

Troubleshoot the Dynamic Attributes Connector

How to troubleshoot issues with the dynamic attributes connector.

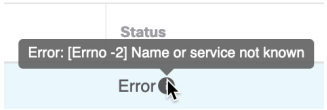
- Troubleshoot error messages, on page 1
- Get your tenant ID, on page 2
- Manually get a certificate authority (CA) chain, on page 2

Troubleshoot error messages

This reference provides error messages and troubleshooting solutions for dynamic attributes connectors and adapters in the dynamic attributes connector.

Problem: name or service not known error

This error is displayed as a tooltip when you hover the mouse over an error condition on an adapter or connector. An example follows; yours might look different.

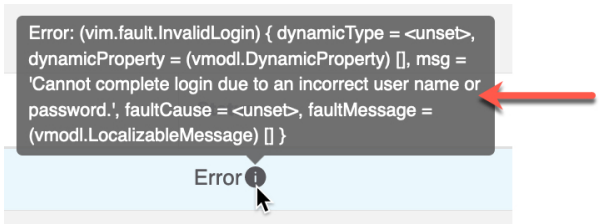


Solution: Edit the connector or adapter and check for:

- A trailing slash on a host name
- Verify the password is correct

Problem: incorrect username or password

This error is displayed as a tooltip when you hover the mouse over an error condition on a connector.



Solution: Edit the connector and change the user name or password.

Get your tenant ID

This task provides your tenant ID to Cisco TAC for troubleshooting assistance with the dynamic attributes connector.

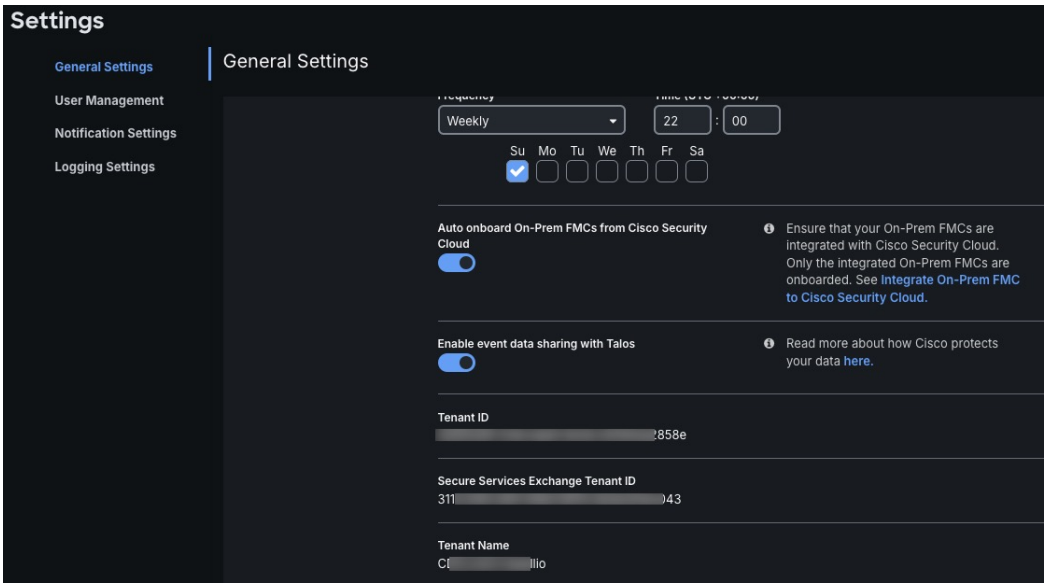
If you require assistance with the dynamic attributes connector, you must provide your tenant ID to Cisco TAC so we can look at your logs.

Procedure

Step 1 Click **Administration** > **General Settings**.

Step 2 Copy your tenant ID to the clipboard to provide to Cisco TAC.

A sample follows.



Manually get a certificate authority (CA) chain

If the certificate authority chain is not fetched automatically, use one of these browser-specific procedures to get a certificate chain to securely connect to vCenter or Firewall Management Center .

