Platform Settings Policies

The following topics explain platform settings policies and how to deploy them to managed devices:

Introduction to Platform Settings

A platform settings policy is a shared set of features or parameters that define the aspects of a managed device that are likely to be similar to other managed devices in your deployment, such as time settings and external authentication.

A shared policy makes it possible to configure multiple managed devices at once, which provides consistency in your deployment and streamlines your management efforts. Any changes to a platform settings policy affects all the managed devices where you applied the policy. Even if you want different settings per device, you must create a shared policy and apply it to the desired device.

For example, your organization's security policies may require that your appliances have a "No Unauthorized Use" message when a user logs in. With platform settings, you can set the login banner once in a platform settings policy.

You can also benefit from having multiple platform settings policies on a Firepower Management Center. For example, if you have different mail relay hosts that you use under different circumstances or if you want to test different access lists, you can create several platform settings policies and switch between them, rather than editing a single policy.

Related Topics

Configure Platform Settings for Classic Devices

System Configuration Settings

Requirements and Prerequisites for Platform Settings Policies

Model Support

Any, but you must create the correct type of policy for the target devices:

- **Firepower Settings** to create a shared policy for Classic managed devices: ASA FirePOWER, NGIPSv.
- **Threat Defense Settings** to create a shared policy for Firepower Threat Defense managed devices.

Supported Domains

Any

User Roles

Admin

Access Admin

Network Admin

Managing Platform Settings Policies

Use the Platform Settings page (**Devices** > **Platform Settings**) to manage platform settings policies. This page indicates the type of device for each policy. The Status column shows the device targets for the policy.

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 Manage your platform settings policies:

- Create — To create a new platform settings policy, click **New Policy**; see Create a Platform Settings Policy, on page 3.
- Copy — To copy a platform settings policy, click **Copy** ( ).
- Edit — To modify the settings in an existing platform settings policy, click **Edit** ( ).
- Delete — To delete a policy that is not in use, click **Delete** ( ), then confirm your choice.

Caution You should not delete a policy that is the last deployed policy on any of its target devices, even if it is out of date. Before you delete the policy completely, it is good practice to deploy a different policy to those targets.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Create a Platform Settings Policy

Platform settings for Firepower Threat Defense devices differ from platform settings for Classic devices. When you create a new platform settings policy you must choose a type: *Firepower* (for Classic managed devices) or *Threat Defense* (for FTD devices).

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 Click **New Policy**.

Step 3 Choose a device type from the drop-down list:

- **Firepower Settings** to create a shared policy for Classic managed devices.
- **Threat Defense Settings** to create a shared policy for Firepower Threat Defense managed devices.

Step 4 Enter a **Name** for the new policy and optionally, a **Description**.

Step 5 Optionally, choose the **Available Devices** where you want to apply the policy and click **Add to Policy** (or drag and drop) to add the selected devices. You can enter a search string in the **Search** field to narrow the list of devices.

Step 6 Click **Save**.
The system creates the policy and opens it for editing.

Step 7 Configure the platform settings based on the device platform type:

- For Firepower Settings, see Platform Settings for Classic Devices.
- For Threat Defense Settings, see Platform Settings for Firepower Threat Defense.

Step 8 Click **Save**.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Setting Target Devices for a Platform Settings Policy

You can add targeted devices at the same time you create a new policy, or you can change them later.

Procedure

Step 1 Choose **Devices** > **Platform Settings**.

Step 2 Click **Edit** ( ) next to the platform settings policy that you want to edit.

Step 3 Click **Policy Assignment**.

Step 4 Do any of the following:

- To assign a device, high-availability pair, or device group to the policy, select it in the **Available Devices** list and click **Add to Policy**. You can also drag and drop.
- To remove a device assignment, click **Delete** ( ) next to a device, high-availability pair, or device group in the **Selected Devices** list.

Step 5 Click **OK**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.