Industrial Operations Kit User Guide

First Published: 2016-01-15

The Industrial Operations Kit (IOK) virtual appliance serves as a controller to manage and monitor all the individual virtual machines (VMs) provided within the IOK. The IOK simplifies Field Area Network (FAN) deployment by automating the configuration of multiple network and security management system components as individual virtual machines within the Cisco UCS server (hereafter referred to as *server*). The virtual appliances are created during initial IOK software installation. For more information, see VMware Environment on Server.

Note: Follow the instructions in this guide to configure your IOK software. Otherwise, your system may not function normally.

Conventions

This document uses the following conventions.

Conventions	Indication
bold font	Commands and keywords and user-entered text appear in **bold** font.
italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in *italic* font.
[ ]	Elements in square brackets are optional.
{x | y | z }	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
courier font	Terminal sessions and information the system displays appear in courier font.

Conventions	Indication
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note: Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution: Means *reader be careful.* In this situation, you might perform an action that could result in equipment damage or loss of data.

Warning: IMPORTANT SAFETY INSTRUCTIONS

Means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Regulatory: Provided for additional information and to comply with regulatory and customer requirements.

Information About Industrial Operations Kit

The Industrial Operations Kit (IOK) is a Cisco software solution that incorporates multiple virtual appliances for management, network, and security-related head-end network services for the Cisco Smart Grid Multi-Services Field Area Network Solution. The IOK software bundle download provides an entire head-end infrastructure (composed mostly of Cisco components) and the automation required for installation and on-going operations of that head-end infrastructure.

Figure 1 on page 3 illustrates a typical Field Area Network (FAN). In this example, a Cisco 1000 Series Connected Grid Router (CGR or Cisco IOS router) communicates with the systems within the head-end infrastructure.

Within a FAN, each IOK can support up to 1000 of the following three Cisco IOS routers (end devices) in any combination:

Note: See Related Documentation for details on supporting documentation for all of the systems below.

- Cisco 1000 Series Connected Grid Routers (CGR 1240 and CGR 1120), Cisco IOS Release 15.5(3)M, 15.5(2)T2, and 15.4(3)M4.

  Refer to the *Release Notes* for minimum software release and firmware requirements. The IOK does not communicate with Cisco 1000 Series routers running CG-OS.

- Cisco 819 hardened Integrated Services Router (C819HG-4G-V-K9, C819HG-4G-A-K9, C819HG-U-K9, C819HGW-S-A-K9, and C819H-K9), Cisco IOS Release 15.6(1)T0a, 15.5(3)M1, 15.5(3)M, 15.5(2)T2, and 15.4(3)M4.

- Cisco 800 Series Industrial Integrated Services Routers (IR 809 and IR 829), Cisco IOS Release 15.5(3)M0a and 15.5(3)M.

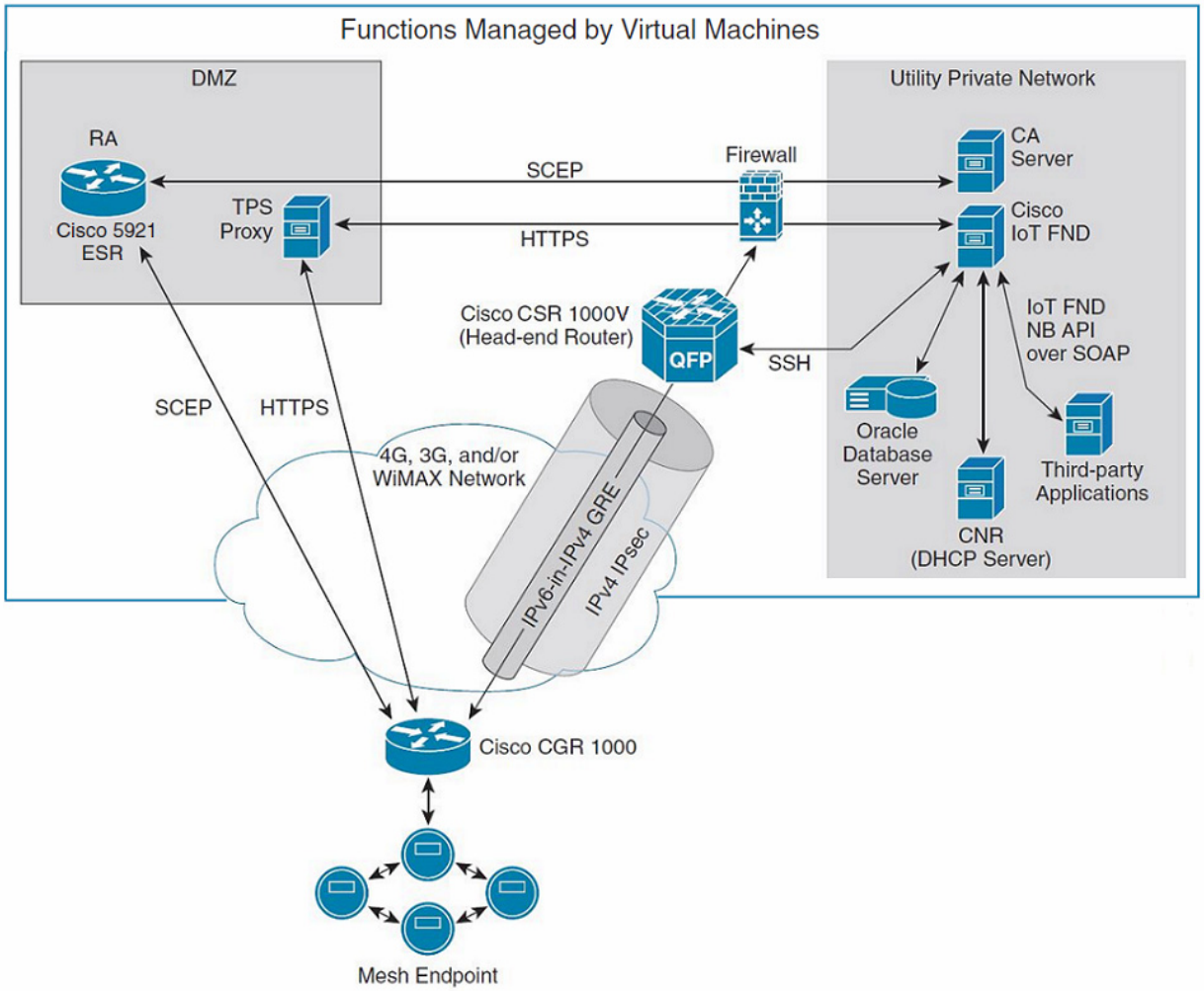
Additionally, each IOK can support up to 250,000 IPv6 CG-mesh endpoints through the Cisco Connected Grid WPAN Module for CG-Mesh deployment.

Note: The number of endpoints that IOK can support is limited by the license file of Cisco IoT Field Network Director (IoT FND), which manages the connected grid systems.

Figure 1 on page 3 shows a typical FAN deployment for Cisco IOS routers. IOK can operate with either an integrated RSA type CA server virtual appliance or an external CA server.

Note: IOK currently does not provide an integrated ECC type CA server.

Figure 1 Typical Field Area Network Deployment for Cisco IOS Routers



The functions of each of the following systems are handled by a separate virtual machine on the server:

- Registration Authority (RA), which is based on Cisco 5921 Embedded Services Router (Cisco 5921 ESR), authenticates and authorizes incoming Simple Certificate Enrollment Protocol (SCEP) requests from the Cisco IOS router.
- Tunnel Proxy Server (TPS) for secure tunnel provisioning.
- Certificate Authority (CA) server, which grants all SCEP requests received from the RA.
- IoT FND (based on Release 3.0 software or later), which manages the connected grid systems.
- Oracle database, which provides database services for IoT FND, is integrated into IoT FND.
- Cisco Prime Access Registrar (CPAR), which provides TACACS+ service for CGR command authorization as well as RADIUS authentication and accounting services for CGR.

  Note: In IOK 2.0, CPAR is replaced by FreeRADIUS, which is integrated into Orchestration VM.

- Head-end router (HER), which is based on Cisco Cloud Services Router 1000 Series (CSR1000V) that supports up to 1000 FlexVPN tunnels in total with up to five CSR1000V routers.

In addition to the functions above, a virtual appliance identified as Orchestration serves as a controller to manage provisioning of configurations across all of the other virtual appliances. The Orchestration virtual appliance is created during initial software installation. For more details, refer to VMware Environment on Server.

VMware Environment on Server

ESXi Hypervisor runs on the host server and provides a VMware layer upon which the virtual appliances operate.

The software bundle provides a Windows 7 based executable installer that automatically deploys and configures each of the individual VMware virtual appliances onto the ESXi host server. Additionally, the installer brings up the Guest OS and application services by leveraging the customer-specific Configuration Template XML file. (See Figure 2 on page 4.)

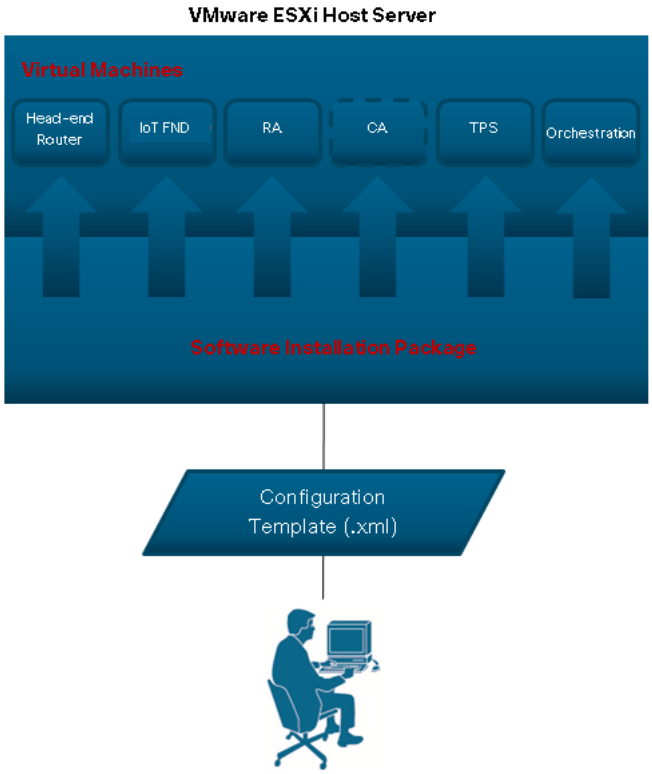
Note: Make sure that the ESXi server supports Red Hat Enterprise Linux (RHEL) Release 7.1(x86_64), which is the Guest OS for IoT FND.

You will enter key information such as IP addresses for all the virtual systems being configured in to the Configuration Template XML file.

Note: You must enter all the requested information in the Configuration Template XML file (detailed in the Prerequisites section) **before** you can initiate the software install. In the Configuration Template XML file, you can also configure IOK to leverage Cisco IOS as the DHCPv6 server for CGRs to provide IPv6 addresses to the endpoints.

The IOK can operate with either an integrated Certification Authority (CA) server virtual appliance or an external Certification Authority (CA) server. If you use an external CA server, no CA virtual appliance will be installed as part of the process illustrated in Figure 2 on page 4.

Figure 2 Installation of Virtual Machines on Server

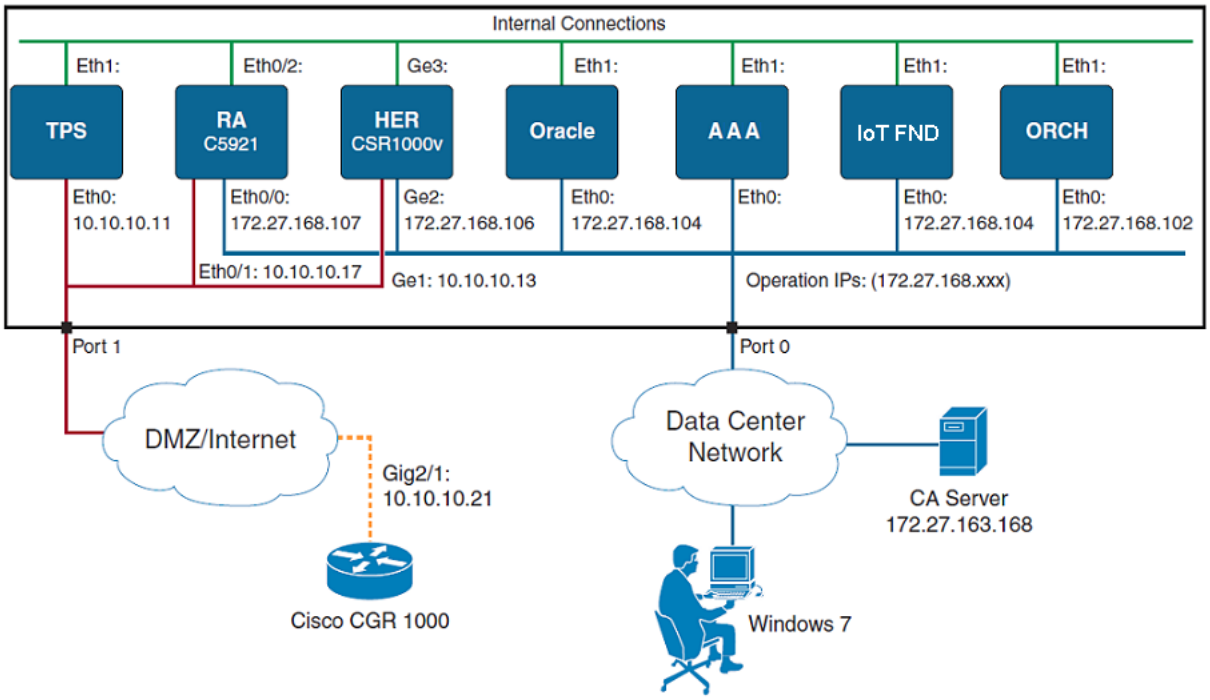


During installation, the software records details on each step into the log file `CISCO-IOK-STD-2.0.16_build-X\log\cisco_iok_installer.log`. If the installation fails, the log file identifies the exact step that failed and the reason for the failure. When you resolve the issue and rerun the installation, it is recommended that you run a fresh installation.

You also have the option to overwrite the VMs by forcing a complete re-installation. In this case, the installer replaces all of the existing installed VMs and redoes all the steps.

Figure 3 on page 5 shows an implementation with an external CA server; therefore, no virtual machine was defined and installed for the CA server.

Figure 3 Example Industrial Operations Kit Configuration Showing Port Mapping of Virtual Machines to DMZ and Data Center Networks with no CA Virtual Machine Installed



Note: Figure 3 on page 5 only illustrates IPv4 addressing. IPv6 addressing might also be required when managing endpoints within the Industrial Operations Kit. You enter all IPv4 and IPv6 addresses relevant to the Industrial Operations Kit through the Configuration Template (.xml) as detailed in Table 1 on page 7. The Windows 7 PC on which the software bundle installer resides **must be** able to reach the server through the Data Center network interface.

Note: Oracle is embedded in IoT FND so they have the same IP address. You do not need to configure the Oracle IP address in the **`cisco_iok_installer.xml`** file.

System Requirements

When using a Cisco UCS Server installed with all the virtual machines (ORCHESTRATION, IOT-FND, TPS, HERs (CSR1k, no more than five HERs), RA (Cisco 5921), and CA (internal server installation is optional; if you have an existing external CA server, we recommend you use that system), we recommend the following resource allocation for each VM.

VM	CPU	Memory (GB)	Disk (GB)
CISCO-IOK-CA	2	4	50
CISCO-IOK-FND/Oracle	4	24	300
CISCO-IOK-HER	1	4	8
CISCO-IOK-HER-1	2	4	8
CISCO-IOK-HER-2	2	4	8
CISCO-IOK-HER-3	2	4	8
CISCO-IOK-HER-4	2	4	8
CISCO-IOK-HER-5	2	4	8
CISCO-IOK-ORCHESTRATION/FreeRADIUS	1	8	200
CISCO-IOK-RA	2	4	50
CISCO-IOK-TPS	1	4	50
In Total	19	64	690

The server must also meet the following additional requirements:

- Two Gigabit Ethernet ports
- VMware vSphere® ESXi™ 5.1 Update 3 or ESXi™ 5.5 Update 2

Prerequisites

- You must have a valid license (production or evaluation) for VMware Hypervisor ESXi 5.1 Update 3 or ESXi™ 5.5 Update 2 with Redhat Enterprise Linux Release 7.1(x86_64) support, and it must be installed on the server before you install the Industrial Operations Kit software bundle.
- You must have a production or evaluation license for IoT FND, an ESR license for RA, a CSR license for HER (only AX and SEC level license works with IOK).
- Verify that you have the IOK software bundle available on a Windows 7 PC that can reach the VMware ESXi host server (Cisco UCS) through network connections.
- Verify that the ESXi host server is active and has two Gigabit Ethernet ports available.
- Disconnect the ESXi host server from the VMware vCenter server application before installing the IOK software package.
- Verify that the following virtual machine IP addresses that will be entered in to the Configuration Template do not conflict with one another:
  - Data center IP addresses for all virtual machines
  - DMZ IP addresses for TPS, RA, and Head-end router
  - IPv6 addresses used by IoT FND and the Head-end router
  - DHCPv4 and DHCPv6 address pool

  - Mesh IPv6 prefix delegation and other IPv6 prefix that is already existing in VM

- Ensure that you have all the information listed in Table 1 on page 7 available for entry into the Configuration Template.

  We recommend using `cisco_iok_config.exe` to generate a new Configuration Template file. You can also use an HTML editor when entering values in the Configuration Template to ensure better clarity between the variable name and its brackets and the required value and to prevent accidental deletion of the brackets.
  Example: <login>*username*</login>.
  Missing brackets will result in an installation failure.

Table 1 Information Required for the Configuration Template (.xml)

System	Variable	Description
Server <esxi info>	Information required for the server, on which the Industrial Operations Kit (IOK) installs all of the VMware machines.	
	<host_ip>*ip address*</host_ip>	Enter the IP address of the server, which serves as the ESXi host.
	<login>*username*</login>	Enter the login username for the server. **Note:** If you do not enter a value in this template, you can enter this value during installation of the software. The username **must be** either the root or have root privilege. The username and password are only used during the installation.
	<password>*password*</password>	Enter the login password for the server. **Note:** Alternatively, you can enter this value during the software installation process. The password you enter is not saved.
	<dmz_port>*vmnic1*</dmz_port>	Enter the Ethernet NIC port that connects to the DMZ network. Format of value is vmnic0, vmnic1, and so on. Default value is vmnic1.
Data Center network settings. <datacenter_interface>	Information required for connection to the Data Center network (Private Network).	
	<gateway>*ip address*</gateway>	Enter the gateway address for the Ethernet port on the server (IOK) that connects to the Data Center network.
	<netmask>*mask address*</netmask>	Enter the subnet mask address for the Data Center network. Default value is 255.255.255.0
	<dns>*ip address*</dns>	Enter the Domain Name Server (DNS) address for the Data Center network.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
DMZ network settings. <dmz_interface>	Information required for connection to the DMZ network.	
	<gateway>*ip address*</gateway>	Enter the gateway address for the Ethernet port on the server (IOK) that connects to the DMZ network.
	<netmask>*mask address*</netmask>	Enter the subnet mask address for the DMZ network. Default value is 255.255.255.0
	<dns>*ip address*</dns>	Enter the Domain Name Server (DNS) address for the DMZ network. **Note:** You may leave this field blank if you do not know the DNS address.
NTP server <ntp_server>	Information required for the NTP server(s). You can define multiple NTP servers.	
	<server>*ip address* | *server name*</server>	Enter either the IP address or name of the NTP server. When you use an NTP server name, the server must have a DNS defined that is accessible to the UCS server.
	<version>*version*</version>	Enter the NTP protocol version. If you do not enter an NTP protocol version, the software assigns the default value of 4 (NTPv4). You can also assign a value of 3 (NTPv3).
<vm_provision>	Information required to provision the FND/Oracle, TPS, and ORCHESTRATION virtual appliances.	
<RSA certificate>	RSA certificate is required for security. You can use either the CA virtual machine or an external server. If you use an external server, you will need to provide the SCEP URL and CA certificate.	
	<using_external_ca>*true* | *false* </using_external_ca>	Enter *false* if you want to use the CA server virtual machine. Enter *true* if you want to use an external CA server.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
External CA <external_ca>	Information required if you are using an external CA server.	
	<scep_url>URL</scep_url>	Enter the SCEP URL. The head-end router (CSR 1000V) and CGR 1000 router require the SCEP to enroll the certificates.
	<ca_cert>*customer CA certificate*</ca_cert>	Enter the CA certificate provided by the customer's Certificate Authority infrastructure.
	<nms_cert>*NMS certificate*</nms_cert>	Enter the FND server certificate in pfx/PKCS12 format.
	<nms_cert_password>*NMS certificate import password*</nms_cert_password>	Enter the certificate password set when you imported the pfx certificate.
	<tps_cert>*TPS certificate*</tps_cert>	Enter the TPS server certificate in pfx/PKCS12 format.
	tps_cert_password>*TPS certificate import password*</tps_cert_password>	Enter the certificate password set when you imported the pfx certificate.
Internal CA server <internal_ca>	Information required if you install an CA server virtual machine.	
	<ca_ipv4>*IPv4 address*</ca_ipv4>	Enter the IPv4 address for the CA virtual machine.
	<login>**admin**</login>	Enter admin as username login for the CA virtual machine.
	<password>*password*</password>	(Optional) Password required to turn on privileged commands. You can configure this later.
	<enable_secret>*password*</enable_secret>	(Optional) Enables the newly defined password.
ECC certificate	(Optional) Only required if mesh endpoints (such as smart meters) are deployed in the field. For router-only deployment, leave this part unconfigured.	
<ecc_certificate>	<ca_cert>CA *certificate*<ca_cert>	Enter path for customer-provided ECC Root CA certificate (pem/cer format).
	<subca_cert>*CA certificate*<ca_cert>	(Optional) Enter path for customer-provided ECC Sub CA certificate in pem/cer format. **Note:** Sub CA is not supported in IOK 2.0. Do not enter value in this field.
	<cpar_cert>*CA certificate*<cpar_cert>	Enter path for FreeRADIUS/CPAR ECC certificate in pfx/PKCS12 or pem/cer format.
	<cpar_cert_password>*password* <cpar_cert_password>	Import password to protect the private key for CPAR ECC certificate.
Operation IPs <vm_ip>	Operation IP addresses must be reserved for each of the following virtual machines (FND/Oracle, TPS, and Orchestration) installed on the server. (See Figure 3 on page 5.)	
	<nms_ipv4>*ip address*</nms_ipv4>	Enter the FND operation IPv4 address.
	<orch_ipv4>*ip address*</orch_ipv4>	Enter the Orchestration/Controller operation IPv4 address.
	<tps_ipv4>*ip address*</tps_ipv4>	Enter the TPS operation IPv4 address.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
License <license>	Information about the FND license.	
	<nms_license>*FND license*</nms_license>	(Optional) Enter the file path of the FND production or evaluation license on the Windows 7 PC where the installer resides. FND can support up to 25 end devices without a license.
Router Provision <router_provisions>	Information about the software Head-end router (HER: CSR1000V) and Registration Authority router (RA: ESR5921). Each router will have at least two interfaces, one is connecting to the operation datacenter; the other is connecting to the DMZ/public network.	
Head-end Router <router_csr1000v_her>	Information required for the Head-end router, Cisco CSR 1000V, that connects to both the Public Network (DMZ network) and Private Network (Data Center network). You **must** define at least one interface to each of the networks. (See Figure 1 on page 3).	
<datacenter_interface>	<ipv4>*ip address*</ipv4>	Enter the IPv4 address for the router interface that will connect to the Data Center network (Private Network).
	<ipv6>*ip address/prefix*</ipv6>	(Optional) Enter the IPv6 address for the router interface that will connect to the Private Network (Data Center network). Otherwise, leave this field blank. Example IPv6 address: 2001:1234::1/64.
<dmz_interface>	<ipv4>*ip address*</ipv4>	Enter the IPv4 address for the router interface that will connect to the Public Network (DMZ).
	<ipv6>*ip address*</ipv6>	(Optional) Enter the IPv6 address for the router interface that will connect to the Public Network (DMZ). Otherwise, leave the field blank.
<loopback_interface>	<ipv4>*ip address*</ipv4>	Loopback interface reserved for FlexVPN virtual template. All defined FlexVPNs will use this interface for traffic forwarding. Enter the IPv4 address for the router loopback interface. **Note:** Interface can also be used by the FND and Data Center network for management purposes. IP addresses can be pulled from the IP pool defined in the <ip_management> section.
	<netmask>*ip address*</netmask>	Enter the mask address for the loopback interface. Default value is 255.255.255.0
	<ipv6>*ip address*</ipv6>	(Optional) Enter the IPv6 address for the loopback interface. Otherwise, leave the field blank. **Note:** We recommend that you not configure the IPv6 loopback address.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
Router Login Username <login>	Information about the Head-end router login username and secret word.	
	<password>*password*</password>	Enter the password for the router login username or leave the field blank and enter it during installation.
	<enable_secret>*secret*</enable>	Enter the router secret word to turn on privileged commands or leave field blank and enter it during installation.
Registration Authority <router_esr5921_ra>	Information on the router, Cisco 5921 ESR, that serves as Registration Authority. You **must** define at least one interface to the Public Network (DMZ network) and one interface to the Private Network (Data Center network). (See Figure 1 on page 3).	
<datacenter_interface>	<ipv4>*ip address*</ipv4>	Enter the IP address for the RA router that will connect to the FND and CA server in the Private Network (Data Center network). **Note:** FND and CA server must be able to reach this router.
	<ipv6>*ip address*</ipv6>	(Optional) Enter the IPv6 address for the router interface that will connect to the Private Network (Data Center network). Otherwise, leave the field blank.
<dmz_interface>	<ipv4>*ip address*</ipv4>	Enter the IP address for the RA router that will connect to the Public Network (DMZ). **Note:** Interface must be reachable by field end devices before the secure tunnel is established.
	<ipv6>*ip address*</ipv6>	(Optional) Enter the IPv6 address for the router interface that will connect to the Public Network (DMZ). Otherwise, leave the field blank.
Router Login Username <login>	Information about Registration Authority router login username and secret word.	
	<password>*password*</password>	Enter the password for the router login username or leave the field blank and enter it during installation.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
<mesh_provision>	(Optional) Only required if the Head-end infrastructure needs to support mesh endpoints. For router only deployment, leave this section unconfigured.	
	IPv6 address information for FND and Orchestration virtual machine interfaces in the Data Center network and in some cases the Service Provider data collection engine (CE). **Note:** The gateway IPv6 address is only required when CE is not in the subnet as the FND Virtual machine. **Note:** Ensure that the IPv6 addresses for FND, Orchestration and HER virtual machines are in the same subnet.	
	<nms_ipv6>*ipv6 address*</nms_ipv6>	IPv6 address for the FND virtual machine interface in the Data Center network.
	<orch_ipv6>*ipv6 address*</orch_ipv6>	IPv6 address for service provider data collection engine (CE). **Note:** Optional configuration if the IPv6 DHCP server for mesh endpoints is configured on CGR 1000.
	<ce_ipv6>*ipv6 address*</ce_ipv6>	IPv6 address for service provider data collection engine (CE).
	<dc_ipv6_gateway/>	(Optional) Only required when the IPv6 address for the CE is not in the same subnet as the FND virtual machine.Data center IPv6 gateway address. Only required if CE IPv6 is not in the same subnet as FND IPv6.
<ip_management>	These IPs will be used as IP pools for field end devices and headend router loopback interfaces. FND will communicate with end devices and head-end router through them. To add multiple IP pools, keep adding <ipv4_pool> or <ipv6_pool> entries.	
<ipv4_pool>	Information on IPv4 pools for field end devices and Head-end router loopback interfaces.	
	<ip_subnet>*subnet*</ip_subnet>	Define an IPv4 subnet such as 192.168.100.0.
	<ip_netmask>*mask address*</ip_netmask>	Enter the mask address. Default value is 255.255.255.0
	<ip_start>*ip address*</ip_start>	Enter the starting IPv4 address within the subnet.
	<ip_end>*ip address*</ip_end>	Enter the ending IPv4 address within the subnet.
<ipv6_pool>	Information on IPv6 pools for field end devices and Head-end router loopback interfaces. Interfaces are also a path for communication with FND.	
	<ip_prefix>*prefix scope*</ip_prefix>	Define the prefix scope such as 2001:cafe:bear::/64.
	<ip_start>*ip address*</ip_start>	Enter the starting IPv6 address within the prefix scope.
	<ip_end>*ip address*</ip_end>	Enter the ending IPv6 address within the prefix scope.

