IGEL Cloud Gateway (ICG)

- ICG Manual(see page 3)
- ICG FAQ(see page 90)
- ICG How-Tos(see page 92)
- ICG Release Notes(see page 161)
- ICG Field Experience(see page 220)

ICG Manual

The IGEL Cloud Gateway (ICG) enables the Universal Management Suite (UMS) to securely manage endpoint devices outside the company network.

- What is New in ICG 2.05.100?(see page 4)
- Prerequisites(see page 5)
- When to Use ICG(see page 7)
- Limitations(see page 11)
- Installation and Setup(see page 12)
- Connecting the Devices(see page 50)
- Administration(see page 58)

What is New in ICG 2.05.100?

You will find the release notes for IGEL Cloud Gateway 2.05.100 both as a text file next to the installation programs under igel.com/software-downloads/enterprise-management-pack/[1] **> IGEL CLOUD GATEWAY** and in the Knowledge Base under Notes for Release 2.05.100(see page 167).

1 https://www.igel.com/software-downloads/enterprise-management-pack/

Prerequisites

> **ICG Appliance Is No Longer Supported**
>
> ICG 1.01 and ICG 1.02 (virtual appliance in OVA/OVF format) have reached the End of Maintenance on March 1, 2020.

For installing and deploying a working environment with the UMS (Universal Management Suite) and IGEL Cloud Gateway, you need the following components:

Universal Management Suite (UMS)

Universal Management Suite (UMS) 5.06.100 or higher is required for basic functionality. If Shadowing or Secure Shadowing is needed, version 6.02.110 or higher is required.

Devices with IGEL OS Firmware

For basic functionality, IGEL OS 10.02.100 or higher is required. If Shadowing or Secure Shadowing is needed, version 11.02.100 or higher is required.

Linux Host

Hardware

- 8 GB RAM (recommended)
- 2 CPUs
- 20 GB HDD (recommended)

The ICG service requires min. 2 GB RAM, 2 CPUs, and 2 GB of free disk space (depends strongly on the number of devices to be managed).

Operating System

The following Linux distributions are supported (64-bit variant):

- Amazon Linux v2
- Debian 10
- Debian 9
- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04
- Oracle Linux 8
- Oracle Linux 7
- Red Hat Enterprise Linux (RHEL) 8
- Red Hat Enterprise Linux (RHEL) 7

- SUSE Enterprise Server 15
- SUSE Enterprise Server 12

Certificates

For the communication between the ICG and the devices, a certificate chain must be provided. The requirements are described under Certificate Requirements and Recommendations for the IGEL Cloud Gateway (ICG)(see page 14). The different methods for obtaining the certificate chain are described under Installing an Existing Certificate Chain(see page 16), Creating Certificates from an Existing Root Certificate(see page 27), and Creating a Certificate Using the UMS(see page 35).

> Please also note our Installation and Sizing Guidelines for IGEL UMS in the UMS manual.

When to Use ICG

Typical Scenarios

The IGEL Cloud Gateway (ICG) is required if the UMS and the devices are not in the same network. The following scenarios are typical use cases for the ICG:

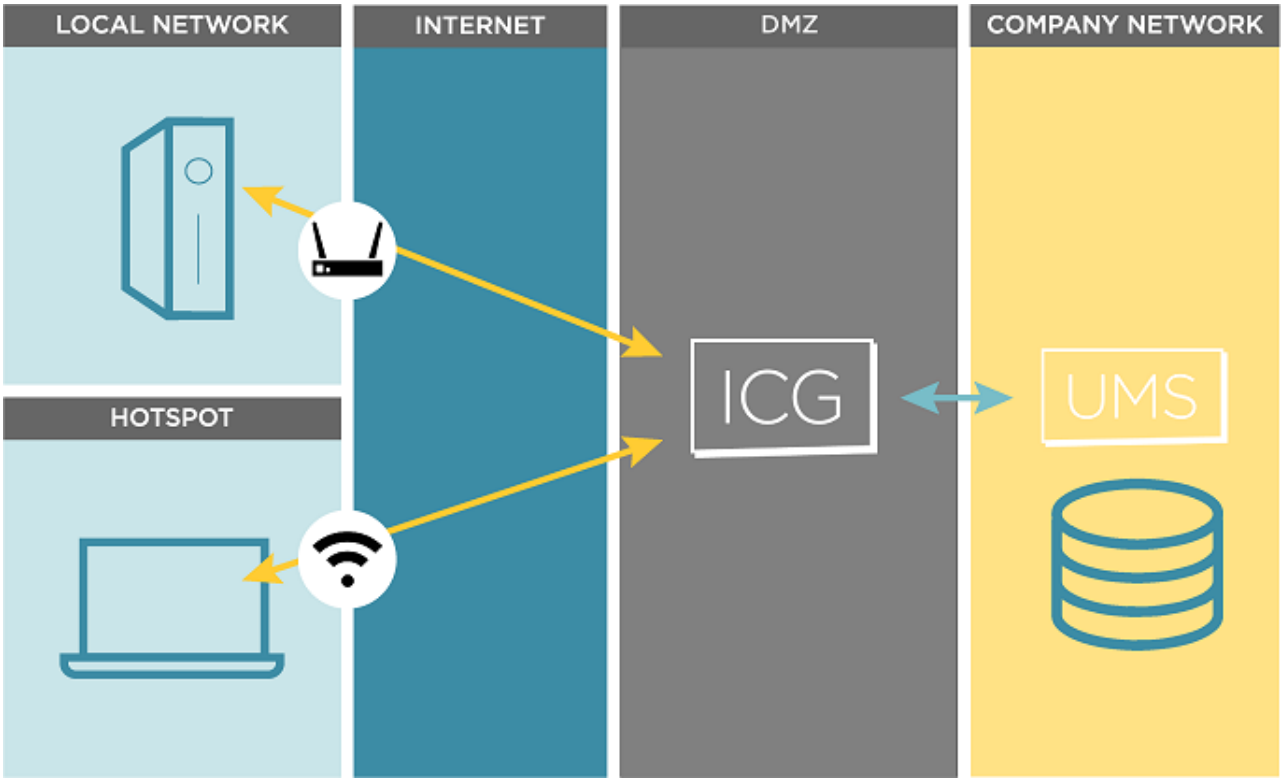
- The endpoint devices (IGEL UD, UD Pocket or devices converted by UDC3/OSC) of all geographically dispersed branches of a company are to be managed by one central UMS.
- UD Pocket or devices converted by UDC3/OSC are to be managed by the UMS which is residing on premises.

For detailed information on UMS installation scenarios, see the Installation and Sizing Guidelines for IGEL UMS.

The possible network topologies are listed below.

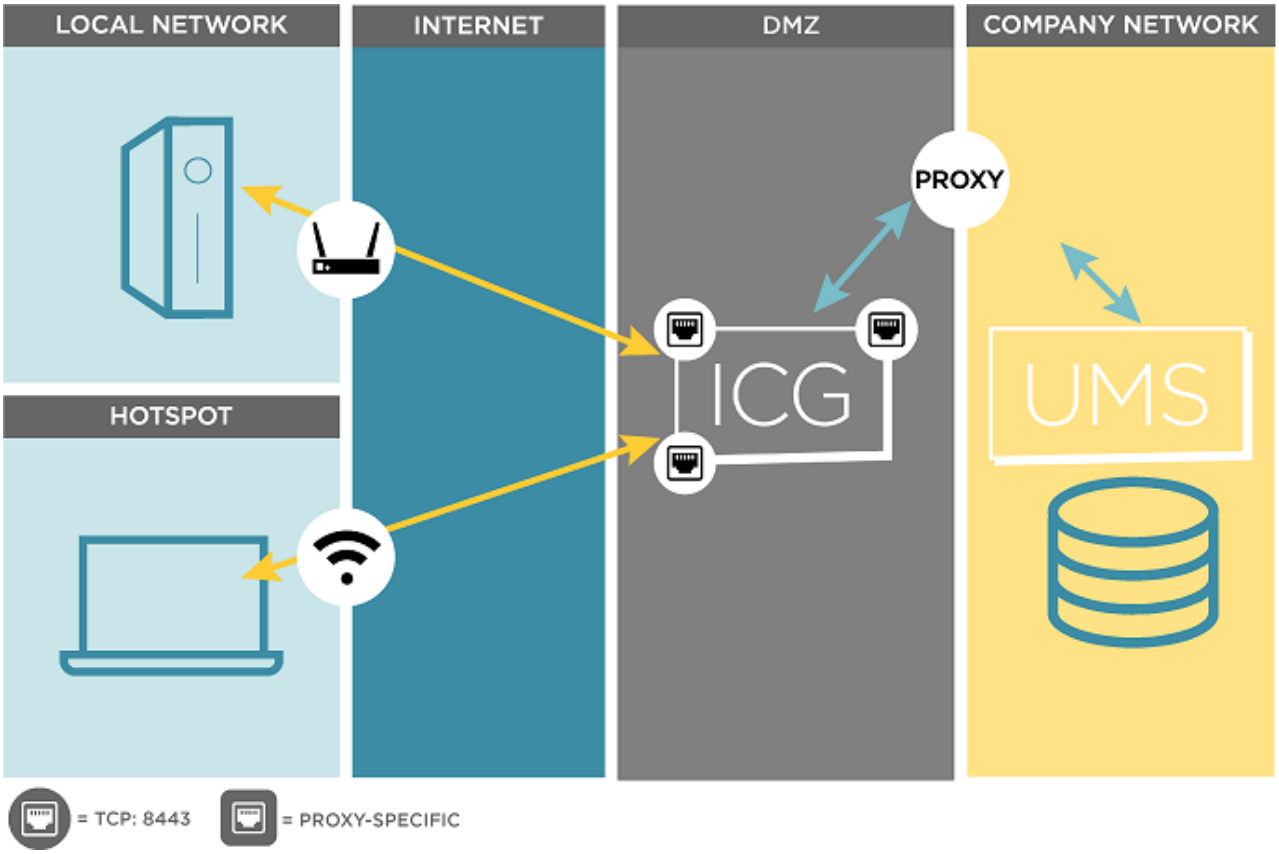
Network Topologies

ICG in the Demilitarized Zone (DMZ) of the Company Network

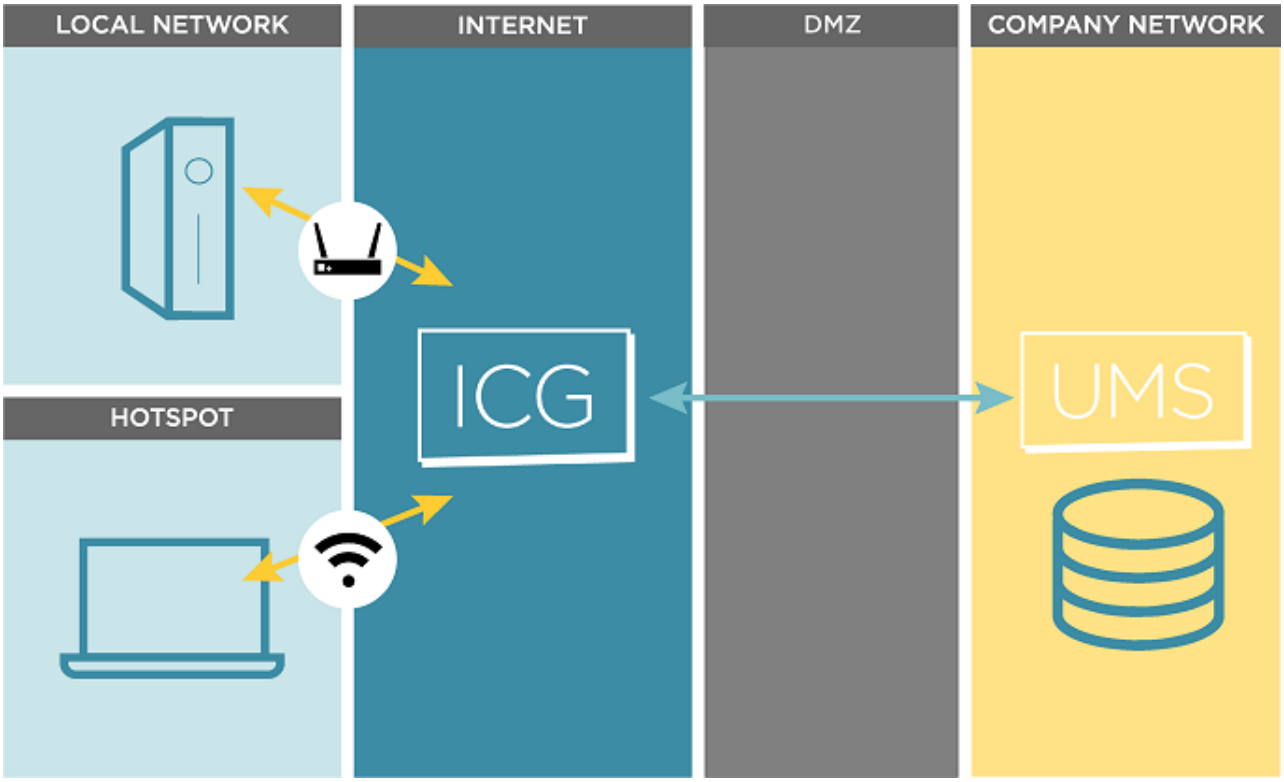


ICG in the Demilitarized Zone (DMZ) of the Company Network and Proxy

This scenario is supported as of UMS version 5.08.

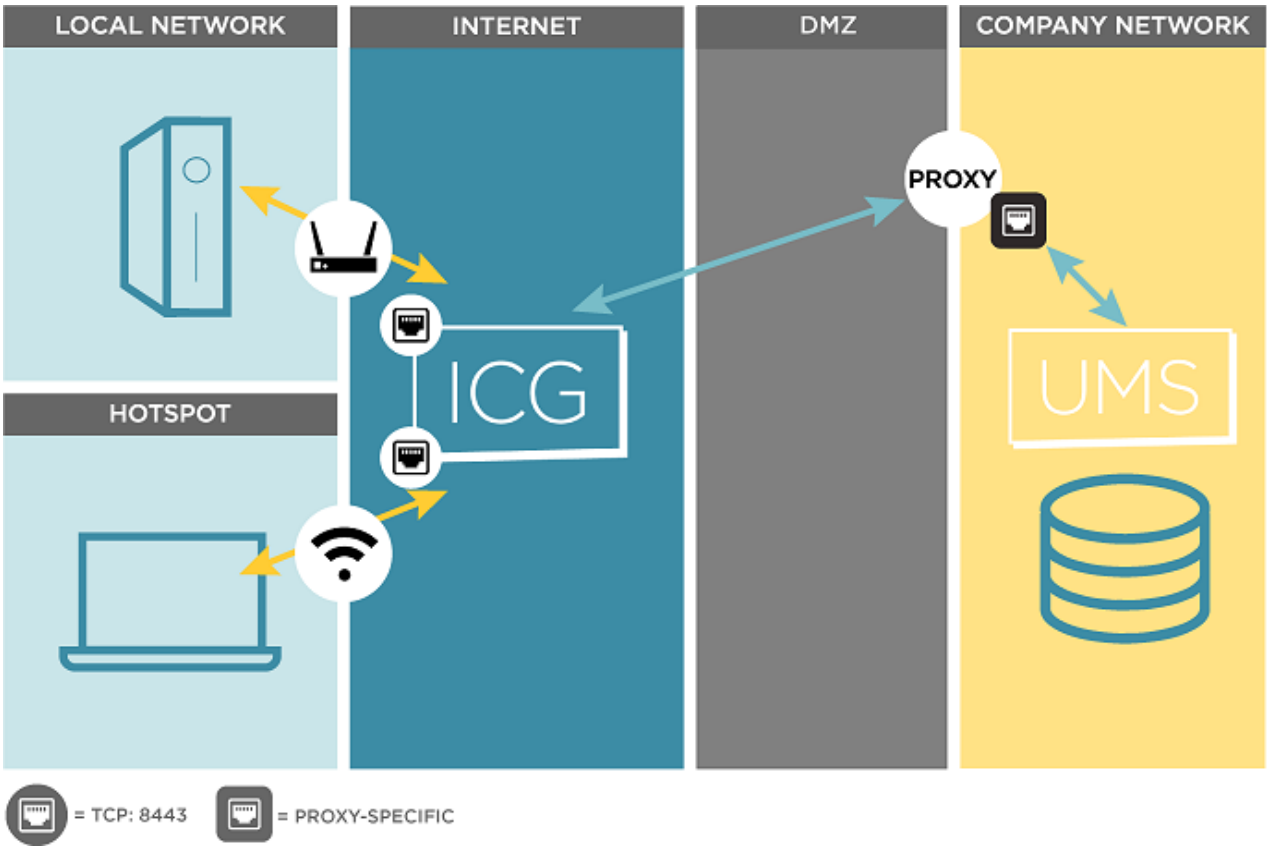


ICG on the Internet (e.g. at a Cloud-Hosting Provider)



ICG on the Internet with Proxy (e.g. at a Cloud-Hosting Provider)

> This scenario is supported as of UMS version 5.08.


LOCAL NETWORK
INTERNET
DMZ
COMPANY NETWORK
PROXY
ICG
UMS
HOTSPOT
= TCP: 8443
= PROXY-SPECIFIC

Limitations

The IGEL Cloud Gateway (ICG) supports all features of the Universal Management Suite (UMS) except the following:

- Universal Firmware Update over the WebDav capability of the UMS; FTP can be used as an alternative. For further information, see Universal Firmware Update.
- Custom Partition over the WebDav capability of the UMS; FTP can be used as an alternative. For further information, see Universal Firmware Update.

Secure Shadowing

Secure shadowing over ICG is supported with UMS 6.03.100 or higher and IGEL OS 11.02.100 or higher.

Secure Terminal

Secure terminal over ICG is supported with UMS 6.04.100 or higher and IGEL OS 11.02.100 or higher.

ICG and TLS Inspection

With ICG version 2.x and UMS version 6.x, it is currently not possible to inspect the TLS traffic between any of the components. The inspection would break TLS and interrupt communication between the products.

Installation and Setup

This article describes the installation and setup of the IGEL Cloud Gateway (ICG).

1. Preparing the machine for ICG installation:
    - Using IGEL Cloud Gateway on Azure Marketplace(see page 93)
    - Preparing a Linux Machine for Installing IGEL Cloud Gateway (ICG)(see page 105) (example of a local machine)
2. Providing the appropriate certificates; see Certificate Requirements and Recommendations for the IGEL Cloud Gateway (ICG)(see page 14). Select one of the following sections, according to your needs and environment:
    - Installing an Existing Certificate Chain(see page 16)
    - Creating Certificates from an Existing Root Certificate(see page 27)
    - Creating a Certificate Using the UMS(see page 35)
3. Installing the IGEL Cloud Gateway using the ICG Remote Installer; see Installing the IGEL Cloud Gateway(see page 40). This is the recommended way; however, it is possible to install the ICG manually; see Installing the ICG without Remote Installer(see page 111).

Providing the Certificates

- Certificate Requirements and Recommendations for the IGEL Cloud Gateway (ICG)(see page 14)
- Installing an Existing Certificate Chain(see page 16)
- Creating Certificates from an Existing Root Certificate(see page 27)
- Creating a Certificate Using the UMS(see page 35)

Certificate Requirements and Recommendations for the IGEL Cloud Gateway (ICG)

For a successful deployment of the IGEL Cloud Gateway (ICG), a certificate chain for communication with the devices must be provided. This certificate chain must meet a few requirements. Also, the validity period of the root certificate should be as long as possible.

Recommendation: Validity Period of the Root Certificate

The validity period of the root certificate should be as long as possible. When the root certificate expires, all certificates must be exchanged, and all devices must be registered again.

Requirement: BasicConstraint for CA Certificates

The root CA certificate and every intermediate CA certificate must be marked as CA certificate as defined in X509v3 extensions: 2.5.29.19. This is the case if the BasicConstraint extension "is_ca" is set to "true". If it is set to "false", the certificate can not be used for signing other certificates.

Requirement: If a CA Counter Exists, It Must Be Set Correctly

Some CA certificates have a CA counter, which is defined in X509v3 extensions: 2.5.29.19. The CA counter describes how many members can be added to the certificate chain. If, for instance, the CA counter of the current certificate is 1, it is possible to sign a certificate with which one further certificate can be signed. The CA counter of this certificate is 0, so it can only sign end certificates.

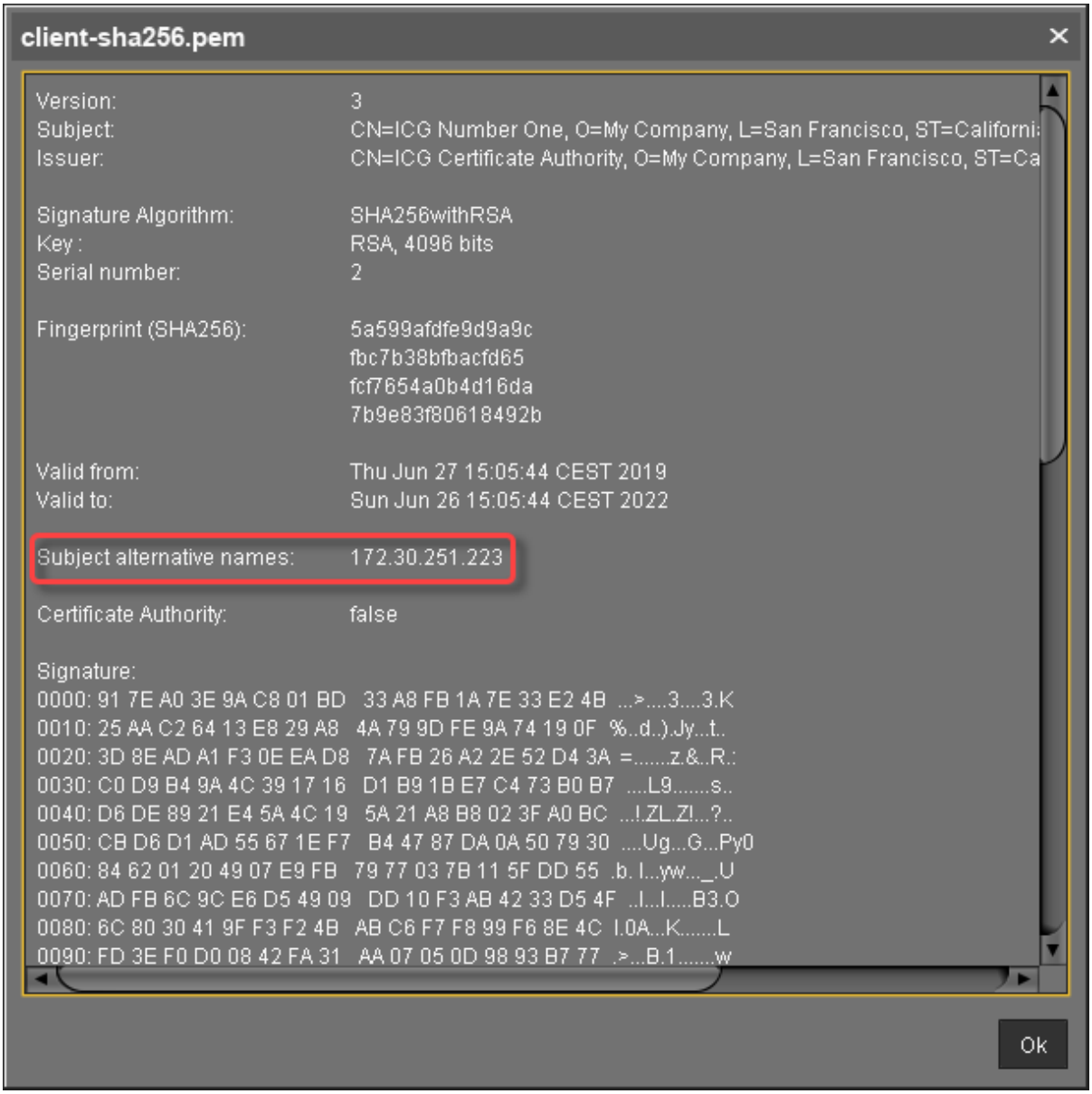
With UMS 6.02 or higher, you can review the CA counter of a certificate by selecting the context menu and then selecting **Show certificate content**.

Requirement: End Certificate Must Be Marked and Provide Correct Subject Alternative Name

The certificate which is to be installed on the IGEL Cloud Gateway must be marked as the end certificate.

The end certificate must have a Subject Alternative Name (X509v3 extensions 2.5.29.17) that contains all hostnames or IP addresses via which the UMS and the devices will contact the IGEL Cloud Gateway.

With UMS 6.02 or higher, you can check this by selecting the context menu and then selecting **Show certificate content**. The certificate content view should look similar to this:


client-sha256.pem
Version: 3
Subject: CN=ICG Number One, O=My Company, L=San Francisco, ST=Californi
Issuer: CN=ICG Certificate Authority, O=My Company, L=San Francisco, ST=Ca
Signature Algorithm: SHA256withRSA
Key : RSA, 4096 bits
Serial number: 2
Fingerprint (SHA256): 5a599afdfe9d9a9c fbc7b38bfbacfd65 fcf7654a0b4d16da 7b9e83f80618492b
Valid from: Thu Jun 27 15:05:44 CEST 2019
Valid to: Sun Jun 26 15:05:44 CEST 2022
Subject alternative names: 172.30.251.223
Certificate Authority: false
Signature:
0000: 91 7E A0 3E 9A C8 01 BD 33 A8 FB 1A 7E 33 E2 4B ...>....3....3.K
0010: 25 AA C2 64 13 E8 29 A8 4A 79 9D FE 9A 74 19 0F %..d..).Jy...t..
0020: 3D 8E AD A1 F3 0E EA D8 7A FB 26 A2 2E 52 D4 3A =.....z.&..R.:
0030: C0 D9 B4 9A 4C 39 17 16 D1 B9 1B E7 C4 73 B0 B7 ....L9.....s..
0040: D6 DE 89 21 E4 5A 4C 19 5A 21 A8 B8 02 3F A0 BC ...!.ZL.Z!...?..
0050: CB D6 D1 AD 55 67 1E F7 B4 47 87 DA 0A 50 79 30 ....Ug...G...Py0
0060: 84 62 01 20 49 07 E9 FB 79 77 03 7B 11 5F DD 55 .b. I...yw..._.U
0070: AD FB 6C 9C E6 D5 49 09 DD 10 F3 AB 42 33 D5 4F ..l...I.....B3.O
0080: 6C 80 30 41 9F F3 F2 4B AB C6 F7 F8 99 F6 8E 4C l.0A...K.....L
0090: FD 3E F0 D0 08 42 FA 31 AA 07 05 0D 98 93 B7 77 .>...B.1.....w
Ok

Installing an Existing Certificate Chain

Overview

You can use a certificate chain that is already used in your working environment. The certificate chain must contain a root CA certificate and an end certificate and may contain one or more intermediate CA certificates.

To make sure that your certificates can be used by your IGEL Cloud Gateway installation, see Certificate Requirements and Recommendations for the IGEL Cloud Gateway (ICG)(see page 14).

In the example described here, the following certificate chain is used:

- Root certificate
- Intermediate CA certificate
- End certificate

When the certificate chain is in place, you can continue with Installing the IGEL Cloud Gateway(see page 40).

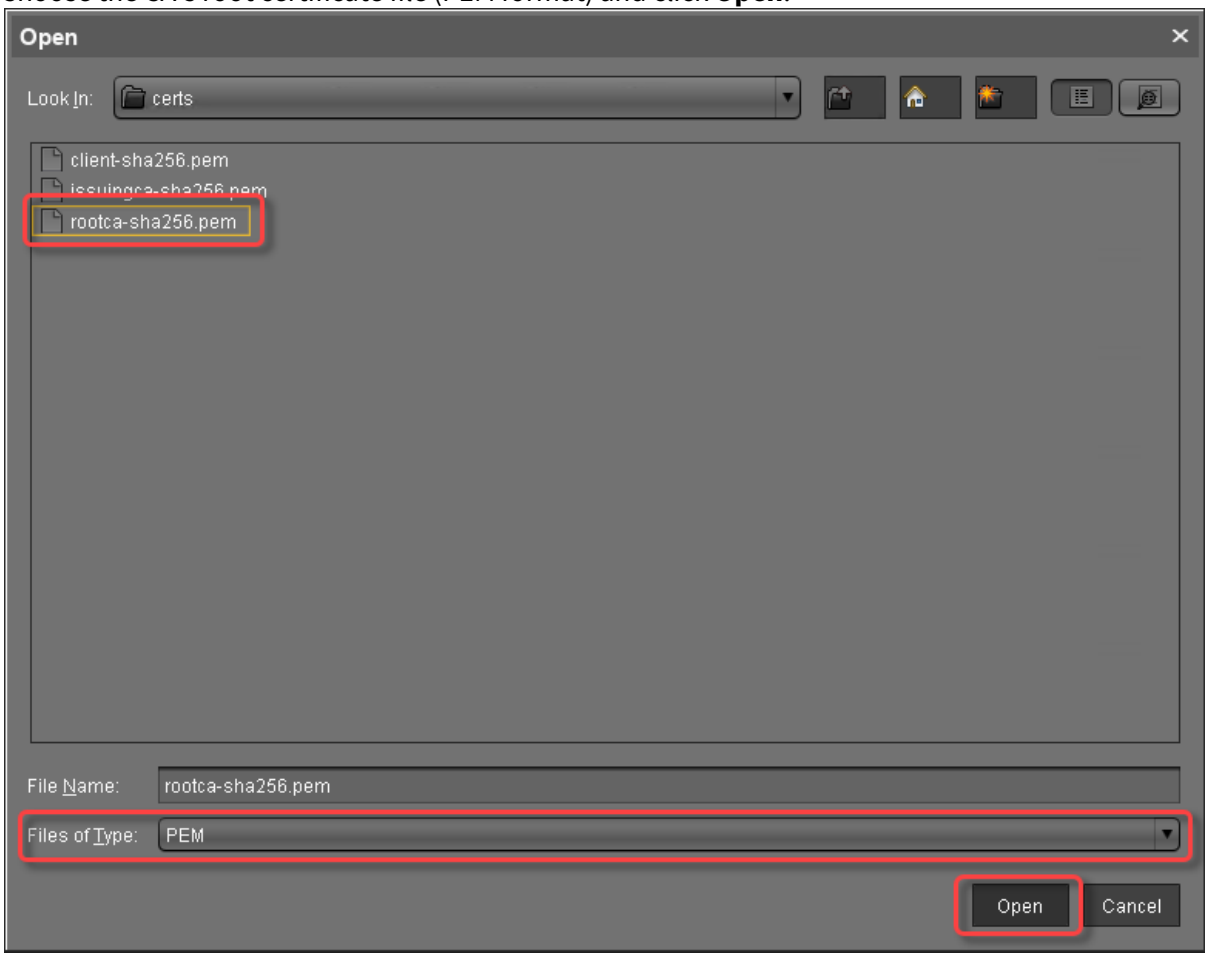
With UMS 6.03 or higher, you can use the ICG remote installer for installing certificates. This procedure is described here. For the procedure with UMS 6.02 or lower, see the how-to Installing an Existing Certificate Chain (UMS 6.02 or Older)(see page 127).

Importing the Root Certificate

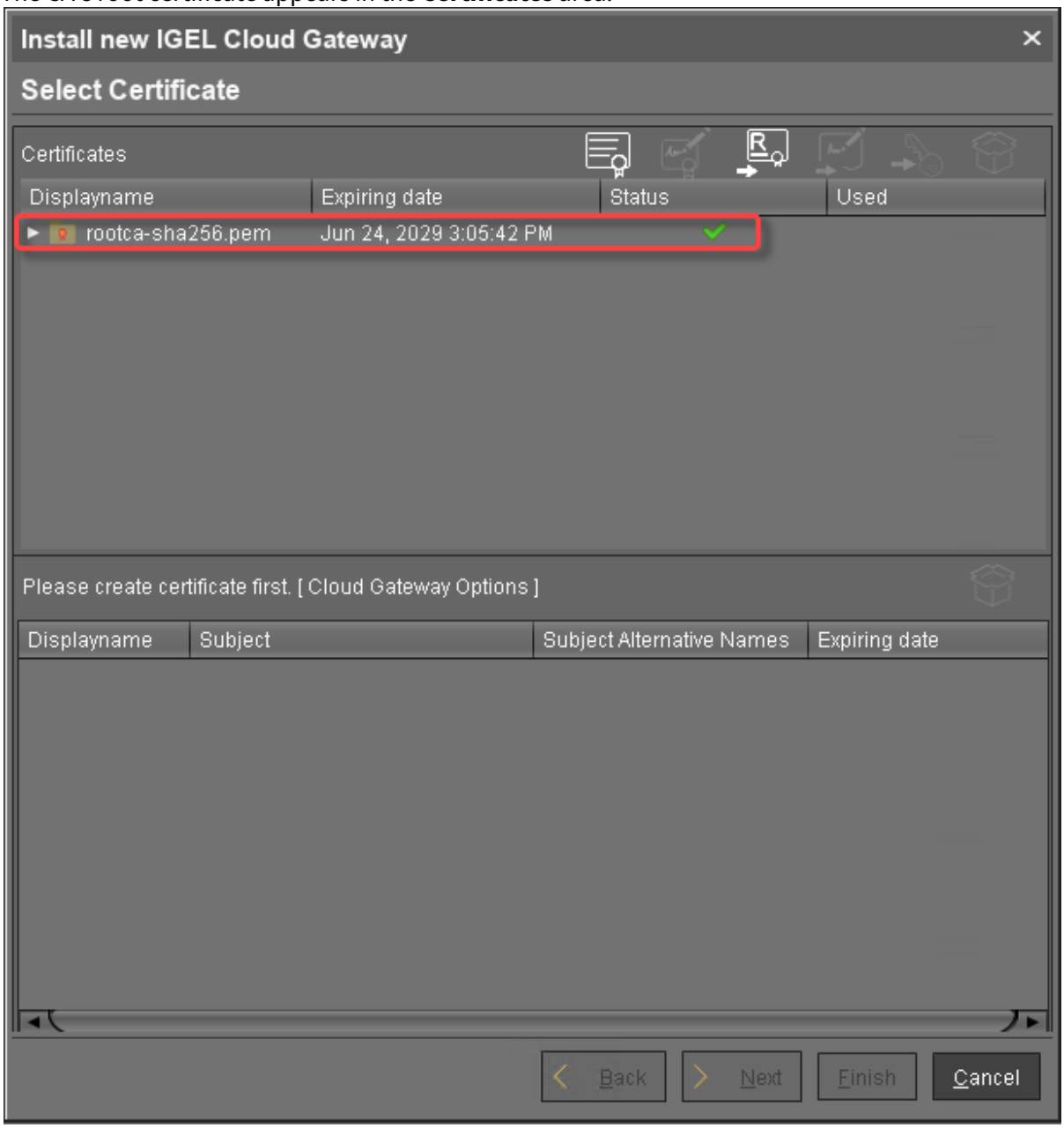
> The validity period of the root certificate should be as long as possible. When the root certificate expires, all certificates must be exchanged, and all devices must be registered anew.

1. In the UMS Console, go to **UMS Administration > UMS Network > Igel Cloud Gateway**.
2. In the toolbar in the upper right, click the icon (**Install new IGEL Cloud Gateway**).
3. The ICG remote installer opens. Any existing ICG certificates are shown in the **Certificates** area.
4. Click to import the root certificate.

5. Choose the CA's root certificate file (PEM format) and click **Open**.



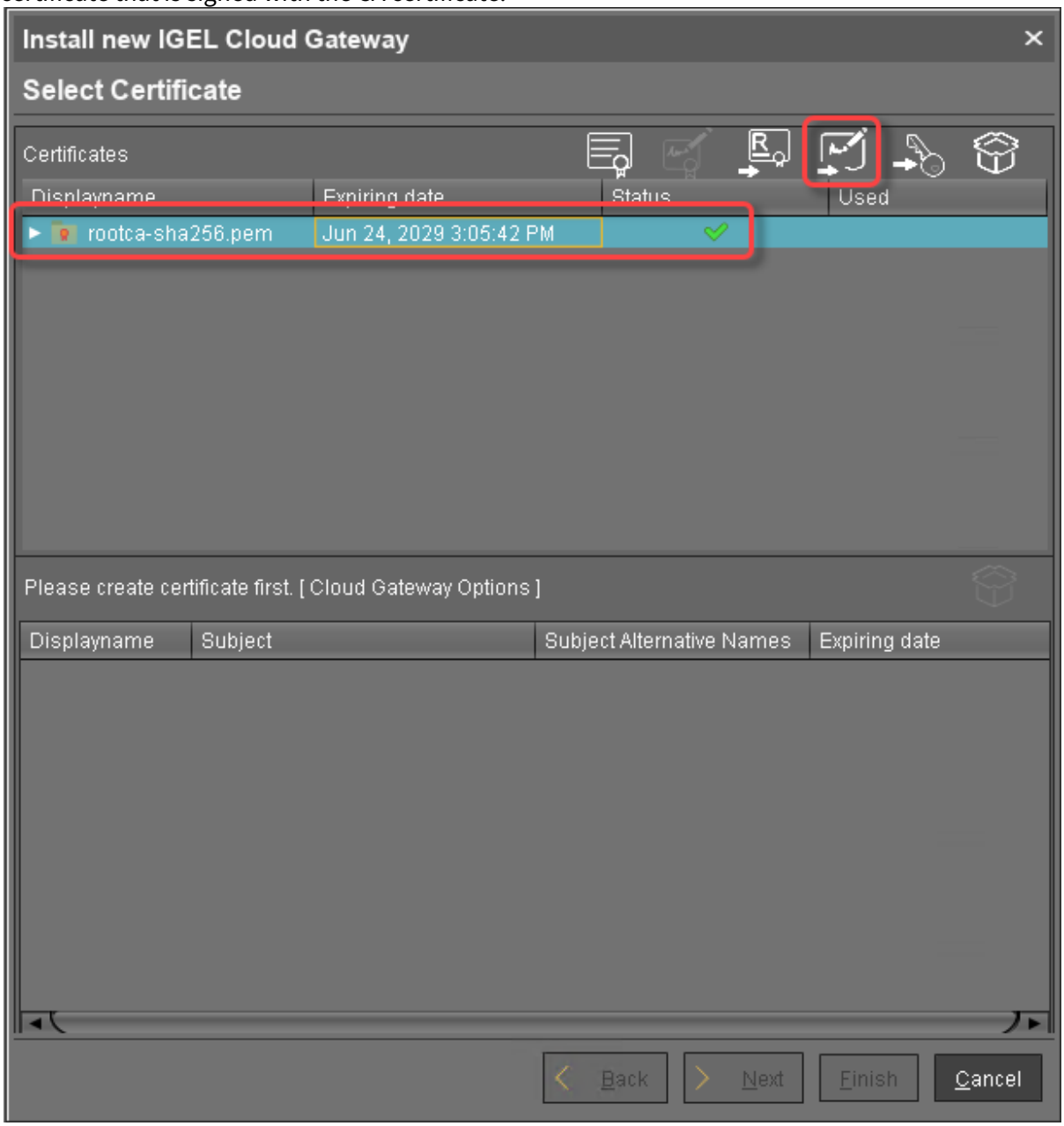
The CA's root certificate appears in the **Certificates** area.



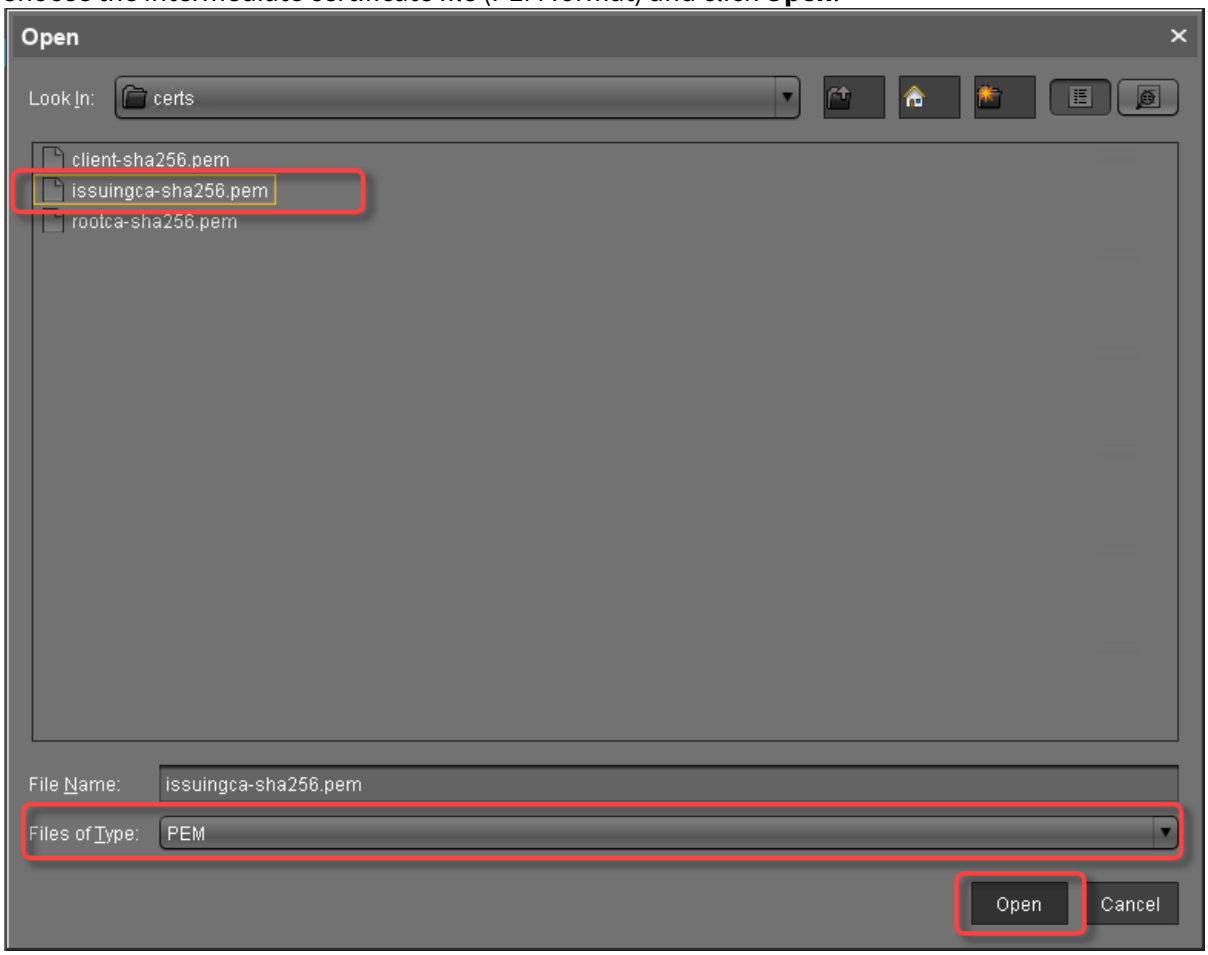
6. Continue by importing the intermediate certificate.

Importing the Intermediate Certificate

1. In the ICG remote installer, select the CA certificate and click to import the intermediate certificate that is signed with the CA certificate.

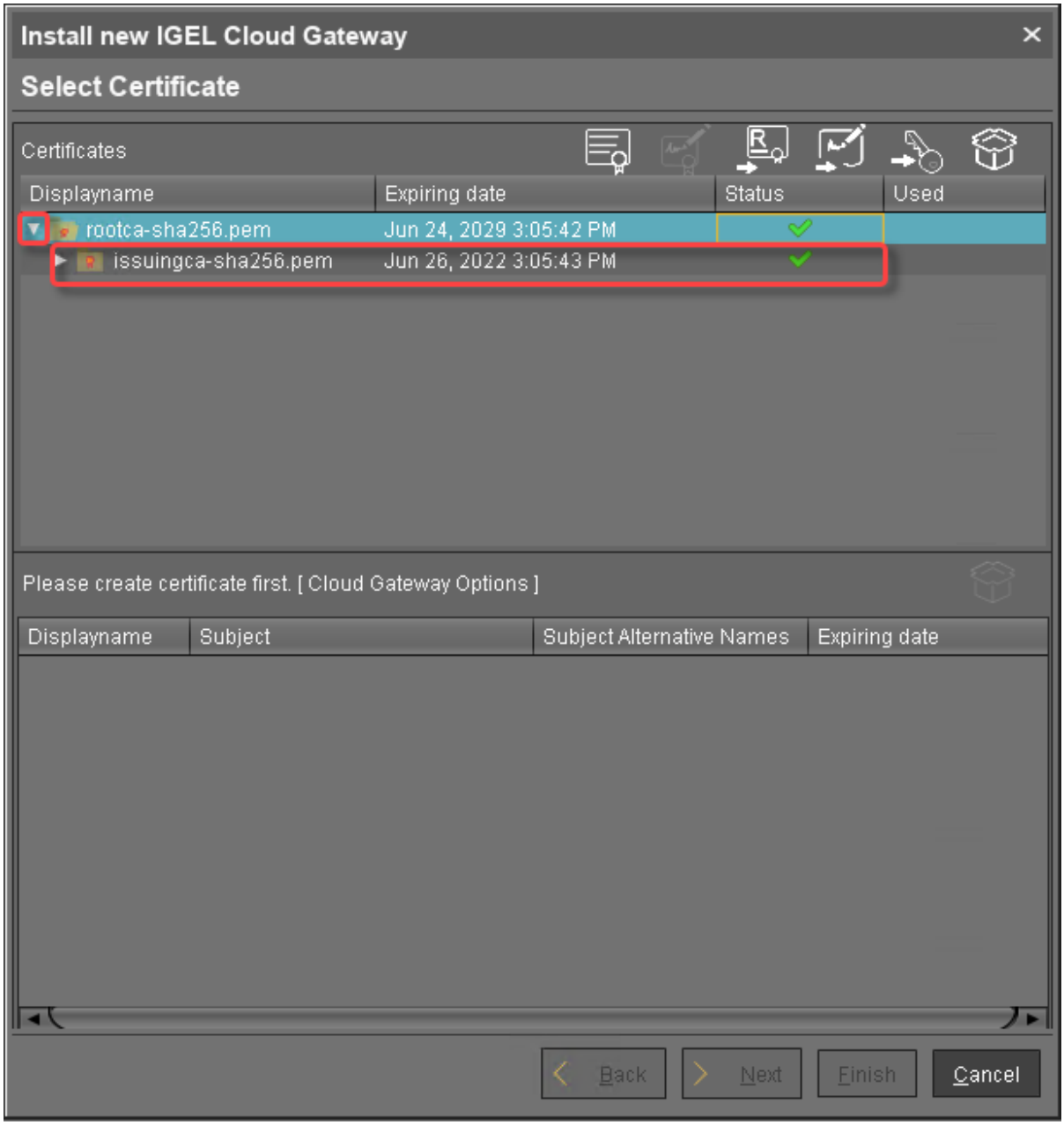


2. Choose the intermediate certificate file (PEM format) and click **Open**.



When you click the arrow next to the root certificate, the intermediate certificate appears in the

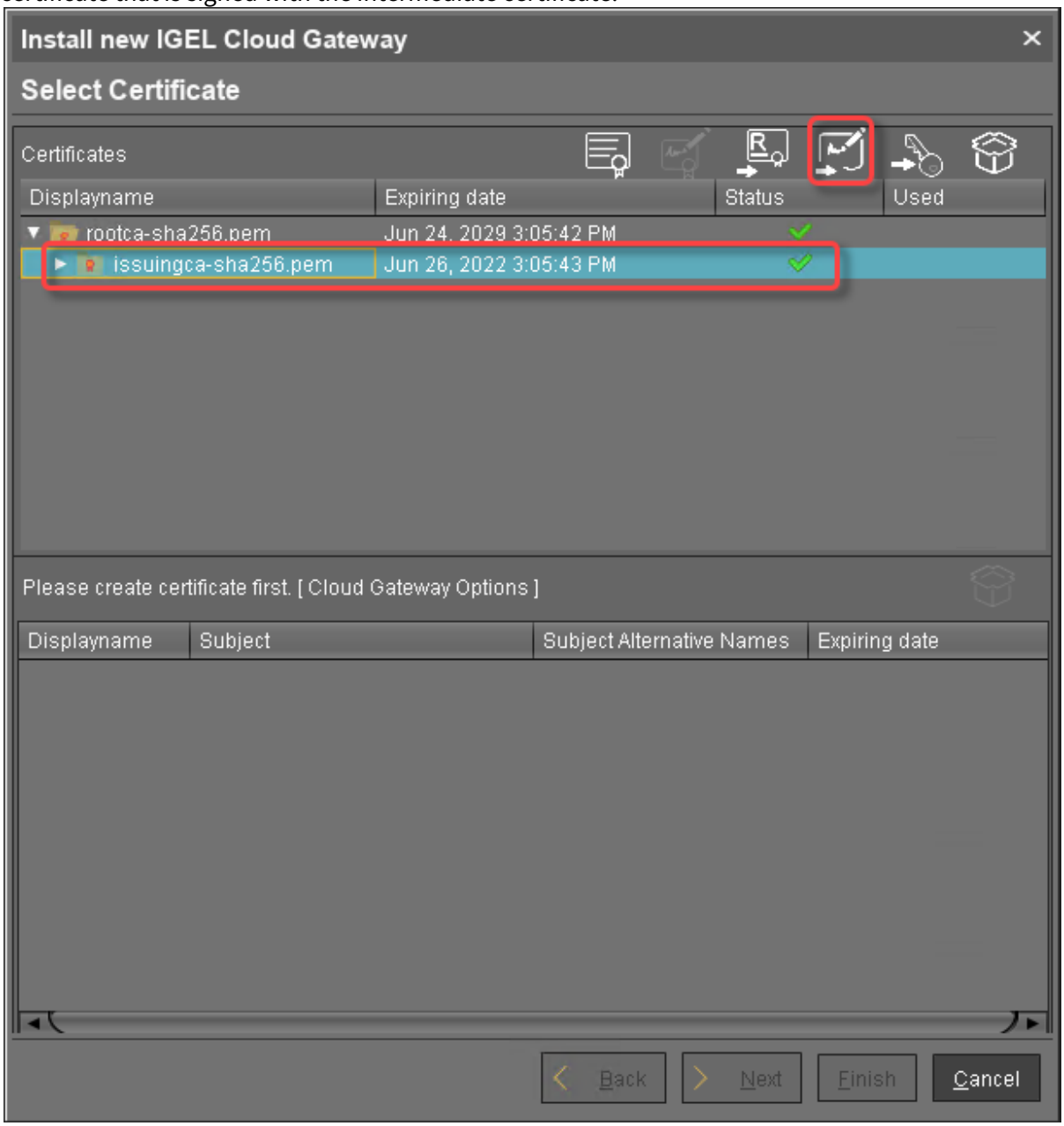
list.



