



## Configure a Basic Policy

Configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

You can also customize your security policy to include more advanced inspections.

- [Configure interfaces, on page 1](#)
- [Configure the DHCP server, on page 6](#)
- [Add the default route, on page 8](#)
- [Configure NAT, on page 10](#)
- [Configure an access control rule, on page 13](#)
- [Deploy the configuration, on page 15](#)

## Configure interfaces

When you use the Firewall Device Manager for initial setup instead of using the CLI, the following interfaces are preconfigured:

- Ethernet 1/1—**outside**, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— **inside**, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within Firewall Device Manager before registering with the Firewall Management Center, then that configuration is preserved.

If you used the CLI for initial setup, there is no preconfiguration of your device.

In both cases, you need to perform additional interface configuration after you register the device. For CLI initial setup, you must add the VLAN1 interface for the inside switch ports. Additional configuration includes

converting switch ports to firewall interfaces as desired, assigning interfaces to security zones, and changing IP addresses.

The following example configures a routed-mode inside interface (VLAN1) with a static address and a routed-mode outside interface using DHCP (Ethernet1/1). It also adds a DMZ interface for an internal web server.

## Procedure

**Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) for the device.

**Step 2** Click **Interfaces**.

**Figure 1: Interfaces**

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitorin	Port Mode	VLAN Usage	SwitchPo	Virtual Router
Management1/1	management	Physical				Disabled			Global	
Ethernet1/1	outside	Physical	outside		10.89.5.29/255.255.255.192...	Disabled			Global	
Ethernet1/2		Physical				Disabled	Access	1		
Ethernet1/3		Physical				Disabled	Access	1		
Ethernet1/4		Physical				Disabled	Access	1		

**Step 3** If you used the CLI for initial setup, enable the switch ports.

a) Click **Edit** (✎) for the switch port.

**Figure 2: Enable Switch Port**

### Edit Physical Interface

**General** Hardware Configuration

Interface ID:  
Ethernet1/2

Enabled

Description:

Port Mode:  
Access

VLAN ID:  
1  
(1 - 4070)

Protected:

b) Enable the interface by checking the **Enabled** check box.

- c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.
- d) Click **OK**.

**Step 4** Add (or edit) the **inside** VLAN interface.

- a) Click **Add Interfaces > VLAN Interface**, or if this interface already exists, click **Edit** (🔗) for the interface.

**Figure 3: Add VLAN Interface**

**Add VLAN Interface**

**General** IPv4 IPv6 Advanced

Name: inside

Enabled

Description:

Mode: None

Security Zone: inside\_zone

MTU: 1500  
(64 - 9198)

Priority: 0 (0 - 65535)

VLAN ID \*: 1 (1 - 4070)

Disable Forwarding on Interface Vlan: None

Associated Interface	Port Mo...
No records to display	

- b) From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**. For example, add a zone called **inside\_zone**. You apply your security policy based on zones or groups. If VLAN1 was preconfigured, the rest of these fields are optional.
- c) Enter a **Name** up to 48 characters in length. For example, name the interface **inside**.
- d) Check the **Enabled** check box.
- e) Leave the **Mode** set to **None**.

- f) Set the **VLAN ID** to **1**.

By default, all of the switchports are set to VLAN 1; if you choose a different VLAN ID here, you need to also edit each switchport to be on the new VLAN ID.

You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

- g) Click the **IPv4** and/or **IPv6** tab.

- **IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

For example, enter **192.168.1.56/24**

**Figure 4: Set Inside IP Address**

**Add VLAN Interface**

General **IPv4** IPv6 Advanced

IP Type:  
Use Static IP

IP Address:  
192.168.1.56/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

- h) Click **OK**.

**Step 5** Click **Edit** (✎) for Ethernet1/1 that you want to use for **outside**.

The **General** page appears.

Figure 5: General

## Edit Physical Interface

General IPv4 IPv6 Path Monitoring Harc

Name:

Enabled

Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:   
(64 - 9198)

Priority:   
(0 - 65535)

Propagate Security Group Tag:

NVE Only:

- From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**. For example, add a zone called **outside\_zone**.  
If VLAN1 was pre-configured, the rest of these fields are optional.
- Enter a **Name** up to 48 characters in length.  
For example, name the interface **outside**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- Click the **IPv4** and/or **IPv6** tab.
  - IPv4**—Choose **Use DHCP**, and configure the following optional parameters:
    - Obtain default route using DHCP**—Obtains the default route from the DHCP server.
    - DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.