Table 1 Information Required for the Configuration Template (.xml) (continued)

System	Variable	Description
<ipv6_pd_pool>	Information on IPv6 pd pool is to provide the prefix to be assigned to the FAR with mesh endpoint support. It's not for the HER loopback interface.	
	<ip_prefix>*prefix scope*</ip_prefix>	Define the prefix scope such as 2001:cafe:bear::/64.
	<ip_start>*ip address*</ip_start>	Enter the starting IPv6 address within the prefix scope.
	<ip_end>*ip address*</ip_end>	Enter the ending IPv6 address within the prefix scope.
	<subrouter_prefix_length>*length* </subrouter_prefix_length>	Enter the sub-router prefix length.
(Optional) Device Import <device_import>	You can configure field end device files prior to the software bundle installation so that the installer will automatically import the devices in to FND database as part of the installation. The format for listing each imported device file: <device_file>*filepath*</device_file>. If you have no device file for import, then leave the tag value empty.	

Generating Certificates

Before installing the Industrial Operations Kit, you must generate certificates for the TPS and FND virtual machines, IoT Device Manager (IoT-DM), CGR, and RA.

This section includes the following topics:

Generating RSA Certificates for FND and TPS

If you are using an internal CA, ignore this section.

If you are using an external CA, refer to the “Generating Certificates for IoT FND and the IoT FND TPS Proxy” section in *Cisco IoT Field Network Director User Guide, Release 3.0.x*, for detailed information on generating RSA certificates for FND and TPS.

Generating ECC Certificates

The following sections describe enrolling the ECC certificates for Mesh. For the Radius ECC certificates, you can use the same process.

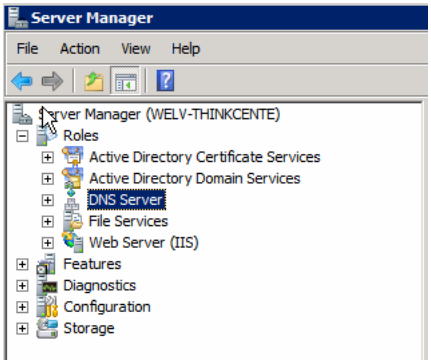
Note: The information in this section is for your reference only. For more details, refer to the Microsoft website.

This section includes the following topics:

- Exporting CA Server Certificate, page 38
- Installing Industrial Operations Kit on the Server, page 39

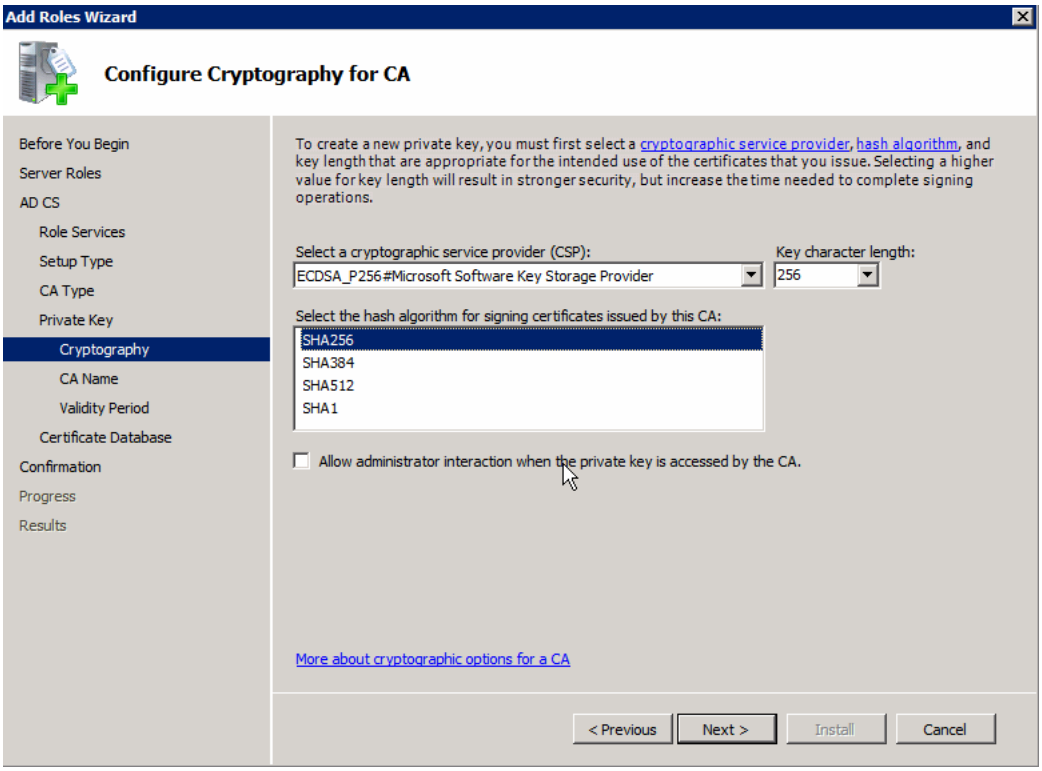
Prerequisites

1. Make sure that the following three roles have been added to your Windows 2008 server:
   - Active Directory Domain Service
   - Active Directory Certificate Services
   - DNS Server



2. Make sure the following CA requirements are configured:
   - Cryptographic Service Provider: ECDSA_P256
   - Key length: 256

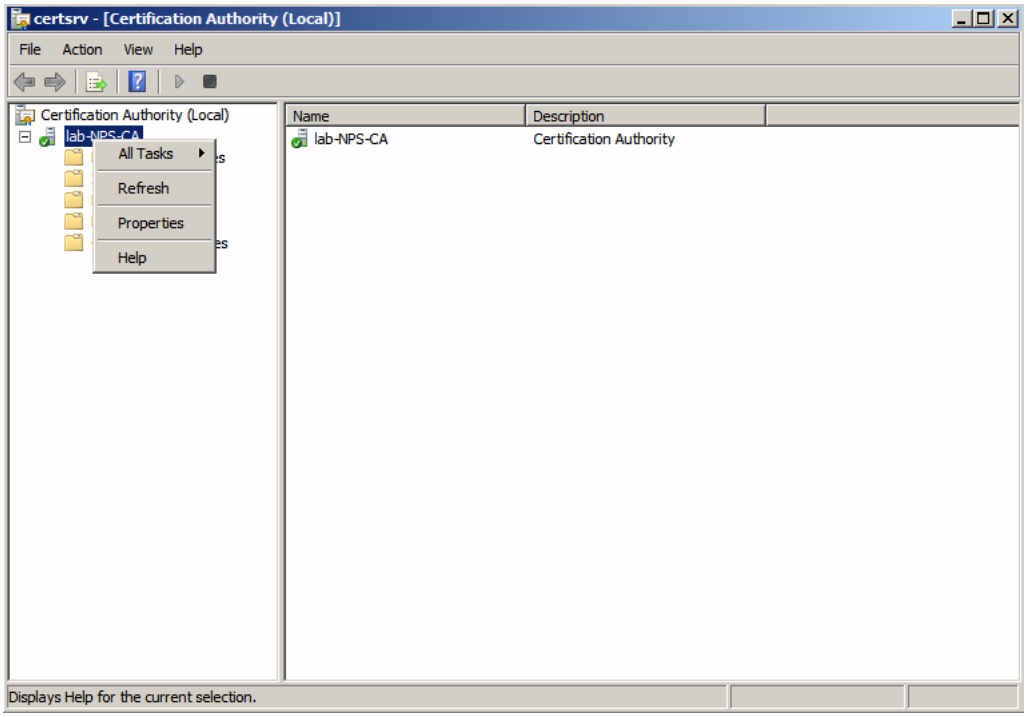
– Hash algorithm for signing certificates: SHA256



Creating and Configuring the Template for CGE on the NPS

Follow these steps to create and configure the template for CGE on the NPS:

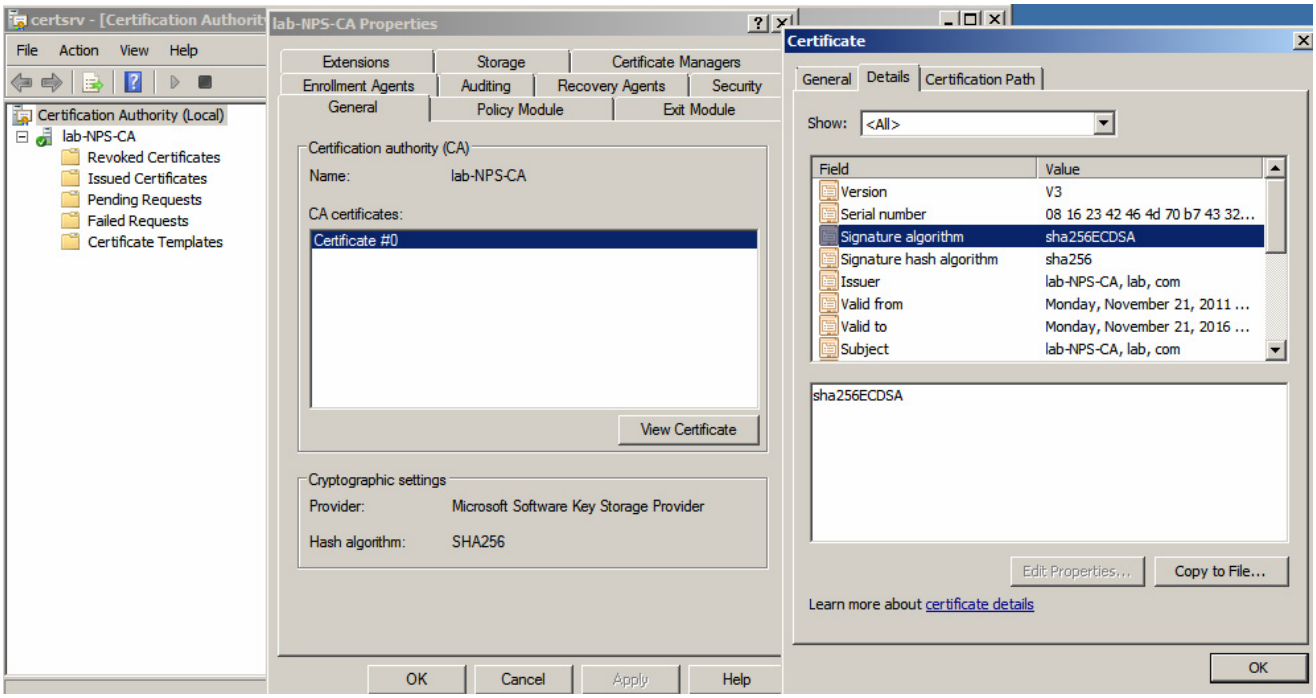
1. Launch Certification Authority from within the Administrative Tools on the CA/Sub-CA Server running the ECC algorithm. Right-click and select **Properties**.



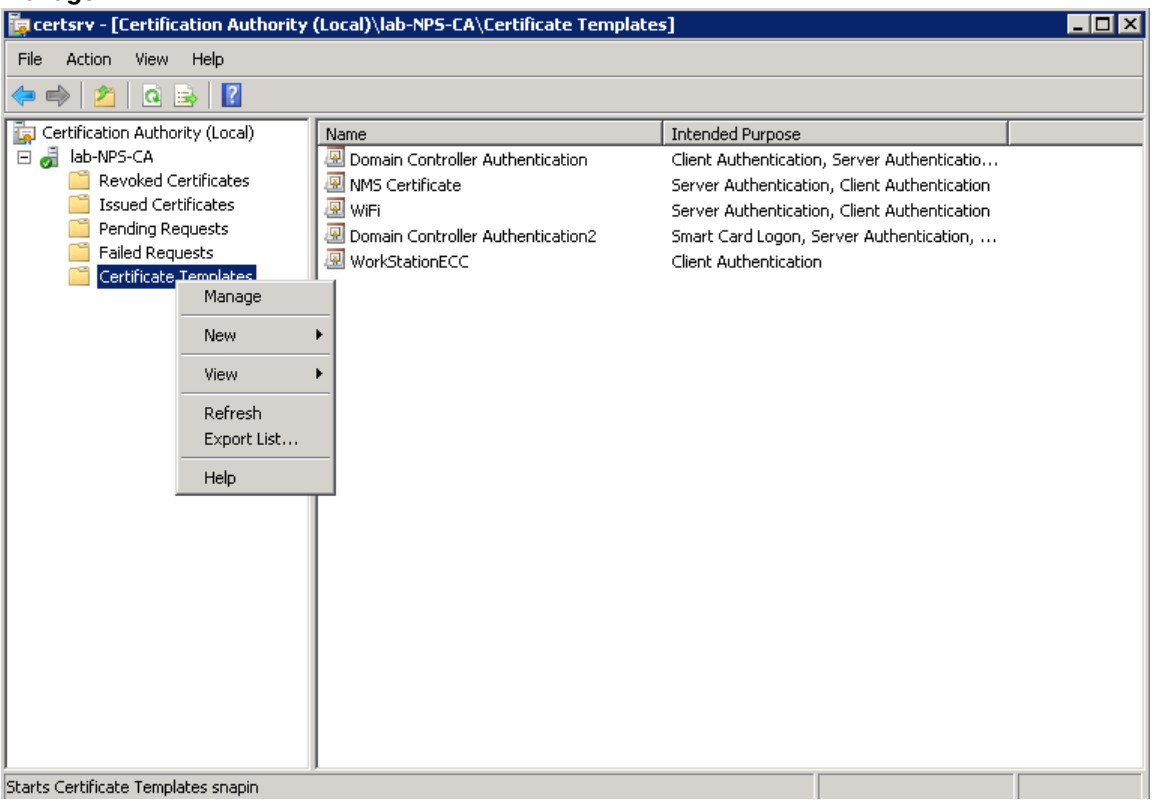
2. In the General tab:

   a. Select **View Certificate** and click the **Details** tab.

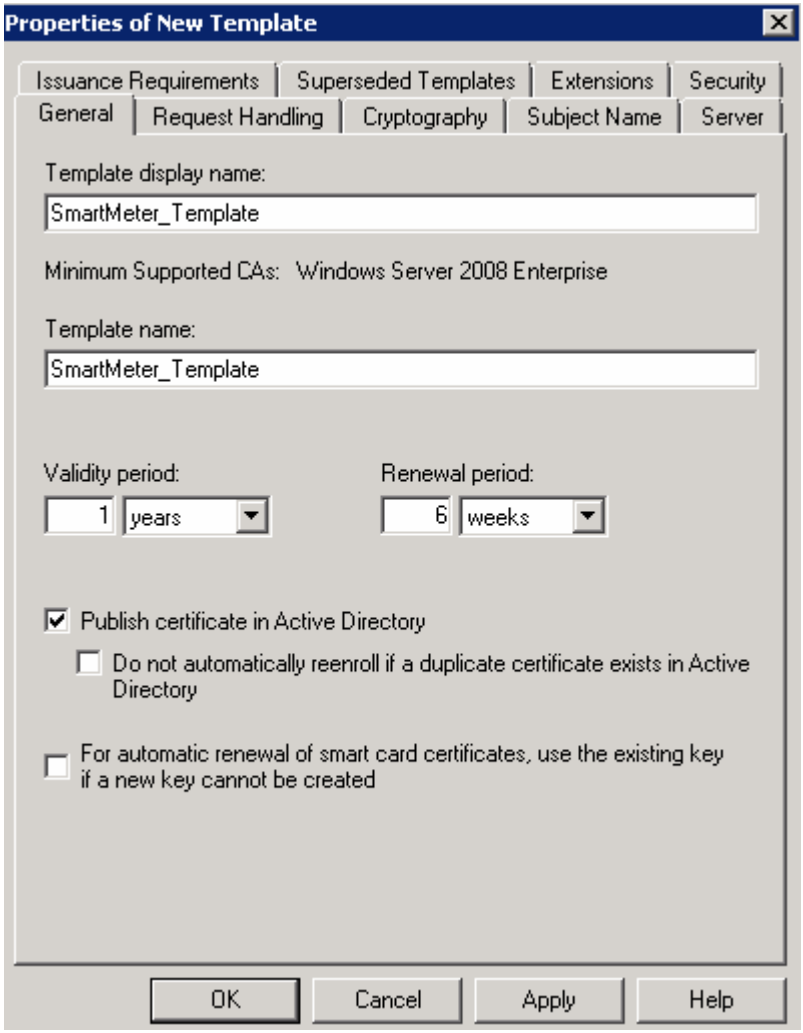
b. Scroll down and check the Signature algorithm used is SHA256ECDSA. The Public key should be ECC (256 Bits).



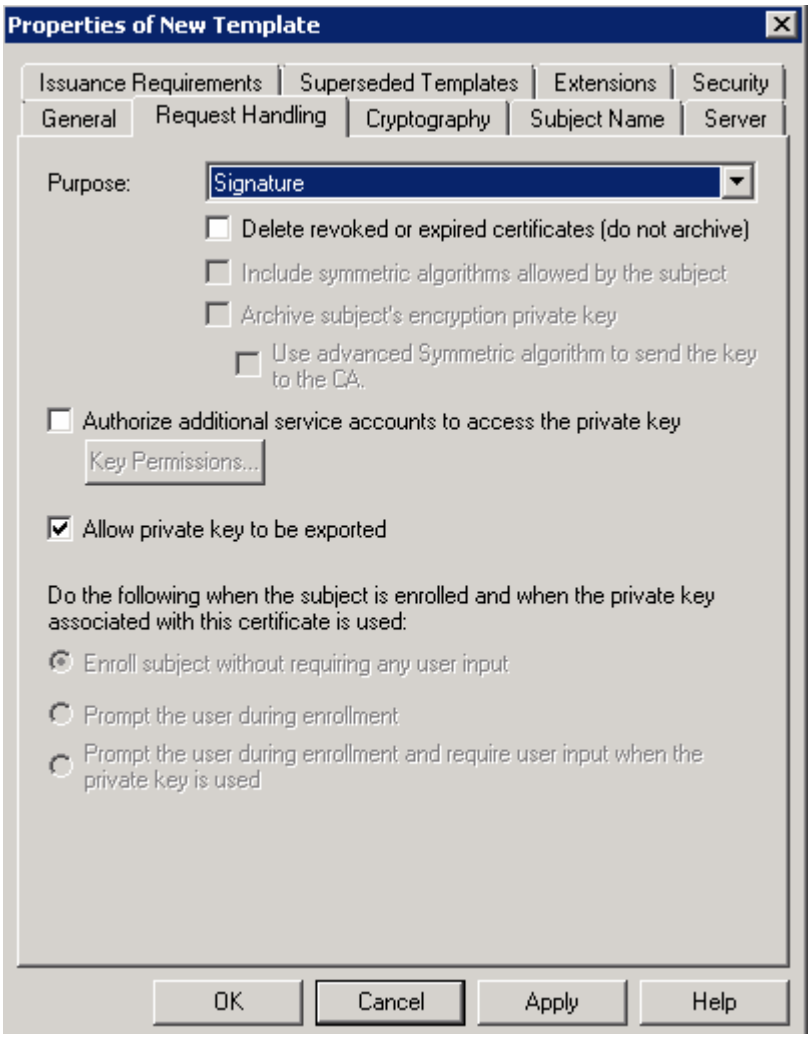
3. In the Certification Authority Console, right-click **Certificate Templates** in the left pane, right-click and select **Manage**.



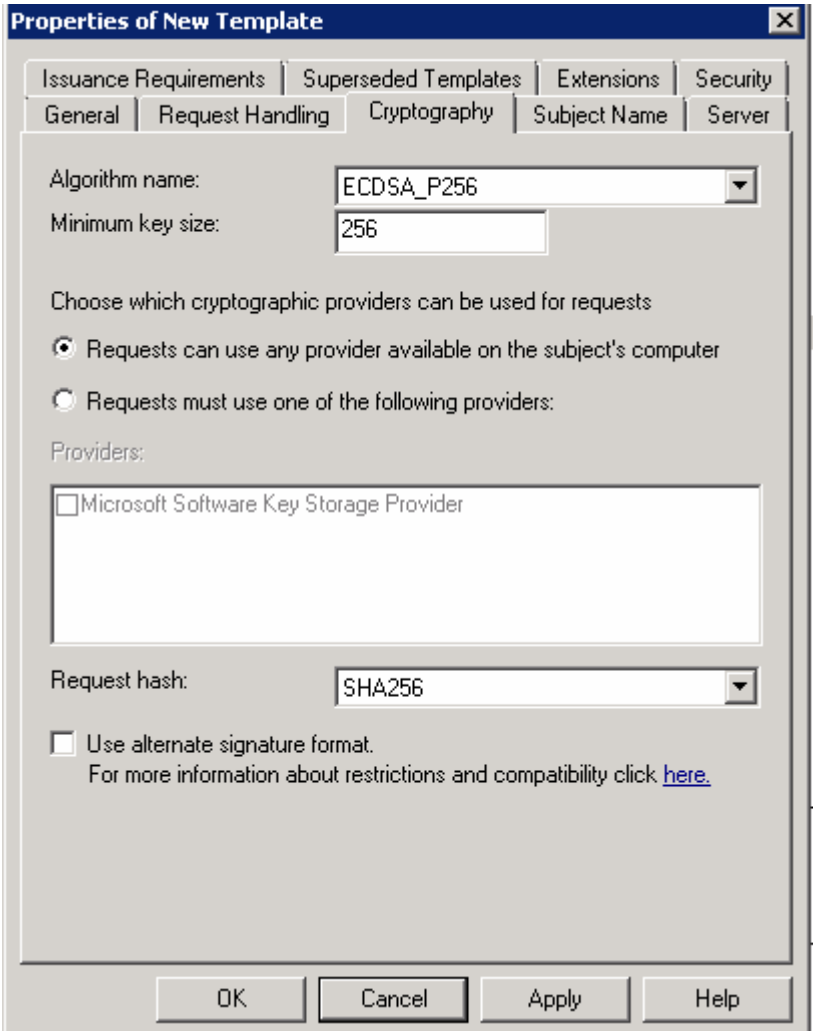
4. Select and duplicate the Computer certificate template from the Certificates Console. Select **Windows Server 2008 Enterprise for Windows**.
5. Fill in the certificate template as WorkStationEcc and select the **Publish certificate in Active Directory** check box.