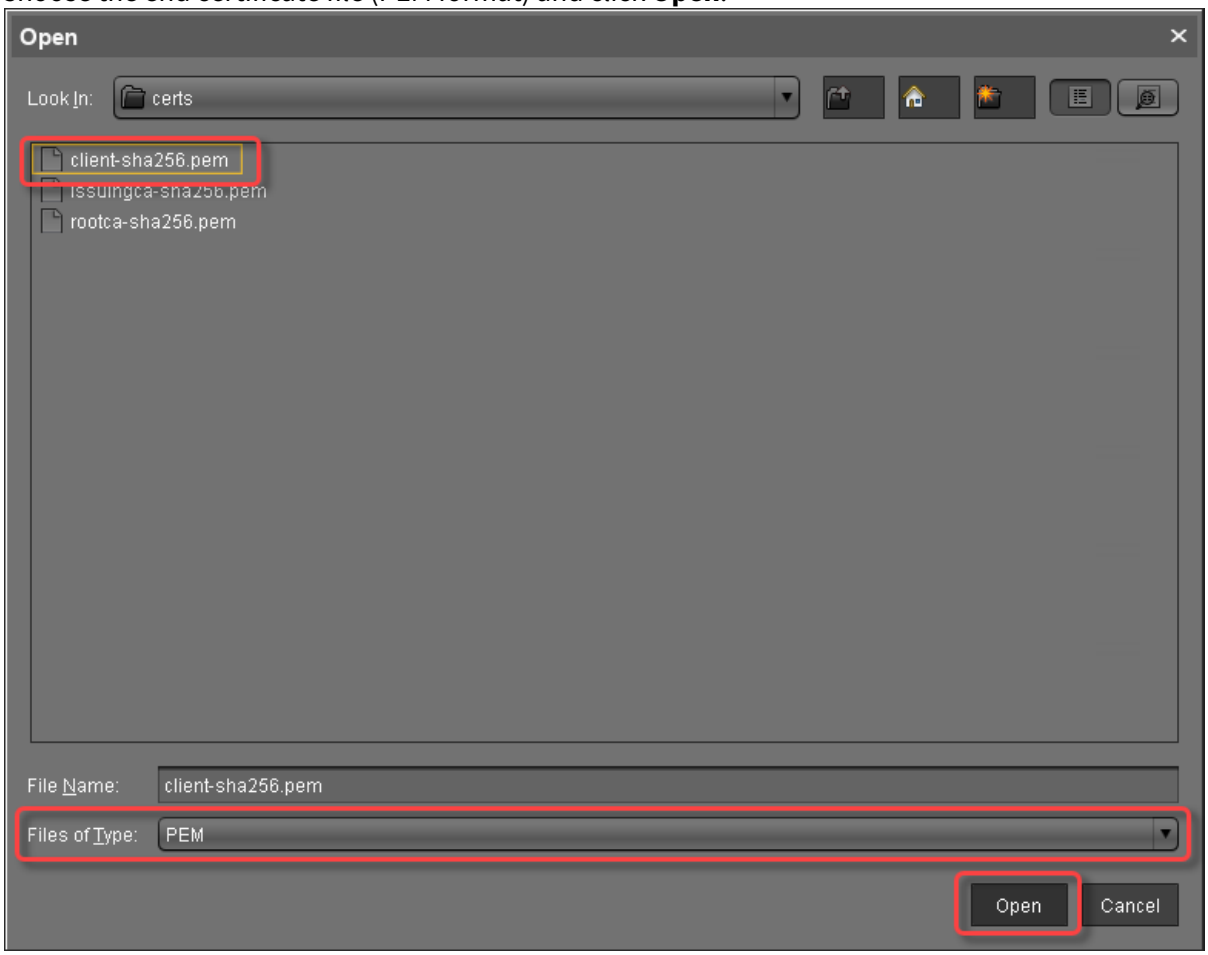
3. Continue by importing the end certificate.

Importing the End Certificate

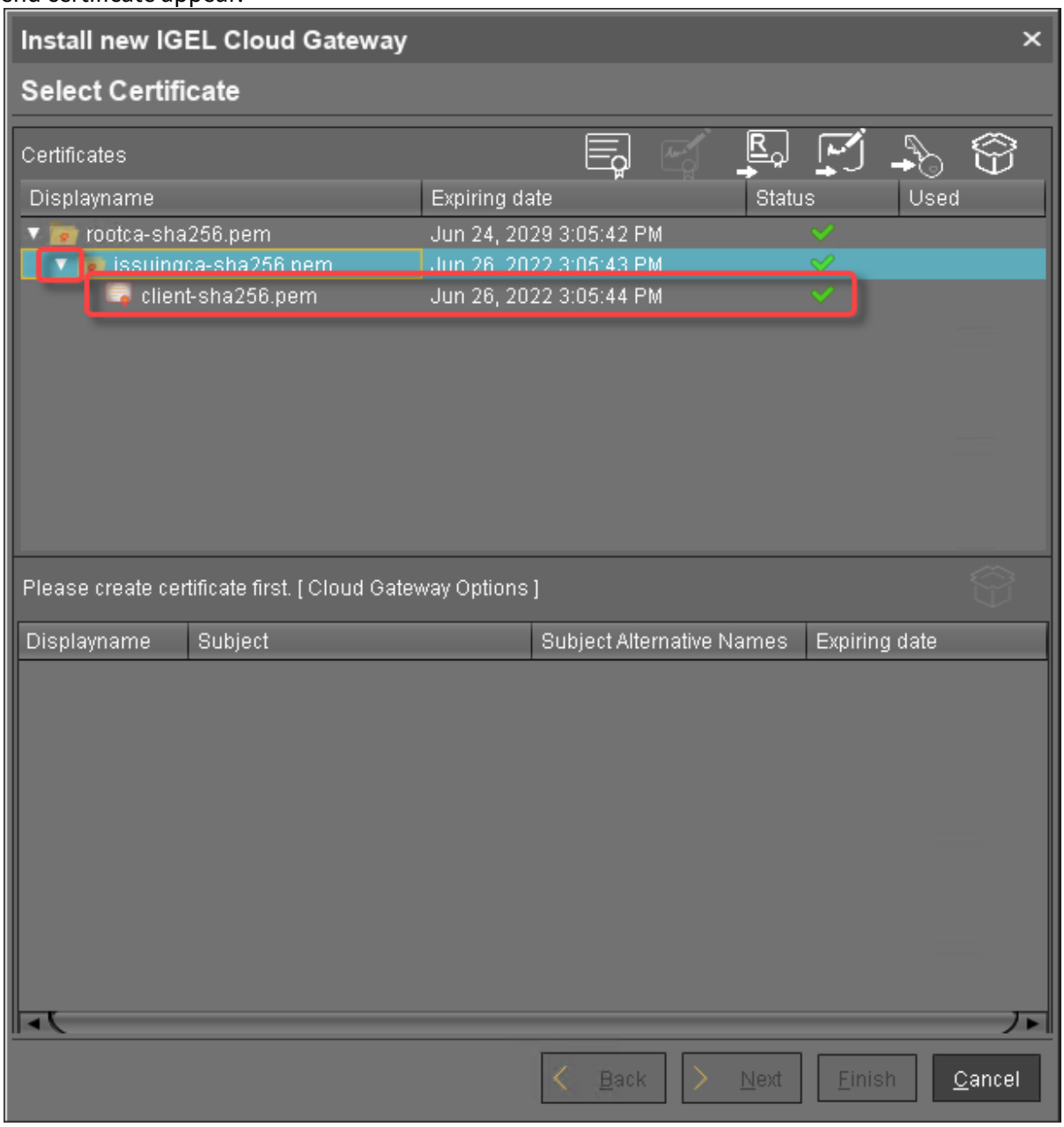
1. In the ICG remote installer, select the intermediate certificate and click to import the end certificate that is signed with the intermediate certificate.



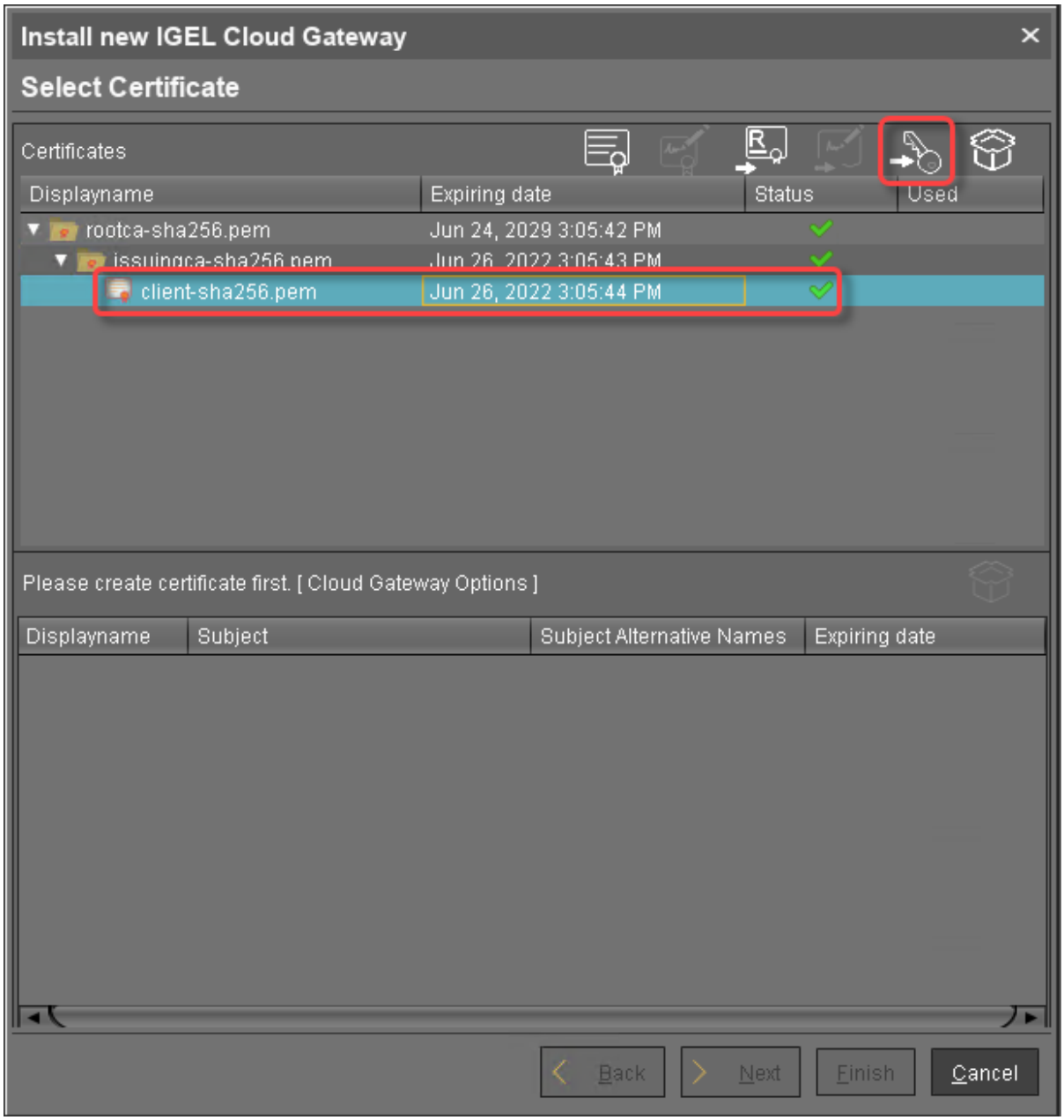
2. Choose the end certificate file (PEM format) and click **Open**.



3. Click the arrow symbol of the intermediate certificate nearest to the end certificate to make the end certificate appear.

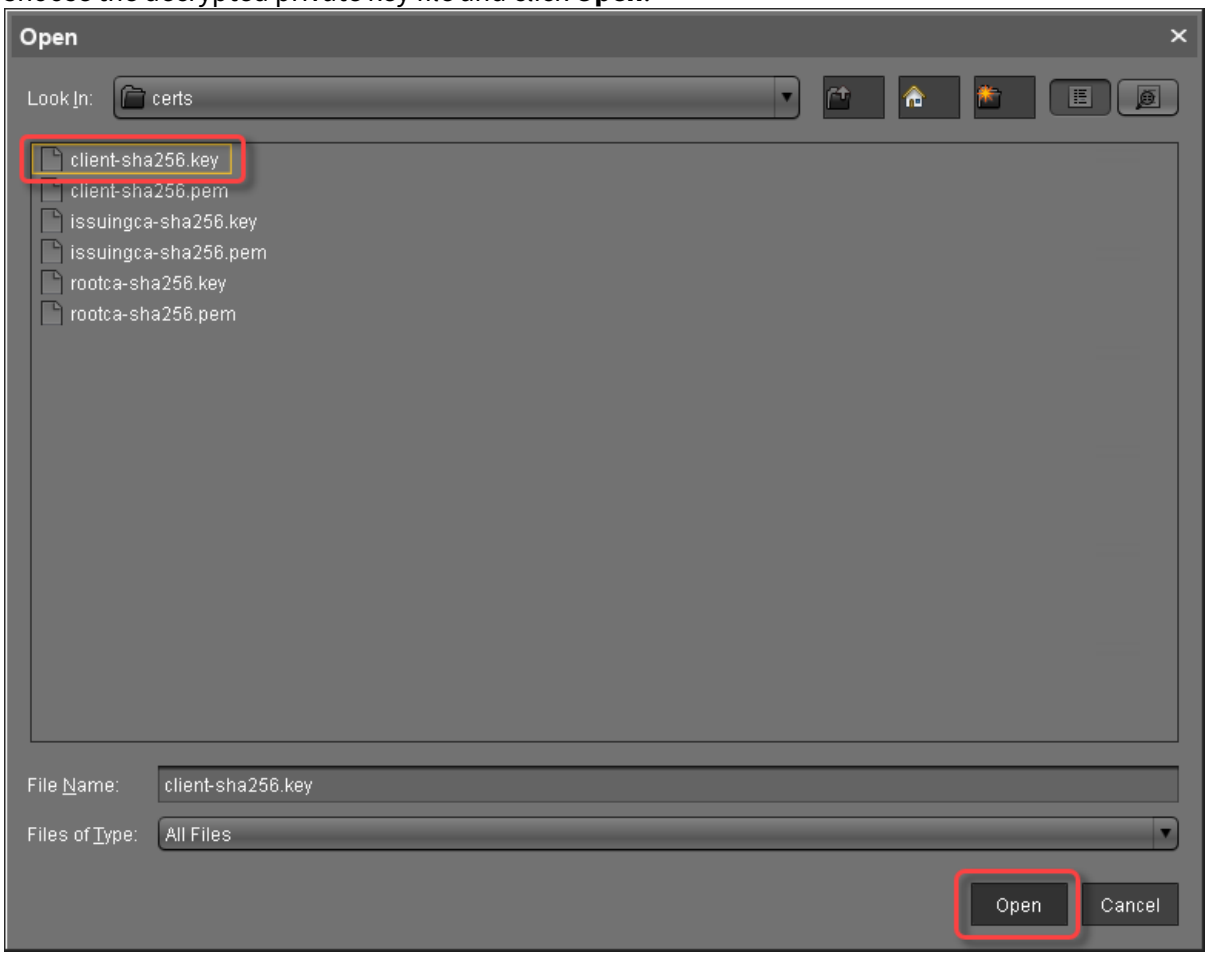


4. Select the end certificate and click to import the decrypted private key.

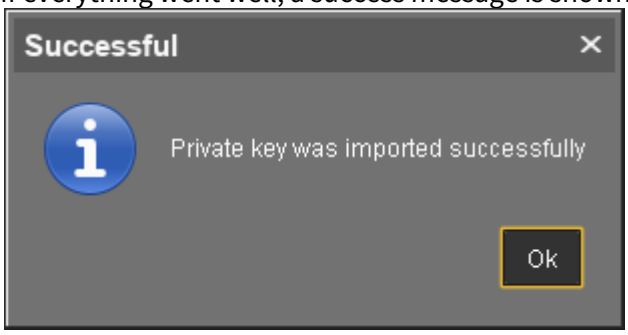


> ⓘ If the private key is protected with a passphrase, you need to decrypt it using the OpenSSL command line tool: `openssl rsa -in encrypted.key -out decrypted.key`

5. Choose the decrypted private key file and click **Open**.



If everything went well, a success message is shown.



6. Continue with Installing the IGEL Cloud Gateway(see page 40).

Creating Certificates from an Existing Root Certificate

Required Certificate Files

The following files are required:

- CA certificate
- CA private key

> If you need to export the CA signing root certificate and key from a Microsoft CA server, you can follow this document from Cisco: How do I export and convert a pfx CA root certificate and key from a Microsoft CA server[2]

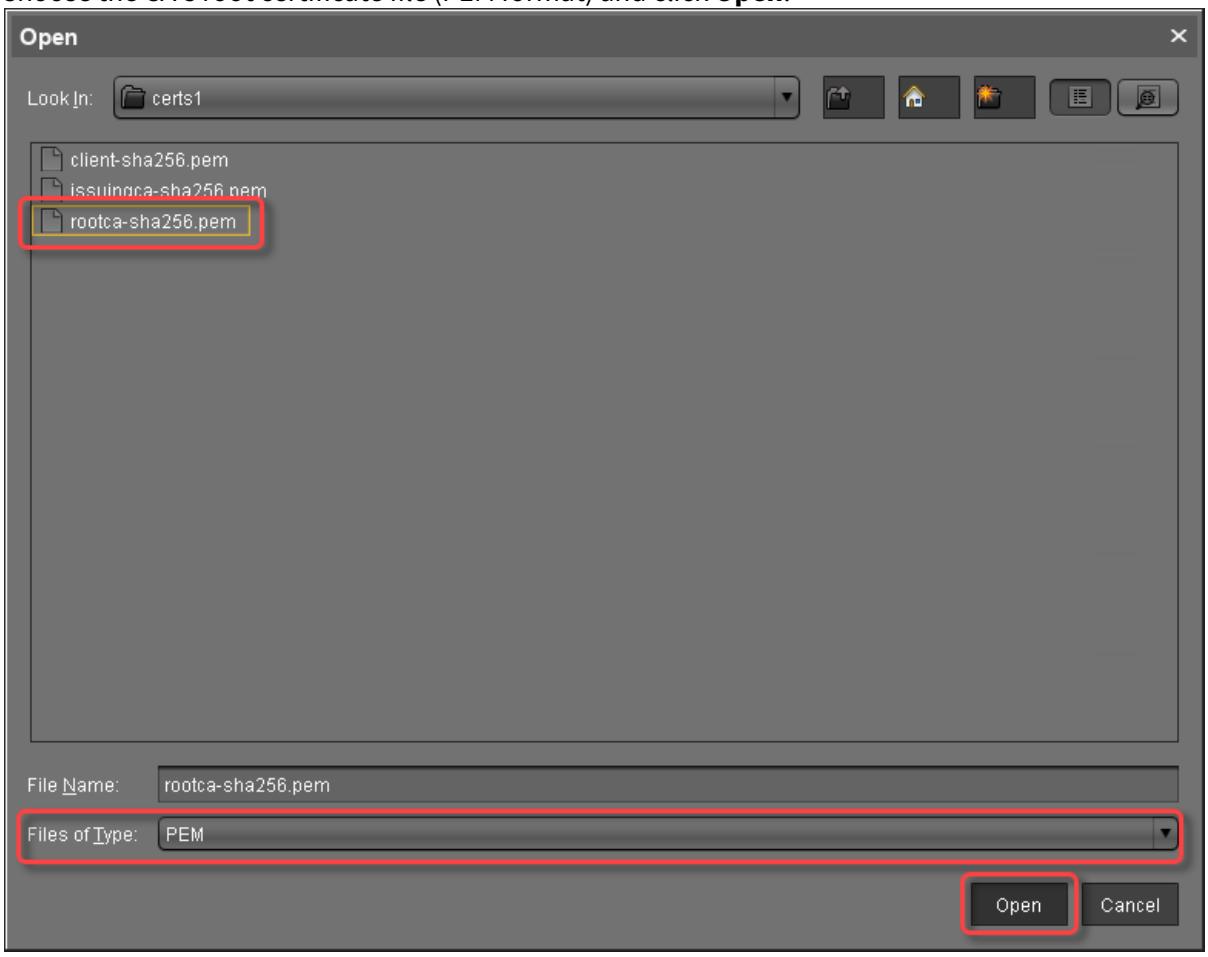
With UMS 6.03 or higher, you can use the ICG remote installer for installing and creating certificates. This procedure is described here. For the procedure with UMS 6.02 or lower, see the how-to Creating Certificates from an Existing Root Certificate (UMS 6.02 or Older)(see page 133).

Importing Your Existing Private CA Files into the UMS

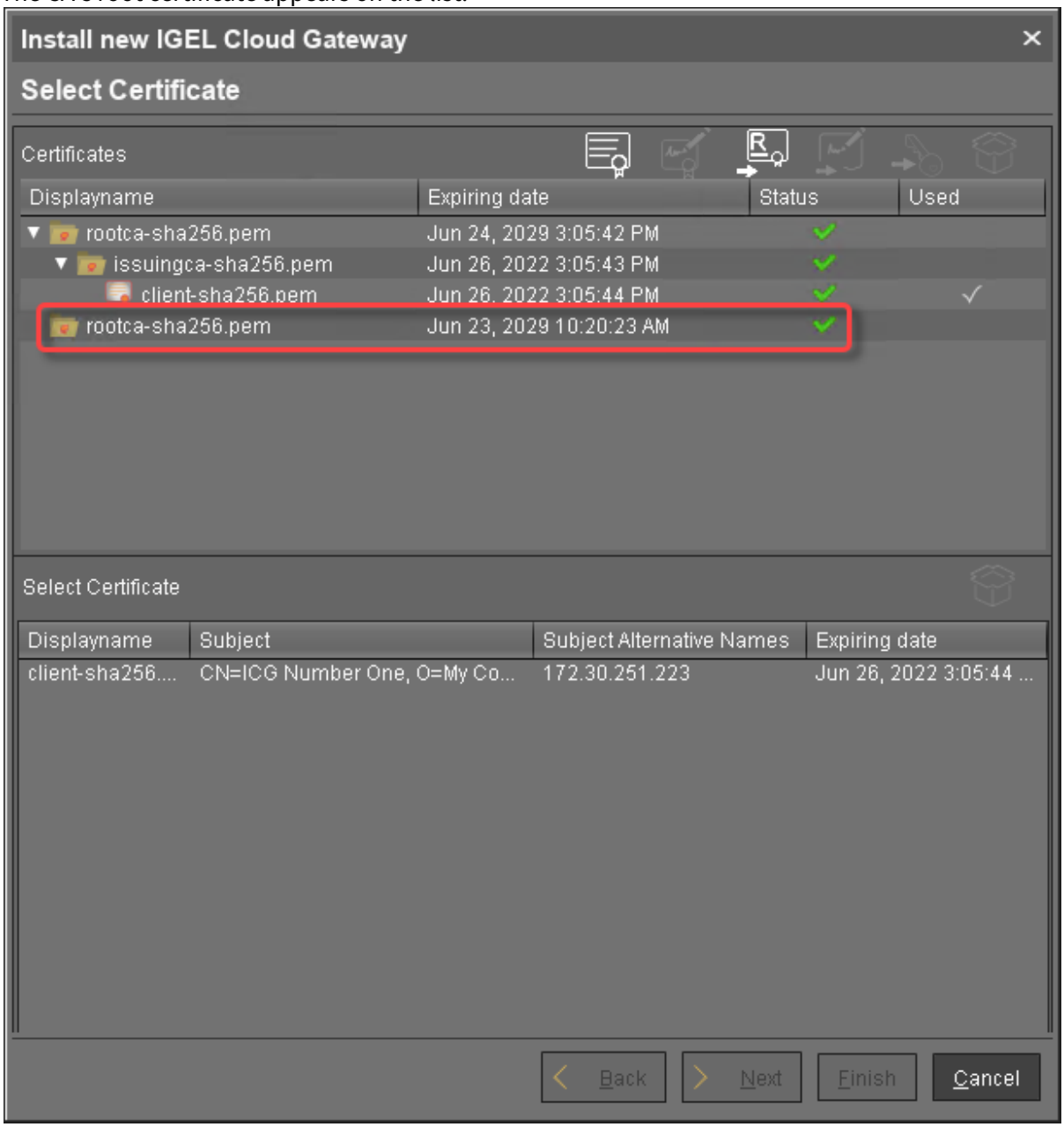
1. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.
2. In the toolbar in the upper right, click the icon (**Install new IGEL Cloud Gateway**).
3. The ICG remote installer opens. Any existing ICG certificates are shown in the **Certificates** area.
4. Click to import the root certificate.

2 http://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html

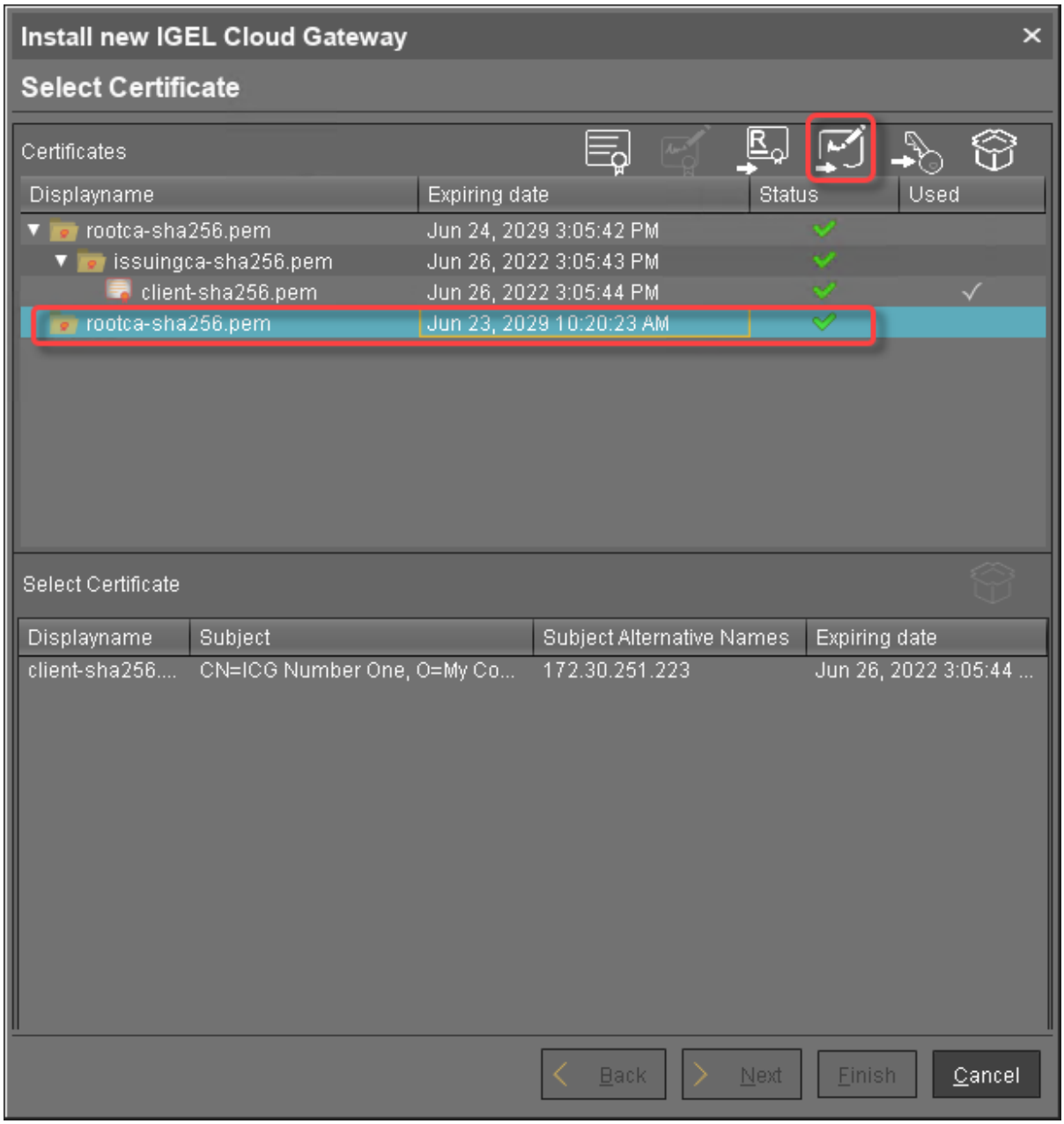
5. Choose the CA's root certificate file (PEM format) and click **Open**.



The CA's root certificate appears on the list.

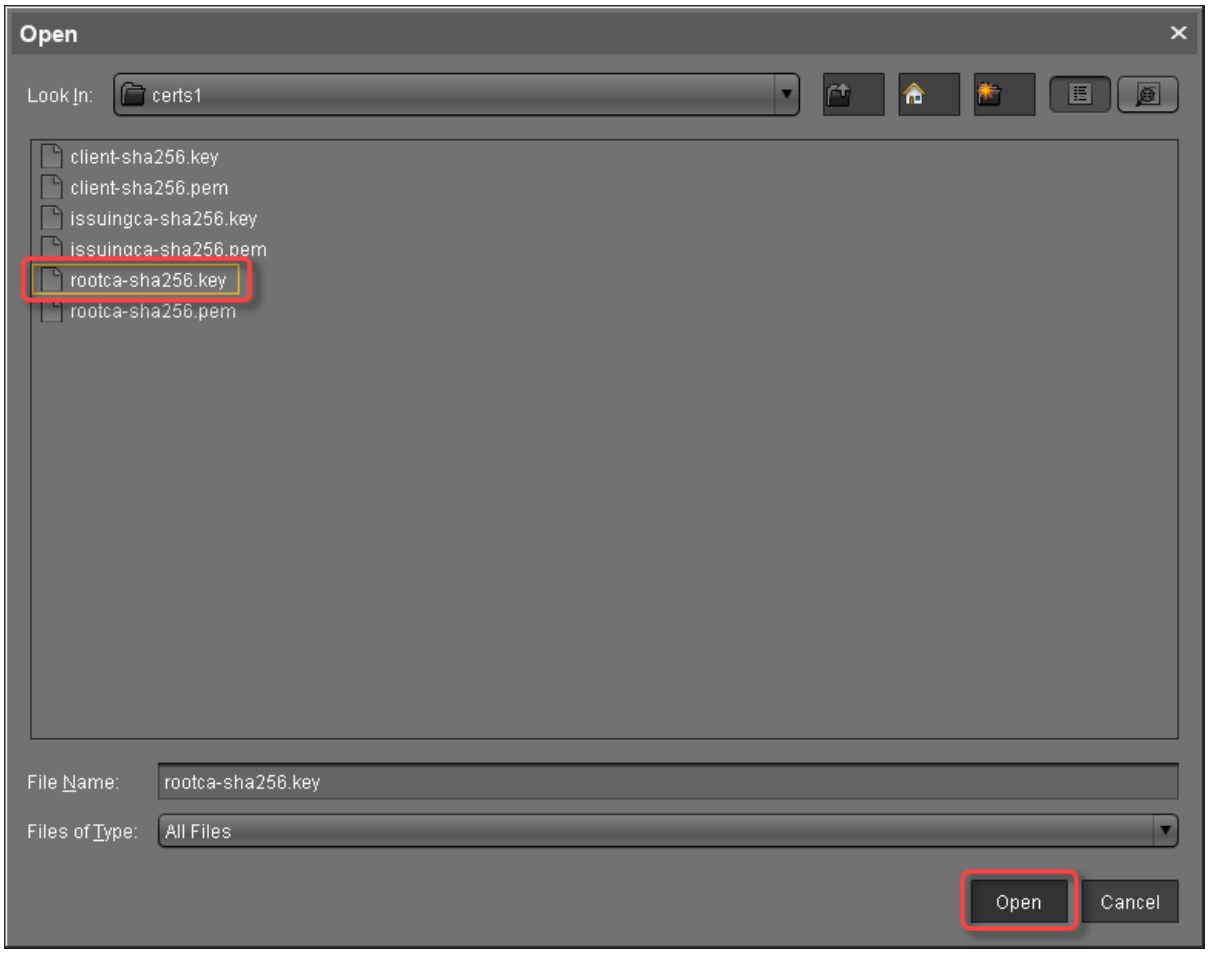


6. Select the CA certificate and click to import the decrypted private key for the CA certificate.

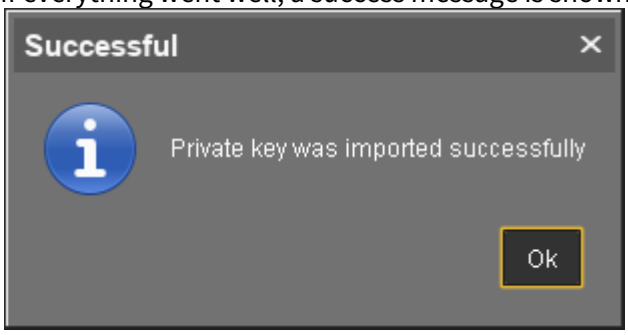


> ⓘ If the private key is protected with a passphrase, you need to decrypt it using the OpenSSL command line tool: `openssl rsa -in encrypted.key -out decrypted.key`

7. Choose the decrypted private key file for the CA certificate and click **Open**.



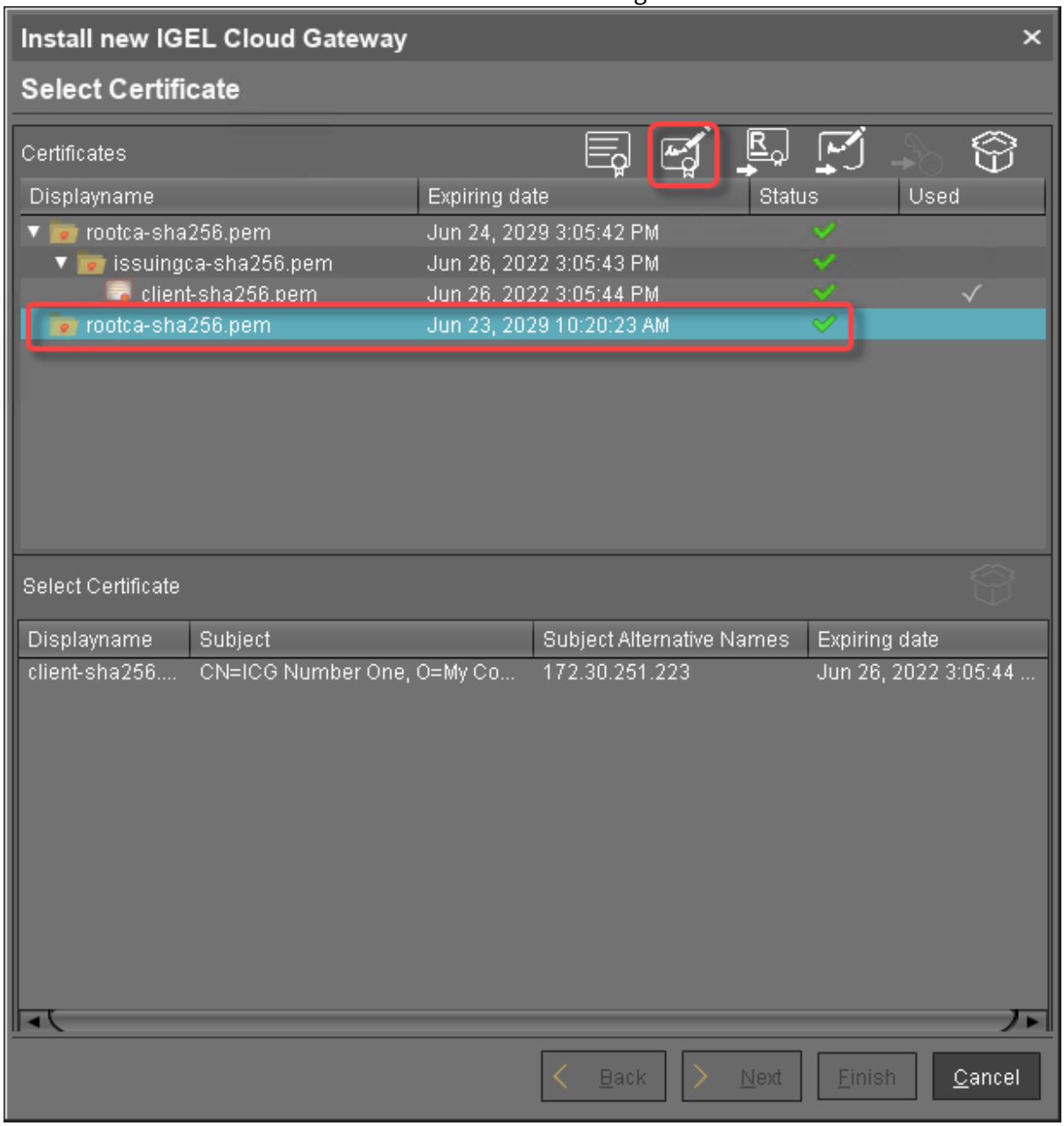
If everything went well, a success message is shown.



8. Continue by creating a signed certificate.

Creating a Signed Certificate

1. Select the CA's root certificate and click to create a signed certificate.

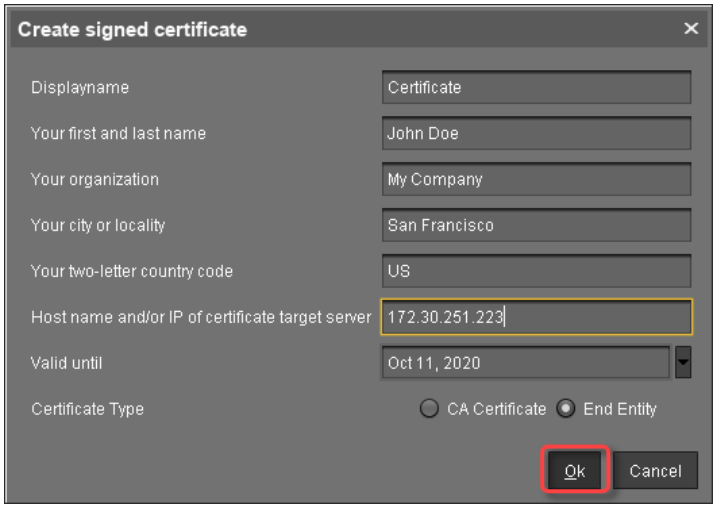


2. Fill in the certificate fields:
   - **Display name**: Name of the certificate
   - **Your first and last name**: Name of the certificate holder
   - **Your organization**: Organization or company name
   - **Your city or locality**: Location
   - **Your two-letter country code**: ISO 3166 country code, e.g. `US`, `UK` or `ES`
   - **Hostname and/or IP address of certificate target server**: Hostname(s) or IP address(es) for which the certificate is valid. Multiple entries are allowed, separated by semicolons.

> All IP addresses and hostnames by which the ICG will be reachable from within the company network or from outside must be provided here.

- **Valid until**: Local date on which this certificate expires. (Default: one year from now)
- **Certificate Type**: Select "End Entity".

3. Click **OK**.

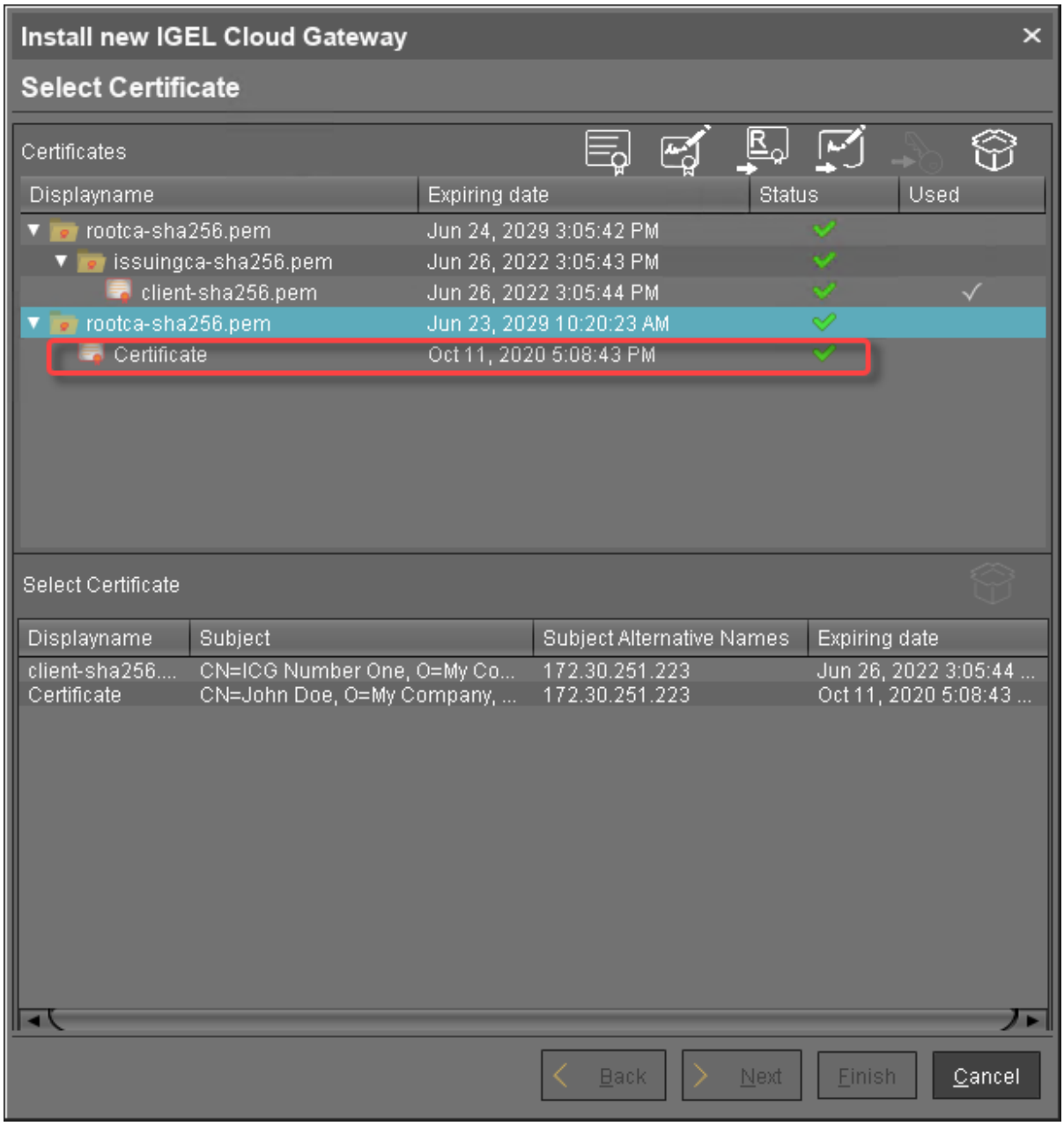


A key pair and a certificate are generated.

> Generating keys may take substantial time on virtual machines (VMs), as these do not have a powerful (pseudo) random number source. On Linux VMs, this can be improved by installing the haveged[3] package.

3 http://www.issihosts.com/haveged/

The signed certificate appears on the list.



4. Continue with Installing the IGEL Cloud Gateway(see page 40).

Creating a Certificate Using the UMS

To install the IGEL Cloud Gateway (ICG), you must provide a signed certificate. In order to generate a signed certificate, a root certificate must be generated first.

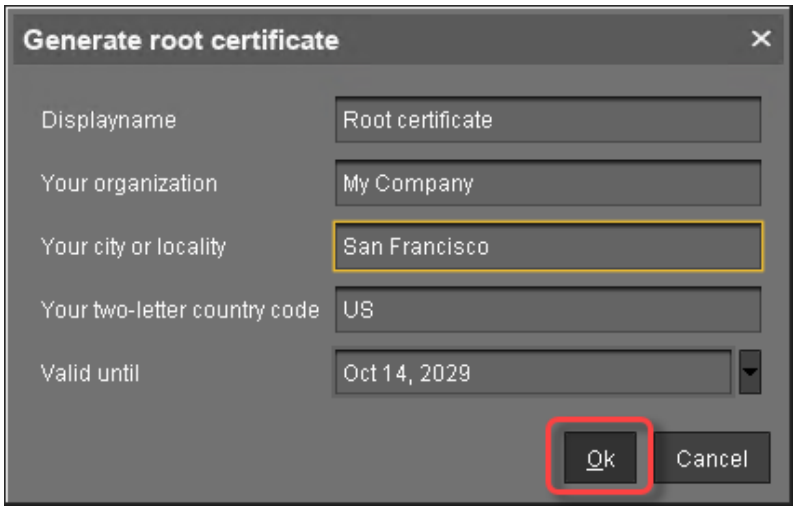
With UMS 6.03 or higher, you can use the ICG remote installer for creating certificates. This procedure is described here. For the procedure with UMS 6.02 or lower, see the how-to Creating Certificates from an Existing Root Certificate (UMS 6.02 or Older)(see page 133).

Creating the Root Certificate

1. In the UMS Console, go to **UMS Administration > UMS Network > Igel Cloud Gateway**.
2. In the toolbar in the upper right, click the icon (**Install new IGEL Cloud Gateway**).
3. The ICG remote installer opens. Any existing ICG certificates are shown in the **Certificates** area.
4. Click to generate a root certificate.
5. Fill in the certificate fields:
   - **Displayname**: Name for the certificate; free text entry
   - **Your organization**: Organization or company name
   - **Your city or locality**: Location
   - **Your two-letter country code**: ISO 3166 country code, e.g. `US`, `UK` or `ES`
   - **Valid until**: Local date on which the certificate expires. (Default: 10 years from now)

   > Make sure to define a long duration for the root certificate; 10 years or more are highly recommended. When the root certificate expires, all devices connected to the ICG must be registered again.

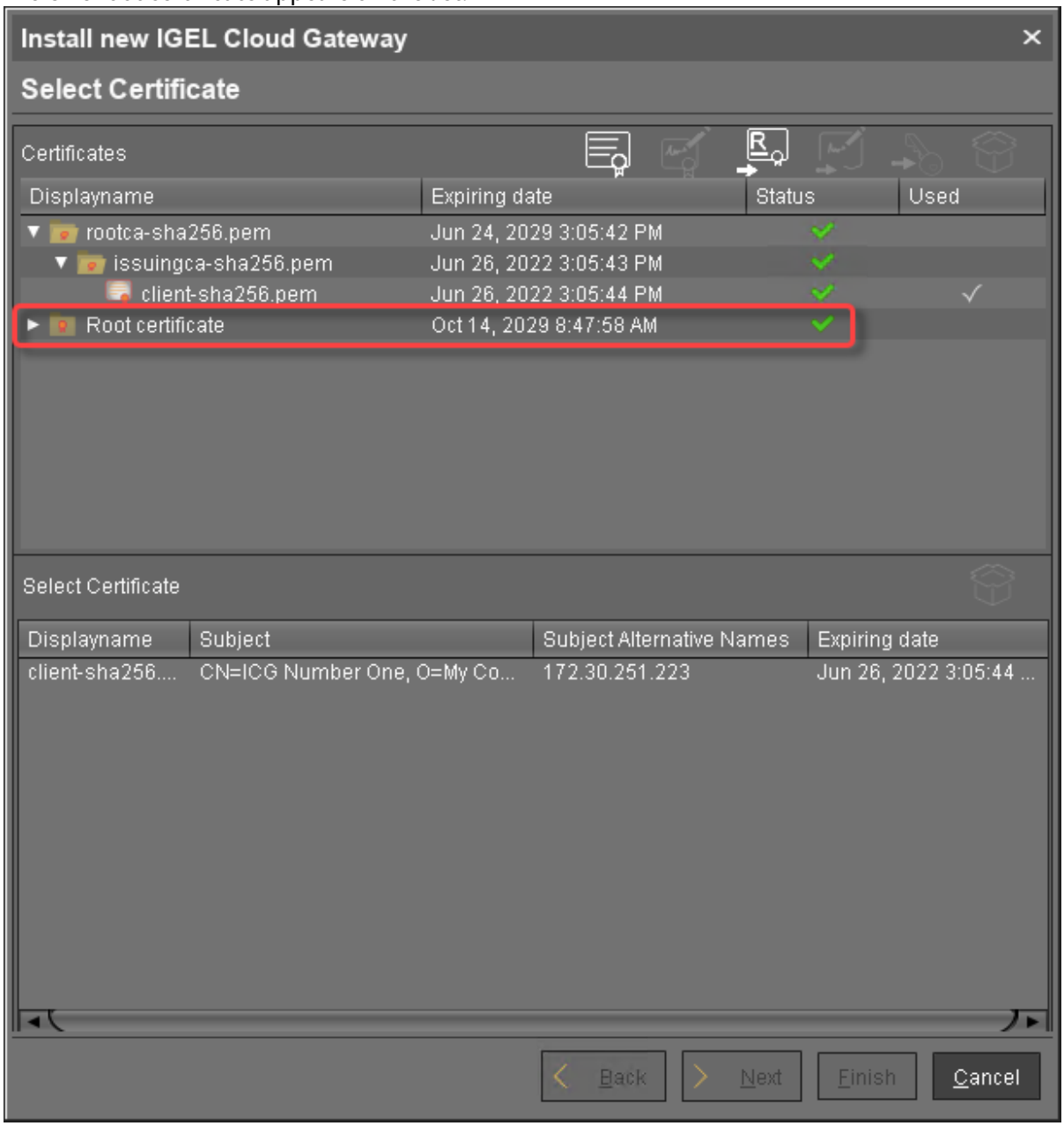
6. Click **OK**.



A key pair and a certificate are generated.

> Generating keys may take substantial time on virtual machines (VMs), as these do not have a powerful (pseudo) random number source. On Linux VMs this can be improved by installing the haveged[4] package.

The CA's root certificate appears on the list.



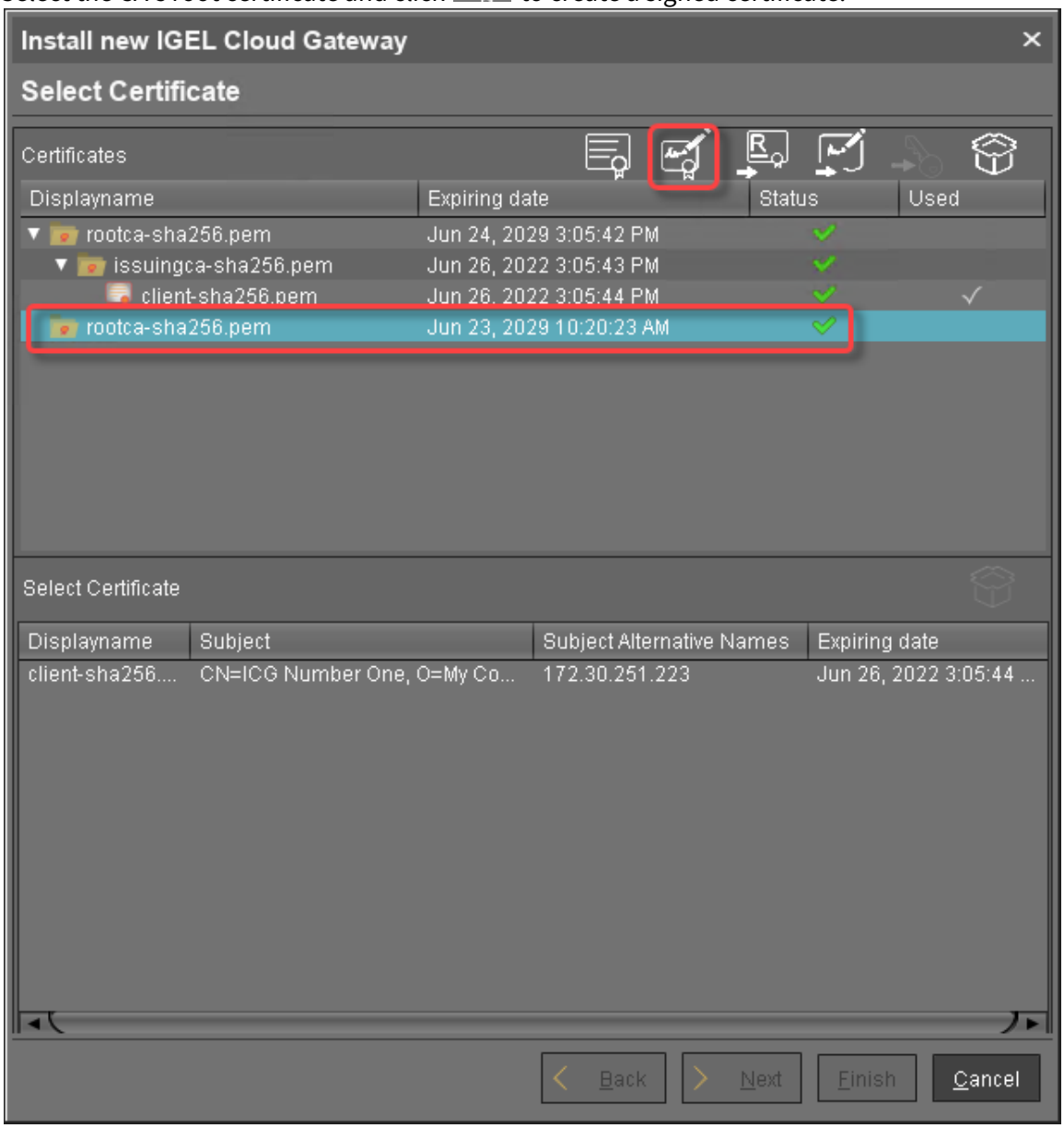
The CA is now ready to use.

