Mandiant

PROXY SETTINGS

The Proxy Rules page is where you manage the creation of proxy settings and certificates for use with proxies. Proxy use is supported between many of Security Validation's components. The Director, Actors, Zones, Update Service, Integrations, and Threat Intel Integrations can all use proxies, using the Director, Actor, or Zone as the source.

> If your Actor acts as a proxy for another Actor, it requires additional memory to ensure Actions run correctly and patches can be applied. Make sure the Actor has a minimum 8 GB memory.

The following are the available proxy types you can use when creating a proxy definition:

- **http**: plain HTTP proxy, no authentication
- **http_auth**: HTTP proxy using basic authentication
- **http_kerberos**: HTTP proxy using Kerberos authentication
- **http_ntlm**: HTTP proxy using NTLMv2 authentication
- **https**: same as an HTTP proxy but with a HTTPS connection to the proxy
- **https_auth**: HTTPS proxy using basic authentication
- **https_kerberos**: HTTPS proxy using Kerberos authentication
- **http_https_auto**: a combination of the http and https proxy types where it automatically picks which one to use based on the destination; the proxy server must support both http and https
- **http_https_auto_auth**: a combination of the http and https proxy types with basic authentication where it automatically picks which one to use based on the destination; the proxy server must support both http and https
- **os_defined**: automatically detect the proxy configured on the OS. Registry based, Windows OS only.
- **saml**: HTTP proxy using SAML for authentication
- **socks**: SOCKS proxy
- **socks_auth**: SOCKS proxy requiring authentication
- **ssl_mitm**: For SSL Man-in-the-middle, you must first upload the SSL cert of the proxy and set it on the proxy, and that is the cert that will be trusted when sending traffic through the proxy.

For more detailed information about each proxy type, see **Proxy Overview** (https://docs.mandiant.com/home/msv-proxy-overview).

To create a Proxy Definition

1. Go to **Settings > Director Settings**.
2. Select **Proxy Rules**.
3. Click **Add Proxy Definition**.
4. Fill out the general fields of the definition form.
    a. **Name**: Use a descriptive name.
    b. (Optional) **Description**: This description appears when you select a proxy from a drop-down list to help users select the correct proxy.
    c. **Proxy type**: Several options are available, including two that support both HTTP and HTTPS for the same IP and port combination.
    d. **Host:** Enter a fully-qualified hostname or IP address. Specify which type of entry this is using the **Hostname** or **IP** selector.
    e. **Proxy Port**: Specify the port used by your proxy.
5. Additional fields are also required based on the Proxy type. Fill those out.
    a. **Auth username**
        i. When proxy type = **http_ntlm**, use this format: ***username@domain***.

ii. When proxy type = **http_ntlm**, use this format: ***username@domain***.

ii. For all other proxy types, use this format: ***domain\username***.

b. **Auth password**

c. For proxy type = **http_kerberos**, enter the **Kerberos domain controller**.

d. For proxy type = **http_kerberos**, enter the **Kerberos realm**.

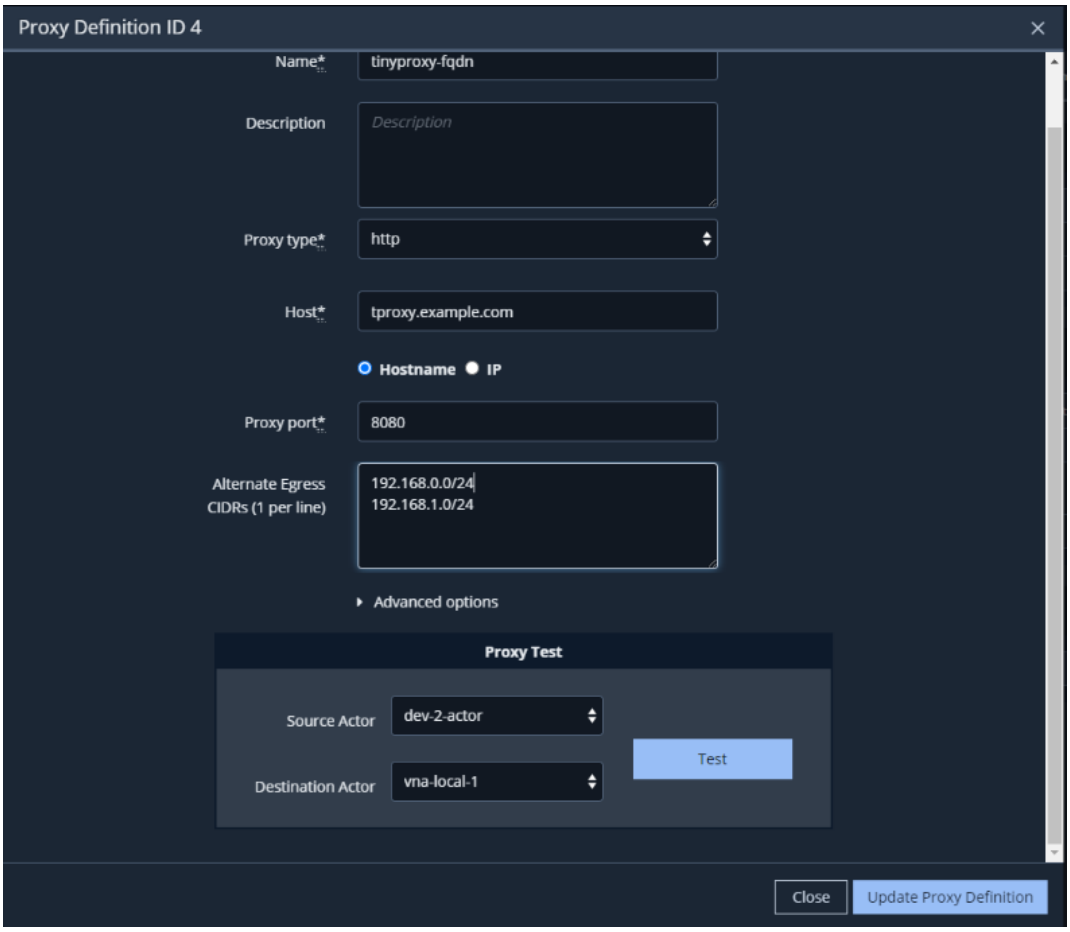
e. For proxy type = **http_ntlm**, select a **Configuration File**.