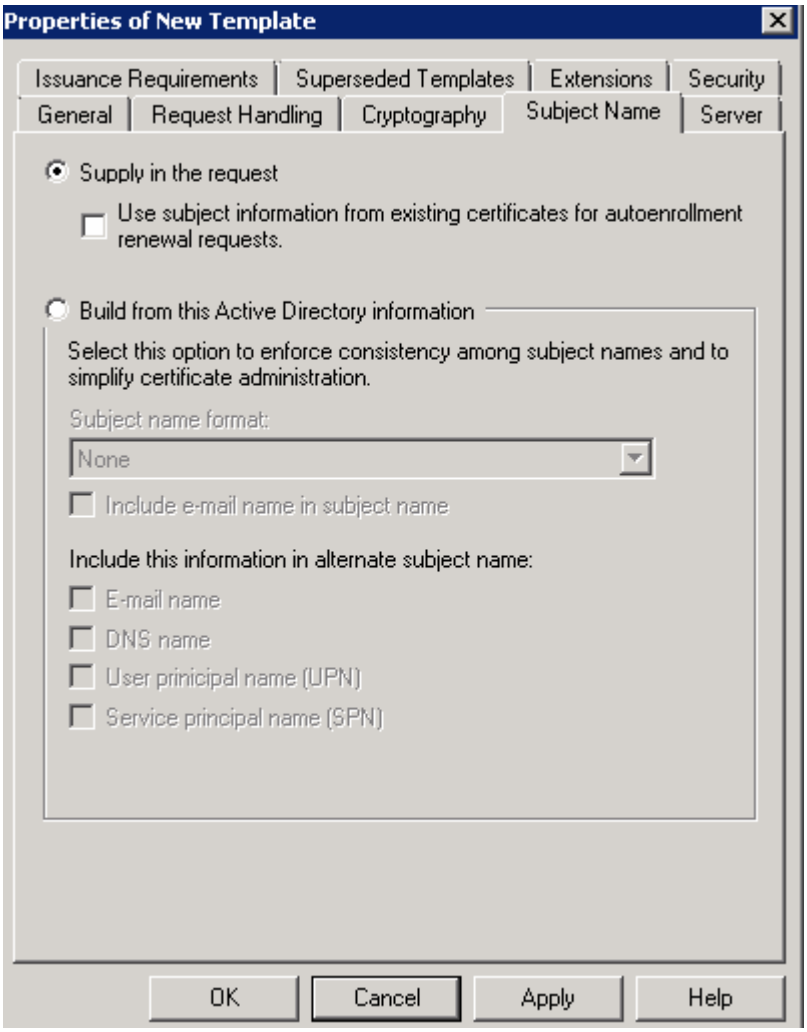
6. On the **Request Handling** tab, choose **Signature** from the **Purpose** drop-down list. Select **Yes** in the Certificate Templates warning dialog. To allow certificate private key exports in the Request Handling tab, select **Allow private key to be exported**.



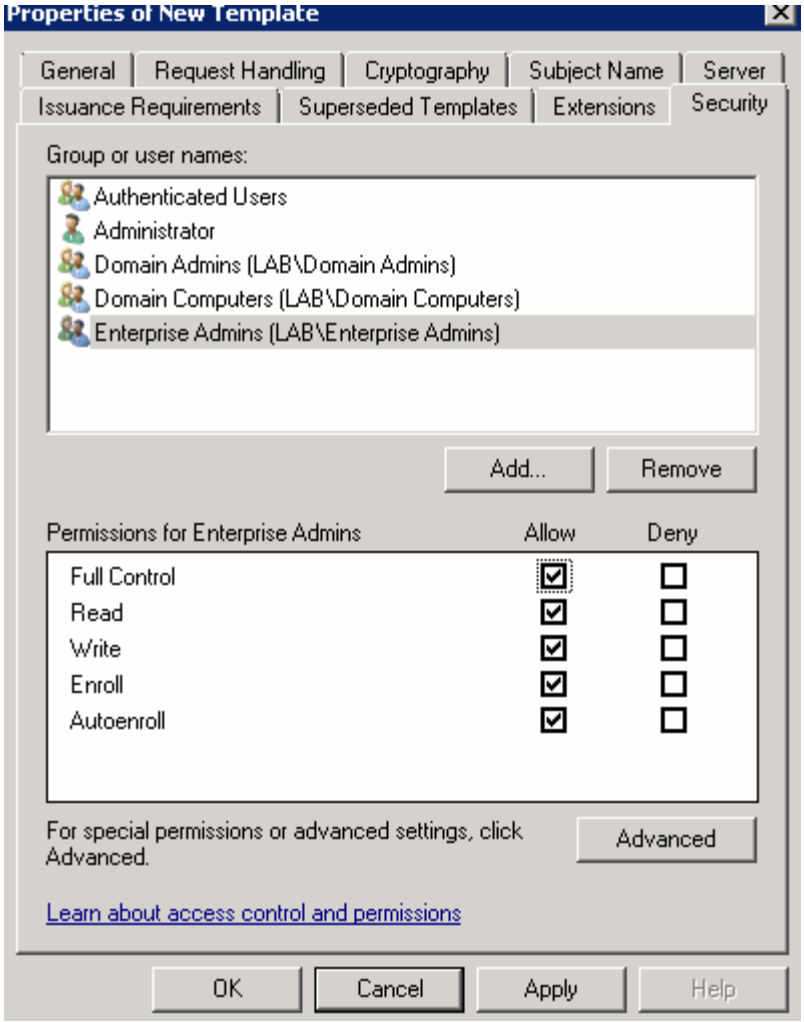
7. On the **Cryptography** tab, choose **ECDSA_P256** for the algorithm name. Enter **256** in the Minimum key size field. For the Request hash, choose **SHA256**.



8. On the **Subject Name** tab, select **Supply in the request** to enter the Subject Name and Common Name. This can be the EUI64 MAC address string of a smart meter and is used for additional user authentication against the RADIUS server.



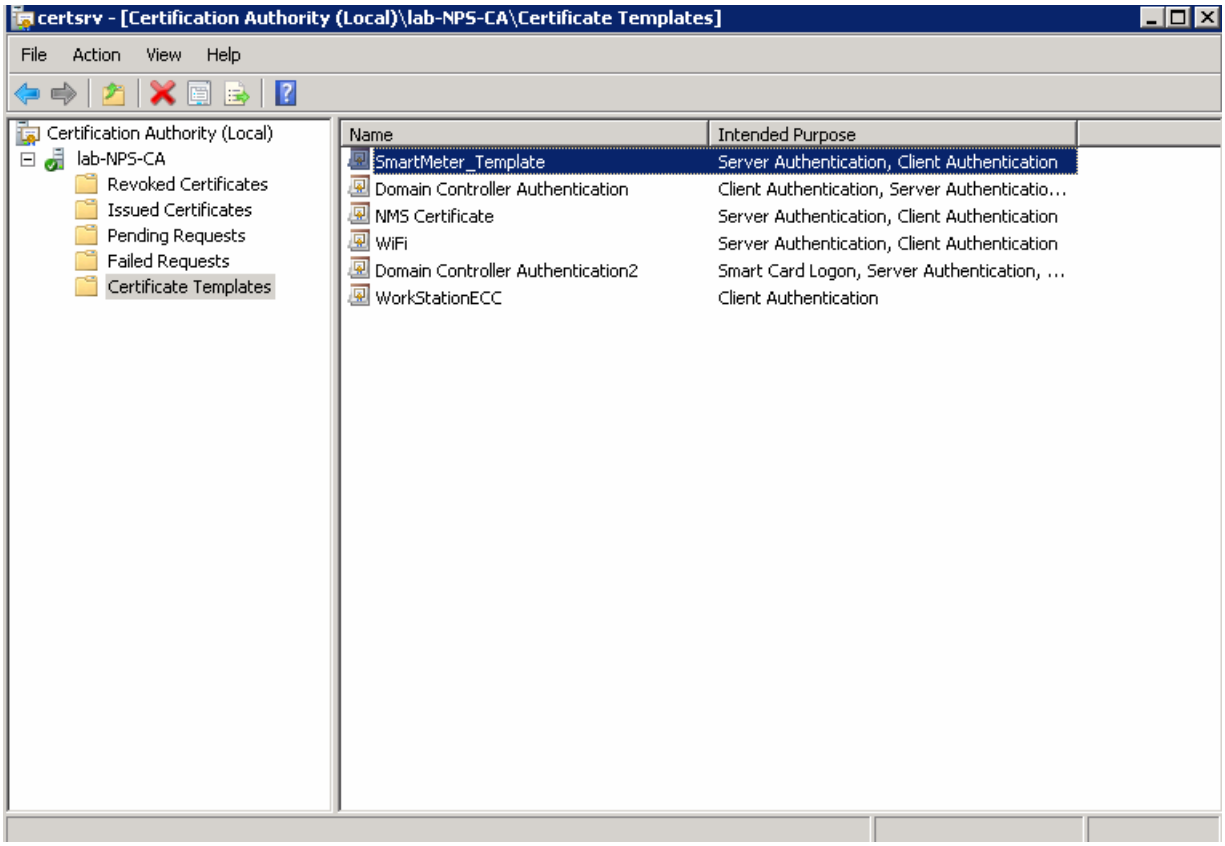
9. On the **Security** tab, for all listed group or user names, ensure that the **Enroll** and **Autoenroll** permissions are selected.



10. Close the Certificate Template Console and select the Certificate Templates folder from the Certification Authority Console.

    a. Select **New**, and then set Certificate Template to Issue.

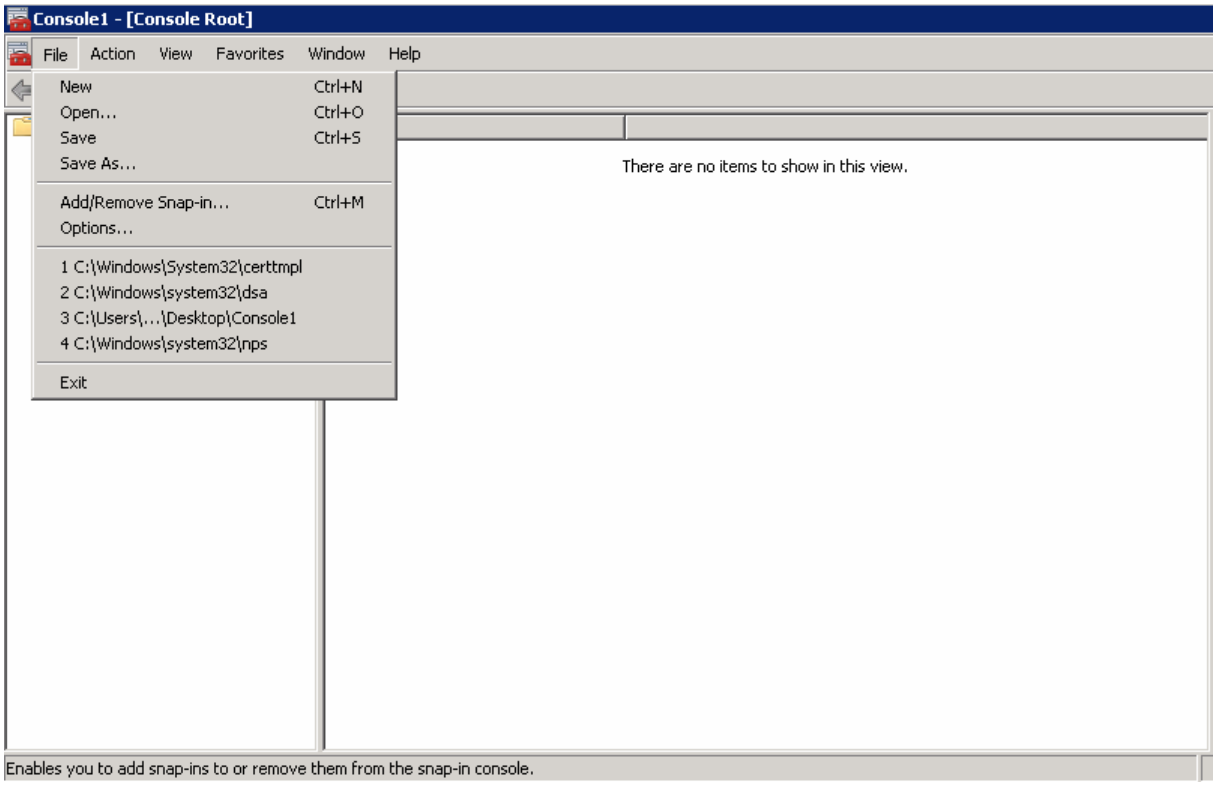
b. Select the new certificate template, WorkStationEcc, and then click **OK**. The new certificate template should be listed within the Certificate Templates folder of the Certification Authority Console.



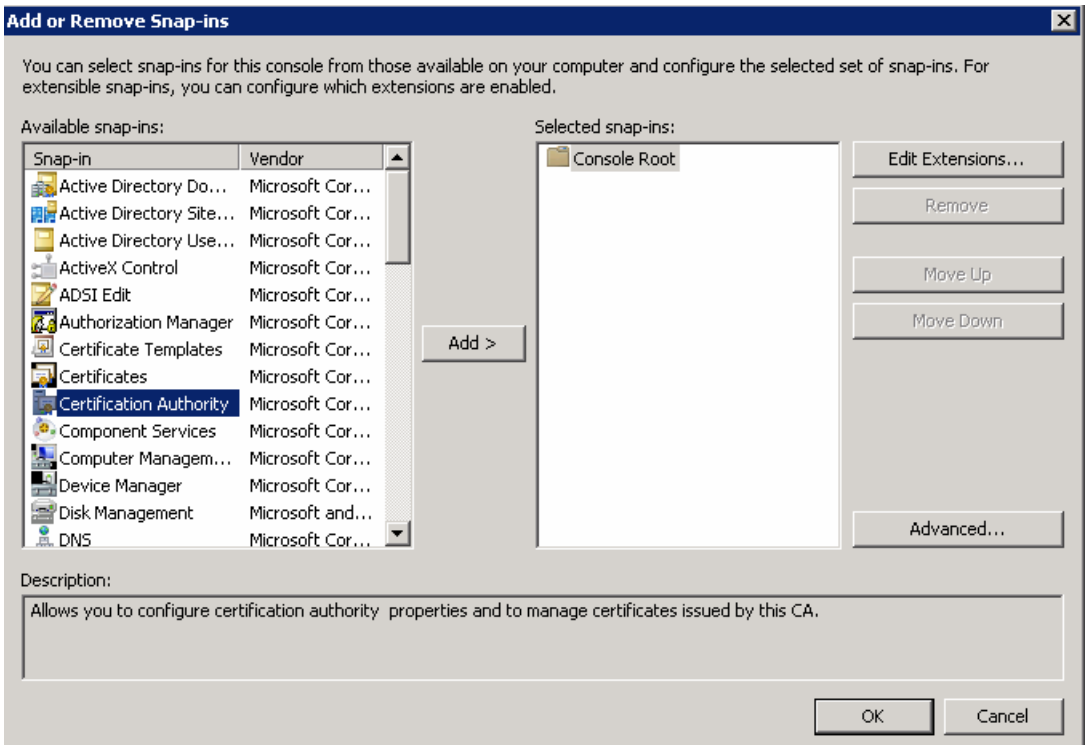
Generating the CGE Certificates

The following steps guide the administrator of the NPS servers to generate a certificate from the CA using the template that was created above (WorkStationEcc).

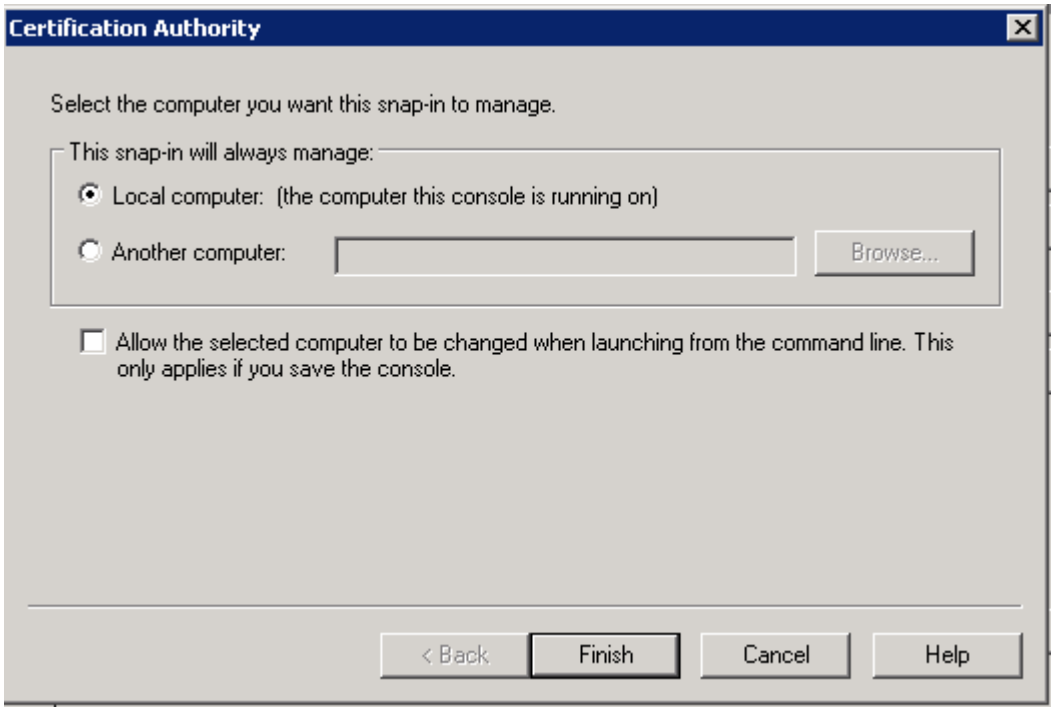
1. Open the MMC (Microsoft Management Console) application on Windows Server 2008 R2 (Run -> mmc) and make sure that the Local Computer Certificates Snap-In is loaded. But for the first configuration for MMC, you can click **File** and **Add/Remove Snap-in...** and a popup window displays.



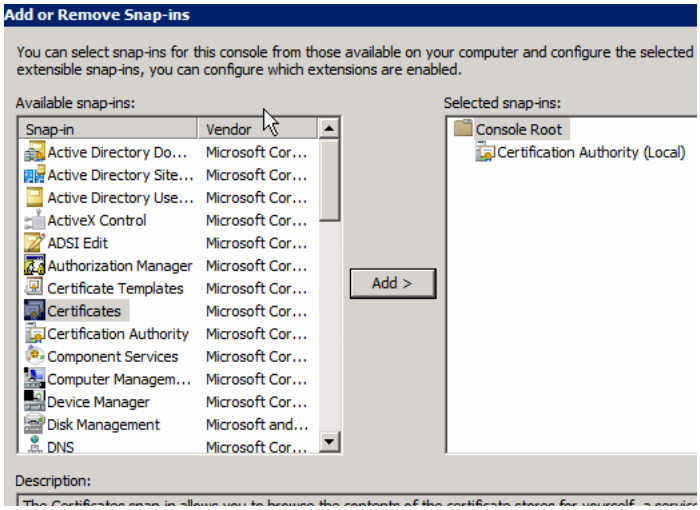
Select **Certificate Authority** in the left pane and click **Add >**. Click **OK**.



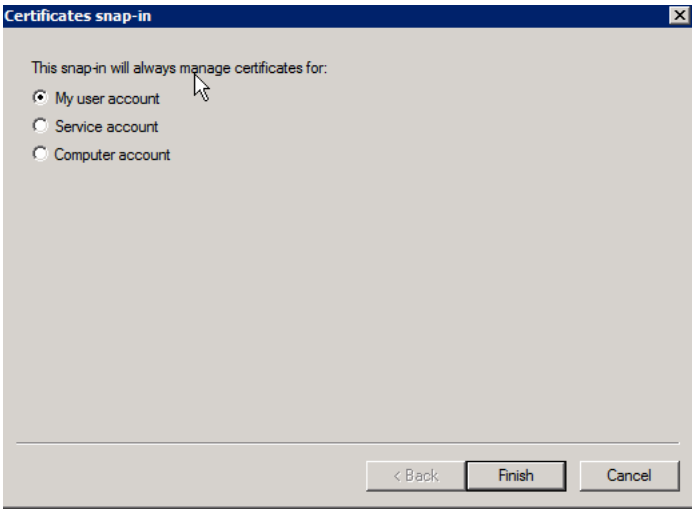
Select **Local Computer** and click **Finish**.



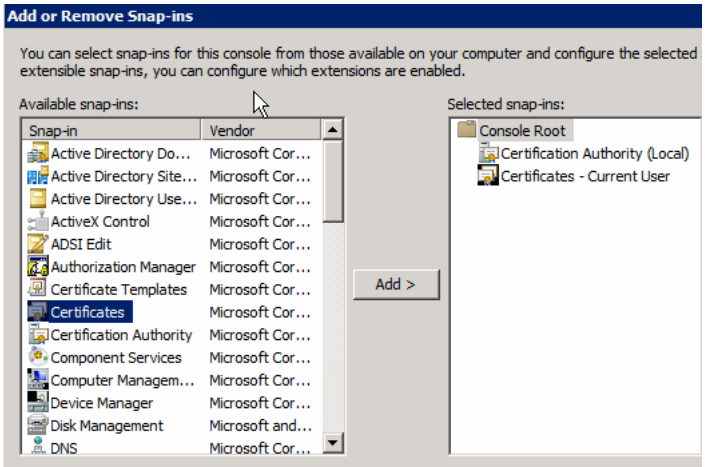
In the Add or Remove Snap-ins window, select **Certificates** in the left pane and click **Add >**. Click **OK**.



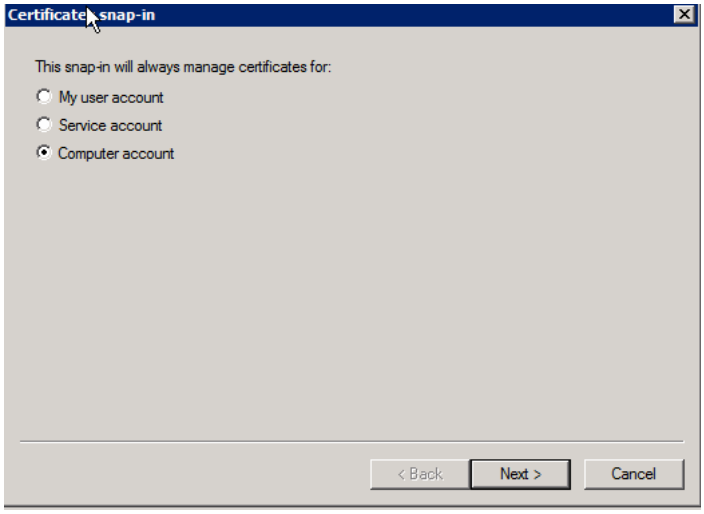
Select **My user account** and click **Finish**.



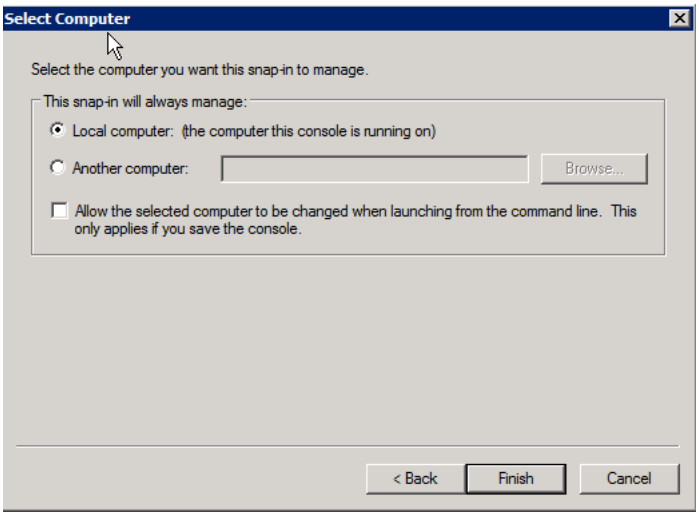
In the Add or Remove Snap-ins window, select **Certificates** in the left pane and click **Add >**. Click **OK**.



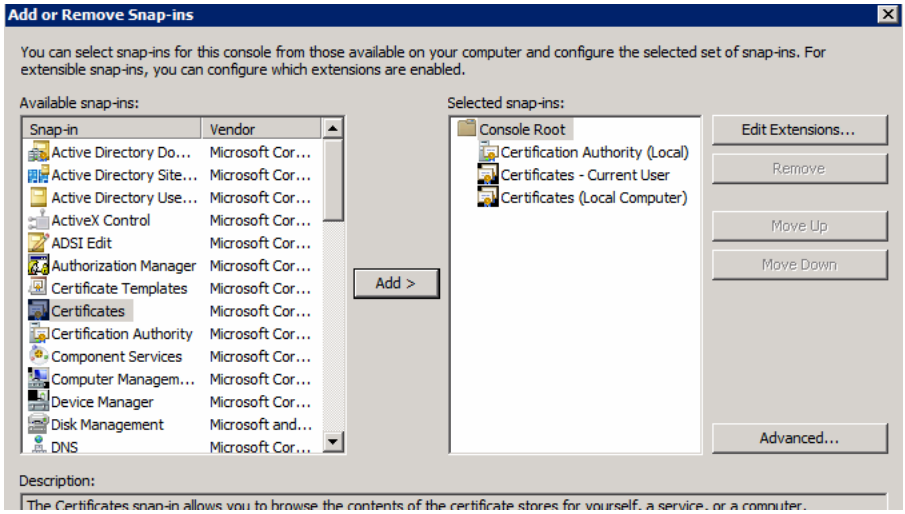
Select **Computer account** and click **Next**.

