use Secure Workload Catch All** option while configuring the FMC external orchestrator.

Rule order matches the standard policy enforcement order for Secure Workload policies and workspaces.

If you delete or modify these rules in FMC, your changes will be overwritten the next time Secure Workload pushes updates to the FMC.

If you create additional access control rules in the FMC that are independent of this integration, and you configure the integration to merge rather than overwrite existing rules, this integration does not change your independent rules, as long as they are not named using one of the prefixes described above.

Converted Dynamic Objects: Details

To view dynamic objects, go to the FMC web interface and select **Objects > Object Management > External Attributes > Dynamic Objects**.

Dynamic objects converted from Secure Workload scopes, inventory filters, and clusters, plus additional dynamic objects required by this integration, are displayed in the FMC list of dynamic objects in the following formats depending on the Secure Workload version:

- In Secure Workload 3.7:
  - In the **Name** column, dynamic objects are listed in the format *WorkloadObj_<Secure Workload inventory filter name>*.
  - In the **Description** column, UUIDs are displayed. If the UUIDs of any object is missing, the Secure Workload inventory filter name is displayed.
- In Secure Workload 3.6: Dynamic objects are listed with the *WorkloadObj_* prefix.

If you need to edit these objects: Edit the scopes, inventory filters, and clusters in Secure Workload. Any changes you make in FMC will be overwritten the next time Secure Workload updates the integration.

Use dynamic objects generated by this integration for other purposes with caution, as their membership is subject to change.

This integration does not affect any dynamic objects created and maintained using other mechanisms.

Deployment Considerations for Secure Workload Versions 3.7 and 3.6

For all 3.7 versions:

Only one FMC orchestrator is supported per Secure Firewall Management Center (formerly known as Firepower Management Center).

Note The Cisco Secure Workload FMC external orchestrator can identify failovers if the FMC stops responding. In case of a failover, the system clears the data in-memory and begins to re-sync with an active FMC instance. A situation may arise where the FMC takes too long to replicate the current configuration into Secure Workload causing the external orchestrator to time out and re-attempt synchronization. The timeout for this configuration sync is 10 minutes.

The FMC also protects itself from too many queries in use by a single endpoint as of FMC 7.2 and earlier. If the FMC detects more than 120 requests in a minute, it responds with an HTTP 429 "Too Many Requests" for a minute after reaching 120 requests. This throttling is avoided in most FMC endpoints by using bulk inserts and reads. However, gathering the content for all Dynamic Objects results in a request for each one.

The limits to a properly behaving integration are based on the time it takes for the Secure Workload orchestrator to fetch all components of the policy (limited by 10 minutes). Each object request is impacted by the network latency, model, and load of the FMC.

For example, the first minute is spent gathering the general FMC information (number of FTDS, ACPs, and Domains) then the remainder is split between 4.5 minutes gathering Dynamic Object / Inventory Filter (540) and the next 4.5 minutes synchronizing the Policy rules (11,250).

Therefore, a reasonable load for the current versions of the product integrations would be 10 minutes = 1 minute (for setup) + (0.024 seconds * number of rules in the SW policy) + (0.5 seconds * number of Inventory filters in use). Exceeding this limit results in a partial load that is noted when the ACP remains in the "out-of-sync" state in the FMC.

For all 3.6 versions:

Only one FMC orchestrator is supported per Firepower Management Center.

If you are using version 3.6.1.36 or later and your deployment uses domains:

All enforced policies in all Secure Workload workspaces are pushed to all access control policies within the domain(s) that you specify in the FMC orchestrator configuration. (Excepting access control policies that are not assigned to at least one FTD device.)

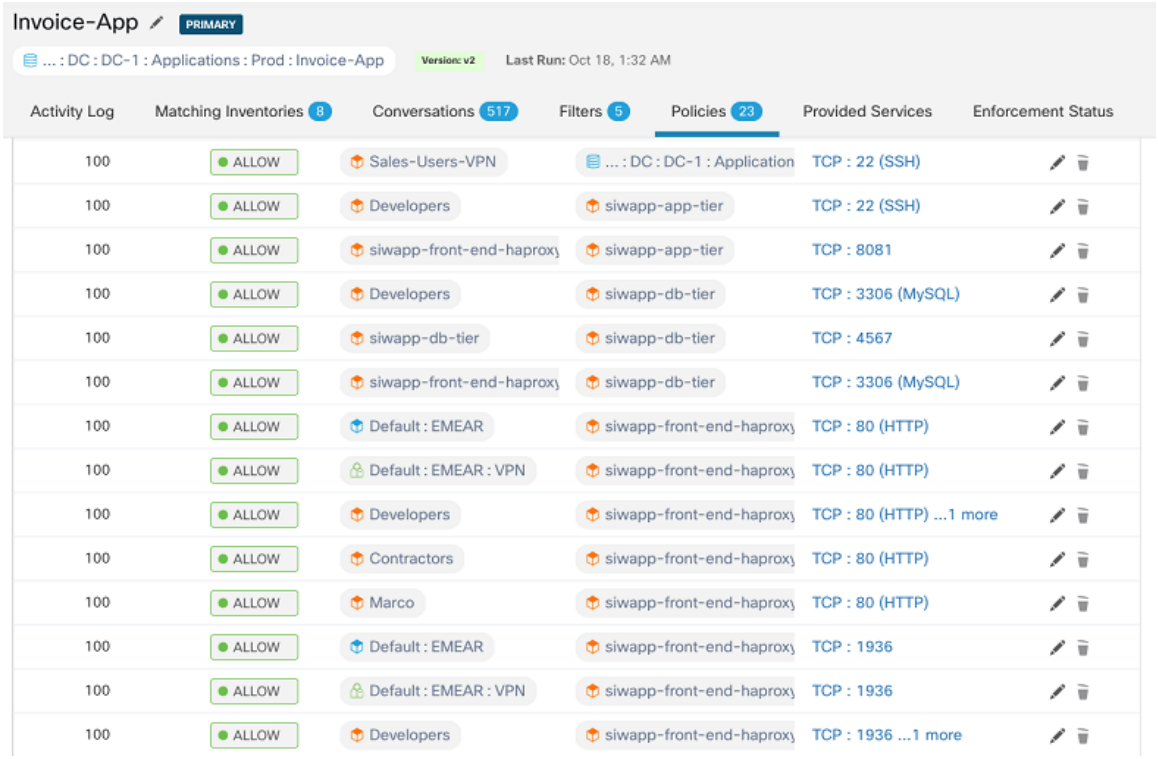
If your deployment does not use domains OR you are using a 3.6 version earlier than 3.6.1.36:

All enforced policies in all Secure Workload workspaces are pushed to all access control policies that are assigned to an FTD device.

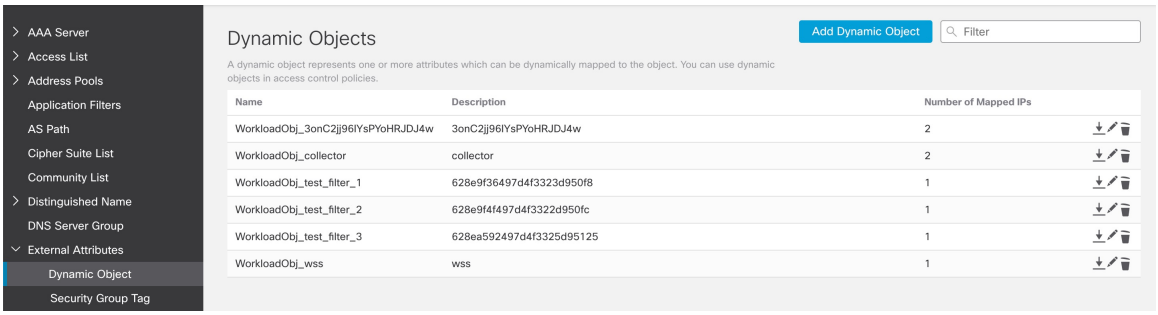
Configuration Example with Dynamic Objects

The following examples are of Secure Workload version 3.7 integration with Secure Firewall Management Center version 7.0.1.

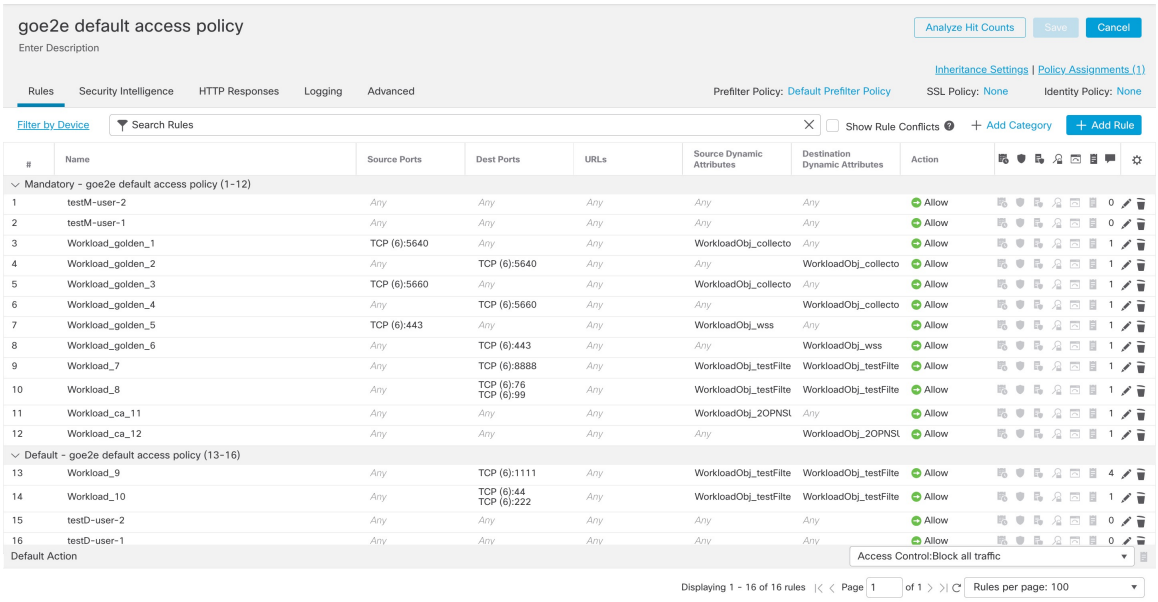
Segmentation Policies in Secure Workload



Dynamic Objects in FMC

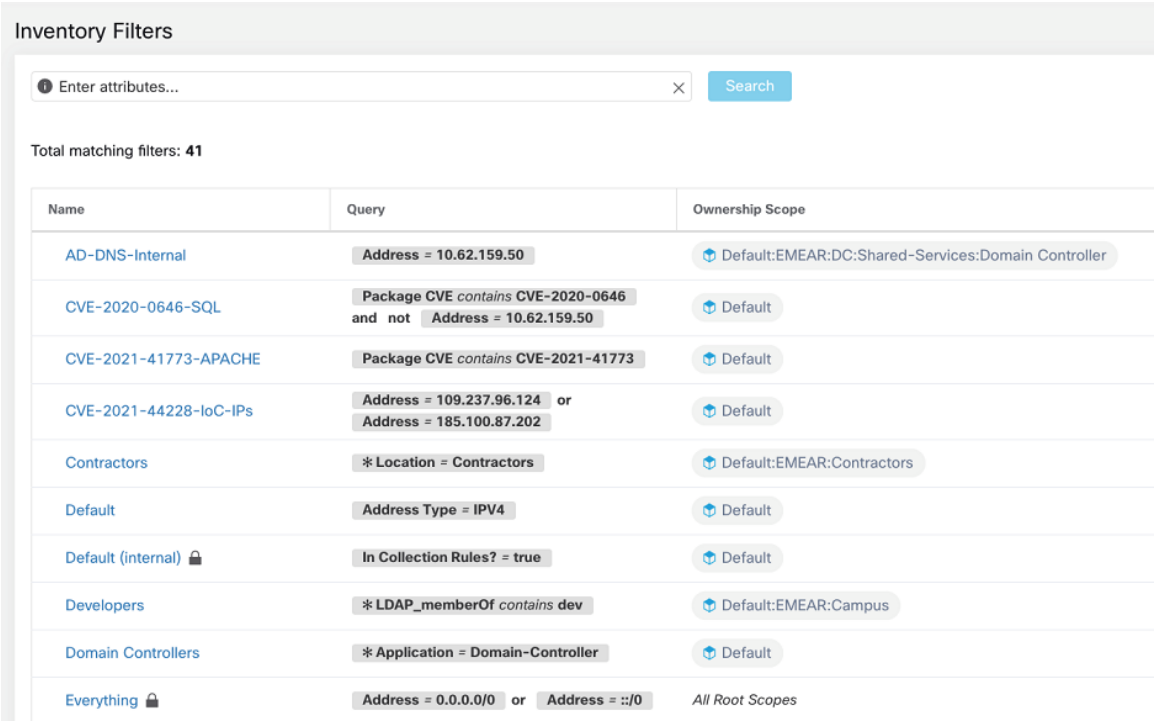


Access Control Policy in FMC



Scopes and Inventory in Secure Workload

Filters in Secure Workload



Supported Deployments

Product Versions

Key Features	Secure Workload Version	Secure Firewall Management Center and Secure Firewall Threat Defense Version
Simplified workflow for the mapping of Scope to Access Control Policies for Secure Firewall Management Center (FMC) and Firepower Threat Defense (FTD) enforcement.	3.9.1.1	7.2 for Segmentation and Virtual Patching 7.1.x for Virtual Patching 7.0.1 for Segmentation
• FMC connector to simplify FMC onboarding. • Ability to perform topology aware enforcement with ACP to Scope Mapping. • Virtual Patching to publish CVEs from workloads.	3.8.1.1 3.8.1.36	7.2 for Segmentation and Virtual Patching 7.1.x for Virtual Patching 7.0.1 for Segmentation

Key Features	Secure Workload Version	Secure Firewall Management Center and Secure Firewall Threat Defense Version
• Ability to change the priority of Secure Workload segmentation policies displayed as rules under the Mandatory and Default sections of Access Control policy in FMC. • Ability to use either the CSW catch-all rules or their FMC equivalent, the default action of the access control policy.	3.7.1.5	7.1 7.0.1
Support for FMC domains when using access control policies with dynamic objects	3.6.1.36	7.1 7.0.1
Access control policies with dynamic objects **Note** Prefilter policies are not supported from Secure Workload version 3.6 and later.	3.6	7.1 7.0.1
Prefilter policies	3.5	7.0 6.7 6.6

Supported Secure Firewall Platforms and Deployments

- Only Secure Firewall Threat Defense devices managed by Secure Firewall Management Center are supported.
- FMC high availability is supported if configured.