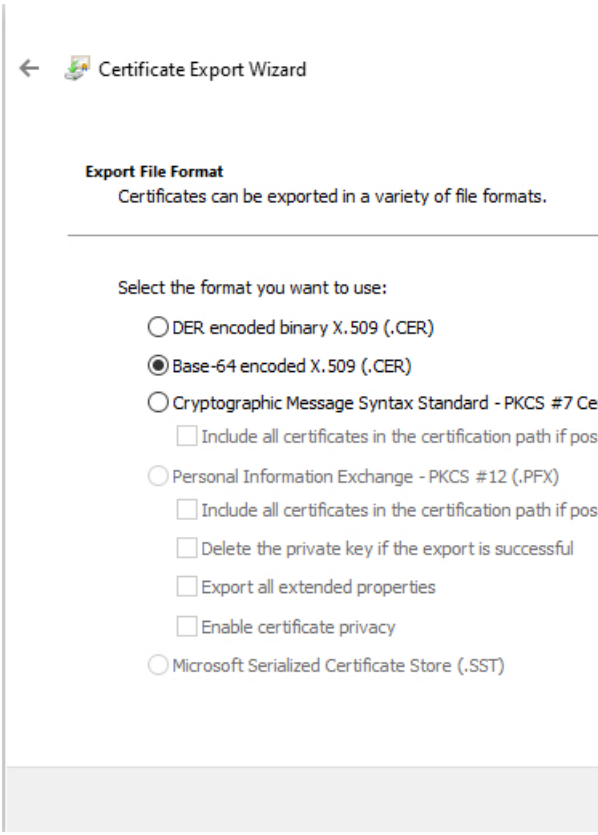
The *certificate chain* is the root certificate and all subordinate certificates.

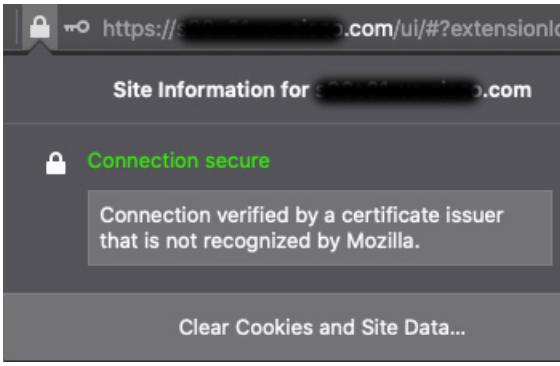
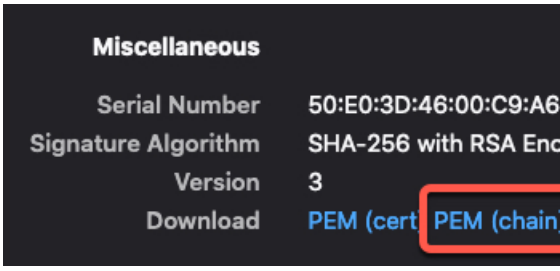
Procedure

	Command or Action	Purpose

Step 1	Get a Certificate Chain—Mac (Chrome and Firefox)	**a.** Open a Terminal window.
		b. Enter this command:
		`security verify-cert -P url[:port]`
		where *url* is the URL (including scheme) to vCenter or Firewall Management Center . For example:
		`security verify-cert -P https://myvcenter.example.com`
		If you access vCenter or Firewall Management Center using NAT or PAT, you can add a port as follows:
		`security verify-cert -P https://myvcenter.example.com:12345`
		c. Save the entire certificate chain to a plaintext file.
		• *Include* all `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` delimiters.
		• *Exclude* any extraneous text (for example, the name of the certificate and any text contained in angle brackets (< and >) as well as the angle brackets themselves.
		d. Repeat these tasks for vCenter Firewall Management Center .

Step 2	Get a Certificate Chain—Windows Chrome	**a.** Log in to vCenter or Firewall Management Center using Chrome. **b.** In the browser address bar, click the lock to the left of the host name. **c.** Click **Certificate**. **d.** Click the **Certification Path** tab. **e.** Click the top (that is, first) certificate in the chain. **f.** Click **View Certificate**. **g.** Click the **Details** tab.

	Command or Action	Purpose
		h. Click **Copy to File**. **i.** Follow the prompts to create a CER-formatted certificate file that includes the entire certificate chain. When you're prompted to choose an export file format, click **Base 64-Encoded X.509 (.CER)**.  Follow the prompts to complete the export. Open the certificate in a text editor. Repeat the process for all certificates in the chain. You must paste each certificate in the text editor in order, first to last. Repeat these tasks for vCenter or Firewall Management Center .
Step 3	Get a Certificate Chain—Windows Firefox	**a.** Log in to vCenter or Firewall Management Center using Firefox.

	Command or Action	Purpose
		b. Click the lock to the left of the host name. **c.** Click the right arrow (**Show connection details**).  **d.** Click **More Information**. **e.** Click **View Certificate**. **f.** If the resulting dialog box has tab pages, click the tab page corresponding to the top-level CA. **g.** Scroll to the Miscellaneous section. **h.** Click **PEM (chain)** in the Download row.  **i.** Save the file. Repeat these tasks for vCenter or Firewall Management Center .