4 http://www.issihosts.com/haveged/

Creating the Signed Certificate

Creating Certificates from an Existing Root Certificate

1. Select the CA's root certificate and click to create a signed certificate.



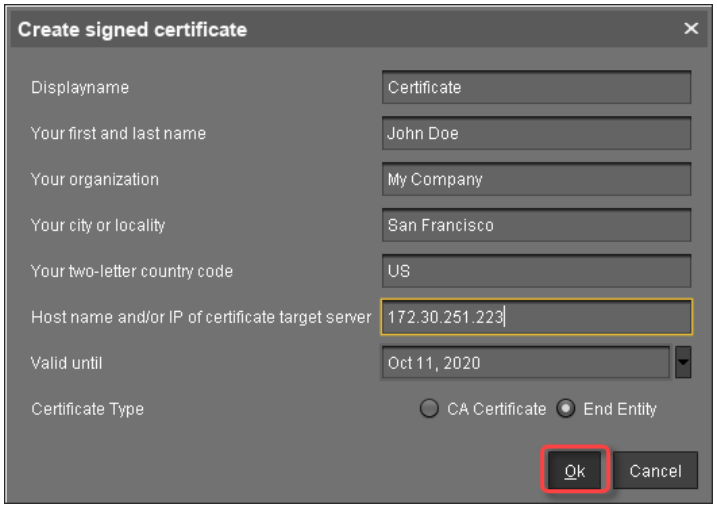
2. Fill in the certificate fields:
   - **Display name**: Name of the certificate

- **Your first and last name**: Name of the certificate holder
- **Your organization**: Organization or company name
- **Your city or locality**: Location
- **Your two-letter country code**: ISO 3166 country code, e.g. `US`, `UK` or `ES`
- **Hostname and/or IP address of certificate target server**: Hostname(s) or IP address(es) for which the certificate is valid. Multiple entries are allowed, separated by semicolons.

> ⓘ All IP addresses and hostnames by which the ICG will be reachable from within the company network or from outside must be provided here.

- **Valid until**: Local date on which this certificate expires. (Default: one year from now)
- **Certificate Type**: Select "End Entity".

3. Click **OK**.

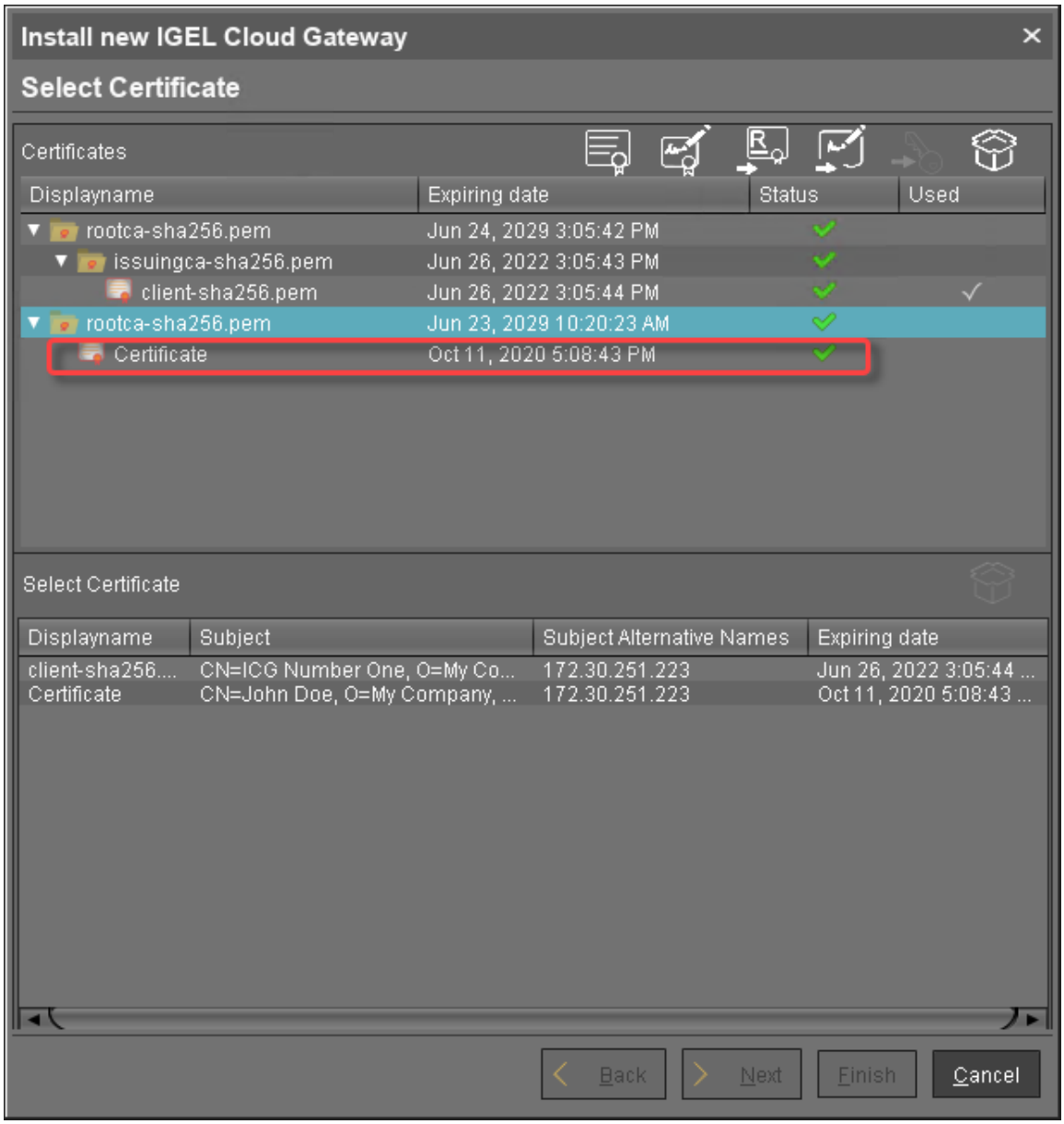


A key pair and a certificate are generated.

> ⓘ Generating keys may take substantial time on virtual machines (VMs), as these do not have a powerful (pseudo) random number source. On Linux VMs, this can be improved by installing the haveged[5] package.

5 http://www.issihosts.com/haveged/

The signed certificate appears on the list.



4. Continue with Installing the IGEL Cloud Gateway(see page 40).

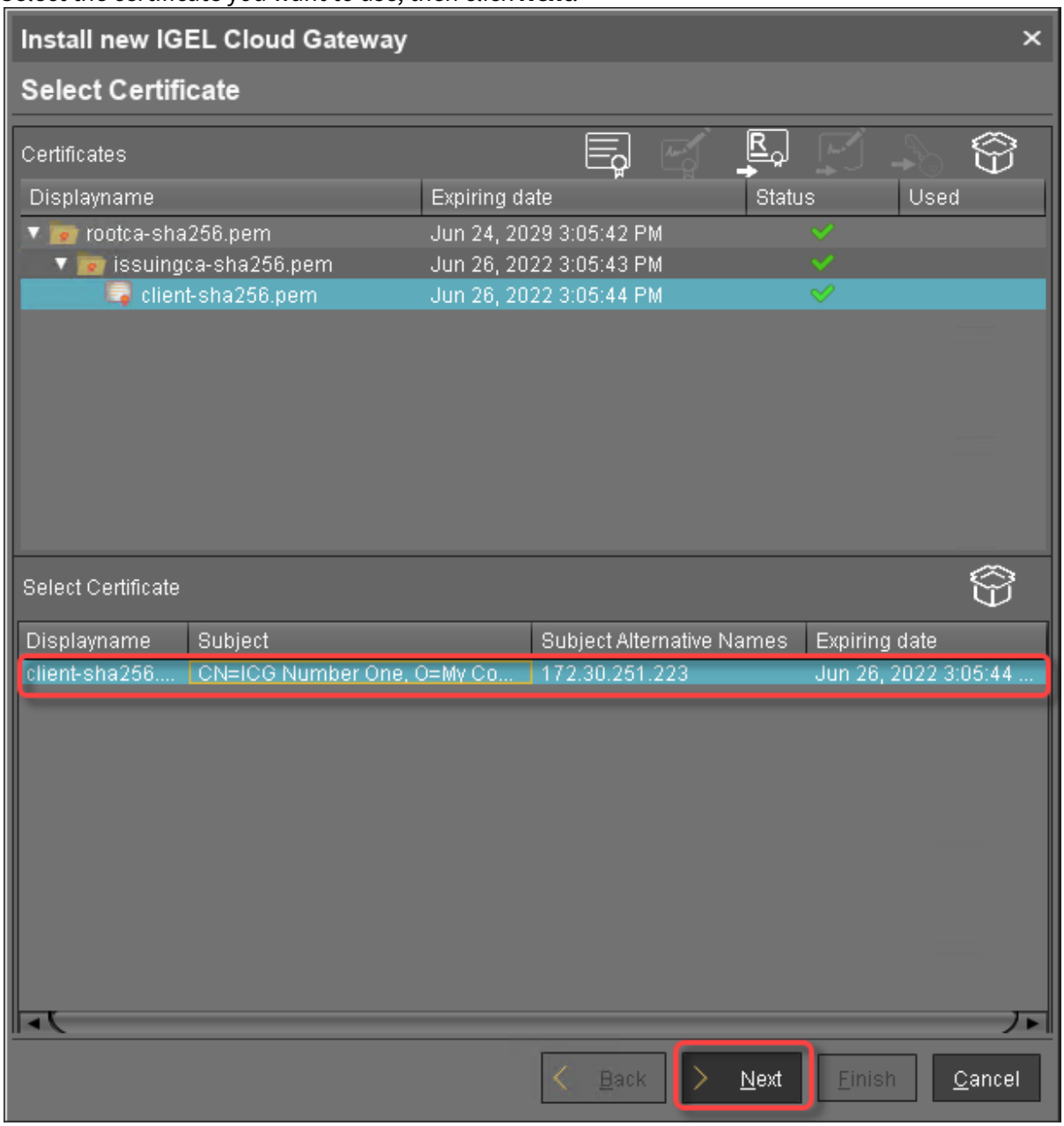
Installing the IGEL Cloud Gateway

The recommended method to install the ICG is to use the ICG remote installer. The ICG remote installer is available as of UMS 5.09.100. If you cannot or do not want to use the remote installer, you can install the ICG manually, see Installing the ICG without remote installer(see page 111).

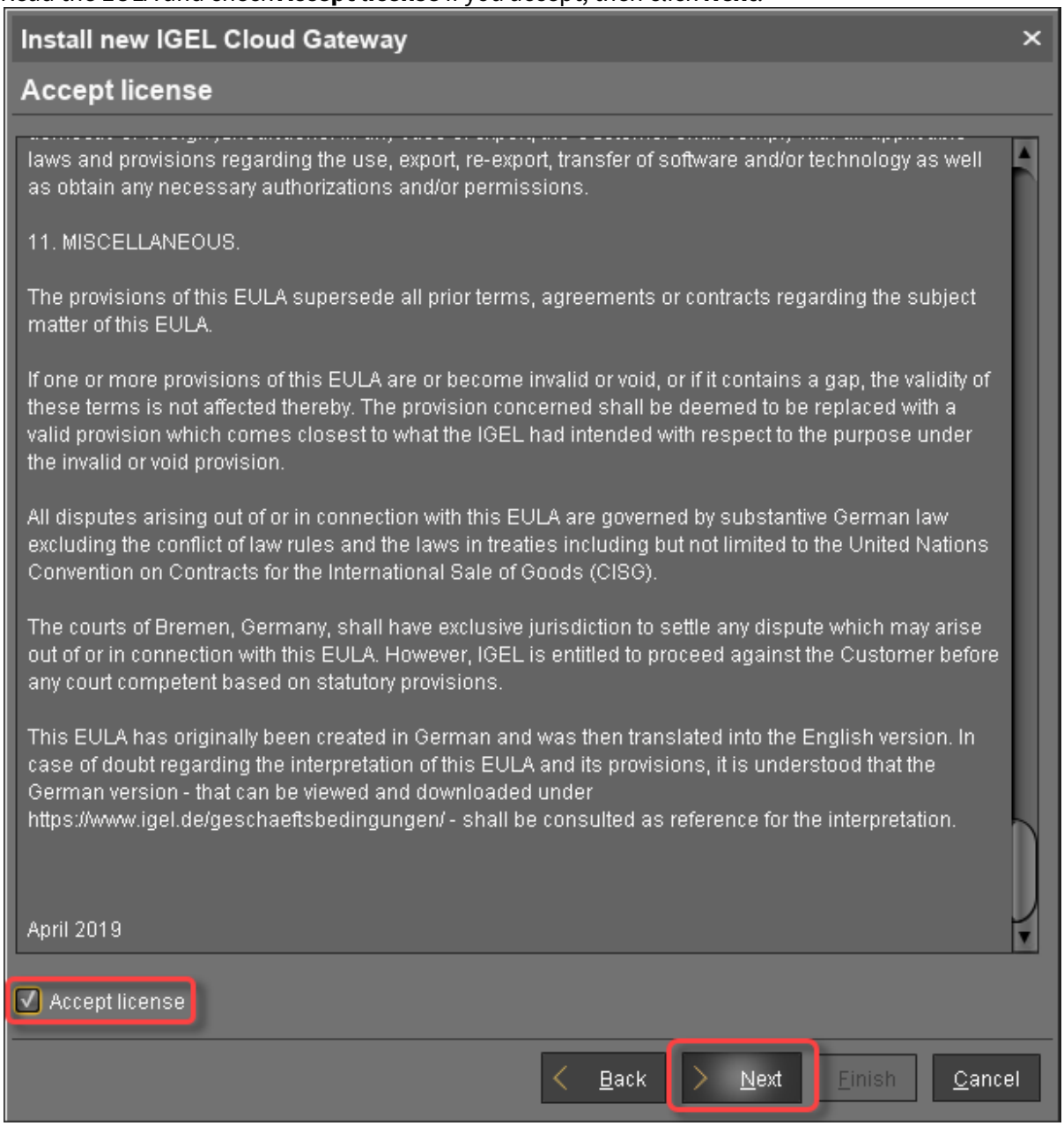
The procedure described here is valid for UMS 6.03 or higher. For UMS 6.02 or lower, see the how-to Installing IGEL Cloud Gateway (UMS 6.02 or Lower)(see page 147).

1. Start the UMS Console.
2. Go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.
3. If the ICG remote installer is not already running, go to **UMS Administration > UMS Network > IGEL Cloud Gateway** and click .
   The ICG remote installer opens. In the **Select Certificates** area, all certificates that can be used for the ICG are listed. If you need a certificate, you can use the ICG remote installer to install one; see Providing the Certificates(see page 13).

4. Select the certificate you want to use, then click **Next**.



5. Read the EULA and check **Accept license** if you accept, then click **Next**.



6. Enter the installation parameters:
   - **SSH host**: Address of the host the ICG is to be installed on. This field is prepopulated with a host that has been derived from the certificate. If more than one hosts are specified in the certificate, ensure that this is the one that is used for communication between UMS and ICG.
   - **SSH port**: SSH port (default: 22)

     ⓘ The SSH user needs root privileges, otherwise the remote installer will not be able to perform all required installation tasks.

UMS 5.09.110 or higher: It is sufficient for the SSH user to have sudo privileges.

Root access to the SSH server is a security risk!
If you permit root login for SSH, it is recommended to disable root login when the ICG installation has finished.

Key-based authentication is not supported by the remote installer. If you are using key-based authentication, you will have to install manually, see Installing the ICG without remote installer(see page 111).

- **SSH user**: The user that the remote installer uses to authenticate against the SSH server and execute the installer

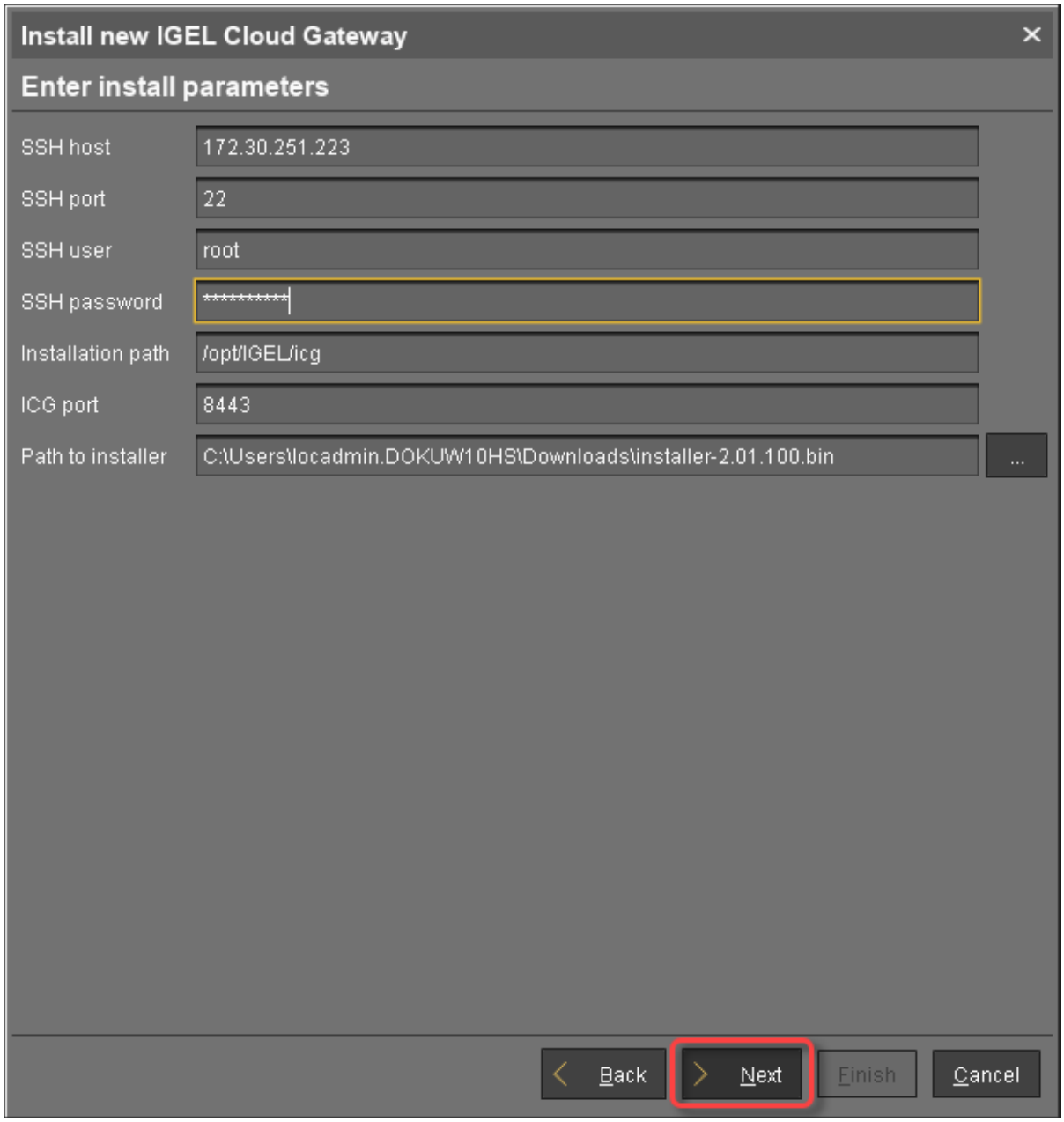
  Username "icg" Is Reserved

  Do not use "icg" as a username for the remote installer; this is the username under which the Tomcat server is running.

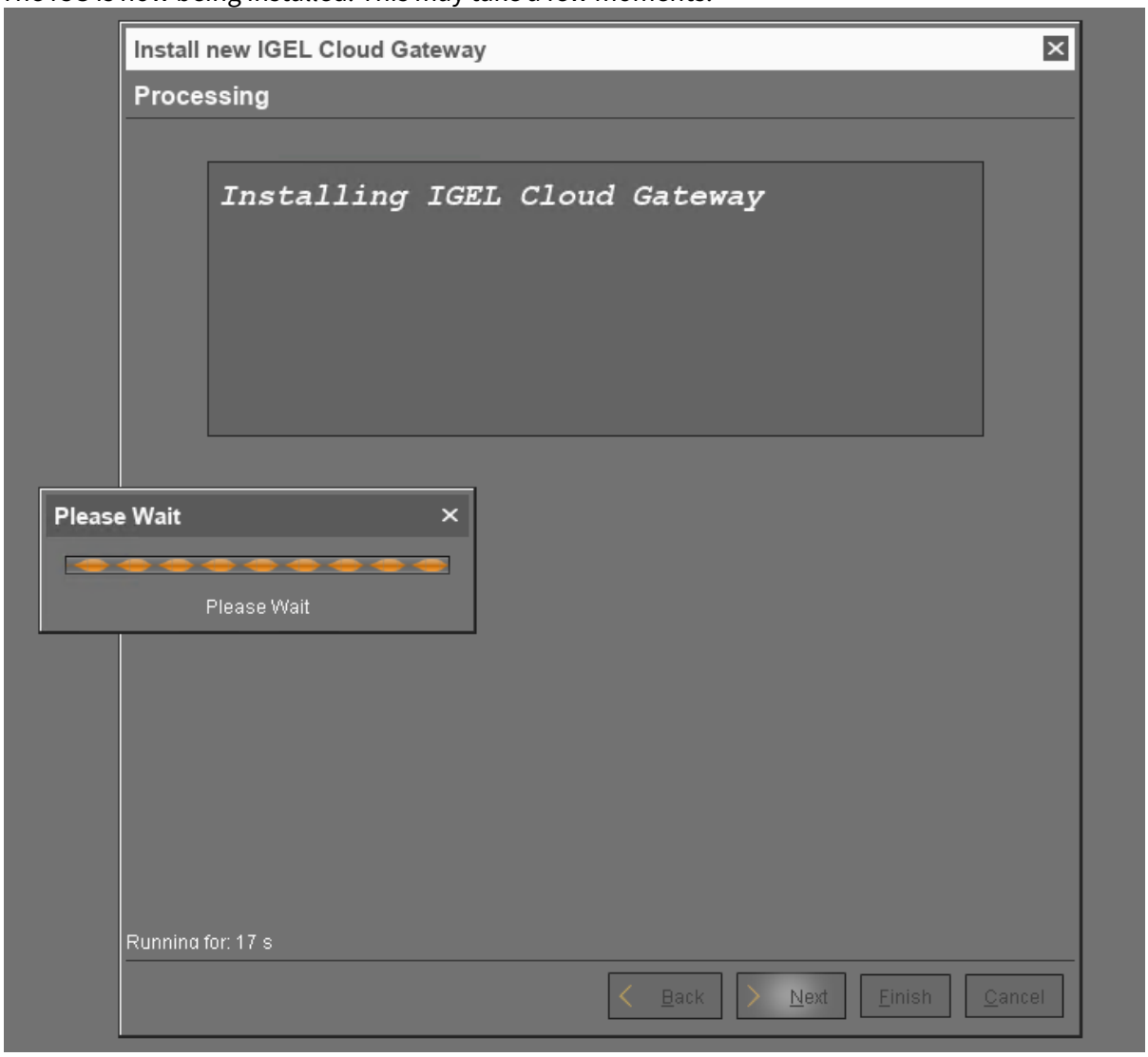
- **SSH password**: Password for the user that is specified as **SSH user**
- **Installation path**: Installation path on the server (default: `/opt/IGEL/icg`)
- **ICG port**: The port the ICG will be listening on. Privileged ports can be used, too, e.g. port 443. (Default: 8443)
- **Path to installer**: The local path to the `.bin` file containing the installer

  ICG installers are available from https://www.igel.com/software-downloads/enterprise-management-pack/

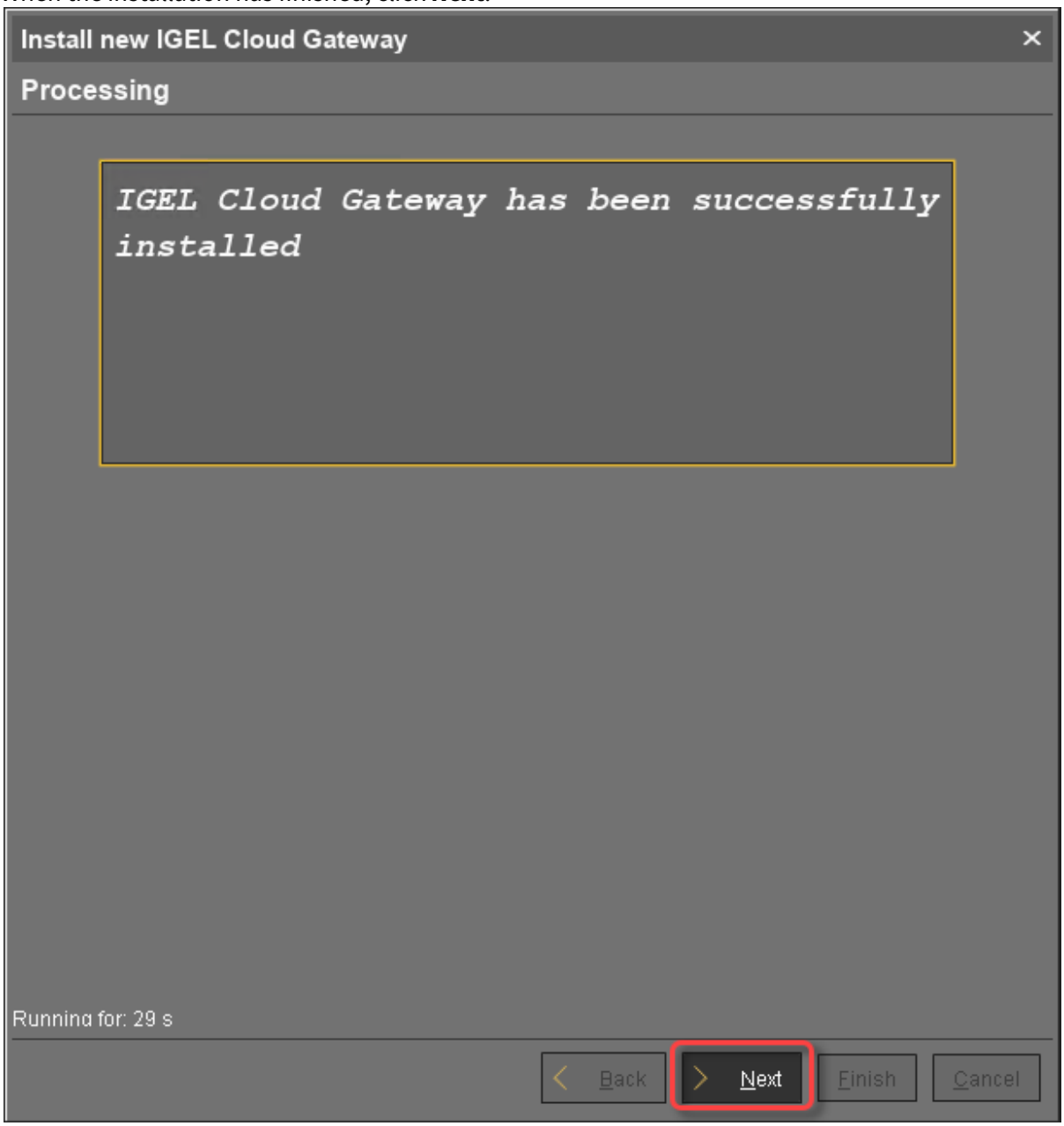
7. Click **Next**.


Install new IGEL Cloud Gateway
Enter install parameters
SSH host
172.30.251.223
SSH port
22
SSH user
root
SSH password
****
Installation path
/opt/IGEL/icg
ICG port
8443
Path to installer
C:\Users\locadmin.DOKUW10HS\Downloads\installer-2.01.100.bin
...
Back
Next
Finish
Cancel

The ICG is now being installed. This may take a few moments.

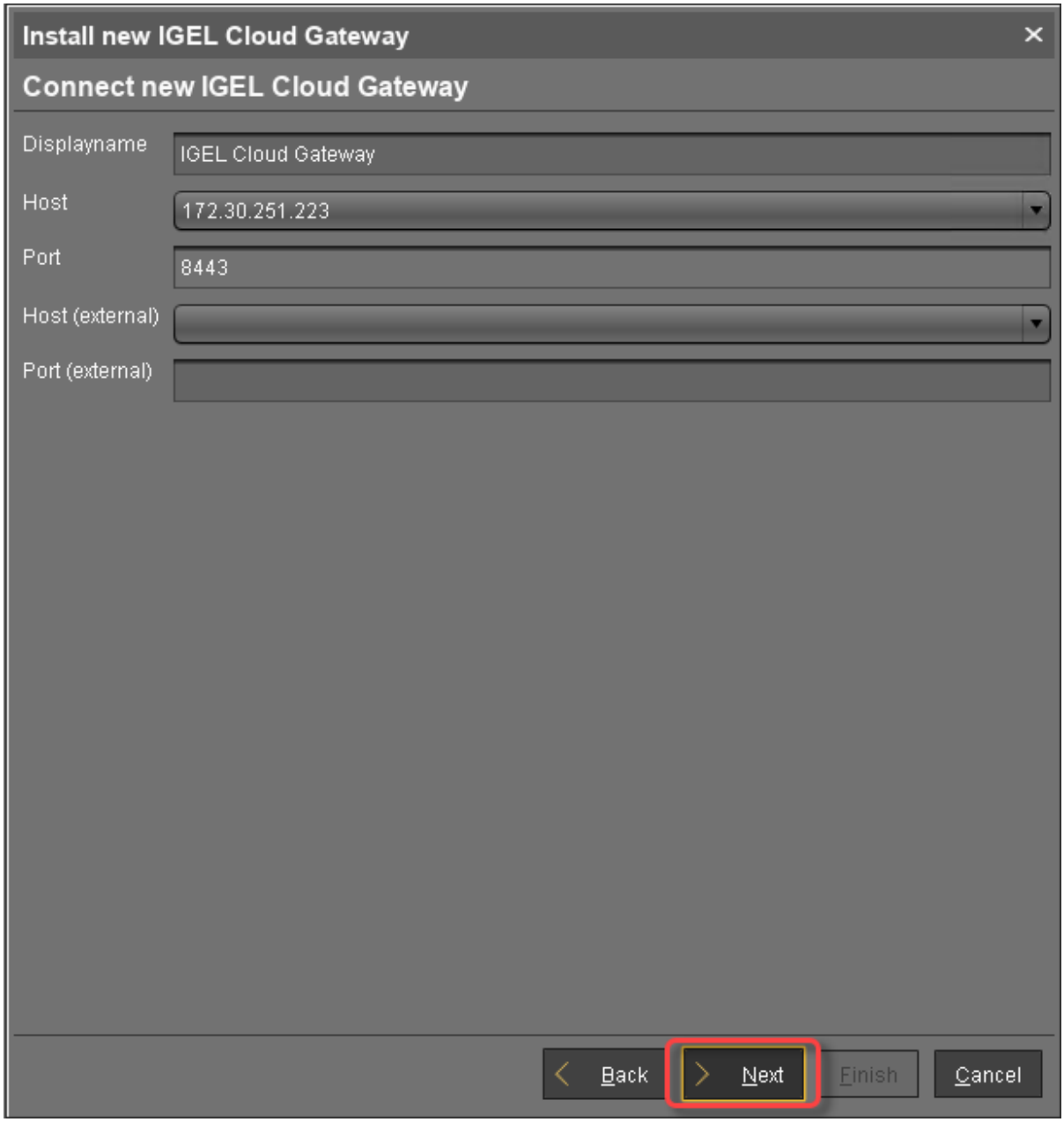


8. When the installation has finished, click **Next**.



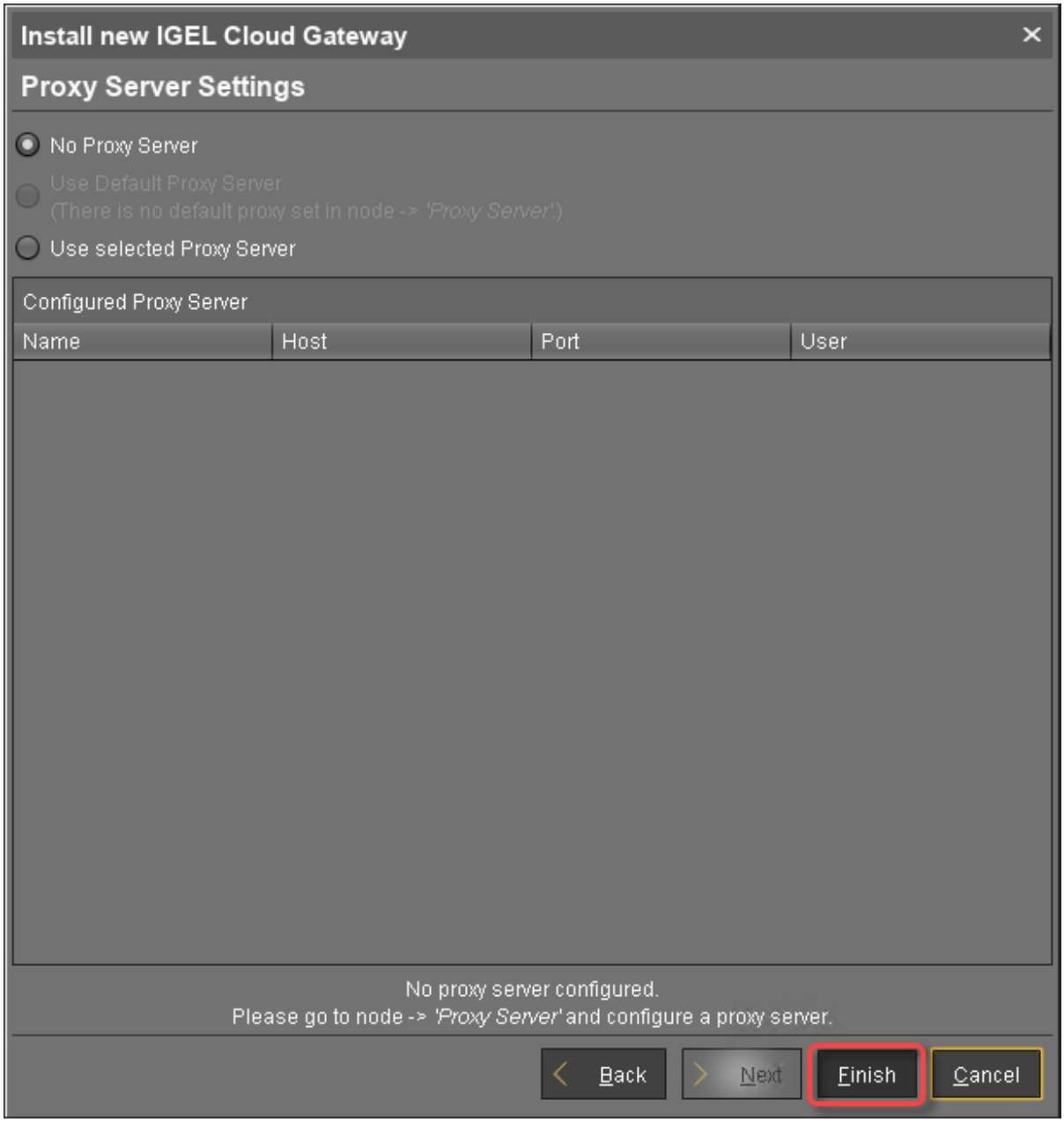
9. Enter a display name and the connection details for the ICG:
   - **Displayname**: The name used for listing the ICG under **UMS Administration > IGEL Cloud Gateway**.
   - **Host**: Internal host used by the UMS for connecting to the ICG.
   - **Host (external)**: External host used by endpoint devices to connect to the ICG; only required if the devices use a separate address, not the one specified under **Host**.
   - **Port**: Port used by the endpoint devices if they connect to the ICG using the address provided under **Host (external)**. If the devices use the address under **Host**, this field can be left empty.

10. Click **Next**.



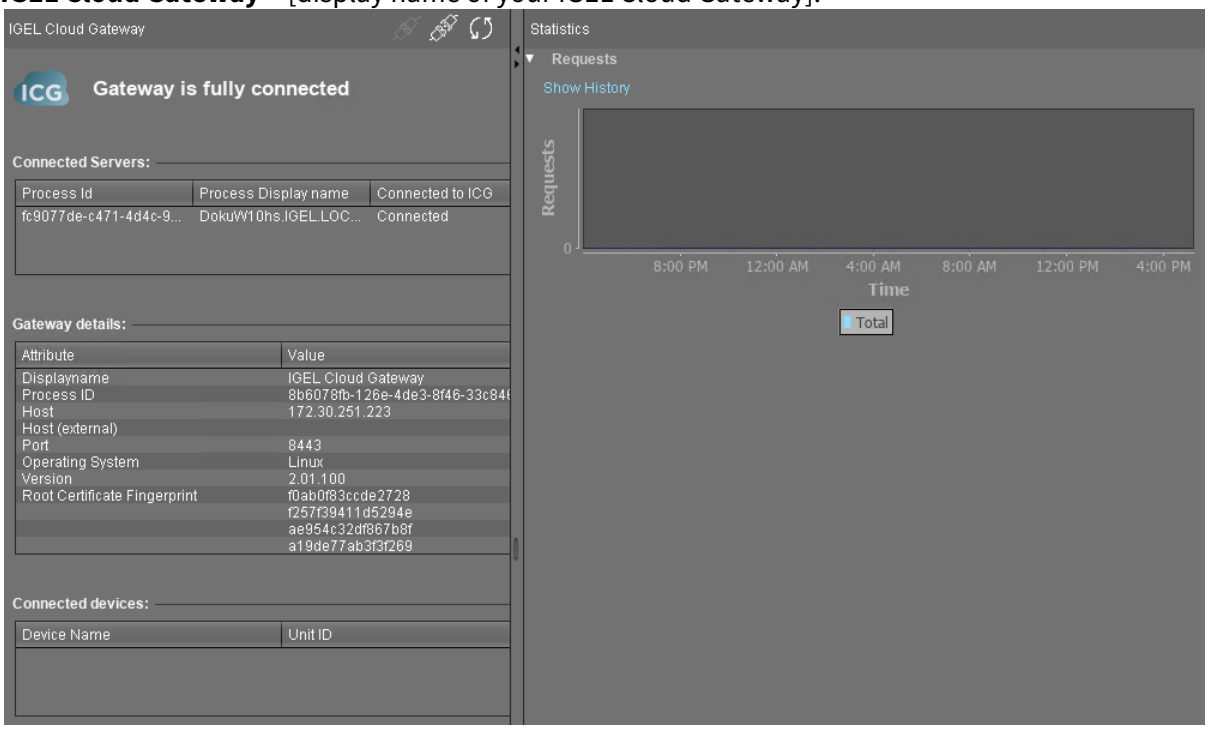
11. If desired, you can now define a proxy. Make your settings as required.

12. Click **Finish**.



The newly installed ICG is now listed under **UMS Administration > IGEL Cloud Gateway**.

13. To review the status of the ICG and basic data about the installation, go to **UMS Administration > IGEL Cloud Gateway >** [display name of your IGEL Cloud Gateway].



Connecting the Devices

- Generating and Distributing First-Authentication Keys for Devices(see page 51)
- Connecting a Device to the IGEL Cloud Gateway(see page 53)
- Toggling between ICG and Direct Connection(see page 57)

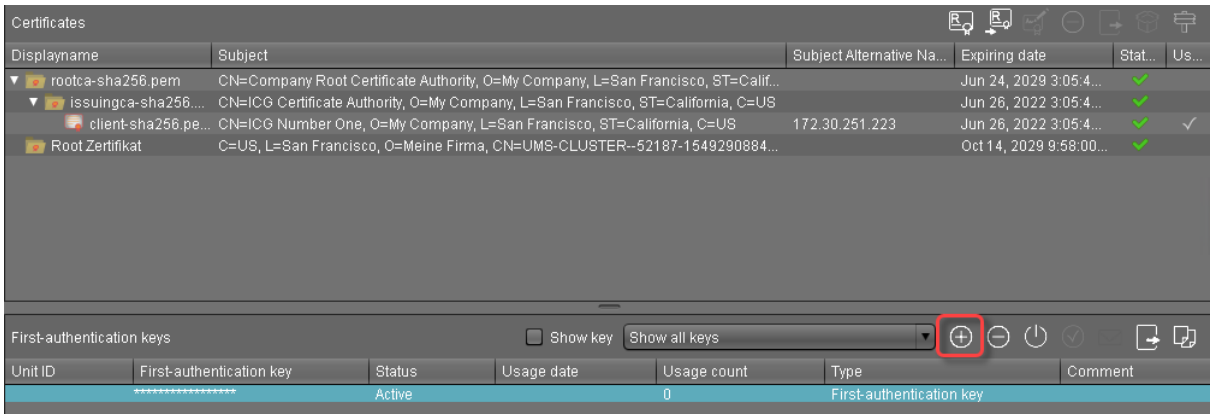
Generating and Distributing First-Authentication Keys for Devices

To establish a connection with the ICG, every device must authenticate with the ICG. For this purpose, a first-authentication key must be generated. On first contact with the ICG, the device must present this key.

There are various methods of generating first-authentication keys. The most common one is described here; for alternative methods, see All Methods of Generating First-Authentication Keys for Devices(see page 143).

Creating a New Mass-Deployment Key for Arbitrary Devices

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. Click .



3. Select **Create new mass-deployment key**.
4. Activate or deactivate **Generate random mass-deployment key** to choose the method of key generation:
   - ☑ The key is generated by the UMS.
   - ☐ You can enter a key of your own in the entry field.
5. Click **OK**.
   One or more new entries appear in the list.

Distributing the Key via E-Mail or Printed Letter

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication key**, select the desired password entries and click to copy the credentials to the clipboard.
   The data required for connecting a device to the ICG is in the clipboard: host address, ICG server certificate fingerprint, and the password.
   The contents of the clipboard will look similar to the following example:

```
----------------------------------------------------------------
----------------------------------------------------------------
```

```
Host: 222.222.222.222
Port: 8443
Root Certificate Fingerprint
Part 1: 1231231231231231
Part 2: 2342342342342342
Part 3: 3453453453453453
Part 4: 4564564564564564
-----------------------------------------------------------------
-----------------------------------------------------------------
First-authentication key: 17171717171717171
-----------------------------------------------------------------
```

The clipboard contains data for all active ICGs. In the example above, 1 ICG connection is active. If, for instance, 3 ICG were active, the data for those 3 ICG would be included.

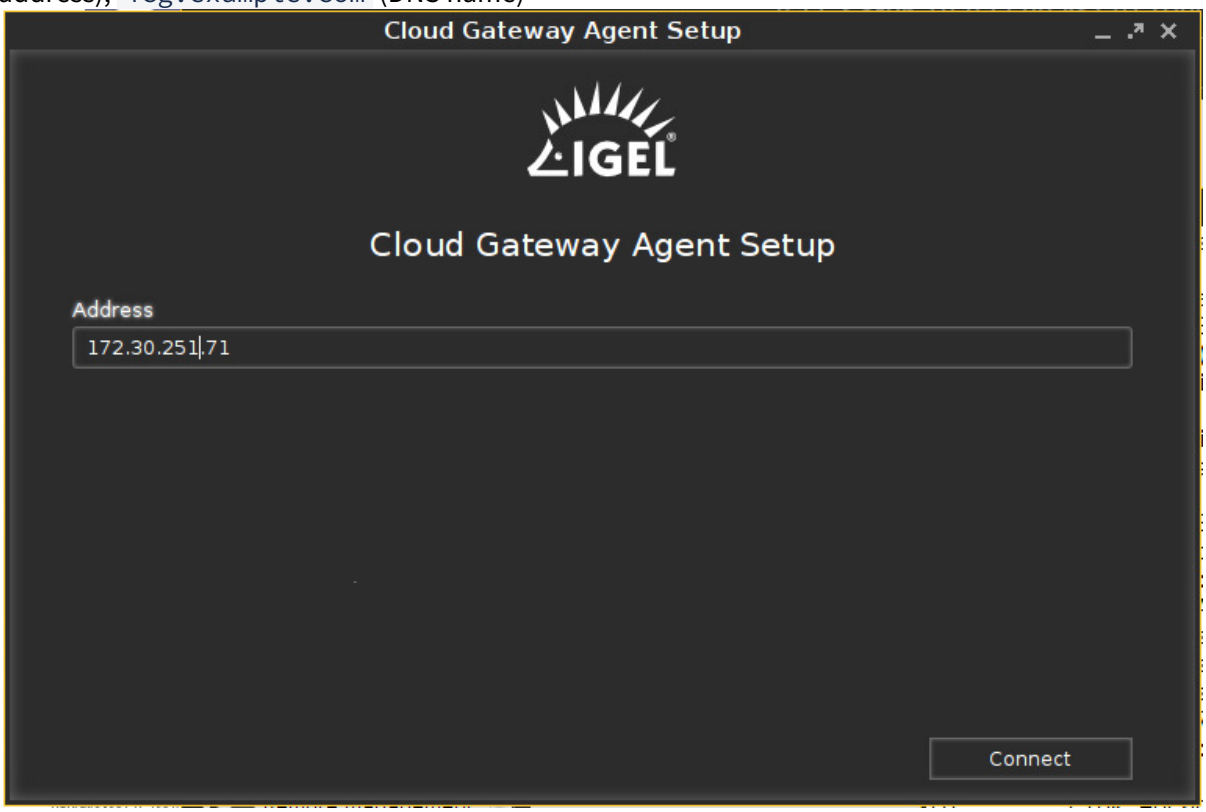
3. To send the credentials via e-mail, paste the data into an encrypted e-mail. To send the credentials in a printed letter, paste the data in your e-mail program or word processor.

Connecting a Device to the IGEL Cloud Gateway

When the credentials are available at the user / device side, the device is ready to connect to the UMS.

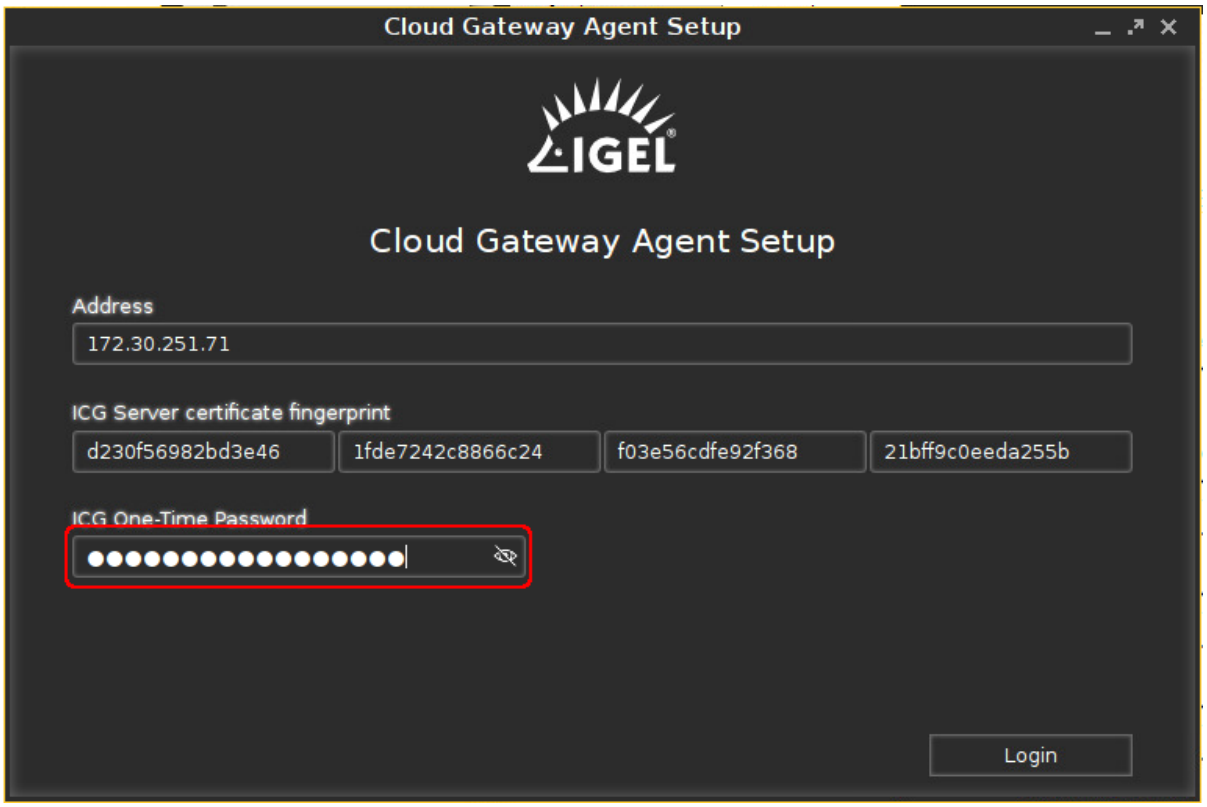
If the device has not been configured yet, the Setup Assistant will start automatically on system startup; see the Setup Assistant chapter in the IGEL OS manual. The ICG Agent Setup, which is described here, is embedded in the Setup Assistant. The procedure is identical both for the standalone ICG Agent Setup and the one embedded in the Setup Assistant.

1. From **Start Menu >** (System) open **ICG Agent Setup**.
2. Enter the ICG server IP address or DNS name into **Address**. Examples: `172.30.251.71` (IP address), `icg.example.com` (DNS name)



3. Click **Connect**.
   The setup utility checks connectivity and displays 3/4 of the ICG server certificate fingerprint.
4. Enter the missing part of the **ICG server certificate fingerprint**. Any part of the fingerprint may be missing; this is determined randomly.

5. Enter the **ICG One-Time Password**. Click the eye icon to toggle visibility of the password.



6. Click **Login**.
   The message **ICG connection ready!** is displayed.

7. Click **Finish**.

   The ICG connection icon is shown in the task bar.

Toggling between ICG and Direct Connection

If the device is (temporarily) moved to a company's local network where a direct connection to the UMS is possible, it may be feasible to switch from ICG use to direct connection. This can be done using a registry parameter.

To switch from ICG to direct connection:

1. Open the device's Setup and go to **System > Registry > system > remotemanager > enable_icg** (full parameter name: **system.remotemanager.enable_icg**).
2. Deactivate **Enable ICG**.
3. Click **Apply** or **Ok**.
   The device cancels its connection to the ICG and automatically establishes a direct connection to the UMS. The tray icon changes to .

To switch from direct connection to ICG:

1. Open the device's Setup and go to **System > Registry > system > remotemanager > enable_icg** (full parameter name: **system.remotemanager.enable_icg**).
2. Activate **Enable ICG**.
3. Click **Apply** or **Ok**.
   The device cancels its direct connection to the UMS and automatically establishes a connection to the ICG. The tray icon changes to .

