



Recommended Policy and Rule Settings

- [Recommended Policy and Rule Settings, on page 1](#)
- [Decryption Policy Settings, on page 2](#)
- [Access Control Policy Settings, on page 3](#)

Recommended Policy and Rule Settings

We recommend the following policy settings:

- Decryption policy:
 - Default action **Do Not Decrypt**.
 - Enable logging.
 - Set **Undecryptable Actions** to **Block** for both **SSL v2 Session** and **Compressed Session**.
 - Enable TLS 1.3 decryption in the policy's advanced settings.
- decryption rule: Enable logging for every rule except those with a **Do Not Decrypt** rule action. (It's up to you; if you want to see information about traffic that isn't decrypted, enable logging for those rules also.)
- Access control policy:
 - Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
 - Set the default policy action to **Intrusion Prevention: Balanced Security and Connectivity**.
 - Enable logging.

Related Topics

- [Decryption Policy Settings, on page 2](#)
- [Decryption Rule Settings](#)
- [Access Control Policy Settings, on page 3](#)

Decryption Policy Settings

How to configure recommended the following best practice settings for your decryption policy:

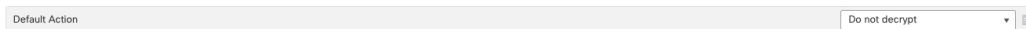
- Default action **Do Not Decrypt**.
- Enable logging.
- Set **Undecryptable Actions** to **Block** for both **SSL v2 Session** and **Compressed Session**.
- Enable TLS 1.3 decryption in the policy's advanced settings.

Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies > Access Control > Decryption**.

Step 3 Click **Edit** (✎) next to your decryption policy.

Step 4 From the **Default Action** list at the bottom of the page, click **Do Not Decrypt**.
The following figure shows an example.



Step 5 At the end of the row, click **Logging** (📄).

Step 6 Select the **Log at End of Connection** check box.

Step 7 Click **OK**.

Step 8 Click **Save**.

Step 9 Click the **Undecryptable Actions** tab.

Step 10 We recommend setting the action for **SSLv2 Session** and **Compressed Session** to **Block**.

You shouldn't allow SSL v2 on your network and compressed TLS/SSL traffic is not supported so you should block that traffic as well.

See the section on Default Handling Options for Undecryptable Traffic in the [Cisco Secure Firewall Management Center Device Configuration Guide](#) for more information about setting each option.

The following figure shows an example.

SSL Policy Example

Enter Description

Rules Trusted CA Certificates **Undecryptable Actions** Advanced Settings

Decryption Errors	Block
Handshake Errors	Inherit Default Action
Session not cached	Inherit Default Action
Unsupported Cipher Suite	Inherit Default Action
Unknown Cipher Suite	Inherit Default Action
SSLv2 Session	Block
Compressed Session	Block

Revert to Defaults

Step 11 Click the **Advanced Settings** tab page.

Step 12 Select the **Enable TLS 1.3 Decryption** check box. For more information about the other options, see the section on advanced decryption options in the section on Default Handling Options for Undecryptable Traffic in the [Cisco Secure Firewall Management Center Device Configuration Guide](#).

Applies to 7.1.0 and later

Block flows requesting ESNi

Disable HTTP/3 advertisement

Propagate untrusted server certificates to clients

Applies to 7.2.0 and later

Enable TLS 1.3 Decryption

Applies to 7.3.0 and later

Enable adaptive TLS server identity probe

Advanced options are available only with Snort 3

Revert to Defaults

Step 13 At the top of the page, click **Save**.

What to do next

Configure decryption rules and set each one as discussed in [Decryption Rule Settings](#).

Access Control Policy Settings

How to configure recommended the following best practice settings for your access control policy:

- Associate your decryption policy with an access control policy. (If you fail to do this, your decryption policy and rules have no effect.)
- Set the default policy action to **Intrusion Prevention: Balanced Security and Connectivity**.
- Enable logging.

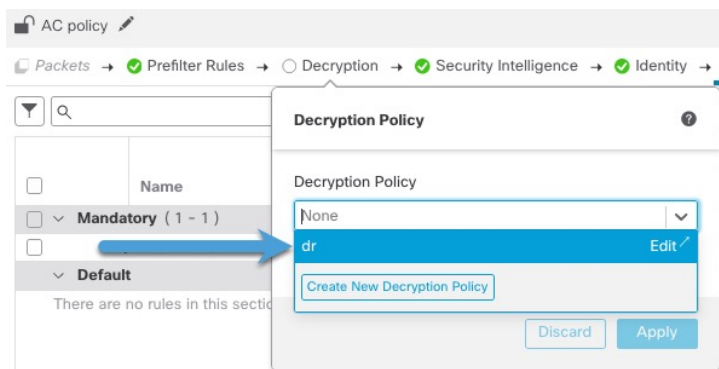
Step 1 Log in to the Secure Firewall Management Center if you haven't already done so.

Step 2 Click **Policies > Access Control**.

Step 3 Click **Edit** (✎) next to your access control policy.

Step 4 (If your decryption policy is not set up yet, you can do this later.)

a) Click the **Decryption** link at the top of the page as the following figure shows.

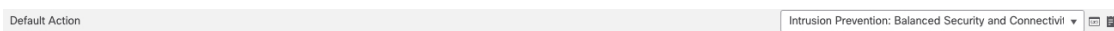


b) From the list, click the name of your decryption policy.

c) Click **Apply**.

d) At the top of the page, click **Save**.

Step 5 From the **Default Action** list at the bottom of the page, click **Intrusion Prevention: Balanced Security and Connectivity**. The following figure shows an example.



Step 6 Click **Logging** (📄).

Step 7 Select the **Log at End of Connection** check box and click **OK**.

Step 8 Click **Save**.

What to do next

See [Decryption Rule Examples](#).