  If you include the hostname/IP address of the standby/secondary FMC when configuring the FMC external orchestrator, then when FMC switches to the new active primary appliance, the integration automatically switches to use the new active FMC.
- Secure Firewall Threat Defense (FTD) Routed and Transparent firewall modes are both supported.

  For more information about Secure Firewall Threat Defense modes, see the Transparent or Routed Firewall Mode for Secure Firewall Threat Defense chapter in the *Secure Firewall Management Center Configuration Guide* for your version.

Additional Requirements for Secure Workload Versions 3.7 and 3.6

We recommend using a dedicated FMC for this integration.

Additional Requirements for Cisco Tetration Version 3.5

FTDs must be assigned to a dedicated domain, used solely for the integration with Tetration. This is to ensure that the assigned FTDs are the only devices that the Tetration policies are pushed to.

For more information about creating new domains, managing domains, and moving devices between domains, see the Domain Management section in the Deployment Management chapter of the Firepower Management Center Configuration Guide for your Firepower version. For example: Firepower Management Center Configuration Guide, Version 6.7

.

Implementing This Integration for Secure Workload Version 3.9.1.1

This section applies for all version 3.9 builds.

Settings in 3.9.1.1

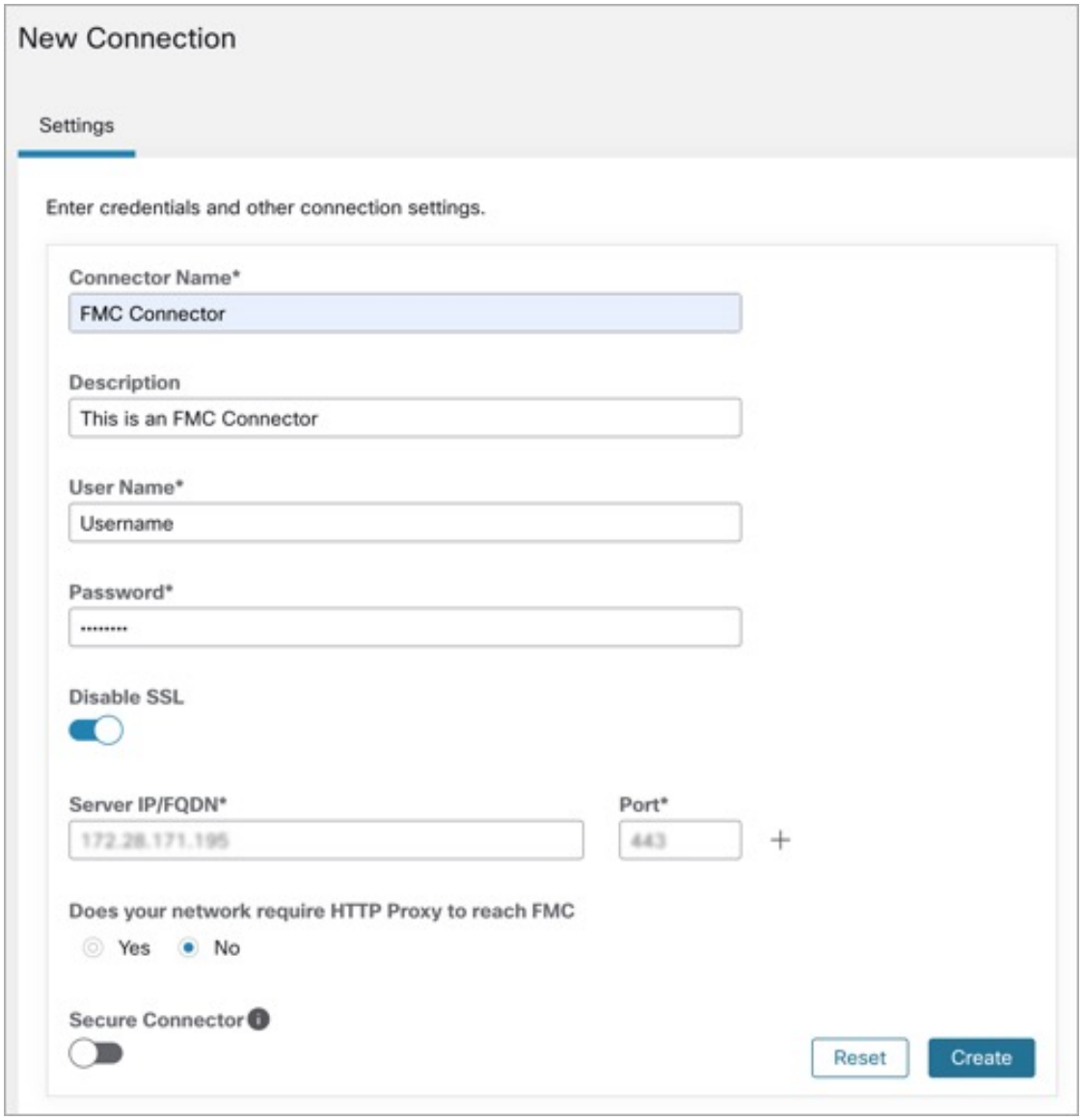
Create the FMC connector in Secure Workload to establish communication with the Secure Firewall Management Center.

1. From the navigation pane, choose **Manage** > **Workloads** > **Connectors**.
2. Under **Firewall**, click **Cisco Secure Firewall**.
3. Click **Configure your new connector here**.
4. In the **New Connection** page, enter the credentials and other connection settings as follows:

Fields	Description
Connector Name	Enter a unique name for the FMC connector.
Description	Enter a description.
Username and Password	Enter the credentials that are used to communicate with the FMC.
CA Certificate	To use secure authentication, enter the CA Certificate that Secure Workload uses to authenticate this FMC, or you can **Disable SSL** where the network is trusted and Secure Workload does not validate the certificate. You can obtain the CA certificate from FMC using the Object Management workflow.
Server IP/FQDN* and Port	Enter the Server IP address and Port Number for the associated FMC. The hostname must be a fully qualified domain name or an IP address of FMC.

Fields	Description
Does your network require HTTP Proxy to reach FMC	If yes, enter the Proxy URL in the format <proxy.host> : <proxy.port>
Secure Connector	Enable if a Secure Connector is used to tunnel connections from Secure Workload to FMC. Note that before you enable this option, you must have a Secure Connector deployed.

5. Click **Create**.



Segmentation in 3.9.1.1

Secure Workload enforced segmentation policies are converted into Access Control Policies, utilizing IP address sets derived from scopes, inventory filters, and clusters. These sets are transformed into dynamic objects within the Secure Firewall Management Center.

Converted segmentation policies from Secure Workload are added to the Secure Firewall Management Center as rules in the respective sections of the access control policy. The Absolute policies are added in the Mandatory rules section and the Default policies are added in the Default rules section.

The following types of access control rules are added:

- Rules with prefix: *Workload_golden_*:

  These rules, called golden rules, ensure that Secure Workload can communicate with any Secure Workload agents that are installed on workloads behind the Secure Firewalls.

- Rules with prefix: *Workload_*:

  These are the rules that are converted from segmentation policies in application workspaces for which enforcement is enabled.

- Rules with prefix: *Workload_ca_*:

  These are the converted catch-all rules for each enforced application workspace. From Secure Workload version, you can use the catch-all rules of Secure Workload only if you have selected the Use Secure Workload Catch-All option while configuring the FMC connector.

- Dynamic objects are created with the prefix: *WorkloadObj_*

Note

- If you delete or modify these rules in FMC, your changes will be overwritten the next time Secure Workload pushes updates to the FMC.
- If you create more access control rules in the FMC that are independent of this integration, and you configure the integration to merge rather than overwrite existing rules, this integration does not change your independent rules, as long as they are not named using one of the prefixes described above.

Add ACP Mapping

1. In the **Segmentation** tab, click **+ Add** to map an Access Policy.
2. In the **Add ACP Mapping** window, choose an **Access Policy** from the drop-down list and map it to a Scope. You can map an Access Policy to only one Scope.
3. Check the **Use Secure Workload Catch All** check-box to enable catch-all rules from Secure Workload. The catch-all Secure Workload rules are listed after all other rules (Secure Workload rules and rules created directly in FMC, if any) in the Default section of Access Control Policies. If you decide to disable catch-all rules from Secure Workload, deselect this option to use the Default Action of the FMC Access Control Policy.
4. Select an option in the **Enforcement Mode**.
   - **Merge**: Secure Workload policy rules are added along with the existing rules created by users. You can configure the priority as explained in the next step.

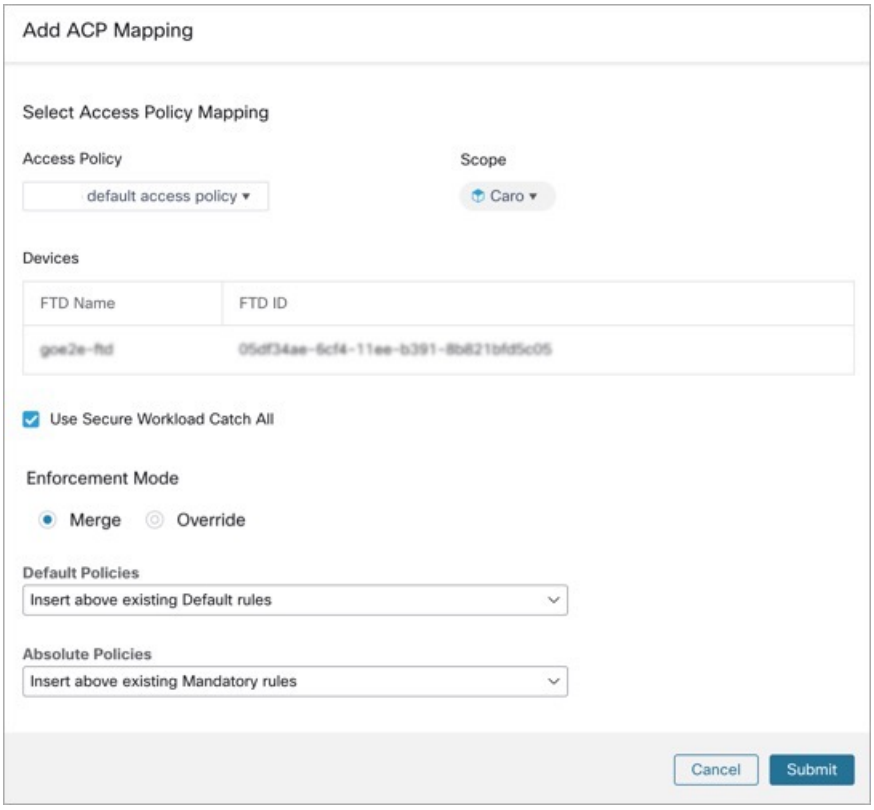
- **Override**: The existing rules created by users are replaced by Secure Workload policy rules.

Note The priority drop-down list is available only when **Merge** is selected as the Enforcement Mode.

5. In the **Absolute** and **Default Policies** drop-down menus, choose the required option to set the priority for Secure Workload policies to be higher or lower to the pre-existing rules in the respective section of the Access Control Policy in FMC.
   - Choosing Insert above existing Mandatory rules makes Secure Workload policies take higher priority over Mandatory rules.
   - Choosing Insert below existing Mandatory rules makes Secure Workload policies take lower priority over Mandatory rules.

   For example, in the **Absolute Policies** drop-down list, if you choose Insert above existing Mandatory rules, the Secure Workload rules are configured at the beginning of the Mandatory section followed by any pre-existing access control rules in the Secure Firewall Management Center. When a new rule is created, the rule order of the Access Control Policy is updated based on the selected priority for policies in Secure Workload.
6. Click **Submit**.