f. For proxy type = **ssl_mitm**, select or clear **Transparent**.

6. (Optional) Alternate Egress IP addresses / CIDRs (1 per line): Enter outgoing interfaces (IP addresses or CIDR blocks) that relate to the proxy being defined. If the proxy is load-balanced or multi-homed (more than one interface), this can help to match integration events to traffic between Actors and the proxy. Entries should be one per line and have the following format:
   - 192.168.252.25 (e.g., individual IP address)
   - 192.168.252.25/32 (e.g., individual IP address but using CIDR notation)
   - 192.168.252.0/25 (e.g., CIDR notation; all 255 addresses in this block are used by proxy)

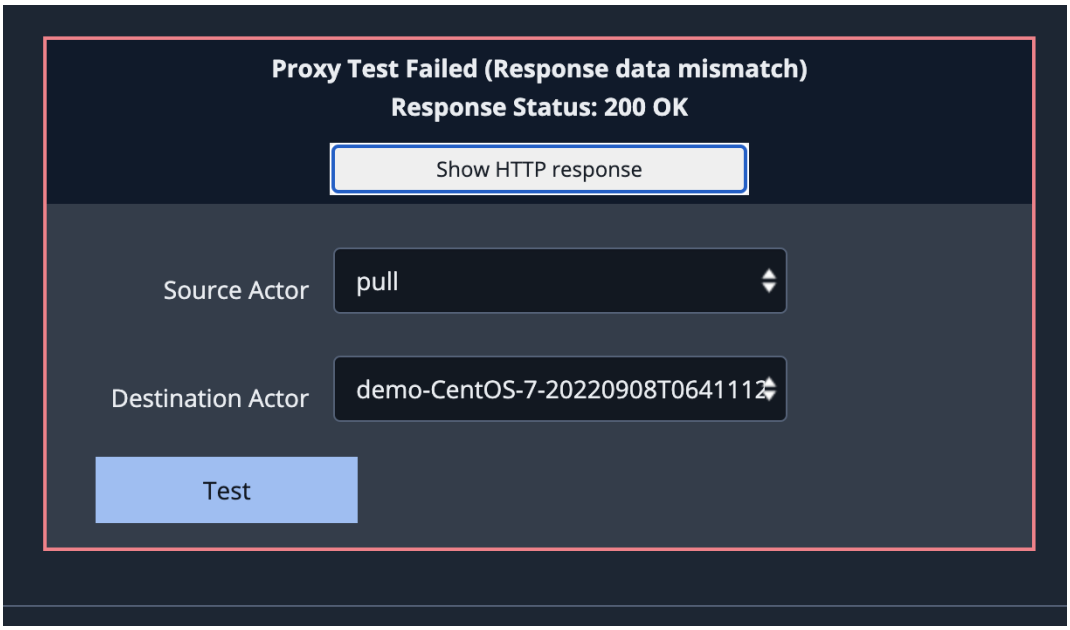
7. (Optional) Expand **Advanced options** and enter the **User-Agent header**.
8. (Optional) Run a **Proxy Test**.
   a. Select a Source and Destination Actor or Director combination.
   b. Click **Test**.

Integrations can have proxy assignments but the proxy rules associated with them cannot be tested through this proxy test. If you want to test an integration's proxy definition, go to the Integration and run the integration test.