Administration

- Updating the IGEL Cloud Gateway (ICG)(see page 59)
- Configuring the ICG Connection Limit(see page 61)
- Renewing a Signed Certificate for the ICG(see page 62)
- Exchanging the Root Certificate for ICG(see page 67)
- Moving an Endpoint Device to an ICG(see page 84)
- Removing an Endpoint Device from ICG(see page 86)
- Network Ports Used(see page 87)
- Controlling the ICG Daemon(see page 88)
- Optional: Adding a TXT Record for the ICG Server(see page 89)

Updating the IGEL Cloud Gateway (ICG)

You can update your IGEL Cloud Gateway (ICG) from the IGEL Universal Management Suite (UMS).

Prerequisites

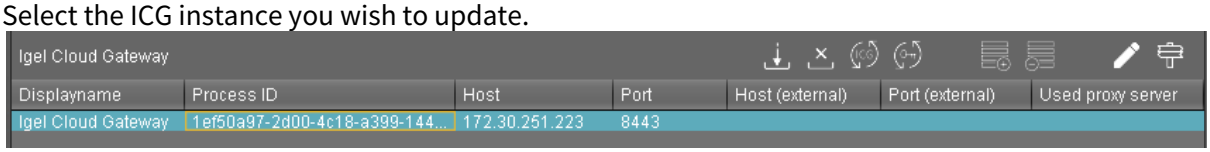
- UMS 5.09.100 or higher
- New version of ICG has been downloaded from https://www.igel.com/software-downloads/enterprise-management-pack/
- Root access to the host running the ICG

> **Upgrading from ICG 1.x not Supported**
>
> Upgrading from ICG 1.x (based on OVA) to 2.x is not supported.
> The supported method is a new installation on a Linux server; see Installation and Setup(see page 12).

Steps

To update the ICG, proceed as follows:

1. Start the UMS Console.
2. Go to **UMS Administration > UMS Network > Igel Cloud Gateway**.
3. Select the ICG instance you wish to update.



4. In the toolbar in the upper right, click the icon.
   The update wizard opens.
5. Enter the following installation parameters:
   - **SSH host**: The host the ICG is running on (Default: `localhost`)
   - **SSH port**: SSH port (Default: `22`)

   > The SSH user must have root access.

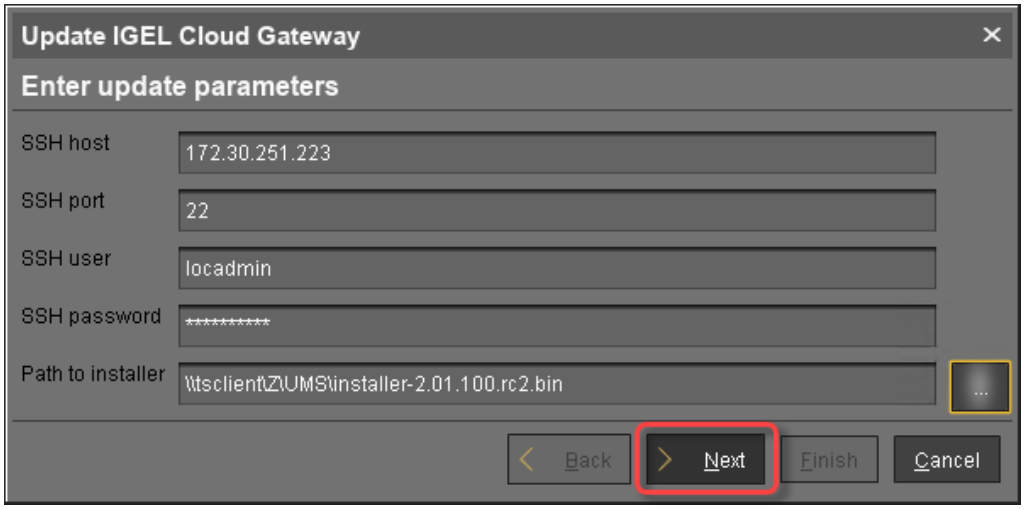
   > Root access to the SSH server is a security risk!
   > Make sure you disable root access to the SSH server when ICG installation has finished.

> As of UMS 5.09.110, it is no longer necessary to use the root user and sufficient for the ssh user to have sudo privileges.

- **SSH user**: SSH user
- **SSH password**: SSH user password
- **Installation path**: Installation path (Default: `/opt/IGEL/icg`)
- **ICG port**: ICG port (Default: `8443`)
- **Path to installer**: The path to the .bin file containing the installer.

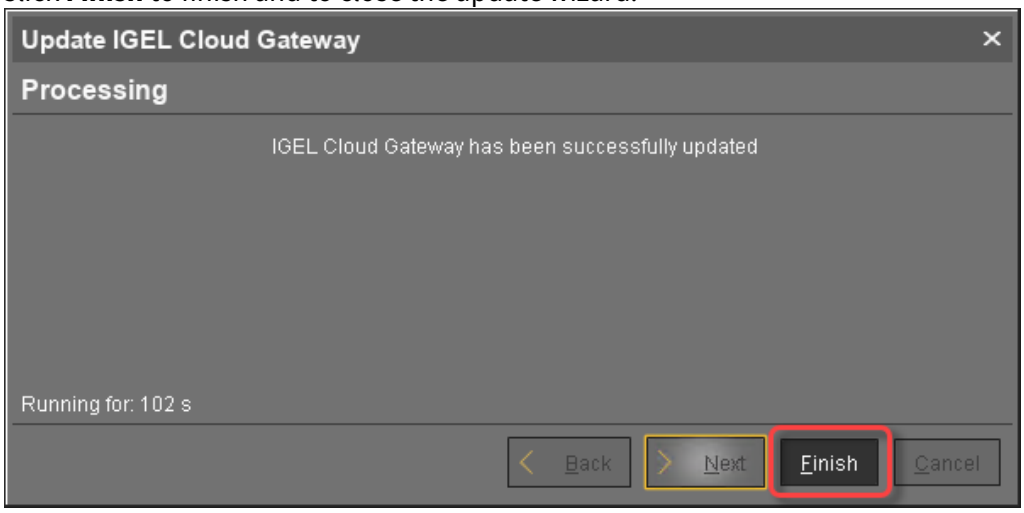
> ICG installers are available under https://www.igel.com/software-downloads/enterprise-management-pack/.

6. Click **Next**.



The ICG is now being updated. This may take a moment.
When the update is complete, the update wizard shows a success message.

7. Click **Finish** to finish and to close the update wizard.



Configuring the ICG Connection Limit

You can set a limit for the number of endpoint device connections that an ICG instance will accept. You can set the limit globally for all ICG instances or individually for each ICG instance.

When the limit is reached, the ICG will reject any further connections to endpoint devices. The rejection of device connections will be logged.

Configuring a Global Connection Limit

1. Go to **UMS Administration > IGEL Cloud Gateway** and click (upper right).
2. In the **ICG Connection Limit** dialog, select **Use global connection limit for all ICGs**.
3. Under **Confine connection amount to:**, enter the desired limit.
4. Click **Ok**.

Configuring Individual Connection Limits for Each ICG Instance

1. Go to **UMS Administration > IGEL Cloud Gateway** and click (upper right).
2. In the **ICG Connection Limit** dialog, select **Use specific connection limits for each ICG**.
3. Under **Confine connection amount to:**, enter the desired limit for each ICG instance or leave it at **Allow unlimited connections**, according to your needs.
4. Click **Ok**.

Checking the Logs for Rejected Connections

The following steps must be executed on each ICG host.

1. Open a terminal on the host and log in as the user that was defined for installing the ICG (see Installing the IGEL Cloud Gateway(see page 40)).
2. Open the configuration file `logback-spring.xml` in a text editor, e. g. vi:
   `sudo vi /opt/IGEL/icg/usg/conf/logback-spring.xml`
3. Change the `<logger>` element like so:
   `<logger name="de.igel" level="DEBUG"/>`
4. Restart the ICG:
   `sudo systemctl restart icg-server.service`
5. To find out which connections have been rejected, open the log file `/opt/IGEL/icg/usg/logs/usg.log` and look for entries that read `Max connections limit has exceeded. Device [devicename] is rejected`

Renewing a Signed Certificate for the ICG

When the signed certificate of your ICG installation is about to expire, you must renew it, that is, replace it by a newer certificate which is compatible to the current one. The new certificate is compatible if the following conditions are met:

- The new certificate is issued from the same root certificate as the current certificate
- The new certificate contains the same IP addresses or host names as the current certificate
- The new certificate is a signed certificate

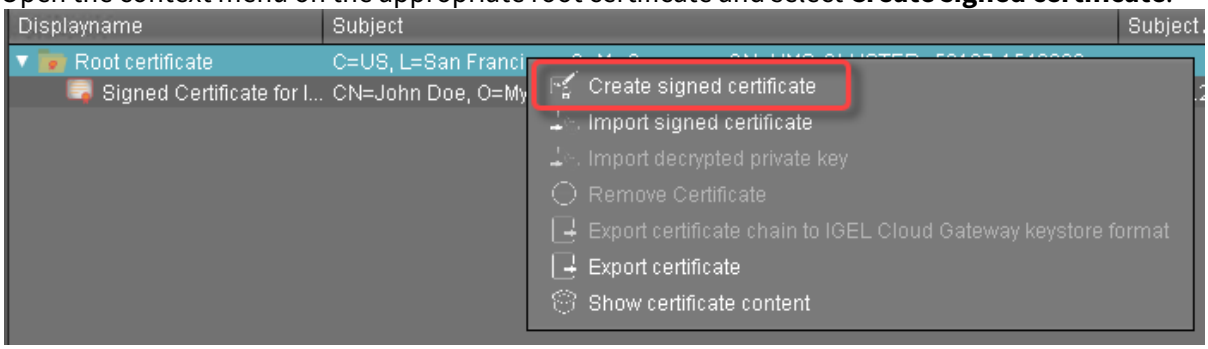
You can renew a certificate using the update keystore function of the UMS or locally on the machine hosting the ICG. Using the update keystore function of the UMS is recommended; this method is described in this chapter.

Creating a New Certificate

If you do not already have a new certificate:

1. In the UMS Console, go to **UMS Administration > UMS Network > Global Configuration > Cloud Gateway Options**.

2. Open the context menu on the appropriate root certificate and select **Create signed certificate**.

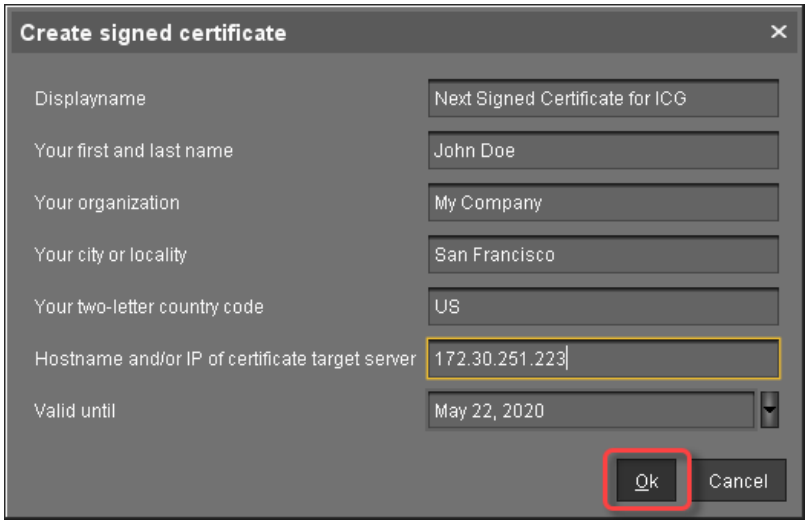


3. Fill in the certificate fields (most likely, the data will be the same as for the current certificate):
   - **Displayname**: Name of the certificate

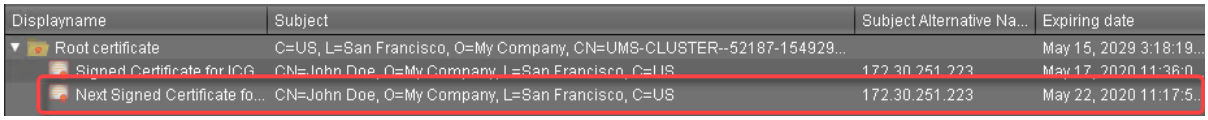
   > The display name in the server certificate must not be the same as in the root certificate.

   - **Your first and last name**: Name of the certificate holder
   - **Your organization**: Organization or company name
   - **Your city or locality**: Location
   - **Your two-letter country code**: ISO 3166 country code, e.g. `US`, `UK` or `ES`
   - **Hostname and/or IP address of certificate target server**: Same Host name(s) or IP address(es) as in the current certificate.
   - **Valid until**: Local date on which the certificate expires. (Default: one year from now)

4. Click **OK**.



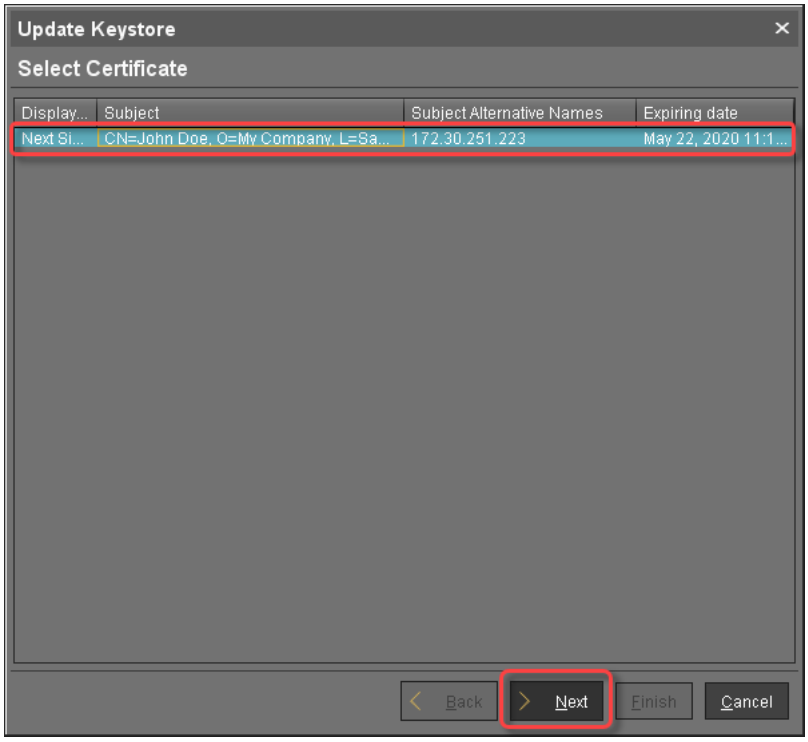
The new certificate is shown.



Updating the Keystore

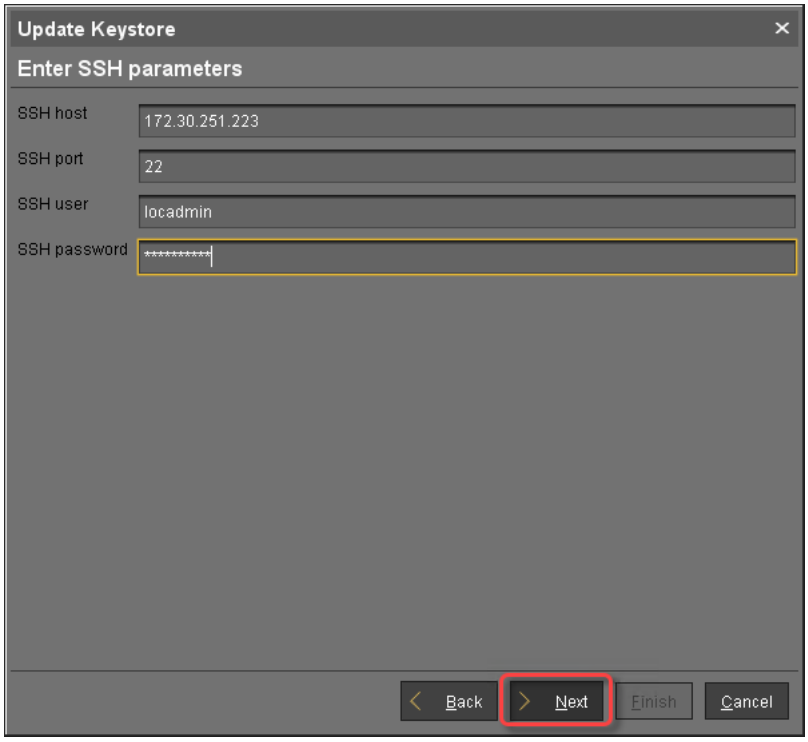
1. In the UMS console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.
2. Select the ICG for which you want to renew the certificate and click .
   The Update Keystore wizard opens; it shows the certificates which can be used for renewal.

3. Select the new certificate and click **Next**.



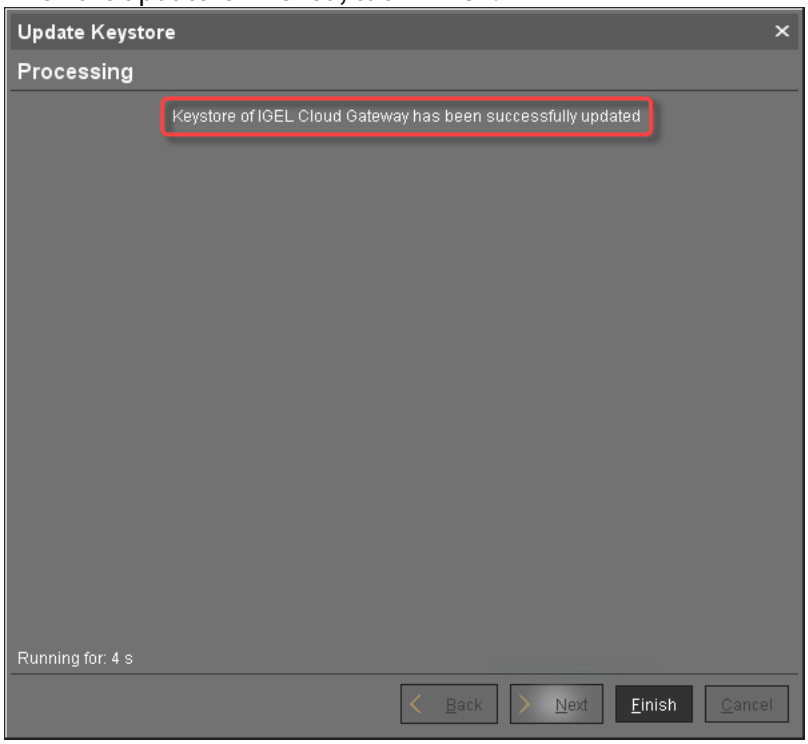
4. Enter the SSH parameters:
   - **SSH host**: IP address or hostname under which the UMS can reach the ICG
   - **SSH port**: SSH port (Default: `22`)
   - **SSH user**: The same user that has been used for the remote installer
   - **SSH password**: Password for the user-specified as **SSH user**

5. Click **Next**.

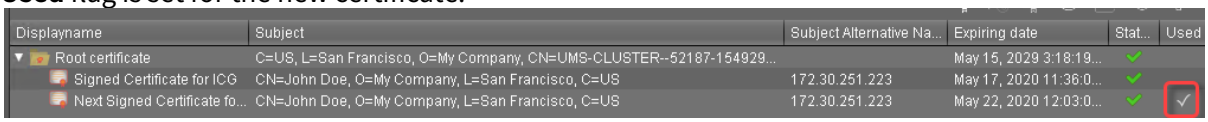


The Keystore of the ICG is updated with the new certificate.

6. When the update is finished, click **Finish**.



7. Go to **UMS Administration > Global Configuration > Cloud Gateway Options** and check if the **Used** flag is set for the new certificate.



Displayname	Subject	Subject Alternative Na...	Expiring date	Stat...	Used
Root certificate	C=US, L=San Francisco, O=My Company, CN=UMS-CLUSTER--52187-154929...		May 15, 2029 3:18:19...	✓	
Signed Certificate for ICG	CN=John Doe, O=My Company, L=San Francisco, C=US	172.30.251.223	May 17, 2020 11:36:0...	✓	
Next Signed Certificate fo...	CN=John Doe, O=My Company, L=San Francisco, C=US	172.30.251.223	May 22, 2020 12:03:0...	✓	✓

Exchanging the Root Certificate for ICG

Overview

With UMS 6.06 or higher, you can exchange the root certificate for an ICG without the need to manually reregister the connected devices. However, there will be a short interruption as the devices reconnect to switch over to the new certificate.

Environment

- ICG 2.02 or higher
- UMS 6.06 or higher
- IGEL OS 11.04.240 or higher is installed on the devices, or the upload source is available and configured on the devices. For details, see Firmware Update.

Use Cases

- The root certificate is about to expire.
- You want to change the public CA.
- New security rules must be implemented, or algorithms are outdated.

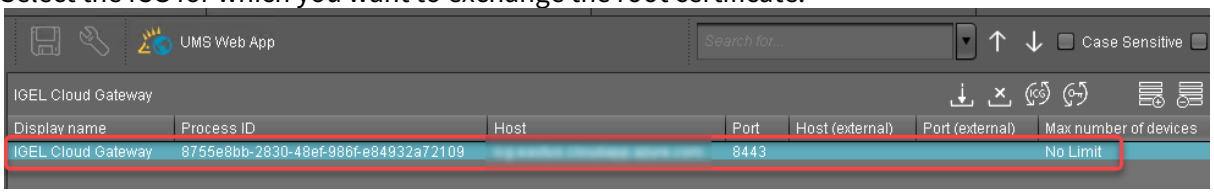
Instructions

The procedure includes the following steps:

1. Choosing the Desired End Certificate(see page 67)
2. Updating the Devices(see page 69) (where necessary)
3. Restarting the Devices(see page 74)
4. Updating the Keystore(see page 79)

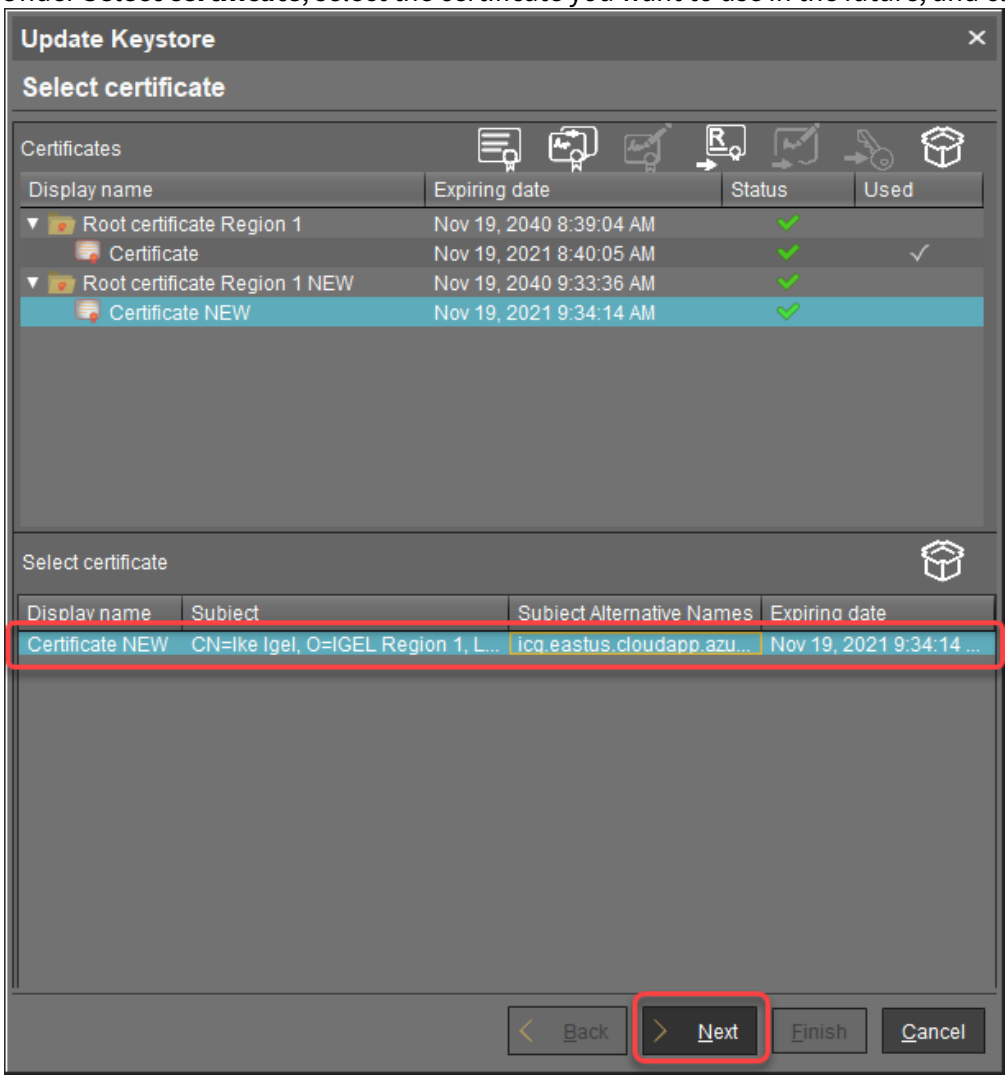
Choosing the Desired End Certificate

1. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.
2. Select the ICG for which you want to exchange the root certificate.

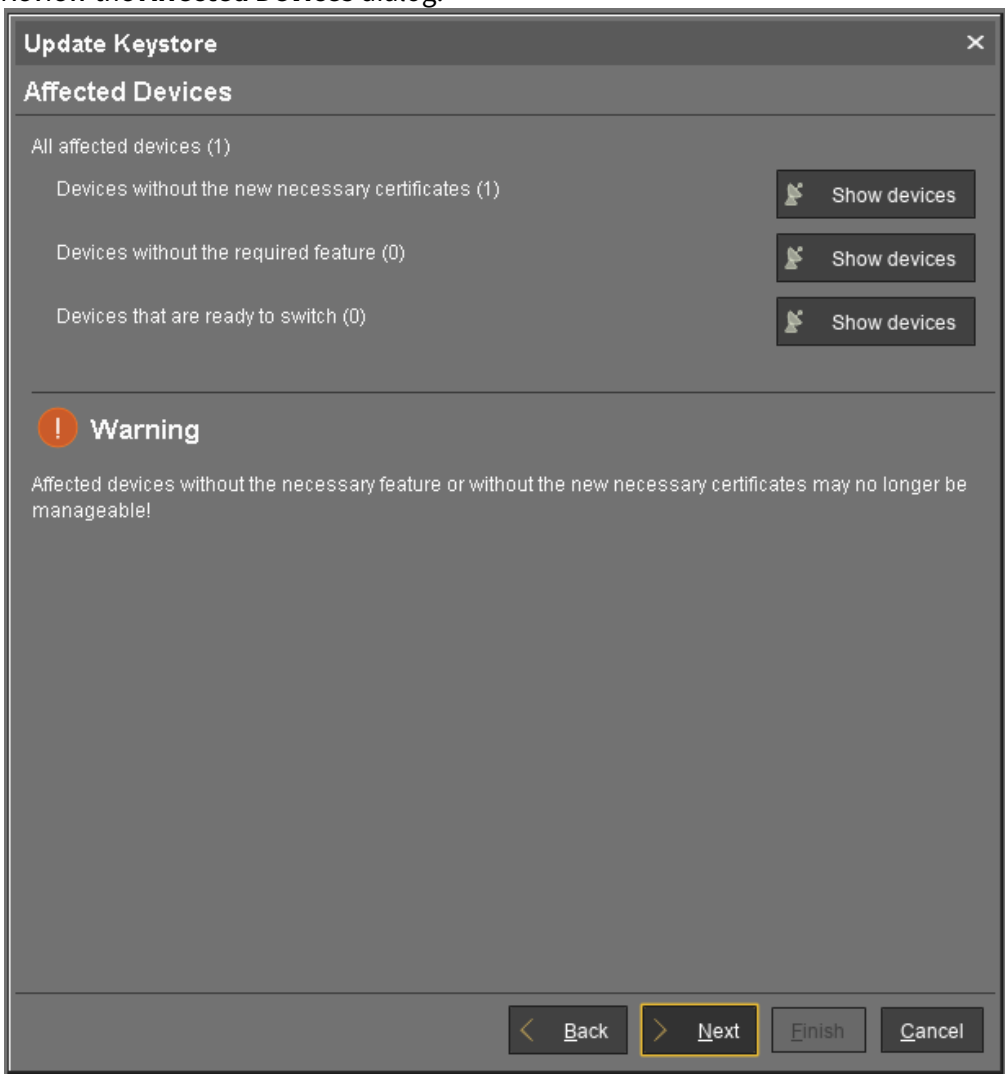


3. Click to open the **Update Keystore** dialog.

4. Under **Select certificate**, select the certificate you want to use in the future, and click **Next**.



5. Review the **Affected Devices** dialog.



Choose the appropriate method according to the displayed numbers:

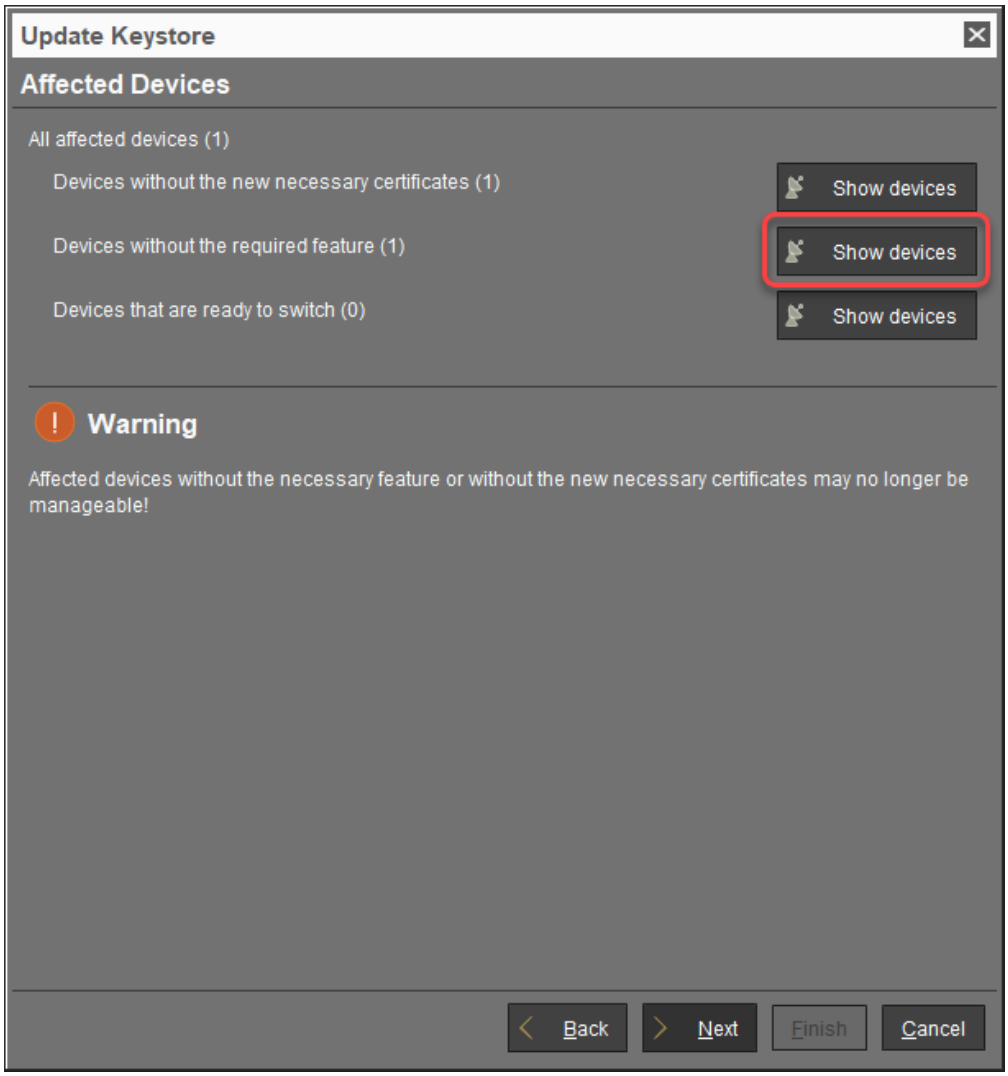
Devices without the new necessary certificates ([number])	Devices without the required feature ([number])	If the 1st and 2nd Columns Are True, Continue with...
≥ 1	≥ 1	Updating the Devices(see page 69)
≥ 1	0	Restarting the Devices(see page 74)

Updating the Devices

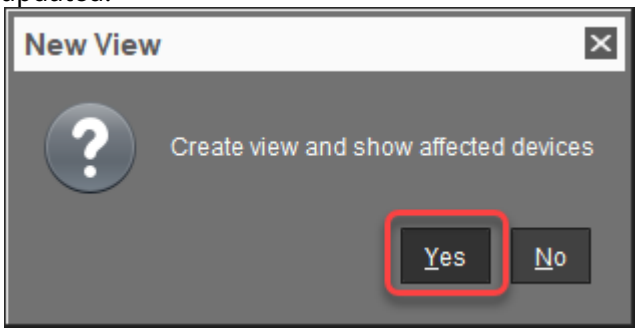
The devices listed at **Devices without the required feature** do not have the capability to exchange the ICG certificate and must be updated to IGEL OS 11.04.240 or higher.

To update these devices:

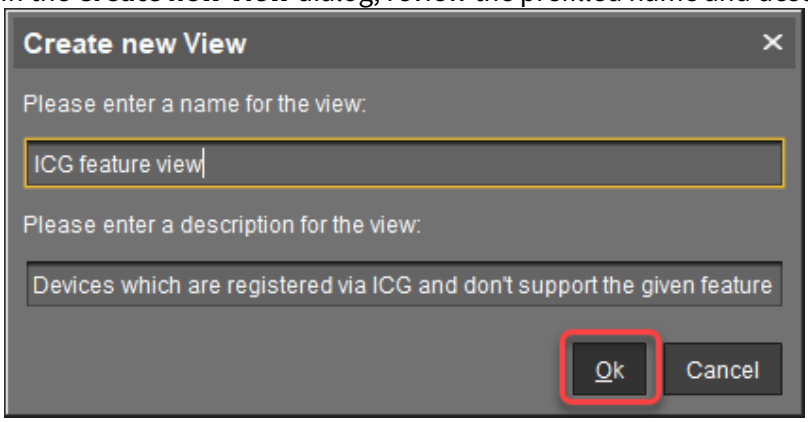
1. Click **Show devices**.



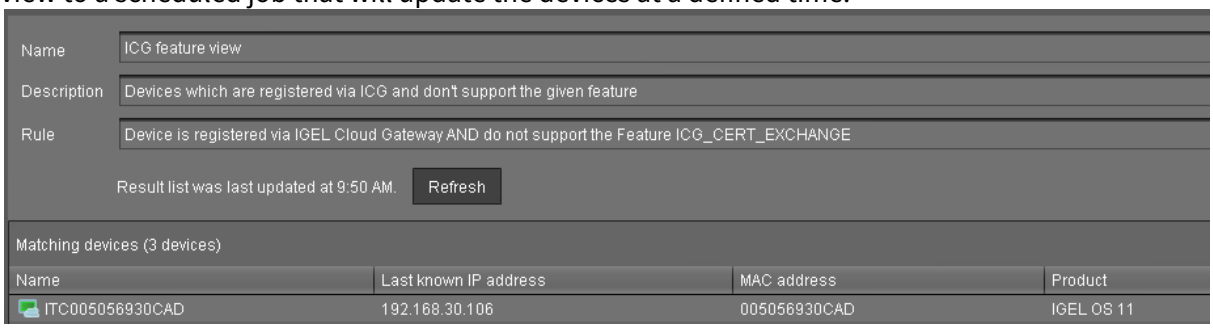
2. In the confirmation dialog, click **Yes** to create a view that collects the devices that need to be updated.



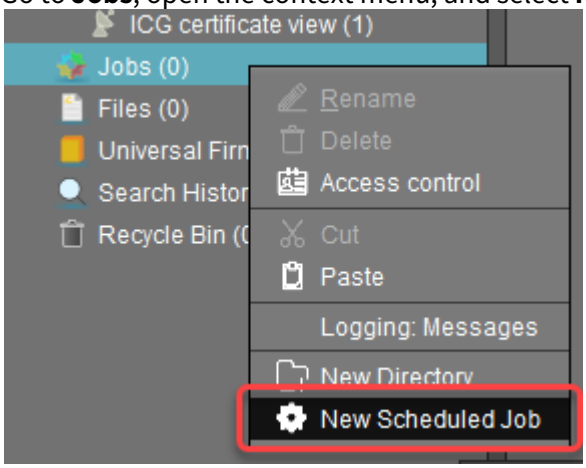
3. In the **Create new View** dialog, review the prefilled name and description, and click **Ok**.



The view is created, and the UMS Console switches to the newly created view. We will assign this view to a scheduled job that will update the devices at a defined time.

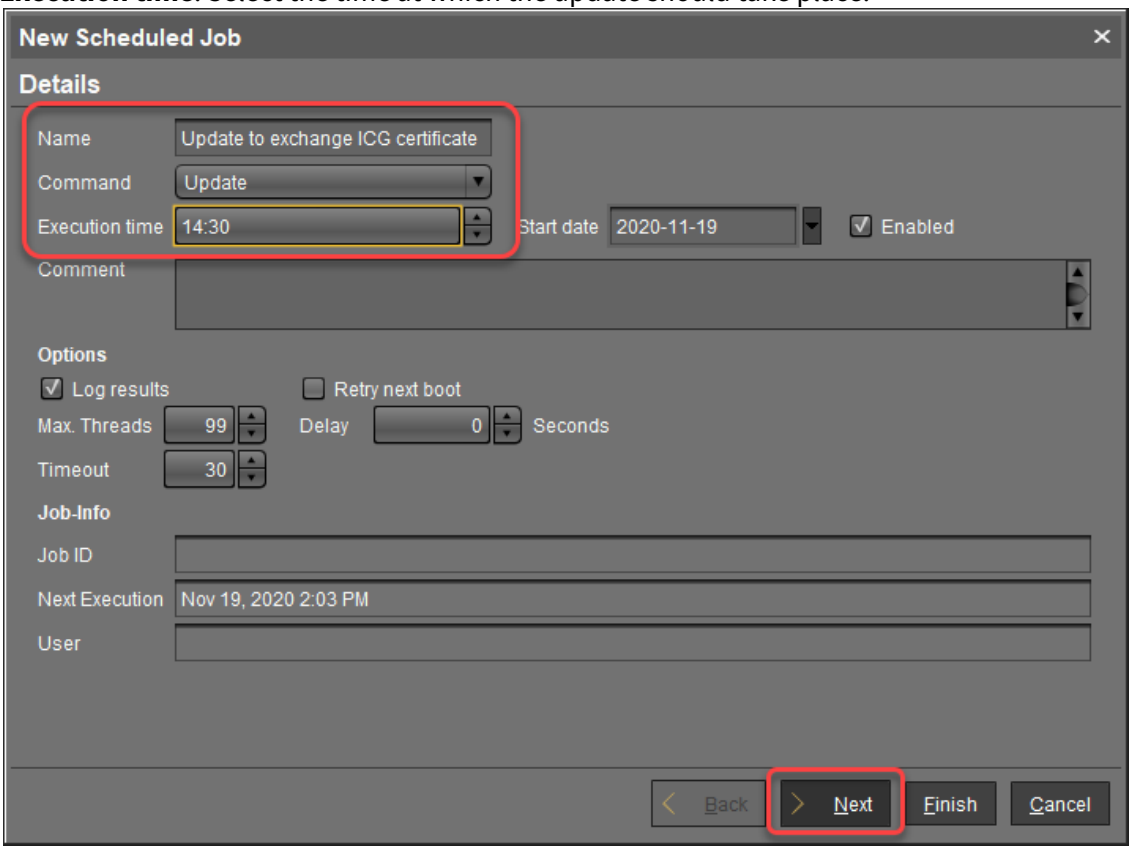


4. Go to **Jobs**, open the context menu, and select **New Scheduled Job**.

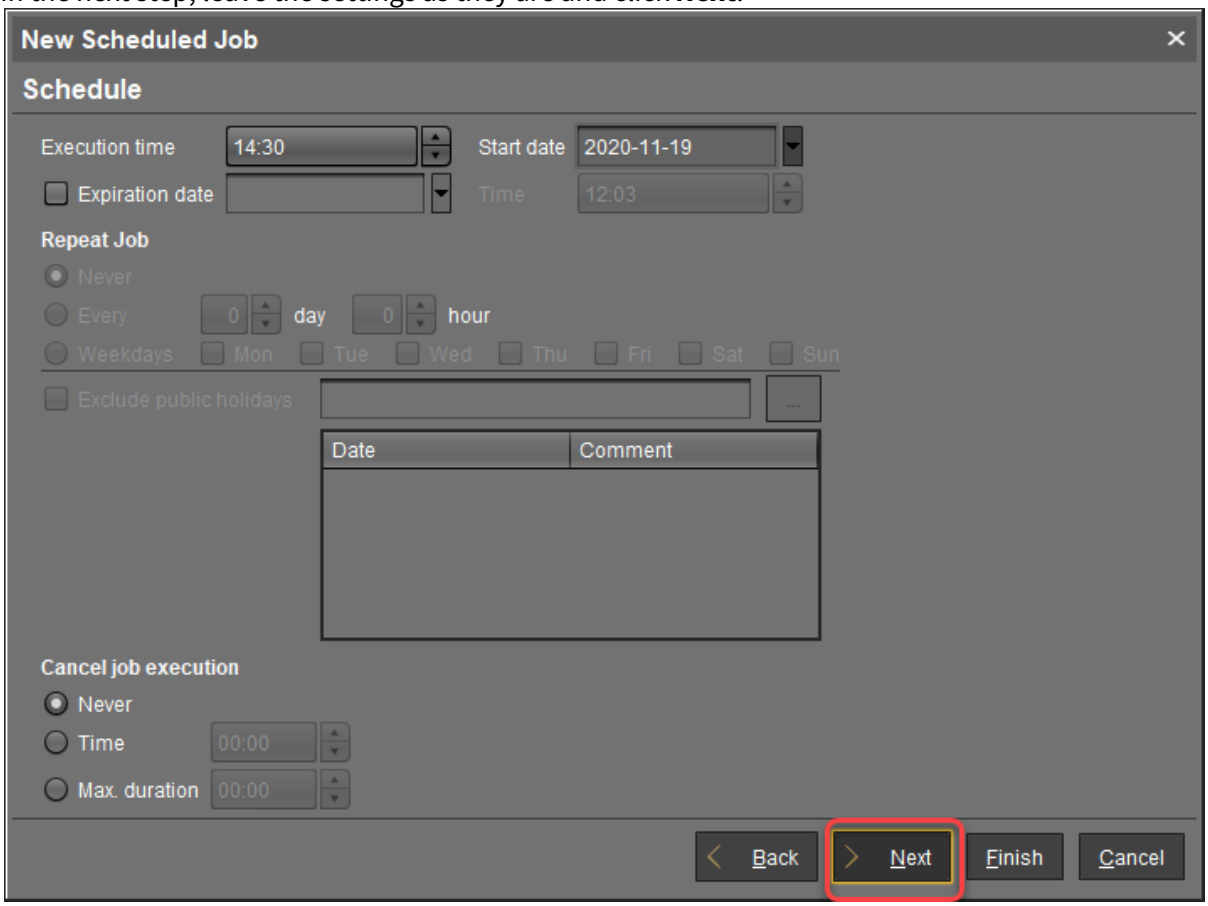


5. In the **New Scheduled Job** window, change the settings as follows and click **Next**:
   - **Name**: A name for the job
   - **Command**: Select "Update".

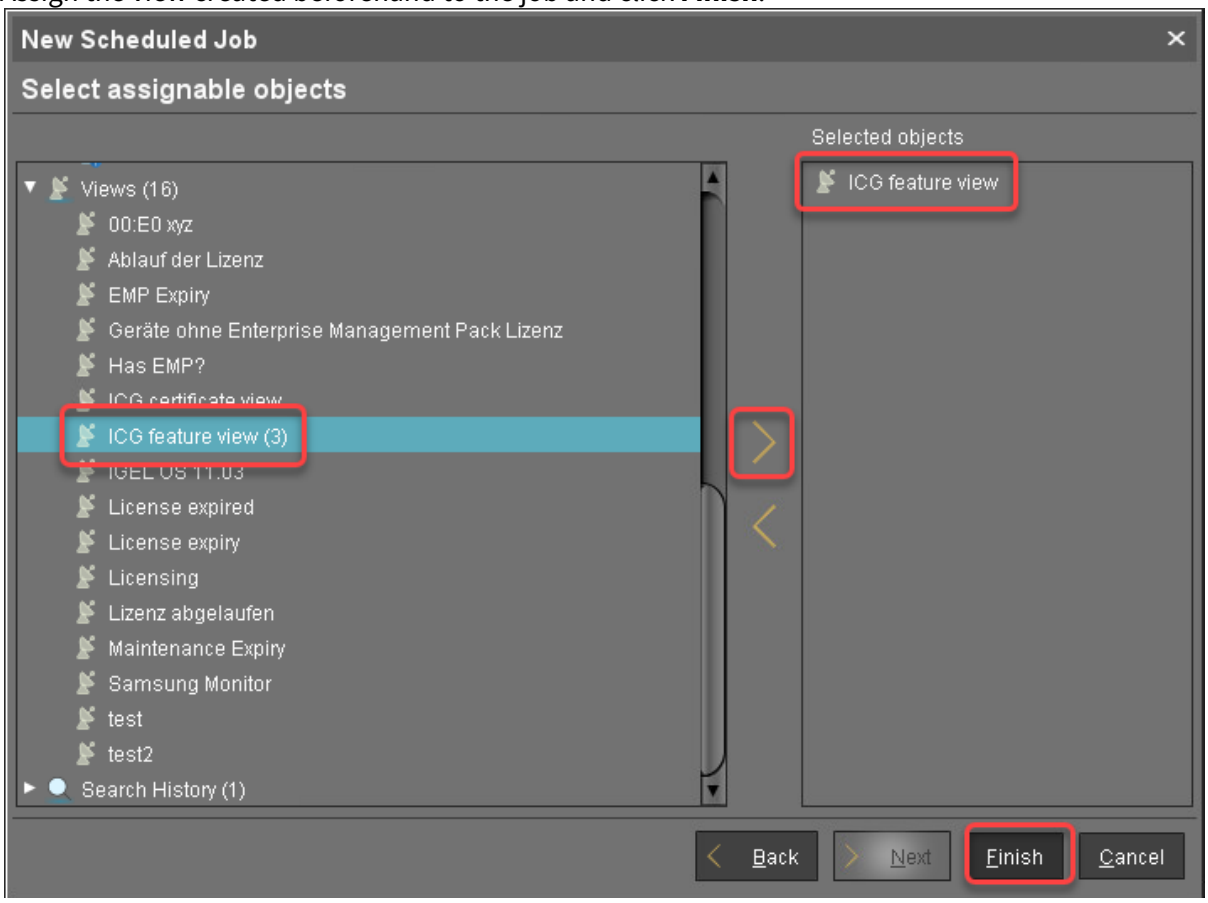
- **Execution time**: Select the time at which the update should take place.



6. In the next step, leave the settings as they are and click **Next**.



7. Assign the view created beforehand to the job and click **Finish**.

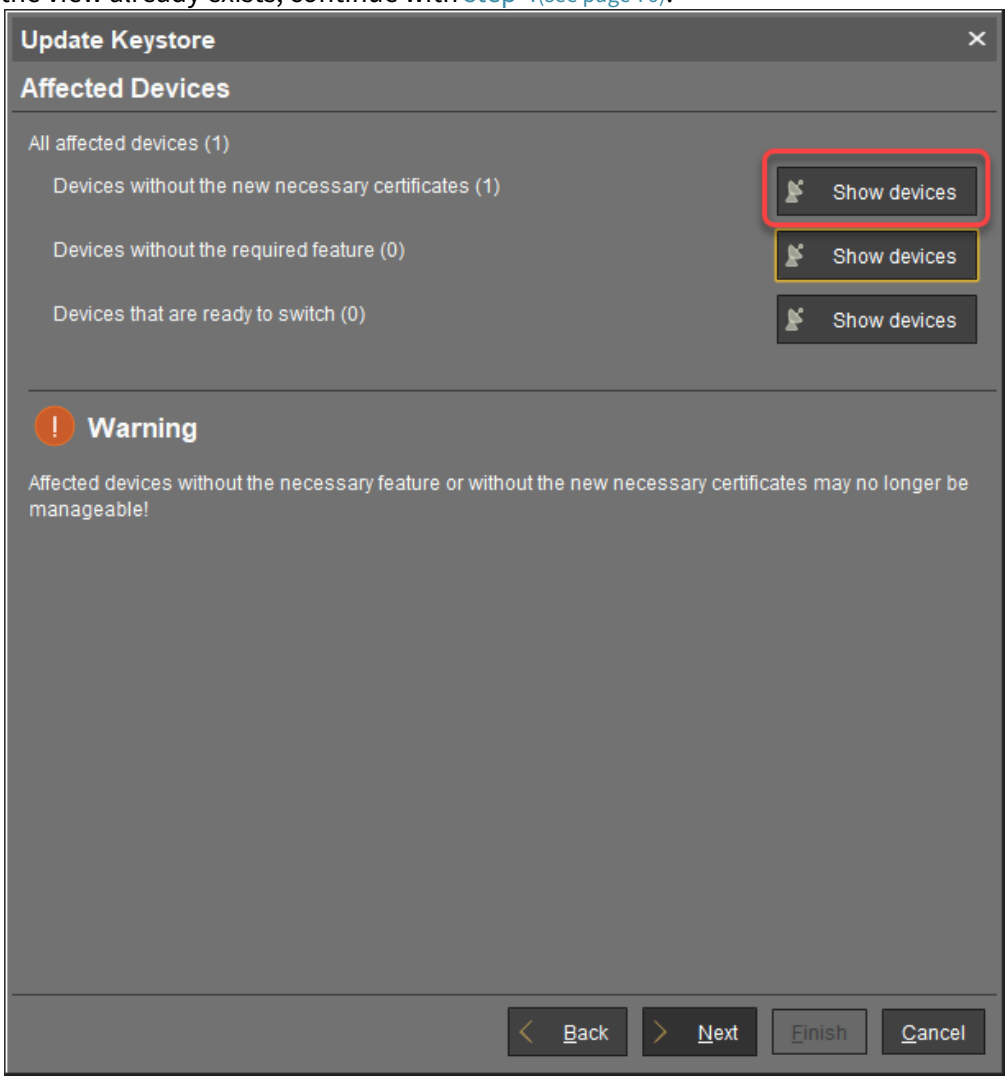


8. Make sure that IGEL OS 11.04.240 or higher is available and the upload source is available and configured on the devices; for details, see Firmware Update.
   The firmware will be updated at the specified time.
9. When the devices are updated, continue with Restarting the Devices(see page 74).

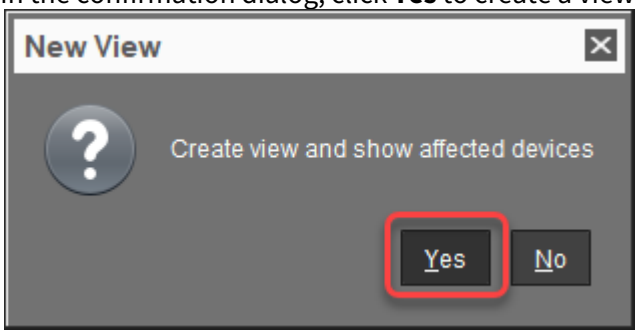
Restarting the Devices

When the devices are updated, they have the feature required to receive the new ICG root certificate. They will receive the new root certificate on reboot, for which we will create a scheduled job.