Figure 6: Set Outside IP Address

### Edit Physical Interface

General **IPv4** IPv6 Path Monitoring

IP Type:

Obtain default route using DHCP:

DHCP route metric:

(1 - 255)

- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

f) Click **OK**.

**Step 6** Configure a DMZ interface to host a web server, for example.

- Disable switch-port mode for the switch port you want to use for the DMZ by clicking the slider in the **SwitchPort** column so it shows as disabled (☐).
- Click **Edit** (✎) for the interface.
- From the **Security Zone** drop-down list, choose an existing DMZ security zone or add a new one by clicking **New**.  
For example, add a zone called **dmz\_zone**.
- Enter a **Name** up to 48 characters in length.  
For example, name the interface **dmz**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- Click the **IPv4** and/or **IPv6** tab and configure the IP address as desired.
- Click **OK**.

**Step 7** Click **Save**.

## Configure the DHCP server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the firewall.

### Procedure

**Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) for the device.

**Step 2** Choose **DHCP > DHCP Server**.

Figure 7: DHCP Server

The screenshot shows the DHCP Server configuration page. The 'DHCP Server' tab is selected. Settings include: Ping Timeout (50 ms), Lease Length (3600 sec), Auto-Configuration (unchecked), Interface (dropdown), and Override Auto Configured Settings (Domain Name, Primary/Secondary DNS and WINS Servers). A '+ Add' button is highlighted in a red box at the bottom right of the configuration area.

**Step 3** In the **Server** area, click **Add** and configure the following options.

Figure 8: Add Server

The 'Add Server' dialog box shows the following configuration: Interface: inside; Address Pool: 192.168.1.2-192.168.1.55 (with a note '(2.2.2.10-2.2.2.20)'); Enable DHCP Server: checked. Buttons for 'Cancel' and 'OK' are at the bottom.

- **Interface**—Choose the interface name from the drop-down list.
- **Address Pool**—Set the range of IP addresses. The IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enable the DHCP server on the selected interface.

**Step 4** Click **OK**.

**Step 5** Click **Save**.

## Add the default route

The default route normally points to the upstream router reachable from the outside interface. If you obtained the outside address from DHCP, your device might have already received a default route. If you need to manually add the route, complete this procedure.

### Procedure

**Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) for the device.

**Step 2** Choose **Routing > Static Route**.

**Figure 9: Static Route**

The screenshot shows the 'Static Route' configuration page. The navigation menu on the left includes 'Device', 'Routing', 'Interfaces', 'Inline Sets', 'DHCP', 'VTEP', and 'SNMP'. Under 'Routing', 'Static Route' is selected and highlighted with a red box. The main content area features a table with columns: Network, Interface, Leaked from Virtual Router, Gateway, Tunneled, Metric, and Tracked. The table is currently empty, with expandable sections for 'IPv4 Routes' and 'IPv6 Routes'. A red box highlights the '+ Add Route' button in the top right corner.

If you received a default route from the DHCP server, it will show in this table.

**Step 3** Click **Add Route**, and set the following options.

Figure 10: Add Static Route Configuration

**Add Static Route Configuration**

Type:  IPv4  IPv6

Interface\*  
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

- any-ipv4
- gateway
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8

Selected Network

- any-ipv4

Gateway\*  
gateway +

Metric:  
1  
(1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:  
 +

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
- **Available Network**—Choose **any-ipv4** for an IPv4 default route, or **any-ipv6** for an IPv6 default route, and click **Add** to move it to the **Selected Network** list.
- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

**Step 4** Click **OK**.

The route is added to the static route table.

**Step 5** Click **Save**.

# Configure NAT

This procedure creates a NAT rule for internal clients to convert the internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