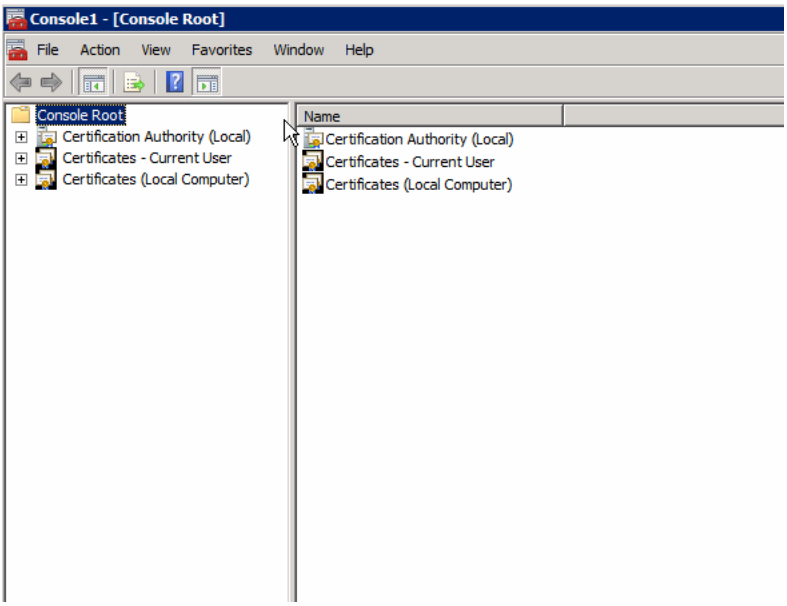


Select **Local Computer** and click **Finish**.

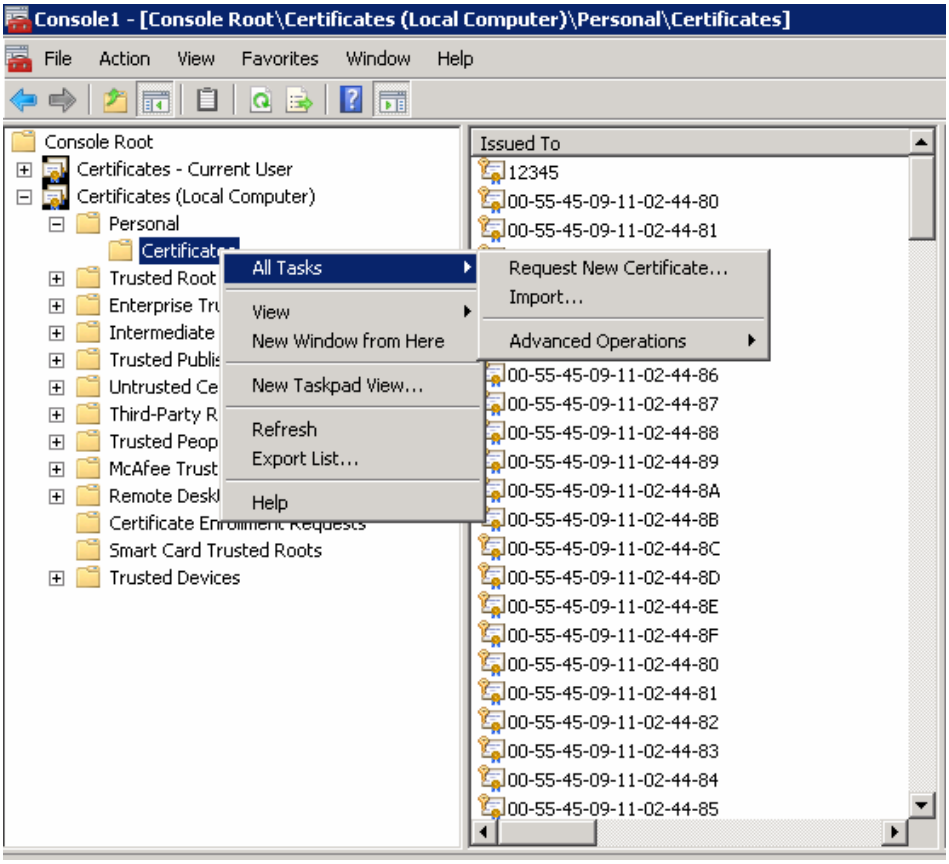


The items are added in the right pane. Click **OK**.

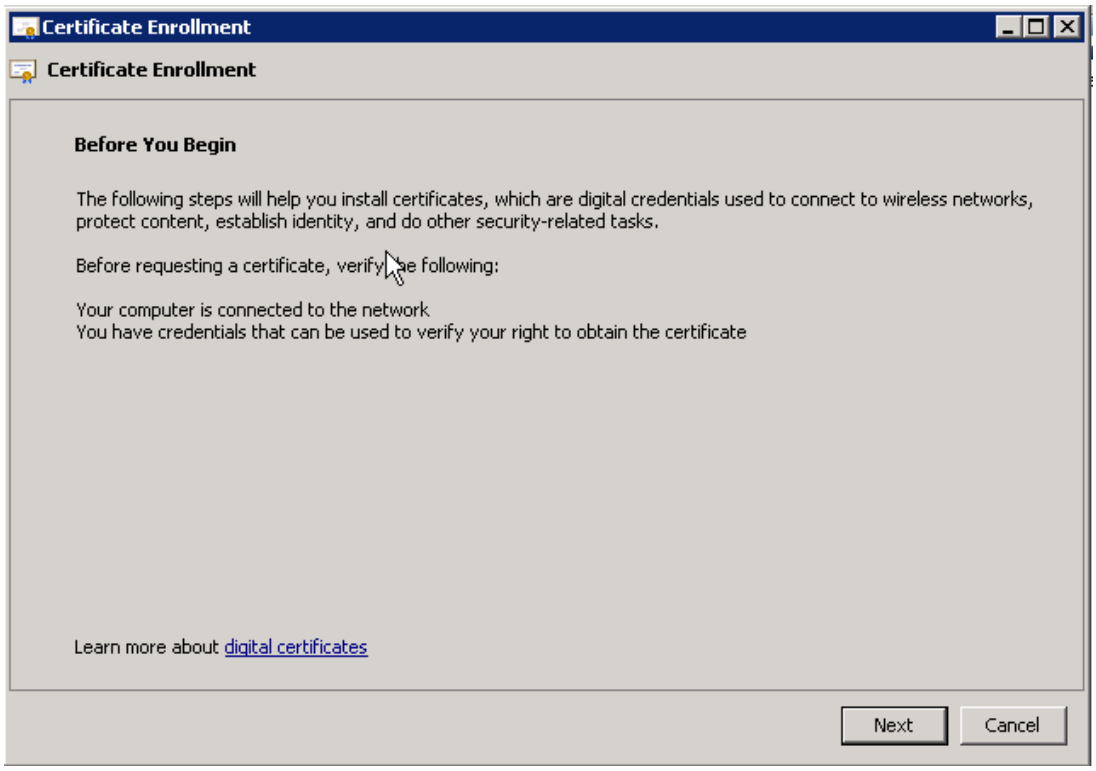




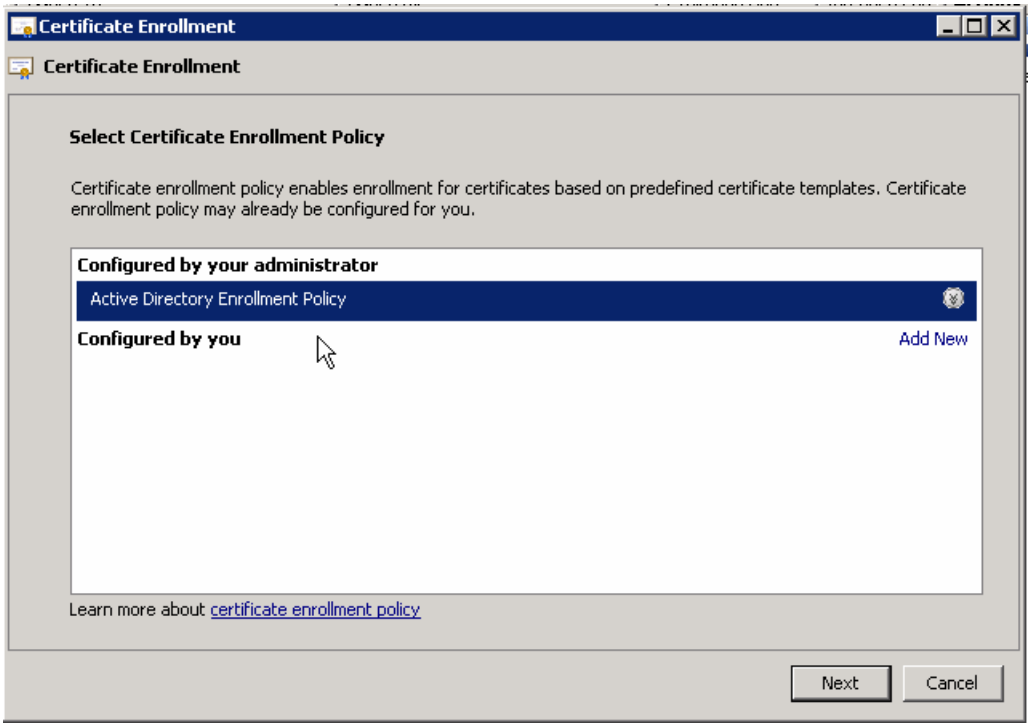
2. Go to Personal -> Certificates -> All Tasks -> Request New Certificate.



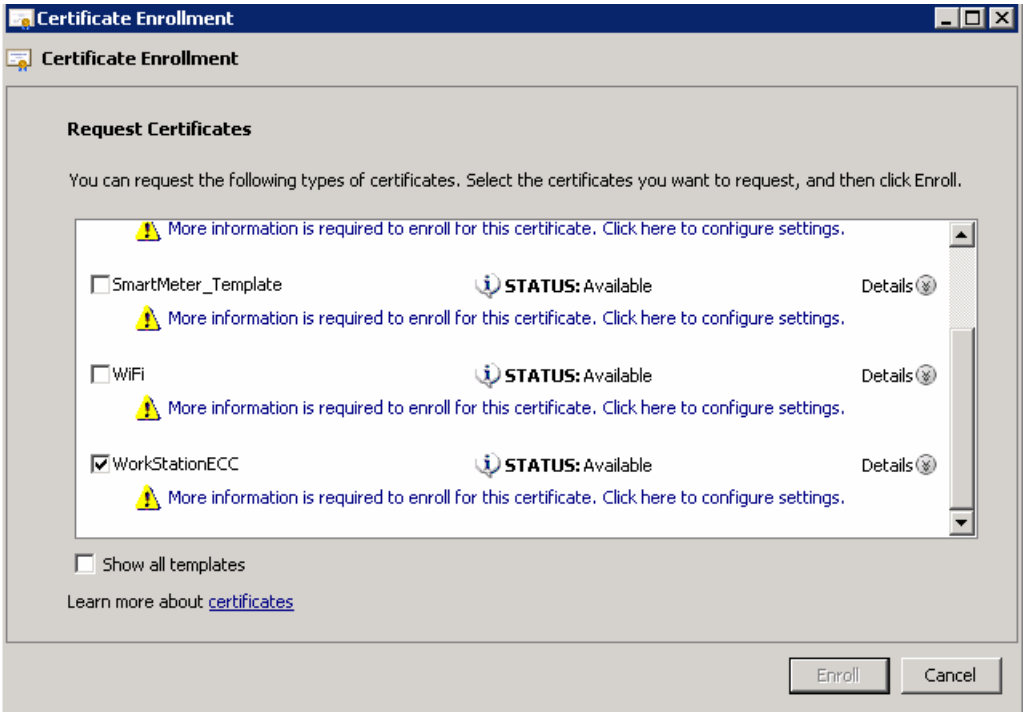
3. Click **Next**.



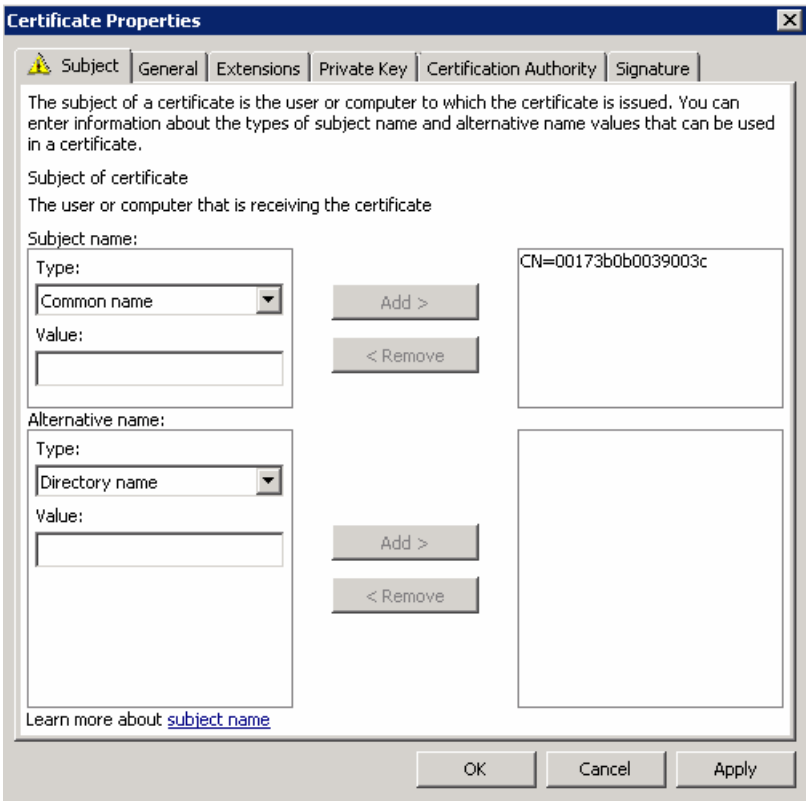
4. Select **Active Directory Enrollment Policy** and click **Next**.



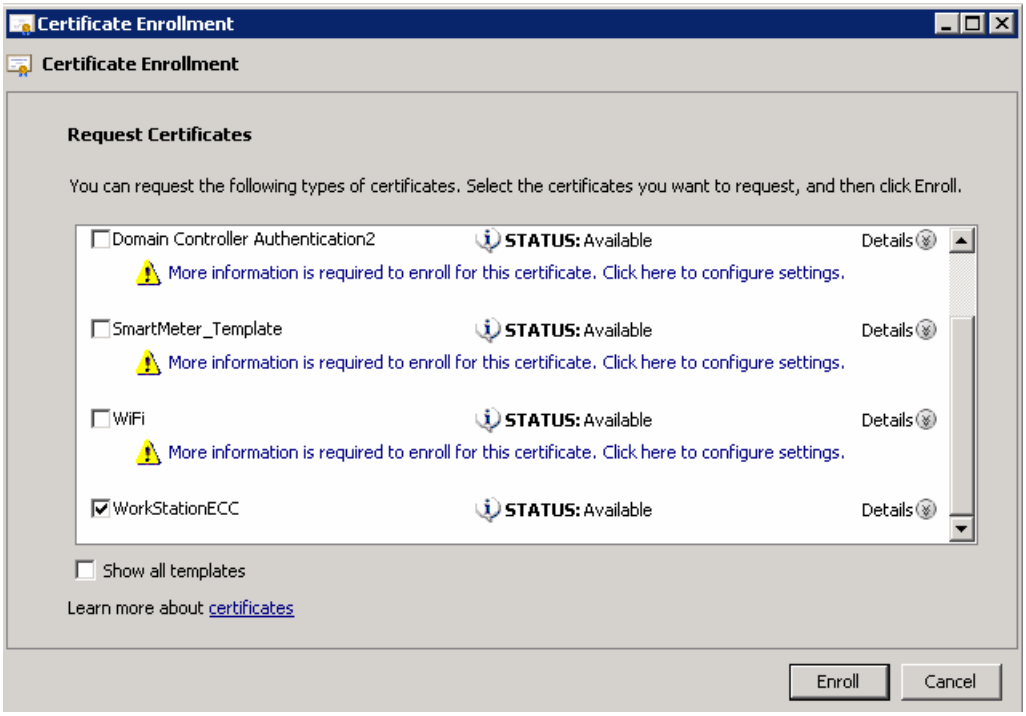
5. Select **WorkStationEcc** and click on the more information link below it.



6. In the **Subject** tab, choose **Common name** from the **Type** drop-down list. After filling in EUI, click **Add >**, and then click **OK**.



7. Click **Enroll** and click **Finish** when enroll is completed.



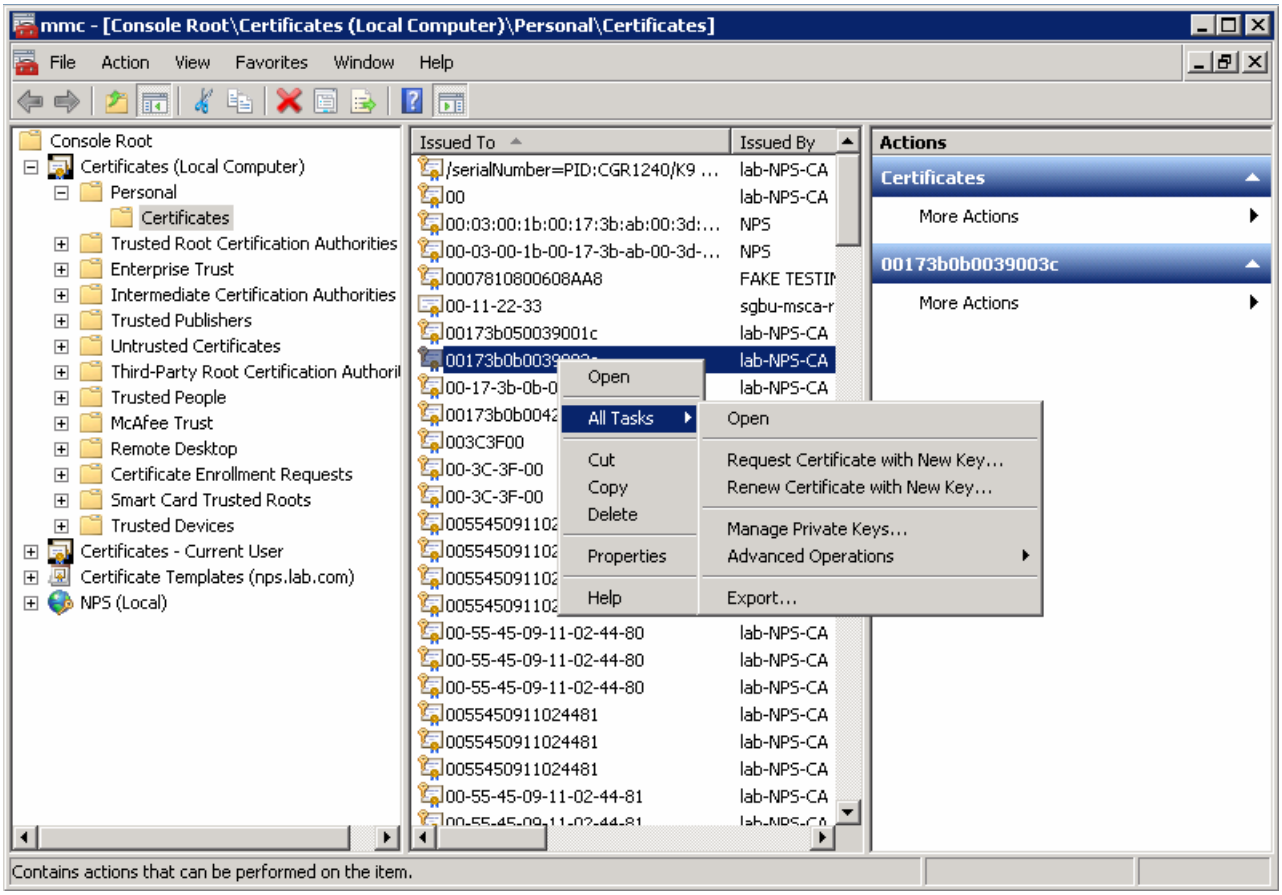
Exporting CG Mesh Node Certificates

There are two certificates that need to be exported. One certificate is with the private key and public key. The other is with the public key only. The one with private key will be programmed into meter. The public key will be added to Active Directory.

This section includes the following topics:

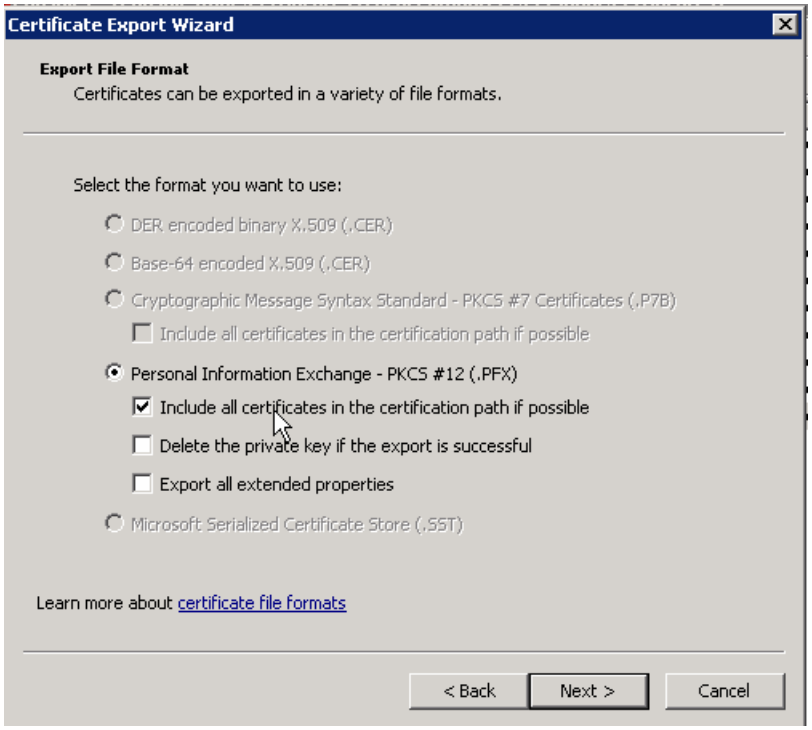
Exporting Certificate with Private Key

1. Return to the MMC application and highlight the newly created certificate (00173b0b0039003c). Right click and select **All Tasks** > **Export**.

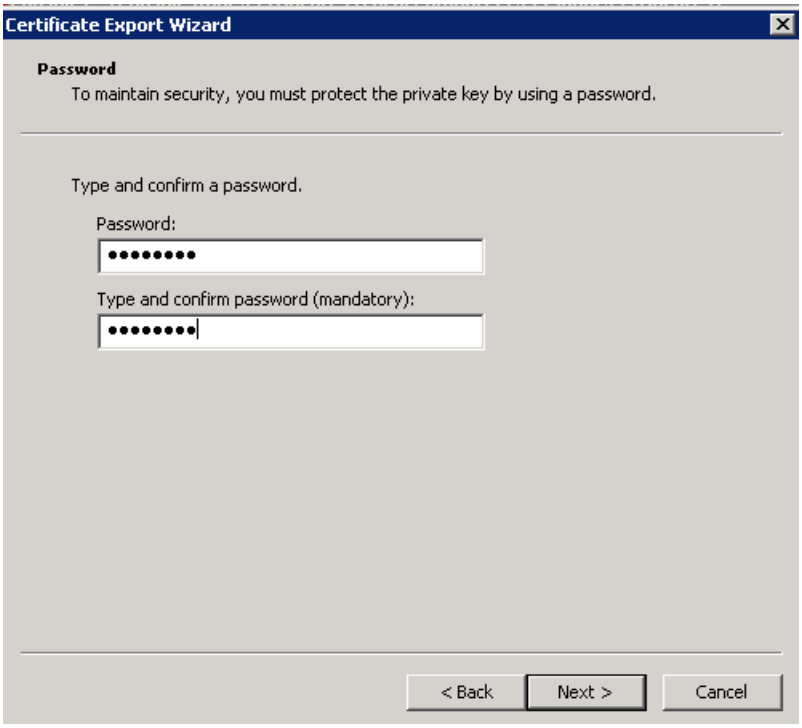


2. Follow the export wizard to the next screen. Select **Yes, export the private key**.

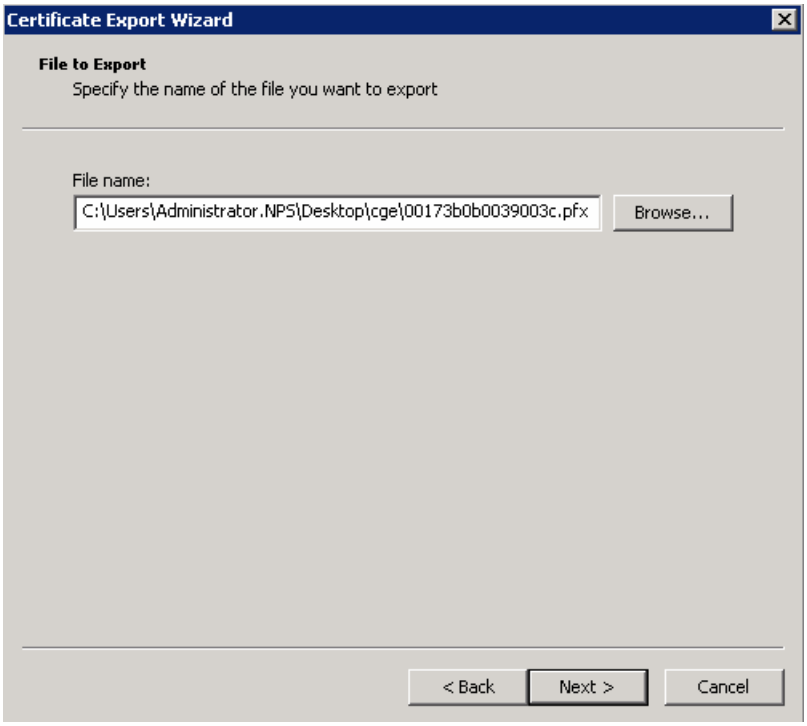
3. Select **Include all certificates in the certification path if possible**. This includes the CA certificate.