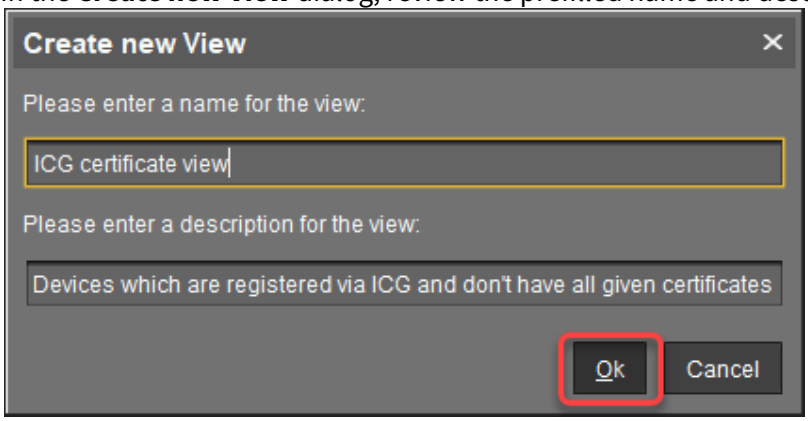
1. If you have not already created a view (see Updating the Devices(see page 69)), click **Show devices**. If the view already exists, continue with step 4(see page 76).



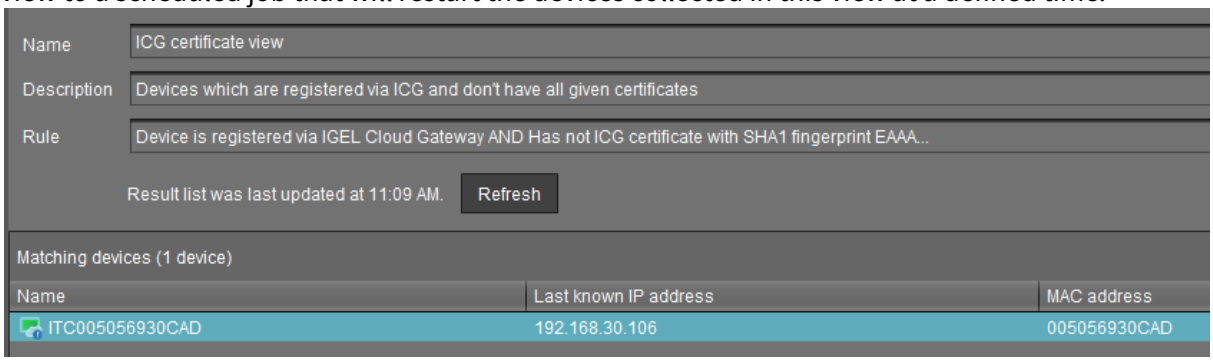
2. In the confirmation dialog, click **Yes** to create a view that collects the affected devices.



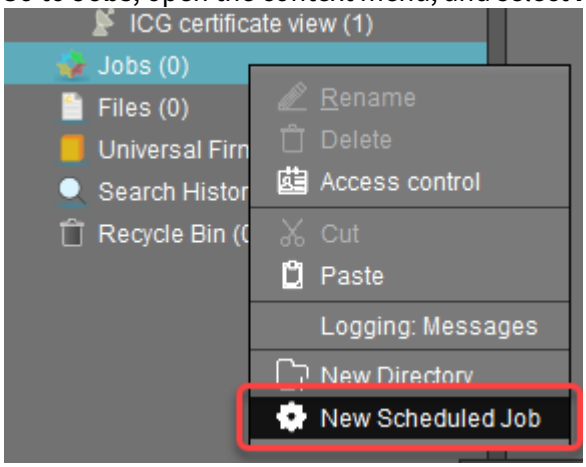
3. In the **Create new View** dialog, review the prefilled name and description, and click **Ok**.



The view is created, and the UMS Console switches to the newly created view. We will assign this view to a scheduled job that will restart the devices collected in this view at a defined time.

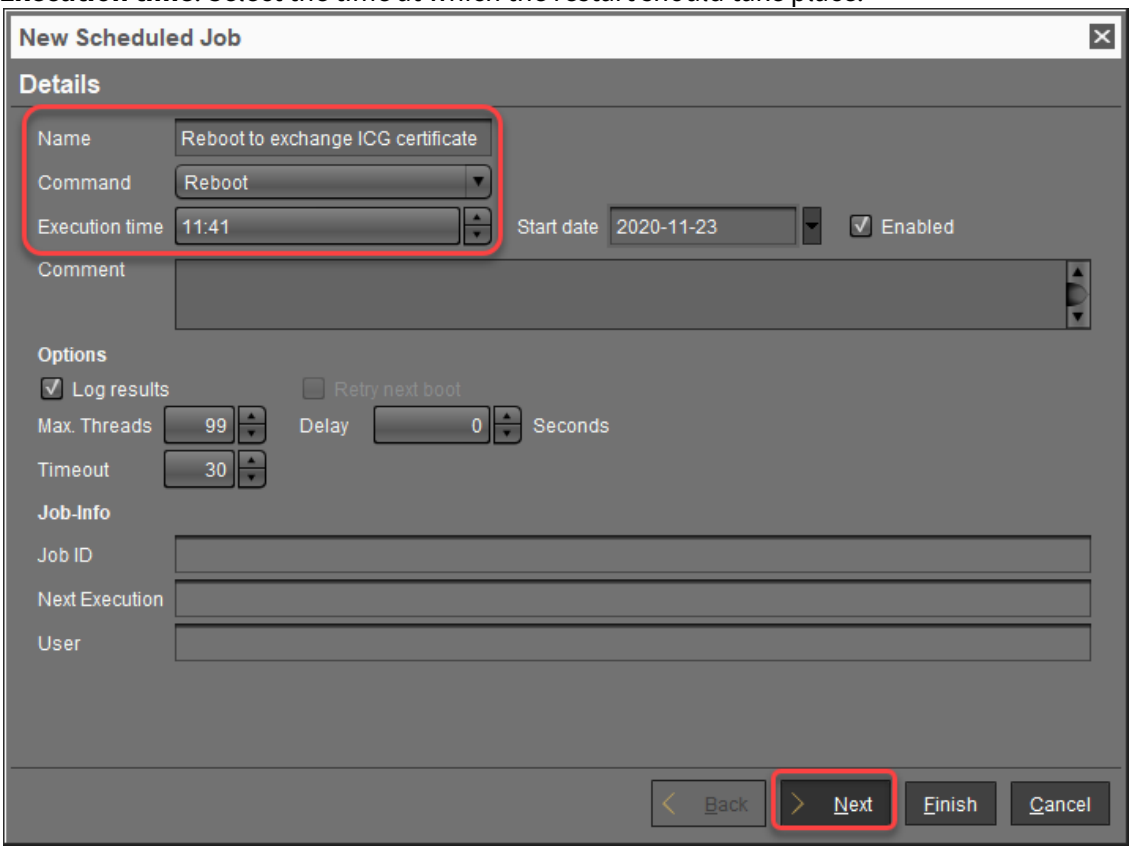


4. Go to **Jobs**, open the context menu, and select **New Scheduled Job**.

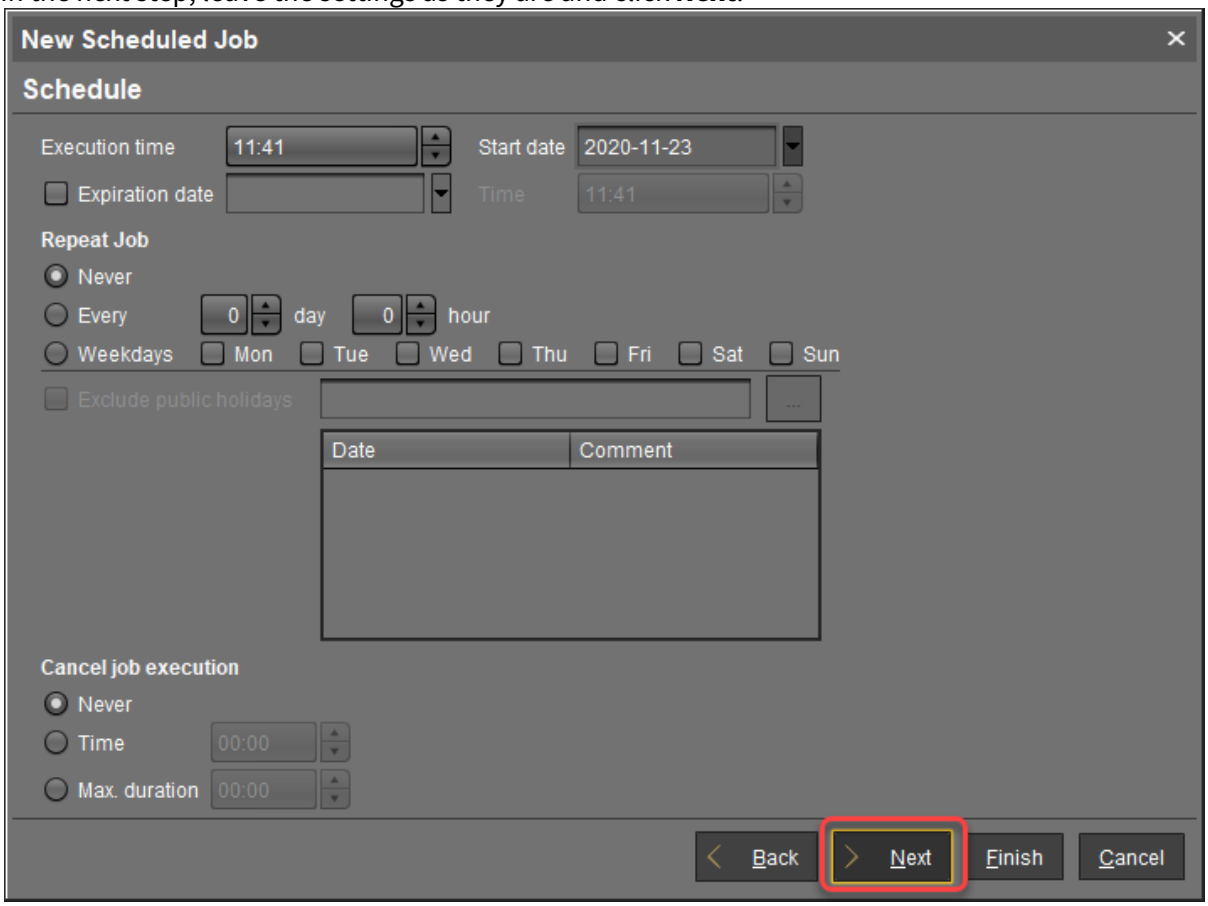


5. In the **New Scheduled Job** window, change the settings as follows and click **Next**:
   - **Name**: A name for the job
   - **Command**: Select "Reboot"

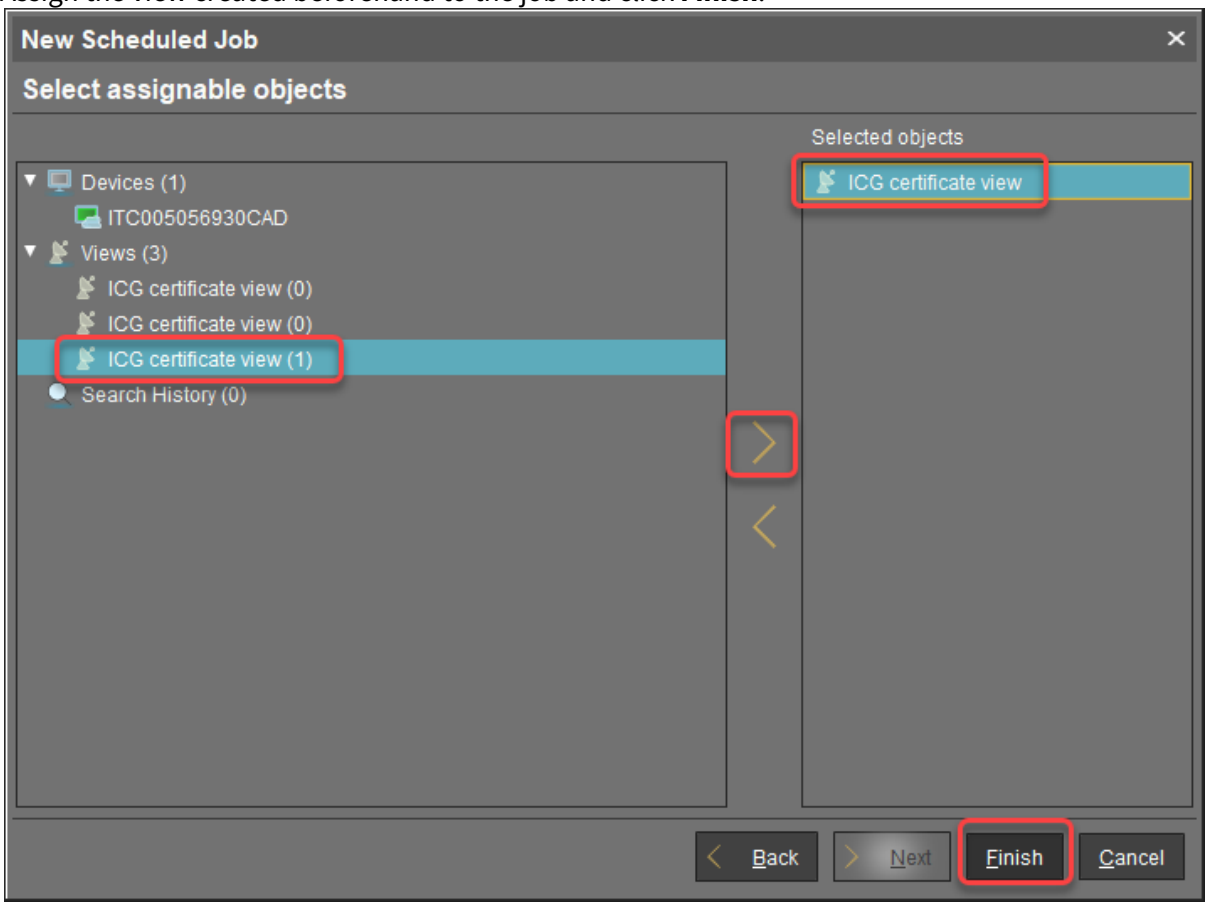
- **Execution time**: Select the time at which the restart should take place.



6. In the next step, leave the settings as they are and click **Next**.



7. Assign the view created beforehand to the job and click **Finish**.

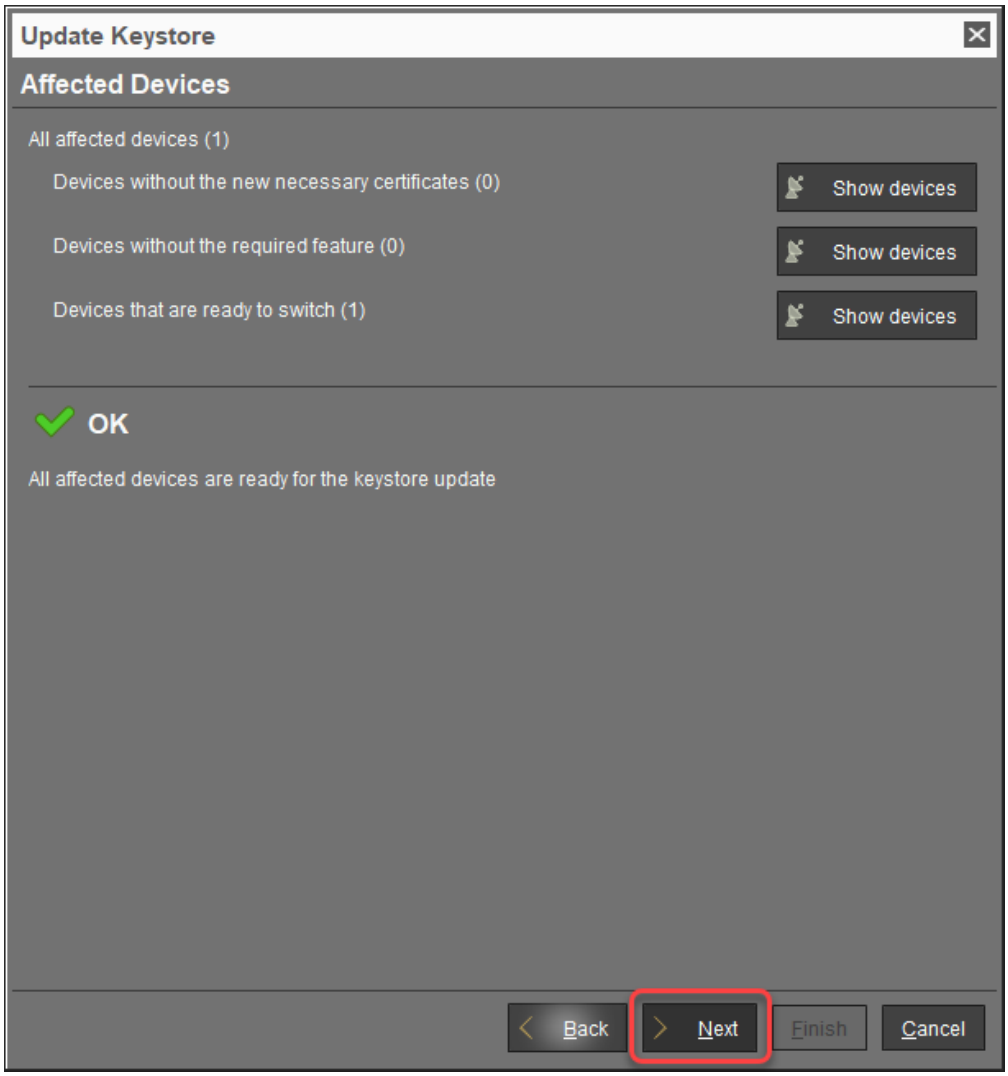


On reboot, the devices will receive all ICG certificates from the UMS; afterward, they are ready to switch to the new certificate.

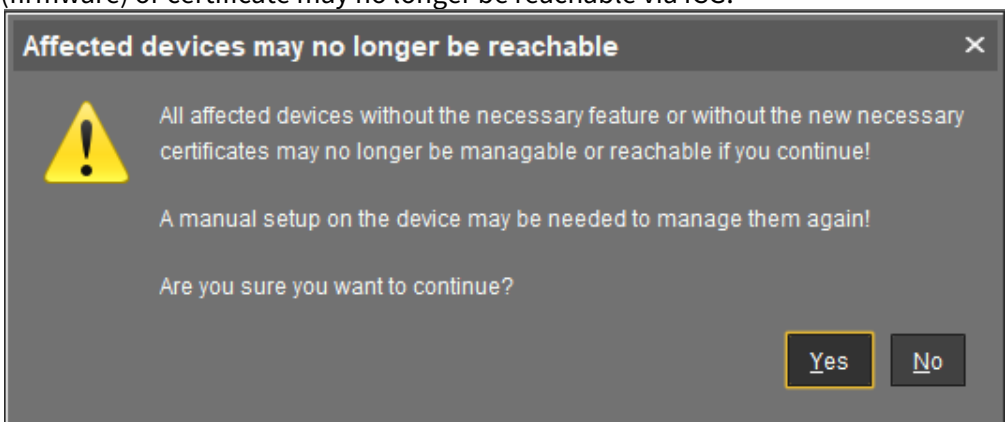
8. Continue with Updating the Keystore(see page 79).

Updating the Keystore

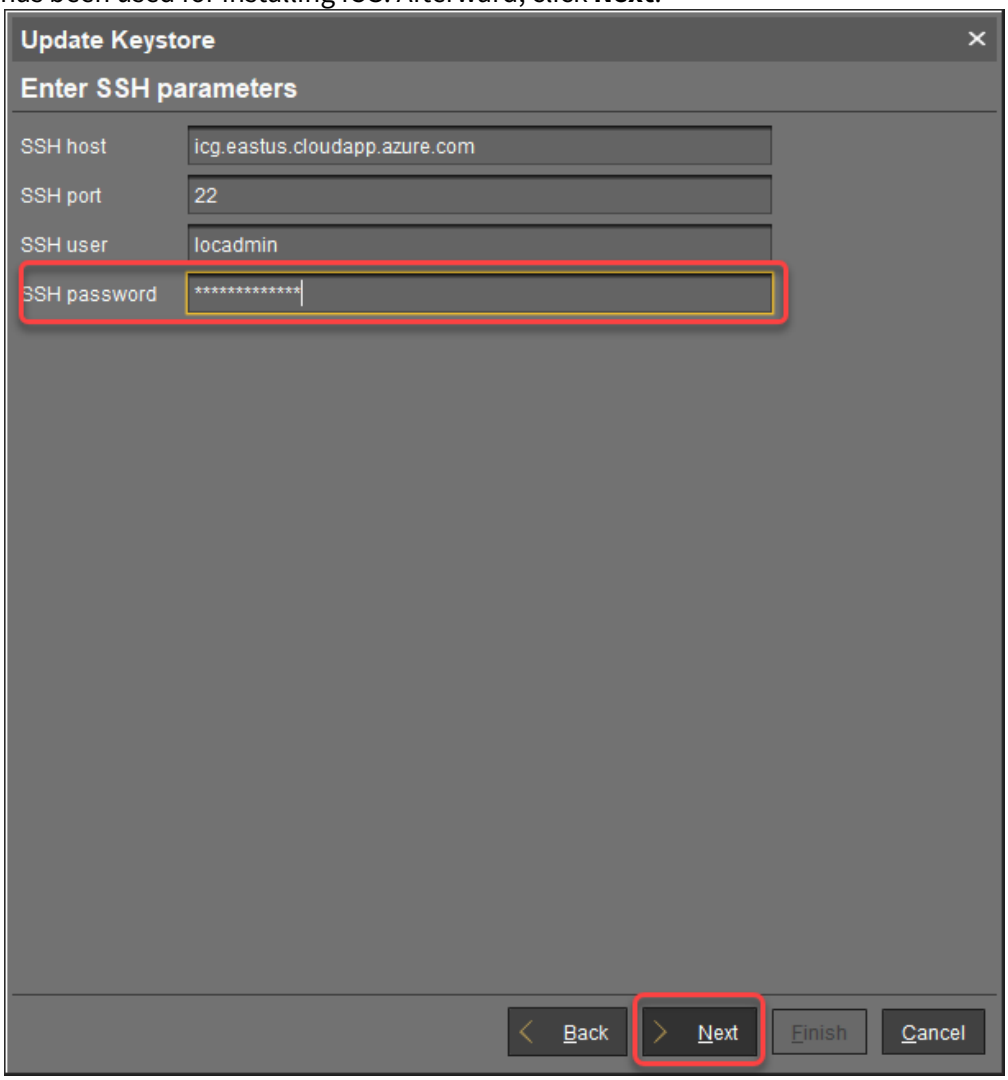
1. To check if the devices are ready, go back to **UMS Administration > UMS Network > IGEL Cloud Gateway**, click to open the **Update Keystore** dialog, select the new certificate, click **Next** and look at the displayed numbers. If the output looks like this, click **Next**.



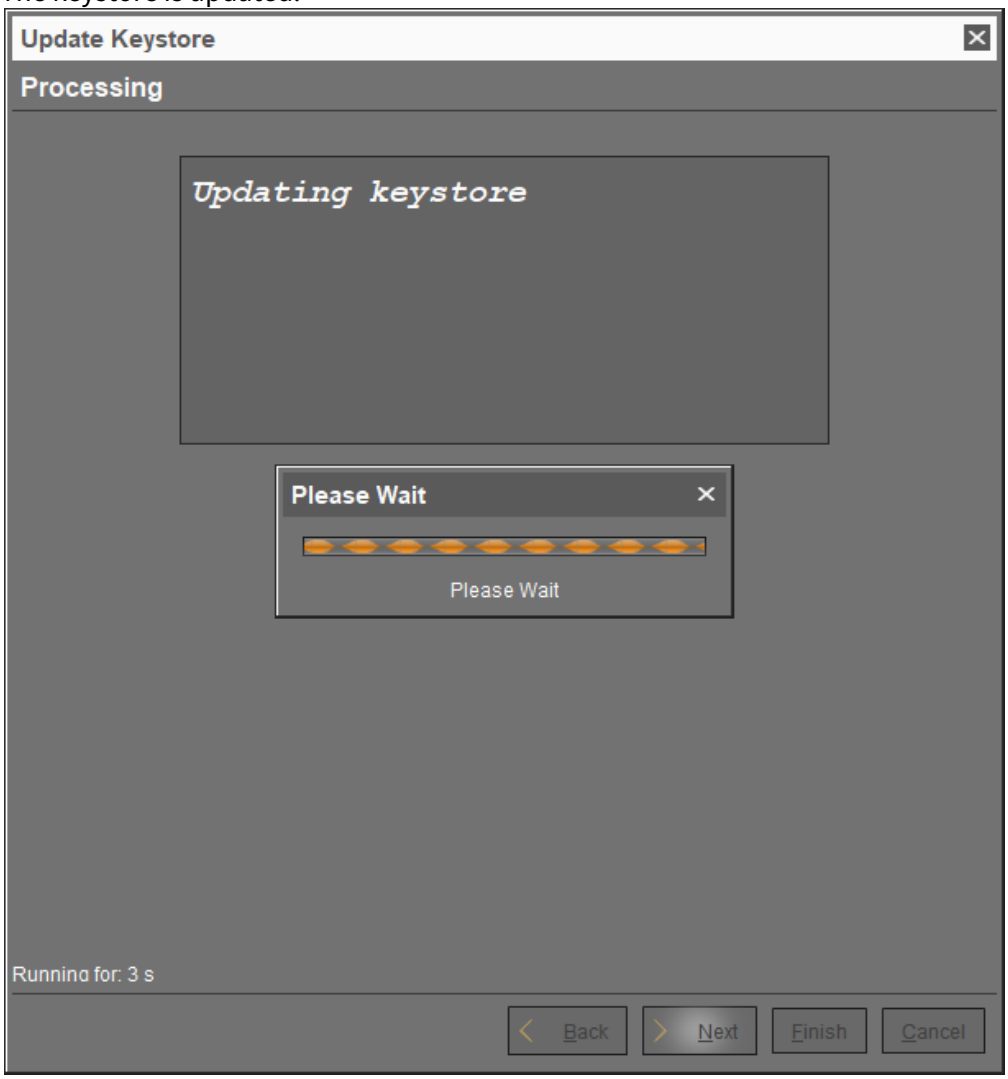
If the following warning message appears, you should check if all devices have been updated successfully. If you click **Yes** to continue, those devices which do not have the required feature (firmware) or certificate may no longer be reachable via ICG.



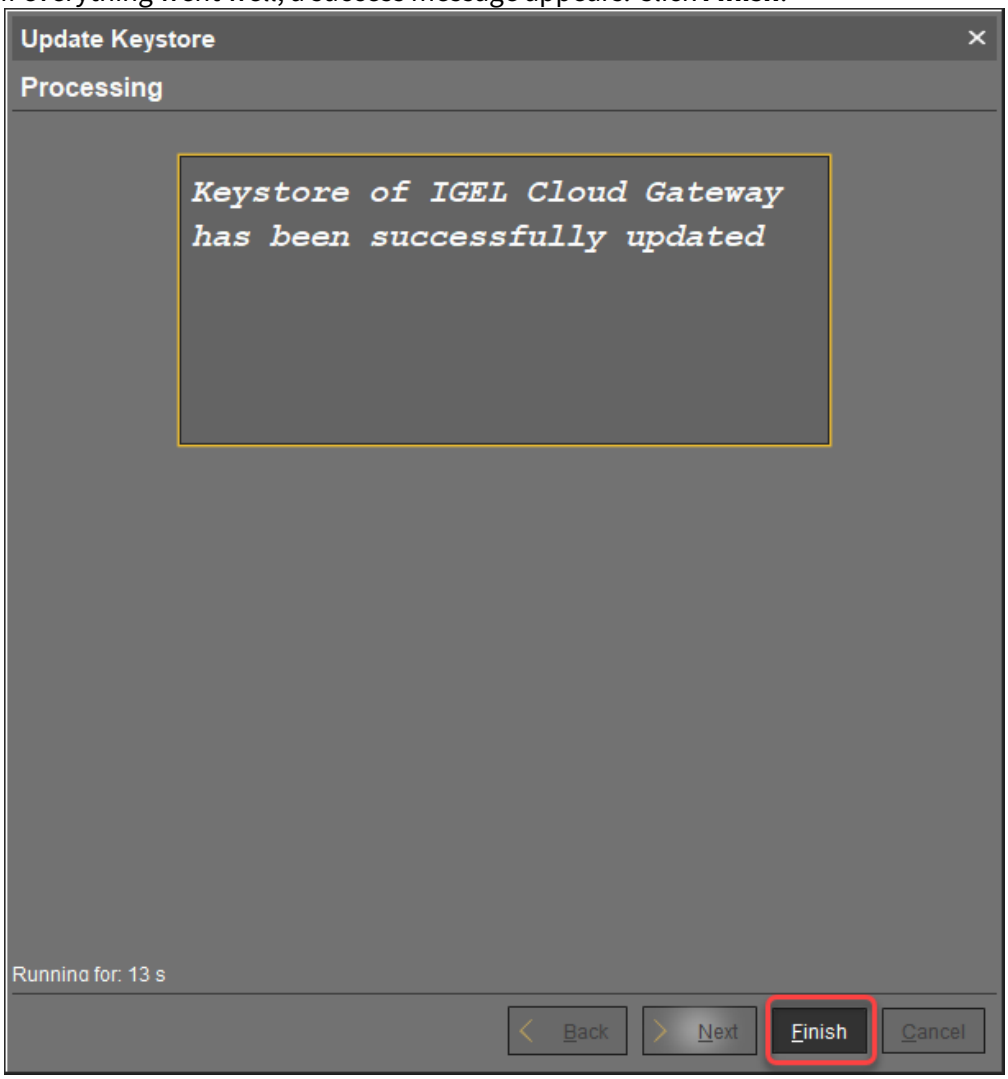
2. Enter the password for the **SSH user** that exists at the ICG server. This is the same password that has been used for installing ICG. Afterward, click **Next**.



The keystore is updated.



3. If everything went well, a success message appears. Click **Finish**.



Moving an Endpoint Device to an ICG

Overview

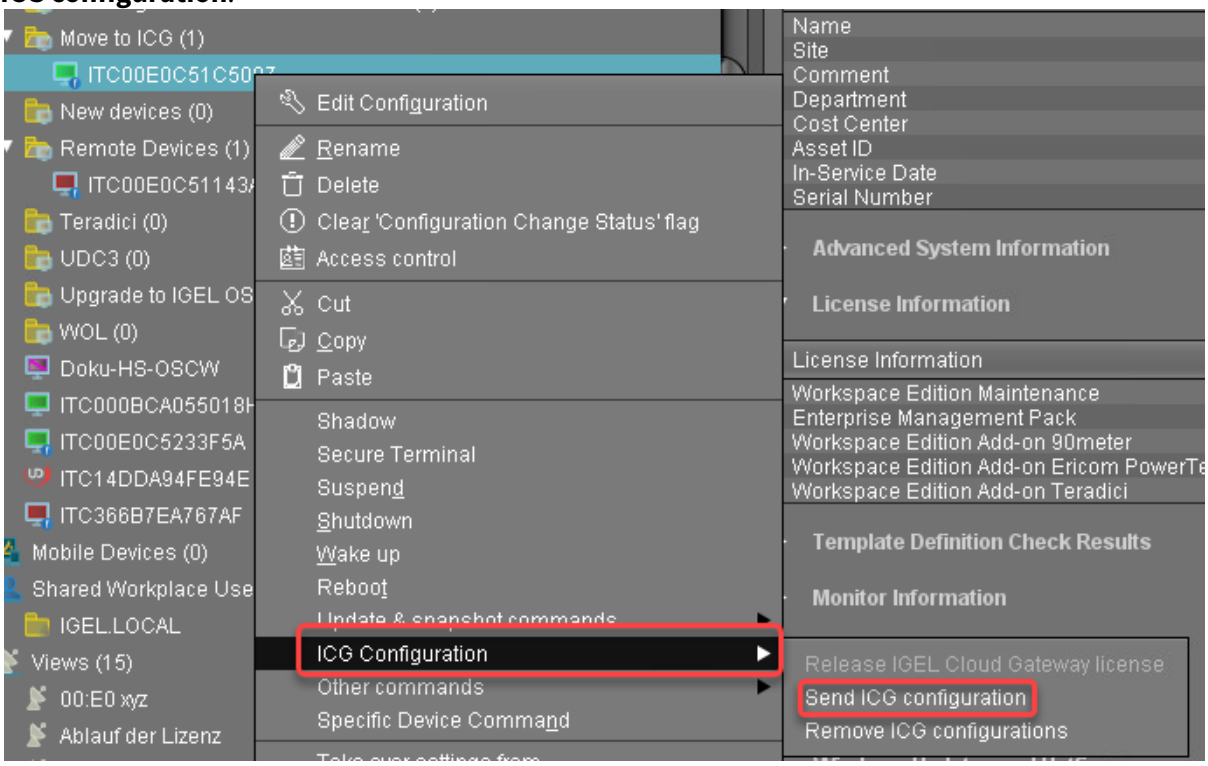
You can move an endpoint device from the local network to a remote location where it will be connected via ICG. Also, you can move an endpoint device from one ICG server to another one.

Environment

- UMS 6.06 or higher
- ICG 2.02 or higher
- IGEL OS 11.04.240 or higher

Instructions

1. Select all devices you want to move, open the context menu and select **ICG Configuration > Send ICG configuration**.



2. In the **Send configuration of one ICG** dialog, select the ICG to which you want to move the devices, and click **Select ICG**:

If everything went well, the devices connect to the specified ICG. If the ICG is not reachable at this moment, the ICG configuration remains unchanged, and the devices stay connected to the local UMS network or to the old ICG.

Removing an Endpoint Device from ICG

Overview

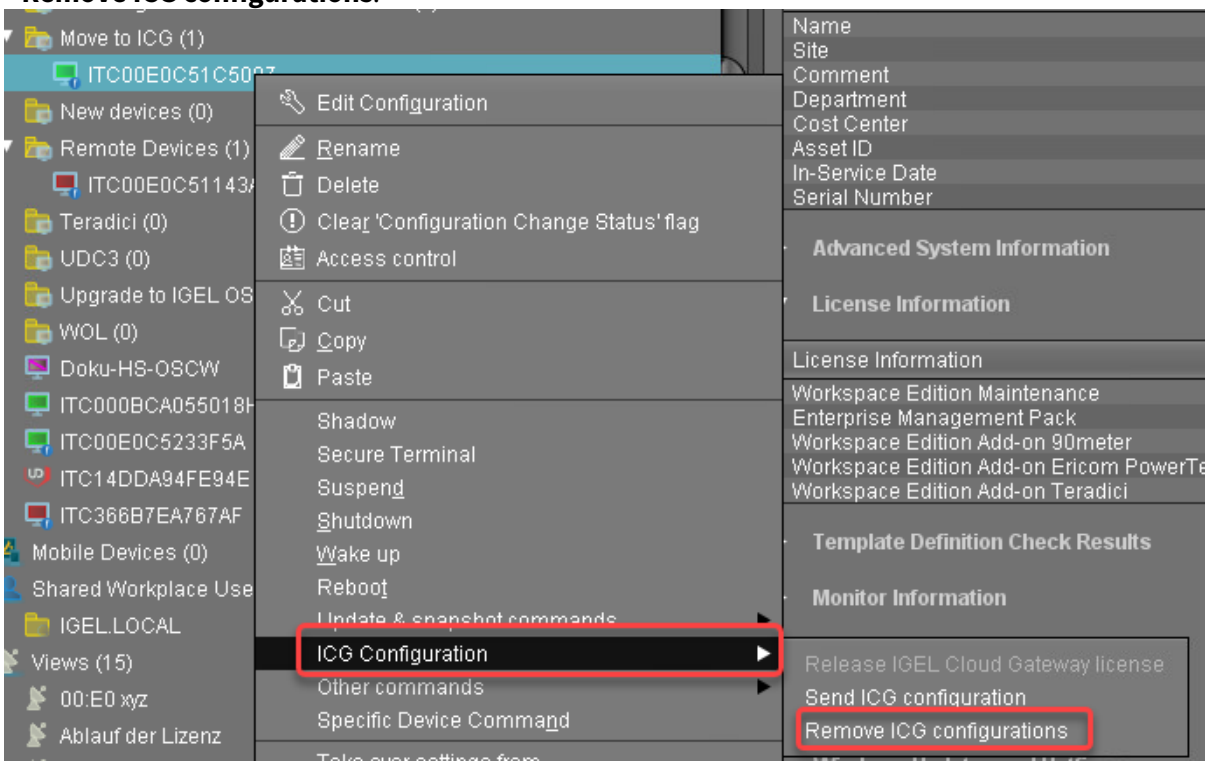
When an endpoint device with an ICG configuration is connected to the local UMS network, it will automatically switch to the local UMS connection. If you want to prevent the device from using the ICG permanently, you can remove its ICG configuration.

Environment

- UMS 6.06 or higher
- ICG 2.02 or higher
- IGEL OS 11.04.240 or higher

Instructions

1. Make sure that the endpoint devices are connected to the local UMS network.
2. Select all devices you want to remove from an ICG, open the context and select **ICG Configuration > Remove ICG configurations**.



The endpoint device is removed from the ICG.

Network Ports Used

By default, the ICG accepts incoming connections on the TCP port 8443, both from the UMS and endpoint devices. This port can be changed

- on the ICG server in the interactive installer
- in UMS in **UMS Administration > UMS Network > IGEL Cloud Gateway**.

Controlling the ICG Daemon

The ICG is started automatically on system boot and immediately after its installation. Additionally, there are commands to control the ICG during operation.

> You must use Systemd or SysVInit commands exclusively. For example, you cannot restart an ICG daemon started with Systemd with a SysVInit command.

> Although the commands return immediately, the ICG takes 10 to 15 seconds to actually start or stop.

On Systemd Installations (recommended)

You can issue the following commands as root:

- View the ICG status: `systemctl status icg-server.service`
- Start the ICG: `systemctl start icg-server.service`
- Restart the ICG (after configuration changes): `systemctl restart icg-server.service`
- Stop the ICG: `systemctl stop icg-server.service`

On Systems using SysVInit

You can issue the following commands as root:

- Start the ICG: `/etc/init.d/tomcat start`
- Restart the ICG (after configuration changes): `/etc/init.d/tomcat restart`
- Stop the ICG: `/etc/init.d/tomcat stop`

Optional: Adding a TXT Record for the ICG Server

You can simplify the entry of the ICG server address for your users with a simple DNS tweak.

▶ Add a TXT record for the host `igel-cloud-gateway` with the contents `https://[ICG IP address]:8443/usg/endpoint`

When users enter their email address `user@example.com` as the server address in the ICG Agent Setup, the setup will look up this record on the `example.com` nameserver and find the gateway address to connect to.

ICG FAQ

- Can I Use Active Directory from a Remote Endpoint Device?(see page 91)

Can I Use Active Directory from a Remote Endpoint Device?

Question

My users are working from remote, so their endpoint devices are connected to the UMS via ICG. Can they log in to their device via Microsoft Active Directory (AD)?

Environment

This article is valid for the following environment:

- IGEL OS 11
- IGEL Unified Management Suite (UMS) 6.01 or higher
- IGEL Cloud Gateway (ICG) 2.01 or higher
- Microsoft Active Directory (AD)

Answer

You can use IGEL Shared Workplace (SWP); with Shared Workplace, users will log in via Active Directory, also if they are connected via ICG.

For complete instructions on setting up IGEL Shared Workplace, see SWP Configuration in the UMS Console.

For a quick reference, see the checklist underneath.

Checklist

✅ All relevant endpoint devices have IGEL Enterprise Management Pack (EMP) licenses.
To check this: In the UMS Console, go to **Server [UMS address] > Devices > [your device]** and scroll to **License Information** in the content panel.
For information on license deployment, see Setting up Automatic License Deployment (ALD) or Manual License Deployment for IGEL OS.

✅ The Active Directory is linked to the UMS.
To check this, open the UMS Console and go to **UMS Administration >Global Configuration > Active Directory / LDAP**.
For further instructions, see Linking an Active Directory.

✅ Shared Workplace is enabled on the relevant endpoint devices, preferably via a profile.
To check this, open the configuration dialog, go to **Security > Logon > Shared Workplace** and make sure that **Activate Shared Workplace** is enabled. Also, check the settings under **Logout Shortcut Locations**.

ICG How-Tos

- Using IGEL Cloud Gateway on Microsoft Azure Marketplace(see page 93)
- Preparing a Linux Machine for Installing IGEL Cloud Gateway (ICG)(see page 105)
- How to Configure Apache Tomcat for TLS 1.2 Only(see page 109)
- Certificate Management(see page 110)
- Installing the ICG without Remote Installer(see page 111)
- Connecting the UMS to the ICG(see page 113)
- Uninstalling ICG(see page 115)
- Updating ICG Manually(see page 116)
- Managing ICG Certificates with UMS(see page 117)
- Using Citrix NetScaler ADC as an SSL Bridge for ICG(see page 120)
- Giving a User sudo Privileges(see page 125)
- Updating Expired ICG Keystores(see page 126)
- Installing an Existing Certificate Chain (UMS 6.02 or Older)(see page 127)
- Creating Certificates from an Existing Root Certificate (UMS 6.02 or Older)(see page 133)
- Transferring the First-Authentication Keys to the Devices(see page 138)
- All Methods of Generating First-Authentication Keys for Devices(see page 143)
- Installing IGEL Cloud Gateway (UMS 6.02 or Lower)(see page 147)
- How to Monitor the IGEL Cloud Gateway(see page 155)
- How to Configure Java Heap Size for the ICG(see page 157)
- Installation of IGEL Cloud Gateway (ICG) on a SELinux System Failed(see page 159)

Using IGEL Cloud Gateway on Microsoft Azure Marketplace

Overview

IGEL offers preconfigured Linux virtual machines on Microsoft Azure Marketplace for installing an instance of IGEL Cloud Gateway (ICG).

This article presents an easy, straightforward way to prepare your virtual machine and install the ICG on it. However, an experienced user might prefer alternative methods or different settings.

> ⚠ Please note that Azure is a Microsoft product, therefore IGEL can not provide support for issues with Azure.

The following steps are required:

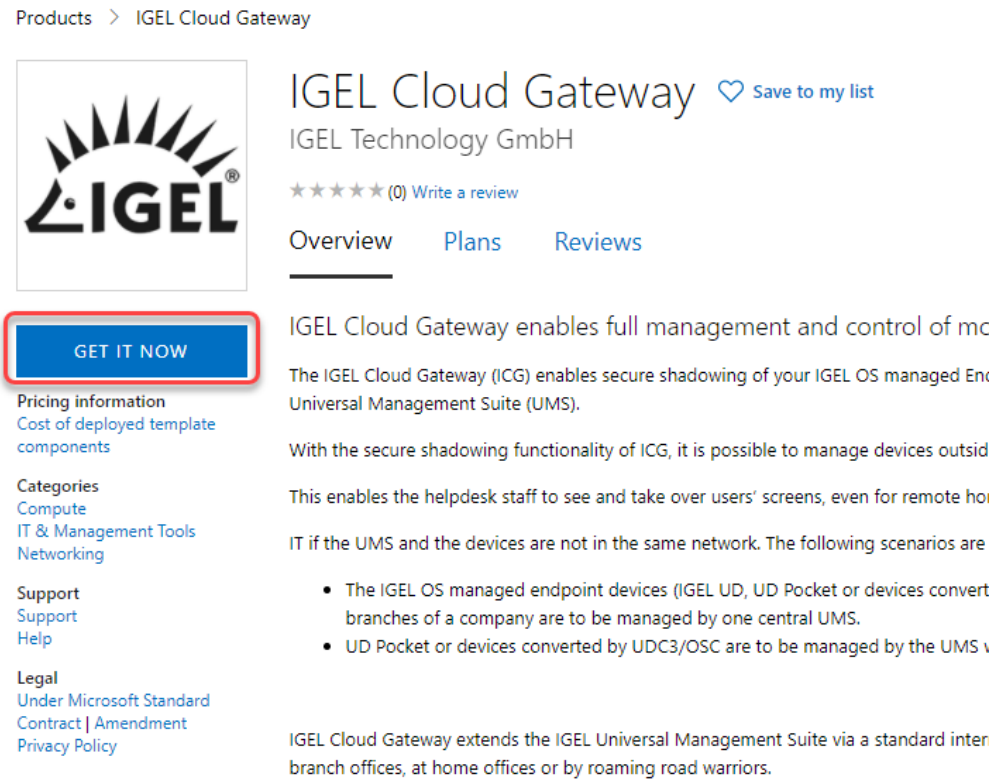
1. Creating the Resources(see page 93)
2. ICG Installation; see the Installation and Setup(see page 12) chapter in the ICG Manual
3. IMPORTANT! Disabling SSH Access(see page 100)

> ⓘ **Updating the ICG or the Keystore**
>
> If you need to update the ICG or the ICG keystore, you must enable SSH access temporarily; see EnablingSSHAccess(see page 102).
> IMPORTANT! Do not forget to disable SSH access afterward; see Disabling SSH Access(see page 100).

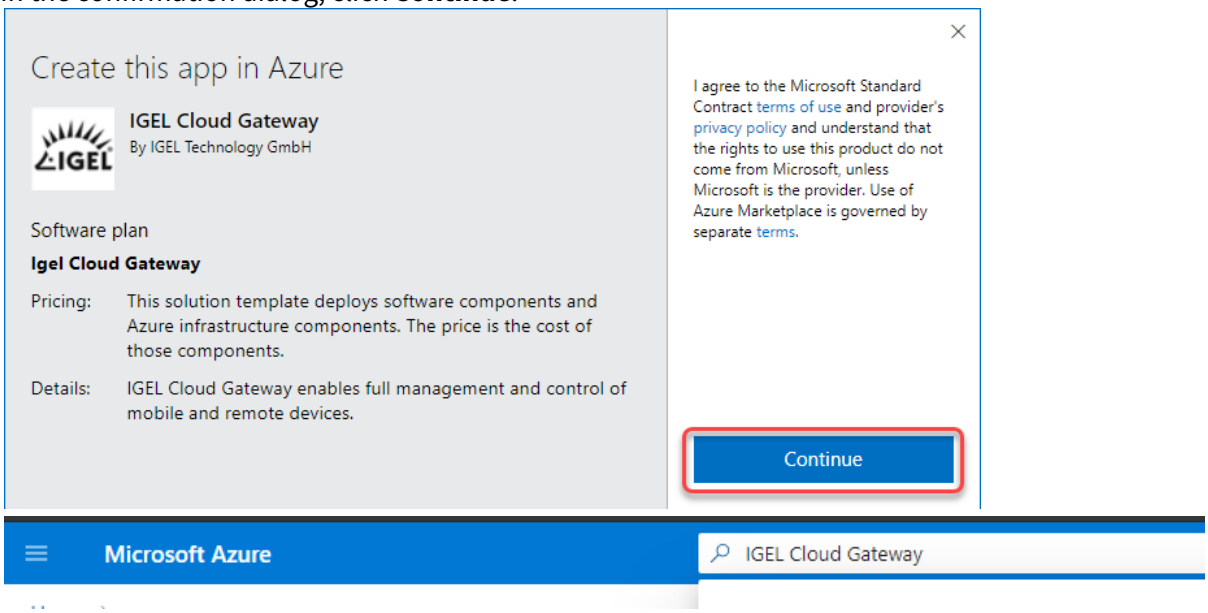
Creating the Resources

1. Log in to your Azure account. If you have no Azure account, create one first.

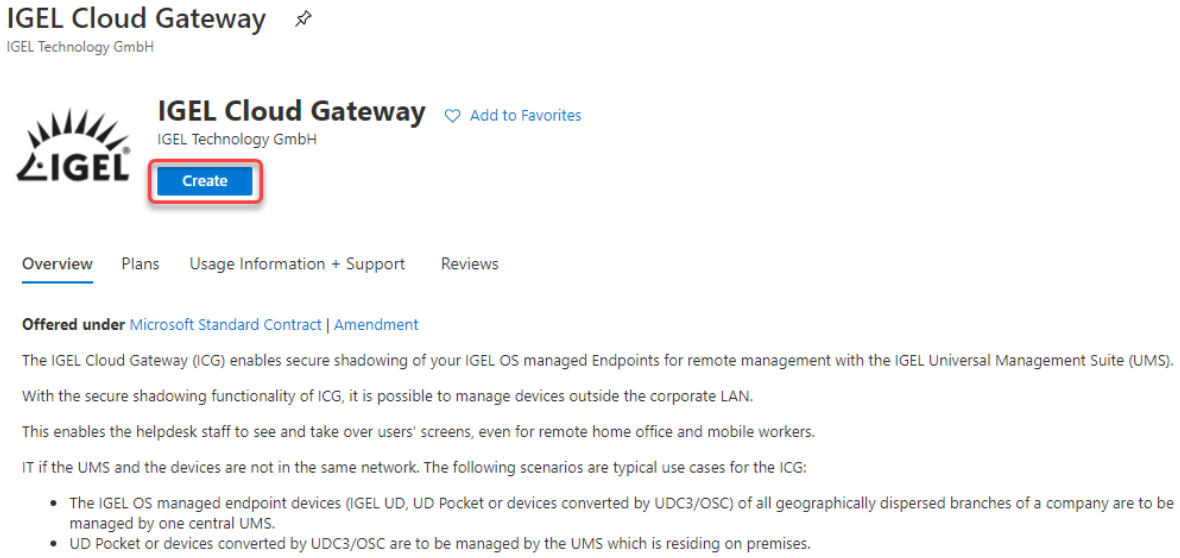
2. Go to https://azuremarketplace.microsoft.com/en-us/marketplace/apps/igeltechnologygmbh.igel-cloud-gateway and click **Get IT NOW**.



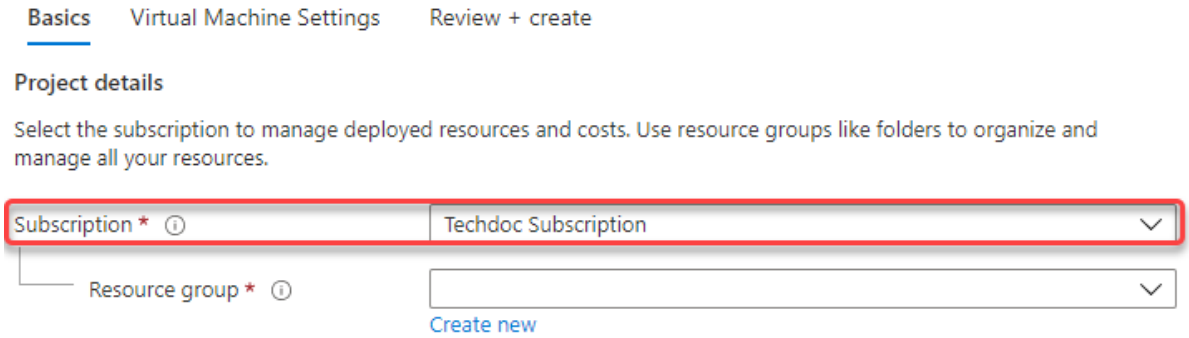
3. In the confirmation dialog, click **Continue**.