## Procedure

**Step 1** Choose **Devices > NAT**, and click **New Policy**.

**Step 2** Name the policy, select the devices that you want to use the policy, and click **Save**.

**Figure 11: New Policy**

**New Policy** ⓘ

**Name:**  
FTD\_policy

**Description:**

**Targeted Devices**  
Select devices to which you want to apply this policy.

**Available Devices and Templates**

Search by name or value

192.168.0.124  
192.168.0.155

**Selected Devices and Templates**

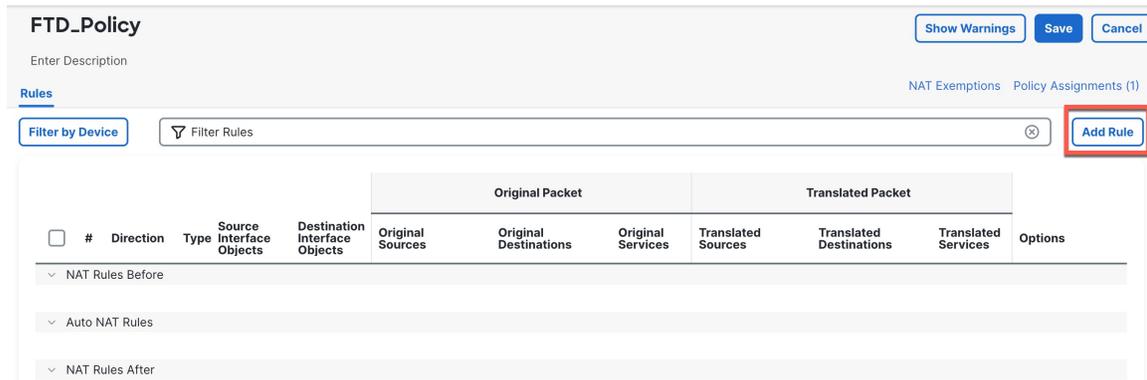
192.168.0.124  
192.168.0.155

Add to Policy

Cancel Save

The policy is added the Firewall Management Center. You still have to add rules to the policy.

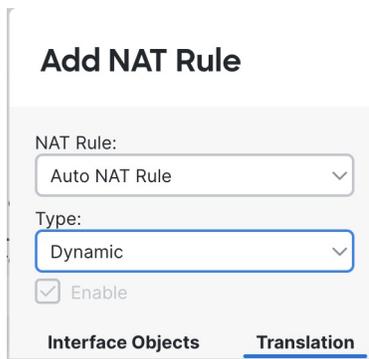
Figure 12: NAT Policy



**Step 3** Click **Add Rule**.

**Step 4** Configure the basic rule options:

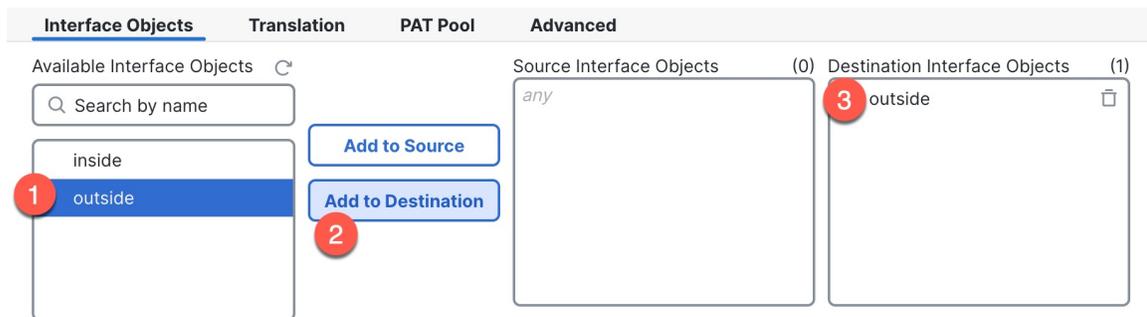
Figure 13: Basic Rule Options



- **NAT Rule**—Choose **Auto NAT Rule**.
- **Type**—Choose **Dynamic**.

**Step 5** On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 14: Interface Objects



**Step 6** On the **Translation** page, configure the following options:

Figure 15: Translation

Interface Objects	Translation	PAT Pool	Advanced
Original Packet		Translated Packet	
Original Source:* <input type="text" value="all-ipv4"/> +		Translated Source: <input type="text" value="Destination Interface IP"/>	
Original Port: <input type="text" value="TCP"/>		Translated Port: <input type="text"/>	
		ⓘ The values selected for Destination Interface Objects in 'Interface Objects' tab will be used	

- **Original Source**—Click **Add (+)** to add a network object for all IPv4 traffic (**0.0.0.0/0**).

Figure 16: New Network Object

### New Network Object ?

**Name**

**Description**

**Network**  
 Host     Range     Network     FQDN

Allow Overrides

**Note**

You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

- **Translated Source**—Choose **Destination Interface IP**.

**Step 7** Click **Save** to add the rule.

The rule is saved to the **Rules** table.

**Step 8** Click **Save** on the **NAT** page to save your changes.

# Configure an access control rule

If you created a basic **Block all traffic** access control policy when you registered the firewall, then you need to add rules to the policy to allow traffic through the firewall. The access control policy can include multiple rules that are evaluated in order.

This procedure creates an access control rule to allow all traffic from the inside zone to the outside zone.

## Procedure

**Step 1** Choose **Policies > Security policies > Access Control**, and click **Edit** (✎) for the access control policy assigned to the device.