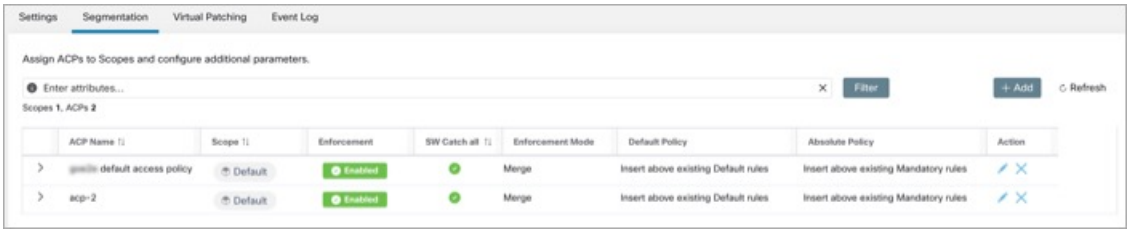
Figure 2: Add ACP Mapping



Edit ACP Mapping

1. Under **Action**, click the pencil icon to edit.
2. Update the details and click **Submit**.
3. Click **Save** to save all edits.

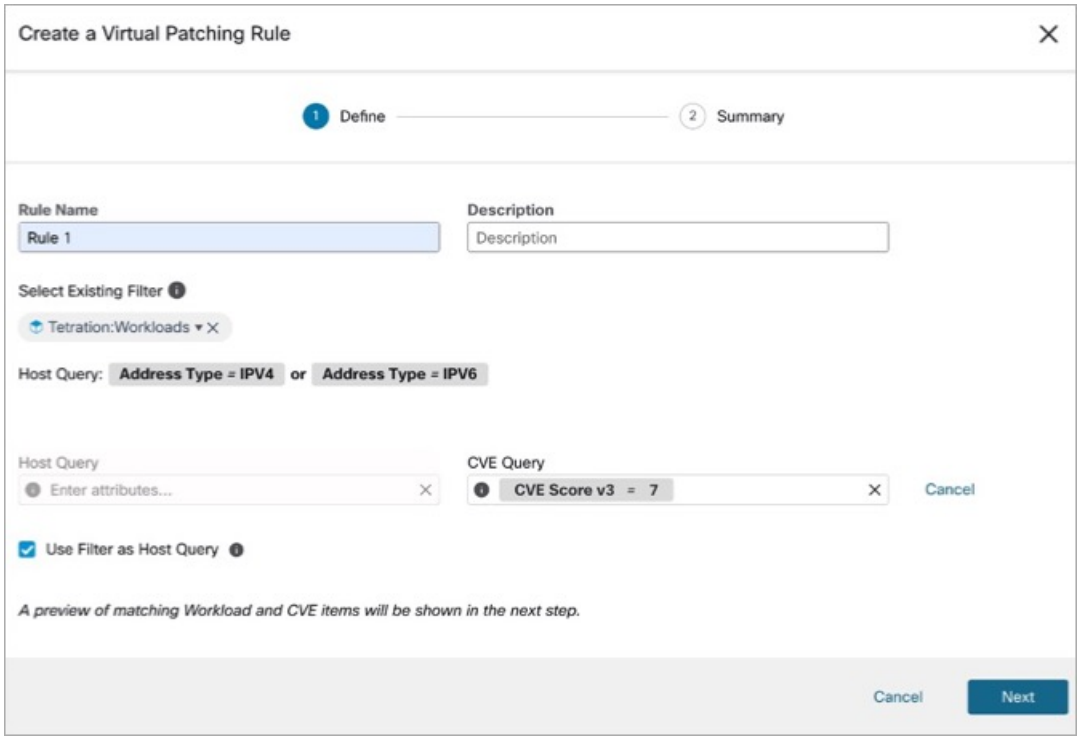
Figure 3: Edit ACP Mapping



Virtual Patching in 3.9.1.1

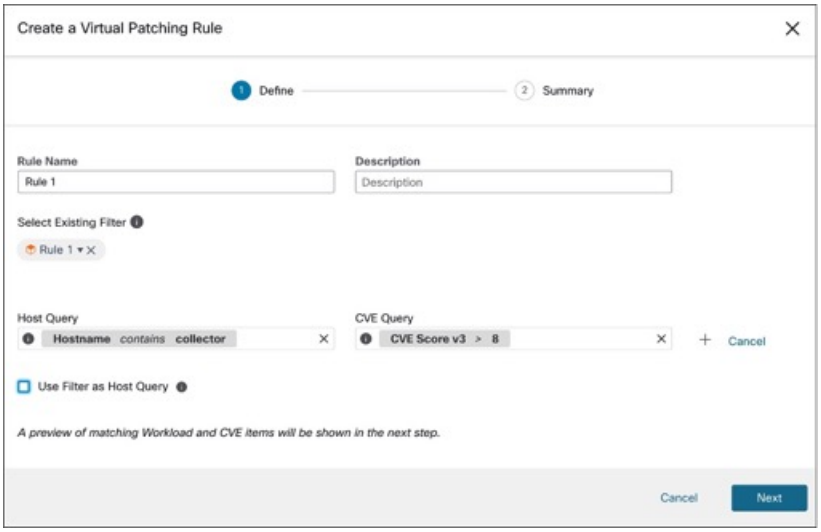
1. In the **Create a Virtual Patching Rule** window, enter a **Rule Name** and **Description**.
2. Select an Existing Filter from the drop-down. You can select an existing scope or subscope to select the hosts to consider for Virtual Patching.
   - By default, the **Use Filter as Host Query** check-box is checked. You can proceed by just entering the CVE query; without creating a new Virtual Patching filter. The Host Query includes the contents of the filter chosen.

Figure 4: Without Creating a New Virtual Patching Filter



- Uncheck the **Use Filter as Host Query** check-box to enter both the Host and CVE query. This creates a new Virtual Patching filter.

Figure 5: Create a New Virtual Patching Filter



3. Enter a Host and CVE query. Click the + icon to add more queries.

Note

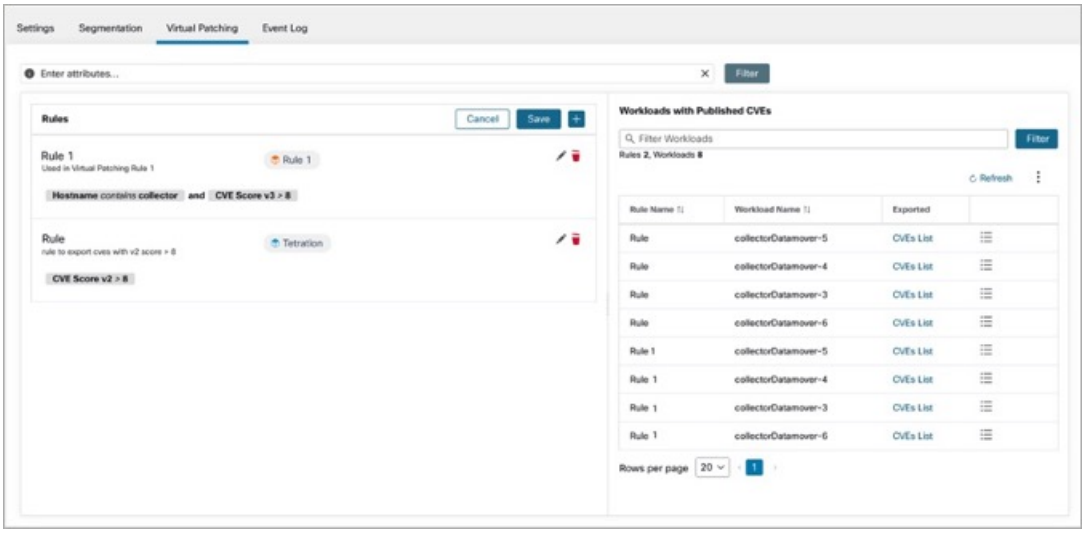
- Hover over the **info** icon to view the supported query formats.
- By default, a Virtual Patching filter is created based on the entered query combination.

4. Click **Next**. In the **Summary** window, lists of matching Workloads and CVEs are displayed. Workloads and CVEs are matched dynamically based on the query.
5. Click **Create**.
6. Added virtual patching rules are displayed under **Rules**. Enter attributes and click **Filter** to narrow down the search results.
7. Workloads with Published CVEs are displayed on the right.
   - Enter attributes and click **Filter** to narrow down the search results.
   - Click the column headers to sort the entries.
   - In the **Exported** column, click **CVEs List** to view a list of all published CVEs of a workload.
   - Click the hamburger menu to view the **Audit Log** of a workload. Logs for the last 48 hours are stored and displayed.

Edit a Virtual Patching Rule

1. Click **Edit** to add more rules, modify the details, and/or delete a rule.

Figure 6: Edit a Virtual Patching Rule



- Click the + icon to add more rules. Click **Save**.
- Click the **bin** icon to delete a rule.

2. Click **the pencil** icon to modify the details of a rule.
3. In the **Edit Virtual Patching Rule** window, modify the Host and CVE Query as required and save the changes.

Event Log in 3.9.1.1

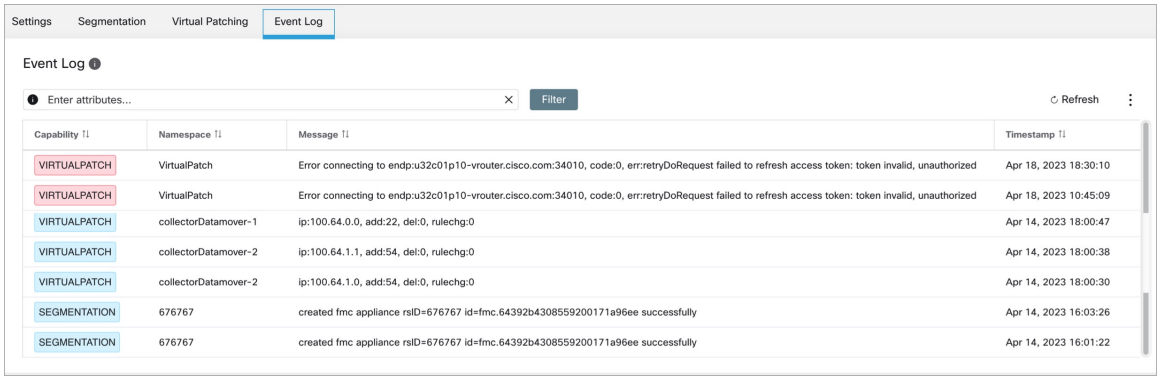
The **Event Log** tab lists the important events or transactions between Secure Workload and Secure Firewall Management Center.

1. Enter attributes to filter the events based on Capability, Event Level, Namespace, and Message.

Note Color codes for the Event level are Information (blue), Warning (orange), and Error (red).

2. Click the column headers to sort the entries.
3. Click the three dot menu icon to download the details in JSON and/or CSV format.
4. Click **Refresh** to reset all filters.

Figure 7: Event Log



Implementing This Integration for Secure Workload Version 3.8.1.1

This section applies for all version 3.8 builds.

About Upgrades

Upgrades to Secure Workload Version 3.8.1.1

- Upgrades from version 3.7.1.5

  FMC External Orchestrator is migrated to Cisco Secure Firewall.

  Your pre-upgrade configurations do not change.

After upgrading to version 3.8.1.1, you can perform the following:

- Publish CVE information from agent-based workloads to Secure Firewall Management Center to fine tune IPS policies by running firewall recommendations.
- Set the priority of segmentation policies to list under Mandatory or Default sections of access control policy.
- To enable or disable the option to use Secure Workload catch-all rules, select or clear the **Use Secure Workload Catch All** option while configuring FMC connector.

Prerequisites for Integration: Secure Workload Version 3.8.1.1

- You have set up a supported Secure Firewall Management Center (FMC) and at least one supported Secure Firewall Threat Defense (FTD) device. You have associated the FTD devices with the FMC, assigned each FTD to an access control policy, and verified that policies can be deployed from the FMC to the FTD(s) and that the system is processing network traffic as expected.

  For complete information, see the Cisco Secure Firewall Management Center documentation for your products, including the Cisco Secure Firewall Management Center documentation roadmaps.

- Your Secure Workload appliance (On-Premises) or account (SaaS) is set up and working as expected.

- If you are using Secure Workload SaaS, or if an on-premises Secure Workload cannot directly reach the FMC appliance, set up a Secure Connector tunnel to provide connectivity between the solution components.

  By default, Secure Workload communicates with the FMC REST API using HTTPS on port 443.

  For instructions on setting up the Secure Connector, see the Secure Workload User Guide, available as online help in your Secure Workload web interface.

How to Implement this Integration for Secure Workload Version 3.8.1.1

The following table provides the end-to-end workflow to set up a Secure Firewall Management Center and configure the integration with Secure Workload version 3.8.1.1 release.

Step	Description	More Information
Before You Begin	Understand how this integration works, the high-level process for implementing it, and any deployment considerations.	See all sections and topics under Important Information for Secure Workload Version 3.8, on page 2.
Before You Begin	Meet requirements and prerequisites	See all sections under Supported Deployments, on page 12 and Prerequisites for Integration: Secure Workload Version 3.8.1.1, on page 21.
1	In Secure Workload: Define scopes, inventory filters, clusters, workspaces, and segmentation policies for your environment.	Discover policies automatically using application dependency mapping or manually create segmentation policies in the application workspace in Secure Workload If you have questions about this, see the Segmentation section of the Secure Workload User Guide, available as online help from your Secure Workload web interface. Alternatively, see Advanced: Use ADM to Generate Segmentation Policies , on page 48.
2	In FMC: At the bottom of each access control policy that is assigned to a Secure Firewall Threat Defense, set the **Default Action** for the policy.	This action will depend on the segmentation policies you create. For example, if you want to block all traffic that is not specifically allowed by segmentation policies, select **Block all traffic**.