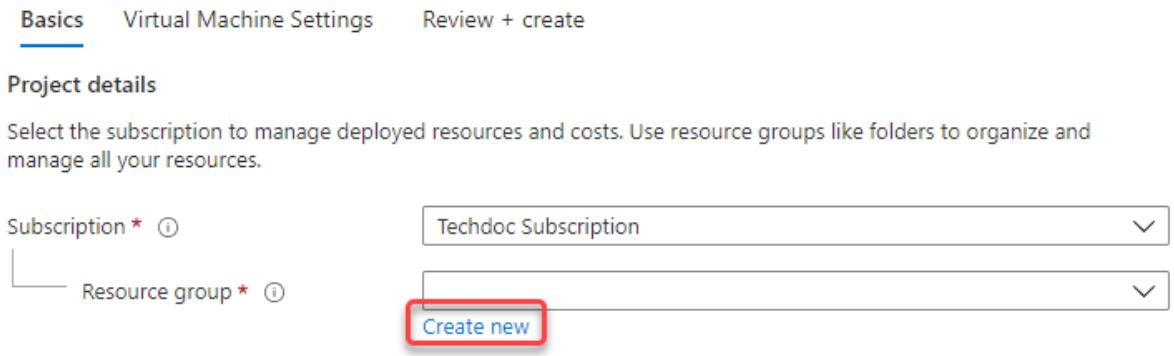
4. On the **IGEL Cloud Gateway** start page, click **Create**.



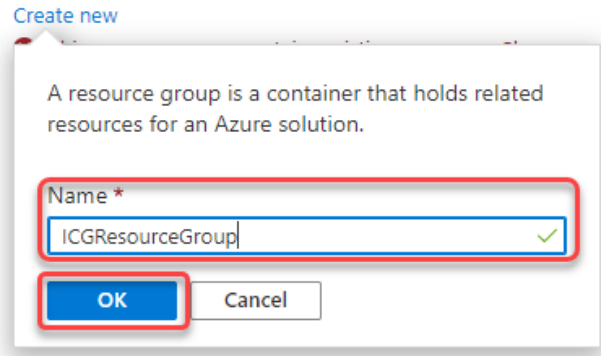
5. In the **Subscription** field, select the Azure subscription that is to be billed for this service.



6. If you have a pre-existent resource group that is empty, you can select it. Otherwise, click **Create new**.



7. In the resource group dialog, enter a **Name** and click **OK**.



8. Edit the following settings according to your needs:
   - **Region**: Choose the appropriate region.

     > It is recommended to define a greater area, which potentially makes your ICG more fail-safe. If your ICG is to be located in Germany, for instance, West Europe would be a good choice.

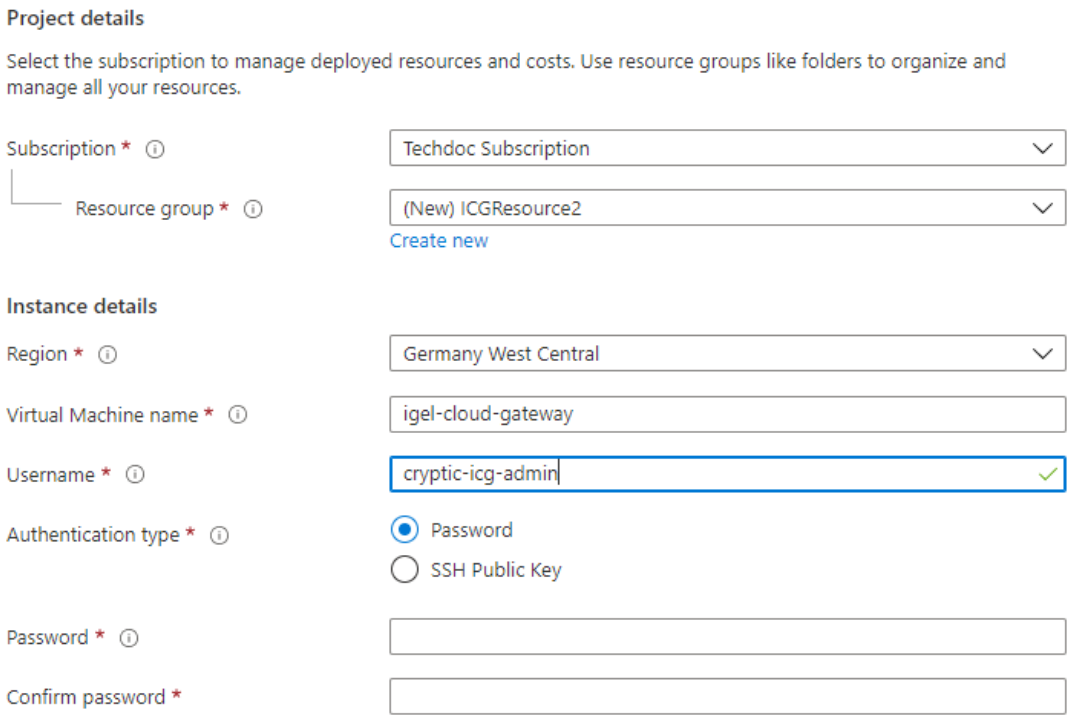
   - **Virtual Machine name**: Enter a name or leave it as it is.
   - **Username**: Enter a username for SSH access. This user account will be used for ICG installation by the UMS.

     > For security reasons, the username should be long (20 to 30 characters) and cryptic.

     > **Username "icg" Is Reserved**
     >
     > Do not use "icg" as a username for the remote installer; this is the username under which the Tomcat server is running.

   - **Authentication type**: Choose **Password**. (Currently, the ICG installation process only supports password authentication.)

- Under **Password** and **Confirm password**, enter a strong password (20 to 30 characters are recommended)

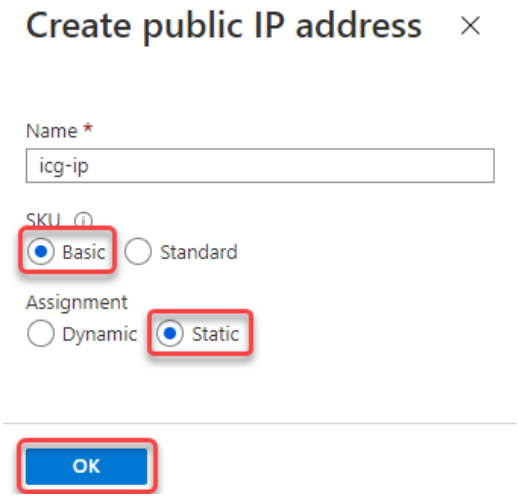


9. Click **Next: Virtual Machine Settings**.
10. Edit the settings according to your needs:
    - **Virtual machine size**: The pre-selected size should be appropriate for typical scenarios. If you need a different size, click **Change size**. The **B** series and **D** series are recommended. For minimum requirements, see Prerequisites(see page 5).
    - **Diagnostic storage account**: Leave this as it is or rename it if desired.

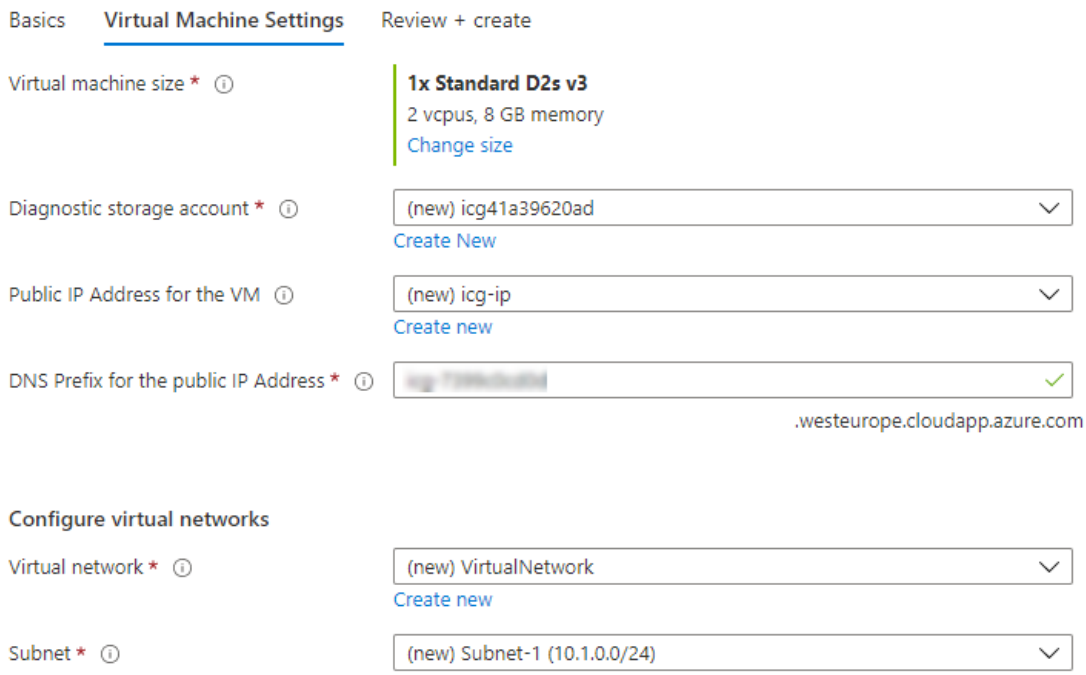
      > ⚠ Do not delete the diagnostic storage account, as the diagnostic data can be important for support cases.

    - **Public IP Address for the VM**: It is recommended to use a static IP address because firewalls typically check against IP addresses, not DNS names.
      i. Click **Create New**.
      ii. Under **Assignment**, select **Static**, then confirm with **OK**.
        - **SKU**: Select **Basic**.
        - **Assignment**: Select **Static**.

iii. Confirm with **OK**.

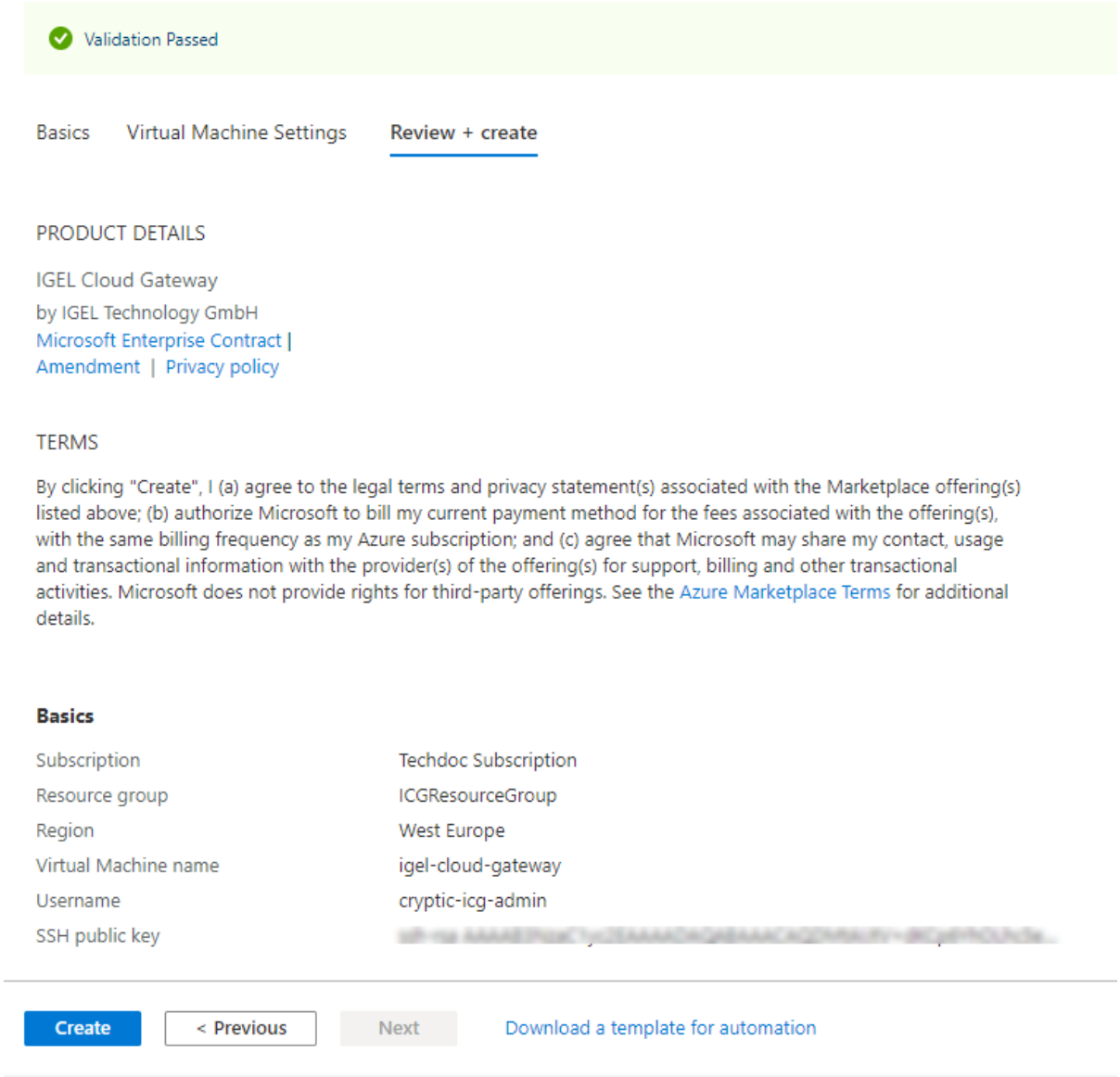


- **DNS Prefix for the public IP Address**: Freely editable component of the DNS name for the ICG. The DNS prefix must be unique within the region; if you enter a DNS prefix that is already in use, a warning will be displayed. The DNS name will be composed like this (example): `icg-abc123.germanywestcentral.cloudapp.azure.com`
- **Virtual network**: For advanced users. Allows for interconnecting networks, e.g. inside Azure or from the on-premises networks via VPN. If not required, leave this setting as it is.
- **Subnet**: Subnet for the virtual network.



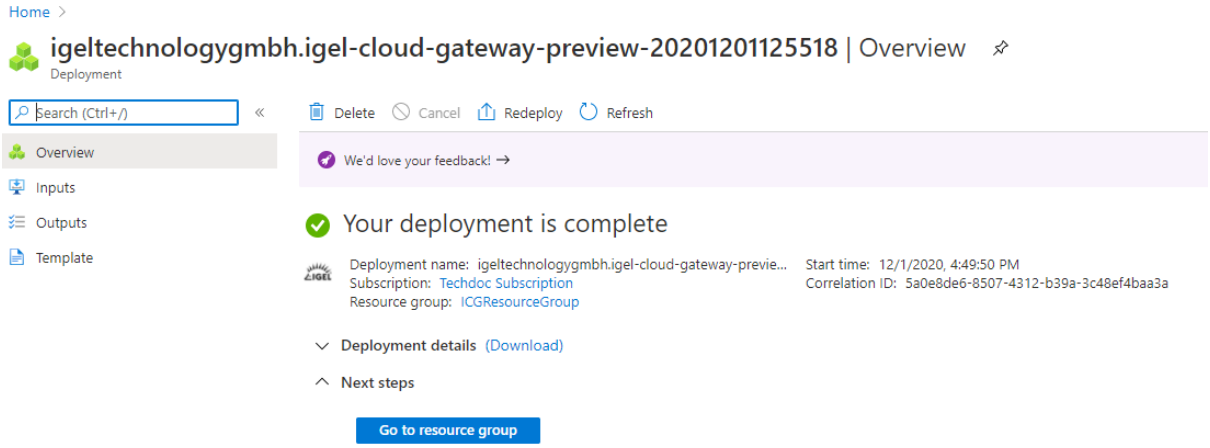
11. Click **Review + create**.
    The settings for the virtual machine are validated. If the validation is passed, the result should look

like this:



12. If the validation has errors, please fix them and retry.
13. To finally create the virtual machine, click **Create**.
    This process should take around 5 minutes.

When everything went well, the page should look like this:



14. Continue with installing the ICG; see the Installation and Setup(see page 12) chapter in the ICG Manual.
15. After the ICG has been installed successfully, do not forget to disable SSH for security reasons; see Disabling SSH Access(see page 100).

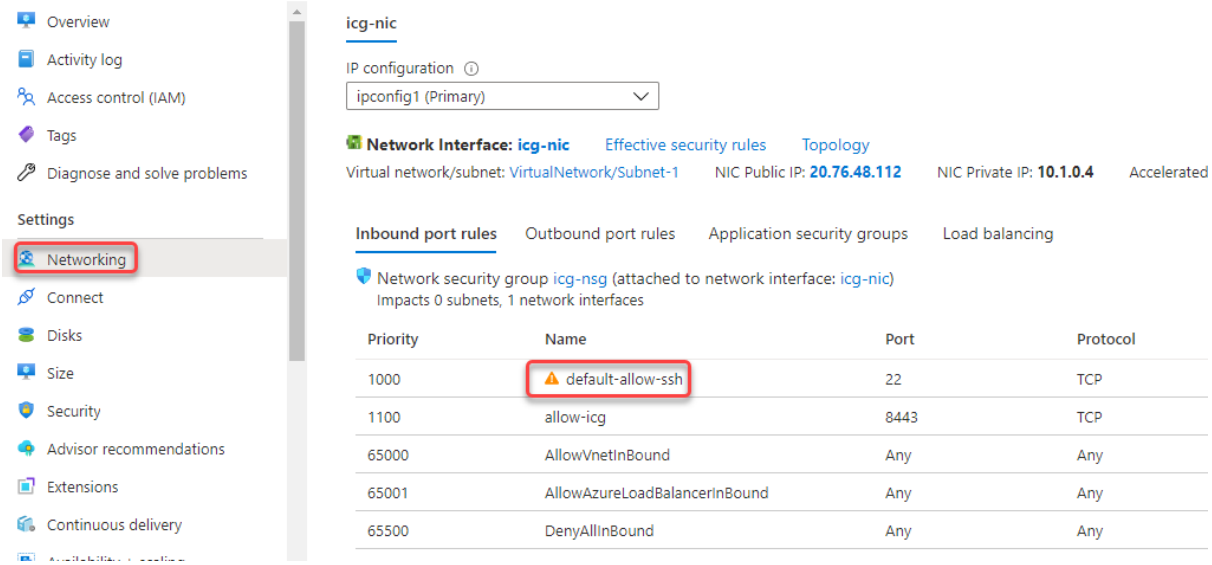
> Do not forget to DISABLE SSH ACCESS because SSH access poses a security risk!

IMPORTANT! Disabling SSH Access

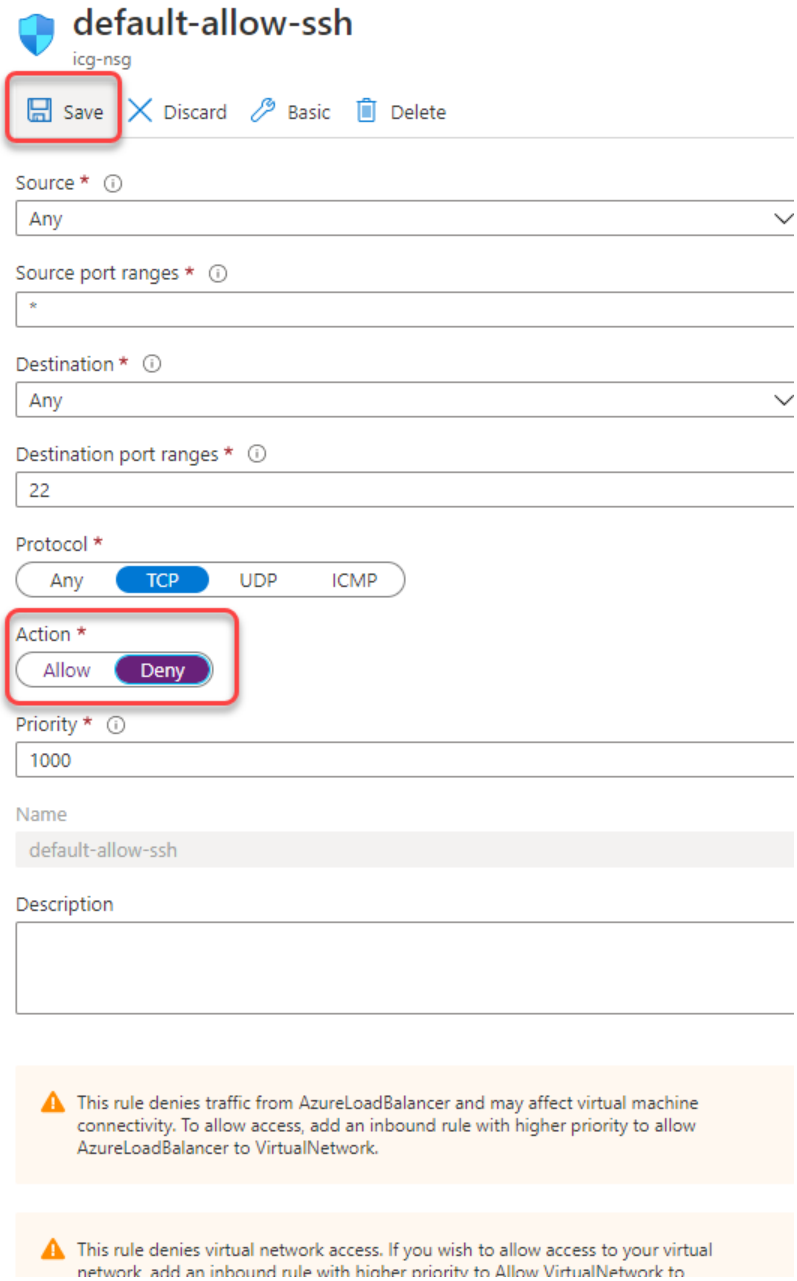
It is highly recommended to disable SSH access when it is not needed anymore.

> When SSH access is disabled, any request to port 22 will be blocked by the Azure firewall, so that requests to port 22 will not even cause any load on the virtual machine.

1. Select **Networking** from the menu and then click **default-allow-ssh**.



2. Switch **Action** from "Allow" to "Deny" and click **Save**.

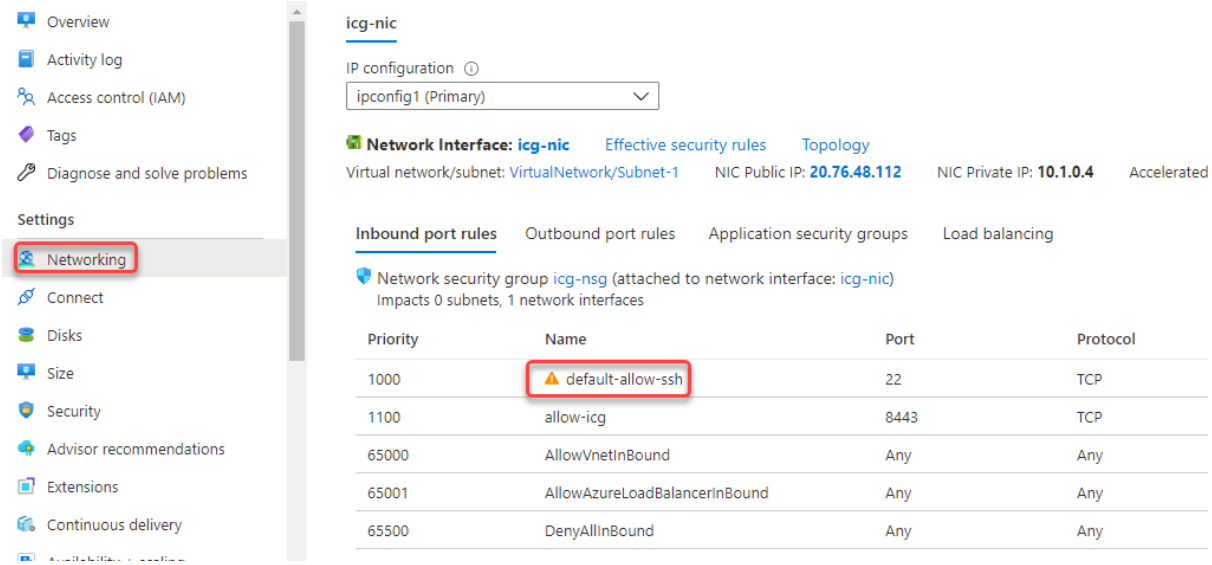


After a few seconds, the security rule is updated. Any traffic for port 22 is blocked.

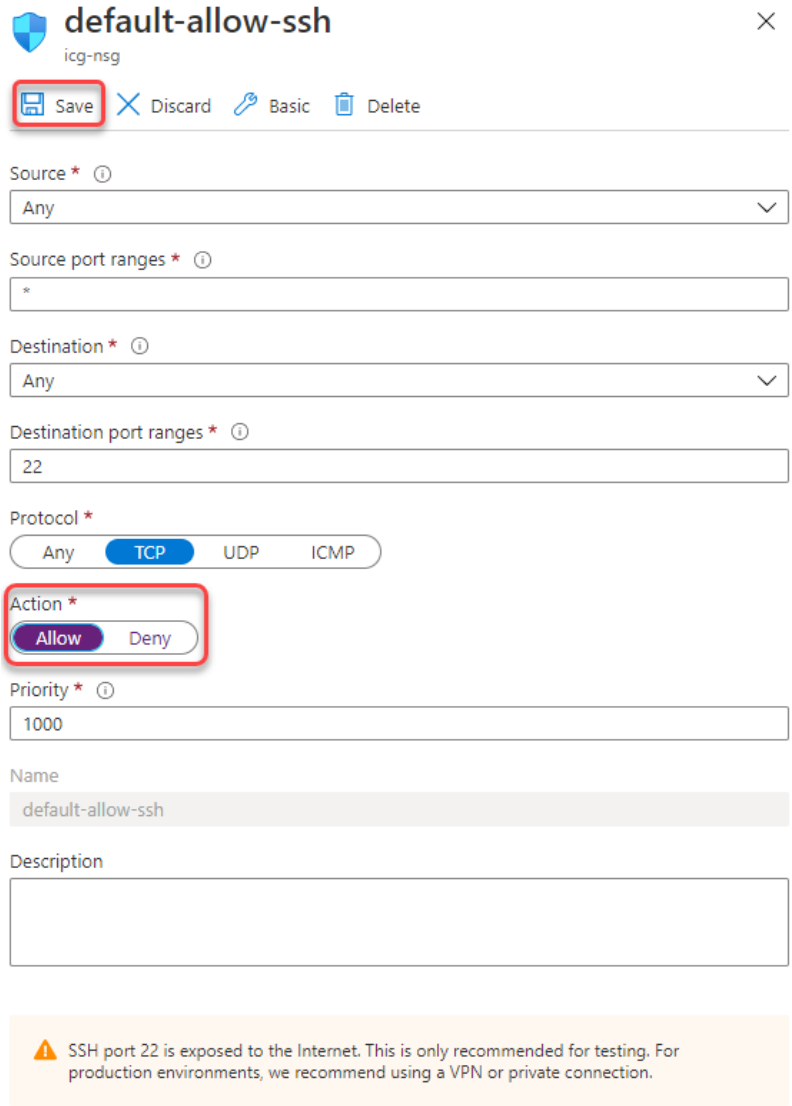
Enabling SSH Access

To make your virtual machine accessible by the UMS, you must enable SSH access. The UMS will use SSH for ICG installation, ICG update, and ICG keystore update. It is highly recommended to disable SSH access after the operation has succeeded (see Disabling SSH Access(see page 100)).

1. Select **Networking** from the menu and then click **default-allow-ssh**.



2. Switch **Action** from "Deny" to "Allow" and click **Save**.



After a few seconds, the security rule is updated. Your virtual machine is accessible over SSH.

3. When you are done, do not forget to disable SSH for security reasons; see Disabling SSH Access(see page 100).

> Do not forget to DISABLE SSH ACCESS because SSH access poses a security risk!

Preparing a Linux Machine for Installing IGEL Cloud Gateway (ICG)

This document describes how to prepare a host machine for installing IGEL Cloud Gateway (ICG). In this example, Ubuntu server 18.04. LTS 64-bit is used.

Setting up a User with the Required Permissions

1. Create the first user with a name of your choice. On the Ubuntu server, the first user created is the one who is allowed to do `sudo`.

   > **Username "icg" Is Reserved**
   >
   > Do not use "icg" as a username for the remote installer; this is the username under which the Tomcat server is running.

2. Enter `sudo su` and the user password to become a system administrator (`root`).

```
locadmin@doc-hs-icg:~$ sudo su
[sudo] password for locadmin:
root@doc-hs-icg:/home/locadmin#
```

Setting a Static IP Address

You can either use DHCP to set a static IP address or configure the IP address on the server via Netplan using a YAML description of the required network interface.

To set a static IP address via Netplan:

1. Enter `ip addr` to find out the name of the network interface.

```
root@doc-hs-icg:/etc/netplan# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 10
0
    link/ether 00:50:56:93:2a:b6 brd ff:ff:ff:ff:ff:ff
    inet 172.30.91.164/16 brd 172.30.255.255 scope global dynamic ens160
       valid_lft 524386sec preferred_lft 524386sec
    inet6 fe80::250:56ff:fe93:2ab6/64 scope link
       valid_lft forever preferred_lft forever
```

   In the above example, the network interface name is `ens160`.

2. To disable the network configuration capabilities of cloud-init, write a file: `nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg`

```
root@doc-hs-icg:/etc/netplan# nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
```

   with the following contents :
   `network: {config: disabled}`

3. Save the file by pressing [Ctrl] + [O] and then [Enter].
4. Press [Ctrl] + [X] to quit the editor.
5. Create the YAML file: `nano /etc/netplan/01-static.yaml`

```
  GNU nano 2.9.3                    /etc/netplan/01-static.yaml                    Modified

network:
  ethernets:
    ens160:
      addresses:
        - 172.30.251.223/16
      dhcp4: no
      gateway4: 172.30.1.1
  version: 2
_

                                    [ Read 9 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

> When editing YAML:
> - use two spaces to indent lines
> - leave no spaces or tabs at the end of lines

6. Save the file and quit the editor.
7. Apply your configuration with `netplan apply`. Take note of any error messages.

```
root@doc-hs-icg:/etc/netplan# netplan apply
root@doc-hs-icg:/etc/netplan#
```

8. Use the command `ip addr` to check whether the IP address has been set successfully.