4. Enter password for certificate which will be used in CGE. For default settings, use the password **Cisco123**.



5. Save the .pfx file.

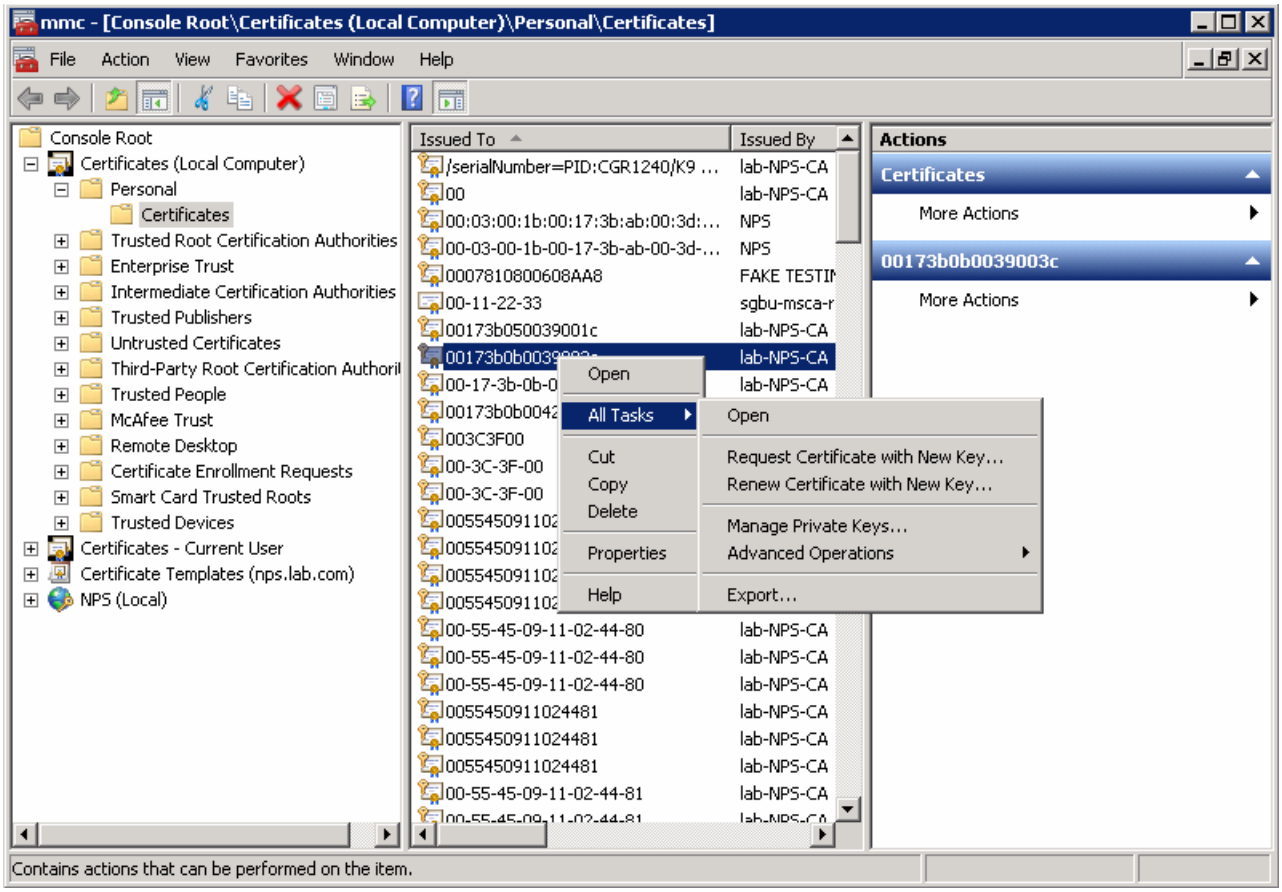


6. Securely transfer the .pfx file from the Desktop to the FND server.

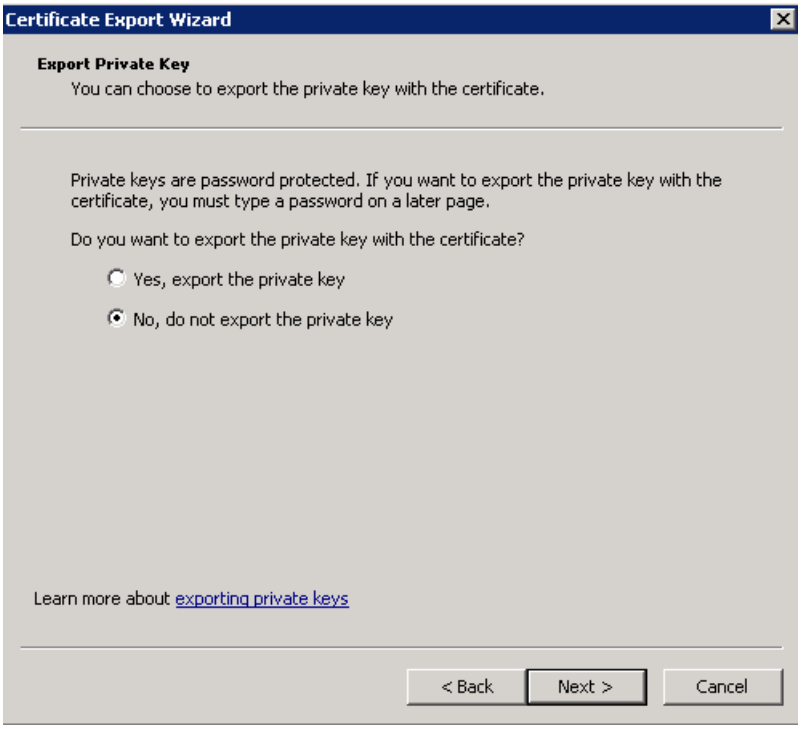
7. For security reasons, it is highly recommended that you delete the .pfx file from the Desktop and empty the Recycle Bin on Windows.

Exporting Certificate with Public Key

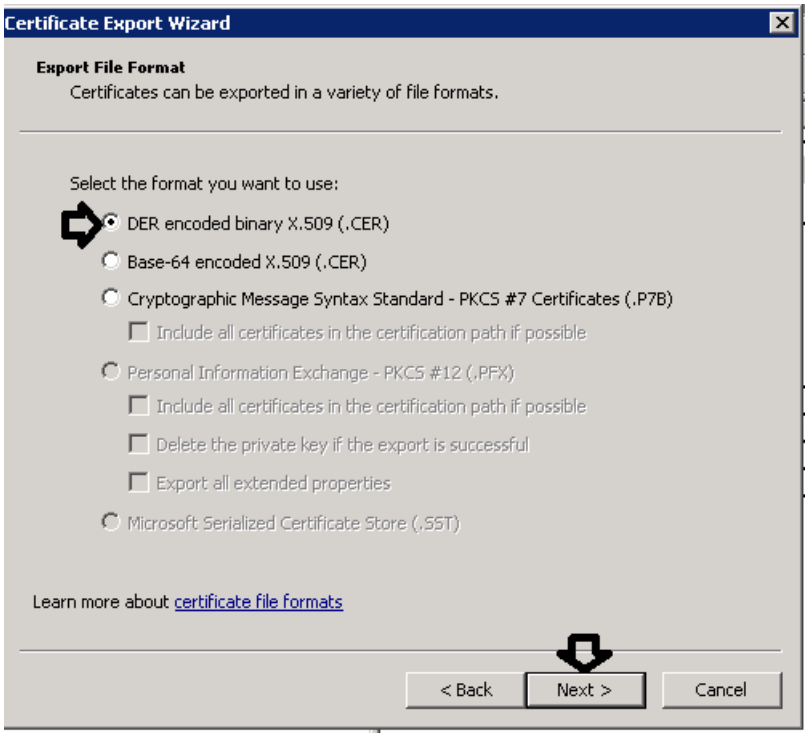
1. Return to the MMC application and highlight the newly created certificate (00173b0b0039003c). Right click and select **All Tasks** > **Export**.



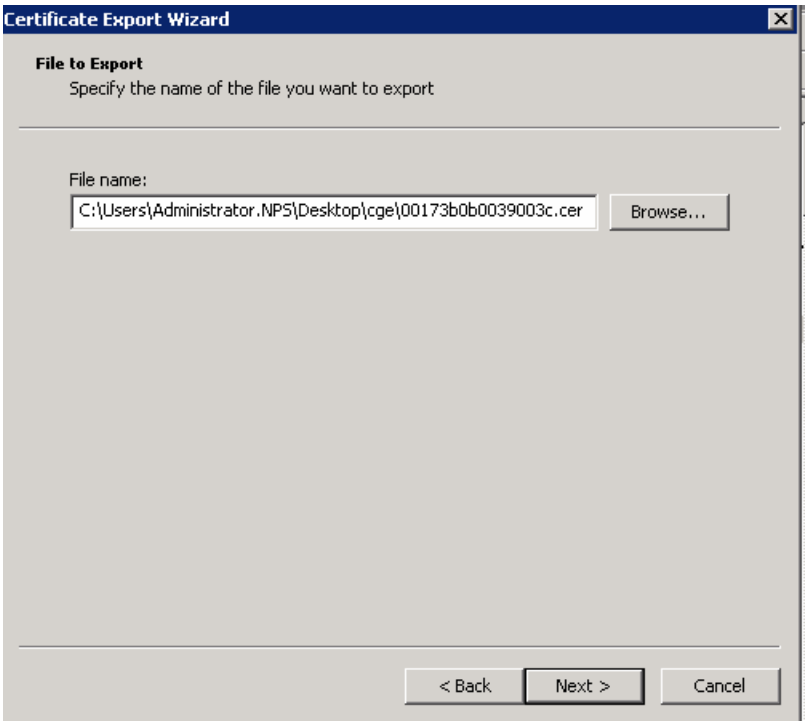
2. Follow the export wizard to the next screen. Select **No, do not export the private key**.



3. Select export file format **DER encoded binary X.509 (.CER)**. Click **Next >**.

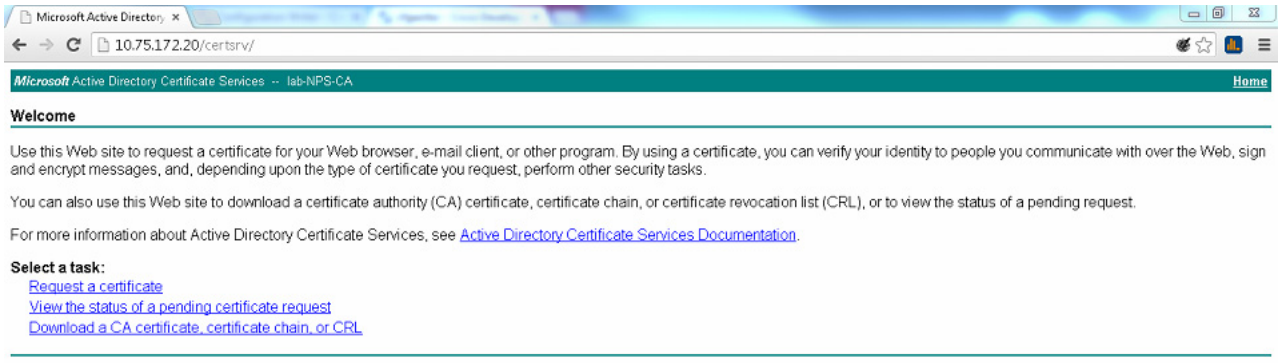


4. Save the .cer file.

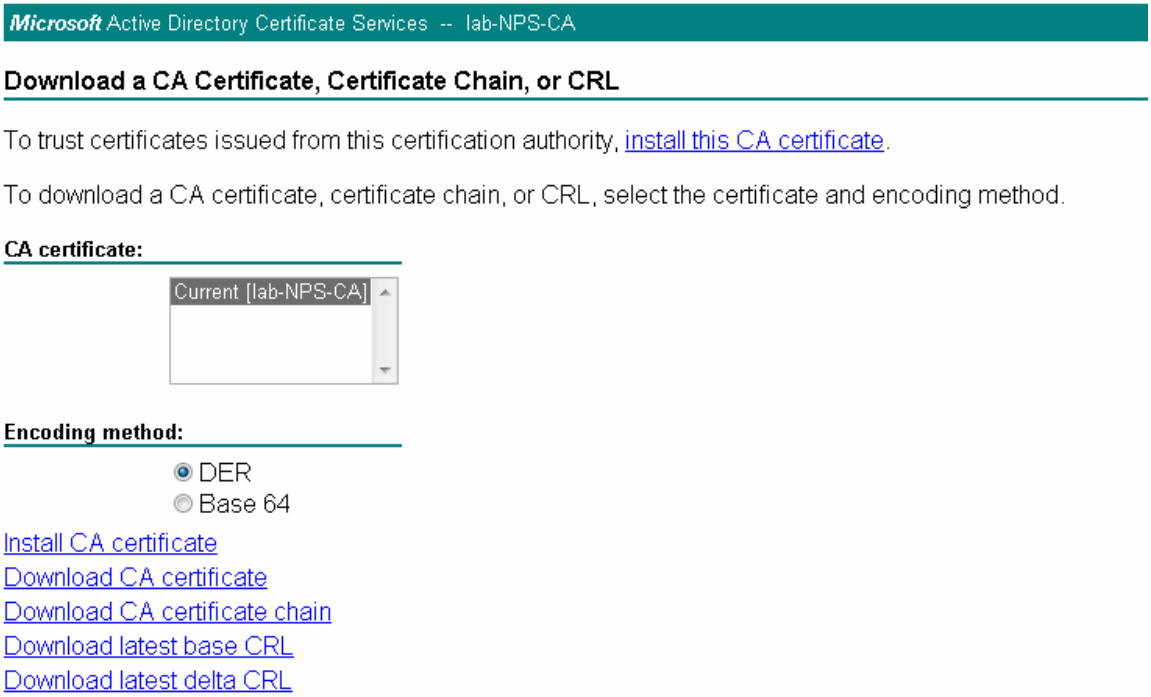


Exporting CA Server Certificate

1. Open the link on the NPS server and click the link of Download a CA certificate, certificate chain, or CRL.



2. Click the link of Download CA certificate, and choose **DER format**.



Installing Industrial Operations Kit on the Server

The Windows 7 installer includes all necessary scripts and dependent libraries to create the various VMware machines for the various systems noted in Figure 2 on page 4 on the server (ESXi host).

BEFORE YOU BEGIN

Ensure that all Prerequisites are met.

Before you install the Industrial Operations Kit (IOK) software bundle, **you must** disconnect the server from the VMware vCenter server application, if in use within your network. You can reconnect to this application when the software installation completes.

Get the IOK software bundle to a Windows 7 PC, and unzip it.

There are two ways to install the software on the server. If you do not need to configure mesh node, there is no need to configure ECC certificates. If you want to configure IOK with ECC certificate, use the **`cisco_iok_config.exe`** tool; otherwise, modify the configuration xml (configuration template) manually and then run the **`cisco_iok_installer.exe`**. The detailed steps are described in the following sections:

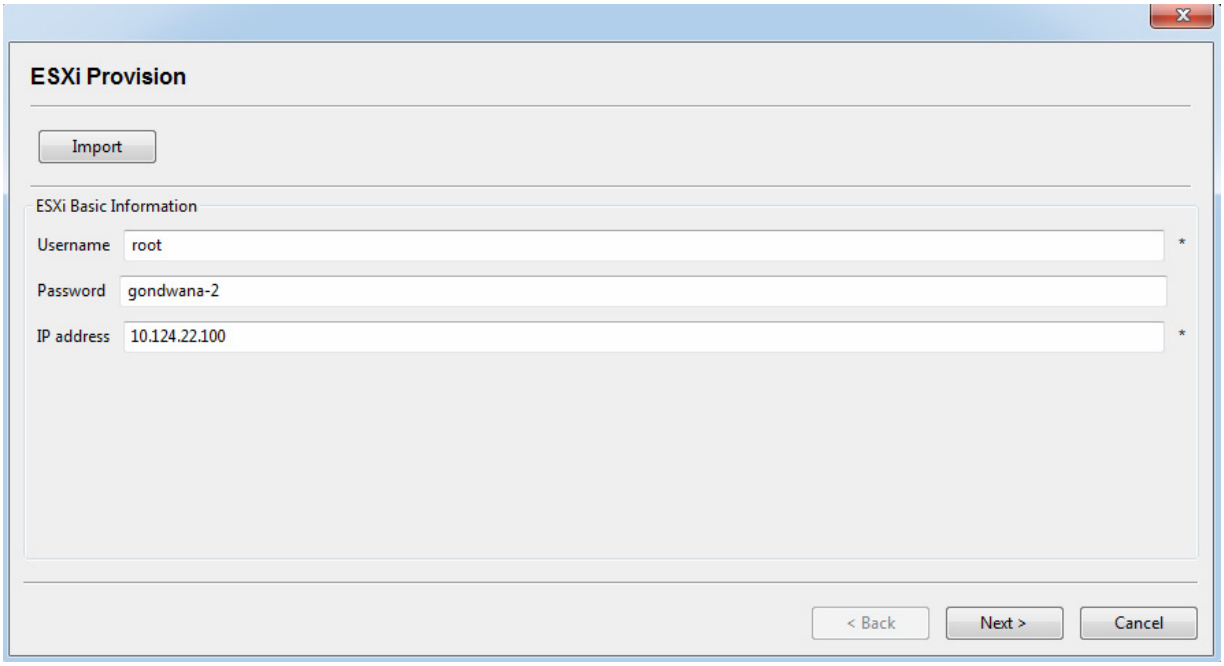
- Installing With the cisco_iok_config.exe Tool, page 40
- Installing by Using the Configuration Template File, page 47

Note: After the installation completes, we recommend that you not change the settings of the VM configuration.

Installing With the cisco_iok_config.exe Tool

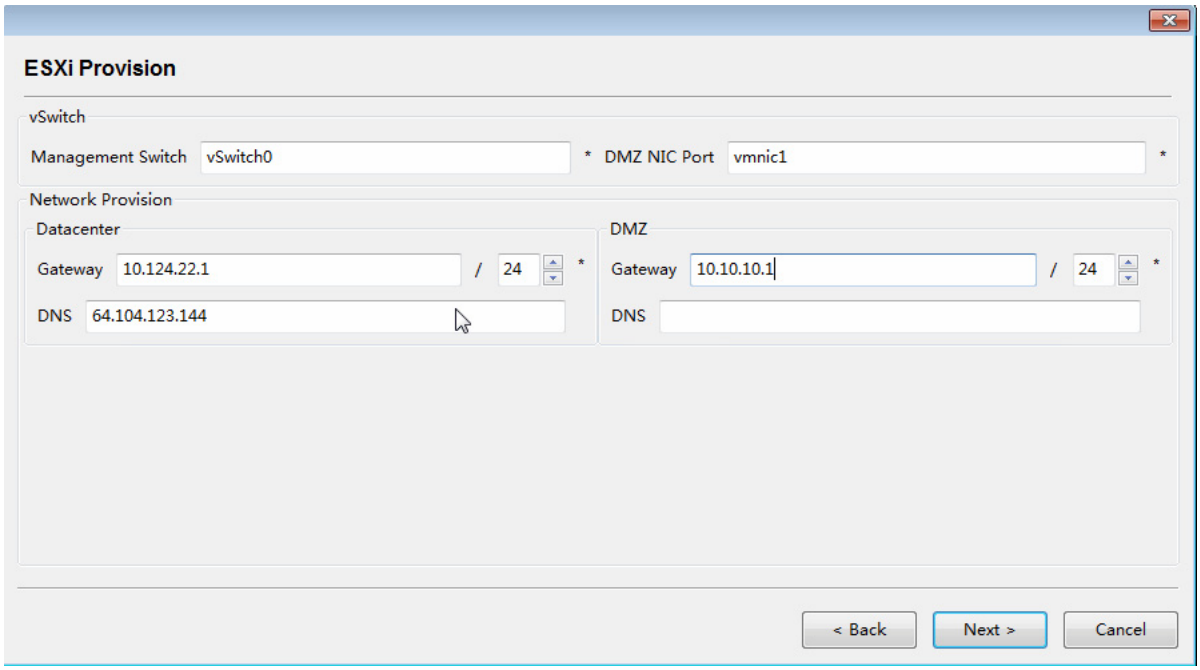
This section provides the procedures of using **`cisco_iok_config.exe`** to generate a new configuration template file and install the IOK software on the server.

1. Double-click the **`cisco_iok_config.exe`** file located at `/path/to/unziped softerware bundle/`. The ESXi Provision window displays.
2. Enter basic ESXi information (Username, Password, and IP address) and click **Next >**.

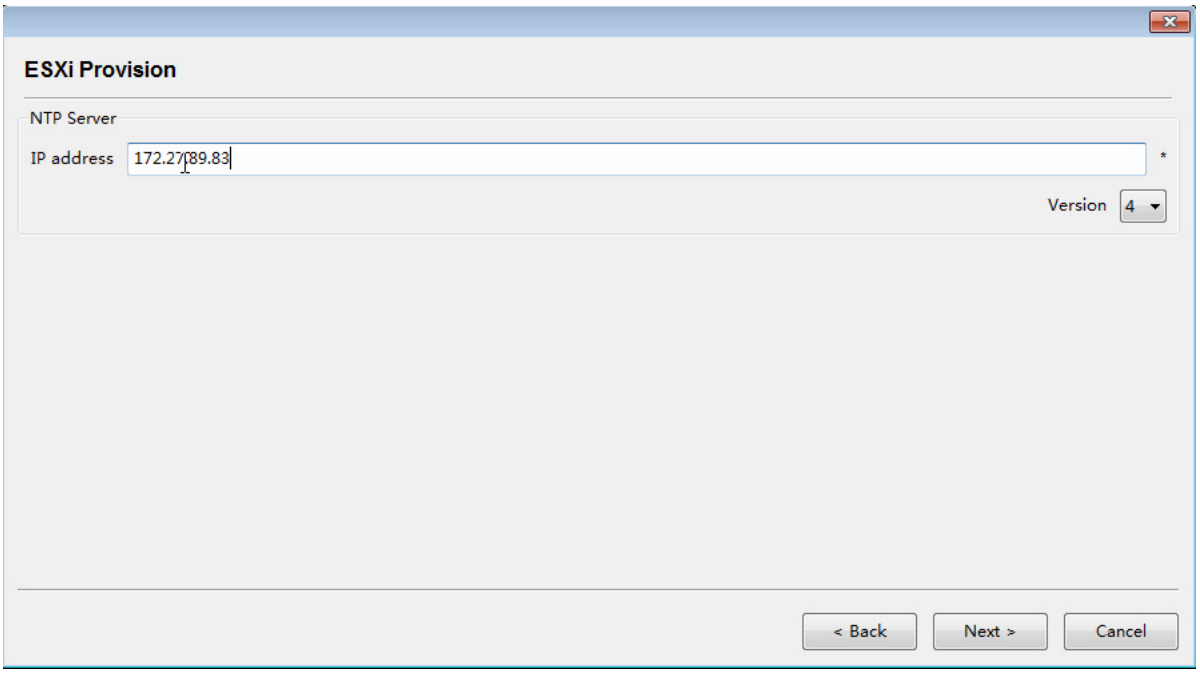


Note: If you have already configured a **`cisco_iok_installer.xml`** file, you can import the settings of this file to the **`cisco_iok_config.exe`** tool by clicking **Import** on the screen. After that, click **Next >** on each screen and you can change the existing values or input new values for the fields.