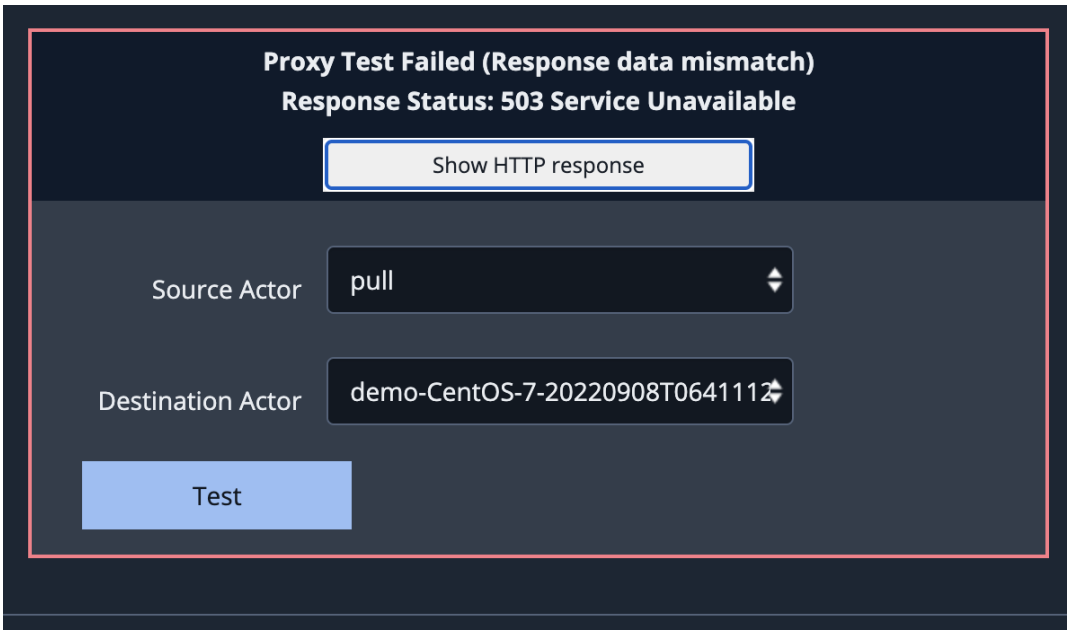


Add Proxy Definition

If the test fails, a results screen appears with a status code error. You can click **Show HTTP Response** to show more details on why the error occurred and resolve the issue before you create the proxy definition.



Proxy Test Failed: 200 OK



Proxy Test Failed: 503 Service Unavailable

9. When you are satisfied with the Proxy definition, click **Create Proxy Definition**.

To Assign the Proxy Definition for communications between Components

You must have one or more proxy definitions created.

1. Go to **Settings > Proxy Rules**.
2. Click **Add Proxy Assignment**.
3. Select the Source.
    a. Choose the category (Director, All Actors and Zones, Actor, or Security Zone).

b. If you are presented with a list, select one or more items from the list.

4. Click **Next**.
5. Select the Destination.
   a. Choose the category (Director, All Actors and Zones, Update Service, Content API, Actor, Security Zone, Integrations, Threat Intel Integrations, Job Notification/AEDA Notification/Operational Status Webhook).

      If your integrations do not support proxy definitions, the Integrations list will be empty.

   b. If you are presented with a list, select one or more items from the list.
6. Click **Next**.
7. Select the Proxy Definition.

   Only valid proxy definitions for your source and destination combination will appear.
8. (optional) Select **Monitor Traffic Only**.
9. Click **Submit**. The proxy rule will be assigned to communications between the specified source and destination.

To add a Proxy Certificate

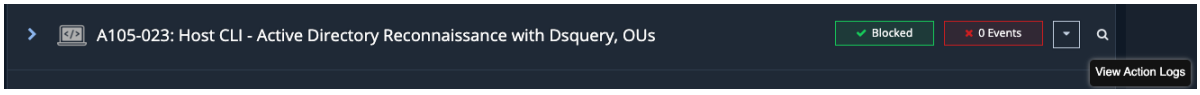
1. Click **Add Proxy Certificate**.
2. Enter a **Name** for the certificate.
3. Browse to and select the **Certificate File**.
4. Click **Save**.

Running Actions involving a Proxy

When running Jobs that may involve a proxy, the Default Proxy will be determined automatically based on the Proxy Rules associated with the Actors being selected to run the Action.

If other Proxy Rules are defined for your environment, you can choose an alternative proxy from the Override Proxy dropdown menu for ad hoc testing. However, when interpreting Job results, it's important to consider the role (if any) of the selected proxy in routing traffic for the Actors being used. For example, if you select a proxy that can't talk to the Actors defined in the job, the Action will be shown as Blocked. But in this case, the Action would be Blocked because of a network timeout, not because it was detected and blocked by a security control.

The role of the proxy (if any) in a Blocked action can be confirmed by clicking **View Action Logs**:



View Action Logs