LDAP Authentication and 3rd Party Certificates

- Verifying LDAP Configurations, on page 1
- 3rd Party Certificates, on page 2
- SSL Issues, on page 4

Verifying LDAP Configurations

Note You can only perform this procedure through the Cisco UCS Central CLI.

It verifies the configuration of the Lightweight Directory Access Protocol (LDAP) provider or the LDAP provider group.

Verifying LDAP Native Authentication

When LDAP fails, verify that Cisco UCS Central can communicate with the LDAP provider:

- The server responds to the authentication request if you provide the correct username and password.
- The roles and locales defined on the user object in the LDAP are downloaded.
- The LDAP group authorization is turned on and the LDAP groups are downloaded.

The first step is to verify that Cisco UCS Central is configured with native authentication.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm security mode.

Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **show default-auth**	Following is an example of the result
		`Default Authentication:`
		`  Realm Authentication Server Group`
		`  ----- ----------------------------`
		`  Local`

Verifying the LDAP Provider Configuration

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters LDAP mode.

Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **show server detail**	Shows server detail:
		`  Hostname or IP address: provider1`
		`  Order: 1`
		`  bindDN:`
		`CN=Administrator,CN=Users,DC=qasamlab,DC=com`
		`  Password:`
		`  Port: 389`
		`  SSL: No`
		`  Basedn: DC=qasamlab,DC=com`
		`  User profile attribute: ciscoavpair`
		`  Filter: cn=$userid`
		`  LDAP Vendor: Open Ldap`

3rd Party Certificates

The following table lists issues related to 3rd party certificates:

Issues	Resolution

Registered Cisco UCS domain fails to register or changes to lost visibility status	Keyring, or certificate configured in Cisco UCS Central, has expired. If the keyring is configured to default, execute the following command to regenerate the default certificate:
	`UCSC # connect policy-mgr`
	`UCSC(policy-mgr)# scope org`
	`UCSC(policy-mgr) /org# scope device-profile`
	`UCSC(policy-mgr) /org/device-profile # scope security`
	`UCSC(policy-mgr) /org/device-profile/security # scope keyring default`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer`
	If the configured keyring is issued by a third party CA, make sure to renew the certificate from the third-party.

Certificate status displays **Not Yet Valid**.	Occurs when Cisco UCS Central is behind in time with CA server. Cisco UCS Central, Cisco UCS domain and the CA server must be synchronized to a valid NTP server.
Certificate status displays **Empty Cert**.	Occurs when the certificate field is empty. Provide content for issued certificates.
Certificate status displays **Failed to Verify with TP**.	Occurs when the configured **Trusted Point** is not the one from which the certificate is issued. Configure the correct **Trusted Point**.
Certificate status displays **Failed to Verify with Private Key**.	Occurs when the certificate contents are wrong and does not match with the certificate request you had created. Make sure to update the certificate information from the certificate request created in the keyring.
Certificate status displays **Certificate Chain Too Long**.	Occurs when the configured **Trusted Point** has a bundled certificate with a depth of 10 or more. This is a product boundary limitation by design.
There are no options to upload or specify CRL.	Cisco UCS Central does not support revoked certificates, so the option to specify CRL is not available.

The `regenerate certificate` command does not work	This command is removed from Cisco UCS Central. Use the following:
	`UCSC # connect policy-mgr`
	`UCSC(policy-mgr)# scope org`
	`UCSC(policy-mgr) /org# scope device-profile`
	`UCSC(policy-mgr) /org/device-profile # scope security`
	`UCSC(policy-mgr) /org/device-profile/security # scope keyring default`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* # set regenerate yes`
	`UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer`

Multidomain certificate does not work.	Cisco UCS Central does not accept multiple DNS entries in a certificate request.

Issues	Resolution
Wildcard certificate does not work.	Cisco UCS Central does not accept wildcards in DNS or subject fields.
Trusted point certificate does not work.	Make sure you have the following order to specify the bundled certificate: 1. Specify the self-signed primary certificate. 2. Specify the subordinate certificate.
Cisco UCS domain registration fails or changes to lost visibility when the configured trust point contains a bundled certificate with depth 2 or more.	Q: If certificate sync fails on both nodes in a cluster setup, what do I do? • When you convert a standalone installation to cluster installation, make sure to recreate the certificate after completing installation on node B. • For an existing cluster setup, contact Cisco Technical Assistance Center.
Certificate sync fails on both the nodes in an HA Cisco UCS Central setup.	Certificate sync fails on both nodes when standalone to HA conversion occurs for Cisco UCS Central setup due to a known issue. Recreate the certificate after HA is ready. For an HA setup that is running, if certificate sync fails, contact Cisco Technical Assistance Center. You can identify certificate sync failure when the browser throws a certificate error. This occurs when you use the IP address of one of the nodes to open the application. It also fails when Cisco UCS Manager registration fails with Cisco UCS Central node IPs of an HA setup.
Certificate is valid, but Cisco UCS Manager still fails to register.	If a certificate configured on Cisco UCS Central contains extra space characters at the end of the certificate, these are incorrectly translated into extra lines on the certificate issued to Cisco UCS Manager, resulting in registration failure. Remove extra space characters, and re-configure it on Cisco UCS Central.

SSL Issues

UCSC third-party certificate request contains required key usages set.

If Customer uses an internal PKI provider, they must use the appropriate template to set both the SSL client, and the SSL server key usages.

Note For Microsoft Enterprise CA, use the computer template to issue third-party certificates.

Cisco UCS Central does not allow you to configure third-party certificates without an SSL client and SSL server key usages.