3. Enter the ESXi provisioning information and then click **Next >**.

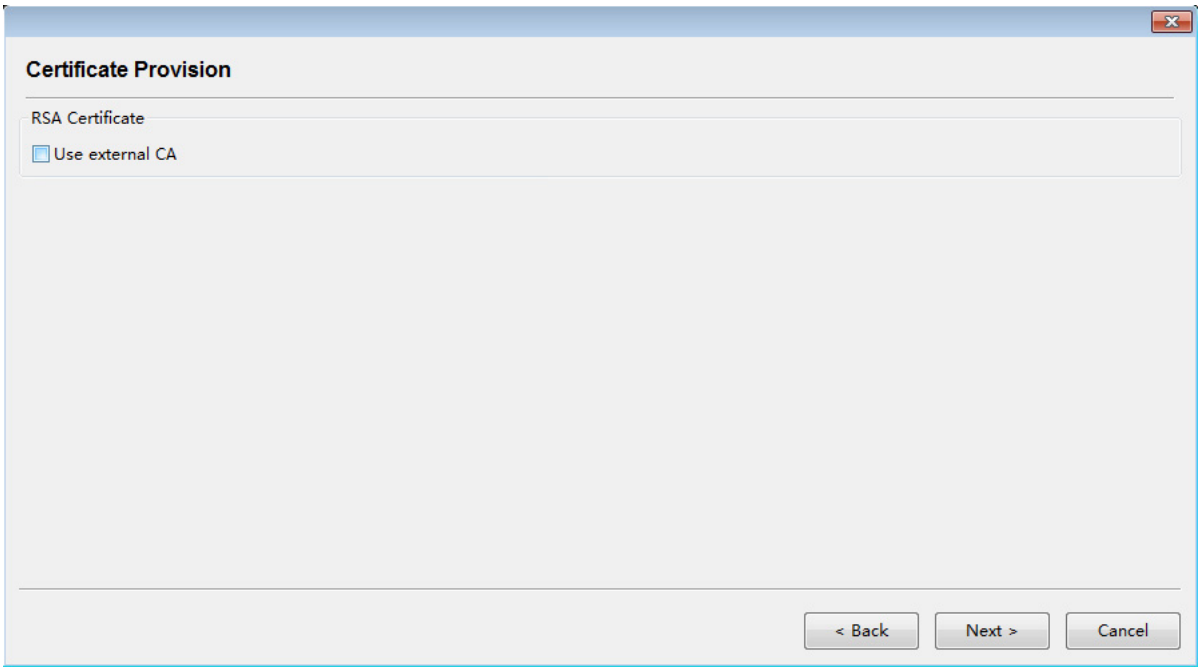


4. Enter the NTP server information and click **Next >**.

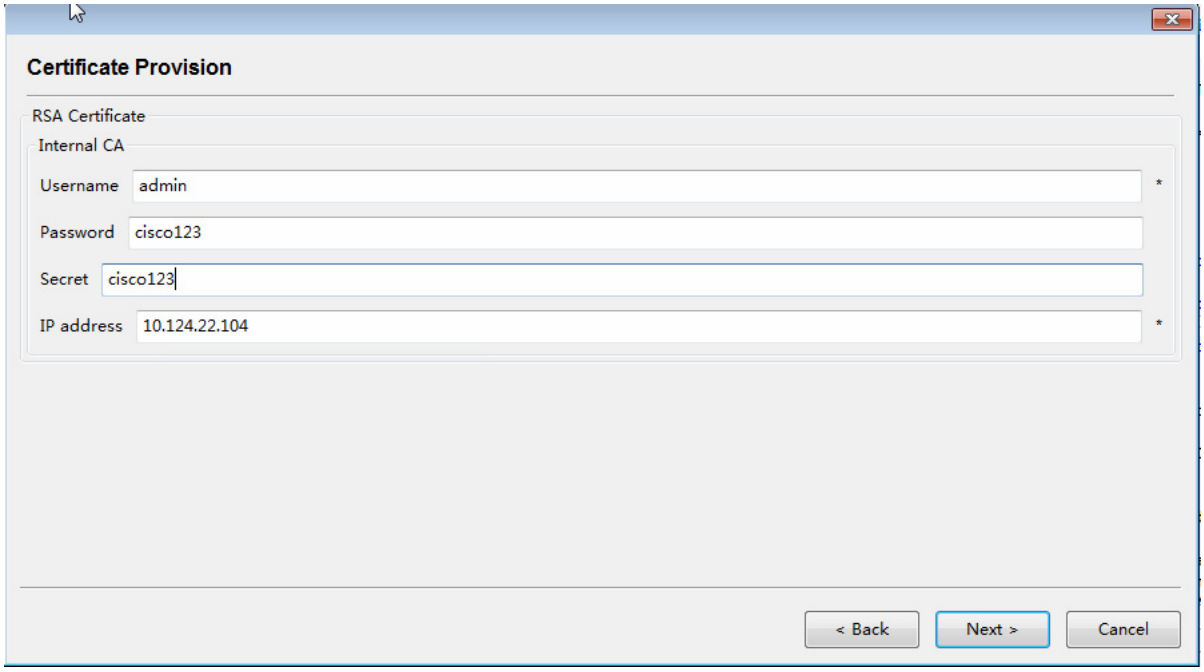


5. Choose to use external CA or internal CA, and click **Next >**.

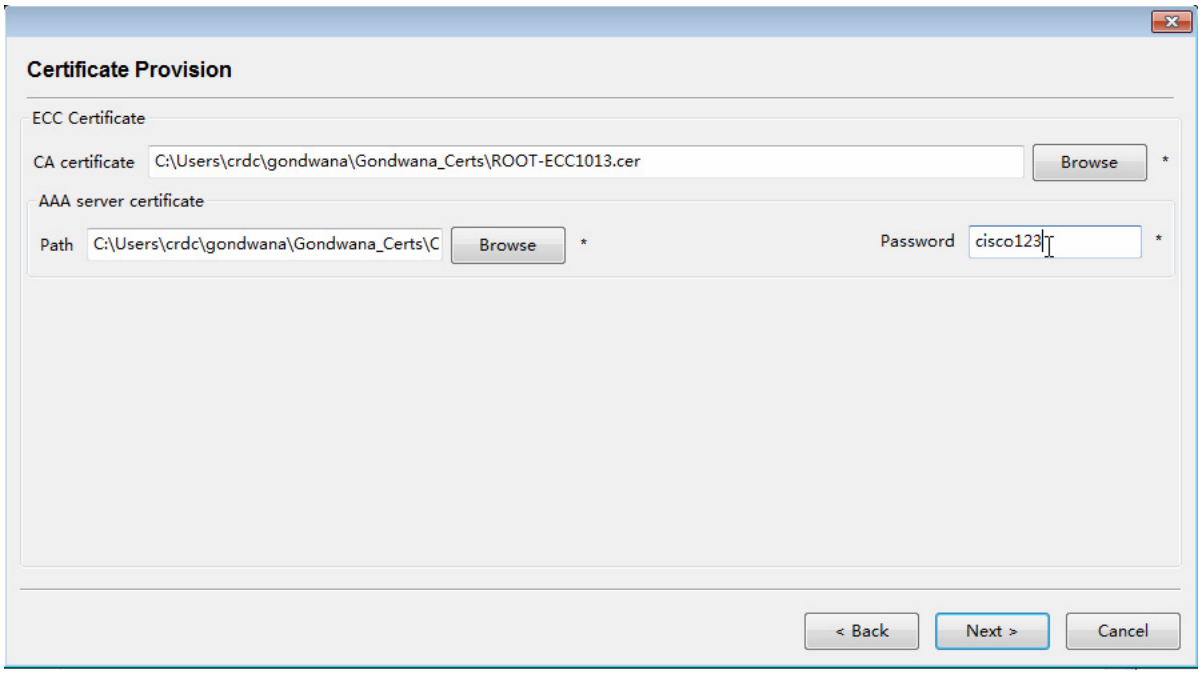
If you choose to use external CA, see Generating Certificates for the instructions on generating the certificates. In the following example, we choose to use internal CA (uncheck the **Use external CA** checkbox).



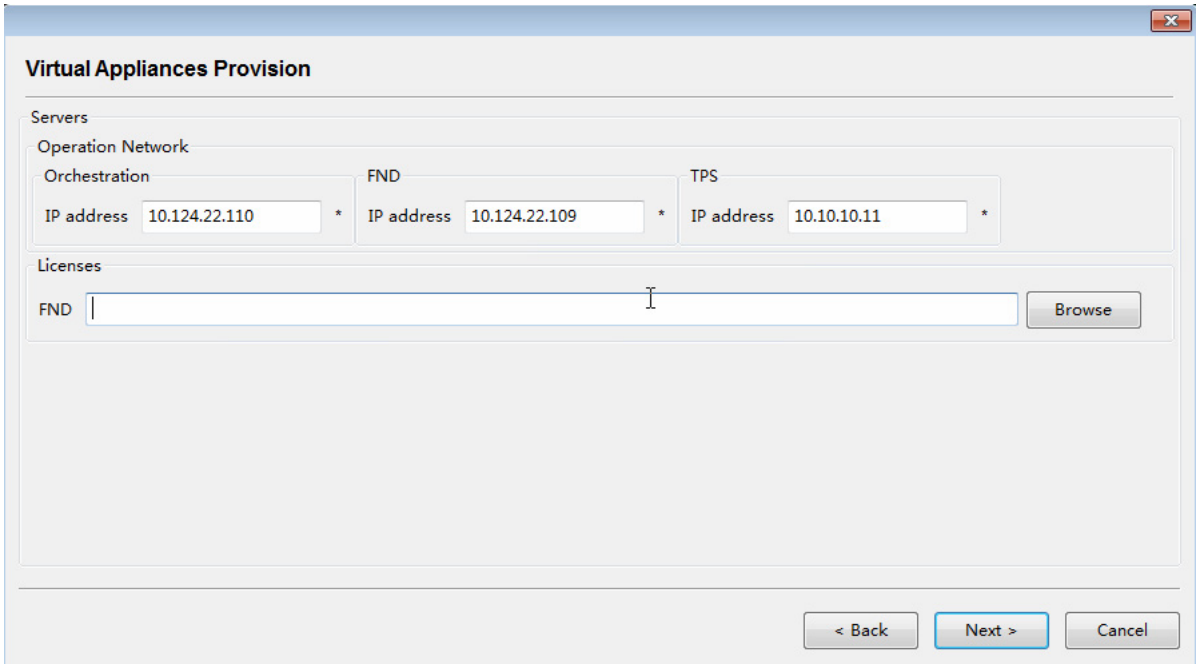
6. Enter internal CA information and click **Next >**.



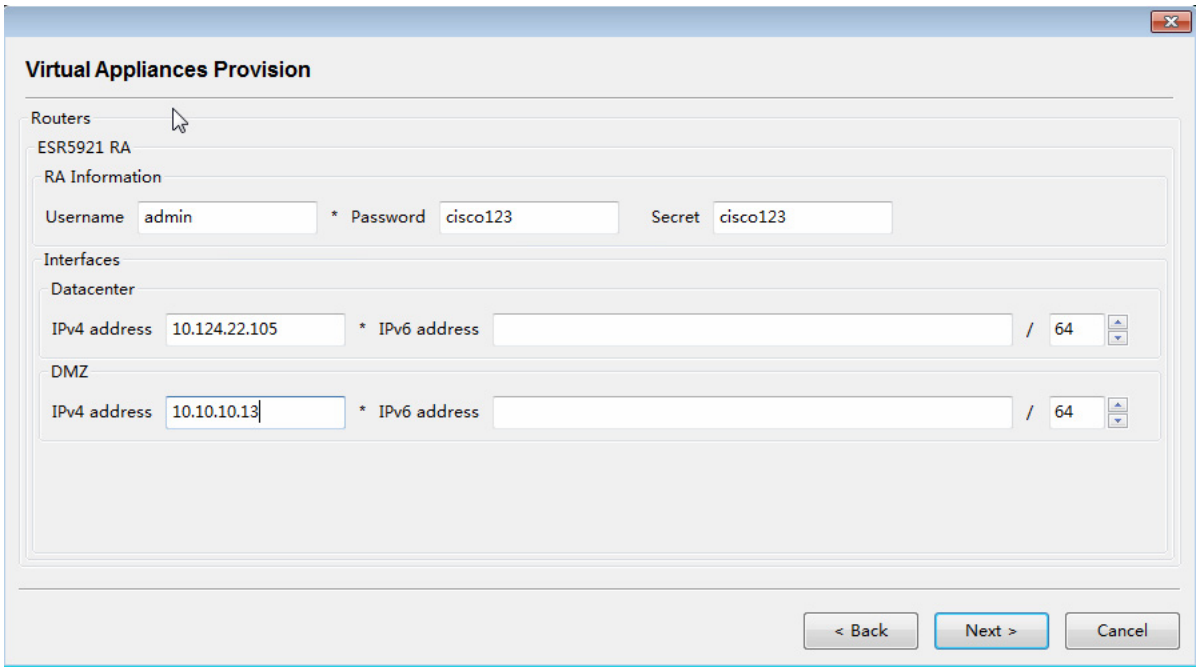
7. Enter the certificate information and then click **Next >**. For more information on generating ECC certificates, see the "Generating ECC Certificates" section on page 13. If you do not need to configure mesh, you are recommended to install by manually modifying the **`cisco_iok_installer.xml.template`** file



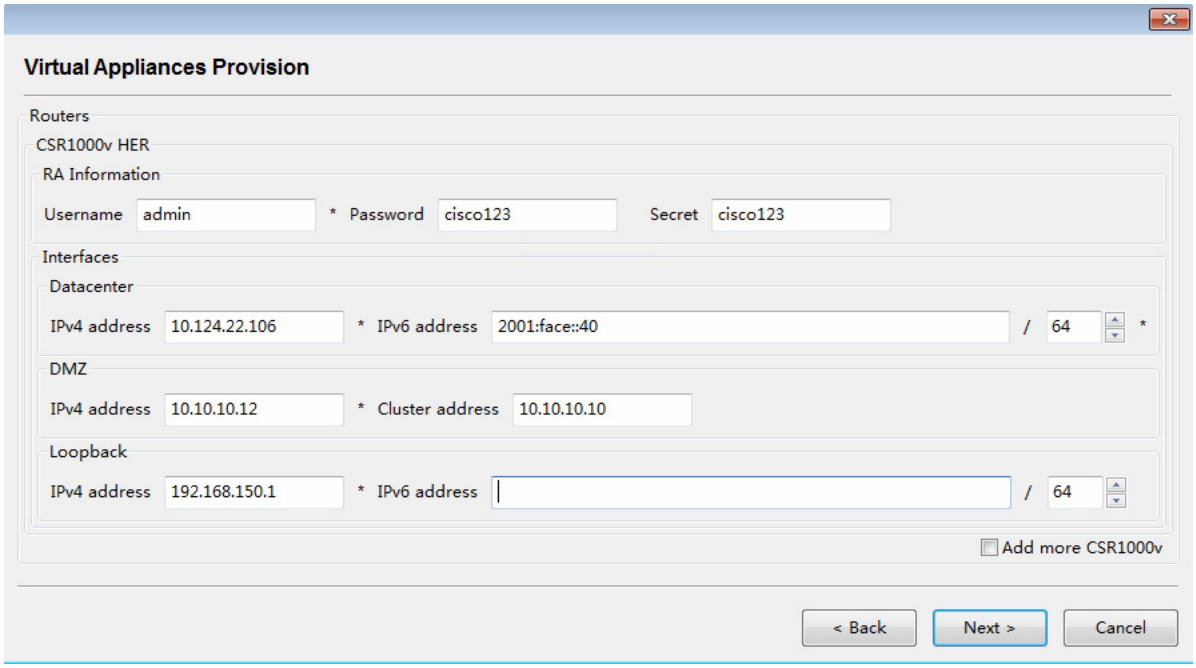
8. Enter the VM information and click **Next >**.



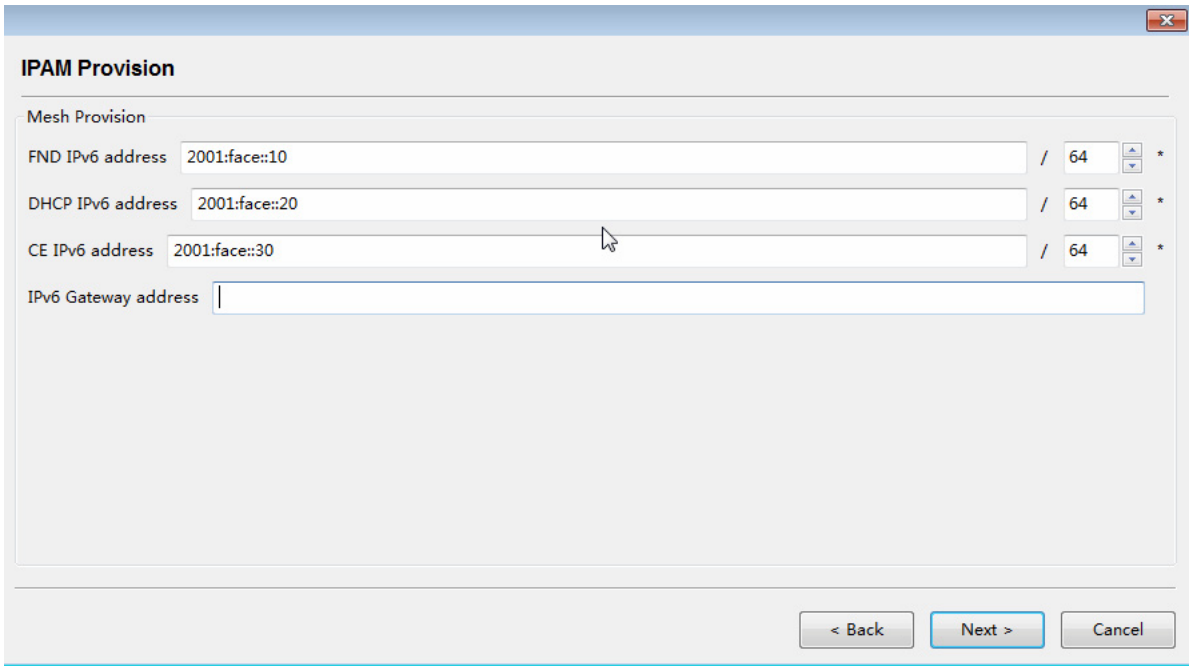
9. Enter the RA VM information and click **Next >**.



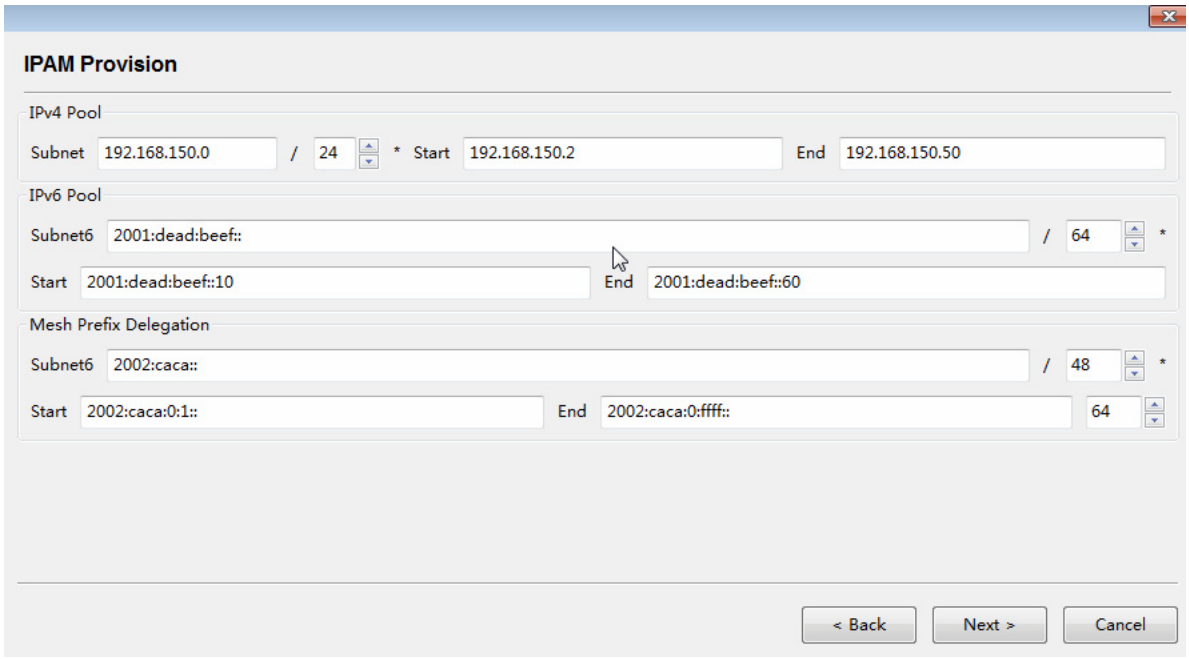
10. Enter the CSR VM information. If you want to configure more than one CSR, check the **Add more CSR1000v** checkbox. Then click **Next >.**



11. Enter the IPv6 addresses for the VMs and click **Next >**.



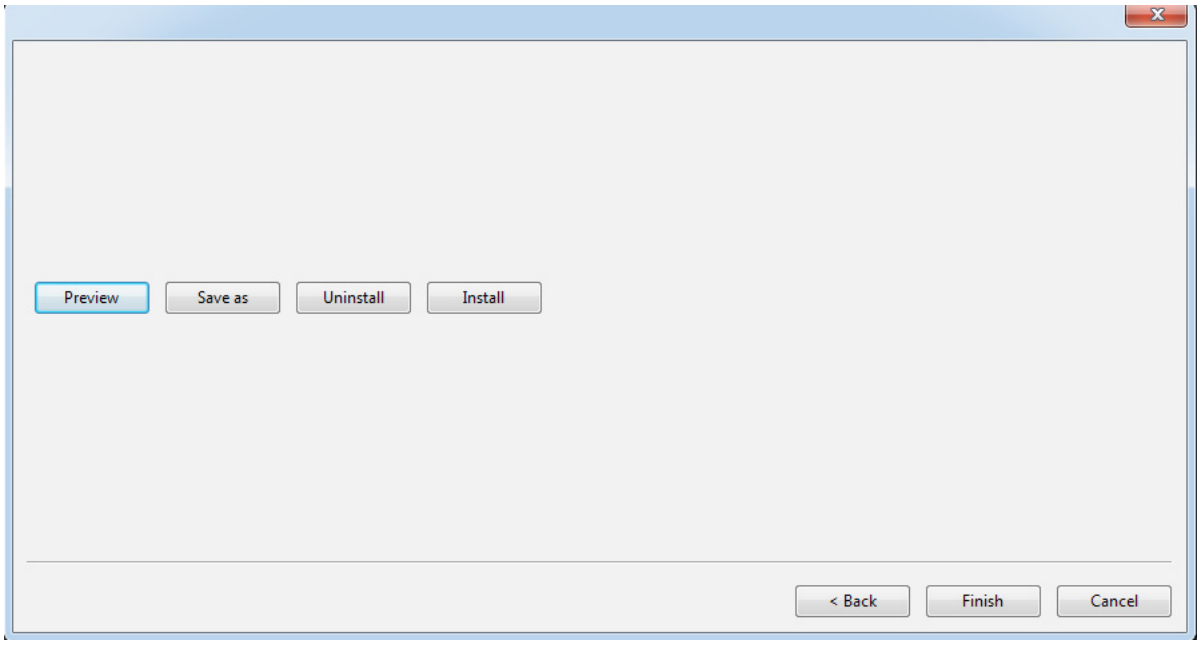
12. Enter the DHCP server information, which is embedded in the Orchestration VM, and then click **Next >**.



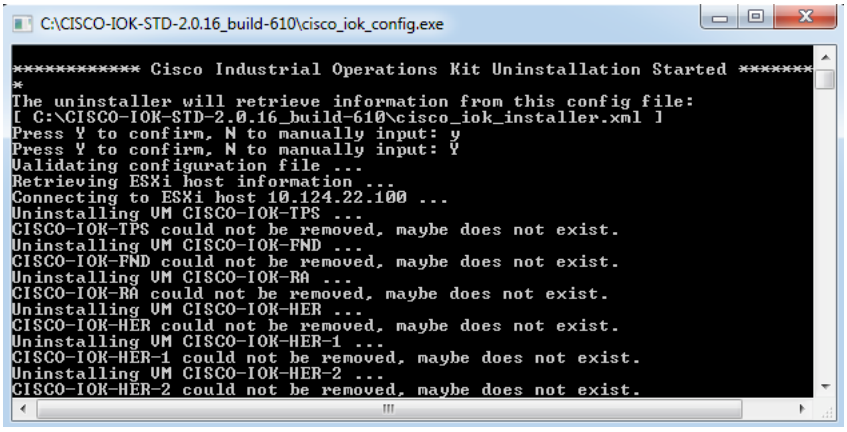
13. Click **Uninstall** to uninstall the previously installed version.

Note: You can preview the configuration file by clicking **Preview** or save the file as `cisco_iok_installer.xml` in the software folder by clicking **Save as**. When you click **Uninstall** or **Install**, the `cisco_iok_installer.xml` file will be saved automatically.

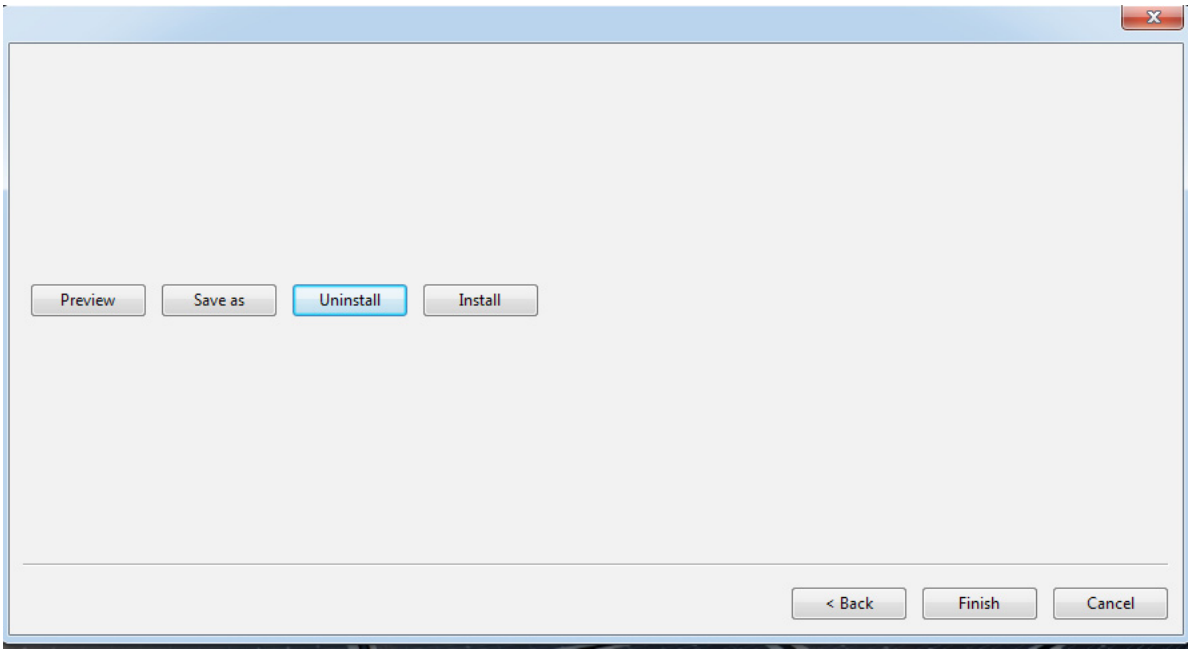
Note: If you already installed release 2.0.12, you need a fresh install to upgrade to release 2.0.16.