Step	Description	More Information
3	In FMC: Create a dedicated user account for this integration.	Requirements for this user account: • The account must have the Administrator role. • (If domains are configured on the FMC) The account must have access to the Global domain. If you have questions about creating user accounts in FMC, see the "Add an Internal User" topic in the online help in Secure Firewall Management Center.
4	In Secure Workload: Create an FMC Connector.	Create only one FMC connector per Secure Firewall Management Center. To create an FMC Connector see Configure the FMC Connector in Version 3.8.1.1, on page 23 section.
5	In Secure Workload: Map Access Control Policy to Scope.	In Manage > Workloads > Connectors > Segmentation, create ACP mapping.
6	In Secure Workload: Create Virtual Patching rule.	In Manage > Workloads > Connectors > Virtual Patching, create a Virtual Patching rule. Workloads with Published CVEs are displayed.
7	In Secure Workload: Enforce policies on desired workspaces.	In the workspace(s), click the **Enforcement** tab, then click the **Enforce Policies** button and complete the wizard.
8	Wait for the new rules to appear in the access control policy or policies.	This takes a variable amount of time, depending on the amount of data to be transferred, the speed of the machines, network bandwidth, etc. To view the rules: In your FMC, choose **Policies** > **Access Control** and click the policy to view.
9	The new access control policies are automatically deployed to the associated managed Secure Firewall Threat Defense devices.	Future changes are also automatically deployed to Secure Firewall Threat Defense devices. If you associate new FTDs later to an existing access control policy, the new FTDs will automatically receive the current rules.

Configure the FMC Connector in Version 3.8.1.1

Before you begin

Complete the steps up to this point in Implementing This Integration for Secure Workload Version 3.8.1.1.

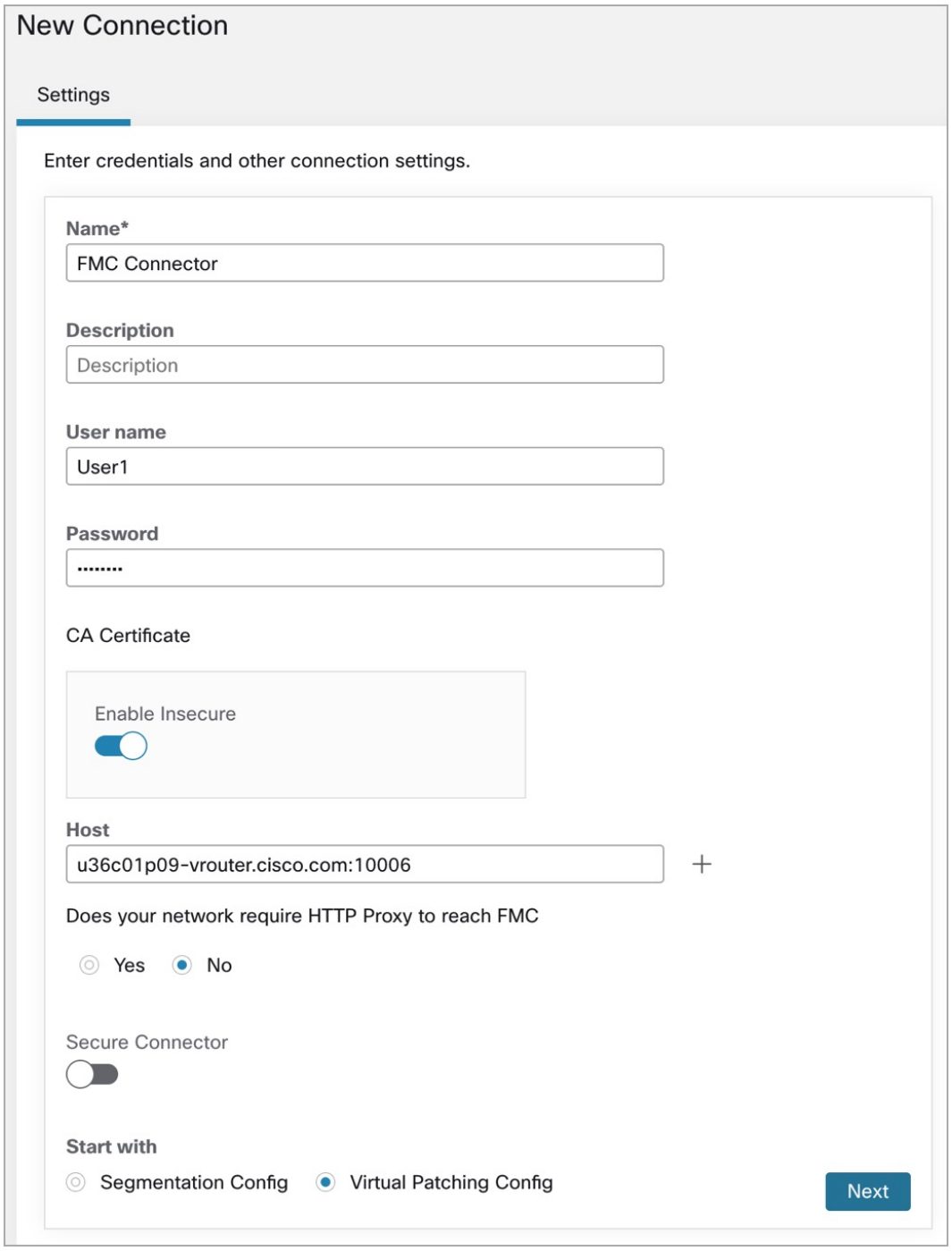
Settings

Create the FMC connector in Secure Workload to establish communication with the Secure Firewall Management Center.

1. Navigate to **Manage** > **Workloads** > **Connectors**.
2. Under **Firewall**, click **Cisco Secure Firewall**.
3. Click **Configure your new connector here**.
4. On the **New Connection** page, enter the credentials and other connection settings as follows:

Fields	Description
Name	Enter a unique name for the FMC connector.
Description	Enter a description.
Username and Password	Enter the credentials that are used to communicate with the FMC.
CA Certificate	Enter the CA Certificate that Secure Workload uses to authenticate this FMC, or you can **Enable Insecure** where the network is trusted and Secure Workload does not validate the certificate. You can obtain the CA certificate from FMC using the Object Management workflow.
Host	Enter the hostname and port number for the associated FMC. The format is <FQDN> : <Port> or <IP> : <Port> The hostname should be a fully qualified domain name or an IP of FMC.
Does your network require HTTP Proxy to reach FMC	Enter the Proxy URL in the format <proxy.host> : <proxy.port>
Secure Connector	Enable if a Secure Connector is used to tunnel connections from Secure Workload to FMC. Before you can enable this option, you must have deployed a Secure Connector.
Start with	Choose **Segmentation Config** or **Virtual Patching Config**. a) **Segmentation Config**: Assign Access Control Policies to Scopes and configure additional parameters. b) **Virtual Patching Config**: Configure rules on CVEs to publish to FMC.

5. Click **Next**.



Segmentation

Secure Workload enforced segmentation policies are converted to Access Control Policies based on IP address sets from scopes, inventory filters, and clusters converted to dynamic objects in the Secure Firewall Management Center.

Converted segmentation policies from Secure Workload are added to the Secure Firewall Management Center as rules in the respective sections of the access control policy. The Absolute policies are added in the Mandatory rules section and the Default policies are added in the Default rule section.

The following types of access control rules are added:

- Rules with prefix: *Workload_golden_*:

  These rules, called golden rules, ensure that Secure Workload can communicate with any Secure Workload agents that are installed on workloads behind the Secure Firewalls.

- Rules with prefix: *Workload_*:

  These are the rules that are converted from segmentation policies in application workspaces for which enforcement is enabled.

- Rules with prefix: *Workload_ca_*:

  These are the converted catch-all rules for each enforced application workspace. From Secure Workload version, you can use the catch-all rules of Secure Workload only if you have selected the Use Secure Workload Catch-All option while configuring the FMC connector.

- Dynamic objects are created with prefix: *WorkloadObj_*

Note

- If you delete or modify these rules in FMC, your changes will be overwritten the next time Secure Workload pushes updates to the FMC.
- If you create additional access control rules in the FMC that are independent of this integration, and you configure the integration to merge rather than overwrite existing rules, this integration does not change your independent rules, as long as they are not named using one of the prefixes described above.

Create ACP Mapping

1. If **Segmentation Config** is selected in Settings, you are navigated to the **Create ACP Mapping** window.
2. Choose an **Access Policy** from the drop-down and map it to a **Scope.** An Access Policy can be mapped to only one Scope.
3. Check the **Use Secure Workload Catch All** check-box to enable catch-all rules from Secure Workload. The catch-all Secure Workload rules are listed after all other rules (Secure Workload rules and rules created directly in FMC, if any) in the Default section of Access Control Policies. If you decide to disable catch-all rules from Secure Workload, deselect this option to use the Default Action of the FMC Access Control Policy.
4. Select an option in the **Enforcement Mode**.
   - **Merge**: Secure Workload policy rules are added along with the existing rules created by users. You can configure the priority as explained in the next step.
   - **Override**: The existing rules created by users are replaced by Secure Workload policy rules.

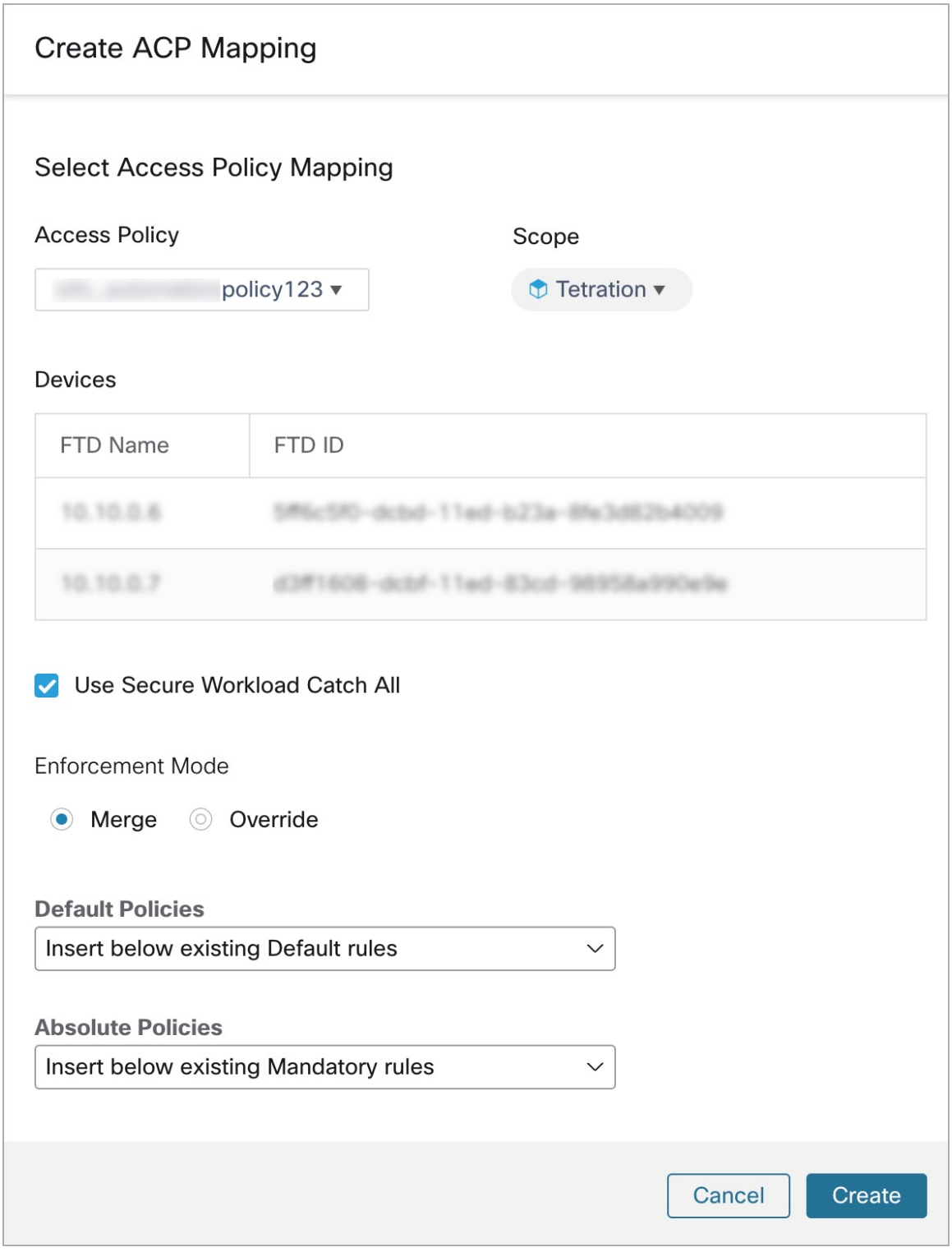
Note The priority drop-down menu options are available only when **Merge** is selected as the Enforcement Mode.

5. In the **Absolute** and **Default Policies** drop-down menus, choose the required option to set the priority for Secure Workload policies to be higher or lower to the pre-existing rules in the respective section of the Access Control Policy in FMC.

   - Choosing Insert above existing Mandatory rules makes Secure Workload policies take higher priority over Mandatory rules.
   - Choosing Insert below existing Mandatory rules makes Secure Workload policies take lower priority over Mandatory rules.

