SPDM Security

SPDM Security

Cisco UCS M6 Servers can contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, the Security Protocol and Data Model (SPDM) Specification enables a secure transport implementation that challenges a device to prove its identity and the correctness of its mutable component configuration. This feature is supported on Cisco UCS C220 and C240 M6 Servers starting with in Cisco UCS Manager, Release 4.2(1d).

Note SPDM is currently not supported on the Cisco UCS C225 M6サーバ and Cisco UCS C245 M6サーバ.

SPDM defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between Baseboard Management Controllers (BMC) and end-point devices over a Management Component Transport Protocol (MCTP). Message exchanges include authentication of hardware identities accessing the BMC. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication, firmware measurement, and certificate management. Endpoint devices are challenged to provide authentication. and BMC authenticates the endpoints and only allows access for trusted entities.

The UCS Manager optionally allows uploads of external security certificates to BMC. A maximum of 40 SPDM certificates is allowed, including native internal certificates. Once the limit is reached, no more certificates can be uploaded. User uploaded certificates can be deleted but internal/default certificates cannot.

A SPDM security policy allows you to specify one of three Security level settings. Security can be set at one of the three levels listed below:

- Full Security:

  This is the highest MCTP security setting. When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. A fault will also be generated if any of the endpoints do not support either endpoint authentication or firmware measurements.

- Partial Security (default):

  When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. There will NOT be a fault generated when the endpoint doesn't support endpoint authentication or firmware measurements.

- No Security

  When you select this setting, there will NOT be a fault generated for any failure (either endpoint measurement or firmware measurement failures).

You can also upload the content of one or more external/device certificates into BMC. Using a SPDM policy allows you to change or delete security certificates or settings as desired. Certificates can be deleted or replaced when no longer needed.

Certificates are listed in all user interfaces on a system.

Creating and Configuring a SPDM Security Certificate Policy using CLI

A Security Protocol and Data Model (SPDM) policy can be created to present security alert-level and certificate contents to BMC for authentication.

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **create spdm-certificate-policy** *policy-name*
3. UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** | **partial** | **no**}
4. (Optional) UCS-A /org/spdm-certificate-policy* # **set descr** *description*
5. UCS-A /org/spdm-certificate-policy* # **create certificate** *certificate-name*
6. UCS-A /org/spdm-certificate-policy* # **set content**
7. UCS-A /org/spdm-certificate-policy # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type **/** as the *org-name* .
Step 2	UCS-A /org # **create spdm-certificate-policy** *policy-name*	Creates a SPDM security certificate policy with the specified policy name, and enters organization SPDM certificate policy mode. **Note** The only supported certificate type is **pem**.
Step 3	UCS-A /org/spdm-certificate-policy* # **set fault-alert** {**full** | **partial** | **no**}	Configures the fault alert level for this policy.

	Command or Action	Purpose
Step 4	(Optional) UCS-A /org/spdm-certificate-policy* # **set descr** *description*	Provides a description for the SPDM security certificate policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCS-A /org/spdm-certificate-policy* # **create certificate** *certificate-name*	
Step 6	UCS-A /org/spdm-certificate-policy* # **set content**	This prompts for the content of the outside certificate. Enter certificate content one line at a time. After End of Certificate, enter ENDOFBUF at the prompt to return to the command line. **Note** To exit without commiting the certificate content, enter **C**.
Step 7	UCS-A /org/spdm-certificate-policy # **commit-buffer**	Commits the transaction to the system configuration.

What to do next

Assign outside security certificates, if desired.

Displaying the Security Policy Fault Alert Level

After the policy is created, you can check the alert level for the SPDM policy.

SUMMARY STEPS

1. UCS-A /org/spdm-certificate-policy # **show fault-alert**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A /org/spdm-certificate-policy # **show fault-alert** **Example:** `UCS-A /server/cimc/spdm-certificate #show fault-alert`	The returned result shows that the setting for this SPDM policy is Partial, the default. `SPDM Fault Alert Setting: Partial`

Loading an Outside SPDM Security Certificate Policy

The SPDM allows you to download an outside security certificate.

Before you begin

Create a SPDM security certificate policy.