```
root@doc-hs-icg:/etc/netplan# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 00:50:56:93:2a:b6 brd ff:ff:ff:ff:ff:ff
    inet 172.30.251.223/16 brd 172.30.255.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet 172.30.91.164/16 brd 172.30.255.255 scope global secondary dynamic ens160
       valid_lft 691137sec preferred_lft 691137sec
    inet6 fe80::250:56ff:fe93:2ab6/64 scope link
       valid_lft forever preferred_lft forever
```

How to Configure Apache Tomcat for TLS 1.2 Only

IGEL Cloud Gateway (ICG) 2.02 or higher already forces the use of TLS 1.2, so no further intervention is needed.

Certificate Management

You can renew your ICG certificate using the ICG Keystore Update Wizard.

Prerequisites

- UMS 5.09.100 or higher
- An ICG keystore you wish to update
- SSH root access to the host running the ICG; as of UMS 5.09.110, it is sufficient for the SSH user to have sudo privileges

The ICG Keystore Update Wizard simplifies the upload of a new keystore to the ICG server.

To update a keystore, proceed as follows:

1. Start the UMS Console.
2. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
3. If your signed certificate has expired, create a new signed certificate:
   a. Select the appropriate root certificate, open the context menu and select **Create signed certificate**.
   b. Enter the required data and click **OK**.
4. Select the signed certificate that is to be used. If you omit this step, an error message will be shown in the next step.
5. Go to **UMS Administration > UMS Network > Igel Cloud Gateway**.
6. In the toolbar in the upper right, click .
   The Keystore Update wizard opens.
7. Select the keystore you want transfer to the ICG server, then click **Next**.
8. Enter the SSH connection parameters:
   - **SSH host**: The host the ICG is running on (Default: `localhost`)
   - **SSH port**: SSH port (Default: `22`)

     > The SSH user must have root access.
     > UMS 5.09.110 and higher: It is sufficient for the SSH user to have sudo privileges.

     > Root access to the SSH server is a security risk!
     > Make sure you disable root access to the SSH server when the keystore updating process has finished.

   - **SSH user**: SSH user
   - **SSH password**: SSH user password
9. Click **Next** to start the update process.
   The keystore is being updated.
10. Click **Finish**.

Installing the ICG without Remote Installer

> The recommended method to install the ICG is to use the ICG Remote Installer. For instructions, see Installation and Setup(see page 12).
> The ICG Remote Installer is available as of UMS 5.09.100.

Creating and Exporting a Certificate in ICG Keystore Format

1. Start the UMS Console.
2. Create a signed certificate if you have not already done so. Depending on your requirements, choose one of the following procedures:
   - Creating a Certificate Using the UMS(see page 35)
   - Creating Certificates from an Existing Root Certificate(see page 27)
   - Installing an Existing Certificate Chain(see page 16)
3. Under **UMS Administration**, go to **Global Configuration > Certificate Management > Cloud Gateway** (UMS 6.06 or higher) resp. **Global Configuration > Cloud Gateway Options** (UMS 6.05 or lower).
4. Right-click the certificate the ICG should be installed with; from the context menu, choose **Export certificate chain to IGEL Cloud Gateway keystore format**.

Uploading the Keystore

You can use SCP (secure copy) to upload the keystore exported from the UMS to the machine on which the ICG will be installed.

From Windows with WinSCP

1. Download the free WinSCP software from https://winscp.net and install it.
2. In WinSCP configure a new session with these settings:
   - **File protocol**: SCP
   - **Host name**: Name or IP address of your ICG machine
   - **Username**: `sshuser`
   - **Password**: the password you have set for `sshuser`
3. Click **Login**.
4. Drag-and-drop the `keystore.icg` file to `sshuser`'s home directory on the ICG machine.

From Linux with SCP

1. In a terminal emulator, change to the directory you saved the keystore file in.
2. Run the following commandline:
   `scp keystore.icg sshuser@[host]:~/`
3. Enter the password you have set for `sshuser.`
   The file is uploaded.

Running the ICG Installer

1. Log into the machine as `root`
2. Copy the uploaded keystore into the current directory with the cp command:
   `cp /home/sshuser/keystore.icg .`

   > Please note that "." (fullstop) is part of the command. The fullstop stands for the current directory. So, you pass the cp command two arguments: " `/home/sshuser/keystore.icg"` and "." for the current directory.

3. Make the ICG installer file executable with the chmod command: `chmod u+x installer-[version].bin`
4. Start the installer with:
   `./installer-[version].bin keystore.icg`
5. Accept the installation path.
6. Accept or change the TCP port for the ICG service (Default: 8443).

   > This port must be permanently available for the ICG.

   The installer configures and starts the Tomcat server, printing environment variables.

   > Do not reboot the system or restart the ICG Tomcat server before the first connection has been made from UMS.

Connecting the UMS to the ICG

For instructions, see Connecting the UMS to the ICG(see page 113).

Connecting the UMS to the ICG

Connecting Directly

1. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.

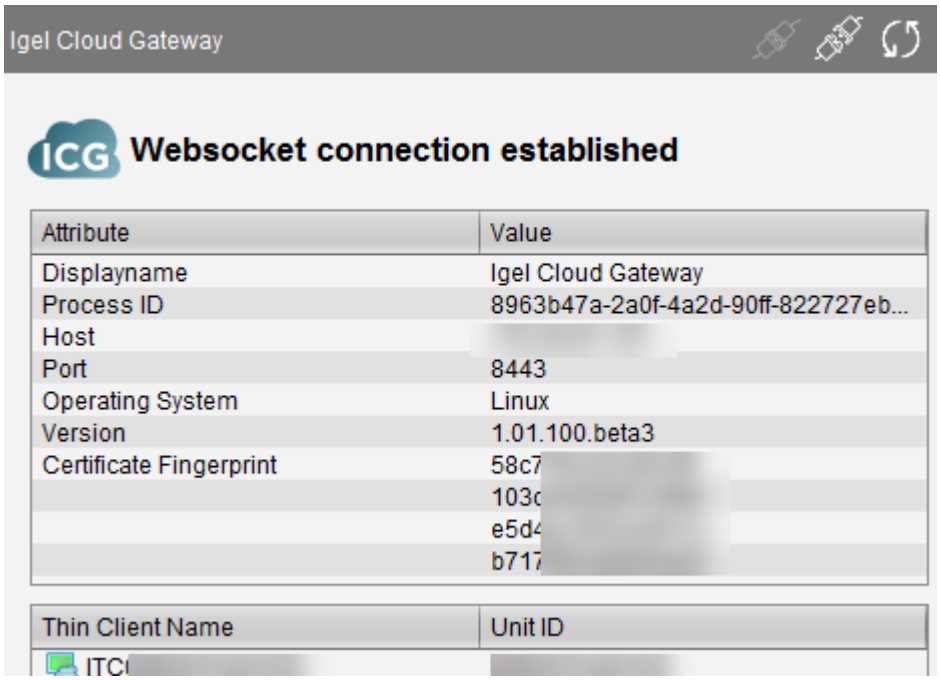
2. Click to add a new gateway instance.

3. Enter the following data:
   - **Displayname**: freely chosen name
   - **Host**: IP or DNS name of the ICG

   > This address must also be present in the ICG certificate; see Updating the IGEL Cloud Gateway (ICG)(see page 59). Otherwise, ICG and UMS will not be able to communicate.

   - **Port**: Listening port of the ICG as defined during the installation; see Installing the ICG without Remote Installer(see page 111). (Default: 8443)

4. Click **Finish**.
   The UMS is now connected to the ICG.



Connecting via a Proxy

A proxy can be located between the UMS and the ICG. For details about the communication between the components and the ports involved, see Geräte und UMS Server kontaktieren sich über ICG, section "Via Proxy".

> The proxy must support websockets with TLS in order to work with ICG.

> Connecting to the ICG via a proxy is supported by UMS version 5.08.100 and higher.

1. In the UMS Console, go to **UMS Administration > Global Configuration > Proxy Server.**
   Learn how to create a new proxy entry in the UMS Manual.

2. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway**.

3. Click to add a new gateway instance.

4. Enter the following data:
   - **Displayname**: freely chosen name
   - **Host**: the gateway IP or DNS name
   - **Port** (Default: 8443)

5. Click **Next**.

6. Choose **Manual Proxy Configuration** and select the proxy you created a few steps earlier.

7. Click **Finish**.
   The UMS is now connected to the gateway.

Uninstalling ICG

ICG includes an uninstall script. To completely remove ICG from the system, proceed as follows:

1. Log in as root or a user with sudo privileges to the ICG host.
2. Change to the directory you installed ICG in (default: /opt/IGEL/icg/).
   It contains the `uninstall.sh` script.
3. To start the uninstall process, run `sudo ./uninstall.sh`
4. A dialog opens. Confirm that you want to remove ICG completely.
   ICG is removed completely.

Updating ICG Manually

1. Upload the new installer to your ICG server using WinSCP on Windows or the `scp` command on Linux.
2. Log into the ICG Virtual Appliance as root or a user with sudo privileges.
3. Copy the uploaded installer into the current directory:
   `cp /home/sshuser/installer-[version].icg`
4. Make the ICG installer executable with `chmod u+x installer-[version].bin`
5. Start the installer with
   `./installer-[version].bin`
6. Accept the installation path.
7. Accept or change the TCP port for the ICG service (default: 8443).
   The installer configures and restarts the Tomcat server, printing environment variables.

Managing ICG Certificates with UMS

The Universal Management Suite (UMS) has a built-in TLS/SSL certificate manager to be used with the IGEL Cloud Gateway (ICG). It produces keystore files suited to the ICG installer.

- Certificate Signing Options(see page 118)
- Using a Publicly Known CA in UMS(see page 119)

Certificate Signing Options

UMS supports three options for ICG certificate signing:

- Use the UMS to create a CA(see page 35) and sign ICG certificates.
    - Advantages: Free of charge, independent
    - Disadvantages: Client users have to check the CA certificate fingerprint when first connecting to ICG, no advanced PKI management features
- Import the root certificate and private key of your existing private CA into UMS(see page 27), and use the certificate to sign a certificate for ICG.
    - Advantages: Free of charge
    - Disadvantages: Client users have to check the CA certificate fingerprint when first connecting to ICG. You may not want to save your CA private key in a networked application such as UMS, and it may be difficult to synchronize it with your main private CA.
- Import the root certificate of a publicly known CA into UMS(see page 119), and an ICG certificate signed by it.
    - Advantages: If the CA is one of the approximately 170 that are supported by IGEL OS, users will not need to check the certificate fingerprint at all.
    - Disadvantages: Cost. You will not be able to sign certificates yourself.

Using a Publicly Known CA in UMS

The following files are needed:

- CA root certificate
- ICG Server certificate signed by the CA
- ICG server private key

To use a publicly known CA in the UMS:

1. In UMS Console go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the **Certificates** section, click to import the root certificate.
3. Choose the CA's root certificate file (in PEM format).
   The CA's root certificate appears in the list.
4. Right-click the CA's root certificate and select **Import signed certificate.**
5. Click **OK**.
   The signed certificate appears in the list.
6. Right-click the signed certificate and select **Import decrypted private key**.

   > If the private key is protected with a passphrase you need to decrypt it using the OpenSSL commandline tool: `openssl rsa -in encrypted.key -out decrypted.key`

7. Choose the decrypted private key file.
   The data can now be used to produce a keystore file for the ICG server.
8. Right-click the signed certificate and select **Export certificate chain in IGEL Cloud Gateway keystore format**.
   The file `keystore.icg` is created. This file will be required for the gateway.
9. Save the `keystore.icg` file.

Using Citrix NetScaler ADC as an SSL Bridge for ICG

This document describes using Citrix NetScaler ADC (Application Delivery Controller) for accepting requests from endpoint devices and forwarding them to IGEL Cloud Gateway (ICG).

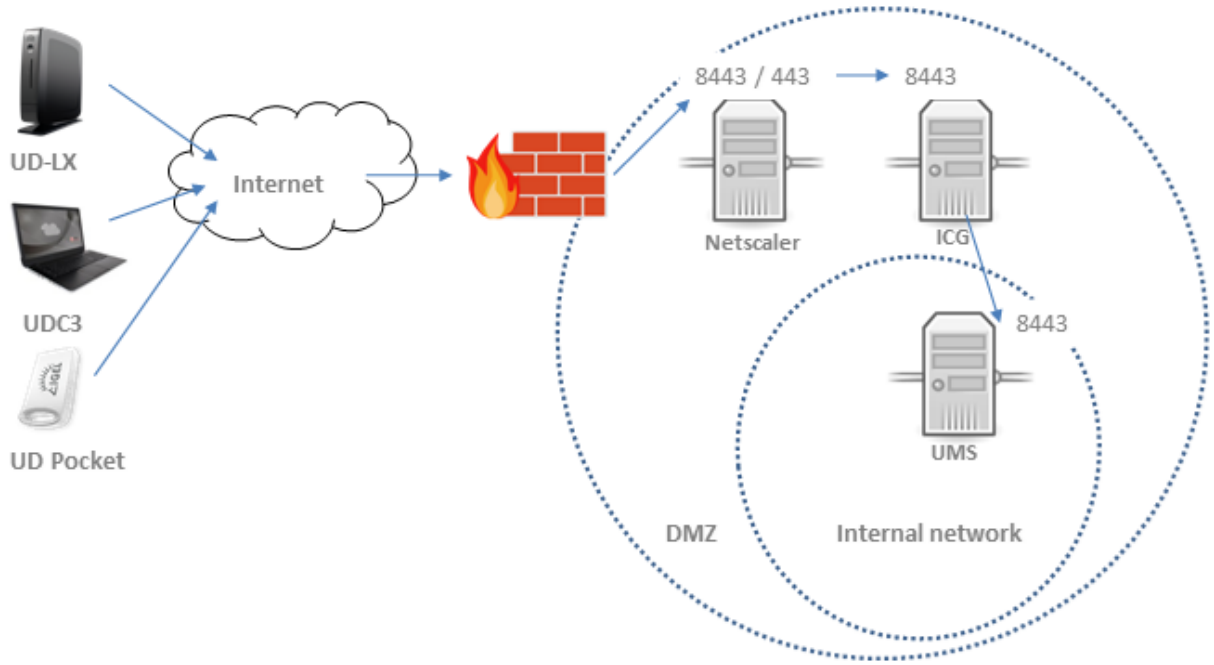
> Please note that IGEL does not support the use of Citrix NetScaler as a load balancer. Using Citrix NetScaler as an SSL bridge, therefore, has no effect on the distribution of requests to the ICG instances.

- Network Topology(see page 121)
- Configuring NetScaler(see page 122)

Network Topology

This is the network topology for Citrix NetScaler ADC for forwarding requests to ICG.

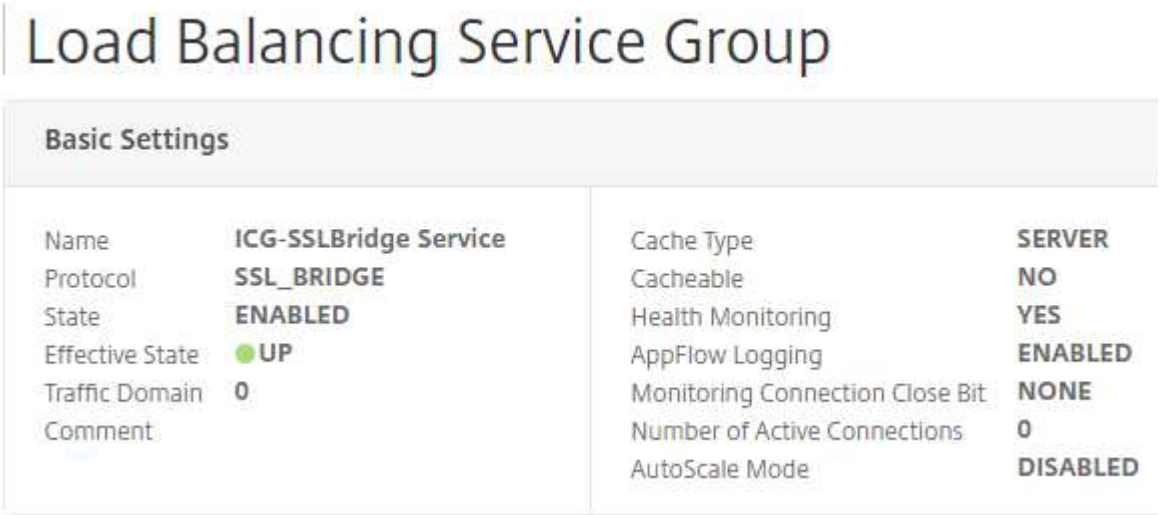
> ⓘ The TLS/SSL certificate that clients see will be the one installed on NetScaler.



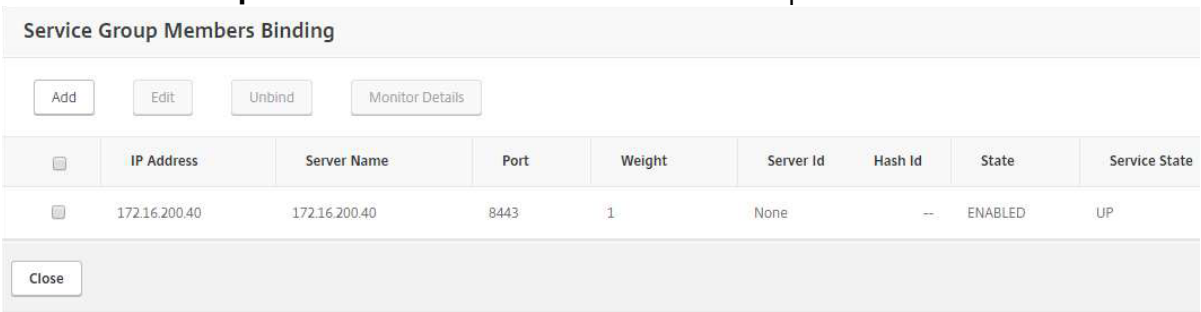
Configuring NetScaler

1. Configure a server object in NetScaler under **Load Balancing**. Pick its IP address from the subnet in which the ICG is located.

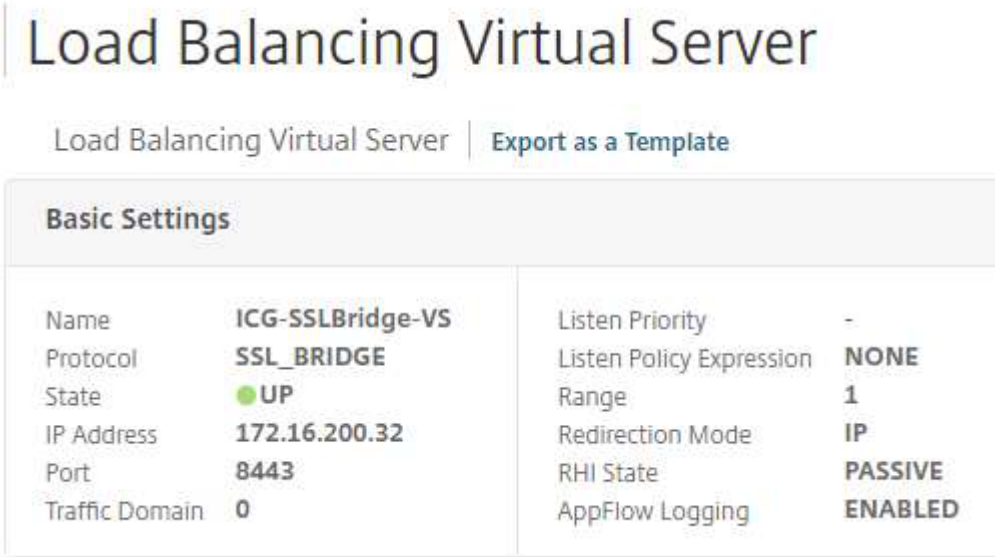
2. Create a **Load Balancing Service Group** with `SSL_Bridge` as the **Protocol**. In the screenshot it is named `ICG-SSLBridge Service.`



3. Add a **Service Group Member** with the ICG's IP address and TCP port.

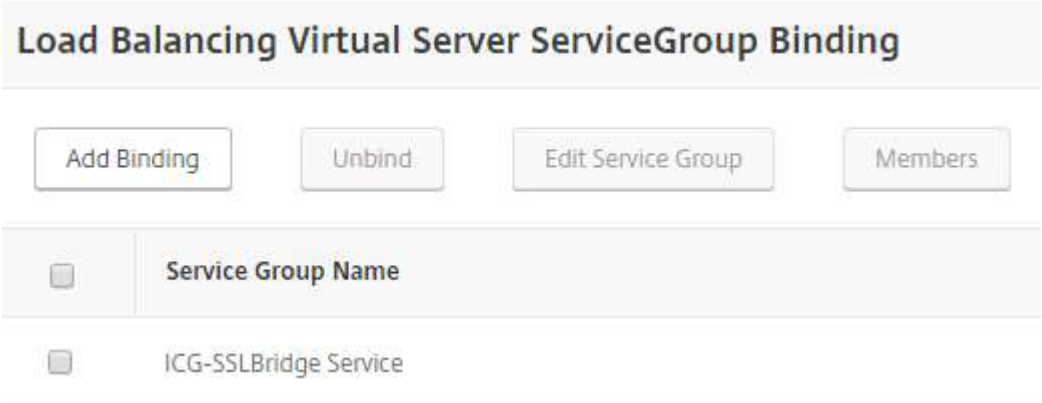


4. Create a **Load balancing Virtual Server.** The IP address and TCP port you configure here will be accessible from the Internet.



5. Add a **Binding** to the load balancing server group, binding the `ICG-SSLBridge Service` you created in step 2.

The load balancing virtual server should now be in the state `UP`, and communication from the Internet should be forwarded to ICG.



Giving a User sudo Privileges

> Giving a user sudo privileges can pose a security risk!
> The instructions described in this how-to should be carried out by experienced users only.

When installing the IGEL Cloud Gateway with the Remote Installer (see Installing the IGEL Cloud Gateway(see page 40)), the Remote Installer will connect to the deployment server via SSH.

For the installer to be able to perform all required installation tasks, the user provided for the SSH login must be either root or (as of UMS 5.09.110) have sudo privileges. The table below shows how to give sudo privileges to a user on the Linux distributions supported by the ICG.

Distribution	sudo included in default installation	Command to add user to sudoer list*
Ubuntu	Yes	`usermod -aG sudo <USERNAME>`
Debian	No Install with this command: `apt install sudo`	`usermod -aG sudo <USERNAME>`
Redhat	Yes	`usermod -aG wheel <USERNAME>`
SLES	Yes	`usermod -aG wheel <USERNAME>` You also need to add the group `wheel` to `/etc/sudoers`.

* Root privileges are required for using `usermod`.

Updating Expired ICG Keystores

> **Security Warning**
>
> Never replace a root certificate!
> The thin clients trust the root certificate. If the root certificate is replaced, the thin clients need to be reregistered with the UMS!

You can update an expired ICG keystore either manually or using the ICG Keystore Update wizard.

To update a keystore manually:

1. Start the UMS Console.
2. Under **UMS Administration**, go to **Global Configuration > Cloud Gateway Options**.
3. Right-click the keystore; from the context menu, choose **Create signed certificate**.
4. Right-click your newly created certificate; from the context menu, choose **Export certificate chain to IGEL Cloud Gateway keystore format**.
5. Now transfer the `keystore.icg` keystore file to the ICG host.
6. Run `/opt/IGEL/icg/keystore_update keystore.icg` as root.
   The keystore will be replaced with the new one and the ICG will be restarted.
   The UMS and the thin clients will automatically reconnect to the ICG.

To update a keystore using the ICG Keystore Update Wizard:

The ICG Keystore Update wizard introduced in UMS 5.09.100 offers a more convenient method to update an expired keystore.

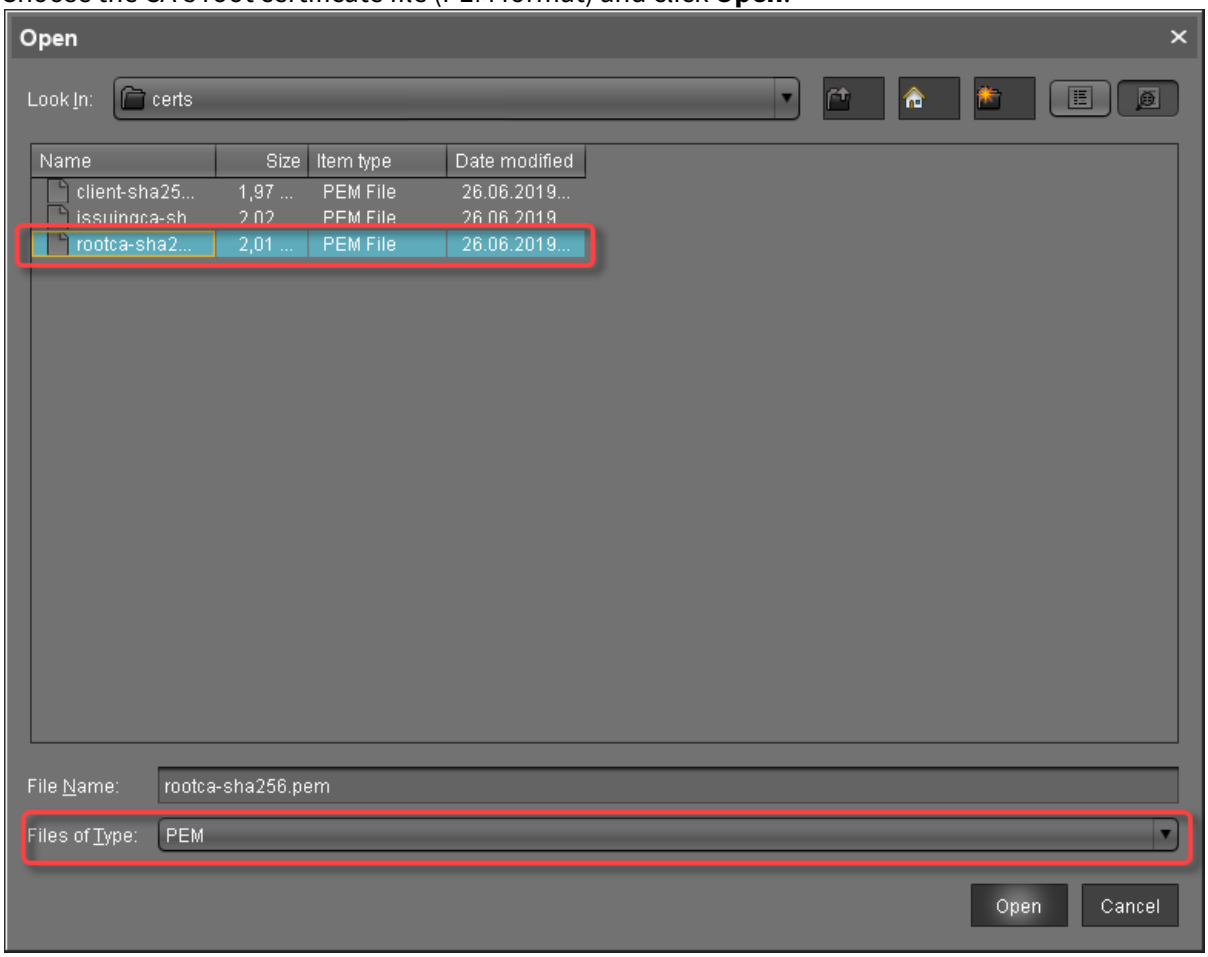
See the chapter Certificate Management.

Installing an Existing Certificate Chain (UMS 6.02 or Older)

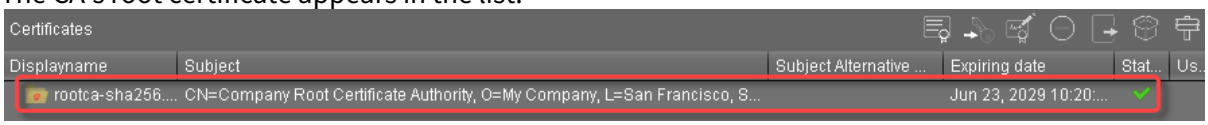
Importing the Root Certificate

> The validity period of the root certificate should be as long as possible. When the root certificate expires, all certificates must be exchanged, and all devices must be registered anew.

1. In the UMS Console, go to **UMS Administration** > **Global Configuration** > **Cloud Gateway Options**.
2. In the **Certificates** section, click to import the root certificate.
3. Choose the CA's root certificate file (PEM format) and click **Open**.

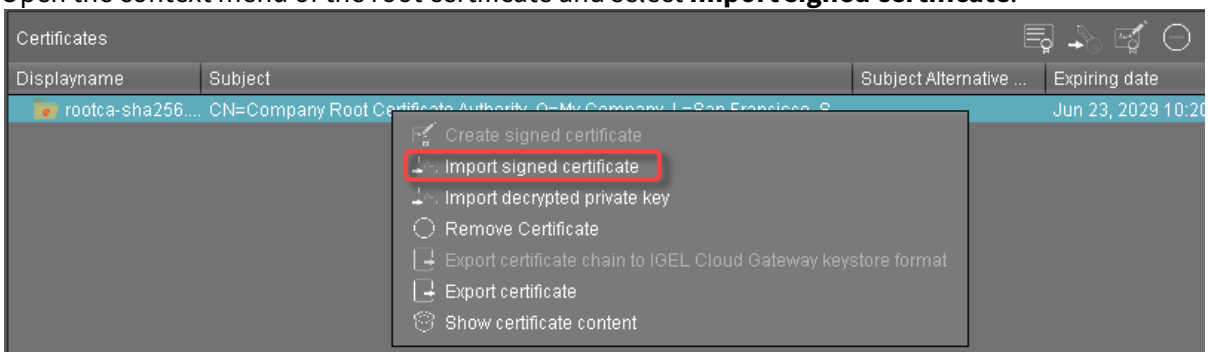


The CA's root certificate appears in the list.

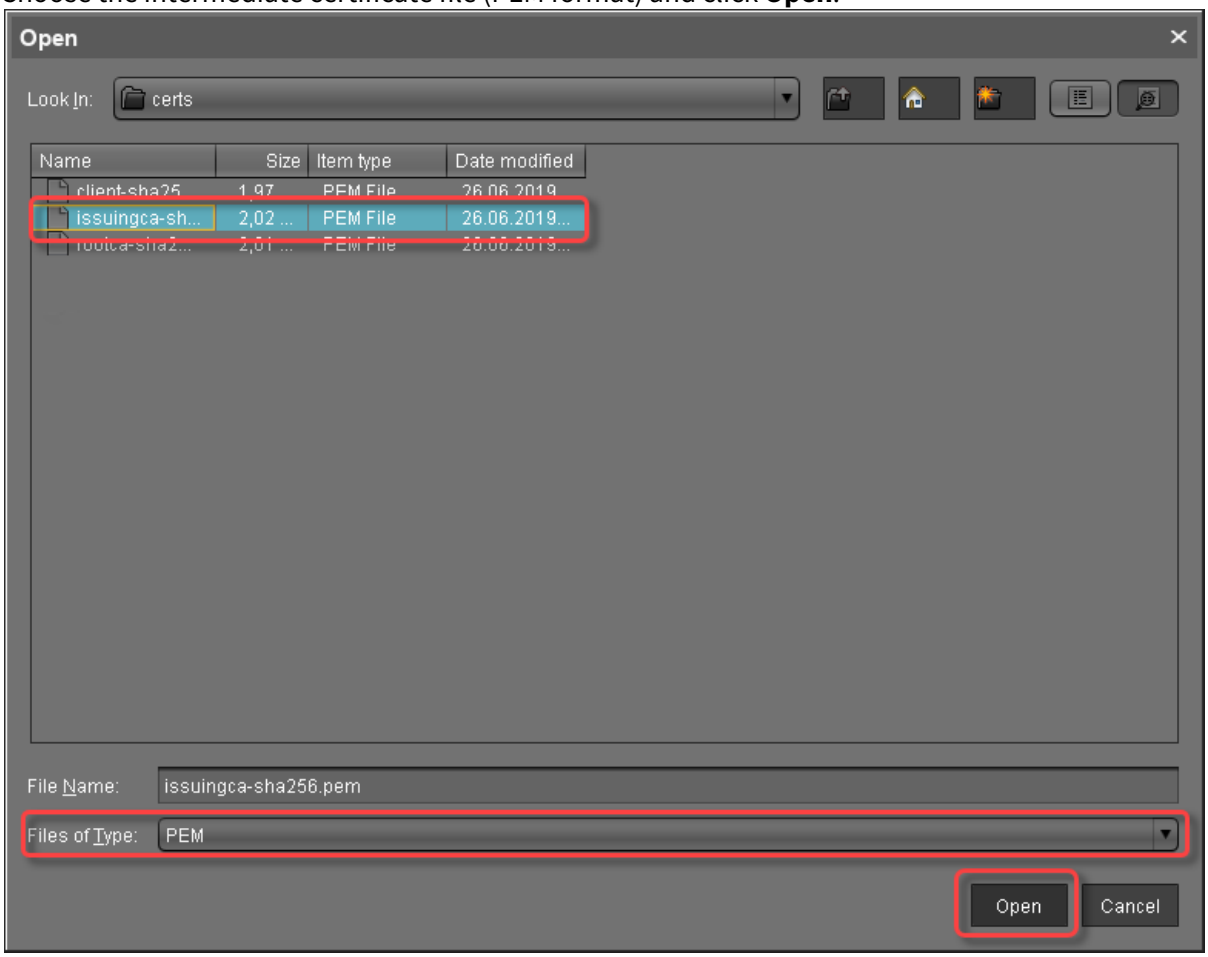


Importing the Intermediate Certificate

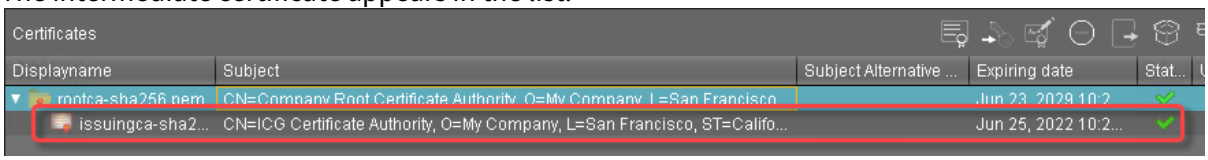
1. In the UMS Console, go to **UMS Administration** > **Global Configuration** > **Cloud Gateway Options**.
2. Open the context menu of the root certificate and select **Import signed certificate**.



3. Choose the intermediate certificate file (PEM format) and click **Open**.

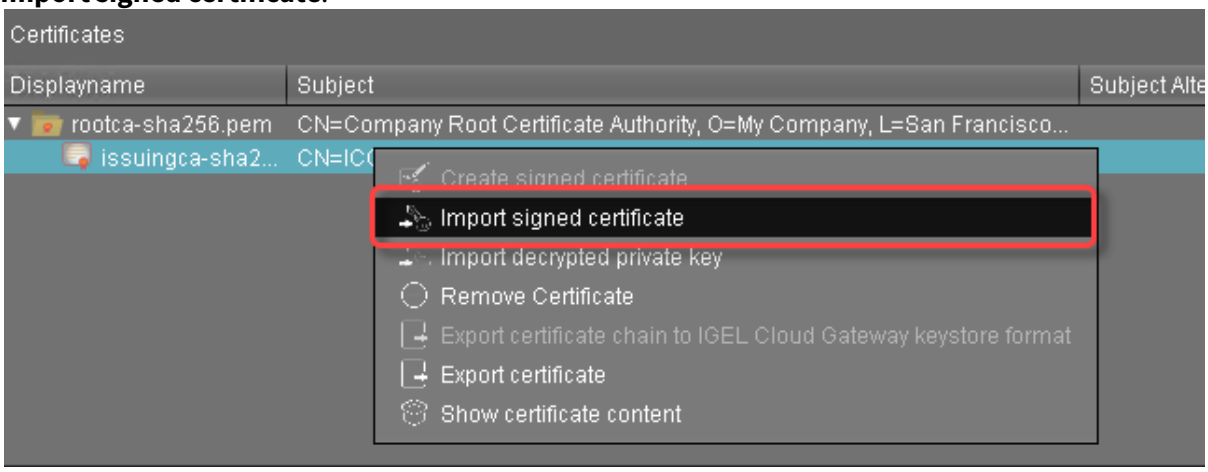


The intermediate certificate appears in the list.

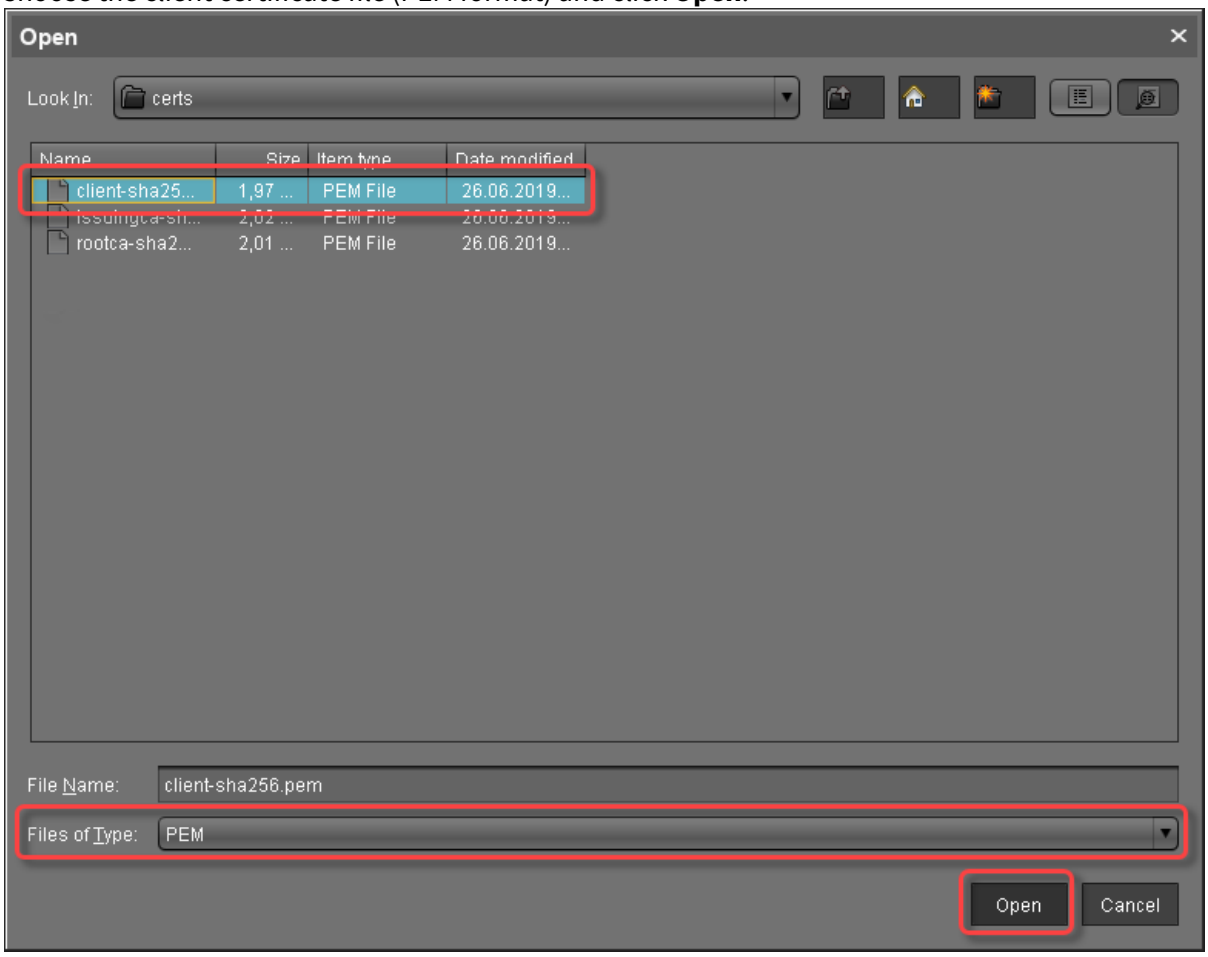


Importing the End Certificate

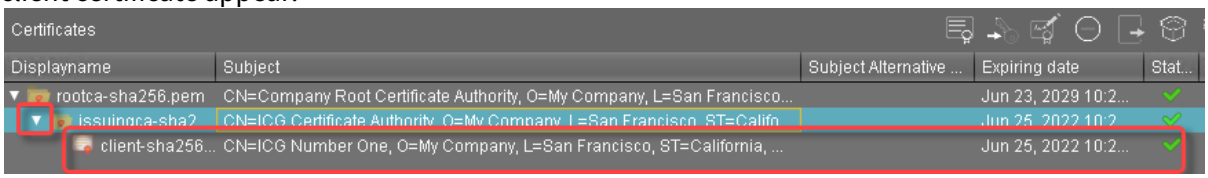
1. In the UMS Console, go to **UMS Administration** > **Global Configuration** > **Cloud Gateway Options**.
2. Open the context menu of the intermediate certificate nearest to the client certificate and select **Import signed certificate**.



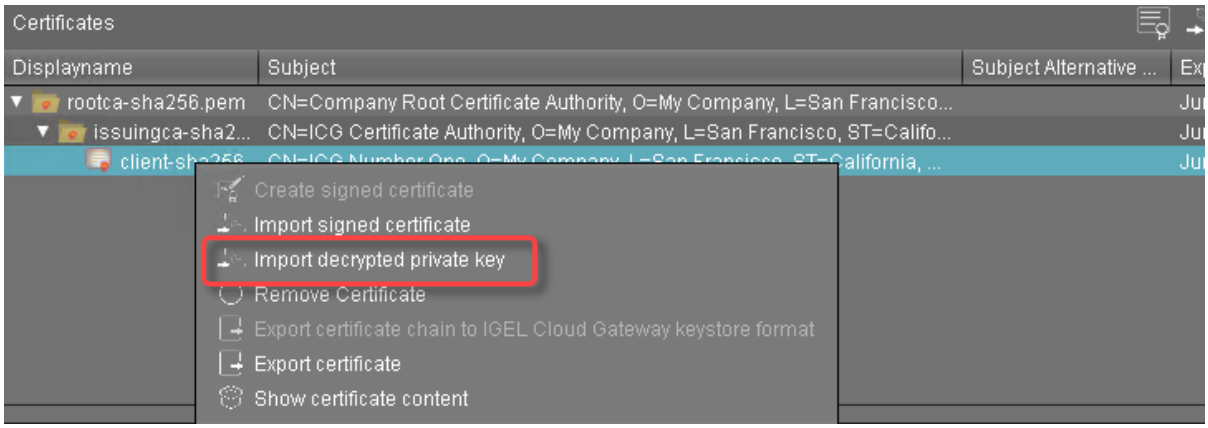
3. Choose the client certificate file (PEM format) and click **Open**.



4. Click the arrow symbol of the intermediate certificate nearest to the client certificate to make the client certificate appear.

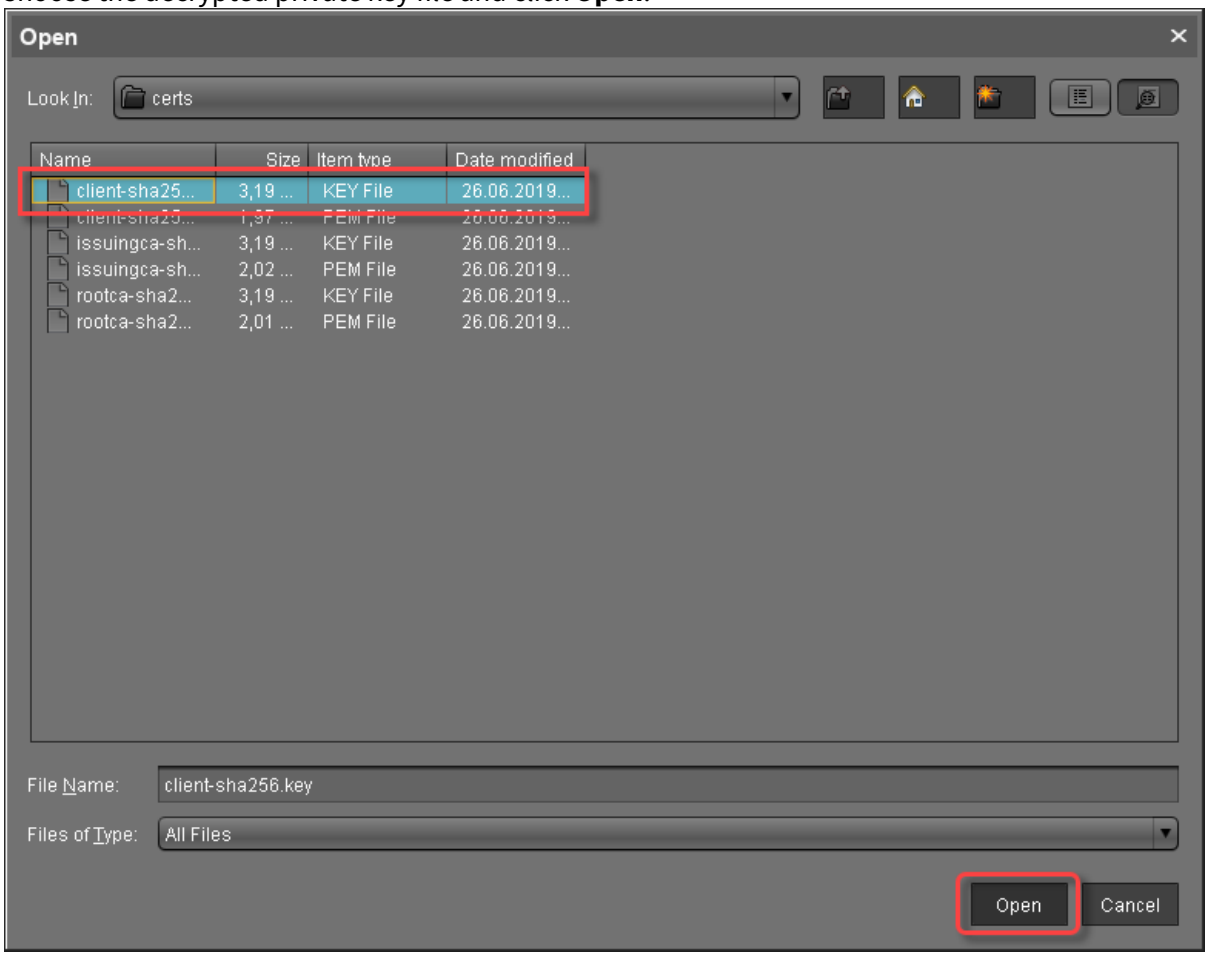


5. Right-click the client certificate and select **Import decrypted private key**.

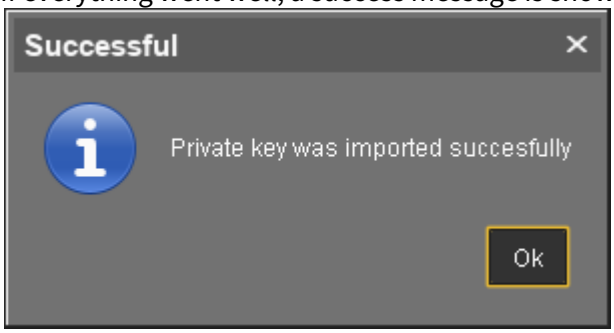


> ⓘ If the private key is protected with a passphrase, you need to decrypt it using the OpenSSL command line tool: `openssl rsa -in encrypted.key -out decrypted.key`

6. Choose the decrypted private key file and click **Open**.



If everything went well, a success message is shown.



7. Continue with Installing the IGEL Cloud Gateway(see page 40).