   For example, in the **Absolute Policies** drop-down menu, if you choose Insert above existing Mandatory rules, the Secure Workload rules are configured at the beginning of the Mandatory section followed by any pre-existing access control rules in the Secure Firewall Management Center. When a new rule is created, the rule order of the Access Control Policy is updated based on the selected priority for policies in Secure Workload.

Figure 8: Create ACP Mapping



6. Click **Create**.

Edit ACP Mapping

1. On the Segmentation tab, click **Edit**.
2. Under **Action**, click the edit icon.
3. Make the required changes and click **Save**.
4. Click the + icon to map another ACP to a Scope.
5. Click **Save** to save all edits.

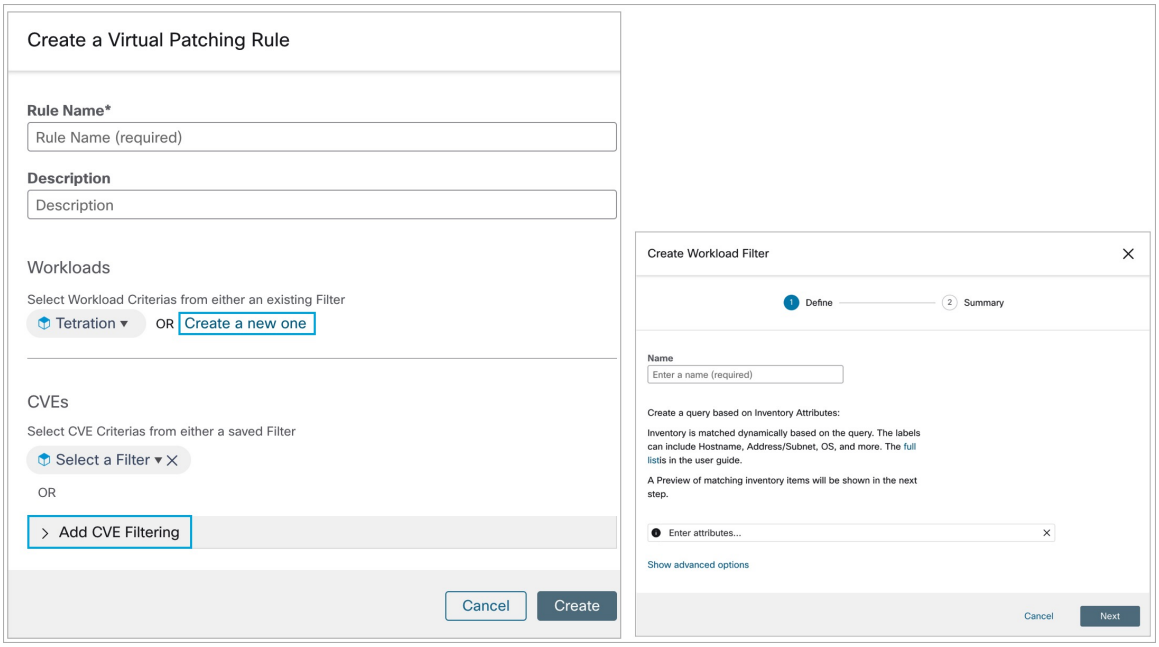
Virtual Patching

Virtual Patching, also known as External Patching and Just-in-time Patching, is a security technique that is used to protect applications and computer systems from known vulnerabilities. Virtual Patching, originally used by the Intrusion Prevention System (IPS), implements temporary fixes or workarounds to address vulnerabilities until a permanent patch can be developed and applied.

For example, organisations following the Software Development Life Cycle, take time to detect, fix, and develop a new version of the application. The system can be protected by introducing a firewall and adding the IPS rules, until the newer version of the application is rolled out. Secure Workload publishes the CVEs to the firewall to consider while creating the IPS policies.

1. If **Virtual Patching Config** is selected in Settings, you are navigated to the **Create a Virtual Patching Rule** window.
2. Enter a **Rule Name** and **Description**.
3. You can either choose an existing workload filter or create a new one.
4. You can either choose an existing CVE filter or add a CVE filter by entering a CVE query.
5. Click **Create**.
6. On the **Virtual Patching** tab, under **Rules**, click **Add Rule** to add one or more rules.

Figure 9: Create a Virtual Patching Rule



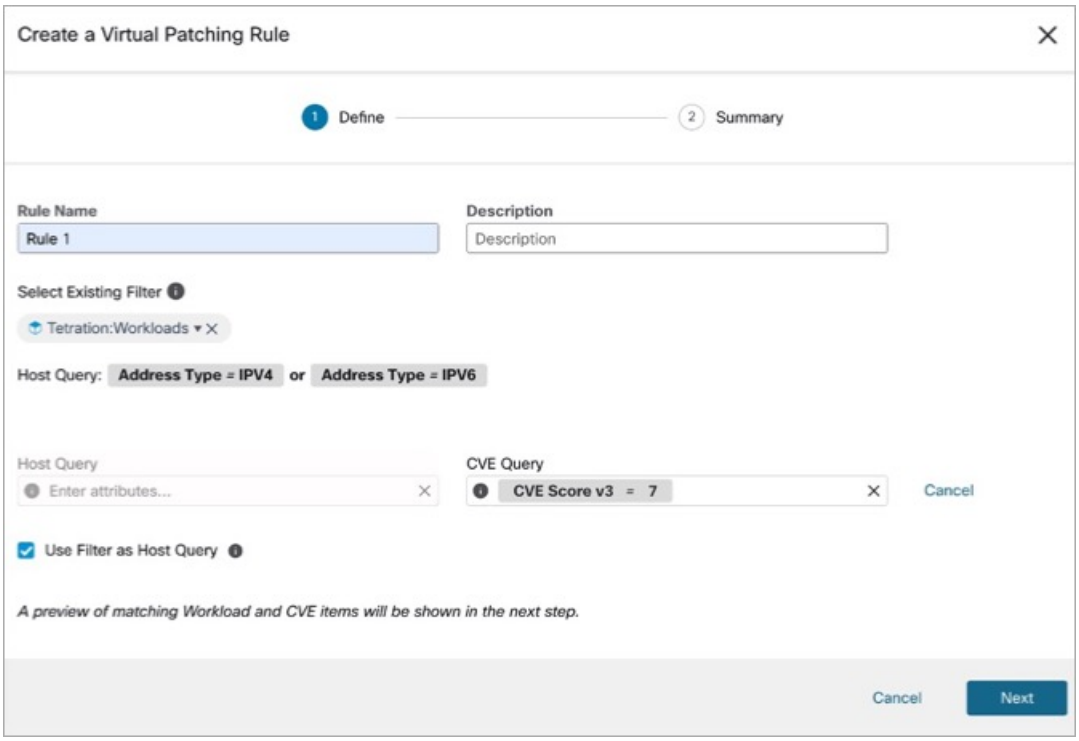
7. Added virtual patching rules are displayed under Rules.
   - You can search by **Rule name** and **Description**.
   - Click the **filter** icon to choose the columns to be displayed.
   - Under **Actions**, click the **edit** icon to modify the details of a Virtual Patching Rule.
   - Under **Actions**, click the **bin** icon to delete a Virtual Patching rule.
8. Workloads with Published CVEs are displayed on the right.
   - You can filter by entering attributes such as Rule Name, Inventory Filter, Workload, and Worst Score.
   - Click the menu icon to download the details in JSON and/or CSV format.
   - Click the column headers to sort the entries.
   - In the **Exported** column, click **CVEs List** to view a list of all published CVEs of a workload.
   - Click the hamburger menu to view the **Audit Log**. Logs for the last 48 hours are stored and displayed.

Virtual Patching in 3.8.1.36

1. In the **Create a Virtual Patching Rule** window, enter a **Rule Name** and **Description**.
2. Select an Existing Filter from the drop-down. You can select an existing scope or subscope to select the hosts to consider for Virtual Patching.

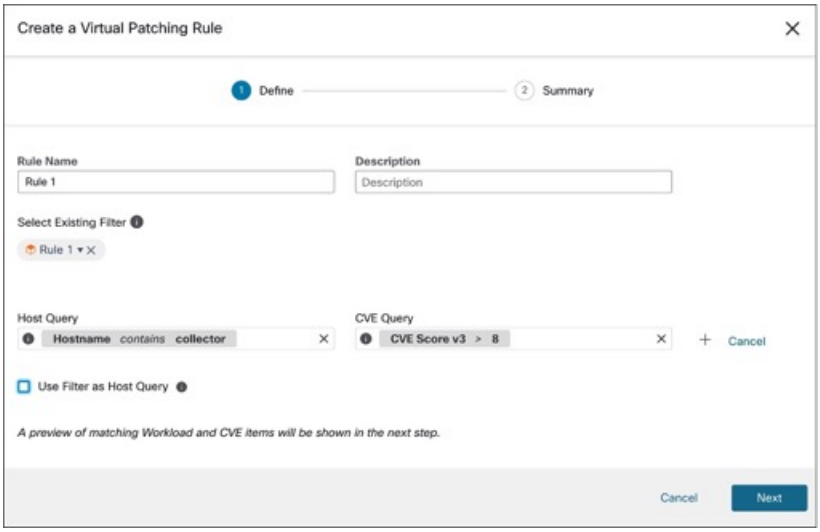
- By default, the **Use Filter as Host Query** check-box is checked. You can proceed by just entering the CVE query; without creating a new Virtual Patching filter. The Host Query includes the contents of the filter chosen.

Figure 10: Without Creating a New Virtual Patching Filter



- Uncheck the **Use Filter as Host Query** check-box to enter both the Host and CVE query. This creates a new Virtual Patching filter.

Figure 11: Create a New Virtual Patching Filter



3. Enter a Host and CVE query. Click the + icon to add more queries.

Note

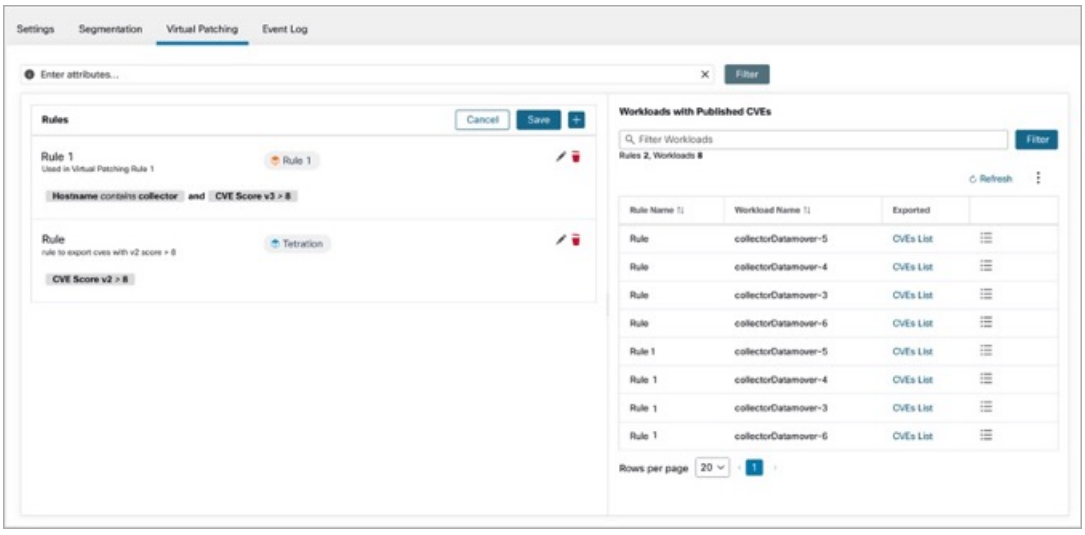
- Hover over the **info** icon to view the supported query formats.
- By default, a Virtual Patching filter is created based on the entered query combination.

4. Click **Next**. In the **Summary** window, lists of matching Workloads and CVEs are displayed. Workloads and CVEs are matched dynamically based on the query.
5. Click **Create**.
6. Added virtual patching rules are displayed under **Rules**. Enter attributes and click **Filter** to narrow down the search results.
7. Workloads with Published CVEs are displayed on the right.
   - Enter attributes and click **Filter** to narrow down the search results.
   - Click the column headers to sort the entries.
   - In the **Exported** column, click **CVEs List** to view a list of all published CVEs of a workload.
   - Click the hamburger menu to view the **Audit Log** of a workload. Logs for the last 48 hours are stored and displayed.

Edit a Virtual Patching Rule

1. Click **Edit** to add more rules, modify the details, and/or delete a rule.

Figure 12: Edit a Virtual Patching Rule



- Click the + icon to add more rules. Click **Save**.
- Click the **bin** icon to delete a rule.

2. Click **the pencil** icon to modify the details of a rule.
3. In the **Edit Virtual Patching Rule** window, modify the Host and CVE Query as required and save the changes.