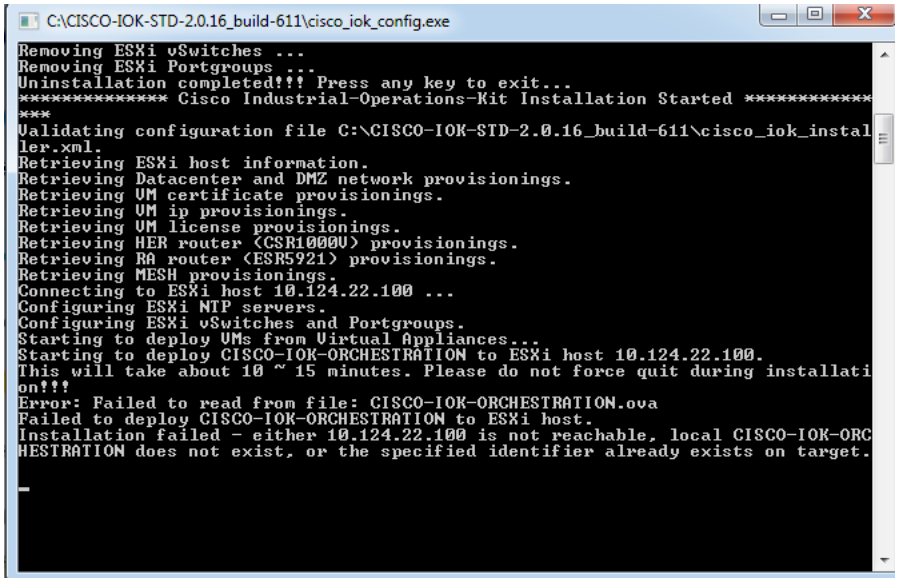
14. Enter **Y** at the command line to proceed the uninstallation.



15. When the uninstall completes, press **Enter** to return to the main configuration window.



16. Click **Install** to execute the installation process.



Installing by Using the Configuration Template File

As an option, if you do not use the **`cisco_iok_config.exe`** tool to generate the configuration template file and install the software, you can use the Configuration Template (.xml) to manually generate a **`cisco_iok_installer.xml`** file and then run the **`cisco_iok_installer.exe`**.

1. Copy the Configuration Template (.xml), **`cisco_iok_installer.xml.template`** and rename it to **`cisco_iok_installer.xml`**, and use an HTML editor to enter the requested information.

An example of **cisco_iok_installer.xml** is shown below. The field in bold indicates that the information needs user entry. For more information on each field, see Table 1 on page 7.

Example Cisco Industrial Operations Kit Configuration Template File

```
<?xml version="1.0" encoding="utf-8"?>
<!-- Cisco Industrial Operations Kit (IOK) configuration template. Please fill in this template
before starting the installer. -->
<iok_config>
  <esxi_info>
    <!-- The ESXi host ip address. This is the target where the IOK solution be deployed. -->
    <host_ip>172.27.168.91</host_ip>
    <!-- The username to login into the ESXi host. If no input, user will be required to -->
    <!-- interactively input during installation. This username should be either root or -->
    <!-- have root privilege. -->
    <login>root</login>
    <!-- The password to login into the ESXi host. For security concern, user may choose -->
    <!-- not to config it here, instead, type it during installation. -->
    <password>cisco123</password>
    <!-- The physical ethernet/NIC port to connect to the DMZ network. If no input, the -->
    <!-- second ethernet port 'vmnic1' will be taken as default. -->
    <dmz_port>vmnic1</dmz_port>
  </esxi_info>

  <!-- To provision Datacenter and DMZ network settings for IOK solution. -->
  <network_provision>
    <!-- The network settings for IOK ethernet port that connects to the datacenter network. -->
    <datacenter_interface>
      <!-- The gateway IPv4 address to the datacenter network. -->
      <gateway>172.27.168.1</gateway>
      <!-- The subnet mask in the datacenter network. -->
      <netmask>255.255.255.128</netmask>
      <!-- Domain name server in the datacenter network. -->
      <dns>172.27.168.183</dns>
    </datacenter_interface>

    <!-- The network settings for IOK ethernet port that connects to the DMZ network. -->
    <dmz_interface>
      <!-- The gateway IPv4 address to the DMZ network. -->
      <gateway>10.10.20.1</gateway>
      <!-- The subnet mask in the DMZ network. -->
      <netmask>255.255.255.128</netmask>
      <!-- Optional: Domain name server in the DMZ network. Leave blank if not available. -->
      <dns></dns>
    </dmz_interface>

    <!-- The NTP server information. Multiple <ntp_server> tags can be added to support -->
    <!-- multiple ntp servers. -->
    <ntp_server>
      <!-- Either NTP ip address or server name. If uses server name, make sure ESXi host -->
      <!-- has appropriate DNS configuration and the DNS server is reachable by ESXi. -->
      <server>171.68.38.66</server>
      <!-- NTP protocol version, if not configured, version 4 will be applied. -->
      <version></version>
    </ntp_server>
  </network_provision>

  <!-- To Provision the NMS, TPS, ORACLE, CPAR and ORCHESTRATION Virtual Appliances. -->
  <vm_provision>
    <!-- RSA Certificate is required for security. -->
    <rsa_certificate>
      <!-- [True|False] Tell installer which CA server to use, either leverage an existing -->
      <!-- customer CA or let installer automatically build its own CA inside the box.  -->
      <using_external_ca>False</using_external_ca>
      <!-- If using external CA, the installer needs to know the SCEP URL, CA certificate -->
```

```
      <!-- the exported NMS and TPS certificates with the passwords to protect private keys. -->
      <external_ca>
        <!-- The SCEP will be needed by headend and field routers to enroll certificates. -->
        <scep_url>http://172.27.163.168/certsrv/mscep/mscep.dll</scep_url>
        <!-- CA certificate provided by customer CA infrastructure (.cer or .pem). -->
        <!-- Please input the file path, such as C:\certs\solution_ca.cer -->
        <ca_cert>c:\Gondwana_Certs\IOK_CA2.cer</ca_cert>
        <!-- NMS certificate in pfx/PKCS12 format -->
        <nms_cert>c:\Gondwana_Certs\IOK_NMS_Cert.pfx</nms_cert>
        <!-- NMS certificate import password. This is usually set when import pfx certificate. -->
        <nms_cert_password>cisco123</nms_cert_password>
        <!-- TPS certificate in pfx/PKCS12 format -->
        <tps_cert>C:\Gondwana_Certs\IOK_TPS_Cert.pfx</tps_cert>
        <!-- TPS certificate import password. This is usually set when import pfx certificate. -->
        <tps_cert_password>cisco123</tps_cert_password>
      </external_ca>
      <!-- If using internal CA, user needs to reserve a datacenter IP and design the login/pwd.
-->
      <!-- everything else will be handled by the installer automatically. -->
      <internal_ca>
        <!-- The reserved Datacenter IPv4 for CA virtual appliance. -->
        <ca_ipv4>172.27.168.96</ca_ipv4>
        <!-- The login name to be created for the CA server. User may ssh into CA by this name. -->
        <login>admin</login>
        <!-- The password to login into the CA server. -->
        <password>cisco123</password>
        <!-- The secret to turn on privileged commands. User may leave it unconfigured here -->
        <!-- and provision it during the installation. -->
        <enable_secret>cisco123</enable_secret>
      </internal_ca>
    </rsa_certificate>

    <!-- Optional. Only required if mesh endpoints (such as smart meters) are deployed in  -->
    <!-- the field. For router only deployment, leave this part unconfigured. -->
    <ecc_certificate>
      <!-- ECC Root CA certificate provided by customer in pem/cer format. -->
      <!-- Please input the file path, such as C:\certs\solution_ecc_ca.cer -->
      <ca_cert>C:\Gondwana_Certs\ECC-root.cer</ca_cert>
      <!-- Optional: ECC Sub CA certificate provided by customer in pem/cer format. -->
      <!-- Leave it blank if no certificate is issued by Sub CA. -->
      <!-- Please input the file path, such as C:\certs\solution_ecc_subca.cer -->
      <subca_cert></subca_cert>
      <!-- CPAR ECC server certificate in pfx/PKCS12 or pem/cer format. -->
      <!-- Please input the file path, such as C:\certs\solution_cpar_ecc.pfx -->
      <cpar_cert>c:\Gondwana_Certs\mymeter1.pfx</cpar_cert>
      <!-- CPAR ECC certificate import password to protect the private key in either -->
      <cpar_cert_password>Cisco123</cpar_cert_password>
    </ecc_certificate>

    <!-- Operation IPs must be reserved for each virtual appliance in the solution box. -->
    <vm_ip>
      <!-- Operation IPv4 addresses for NMS in Datacenter network -->
      <nms_ipv4>172.27.168.93</nms_ipv4>
      <!-- Operation IPv4 addresses for ORACLE in Datacenter network -->
      <oracle_ipv4></oracle_ipv4>
      <!-- Operation IPv4 addresses for CPAR in Datacenter network -->
      <cpar_ipv4></cpar_ipv4>
      <!-- Operation IPv4 addresses for Orchestration/Controller in Datacenter network -->
      <orch_ipv4>172.27.168.92</orch_ipv4>
      <!-- Operation IPv4 for Tunnel Provisioning Service in DMZ network -->
      <tps_ipv4>10.10.20.11</tps_ipv4>
    </vm_ip>
```

```
    <!-- License file path -->
    <license>
      <!-- Optional: Without license, by default NMS can only support up to 25 end devices. -->
      <nms_license>C:\Gondwana_Certs\CGNMSFEAT20140128173424109.lic</nms_license>
      <!-- CPAR license is a must. Without license, CPAR may not function. User needs to either -->
      <!-- purchase a production license or obtain an evaluation license from Cisco. -->
      <cpar_license></cpar_license>
    </license>
  </vm_provision>

  <!-- To provision the software Headend router (HER: CSR1000V) and Registration Authority -->
  <!-- router (RA: ESR5921). Each router will have at least two inerfaces, one connecting  -->
  <!-- to the operation datacenter; the other connecting to the DMZ/public network.  -->
  <router_provision>
    <!-- HeadEnd Router settings -->
    <router_csr1000v_her_1>
        <datacenter_interface>
            <ipv4>172.27.168.95</ipv4>
            <ipv6>2001:fade::151/64</ipv6>
        </datacenter_interface>

        <dmz_interface>
            <ipv4>10.10.20.14</ipv4>
            <ipv6></ipv6>
        </dmz_interface>

        <Loopback_interface>
            <ipv4>192.0.2.2</ipv4>
            <netmask>255.255.255.128</netmask>
            <ipv6>2002:dead:beef::2/64</ipv6>
        </Loopback_interface>

      <login>admin</login>
      <password>cisco123</password>
      <enable_secret>cisco123</enable_secret>
    </router_csr1000v_her_1>

    <router_csr1000v_her>
      <!-- The interface to NMS/Data Center. It must be reachable by NMS & CA server. -->
      <datacenter_interface>
        <!-- IPv4 address reserved for this interface. Pingable from datacenter NMS server. -->
        <ipv4>172.27.168.110</ipv4>
        <!-- IPv6 address reserved for this interface. Pingable from datacenter NMS server. -->
        <!-- Optional: Only required if the headend needs to support the mesh endpoints. -->
        <!-- Example: 2001:DEAD:BEEF::100/64 -->
        <ipv6>2001:fade::150/64</ipv6>
      </datacenter_interface>

      <!-- The interface to DMZ/public network. It must be reachable by field end devices -->
      <!-- before secure tunnel is established. -->
      <dmz_interface>
        <!-- IPv4 address reserved for this interface. DMZ firewall should allow field -->
        <!-- devices to reach this IP through predefined protocols, such as FlexVPN, etc. -->
        <ipv4>10.10.20.13</ipv4>
        <!--Optional: leave it unconfigured if no IPv6 address enabled for this interface. -->
        <ipv6></ipv6>
<cluster_ipv4>10.10.20.10</cluster_ipv4>
      </dmz_interface>

      <!-- The interface bundled with FlexVPN virtual template. It may also be used by -->
      <!-- NMS/Datacenter for management purpose. Customer can pick up ip from the pools -->
      <!-- defined in the <ip_management> section, or use other available IPs. -->
      <Loopback_interface>
        <!-- IPv4 address reserved for FlexVPN virtual template. All the FlexVPN tunnels -->
        <!-- will reach this interface for traffic forwarding. -->
```

```
      <ipv4>192.0.2.1</ipv4>
      <!-- Network mask for this loopback interface. -->
      <netmask>255.255.255.128</netmask>
      <!--Optional: leave it unconfigured if no IPv6 address enabled for this interface. -->
      <ipv6>2002:dead:beef::1/64</ipv6>
    </Loopback_interface>

    <!-- Provision a login username for CSR1000V HER router. -->
    <login>admin</login>
    <!-- Router login password. User may choose to leave it unconfigured here and -->
    <!-- provision it during the installation. -->
    <password>cisco123</password>
    <!-- The router secret to turn on privileged commands. User may choose to leave -->
    <!-- it unconfigured here and provision it during the installation. -->
    <enable_secret>cisco123</enable_secret>
  </router_csr1000v_her>

  <!-- Software registration authority router (RA: ESR5921). -->
  <router_esr5921_ra>
    <!-- The interface to NMS/Data Center. It must be reachable by NMS & CA server. -->
    <datacenter_interface>
      <!-- IPv4 address reserved for this interface. Pingable from datacenter NMS server -->
      <ipv4>172.27.168.111</ipv4>
      <!--Optional: leave it unconfigured if no IPv6 address enabled for this interface. -->
      <ipv6></ipv6>
    </datacenter_interface>

    <!-- The interface to DMZ/public network. It must be reachable by field end devices -->
    <!-- before secure tunnel is established. -->
    <dmz_interface>
      <!-- IPv4 address reserved for this interface. DMZ firewall should allow field -->
      <!-- devices to reach this IP through predefined protocols, such as FlexVPN, etc. -->
      <ipv4>10.10.20.15</ipv4>
      <!--Optional: leave it unconfigured if no IPv6 address enabled for this interface. -->
      <ipv6></ipv6>
    </dmz_interface>

    <!-- Provision a login username for ESR5921 RA router. -->
    <login>admin</login>
    <!-- Provision the router login password. -->
    <password>cisco123</password>
    <!-- The secret to enable cisco router privileged commands. -->
    <!-- Optional: user may leave it blank and provision it during installation. -->
    <enable_secret>cisco123</enable_secret>
  </router_esr5921_ra>
</router_provision>

<!-- Optional: Only required if the headend infrastructure needs to support mesh endpoints. -->
<!-- For router only deployment, leave this section unconfigured. -->
<mesh_provision>
  <!-- IPv6 address for NMS VM interface in Datacenter network, e.g. 2001:DEAD:BEEF::100/64 -->
  <!-- Make sure NMS IPv6 and HER (CSR1000v) data center IPv6 are in the same subnet. -->
  <nms_ipv6>2001:fade::190/64</nms_ipv6>
  <!-- IPv6 address for Orchestration VM interface in Datacenter network. -->
  <!-- Make sure this IPv6, NMS IPv6, and HER (CSR1000v) IPv6 are in the same subnet. -->
  <!-- Optional: If IPv6 dhcp server (for mesh endpoints) is configured on CGR end router, -->
  <!-- <orch_ipv6> is not required. -->
  <orch_ipv6>2001:fade::200/64</orch_ipv6>
  <!-- IPv6 address for service provider data collection engine (CE). -->
  <ce_ipv6>2001:fade::180/64</ce_ipv6>
  <!-- Optional: Only required if CE IPv6 is not in the same subnet as NMS IPv6. -->
  <!-- Data center IPv6 gateway address, for example, 2001:face::1 -->
  <dc_ipv6_gateway></dc_ipv6_gateway>
```

```
</mesh_provision>

<!-- IP pool management for field devices and mesh endpoint devices. -->
<ip_management>
  <!-- These IPs will be used as IP pools for field end devices and headend router loopback -->
  <!-- interfaces. NMS will communicate with end devices and headend router through them. -->
  <!-- To add multiple IP pools, keep adding <ipv4_pool> or <ipv6_pool> entries. -->
  <ipv4_pool>
    <ip_subnet>192.0.2.0</ip_subnet>
    <!-- Sample IPv4 netmask: 255.255.255.0 -->
    <ip_netmask>255.255.255.128</ip_netmask>
    <!-- The start IPv4 address within the subnet -->
    <ip_start>192.0.2.2</ip_start>
    <!-- The end IPv4 address within the subnet -->
    <ip_end>192.0.2.100</ip_end>
  </ipv4_pool>

  <ipv6_pool>
    <!-- Sample prefix: 2001:dead:beaf::/64-->
    <ip_prefix>2002:dead:beef::/64</ip_prefix>
    <!-- The start IPv6 address within the prefix scope -->
    <ip_start>2002:dead:beef::100</ip_start>
    <!-- The end IPv6 address within the prefix scope -->
    <ip_end>2002:dead:beef::150</ip_end>
  </ipv6_pool>

  <ipv6_pd_pool>
    <ip_prefix>2012:cafe::/48</ip_prefix>
    <ip_start>2012:cafe:0:1::</ip_start>
    <ip_end>2012:cafe:0:ffff::</ip_end>
    <subrouter_prefix_length>64</subrouter_prefix_length>
  </ipv6_pd_pool>
</ip_management>

<!-- Optional: If user has field end device files prior to installation, these files can  -->
<!-- be configured here so the installer will push them into the NMS database. Otherwise, -->
<!-- leave it unconfigured. User can always import device files through NMS web GUI after -->
<!-- installation completed. -->
<device_import>
  <!-- Multiple device files are supported by adding more <device_file> entries. -->
  <device_file></device_file>
</device_import>

</iok_config>
```

The template comes with the Industrial Operations Kit software bundle. (See Table 1 on page 7 for details on required information.)

2. Double-click **`cisco_iok_uninstall.exe`** to uninstall the previous installation if any.

3. To install the software bundle on the server, double click **`cisco_iok_installer.exe`** (recommended) or execute it from DOS command line, with or without the *--overwrite* option.

   Note: If you specify the *--overwrite* option, the previous installation will be overwritten. The *--overwrite* option equates to a fresh installation.

   Note: If you already installed release 2.0.12, you need a fresh install to upgrade to release 2.0.16.

   – Software automatically configures the networking connections for the server and then installs, provisions, and brings up each individual virtual machine and its application services.
   (See Figure 2 on page 4.)

   – We highly recommend that you change the default root password when prompted at the end of the installation.

– When the install completes successfully, the following statement is displaysedon the screen:

```
************** Cisco Industrial Operations Kit Installation Completed ************
```

EXAMPLE

```
Listed below is an example of the output that displays on the console after you begin installation.
************** Cisco Industrial Operations Kit Installation Started ***************
Validating configuration file C:\gondwana\cisco_iok_installer\cisco_iok_installer.xml.
Retrieving ESXi host information.
Retrieving Datacenter and DMZ network provisionings.iok
Retrieving VM certificate provisionings.
Retrieving VM ip provisionings.
Retrieving VM license provisionings.
Retrieving HER router (CSR1000V) provisionings.
Retrieving RA router (ESR5921) provisionings.
...
...
...
NOTE: change the default root password for each VM to ensure solution security.
You may either change it now or change it later within each VM guest OS.
Proceed with password change? (y/n) Installation completed!!!
```

Monitoring Industrial Operations Kit Components

After you successfully install the software, you can access the Industrial Operations Kit (IOK) GUI. Errors are logged in an HTML log, which you can access through a browser.

You can monitor the Industrial Operations Kit by using the Orchestration Web Services at:

`https://<orch_ipv4>`

where

<orch_ipv4> is the Orchestration operation ip that you set in the **`cisco_iok_config.exe`** tool or you manually entered in the Configuration Template (.xml).

For more information, see GUI Overview.

Note: The monitoring activity described above is distinct from that provided by IoT-FND.

GUI Overview

This section explains using the Industrial Operations Kit (IOK) GUI to manage and monitor the head-end infrastructure. Installation and configuration file provisioning are described in the "Installing Industrial Operations Kit on the Server" section on page 39.

Note: When using online publications, reference documents matching the Cisco IOS software version running on the routers and switches in your network, and the IoT-FND user manual installed on the FND server.

The IOK GUI allows you to manage FAN configuration and provisioning using the following VMs (Figure 3 on page 5) configured during IOK installation:

- CISCO-IOK-FND—This is the FND FAN management service.
- CISCO-IOK-TPS—This is the secure tunnel provisioning service.
- CISCO-IOK-ORCHESTRATION—This is the orchestration and management services for all Industrial Operations Kit components.

- CISCO-IOK-HER—This is the Head-end Router service (based on the Cisco CSR 1000V).
- CISCO-IOK-RA—This is the Registration Authority (RA) service (based on the Cisco ESR 5921).

This section describes the Industrial Operations Kit GUI, including:

Logging In

Use one of the following supported browsers to access the Industrial Operations Kit GUI:

- Internet Explorer (IE): 9.0 or higher
- Mozilla Firefox: 3.5 or higher
- Safari 6.0 or higher
- Chrome 30 or higher

DETAILED STEPS

To start the Industrial Operations Kit GUI:

1. In your browser, enter the IP address of the Orchestration server.

   Note: This must be an https secure access.

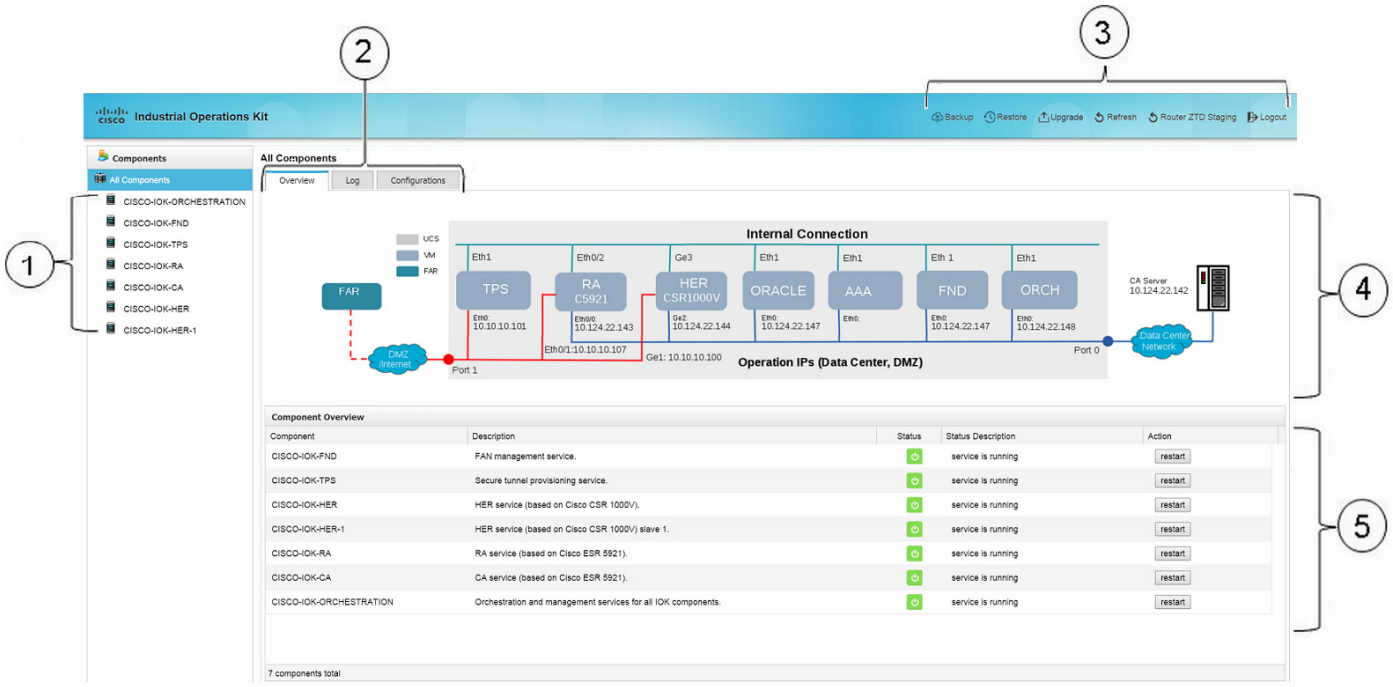
2. Accept the site security certificate.
3. Enter the default login information:

   - Username: **root**
   - Password: **root123**

   Note: The FND deployed by IOK has the same default username **root** and password **root123**.

Figure 4 on page 55 highlights elements of the opening page.

Figure 4 IOK Head-end GUI Opening Page Elements



1	Components Pane	**4**	Information Pane
2	Information Pane tabs	**5**	Component Overview Pane
3	Buttons		

Components Pane

The Components pane (item 1 in Figure 4 on page 55) lists all VMs installed and configured during Industrial Operations Kit installation. Select a component in this pane to view its configuration details in the Information pane (item 2 in Figure 4 on page 55).