**Step 2** Click **Add Rule**, and set the following parameters.

**Figure 17: Source Zone**

The screenshot shows the 'Add Rule' configuration interface. The rule name is 'inside-to-outside'. The 'Action' is set to 'Allow'. The 'Intrusion Policy' is set to 'None'. The 'Zones' tab is selected, showing a list of zones: 'inside (Routed Security Zone)' and 'outside (Routed Security Zone)'. The 'inside' zone is selected with a checkmark. The 'Add Source Zone' button is highlighted with a red circle.

1. Name this rule, for example, **inside-to-outside**.

2. Select the inside zone from **Zones**

3. Click **Add Source Zone**.

**Figure 18: Destination Zone**

The screenshot shows the 'Add Rule' configuration interface. The rule name is 'inside-to-outside'. The 'Action' is set to 'Allow'. The 'Logging' is set to 'OFF'. The 'Time Range' is set to 'None'. The 'Intrusion Policy' is set to 'None'. The 'Zones' tab is selected, showing a list of zones: 'inside (Routed Security Zone)' and 'outside (Routed Security Zone)'. Both 'inside' and 'outside' zones are selected with checkmarks. The 'Add Destination Zone' button is highlighted with a red circle.

4. Select the outside zone from **Zones**.
5. Click **Add Destination Zone**.

Leave the other settings as is.

**Step 3** (Optional) Customize associated policies by clicking on the policy type in the packet flow diagram.

Prefilter, Decryption, Security Intelligence, and Identity policies are applied before an access control rule. Customizing these policies is not required, but after you know your network's needs, they let you improve network performance by either fastpathing trusted traffic (bypassing processing) or blocking traffic so no further processing is required.

**Figure 19: Policies Applied Before Access Control**



- **Prefilter Rules**—The Default Prefilter Policy passes all traffic for the other rules to act on (analyzes). The only change to the default policy you can make is to **block** tunnel traffic. Otherwise, you can create a new prefilter policy to associate with the access control policy that can analyze (pass on), fastpath (bypass further checks) or block.

Prefiltering lets you improve performance by dealing with traffic before it gets any further, by either blocking or fastpathing. In a new policy, you can add *tunnel* rules and *prefilter* rules. A tunnel rule lets you fastpath, block, or rezone plaintext (non-encrypted), passthrough tunnels. A prefilter rule lets you fastpath or block non-tunneled traffic identified by IP address, port, and protocol.

For example, if you know you want to block all FTP traffic on your network, but fastpath SSH traffic from an administrator, you can add a new prefilter policy.

- **Decryption**—Decryption is not applied by default. Decryption is a way to expose network traffic to deep inspection. In most cases, you don't want to decrypt traffic, and can only do so if it is legally allowed. For maximum network protection, a decryption policy might be a good idea for traffic going to critical servers or coming from untrusted network segments.
- **Security Intelligence**—(Requires the IPS license) Security Intelligence is enabled by default. Security Intelligence is another early defense against malicious activity applied before passing connections to the access control policy for further processing. Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names provided by Talos, the threat intelligence organization at Cisco. You can add or delete additional IP addresses, URLs, or domains if desired.

**Note**

If you do not have the IPS license, this policy will not be deployed even though it shows in your access control policy as enabled.

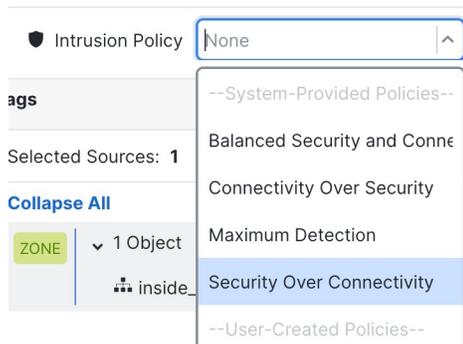
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.

**Step 4** (Optional) Add an Intrusion policy that is applied after the access control rule.

The Intrusion policy is a defined set of intrusion detection and prevention configurations that inspects traffic for security violations. The Firewall Management Center includes many system-provided policies you can enable as-is or that you can customize. This step enables a system-provided policy.

- a) Click the **Intrusion Policy** drop-down list.

Figure 20: System-Provided Intrusion Policies



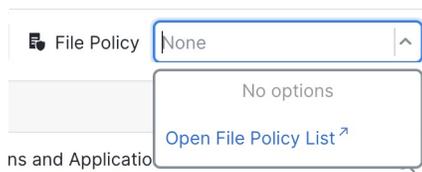
- b) Choose one of the system-provided policies from the list.

We recommend **Balanced Security and Connections** for most use cases.