Event Log

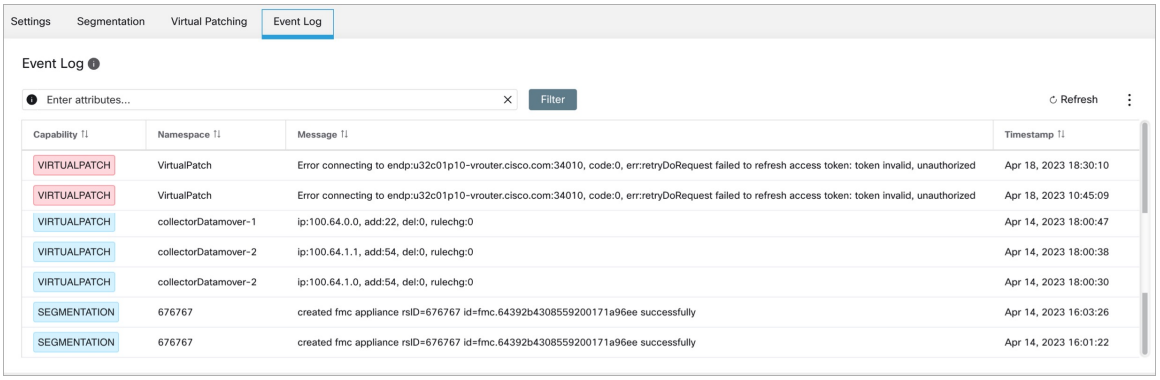
The **Event Log** tab lists the important events or transactions between Secure Workload and Secure Firewall Management Center.

1. Enter attributes to filter the events based on Capability, Event Level, Namespace, and Message.

Note Color codes for the Event level are Information (blue), Warning (orange), and Error (red).

2. Click the column headers to sort the entries.
3. Click the three dot menu icon to download the details in JSON and/or CSV format.
4. Click **Refresh** to reset all filters.

Figure 13: Event Log



Implementing This Integration for Secure Workload Version 3.7.1.5

This section applies for all version 3.7 builds.

About Upgrades

Upgrades to Secure Workload Version 3.7.1.5

- Upgrades from version 3.6.1.36:

  Your pre-upgrade configurations do not change.

- Upgrades from 3.6.x versions prior to 3.6.1.36:

  If domains are configured on your Firepower Management Center and enforcement was enabled in the orchestrator:

By default, all domains are selected for enforcement.

After upgrading to version 3.7.1.5, you can perform the following:

- Set the priority of segmentation policies to list under Mandatory or Default sections of access control policy.
- To enable or disable the option to use Secure Workload catch-all rules, select or clear the **Use Secure Workload Catch All** option while configuring FMC external orchestrator.

Prerequisites for Integration: Secure Workload Version 3.7.1.5

- You have set up a supported Secure Firewall Management Center (FMC) and at least one supported Secure Firewall Threat Defense (FTD) device. You have associated the FTD devices with the FMC, assigned each FTD to an access control policy, and verified that policies can be deployed from the FMC to the FTD(s) and that the system is processing network traffic as expected.

  For complete information, see the Cisco Secure Firewall Management Center documentation for your products, including the Cisco Secure Firewall Management Center documentation roadmaps.
- Your Secure Workload appliance (On-Premises) or account (SaaS) is set up and working as expected.
- If you are using Secure Workload SaaS, or if an on-premises Secure Workload cannot directly reach the FMC appliance, set up a Secure Connector tunnel to provide connectivity between the solution components.

  By default, Secure Workload communicates with the FMC REST API using HTTPS on port 443.

  For instructions on setting up the Secure Connector, see the Secure Workload User Guide, available as online help in your Secure Workload web interface.

How to Implement this Integration for Secure Workload Version 3.7.1.5

The following table provides the end-to-end workflow to set up a Secure Firewall Management Center and configure the integration with Secure Workload version 3.7.1.5 release.

Step	Description	More Information
Before You Begin	Understand how this integration works, the high-level process for implementing it, and any deployment considerations.	See all sections and topics under Important Information for Secure Workload Versions 3.7 and 3.6, on page 5.
Before You Begin	Meet requirements and prerequisites	See all sections under Supported Deployments, on page 12 and Prerequisites for Integration: Secure Workload Version 3.7.1.5, on page 34.

Step	Description	More Information
1	In Secure Workload: Define scopes, inventory filters, clusters, workspaces, and segmentation policies for your environment.	Manually create segmentation policies that you want to apply to the set of workloads that will be defined by dynamic objects in Secure Firewall. If you have questions about this, see the Segmentation section of the Secure Workload User Guide, available as online help from your Secure Workload web interface. Alternatively, see Advanced: Use ADM to Generate Segmentation Policies , on page 48.
2	In FMC: At the bottom of each access control policy that is assigned to a Secure Firewall Threat Defense, set the **Default Action** for the policy.	This action will depend on the segmentation policies you create. For example, if you want to block all traffic that is not specifically allowed by segmentation policies, select **Block all traffic**.
3	In FMC: Create a dedicated user account for this integration.	Requirements for this user account: • The account must have the Administrator role. • (If domains are configured on the FMC) The account must have access to the Global domain. If you have questions about creating user accounts in FMC, see the "Add an Internal User" topic in the online help in Secure Firewall Management Center.
4	In Secure Workload: Create an FMC orchestrator.	Create only one FMC orchestrator per Secure Firewall Management Center. To create an FMC orchestrator using OpenAPI, see Configure the FMC Orchestrator in Version 3.7.1.5, on page 36 section in the user guide in your Secure Workload web portal.
5	In Secure Workload: Enforce policies on desired workspaces. (This is separate from enabling enforcement in the FMC orchestrator.)	In the workspace(s), click the **Enforcement** tab, then click the **Enforce Policies** button and complete the wizard.

Step	Description	More Information
6	Enable enforcement of the orchestrator: If you have not yet selected domains in the FMC orchestrator, do so now.	Edit the FMC orchestrator to select domains. (If your FMC does not have domains configured, you'll need to select the **Global** domain.) When you click **Update** after selecting domains, this enables enforcement of the orchestrator and deploys your Secure Workload policies to your managed FTD devices. For details, see Editing an FMC Orchestrator in Version 3.7.1.5, on page 39.
7	Wait for the new rules to appear in the access control policy or policies.	This takes a variable amount of time, depending on the amount of data to be transferred, the speed of the machines, network bandwidth, etc. To view the rules: In your FMC, choose **Policies** > **Access Control** and click the policy to view.
8	The new access control policies are automatically deployed to the associated managed Secure Firewall Threat Defense devices.	Future changes are also automatically deployed to Secure Firewall Threat Defense devices. If you associate new FTDs later to an existing access control policy, the new FTDs will automatically receive the current rules.

Configure the FMC Orchestrator in Version 3.7.1.5

Before you begin

Complete the steps up to this point in the table in Implementing This Integration for Secure Workload Version 3.7.1.5, on page 33.

Procedure

Step 1 In the Secure Workload web interface, select **Manage > External Orchestrators**.

Step 2 Click **Create New Configuration**

Step 3 Under the **Basic Config** tab, configure the following fields:

Option	Description
Type	Select **FMC**.
Name	Enter a unique name for the FMC orchestrator.
Description	Enter a description for the orchestrator.

Option	Description
Full Snapshot Interval(s)	Enter the full snapshot interval, in seconds. The **Full Snapshot Interval(s)** field specifies how often the FMC external orchestrator tests the FMC connectivity to Secure Workload. If an error occurs (for example, if the FMC is not reachable due to network issues, or if invalid endpoint/user credentials were used) the FMC orchestrator reports the error in the **Status** field. Default value: `3600 seconds`
Username **Password**	Enter the username and password of the dedicated user that you created in FMC, as instructed previously in this document. These credentials are used to communicate with the FMC.
CA Certificate	Enter the CA Certificate that Secure Workload will use to authenticate this FMC. You can obtain this certificate from the FMC using the Object Management workflow. For more information, see the Internal Certificate Authority Objects topics in the Reusable Objects chapter of the *Firepower Management Center Configuration Guide* for your Firepower version.
Accept Self-signed Cert	Select this checkbox to configure the FMC orchestrator to trust a self-signed certificate.
Secure Connector Tunnel	If you are using Secure Workload SaaS, you must enable this option. If you are using an on-premises Secure Workload appliance, you may need to enable this option. Before you can enable this option, you must have deployed a Secure Connector, as described in Prerequisites for Integration: Secure Workload Version 3.7.1.5, on page 34.
Use Secure Workload Catch All	Select this checkbox to enable catch-all rules from Secure Workload. The catch-all Secure Workload rules are listed after all other rules (Secure Workload rules and rules created directly in FMC, if any) in the Default section of access control policies. If you decide to disable catch-all rules from Secure Workload, deselect this option to use the Default Action of the FMC access control policy.

Option		Description
Enforcement Mode	**Merge/ Override**	Select **Merge** or **Override** from the drop-down list. • If you select **Override**, the enforced Secure Workload policies replace any existing FMC access control rules. **Important** If you select this option, all existing rules in all access control policies associated with an FTD (in the domains you select, if applicable) will be deleted and unrecoverable. • If you have rules that you want to retain, we recommend that you either export the rules before continuing with this integration, or use the **Merge** option (described in the next row). **Note** If the **Enforcement Mode** is set to **Merge**: • We recommend that you do not use the prefix `Workload_` for any rules that you enter manually into FMC, as they will be automatically removed. • Avoid performing FTD deployment using the FMC UI and policy enforcement using Secure Workload at the same time. These asynchronous and long running (~2 minutes) operations compete against each other and may cause FTD deployment to fail. If the FTD deployment fails due to competing policy enforcements, you must repeat the deployment.
	Absolute or Default Policy Priority	The priority drop-down menu options are available only when **Merge** is selected as the enforcement mode. In the Absolute or Default Policies drop-down menus, select the required option to display the Secure Workload policies above or below the pre-existing rules in the respective section of access control policy in FMC. For example, in the **Absolute Policies** drop-down menu, if you select **Insert above existing Mandatory rules**, the Secure Workload rules are displayed at the beginning of the **Mandatory** section followed by any pre-existing access control rules in Secure Firewall Management Center. When a new rule is created, the rule order of the access control policy is updated based on the selected priority for policies in Secure Workload.

Step 4 Click on the **Host Lists** link at the left.

Step 5 Enter the host name and port number for the associated FMC.

The `host name` should be a fully qualified domain name for FMC or an IP address.

The `port number` is 443 by default.

If your FMC is deployed in a supported high-availability configuration, also enter the hostname and port for the standby/secondary FMC.

Step 6 Click **Create**.

You may briefly see a green banner that indicates that Secure Workload has successfully connected to your Secure Firewall Management Center.

After the connection is established, Secure Workload fetches any domains configured on your Secure Firewall Management Center. This may take a few minutes.

(If you do not have domains configured, Secure Workload fetches the **Global** domain.)

After domains have successfully been fetched, you will see the option to select domains.

Step 7 If you do not want to deploy policies to your managed Secure Firewall Threat Defense devices now:

When you see the option to select domains, click **Cancel**.

When you are ready to deploy policies, return to the **External Orchestrators** page, edit this orchestrator, click **Domains**, and select domains as described in the next step.

Step 8 Select the domain(s) to which you want to push segmentation policies.

If your Secure Firewall deployment does not have domains configured, select the **Global** domain.

Step 9 Click **Update**.

Segmentation policies are pushed to the access control policies in the domains you selected, and the changes are deployed to the associated Secure Firewall Threat Defense devices.

The amount of time required to push the rules is typically a few minutes, but depends on the number of policy rules and the resource configuration of Secure Firewall Management Center and Secure Firewall Threat Defense devices.

What to do next

Return to the procedure overview table in Implementing This Integration for Secure Workload Version 3.7.1.5, on page 33 and continue with the remaining steps.

Editing an FMC Orchestrator in Version 3.7.1.5

- You can create the FMC orchestrator without specifying domains on which to enforce policy, then edit the orchestrator configuration later to specify domains for enforcement.

  Enforcement occurs when you click **Update** after selecting domains.

- If you edit an FMC external orchestrator, you must enter the FMC account password again.
- If you modify an FMC orchestrator that has domains selected, Secure Workload fetches the domains again.

  Domains that you have already selected remain selected.

- If you modify an orchestrator, the Exernal Orchestrators page may initially show Connection Status as **Failure** while connection and synchronization occur, but this changes to **Success** after a few moments. You can then edit the domains.

Implementing This Integration for Secure Workload Version 3.6

This section applies for all version 3.6.x builds. Build-specific information is labeled as such.

About Upgrades

Upgrades to 3.6.1.36

If domains are configured on your Firepower Management Center and enforcement was enabled in the FMC orchestrator before upgrade to version 3.6.1.36:

By default, all domains are selected for enforcement.

Upgrades from 3.5 to 3.6.1.5

If you configured the FMC integration in version 3.5 and will upgrade to version 3.6.1.5, see important information in the *Cisco Secure Workload Upgrade Guide*. You do not need to use the procedure described below.

Prerequisites for Integration: Secure Workload 3.6

- You have set up a supported Firepower Management Center (FMC) and at least one supported Firepower Threat Defense (FTD) device. You have associated the FTD(s) with the FMC, assigned each FTD to an access control policy, and verified that policies can be deployed from the FMC to the FTD(s) and that the system is processing network traffic as expected.

  For complete information, see the Cisco Secure Firewall Management Center documentation for your products, including the Cisco Secure Firewall documentation roadmap.

- Your Secure Workload appliance (On-Premises) or account (SaaS) is set up and working as expected.

- If you are using Secure Workload SaaS, or if an on-premises Secure Workload cannot directly reach the FMC appliance, set up a Secure Connector tunnel to provide connectivity between the solution components.

  By default, Secure Workload communicates with the FMC REST API using HTTPS on port 443.

  For instructions on setting up the Secure Connector, see the Secure Workload User Guide, available as online help in your Secure Workload web interface.

