Prepare SCEP Servers

Prepare SCEP Server

Integration with SCEP Key Server

In this release, the Cisco Intelligent Node Manager integrates with a Simple Certificate Enrolment Protocol (SCEP) server version 2.2.0. The integration allows you to manage an SCEP server independently, which acts as a centralized and secure certificate management solution.

The benefit of using an SCEP server is that you can create your own application like the iNode manager to manage the nodes.

Limitations:

Intelligent Node software version 4.0.0 is the only version compatible with iNode Manager 24.1.

Configuring a MicroMDM SCEP Server

Before you begin ensure that you have an SCEP server installed. You can download and install the SCEP server from https://github.com/micromdm/scep/releases.

1. Create a new CA.

   ```
   ./scepserver-linux-amd64 ca -init
   ```

2. Start the SCEP server.

   ```
   ./scepserver-linux-amd64 -depot depot -port 2016 -challenge=secret
   ```

3. Create the mdmscep.config file with the following configuration and place it in the TFTP server where the Intelligent Node software version 4.0.0 is located.

   ```
   server-url string  SCEP server URL
   keySize int rsa key size (default 2048)
   challenge string enforce a challenge password

   Example:
   server-url  =  http://175.175.145.254:2016/scep
   keySize = 2048
   challenge = secret
   ```

During deployment, for configuring iNode Manager to use MicroMDM SCEP server, user needs to check if iNode Manager UI is available.

Once UI is available, user should configure SCEP details in the UI.

Till the point SCEP details are not configured in the UI, inode-service-manager pod keeps crashing and eventually will lead to unsuccessful deployment, which is expected.

How to check if CA Certificates are configured correctly

Run following commands from a server/VM which has connectivity to SCEP server.

- http://SCEP_IP:SCEP:PORT/scep?operation=GetCACert

- **scepclient-linux-amd64**

How to change the Certificate in MicroMDM SCEP Server

1. Update the SCEP server certificate and key.

2. Restart the SCEP server service.

3. Reboot all the iNodes via iNode Manager or SNMP.

Above steps ensure that all the iNodes and iNode Manager take the new certificate within a 40-minute time span.

No action is needed at the iNode Manager if there are no changes in

`server-url, keySize, challenge.`

If there are changes, then inode-service-manager pod needs a restart.

`challenge`string is configurable.