SUMMARY STEPS

1. UCS-A /org # **scope spdm-certificate-policy**
2. UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name*
3. UCS-A /org/spdm-certificate-policy* # **set** {*certificate* }
4. UCS-A /org/spdm-certificate-policy # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A /org # **scope spdm-certificate-policy**	Enters SPDM security certificate policy mode.
Step 2	UCS-A org/spdm-certificate-policy# **create spdm-cert** *Certificate name*	Creates a SPDM security certificate policy for the specified external certificate,.
Step 3	UCS-A /org/spdm-certificate-policy* # **set** {*certificate* }	Specifying certificate prompts for the content of the outside certificate. The only supported certificate type is **pem**.
Step 4	UCS-A /org/spdm-certificate-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows loading a certificate for Broadcom of type PEM.

Example

```
UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert?
Name - Certificate name

UCS-A-FI-A /org/spdm-certificate-policy# create spdm-cert Broadcom
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set?
certificate - Certificate content

UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # set certificate
{enter certificate content}
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert* # commit-buffer
UCS-A-FI-A /org/spdm-certificate-policy/spdm-cert# show detail
SPDM Certificate:
Name: Broadcom
Certificate Type: pem
Certificate Content:
```

Viewing the Certificate Inventory

You can view what SPDM certificates have been uploaded and also request further details for a specified certificate.

SUMMARY STEPS

1. UCS-A # **scope server** *server*
2. UCS-A/server # **scope cimc** *server*
3. UCS-A/server/cimc # **scope spdm** *server*
4. UCS-A/server/cimc/spdm # **show certificate**
5. UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**
6. UCS-A /org/spdm-certificate-policy/certificate # **show**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A # **scope server** *server*	
Step 2	UCS-A/server # **scope cimc** *server*	
Step 3	UCS-A/server/cimc # **scope spdm** *server*	
Step 4	UCS-A/server/cimc/spdm # **show certificate**	The returned result shows the certificate inventory.

Step 5	UCS-A/server/cimc/spdm # **show certificate** *certificate-id***detail**
	Example:
	`UCS-A /server/cimc/spdm-certificate #show certificate 3 detail`
	`Certificate Information`
	`Certificate Id : 3`
	`Subject Country Code (C) : US`
	`Subject State (ST) : Colorado`
	`Subject Organization (O) : Broadcom Inc.`
	`Subject Organization Unit(OU) : NA`
	`Subject Common Name (CN) : NA`
	`Issuer Country Code (C) : US`
	`Issuer State (ST) : Colorado`
	`Issuer City (L) : Colorado Springs`
	`Issuer Organization (O) : Broadcom Inc.`
	`Issuer Organization Unit(OU) : NA`
	`Issuer Common Name (CN) : NA`
	`Valid From : Oct 23 00:25:13 2019 GMT`
	`Valid To : Apr 8 10:36:14 2021 GMT`
	`UserUploaded : Yes`
	`Certificate Content : <Certificate String>`
	`Certificate Type : PEM`
		The returned result shows the certificate ID, identifiers, and expiration date.

Step 6	UCS-A /org/spdm-certificate-policy/certificate # **show**
	Example:
	`SPDM Certificate:`
	`Name SPDM Certificate Type`
	`---------- ------------------------------`
	`cert1 Pem`
	Example:
		The returned result shows the type of certificate details.
		The returned result shows the fault alert setting.

	Command or Action	Purpose
	UCS-A /server/cimc/spdm-certificate/certificate #up UCS-A /server/cimc/spdm-certificate #show SPDM Certificate Policy: Name Fault Alert Setting ---------- ---------- Broadcom Full	

Deleting a SPDM Policy

SUMMARY STEPS

1. UCS-A# **scope org** *org-name*
2. UCS-A /org # **delete spdm-certificate-policy** *policy-name*
3. UCS-A /org # **commit-buffer**

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the org-name.
Step 2	UCS-A /org # **delete spdm-certificate-policy** *policy-name*	Deletes the specified SPDM control policy.
Step 3	UCS-A /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes a power control policy called VendorPolicy2 and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # delete spdm-certificate-policy VendorPolicy2
UCS-A /org* # commit-buffer
UCS-A /org #
```