How to Implement This Integration for Secure Workload Version 3.6

The following table provides the end-to-end workflow to set up a Firepower Management Center (FMC) and configure the integration with any Secure Workload version 3.6 release.

Step	Description	More Information
Before You Begin	Understand how this integration works, the high-level process for implementing it, and any deployment considerations.	See all sections and topics under Important Information for Secure Workload Versions 3.7 and 3.6, on page 5.
Before You Begin	Meet requirements and prerequisites	See all sections under Supported Deployments, on page 12 and Prerequisites for Integration: Secure Workload 3.6, on page 40.
1	In Secure Workload: Define scopes, inventory filters, clusters, workspaces, and segmentation policies for your environment.	Manually create segmentation policies that you want to apply to the set of workloads that will be defined by dynamic objects in Firepower. If you have questions about this, see the Segmentation section of the Secure Workload User Guide, available as online help from your Secure Workload web interface. Alternatively, see Advanced: Use ADM to Generate Segmentation Policies , on page 48.
2	In FMC: At the bottom of each access control policy that is assigned to an FTD, set the **Default Action** for the policy.	This action will depend on the segmentation policies you create. For example, if you want to block all traffic that is not specifically allowed by segmentation policies, select **Block all traffic**.
3	In FMC: Create a dedicated user account for this integration.	Requirements for this user account: • The account must have the Administrator role. • (If domains are configured on the FMC) The account must have access to the Global domain. If you have questions about creating user accounts in FMC, see the "Add an Internal User" topic in the online help in Firepower Management Center.

Step	Description	More Information
4	In Secure Workload: Create an FMC orchestrator.	Create only one FMC orchestrator per Firepower Management Center. • For Secure Workload version 3.6.1.36: See Configure the FMC Orchestrator in Version 3.6.1.36, on page 43 • For Secure Workload versions 3.6.1.5 through 3.6.1.20: See Configure the FMC Orchestrator in Secure Workload Versions 3.6.1.5 through 3.6.1.20, on page 45, below. To create an FMC orchestrator using OpenAPI, see the user guide available as online help in your Secure Workload web portal. For version 3.6.1.36, don't miss the section on domains.
5	In Secure Workload: Enforce policies on desired workspaces. (This is separate from enabling enforcement in the FMC orchestrator.)	In the workspace(s), click the **Enforcement** tab, then click the **Enforce Policies** button and complete the wizard.
6	In Secure Workload version 3.6.1.36: Enable enforcement of the orchestrator: If you have not yet selected domains in the FMC orchestrator, do so now.	Edit the FMC orchestrator to select domains. (If your FMC does not have domains configured, you'll need to select the **Global** domain.) When you click **Update** after selecting domains, this enables enforcement of the orchestrator and deploys your Secure Workload policies to your managed FTD devices. For details, see Editing an FMC Orchestrator in Version 3.6.1.36, on page 48.
	In Secure Workload versions 3.6.1.5 through 3.6.1.20: If you have not yet enabled enforcement in the FMC external orchestrator, do so now.	Edit the FMC orchestrator you configured above and select **Enable Enforcement**.
7	Wait for the new rules to appear in the access control policy or policies.	This takes a variable amount of time, depending on the amount of data to be transferred, the speed of the machines, network bandwidth, etc. To view the rules in your Firepower Management Center: In your FMC, choose **Policies** > **Access Control** and click the policy to view.

Step	Description	More Information
8	The new access control policies are automatically deployed to the associated managed FTDs.	Future changes are also automatically deployed to FTD devices. If you associate new FTDs later to an existing access control policy, the new FTDs will automatically receive the current rules.

Configure the FMC Orchestrator in Version 3.6.1.36

Before you begin

Complete the steps up to this point in the table in How to Implement This Integration for Secure Workload Version 3.6, on page 40.

If you are using a 3.6 version earlier than 3.6.1.36, do not use this procedure. Instead, see Configure the FMC Orchestrator in Secure Workload Versions 3.6.1.5 through 3.6.1.20, on page 45.

Procedure

Step 1 In the Secure Workload web interface, select **Manage > External Orchestrators**.

Step 2 Click **Create New Configuration**

Step 3 Under the Basic Configs tab, configure the following fields:

Option	Description
Type	Select **FMC**.
Name	Enter a unique name for the FMC orchestrator.
Description	Enter a description for the orchestrator.
Full Snapshot Interval(s)	Enter the full snapshot interval, in seconds. The **Full Snapshot Interval(s)** field specifies how often the FMC external orchestrator tests the FMC connectivity to Secure Workload. If an error occurs (for example, if the FMC is not reachable due to network issues, or if invalid endpoint/user credentials were used) the FMC orchestrator reports the error in the **Status** field. Default value: `3600 seconds`
Username	Enter the username and password of the dedicated user that you created in FMC, as instructed previously in this document. These credentials are used to communicate with the FMC.
Password	

Option	Description
CA Certificate	Enter the CA Certificate that Secure Workload will use to authenticate this FMC. You can obtain this certificate from the FMC using the Object Management workflow. For more information, see the Internal Certificate Authority Objects topics in the Reusable Objects chapter of the *Firepower Management Center Configuration Guide* for your Firepower version.
Accept Self-signed Cert	Select this checkbox to configure the FMC orchestrator to trust a self-signed certificate.
Secure Connector Tunnel	If you are using Secure Workload SaaS, you must enable this option. If you are using an on-premises Secure Workload appliance, you may need to enable this option. Before you can enable this option, you must have deployed a Secure Connector, as described in Prerequisites for Integration: Secure Workload 3.6, on page 40.
Enforcement Mode	Select **Merge** or **Override** from the drop-down list. • If you select **Override**, the enforced Secure Workload policies replace any existing FMC access control rules. **Important** If you select this option, all existing rules in all access control policies associated with an FTD (in the domains you select, if applicable) will be deleted and unrecoverable. If you have rules that you want to retain, we recommend that you either export the rules before continuing with this integration, or use the **Merge** option (described below). • If you select **Merge**, the rules from Secure Workload are added to the beginning of the list of access control rules. **Note** If the **Enforcement Mode** is set to **Merge**: • We recommend that you do not use the prefix `Workload_` for any rules that you enter manually into FMC, as they will be automatically removed. • Avoid performing FTD deployment via the FMC UI and policy enforcement via Secure Workload at the same time. These asynchronous and long running (~2 minutes) operations compete against each other and may cause FTD deployment to fail. If the FTD deployment fails due to competing policy enforcements, you must repeat the deployment.

Step 4 Click on the **Host Lists** link at the left.

Step 5 Enter the host name and port number for the associated FMC.

The `host name` should be a fully qualified domain name for FMC or an IP address.

The `port number` is 443 by default.

If your FMC is deployed in a supported high-availability configuration, also enter the hostname and port for the standby/secondary FMC.

Step 6 Click **Create**.

You may briefly see a green banner that indicates that Secure Workload has successfully connected to your Firepower Management Center.

After the connection is established, Secure Workload fetches the domains configured on your Firepower Management Center. This may take a few minutes.

(If you do not have domains configured, Secure Workload fetches the **Global** domain.)

After domains have successfully been fetched, you will see the option to select domains.

Step 7 If you do not want to deploy policies to your managed FTD devices now:

When you see the option to select domains, click **Cancel**.

When you are ready to deploy policies, return to the External Orchestrators page, edit this orchestrator, click **Domains**, and select domains as described in the next step.

Step 8 Select the domain(s) to which you want to push segmentation policies.

If your Firepower deployment does not have domains configured, select the **Global** domain.

Step 9 Click **Update**.

Segmentation policies are pushed to the access control policies in the domains you selected, and the changes are deployed to the associated FTD devices.

The amount of time required to push the rules is typically a few minutes, but depends on the number of policy rules and the resource configuration of FMC and FTDs.

What to do next

Return to the procedure overview table in How to Implement This Integration for Secure Workload Version 3.6, on page 40 and continue with the remaining steps.

Configure the FMC Orchestrator in Secure Workload Versions 3.6.1.5 through 3.6.1.20

Use the following procedure to create an FMC external orchestrator using the Secure Workload web interface.

Before you begin

Complete the steps up to this point in the table in How to Implement This Integration for Secure Workload Version 3.6, on page 40.

If you are using version 3.6.1.36, do not use this procedure. Instead, see Configure the FMC Orchestrator in Version 3.6.1.36, on page 43.

Procedure

Step 1 Navigate to **Manage** > **External Orchestrators**.

Step 2 Click **Create New Configuration**

Step 3 Under the Basic Configs tab, configure the following fields:

Option	Description
Type	Select **FMC**.
Name	Enter a unique name for the FMC orchestrator.
Description	Enter a description for the orchestrator.
Full Snapshot Interval (s)	Enter the full snapshot interval, in seconds. The **Full Snapshot Interval (s)** field specifies how often the FMC external orchestrator tests the FMC connectivity to Secure Workload. If an error occurs (for example, if the FMC is not reachable due to network issues, or if invalid endpoint/user credentials were used) the FMC orchestrator reports the error in the **Status** field. Default value: `3600 seconds`
Username	Enter the username and password of the dedicated user that you created in FMC, as instructed previously in this document. These credentials are used to communicate with the FMC.
Password	
CA Certificate	Enter the CA Certificate that Secure Workload will use to authenticate this FMC. You can obtain this certificate from the FMC using the Object Management workflow. For more information, see the Internal Certificate Authority Objects topics in the Reusable Objects chapter of the *Firepower Management Center Configuration Guide* for your Firepower version.
Accept Self-signed Cert	Select this checkbox to configure the FMC orchestrator to trust a self-signed certificate.
Secure Connector Tunnel	If you are using Secure Workload SaaS, you must enable this option. If you are using an on-premises Secure Workload appliance, you may need to enable this option. Before you can enable this option, you must have deployed a Secure Connector, as described previously in this document. For more information about Secure Connector Tunnel, see the User Guide available from your Secure Workload web interface.

Option	Description
Enable Enforcement	Select this checkbox to push policies to the FMC and its managed FTD devices. This checkbox is selected by default. You can select this checkbox even if you have not yet enforced policies for any workspaces; the system will automatically push policies to the FMC and its managed FTDs when you enable enforcement on a workspace. If you deselect this box, policies will not be pushed to the FMC and all rules previously pushed to the FMC will be cleared.
Enforcement Mode	Select **Merge** or **Override** from the drop-down. • If you select **Override**, the enforced Secure Workload policies replace any existing FMC access control rules. **Important** If you select this option, all existing rules in all access control policies associated with an FTD will be deleted and unrecoverable. If you have rules that you want to retain, we recommend that you either export the rules before continuing with this integration, or use the **Merge** option (described below). • If you select **Merge**, the rules from Secure Workload are added to the beginning of the list of access control rules. **Note** If the **Enforcement Mode** is set to **Merge**: • We recommend that you do not use the prefix `Workload_` for any rules that you enter manually into FMC, as they will be automatically removed. • Avoid performing FTD deployment via the FMC UI and policy enforcement via Secure Workload at the same time. These asynchronous and long running (~2 minutes) operations compete against each other and may cause FTD deployment to fail. If the FTD deployment fails due to competing policy enforcements, you must repeat the deployment.

Step 4 Click on the **Host Lists** tab.

Step 5 Enter the host name and port number for the associated FMC.

The `host name` should be a fully qualified domain name for FMC or an IP address.

The `port number` is 443 by default.

If your FMC is deployed in a supported high-availability configuration, also enter the hostname and port for the standby/secondary FMC.

Step 6 Click **Create**.

The amount of time required to push the rules is typically a few minutes, but depends on the number of policy rules and the resource configuration of FMC and FTDs.

After a few minutes, check the status of the integration:

a) On the **External Orchestrators** page, click on the row for your newly-created FMC orchestrator.
b) The Configuration Details dialog box appears. If the connection is successful, the **Progress Status** field shows the number of found FTDs.

What to do next

Return to the procedure overview table in How to Implement This Integration for Secure Workload Version 3.6, on page 40 and continue with the remaining steps.

Advanced: Use ADM to Generate Segmentation Policies

To allow ADM to discover segmentation policies instead of creating them manually:

1. Follow the steps in How to Implement This Integration for Secure Workload Version 3.6, on page 40, but perform the following high-level steps instead of creating the policies manually.
2. In Firepower Management Center:
   a. Use flexconfig to configure the system to export NSEL records (flow data).

      For instructions, see the documentation for your Firepower product at https://www.cisco.com/c/en/us/support/security/defense-center/series.html#~tab-documents.

   b. Ensure that the traffic that you want to affect with your policies is being generated.
3. In Secure Workload:
   a. Deploy an ingest appliance (virtual appliance) to hold the flow data.
   b. Configure an ASA connector to gather the flow data from your Firepower system.

      (This connector gathers flow data from FTD devices.)
   c. Allow some time for the system to gather enough flow data to generate appropriate policies.
   d. Run ADM in all applicable application workspaces
   e. Analyze, validate, and approve the suggested segmentation policies before enforcing them

For details about the Secure Workload steps, see the User Guide in your Secure Workload web interface.

Editing an FMC Orchestrator in Version 3.6.1.36

- You can create the FMC orchestrator without specifying domains on which to enforce policy, then edit the orchestrator configuration later to specify domains for enforcement.

  Enforcement occurs when you click **Update** after selecting domains.
- If you edit an FMC external orchestrator, you must enter the FMC account password again.