Information Pane

The Information pane displays component-related information. This section describes the following:

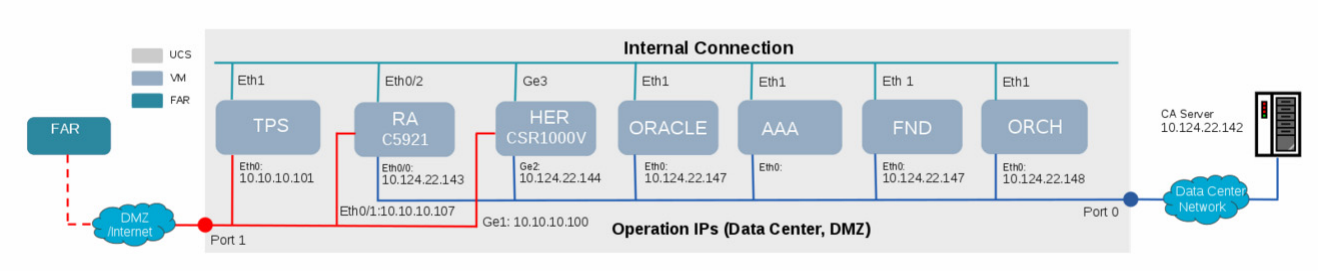
- Viewing Information for All Components, page 55
- Viewing Component-Specific Information, page 56
- Managing IOK VM Licenses, page 57

Viewing Information for All Components

At log in, All Components displays in the Components pane by default. The Overview tab displays a virtual network diagram (Figure 5 on page 56). This snapshot of your virtual network starts at the left with the FAR (end node), and ends at the right with the Certification Authority (CA) server. The diagram displays IP addresses for all IOK VMs. The following states signify the network connection status:

- A red line indicates that the DMZ network connects through UCS port 1.
- A green line indicates internal connections (that is, it is not connected to any UCS port).
- A blue line indicates a connection to the Data Center network through UCS port 0.
- A solid network connection line indicates a direct connection.
- A dashed network connection line indicates that it is not a direct connection (for example, the connection may be through a public network such as a cellular network).

Figure 5 Network Diagram



Note that the CGR or FAN device must go through the RA and TPS VM services to establish a secure tunnel with the HER. Before this tunnel is established, the device cannot reach the data center network.

Viewing Logs

The Logs tab displays network messages for all installed VM components.

Viewing the Current Configuration Template

The Configurations tab displays the current Configuration Template XML file. You configure this file during the Industrial Operations Kit installation.

Viewing Component-Specific Information

When you select a component in the Components pane, the Information pane tabs display basic information and logs.

Components Overview Tab

The Overview tab displays component elements and assigned values, including:

- Guest OS Hostname and Version
- Operation IP Address
- Service Running Status
- Service Uptime
- License Status and License UDI (if applicable)

Components Logs Tab

The Logs tab displays log messages and associated severity levels:

- INFO–These are the lowest severity level log messages.
- WARNING–These log messages are generated on service status changes (for example, on a VM restart).
- ERROR–These messages are generated for critical events and exceptions.

Managing IOK VM Licenses

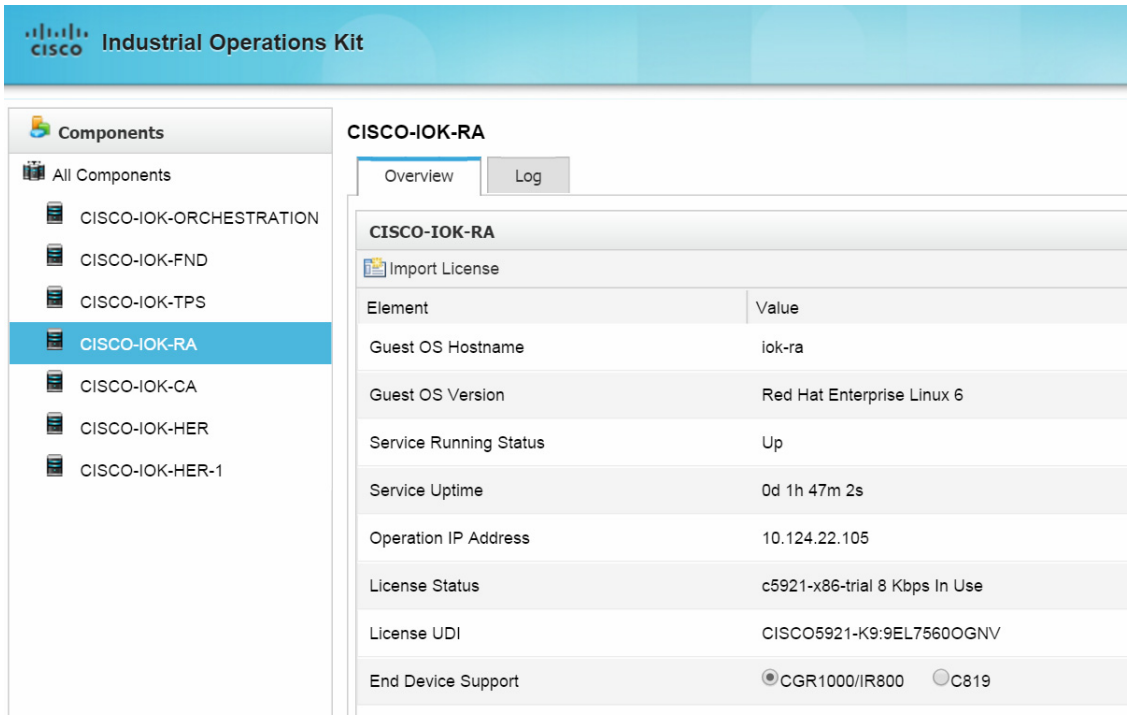
On the Information pane, you can import license files to the following VMs:

- CISCO-IOK-FND
- CISCO-IOK-RA
- CISCO-IOK-HER
- CISCO-IOK-HER-X (X is 1-4)

DETAILED STEPS

To import a license to an IOK VM:

1. In the Components pane, select the desired VM.



2. In the Information pane on the Overview tab, click **Import License**.

3. Click **Browse** to navigate to the desired valid license file.

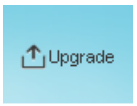
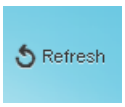
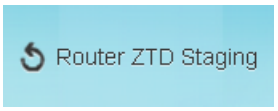
   You must select the proper service license file type when importing licenses.

4. Click **Submit Query**.

   The VM license updates.

Buttons

Along the upper-right in the top banner (item 3 in Figure 4) are the following buttons.

Button	Description
	Backs up all VMs. **Note:** Backups cannot be canceled. You must confirm the backup at the prompt. When complete, a pop-up window shows that the backup is completed.
	Restores all VMs to the selected backup restore point. Backups are listed by date, latest at the top.
	Upgrades all VMs to the selected upgrade tarball. **Note:** If you already installed release 2.0.12, you need a fresh install to upgrade to release 2.0.16.
	Refreshes the view, and returns to the All Components Overview page.
	Accesses the Router ZTD Staging Dialog Box.
	Logs you out of the GUI.

The following are other GUI buttons:

Button	Description
	Displays the Imports License dialog box. **Note:** You must select the proper service license file type when importing licenses.
	Restarts the VM service.
	(All Components Logs tab) Refreshes log messages for the selected component.

Component Overview Pane

Select All Components to display the Component Overview pane (item 4 in Figure 4 on page 55) at the bottom of the Information pane. The Component Overview lists the VMs, their status (Up or Down) and description, and allows you to restart the VM service.

You must confirm that the Industrial Operations Kit VM restarts at the prompt. Also, the Industrial Operations Kit GUI is unavailable during ORCHESTRATION VM restarts.

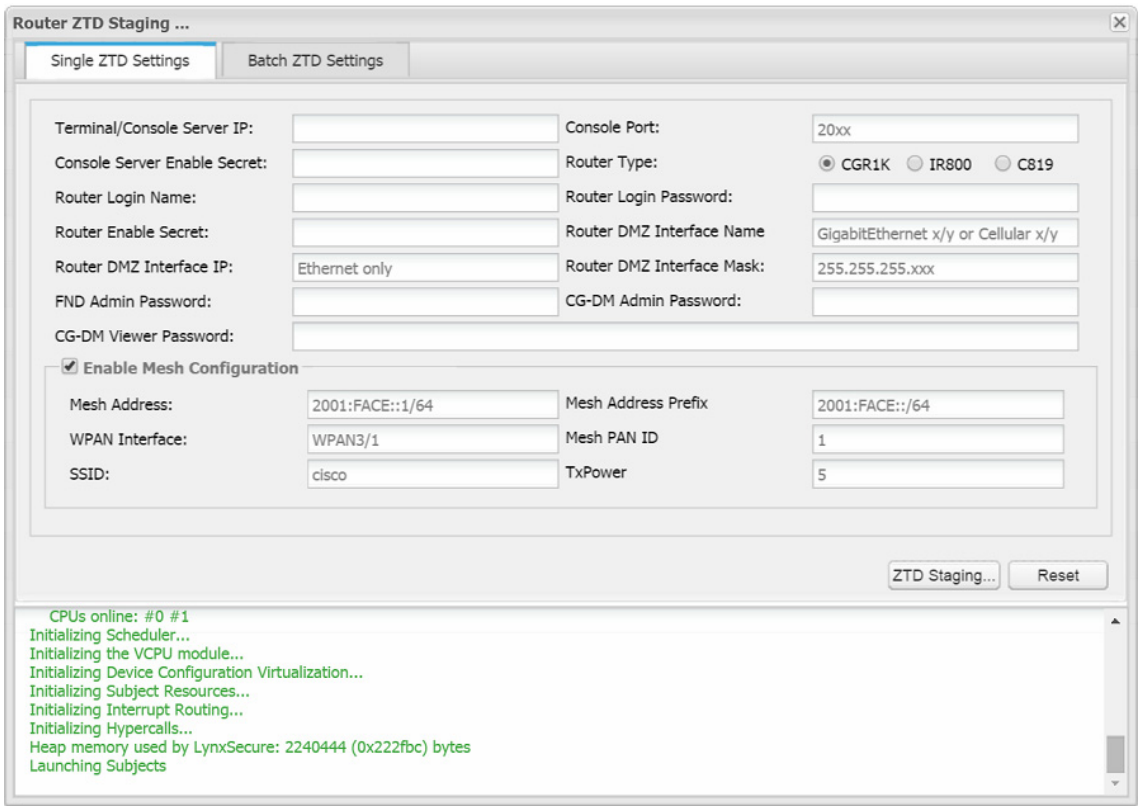
Router ZTD Staging Dialog Box

Use the Router ZTD Staging dialog box to begin zero-touch deployment (ZTD) on assigned CGRs.

To begin router ZTD configuration:

1. Click the **Router ZTD Staging** button.

   The Router ZTD Staging dialog box displays.

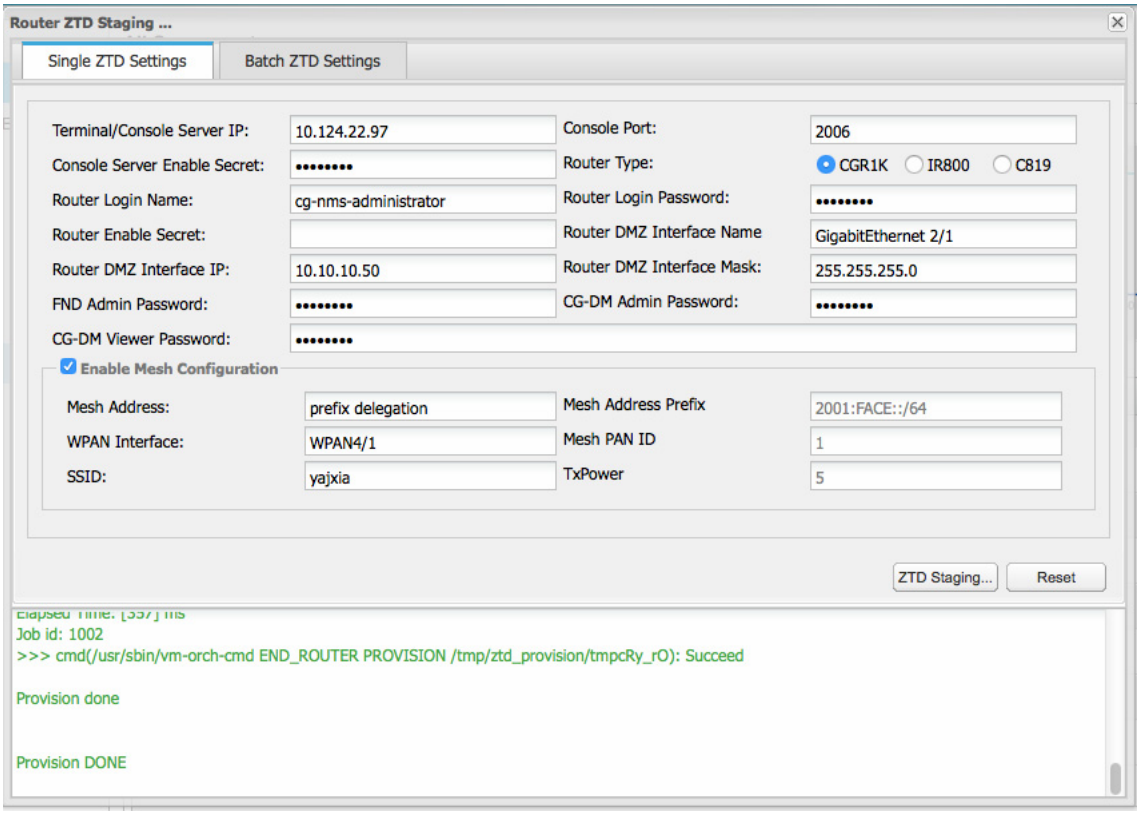


Note: For the **Router Type** field, C819 does not support mesh.

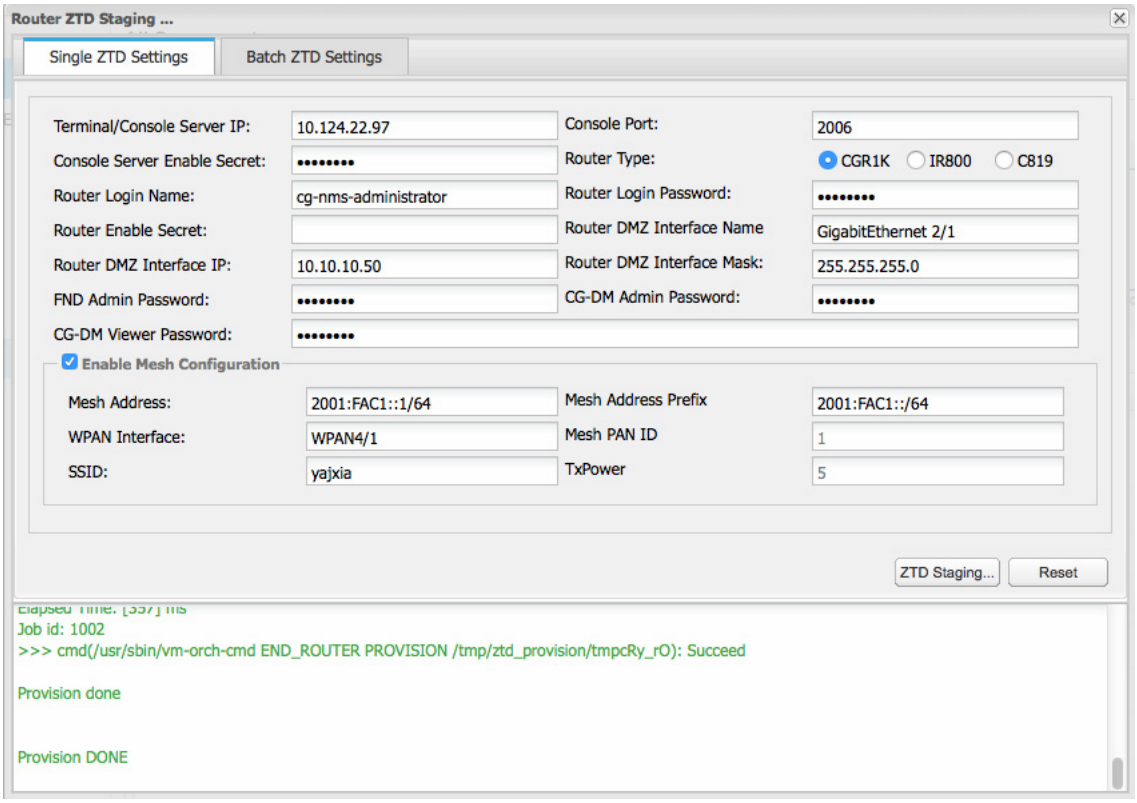
If you choose to configure single ZTD settings, for the Enable Mesh Configuration field, you can choose to

- Enable mesh with prefix delegation (PD), with the prerequisite that you have configured PD in the **`cisco_iok_config.exe`** tool or the Configuration Template (.xml).
- Enable mesh without PD.
- Disable mesh configuration.

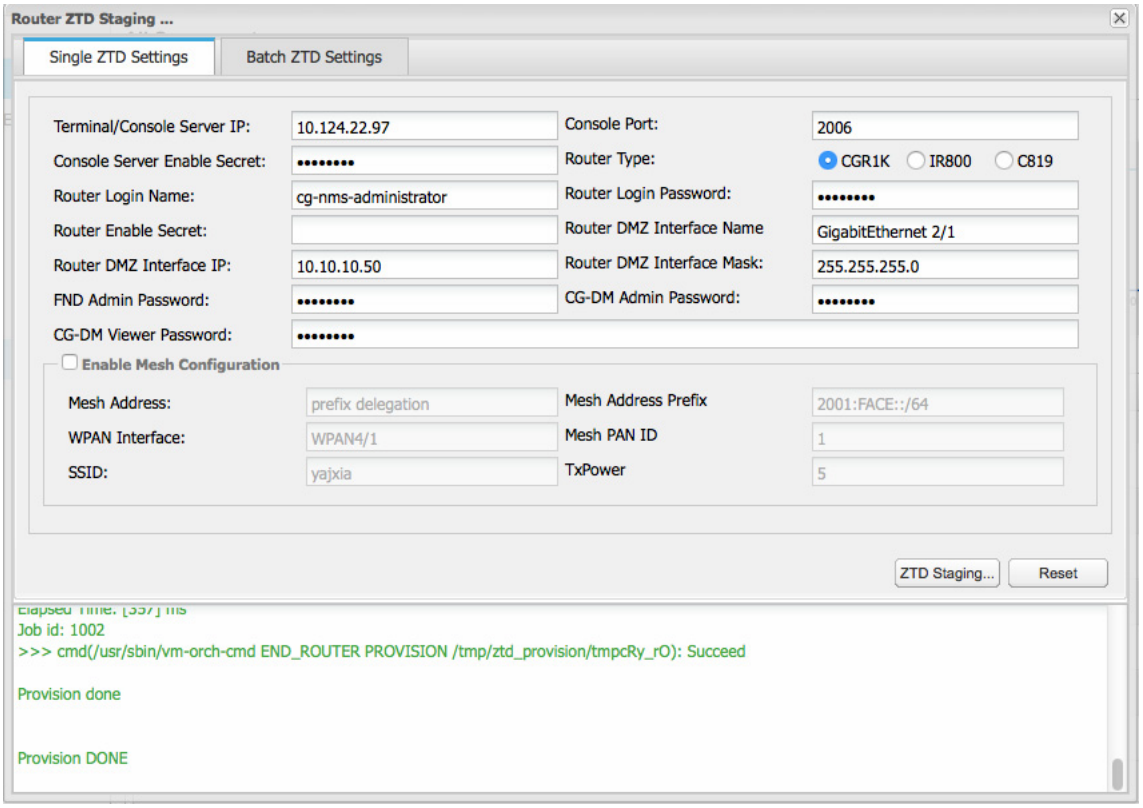
The following figure shows the ZTD settings that enable mesh with prefix delegation (PD) configured.



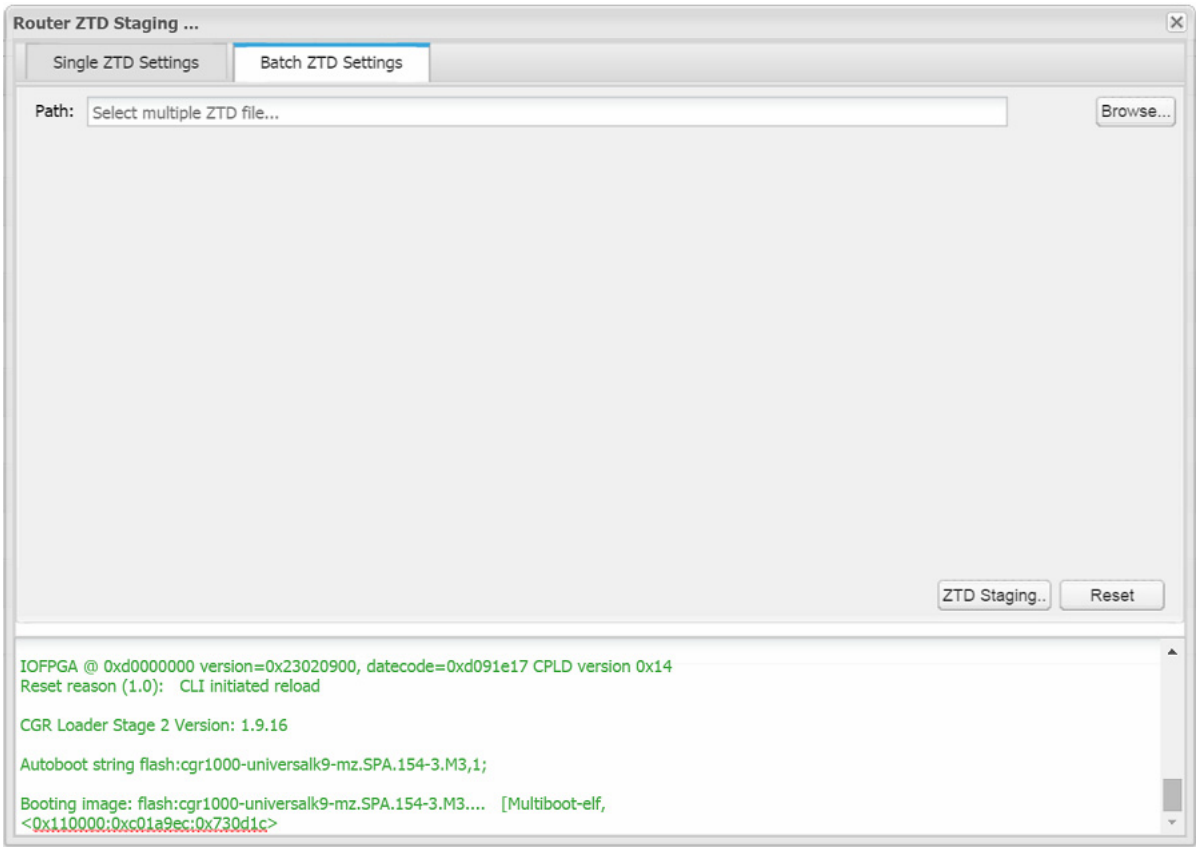
The following figure shows the ZTD settings that enable mesh without PD configured.



The following figure shows the ZTD settings that disable mesh configuration.



2. If you choose batch ZTD settings, click on the **Batch ZTD Settings** tab and then click the **Browse...** button to import a .csv file from your local drive that contains all necessary field values to complete the batch ZTD settings.



An example of the batch ZTD .csv file is as following. The first row contains the fields. The values of each field for the first device are listed in the second row. The values for the second device are listed in the third row. If you have more devices, add more rows to input the values.

```
consoleIp,consolePort,consoleSecret,deviceType,adminUsername,adminPassword,adminEnablePassword,tunn
elSrcInterface,ip,ipMask,defaultGateway,cgnmsAdminPassword,cgnmsAdminEnablePassword,cgdmViewPasswor
d,cgdmTAdminPassowrd,cgdmTViewPassowrd,meshEnabled,meshAddressConfig,meshPrefixConfig,masterWpanInt
erface,meshPanid,meshSsid,meshTxPower

10.124.22.97,2006,cisco123,CGR1000,cg-nms-administrator,cisco123,,GigabitEthernet
2/1,10.10.10.50,255.255.255.0,,cisco123,cisco123,cisco123,cisco123,cisco123,off

10.124.22.97,2008,cisco123,CGR1000,cg-nms-administrator,cisco123,,GigabitEthernet
2/1,10.10.10.52,255.255.255.0,,cisco123,cisco123,cisco123,cisco123,cisco123,off
```

3. Click **ZTD Staging**.

Note: ZTD staging takes approximately 10–15 minutes. Output messages display in the bottom pane.

Log Messages

For FND and TPS messages, refer to the FND and TPS user guides.

Feature History

Feature	Release	Feature Information
Industrial Operations Kit 2.0	CISCO-IOK-STD-2.0.16	■ Support for multiple CSR1000 routers (up to 5) to extend the capability to support up to 1000 FlexVPN tunnels. ■ FreeRADIUS, which replaced CPAR as the AAA server in IOK 2.0, is deployed to the Orchestration VM to reduce the hardware footprint. ■ Support for centralized log files, which are collected from IoT FND, TPS, FreeRADIUS, and Orchestration VM.
Industrial Operations Kit	CISCO-IOK-STD-2.0.12	Initial support of the Industrial Operations Kit software package on Cisco UCS servers.

Related Documentation

Release Notes for IoT Field Network Director, Release 3.0

Cisco IoT Field Network Director User Guide 3.0.x

North Bound API User Guide for the Cisco IoT Field Network Director 3.0.x

Cisco Prime Access Registrar

Cisco 5921 Embedded Services Router

Cisco CSR 1000V Series Cloud Services Router Software Configuration Guide

Cisco 1000 Series Connected Grid Routers Configuration Guides and Release Notes

Cisco 800 Series Integrated Services Routers Software Configuration Guide

Cisco 800 Series Industrial Integrated Services Routers (IR 800)

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see *What's New in Cisco Product Documentation* at: http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html.

Subscribe to *What's New in Cisco Product Documentation*, which lists all new and revised Cisco technical documentation as an RSS feed and delivers content directly to your desktop using a reader application. The RSS feeds are a free service.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies are considered un-Controlled copies and the original on-line version should be referred to for latest version.

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at www.cisco.com/go/offices.