**Step 5** (Optional) Add a File policy that is applied after the access control rule.

- a) Click the **File Policy** drop-down list and choose either an existing policy or add one by choosing the **Open File Policy List**.

Figure 21: File Policy



For a new policy, the **Policies > Security policies > Malware & File** page opens in a separate tab.

- b) See the [Cisco Secure Firewall Device Manager Configuration Guide](#) for details on creating the policy.  
 c) Return to the **Add Rule** page and select the newly created policy from the drop-down list.

**Step 6** Click **Apply**.

The rule is added to the **Rules** table.

**Step 7** Click **Save**.

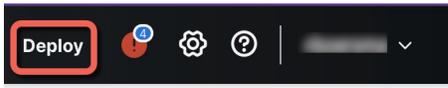
## Deploy the configuration

Deploy the configuration changes to the device; none of your changes are active on the device until you deploy them.

### Procedure

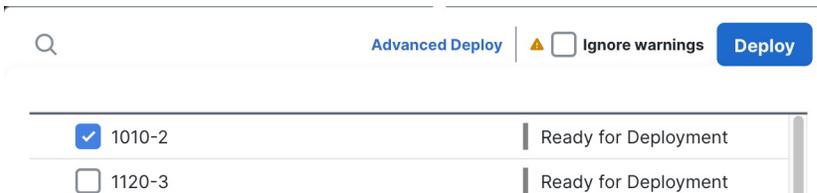
**Step 1** Click **Deploy** in the upper right.

Figure 22: Deploy



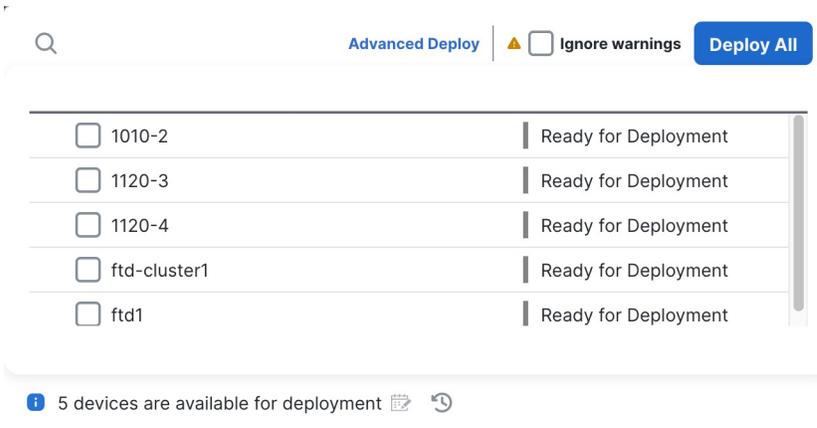
**Step 2** For a quick deployment, check specific devices and then click **Deploy**.

Figure 23: Deploy Selected



Or click **Deploy All** to deploy to all devices.

Figure 24: Deploy All



Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 25: Advanced Deployment

1 device selected

Search using device name, user name, type, group or status

Deploy time: Estimate **Deploy**

Pending Changes Reports

Device	Modified by	Inspect Interru...	Type	Group	Last Deploy Time	Preview
<input type="checkbox"/> ftd1	rboersma, System		FTD		Feb 26, 2024 11:09 ...	Ready for Deployment
<input type="checkbox"/> ftd-cluster1	rboersma, System		FTD		Feb 22, 2024 10:36 ...	Ready for Deployment
<input checked="" type="checkbox"/> 1010-2	rboersma, System		FTD		Feb 22, 2024 11:09 ...	Ready for Deployment

- Access Control Group
  - Access Control Policy: in-out *rboersma, System*
  - Intrusion Policy: No Rules Active *rboersma, System*
  - Network Analysis Policy: Balanced Security and Connectivity *rboersma, System*
- Device Configurations
  - Interface Policy *rboersma*
  - Flex Configuration
    - Template Policy: Unassigned *rboersma*
  - NAT Group
    - Manual NAT Rules: interface\_PAT *rboersma*
  - Security Updates
    - Rule Update: (isp-rel-20240311-2013)

**Step 3**

Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 26: Deployment Status

Search Deploy

Deployments Upgrades Health Tasks

7 total 1 running 6 success 0 warnings 0 failures

Show Pop-up Notifications

ID	Description	Progress	Duration
1010-2	Deployment - Policy and object collection complete.	10%	11s
1120-3	Deployment to device successful.		2m 39s
1120-4	Deployment to device successful.		2m 43s
3110-1	Deployment to device successful.		1m 38s