- If you modify an FMC orchestrator that has domains selected, Secure Workload fetches the domains again.

  Domains that you have already selected remain selected.

- If you modify an orchestrator, the Exernal Orchestrators page may initially show Connection Status as **Failure** while connection and synchronization occur, but this changes to **Success** after a few moments. You can then edit the domains.

How to Implement This Integration for Tetration Version 3.5

The following table provides the end-to-end workflow to set up a Firepower Management Center and configure its integration with Tetration.

Step	Description	Link to Procedure
1	In Tetration: Define scopes, workspaces and segmentation policies for your environment.	See the Segmentation section of the Tetration User Guide: https://<cluster>/documentation/ui/adm.html
2	If you are using Tetration SaaS, or if the FMC appliance is not directly reachable from Tetration, set up a Secure Connector tunnel to provide connectivity.	By default, Tetration communicates with the FMC REST API using HTTPS on port 443. See the Tetration User Guide at https://<cluster>/documentation/ui/software_agents/secure_connector.html
3	Set up a virtual or physical FMC. See your device's associated Getting Started Guide.	Cisco Firepower Management Center Virtual Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-intro.html Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html
4	In FMC: Create a dedicated domain to be used solely for the integration with Tetration.	See the Creating New Domains section in the Deployment Management chapter of the Firepower Management Center Configuration Guide for your Firepower version. For example: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/domain_management.html#task_F3D21E5A48DF4F5FA0B3C1C4A86AA80D

Step	Description	Link to Procedure
5	In FMC: Assign FTD(s) to the FMC, in the dedicated domain that you created above. **Note** This can also be done later in the process, as the Tetration/FMC integration is capable to detect newly-assigned FTDs.	To add managed devices to an FMC, use the **Devices** > **Device Management** page in the FMC GUI. For more information, see the Add Managed Devices to the FMC topic in the Getting Started Guide for your deployment. For example: • Cisco Firepower Management Center Virtual Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcv/fpmc-virtual/fpmc-virtual-initial-admin.html • Cisco Firepower Management Center 1000, 2500, and 4500 Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1000-2500-4500/fmc-1000-2500-4500.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f • Cisco Firepower Management Center 1600, 2600, and 4600 Getting Started Guide: https://www.cisco.com/c/en/us/td/docs/security/firepower/hw/getting-started/fmc-1600-2600-4600/fmc-1600-2600-4600.html#Cisco_Task.dita_009a8ec9-d320-4577-bcf5-9b09bfef3a2f
6	In FMC: Assign an access control and prefilter policy to the FTD(s), under the dedicated domain you created above. The prefilter policy assigned to the FTD(s) must not be the read-only `Default Prefilter Policy`. If the FMC orchestrator finds an FTD with `Default Prefilter Policy` assigned, it will not push policy enforcements to that FTD.	See the Configure Prefiltering topic in the Prefiltering and Prefilter Policies chapter in the Firepower Management Center Configuration Guide for your Firepower version. For example: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_17608

Step	Description	Link to Procedure
7	In FMC: Create a custom internal user account that is dedicated to the Tetration and FMC integration. Note that this internal user account must be: • Assigned the Administrator role. • In the same domain(s) that the associated FTD(s), access, and prefilter policies belong to.	See the Add an Internal User topic in the Firepower Management Center Configuration Guide for your Firepower version. For example: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/user_accounts_fmc.html#task_j5n_1cr_qcb
8	In Tetration: Create an FMC orchestrator.	Configure an FMC Orchestrator in Cisco Tetration Version 3.5, on page 51
9	In Tetration: Perform policy enforcement on desired workspaces.	See the Policies section of the Tetration User Guide: https://<cluster>/documentation/ui/adm/policies.html
10	The FMC policy enforcer deploys the policies to the prefilter policy of all associated FTDs.	In Firepower Management Center, choose **Policies** > **Access Control** > **Prefilter**. Click on the associated policy to view the rules enforced from Tetration to the FTD(s). For more information, see the Prefiltering and Prefilter Policies topics in the Access Control Chapter of the Firepower Management Configuration Guide associated with your Firepower version. For example: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/prefiltering_and_prefilter_policies.html#id_18072

Configure an FMC Orchestrator in Cisco Tetration Version 3.5

Use the following procedure to create an FMC external orchestrator using the Tetration web interface.

Procedure

Step 1 Navigate to **Visibility > External Orchestrators**

Step 2 Click **Create New Configuration**

Step 3 Under the Basic Configs tab, configure the following fields:

Option	Description
Type	Select **FMC**.

Option	Description
Name	Enter a unique name for the FMC orchestrator.
Description	Enter a description for the orchestrator.
Full Snapshot Interval (s)	Enter the full snapshot interval, in seconds. The **Full Snapshot Interval (s)** field specifies how often the FMC external orchestrator tests the FMC connectivity to Tetration. If an error occurs (for example, if the FMC is not reachable due to network issues, or if invalid endpoint/user credentials were used) the FMC orchestrator reports the error in the **Status** field. Default value: `3600 seconds`
Username	Enter the username and password of the dedicated user that you created in FMC, as instructed previously in this document. These credentials are used to communicate with the FMC.
Password	
CA Certificate	Enter the CA Certificate that Tetration will use to authenticate this FMC. You can obtain this certificate from the FMC using the Object Management workflow. For more information, see the Internal Certificate Authority Objects topics in the Reusable Objects chapter of the *Firepower Management Center Configuration Guide* for your Firepower version.
Accept Self-signed Cert	Select this checkbox to configure the FMC orchestrator to trust a self-signed certificate.
Secure Connector Tunnel	If you are using Tetration SaaS, you must enable this option. If you are using an on-premises Tetration appliance, you may need to enable this option. Before you can enable this option, you must have deployed a Secure Connector, as described previously in this document. For more information about Secure Connector Tunnel, see the User Guide available from your Tetration web interface.
Enable Enforcement	Select this checkbox to push policies to the FMC and its managed FTD devices. This checkbox is selected by default. You can select this checkbox even if you have not yet enforced policies for any workspaces; the system will automatically push policies to the FMC and its managed FTDs when you enable enforcement on a workspace. If you deselect this box, policies will not be pushed to the FMC and all prefilter rules previously pushed to the FMC will be cleared.

Option	Description
Enforcement Mode	Select **Merge** or **Override** from the drop-down. • If you select **Override**, the enforced Tetration policies replace any existing prefilter policy rules. **Important** If you select this option, all existing prefilter policy rules will be deleted and unrecoverable. If you have rules that you want to retain, we recommend that you either export the rules before continuing with this integration, or use the **Merge** option (described below). • If you select **Merge**, the rules from Tetration are added to the beginning of the list of prefilter rules. **Note** If the **Enforcement Mode** is set to **Merge**: • We recommend that you do not use the prefix `Tetrul_` for any rules that you enter manually into FMC, as they will be automatically removed. • Avoid performing FTD deployment via the FMC UI and policy enforcement via Tetration at the same time. These asynchronous and long running (~2 minutes) operations compete against each other and may cause FTD deployment to fail. If the FTD deployment fails due to competing policy enforcements, you must repeat the deployment.

Step 4 Click on the **Host Lists** tab.

Step 5 Enter the host name and port number for the associated FMC.

The `host name` should be a fully qualified domain name for FMC or an IP address.

The `port number` is 443 by default.

If your FMC is deployed in a supported high-availability configuration, also enter the hostname and port for the standby/secondary FMC.

Step 6 Click **Create**.

The amount of time required to push the rules is typically a few minutes, but depends on the number of policy rules and the resource configuration of FMC and FTDs.

After a few minutes, check the status of the integration:

a) On the **External Orchestrators** page, click on the row for your newly-created FMC orchestrator.
b) The Configuration Details dialog box appears. If the connection is successful, the **Progress Status** field shows the number of found FTDs.

View Enforcement Status of Domains

For release 3.6.1.36 or later: In the list of orchestrators on the **Manage > External Orchestrators** page:

- For release 3.6.1.36:

  Enforcement always shows **Disabled**.

- For release 3.7:

  If enforcement is enabled for at least one domain, **Enforcement** shows as **Enabled**.

For all of the above releases, to see which domains are enforced:

1. Edit the configuration for the particular FMC orchestrator.
2. Click **Domains**.
3. Enforcement is enabled for all domains listed on this Domains page.

Troubleshoot the Secure Workload/Tetration Integration with Secure Firewall Management Center

Use the following procedures to troubleshoot common configuration issues in the integration between Secure Workload/Tetration and Secure Firewall Management Center.

Troubleshoot Integration Connection Issues

Use the **External Orchestrators** page to identify common issues behind connection failures.

1. Navigate to the **External Orchestrators** page:

   For Secure Workload 3.6: This is under the **Manage** menu.

   For Tetration 3.5: This is under the **Visibility** menu.

2. On the External Orchestrators page, find the row for your FMC orchestrator.
3. The integration connection status appears under the **Connection Status** column. If this column displays `Failure`, click on the row to show more details.
4. In the Configuration Details table, find the **Authentication Failure Error** row.

If the **Authentication Failure Error** field displays `Waiting to connect`, wait another minute or two before refreshing the page.

If the **Authentication Failure Error** row displays an error similar to the following:

```
fmc clusterUUID=602c4264755f0263ee16e5af failed to connect to appliance 172.28.171.193:10447
```

Check for the following configuration issues:

Issue	Troubleshooting Steps
The configured IP `host name` and/or `port number` is invalid.	Ensure that the FMC `host name` and `port number` that you entered into the FMC external orchestrator configuration are correct. Verify your connectivity to the configured IP and port.
The **Username** or **Password** is incorrect.	Ensure that the **Username** and **Password** fields that you entered in the FMC orchestrator configuration match the dedicated user that you created in FMC, and that the user has the required privileges as specified previously in this document. **Note** The number of times in a row that users can enter incorrect web interface login credentials before the system temporarily blocks the account from access for a configurable time period is determined by the **Max Number of Login Failures** Global User Configuration setting in FMC. For more information, see the Global User Configuration Settings topic in the Appliance Platform Settings chapter of the Secure Firewall Management Center guide for your Secure Firewall version.
The **Secure Connector Tunnel** checkbox is checked in the FMC orchestrator's Basic Configs, but the Secure Connector is not deployed correctly.	Ensure that the Secure Connector is deployed correctly. For more informaiton, see the Secure Connector section of the user guide:

(Secure Workload 3.6.1.36 and Later) Status List Does Not Show Per-Domain Enforcement Status

See View Enforcement Status of Domains, on page 54.

(Secure Workload 3.6) Identify Policy Enforcement Issues

- In the FMC, select **Devices** > **Device Management** and ensure that the FTDs are assigned an access control policy.
- Click the access control policy associated with the FTD(s) and verify that the Default section of the rules list includes the expected rules.
- If not, ensure that the dedicated FMC user credentials have the required access.

  If you see only golden rules, you probably have not enforced policy in any application workspaces.

  In the workspace(s), verify that policy enforcement is enabled.
- In the FMC External Orchestrator configuration:
  - Verify that Secure Workload can successfully connect to the FMC.
  - Depending on your 3.6 version and whether your FMC deployment has multiple domains configured:

    Verify that the **Enable Enforcement** checkbox is selected.

    -or-

    Verify that the correct domains are selected.

Tip To view details about an FMC orchestrator, including the number of managed FTD devices that receive policy updates via this orchestrator: Go to **Manage > External Orchestrators** and click the row for your FMC orchestrator. The FTD count appears in the **Progress Status** row of the table that appears.

.

(Tetration 3.5) Identify Policy Enforcement Issues

Use the following steps to verify that your Tetration rules are being enforced on the associated FTD(s):

1. In Secure Firewall Management Center, select **Devices** > **Device Management**.
2. Click the Access Control Policy link for the associated FTD.
3. If the prefilter policy assigned to the FTD access control policy is the default read-only `Default Prefilter Policy`, Tetration skips deploying the policies to the FTD. You must create a custom prefilter policy for Tetration to use in the integration with FMC. (See the applicable step in How to Implement This Integration for Tetration Version 3.5, on page 49.)

If your custom rule does appear in the access control policy list, verify that the rules are being enforced:

1. In Secure Firewall Management Center, navigate to **Policies** > **Access Control** > **Prefilter**.
2. Click on your custom prefilter policy to see its rules list.

If your custom prefilter policy does appear in the access control list, but no enforced Tetration rules are displayed:

- Verify the FMC connectivity
- Verify that the **Enable Enforcement** checkbox is checked in the Tetration **External Orchestrators** configuration.
- Verify that policy enforcement has been performed.

Policy Update Fails in FMC High Availability Deployment

It can take up to 4 minutes for this switchover to complete; during this time, any policy enforcement to the non-active FMC will fail.

Rules from Secure Workload Do Not Appear in Access Control Policy

- Rules are pushed only to access control policies that have at least one FTD assigned.
- Check the connection status of the FMC orchestrator on the External Orchestrators page.
- If you are using Secure Workload version 3.6.1.36, make sure you have selected the expected domains in the FMC orchestrator.

Contact Cisco TAC

If your issue persists, contact the appropriate Cisco support team based on your deployment:

- Secure Workload/Tetration On-Premises - Contact TAC

- Secure Workload/Tetration SaaS - Open a case with the SaaS support team

History of the Secure Workload/FMC Integration

For more information about the history of Secure Workload and FMC integration, and the supported product versions, see Supported Deployments, on page 12.