Product Compatibility in Version 6.2.0.*x*

Integrated Product Compatibility

The required versions for the following integrated products vary by Firepower version:

- Cisco Identity Services Engine (ISE)
- Cisco AMP Threat Grid
- Cisco Firepower User Agent

For more information about the required versions, see the Firepower Compatibility Guide.

Web Browser Compatibility in Version 6.2.0.6

Firepower web UI for Version 6.2.0.6 has been tested on the browsers listed in the following table:

⚠ **Caution** The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 1: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 67	JavaScript, cookies
Mozilla Firefox 60	JavaScript, cookies, TLS v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox web browser search bar and click **Refresh Firefox**. Note that you may lose existing Firefox settings when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.The Firepower Management Center uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the Firepower Management Center Configuration Guide for your version.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari 8 and 9	—
Microsoft Edge	—

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility in Version 6.2.0.5

Firepower web UI for Version 6.2.0.5 has been tested on the browsers listed in the following table:

Caution The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 2: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 64	JavaScript, cookies
Mozilla Firefox 58	JavaScript, cookies, TLS v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and th Login screen takes a long time to load, enter **about:support** in a Firefox web brow search bar and click **Refresh Firefox**. Note that you may lose existing Firefox setti when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. Firepower Management Center uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a truste certificate authority. For more information on replacing server certificates, see t section on system configuration in the Firepower Management Center Configura Guide for your version.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari 8 and 9	—
Microsoft Edge	—

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility in Version 6.2.0.4

Firepower web UI for Version 6.2.0.4 has been tested on the browsers listed in the following table:

Caution The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 3: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 63	JavaScript, cookies
Mozilla Firefox 57	JavaScript, cookies, TLS v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox web browser search bar and click **Refresh Firefox**. Note that you may lose existing Firefox settings when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings.The Firepower Management Center uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the Firepower Management Center Configuration Guide for your version. **Caution** Firefox 56 incorrectly displays HTML instead of the Firepower Management Center UI . We *strongly* recommend using Firefox 57 or later, or Firefox 55 or earlier.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari	Not supported
Microsoft Edge	Not supported

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility in Version 6.2.0.3

Firepower web UI for Version 6.2.0.3 has been tested on the browsers listed in the following table:

Caution The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 4: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 60	JavaScript, cookies
Mozilla Firefox 55	JavaScript, cookies, TLS v1.1 or v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox web browser search bar and click **Refresh Firefox**. Note that you may lose existing Firefox settings when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. The FMC uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the Firepower Management Center Configuration Guide for your version. **Caution** Firefox 56 incorrectly displays HTML instead of the FMC UI . We *strongly* recommend using Firefox 57 or later, or Firefox 55 or earlier.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility in Version 6.2.0.2

Firepower web UI for Version 6.2.0.2 has been tested on the browsers listed in the following table:

Caution The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 5: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 57	JavaScript, cookies
Mozilla Firefox 53	JavaScript, cookies, TLS v1.1 or v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and the Login screen takes a long time to load, enter **about:support** in a Firefox web browser search bar and click **Refresh Firefox**. Note that you may lose existing Firefox settings when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. The FMC uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a trusted certificate authority. For more information on replacing server certificates, see the section on system configuration in the Firepower Management Center Configuration Guide for your version. **Caution** Firefox 56 incorrectly displays HTML instead of the FMC UI . We *strongly* recommend using Firefox 57 or later, or Firefox 55 or earlier.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ...**.
Apple Safari	Not supported.
Microsoft Edge	Not supported.

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Web Browser Compatibility in Version 6.2.0.1

Firepower web UI for Version 6.2.0.1 has been tested on the browsers listed in the following table:

Caution The Chrome browser does not cache static content, such as images, CSS, or Javascript, with the system-provided self-signed certificate. This may cause the system to redownload static content when you refresh. To avoid this, add the self-signed certificate used by the Firepower System to the trust store of the browser/OS or use another web browser.

Table 6: Supported Web Browsers

Browser	Required Enabled Options and Settings
Google Chrome 56	JavaScript, cookies
Mozilla Firefox 52	JavaScript, cookies, TLS v1.1 or v1.2 **Note** If you use a self-signed certificate on the Firepower Management Center and th Login screen takes a long time to load, enter **about:support** in a Firefox web brow search bar and click **Refresh Firefox**. Note that you may lose existing Firefox setti when you refresh Firefox. For more information, see https://support.mozilla.org/en-US/kb/refresh-firefox-reset-add-ons-and-settings. Firepower Management Center uses a self-signed certificate by default; we recommend that you replace that certificate with a certificate signed by a truste certificate authority. For more information on replacing server certificates, see t section on system configuration in the Firepower Management Center Configura Guide for your version. **Caution** Firefox 56 incorrectly displays HTML instead of the Firepower Management Center UI . We *strongly* recommend using Firefox 57 or later, or Firefox 55 or earlier.
Microsoft Internet Explorer 10 and 11	JavaScript, cookies, TLS v1.1 or v1.2, 128-bit encryption, **Active scripting** security setting, Compatibility View, set **Check for newer versions of stored pages** to **Automatically** **Note** If you use the Microsoft Internet Explorer 11 browser, you must disable **Include local directory path when uploading files to server** in your Internet Explorer settings through **Tools > Internet Options > Security > Custom level ....**
Apple Safari	Not supported
Microsoft Edge	Not supported

Note Many browsers use Transport Layer Security (TLS) v1.3 by default. If you have an active SSL policy and your browser uses TLSv1.3, websites that support TLSv1.3 fail to load. As a workaround, configure your managed device to remove extension 43 (TLS 1.3) from ClientHello negotiation. See this software advisory for more information.

Screen Resolution Compatibility

When you access user interfaces to manage Firepower, we recommend using the screen resolutions in the table below. The user interfaces are compatible with lower resolutions, but a higher resolution optimizes the display.

Table 7: Recommended Screen Resolutions by Web Interface

Web Interface	Recommended Screen Resolution
Firepower Management Centers	At least 1280 pixels wide
7000 and 8000 Series devices	
ASDM (managing ASA FirePOWER)	1024 pixels wide by 768 pixels high
Firepower Device Manager (managing Firepower Threat Defense)	1024 pixels wide by 768 pixels high