Creating Certificates from an Existing Root Certificate (UMS 6.02 or Older)

Required Certificate Files

The following files are required:

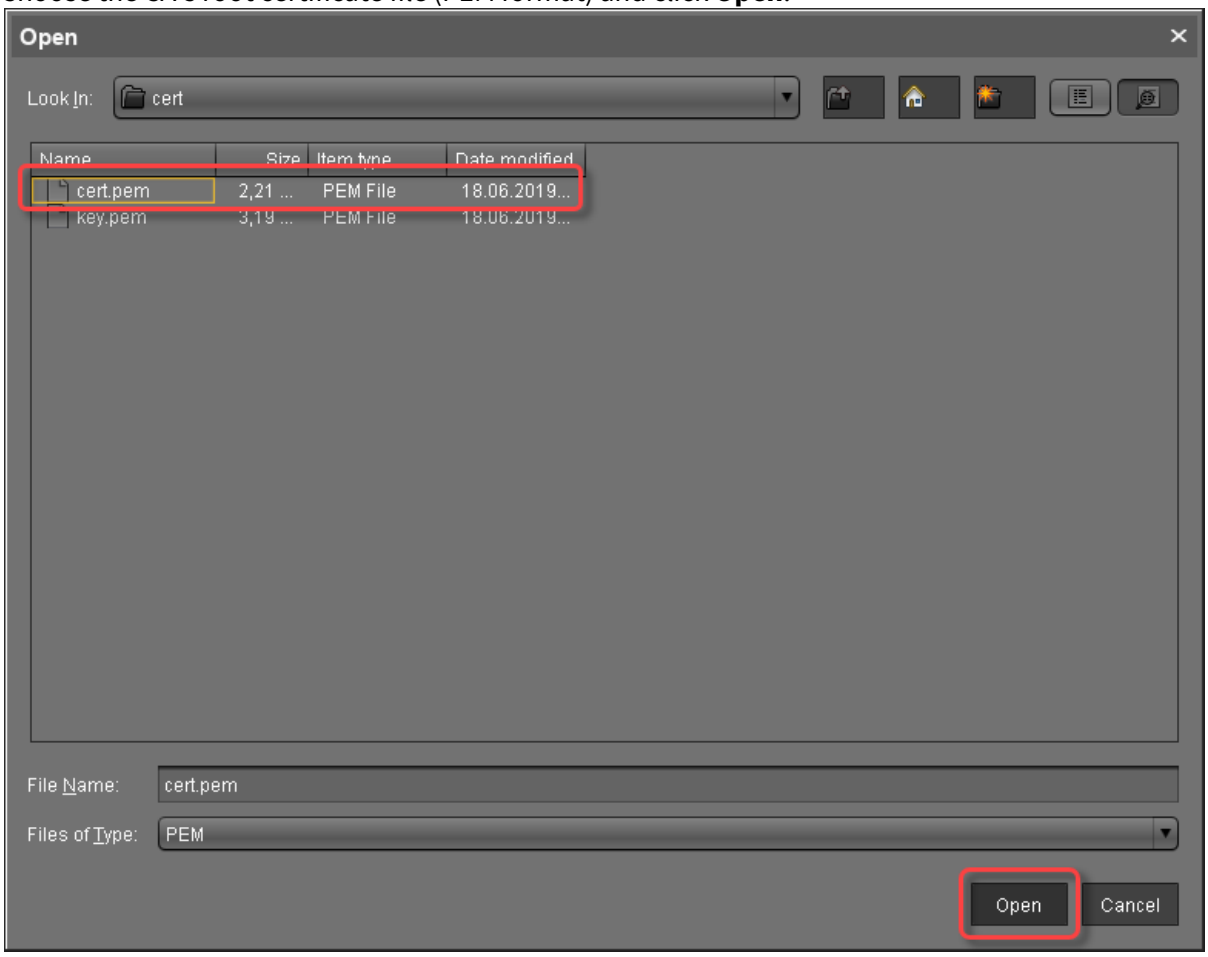
- CA certificate
- CA private key
  If you need to export the CA signing root certificate and key from a Microsoft CA server, you can follow this document from Cisco: How do I export and convert a pfx CA root certificate and key from a Microsoft CA server[6]

Importing Your Existing Private CA Files into the UMS

1. In UMS Console go to **UMS Administration** > **Global Configuration** > **Cloud Gateway Options**.
2. In the **Certificates** section, click to import the root certificate.

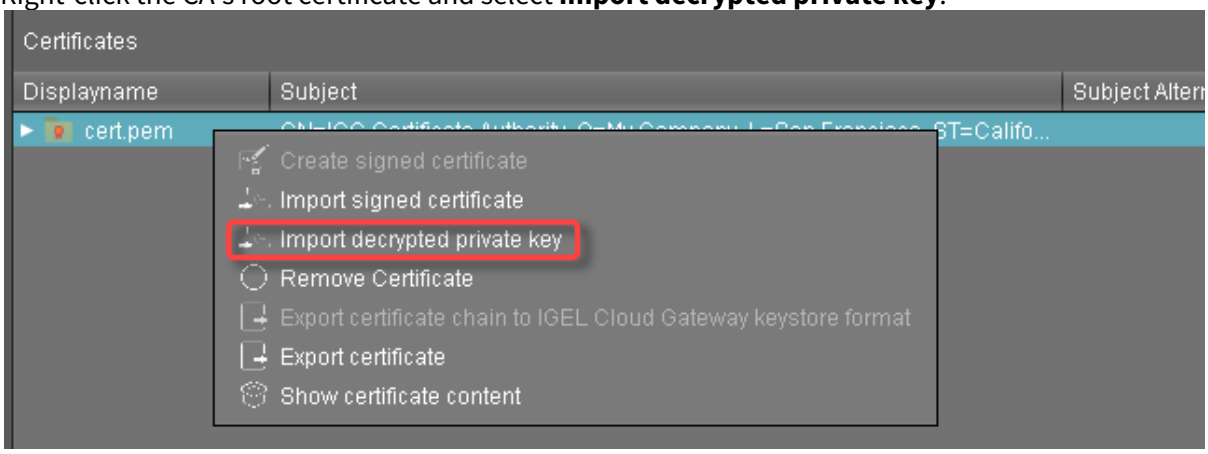
6 http://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/118339-technote-wsa-00.html

3. Choose the CA's root certificate file (PEM format) and click **Open**.



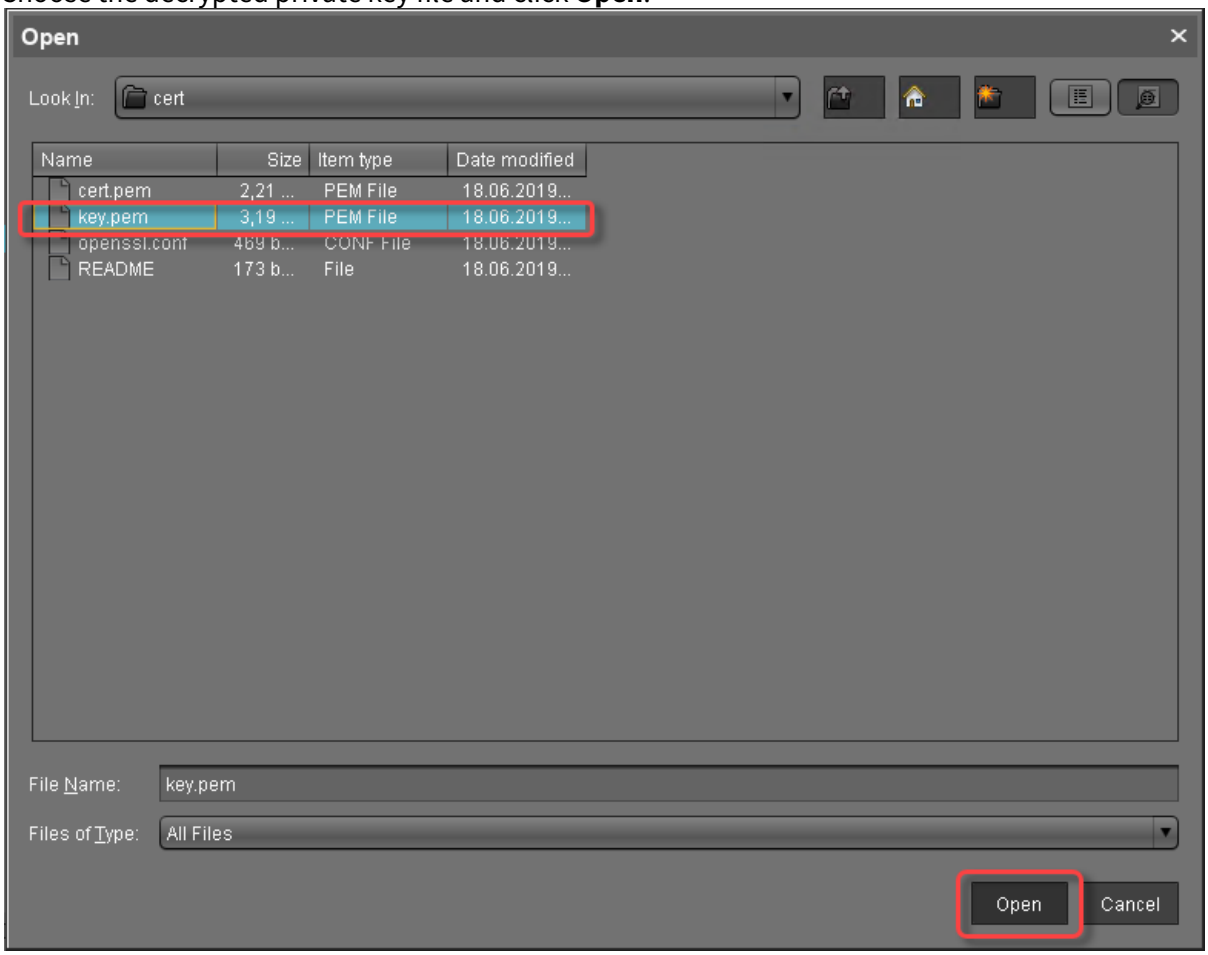
The CA's root certificate appears in the list.

4. Right-click the CA's root certificate and select **Import decrypted private key**.

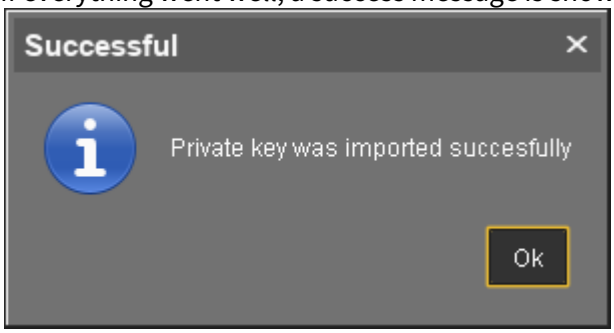


> ⓘ If the private key is protected with a passphrase, you need to decrypt it using the OpenSSL command line tool: `openssl rsa -in encrypted.key -out decrypted.key`

5. Choose the decrypted private key file and click **Open**.



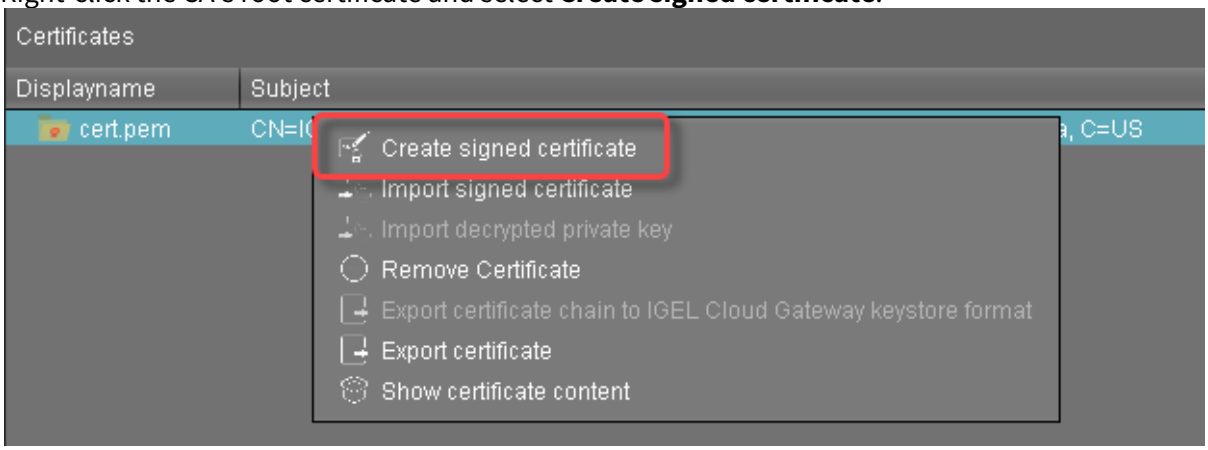
If everything went well, a success message is shown.



The CA is now ready to use.

Creating a Signed Certificate

1. Right-click the CA's root certificate and select **Create signed certificate**.

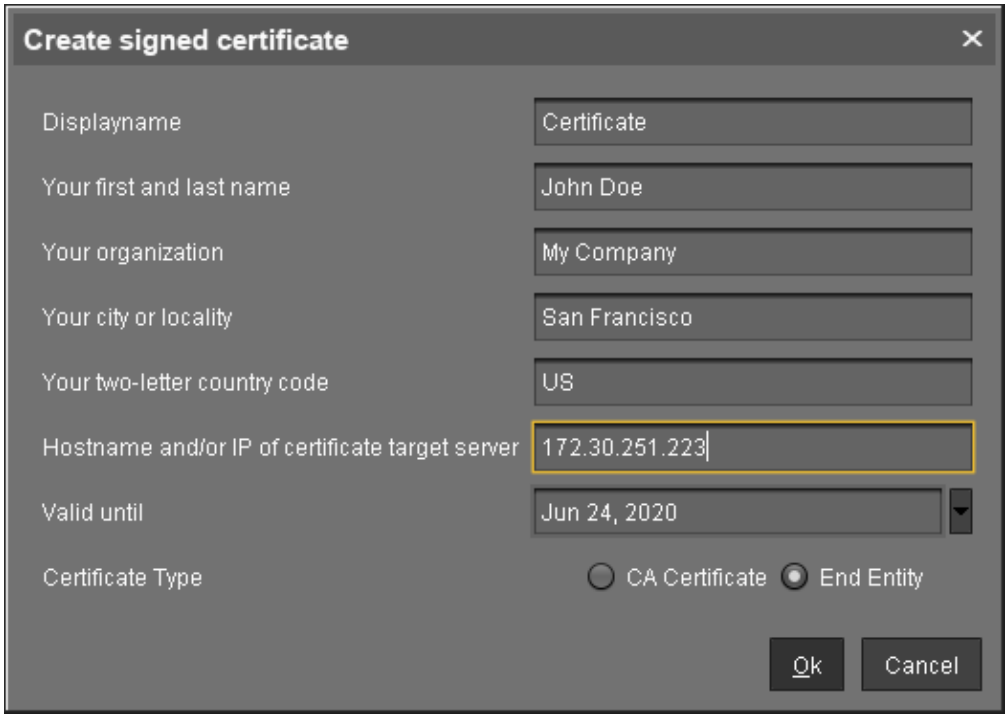


2. Fill in the certificate fields:
   - **Display name**: Name of the certificate
   - **Your first and last name**: Name of the certificate holder
   - **Your organization**: Organization or company name
   - **Your city or locality**: Location
   - **Your two-letter country code**:ISO 3166 country code, e.g. `US` , `UK` or `ES`
   - **Hostname and/or IP address of certificate target server**: Host name(s) or IP address(es) for which the certificate is valid. Multiple entries are allowed, separated by semicolons.

> ⓘ All IP addresses and host names by which the ICG will be reachable from within the company network or from outside must be provided here.

   - **Valid until**: Local date on which this certifcate expires. (Default: one year from now)
   - **Certificate Type**: Select "End Entity".

3. Click **OK**.



A key pair and a certificate are generated.

> Generating keys may take substantial time on virtual machines (VMs), as these do not have a powerful (pseudo) random number source. On Linux VMs this can be improved by installing the haveged[7] package.

The signed certificate appears in the list.

4. Continue with Installing the IGEL Cloud Gateway(see page 40).

7 http://www.issihosts.com/haveged/

Transferring the First-Authentication Keys to the Devices

To connect a device to the ICG, the newly generated credentials (fingerprint, password) must be available on the user resp. device side. In many cases, the user and device are in a remote location, which leaves it to the user to establish the connection to the ICG.

There are multiple possibilities to provide the credentials:

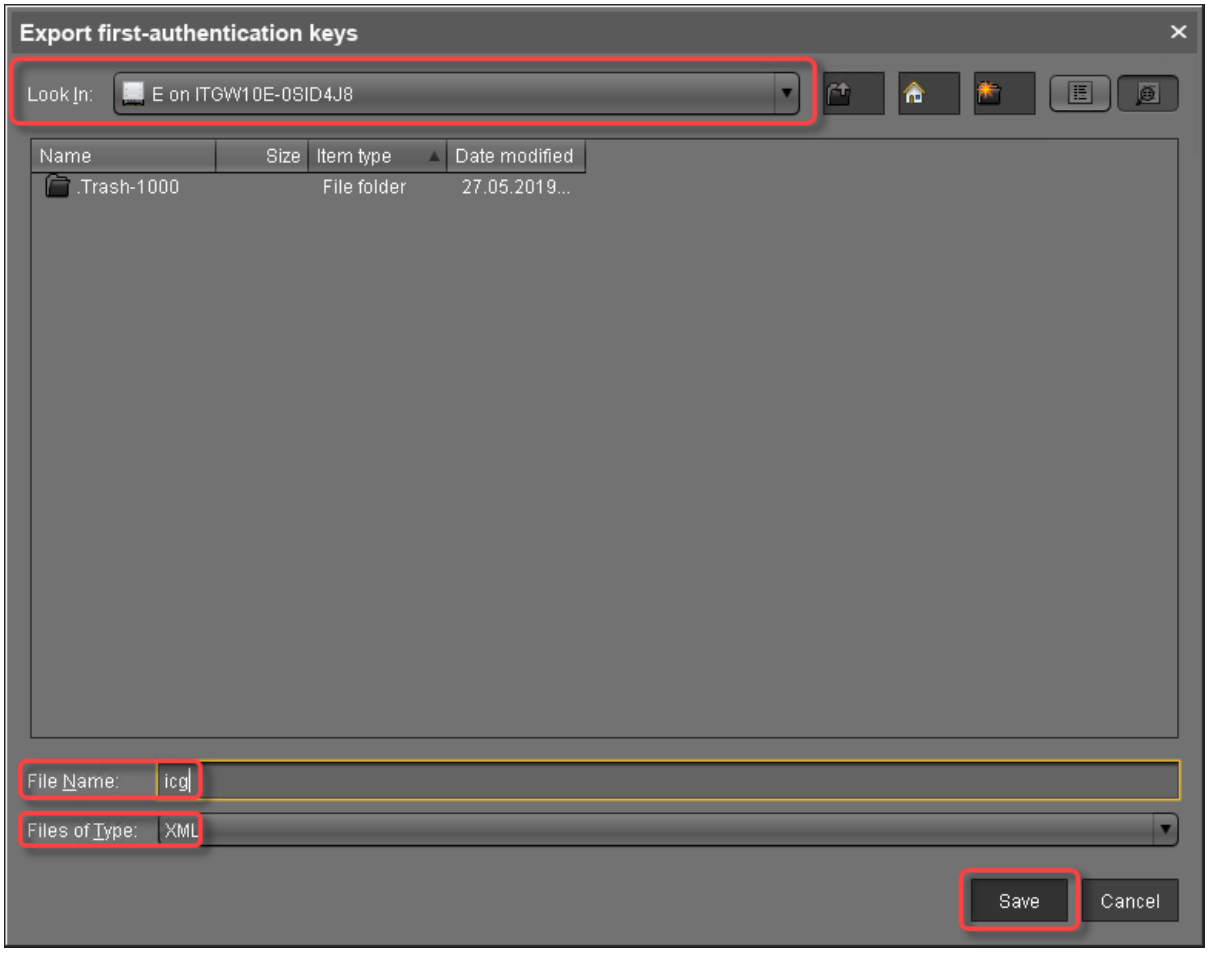
- USB stick that contains the credentials in an XML file
- USB stick that contains the credentials in an HTML file
- E-Mail containing the credentials, created and sent directly from the UMS
- E-Mail or printed letter containing the credentials; the credentials can be inserted via copy & paste.

XML file on a USB stick

To export the XML file from the UMS:

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication keys**, select the desired password entries and click to export the passwords.
3. Under **Look in:**, choose a file path on your USB stick.
4. Enter a **File Name**, e. g. `icg.xml`
5. Under **Files of Type**, choose either "XML" or "HTML" as the file format.

6. Click **Save**.



To retrieve the credentials at the device:

1. On the device, open setup and go to **Devices > Storage Devices > Storage Hotplug**.
2. Activate **Enable dynamic client drive mapping**.
3. Click **Apply**.
4. Insert the USB stick you prepared earlier.
5. Open a **Local Terminal**.
6. Log in as `user`
7. Run the command `ls media` to see removable media.
8. Change to your USB stick with `cd media/[device label]`
9. View the XML file with `cat icg.xml`
   The XML file contains all the data required for connecting a device to the ICG: host address, ICG server certificate fingerprint, and the password:

Now you can copy the missing certificate fingerprint part and the password from the terminal.

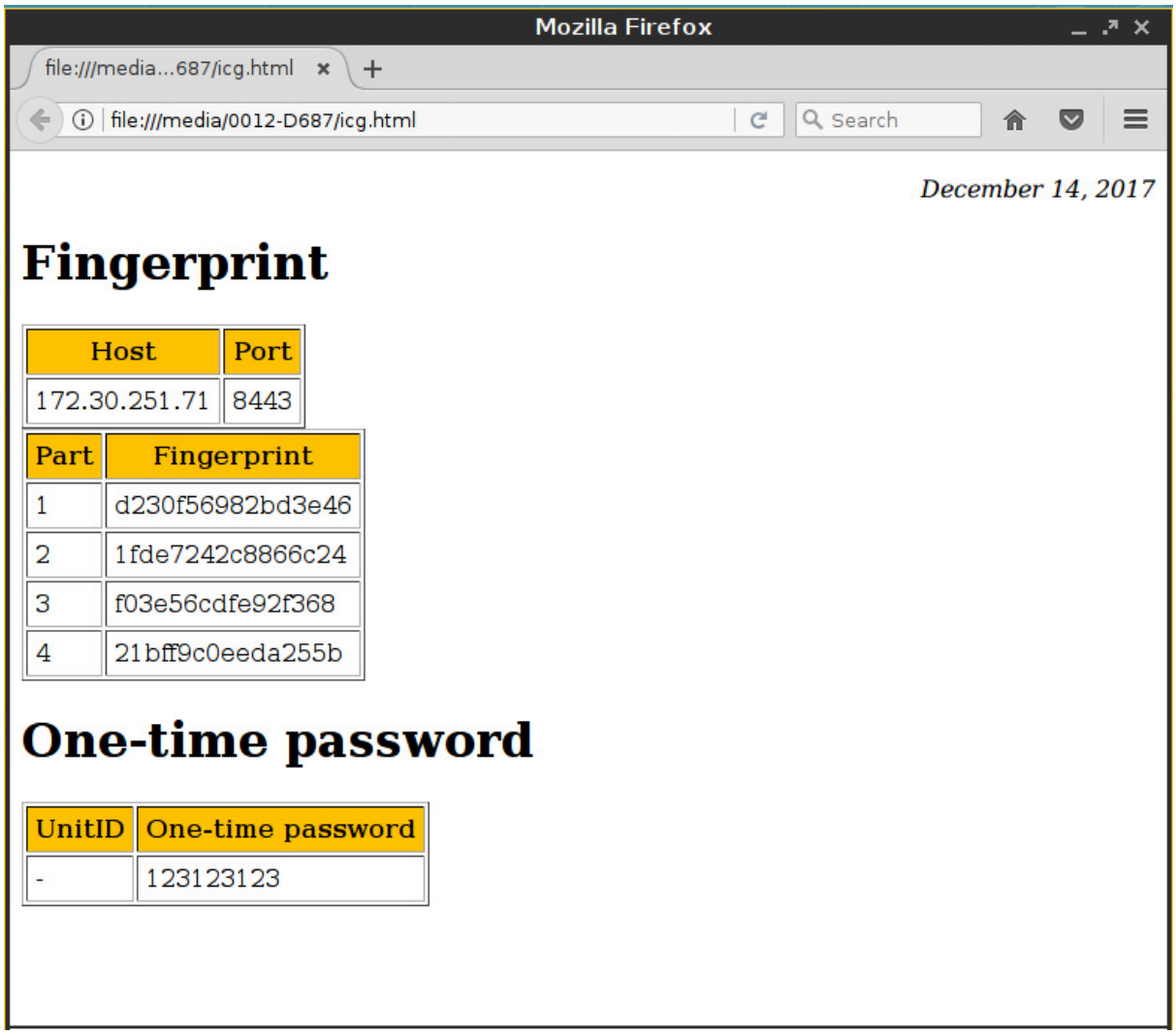
HTML file on a USB stick

To export the HTML file from the UMS:

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication passwords**, select the desired password entries and click to export the passwords.
3. Save the passwords in HTML format as `icg.html` on a USB stick.

To retrieve the credentials at the device:

1. On the device, open setup and go to **Devices > Storage Devices > Storage Hotplug**.
2. Activate **Enable dynamic client drive mapping**.
3. Click **Apply**.
4. Insert the USB stick you prepared earlier.
5. Open a **Local Terminal**.
6. Log in as `user`
7. Run the command `ls media` to see removable media.
8. Change to your USB stick with `cd media/[device label]`
9. View the HTML file with `firefox icg.html`
   The HTML file contains all the data required for connecting a thin client to the ICG: host address, ICG server certificate fingerprint, and the password:

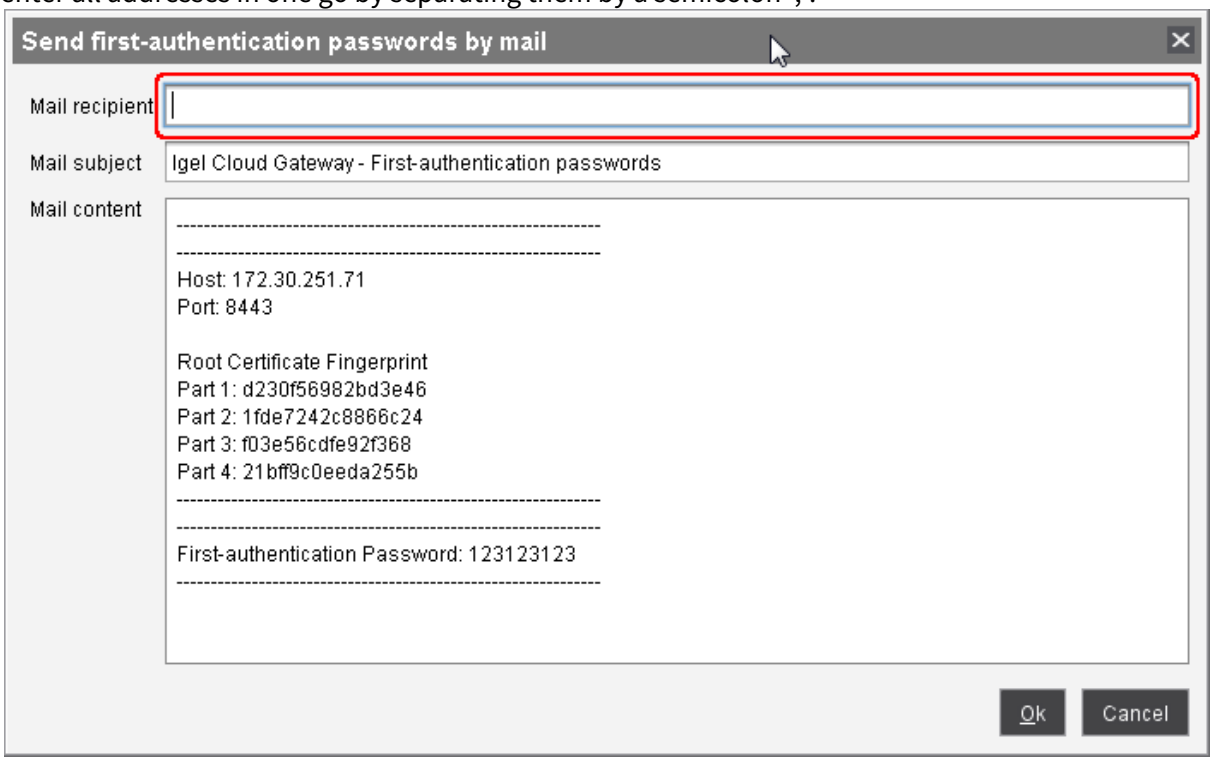


E-Mail created by the UMS

> To send an e-mail directly from the UMS, the e-mail settings must be configured correctly. For more information, see the E-mail Settings chapter in the UMS manual.

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication passwords**, select the desired password entries and click to create an e-mail.
   The dialog **Send first-authentication passwords by mail** opens. The e-mail body contains all the data required for connecting a device to the ICG: host address, ICG server certificate fingerprint, and the password.

3. Enter the **Mail recipient**. To send a multiple-time password to more than one recipients, you can enter all addresses in one go by separating them by a semicolon ';'.



4. Klick **Ok** to send the e-mail.

Manually created E-Mail or Printed Letter

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication passwords**, select the desired password entries and click to copy the credentials to the clipboard.
   The data required for connecting a device to the ICG is in the clipboard: host address, ICG server certificate fingerprint, and the password.
3. To send the credentials via e-mail, paste the data into an encrypted e-mail. To send the credentials in a printed letter, paste the data in your e-mail program or word processor.

All Methods of Generating First-Authentication Keys for Devices

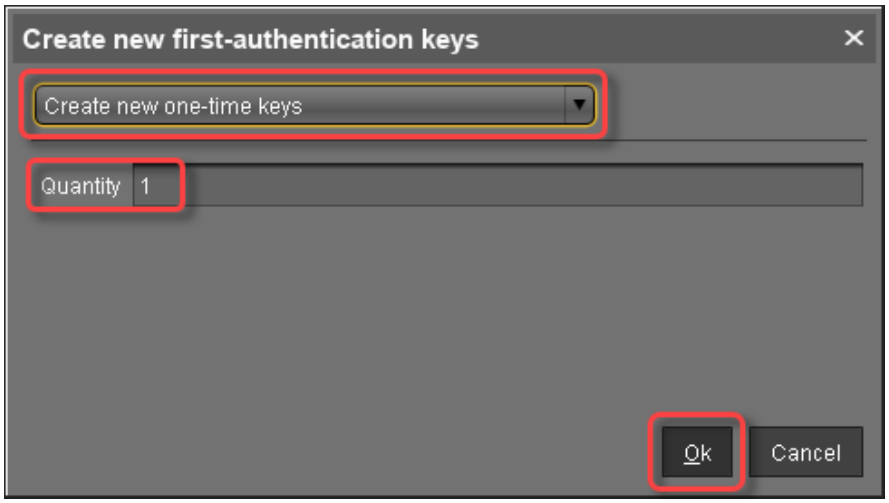
To establish a connection with the ICG, every device must authenticate with the ICG. For this purpose, a first-authentication key must be generated. On the first contact with the ICG, the device must present this key. You have the following possibilities to generate first-authentication keys:

- One-time keys that can be used by any random device, but cannot be re-used by any other device. Hence, the number of keys must match the number of devices.
- One-time keys that can only be used by specified devices and will be invalidated after use.
- Multiple-time keys that can be used by any device and will remain valid after use.

Once the keys for initial authentication are created, you can continue with Transferring the First-Authentication Keys to the Devices(see page 138).

Creating One-Time Keys for Random Devices

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. Click .
3. Select **Create new one-time keys**.
4. Enter the **Quantity** of one-time passwords you want to generate.
5. Click **OK**.



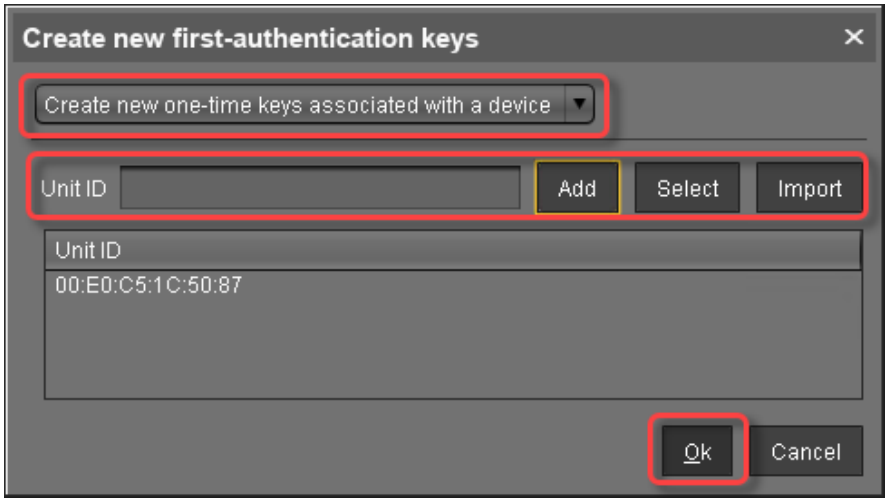
One or more new entries appear in the list, depending on the value entered under **Quantity**.

Creating One-Time Keys for Specific Devices

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. Click .
3. Select **Create new one-time keys associated with a device**.
4. Choose a method to add one or more thin client unit IDs:

- **Add**: Enter a **Unit ID** manually and click **Add**.
- **Select**: Click **Select** and select thin clients with .
- **Import**: Click **Import** and select a CSV file with unit IDs. For instructions on how to create a list of unit IDs, see Creating a Unit ID List for IGEL OS.

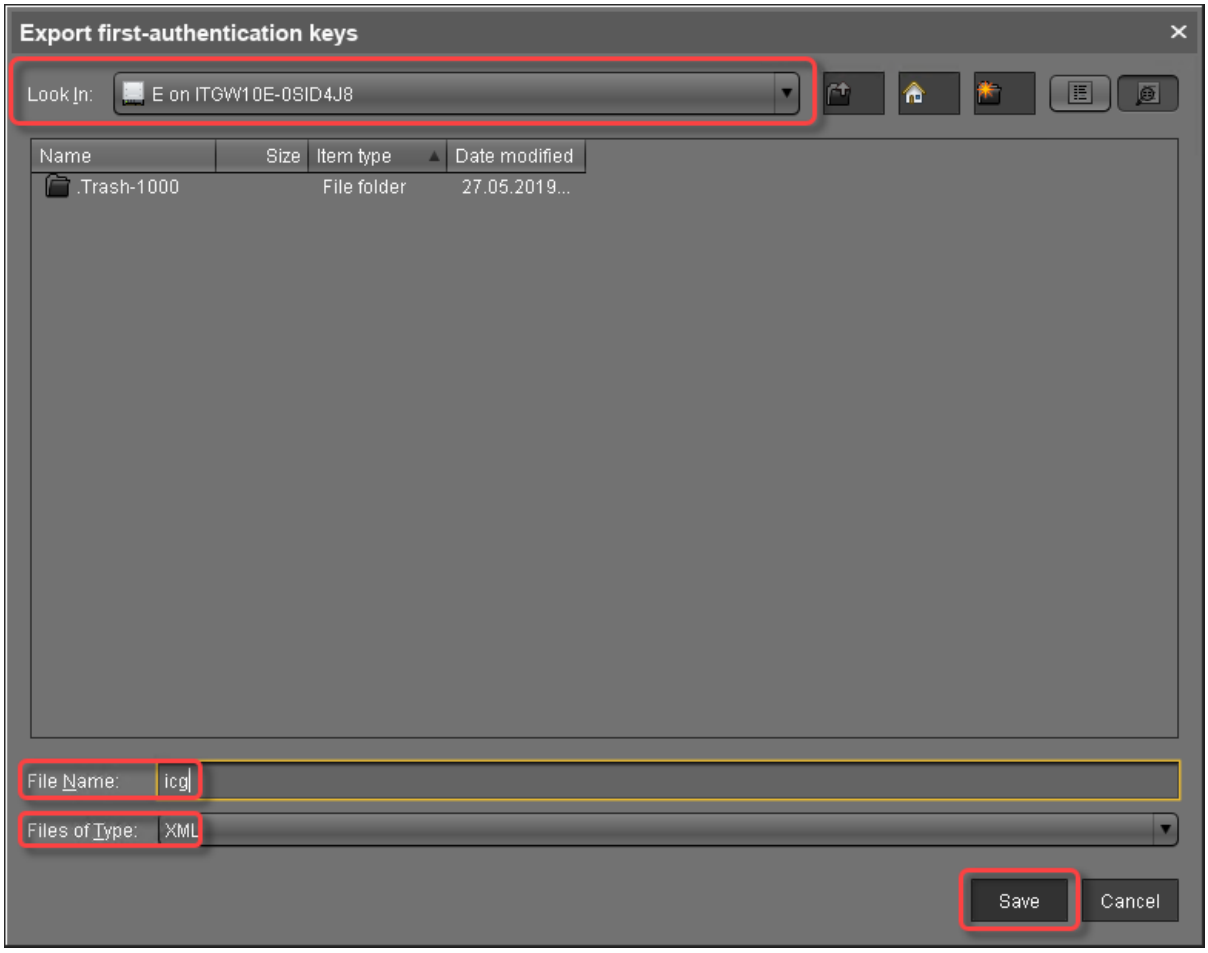
5. Click **OK**.



If everything went well, a success message is shown.

6. Confirm the message.
   One or more new entries appear in the list.
7. Select the new entries and click to export the keys.
8. Under **Look in:**, choose a file path on your USB stick.
9. Enter a **File Name**, e. g. `icg.xml`
10. Under **Files of Type**, choose either "XML" or "HTML" as the file format.

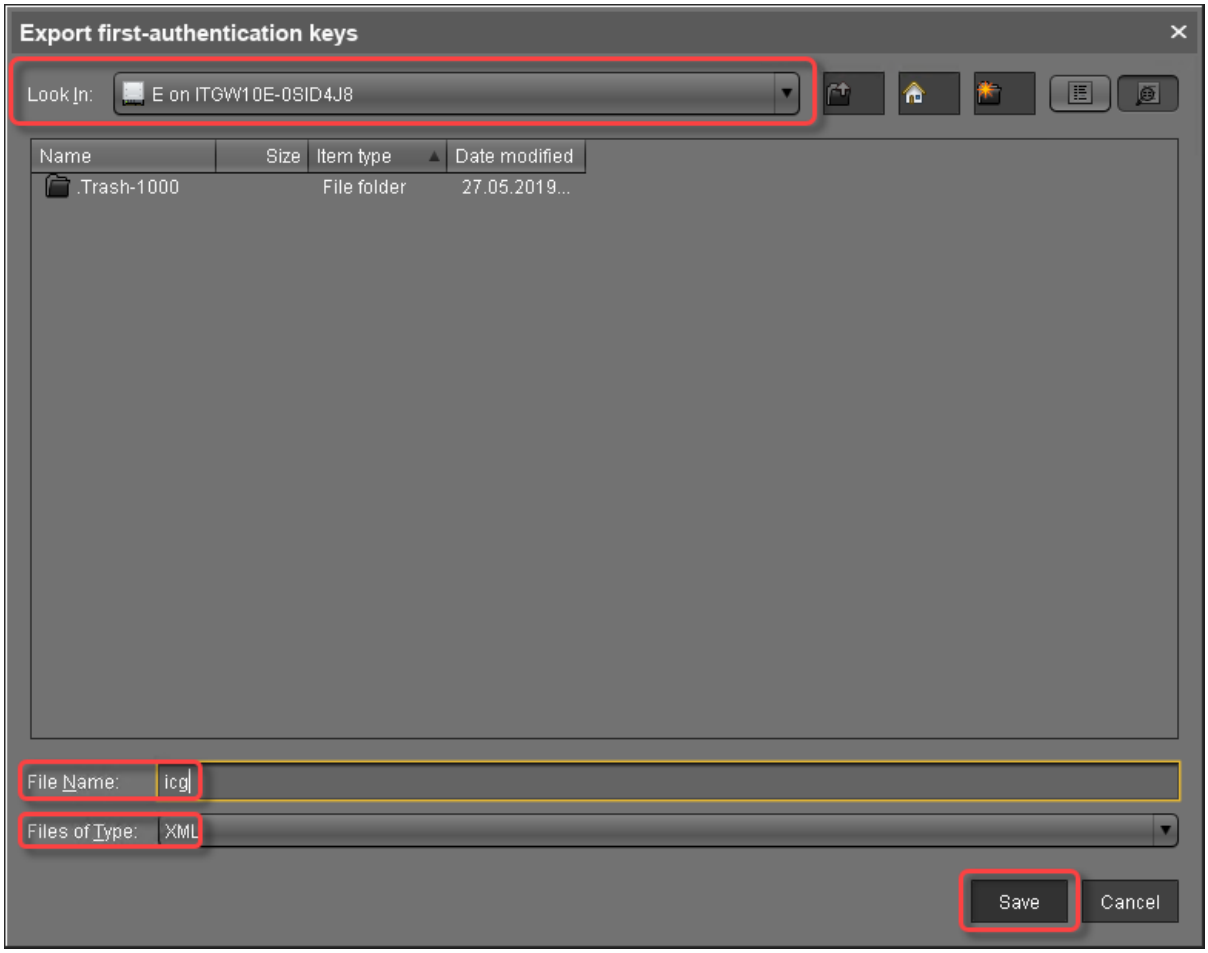
11. Click **Save**.



Creating a New Mass-Deployment Key for Arbitrary Devices

1. Connect a USB stick to the machine on which the UMS Console is running.
2. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
3. Click .
4. Select **Create new mass-deployment key**.
5. Activate or deactivate **Generate random mass-deployment key** to choose the method of key generation:
   - ☑ The key is generated by the UMS.
   - ☐ You can enter a key of your own in the entry field.
6. Click **OK**.
   One or more new entries appear in the list.
7. Select the new entries and click to export the keys.
8. Under **Look in:**, choose a file path on your USB stick.

9. Enter a **File Name**, e. g. `icg.xml`
10. Under **Files of Type**, choose either "XML" or "HTML" as the file format.
11. Click **Save**.



Manually created E-Mail or Printed Letter

1. Go to **UMS Administration > Global Configuration > Cloud Gateway Options**.
2. In the list **First-authentication passwords**, select the desired password entries and click to copy the credentials to the clipboard.
   The data required for connecting a device to the ICG is in the clipboard: host address, ICG server certificate fingerprint, and the password.
3. To send the credentials via e-mail, paste the data into an encrypted e-mail. To send the credentials in a printed letter, paste the data in your e-mail program or word processor.

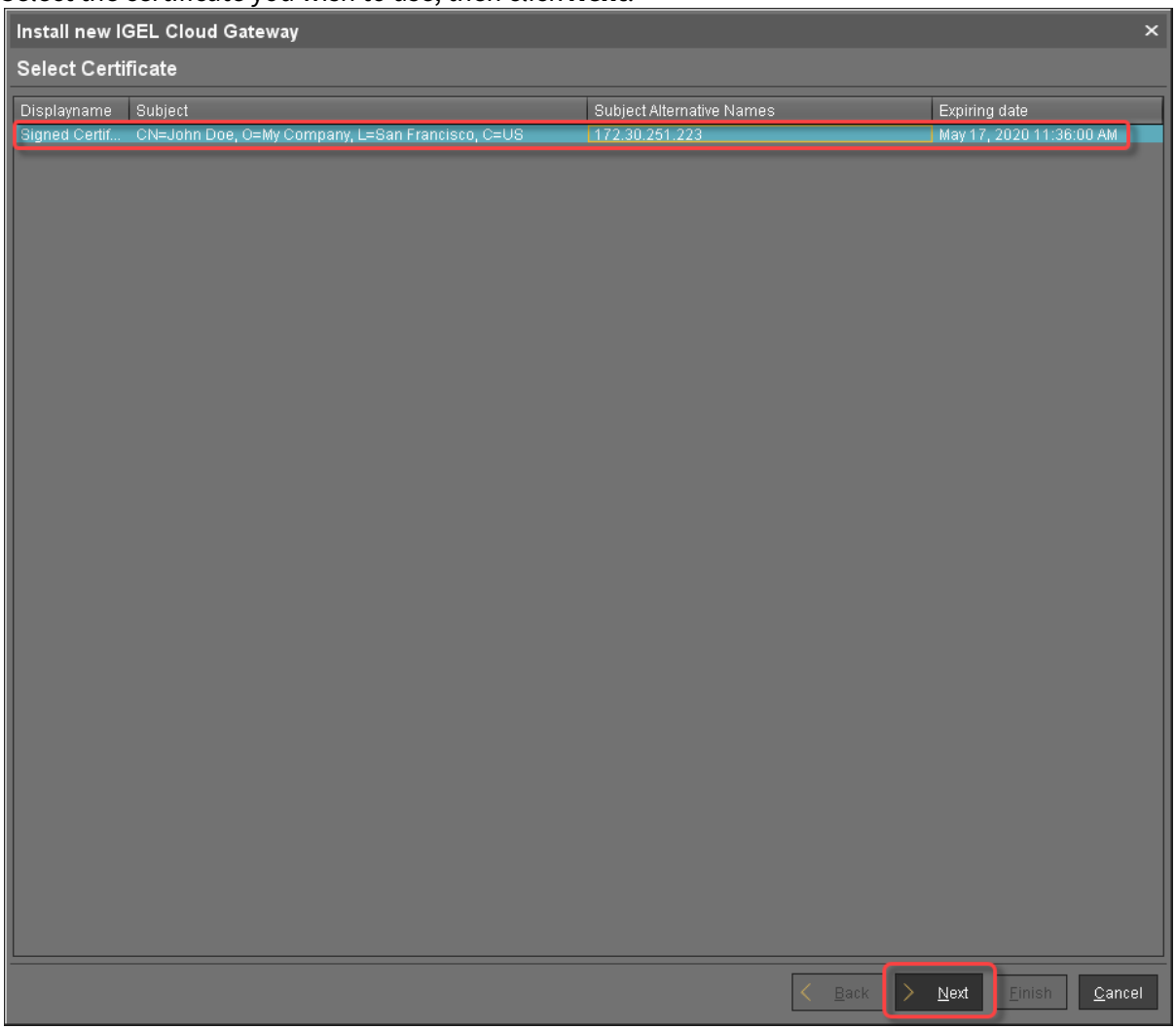
Installing IGEL Cloud Gateway (UMS 6.02 or Lower)

1. Start the UMS Console.

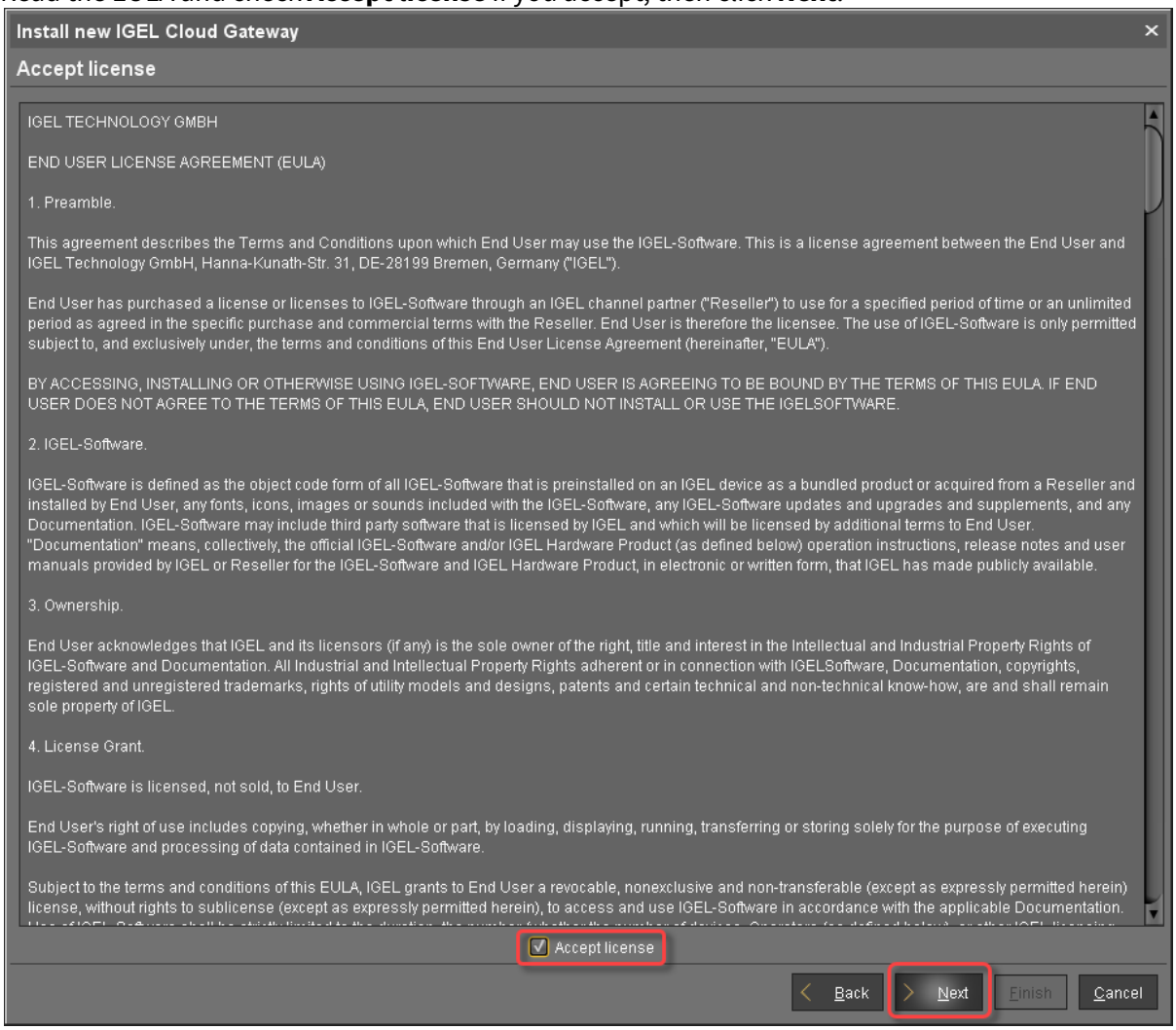
2. Go to **UMS Administration > UMS Network > Igel Cloud Gateway**.

3. In the toolbar in the upper right, click the icon (**Install new IGEL Cloud Gateway**).
   The ICG remote installer opens.

4. Select the certificate you wish to use, then click **Next**.



5. Read the EULA and check **Accept license** if you accept, then click **Next**.



6. Enter the installation parameters:
   - **SSH host**: Address of the host the ICG is to be installed on. This field is prepopulated with a host that has been derived from the certificate. If more than one hosts are specified in the certificate, ensure that this is the one that is used for communication between UMS and ICG.
   - **SSH port**: SSH port (Default: `22`)

> The SSH user needs root privileges, otherwise the remote installer will not be able to perform all required installation tasks.
> UMS 5.09.110 or higher: It is sufficient for the SSH user to have sudo privileges.

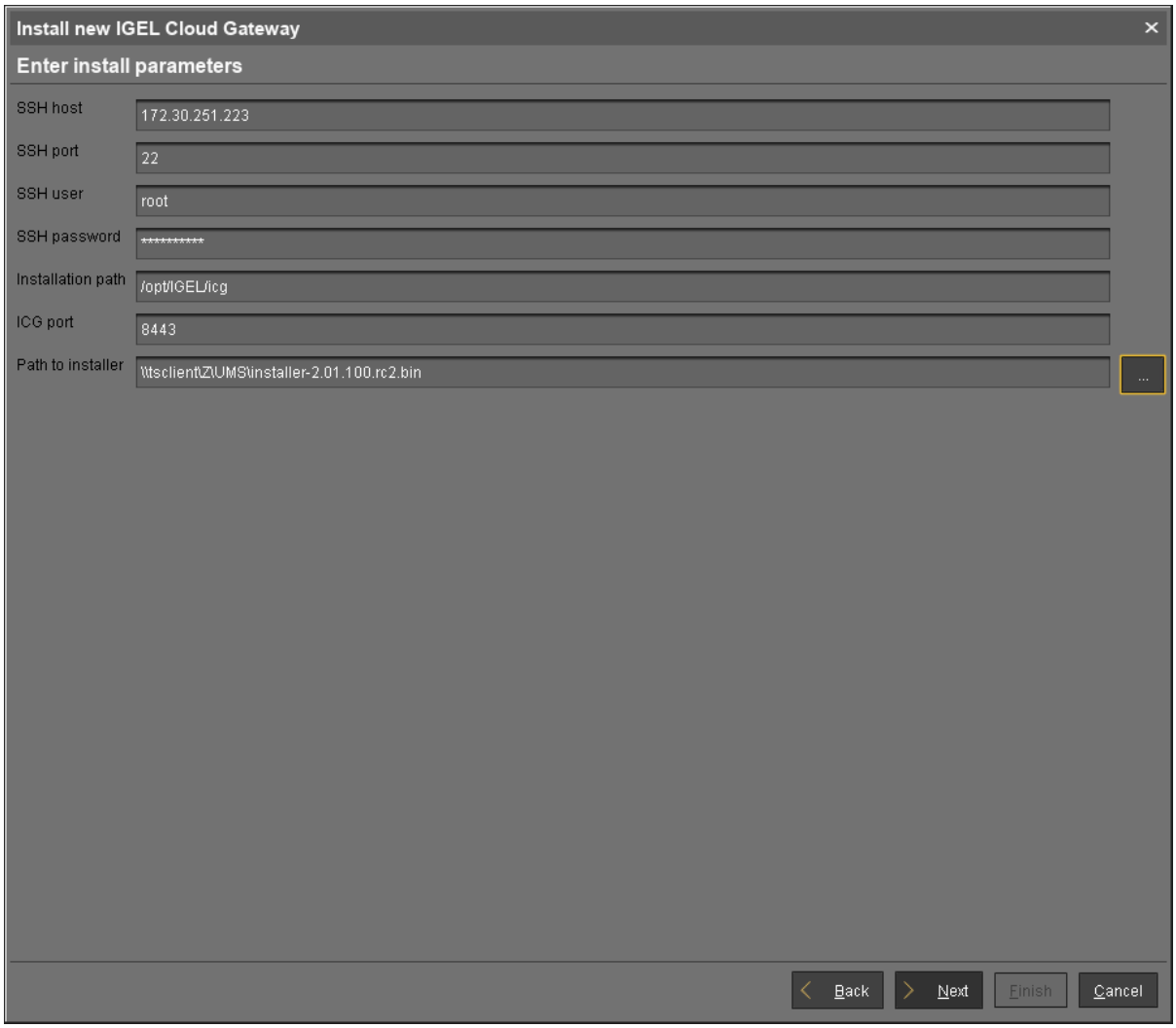
> Root access to the SSH server is a security risk!
> If you permit root login for SSH, it is recommended to disable root login when the ICG installation has finished.

> Key-based authentication is not supported by the remote installer. If you are using key-based authentication, you will have to install manually, see Installing the ICG without remote installer(see page 111).

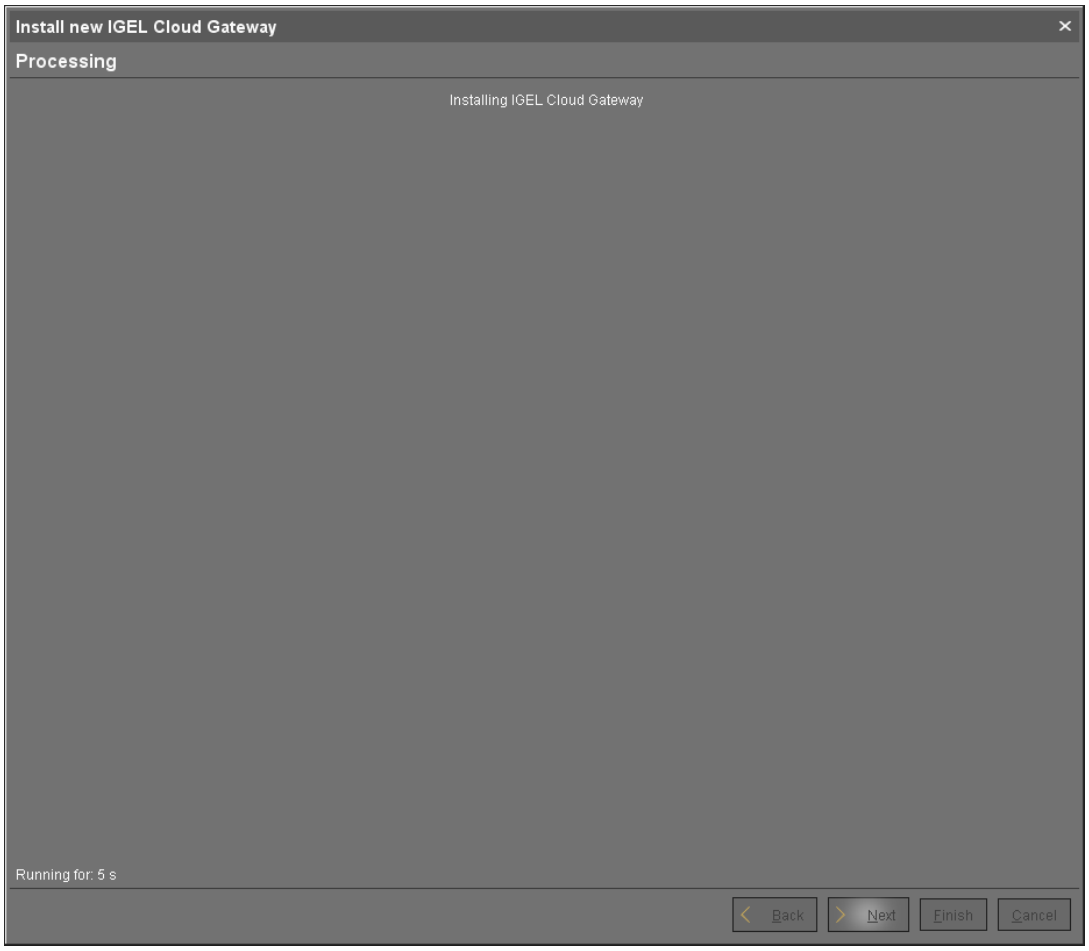
- **SSH user**: The user that remote installer uses to authenticate against the SSH server and execute the installer
- **SSH password**: Password for the user specified as **SSH user**
- **Installation path**: Installation path on the server (Default: `/opt/IGEL/icg`)
- **ICG port**: The port number the ICG will be listening on (Default: `8443`)
- **Path to installer**: The local path to the `.bin` file containing the installer

> ICG installers are available from https://www.igel.com/software-downloads/enterprise-management-pack/

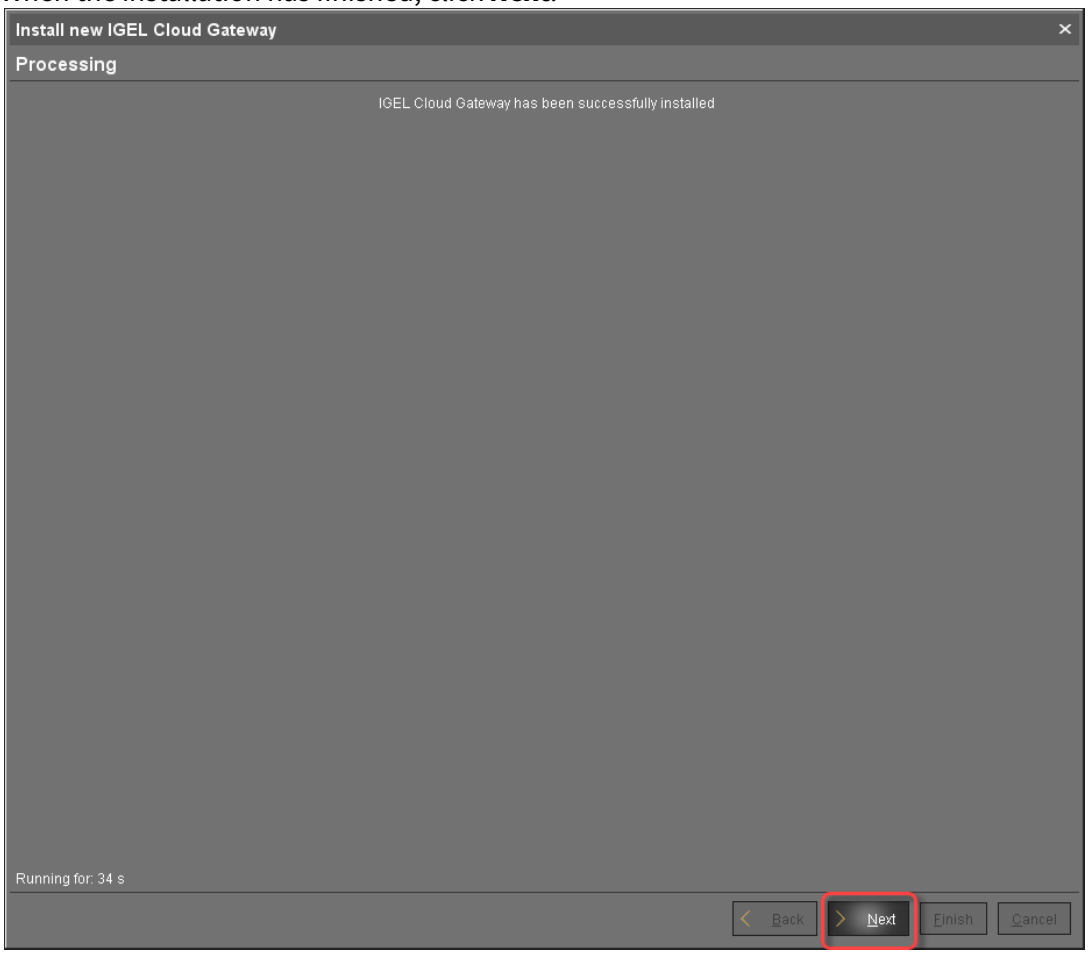
7. Click **Next**.



The ICG is now being installed. This may take a few moments.

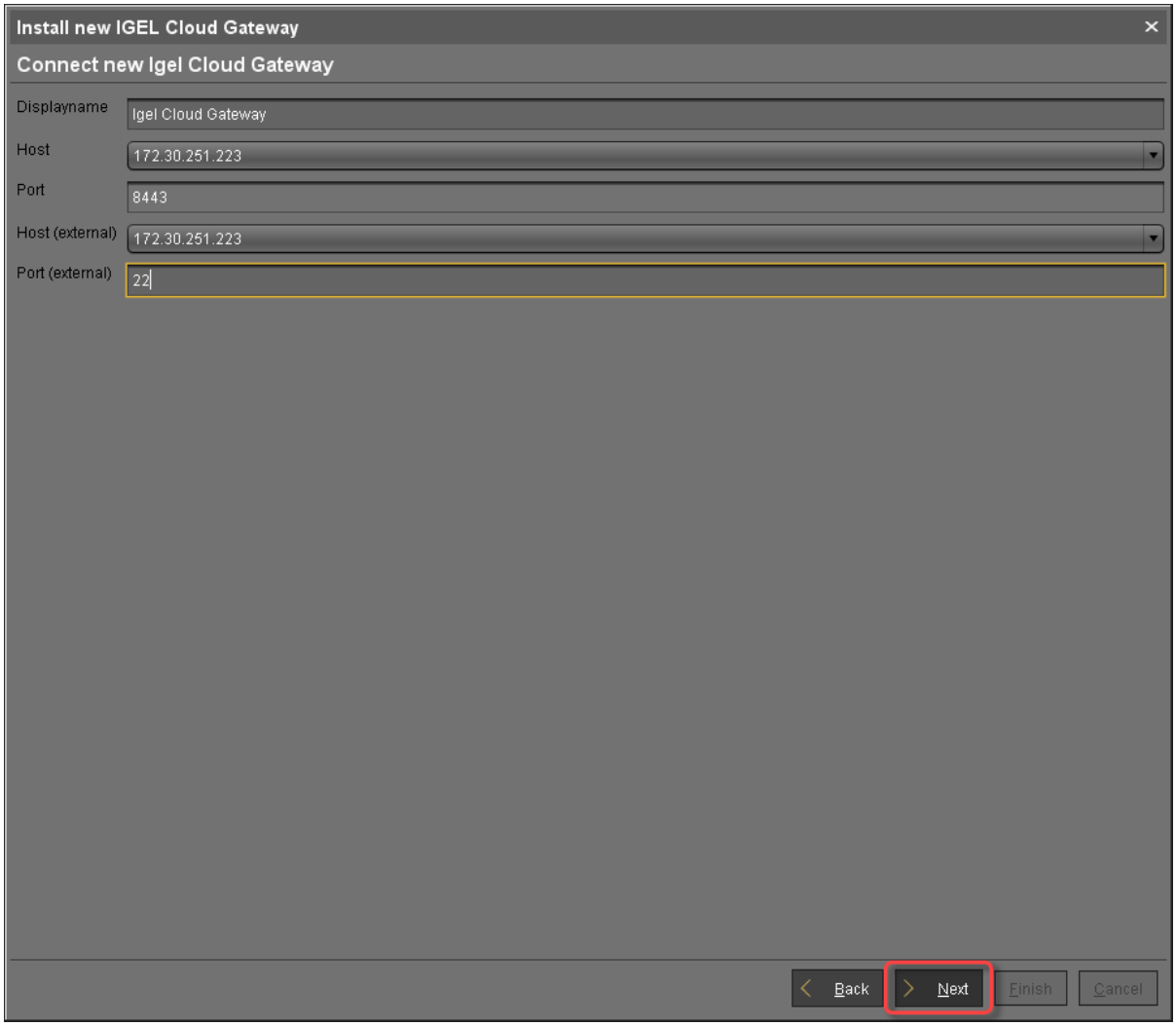

Install new IGEL Cloud Gateway
Processing
Installing IGEL Cloud Gateway
Running for: 5 s
Back
Next
Finish
Cancel

8. When the installation has finished, click **Next**.



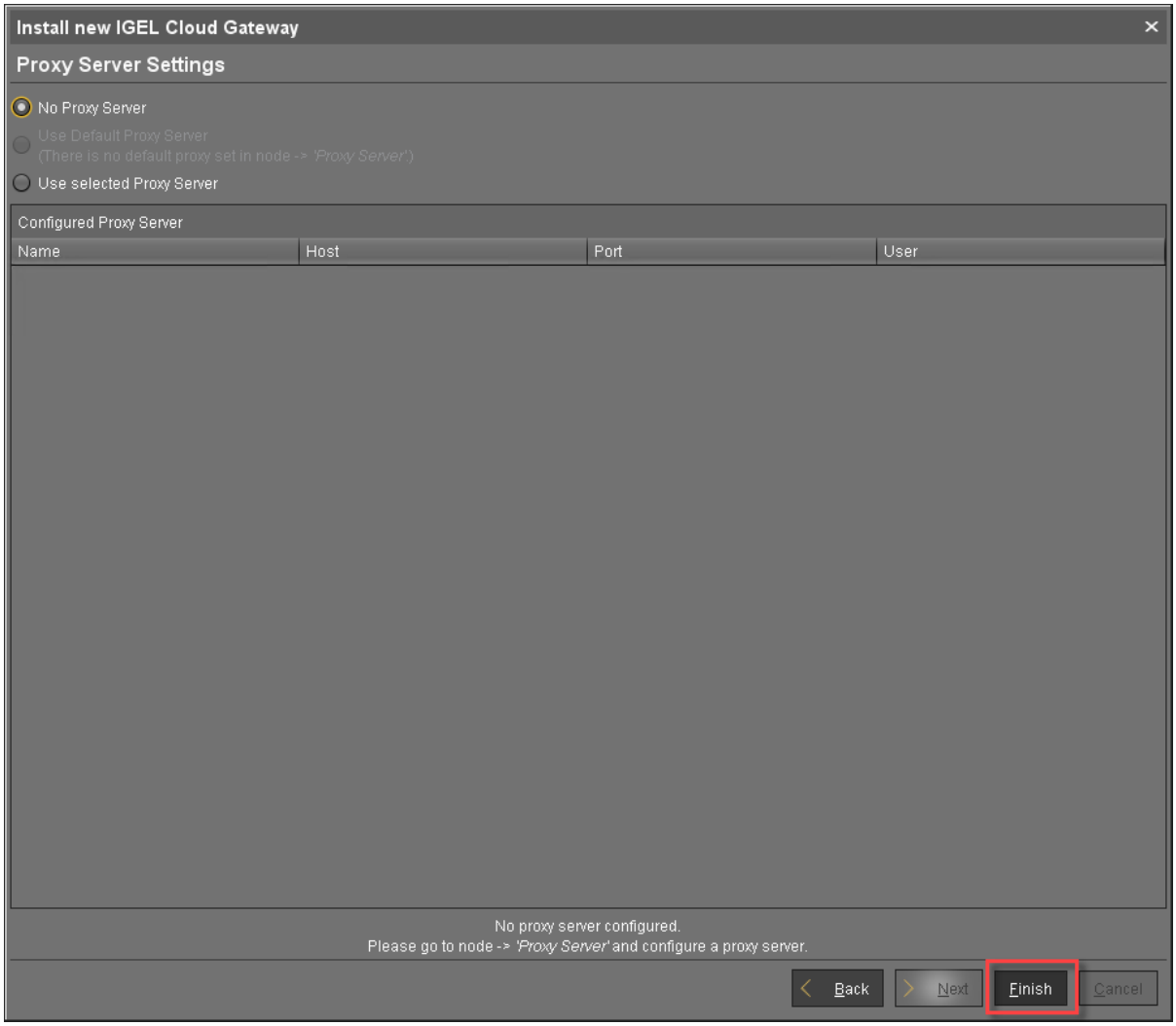
9. Enter a display name and the connection details for the ICG:
   - **Displayname**: The name used for listing the ICG under **UMS Administration > Igel Cloud Gateway**.
   - **Host**: Internal host used by the UMS for connecting to the ICG.
   - **Host (external)**: External host used by endpoint devices to connect to the ICG; only required if the devices use a separate address, not the one specified under **Host**.
   - **Port**: Port used by the endpoint devices if they connect to the ICG using the address provided under **Host (external)**. If the devices use the address under **Host**, this field can be left empty.

10. Click **Next**.

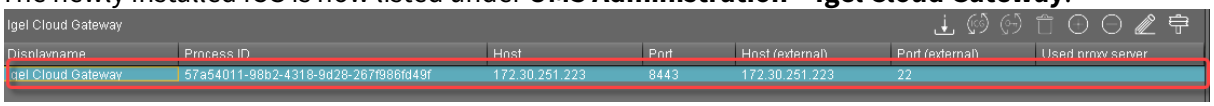


11. If desired, you can now define a proxy. Make your settings as required.

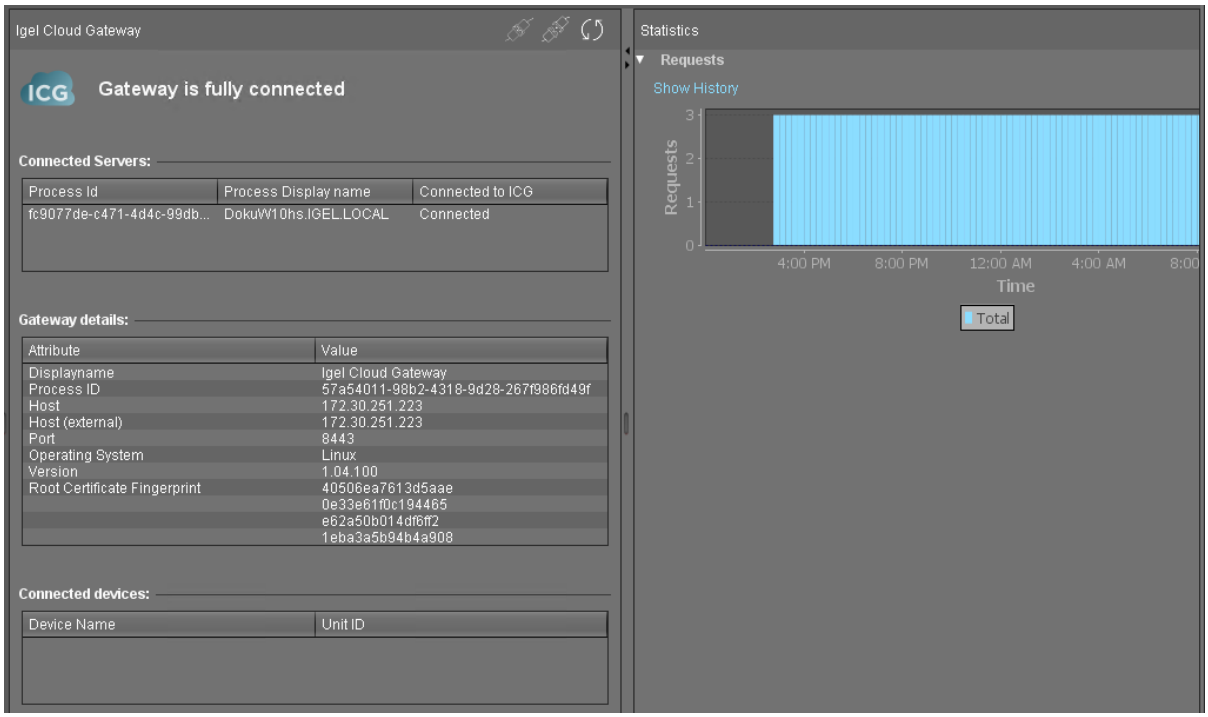
12. Click **Finish**.



The newly installed ICG is now listed under **UMS Administration > Igel Cloud Gateway**.



13. To review the status of the ICG and basic data about the installation, go to **UMS Administration > Igel Cloud Gateway >** [display name of your IGEL Cloud Gateway].



Video tutorial:

Sorry, the widget is not supported in this export.
But you can reach it using the following URL:

https://www.youtube.com/watch?v=kCwfV7aVjCs

How to Monitor the IGEL Cloud Gateway

IGEL Cloud Gateway (ICG) includes a monitoring endpoint solution, which you can integrate into your existing monitoring infrastructure (e.g. Nagios, SolarWinds, Paessler, Logic Monitor, Sensu, etc.). With the monitoring endpoint, you can check the process/service states for the ICG and, thus, react accordingly if any problems are detected.

IGEL Environment

- ICG 2.04.100 or higher

How to Request the Current Status of the ICG

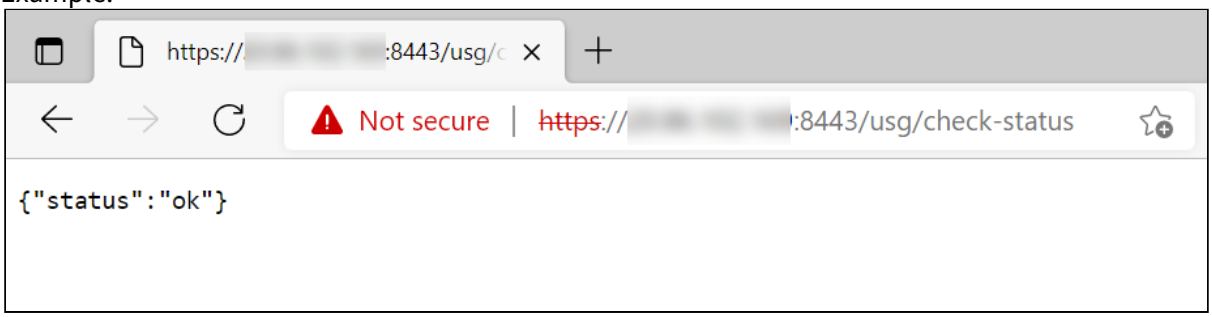
▶ Use the following request to check the status of the ICG: `https://[host]:8443/usg/check-status`
If you use a browser for this purpose and the ICG deploys a self-signed certificate, the browser may display a security/certificate warning. Accept the risk and continue, or make the certificate known to the browser.

The following responses are possible:

1. If the (check status) service is up and running, HTTP status code 200 is returned. The response body contains a `JSON` document with information on the ICG status:
   `{“status”: ”init|ok|warn|err”}`

   For details, see Monitoring the IGEL Cloud Gateway: Possible Statuses(see page 156) below.

   Example:

2. If the check status service is not reachable, HTTP status code 404 is returned.

3. Other common HTTP status codes indicating standard HTTP errors might occur.

> ⓘ Note that the status of the server updates every 30 seconds. For performance reasons, the status is NOT recalculated on each monitoring request, i.e. if a monitoring request is received, but a 30-second interval is not over, the previously saved server status will be shown.

Monitoring the ICG: Possible Statuses

ok	The ICG server is up and running.
warn	There is no UMS Server connected, see Connecting the UMS to the ICG(see page 113).
err	There is no valid ICG certificate. For details on ICG certificates, see Installation and Setup(see page 12).
init	Initialization of the ICG server has not been completed yet (e.g. loading components; connecting to UMS Servers). Note: If the initialization process is not finished within 30 seconds, the status automatically changes to **err**.

Related Topics

How to Check the Current State of the IGEL UMS Server through Your Existing Monitoring Solution

How to Configure Java Heap Size for the ICG

You experience performance issues with the IGEL Cloud Gateway (ICG). Manifold reasons can underlie performance degradation, and there are various solutions like expanding the server's physical RAM, updating the ICG and the UMS components, etc. The following article covers only the increase of the maximum memory allocated to the ICG (Java heap size).

Symptom

You face performance problems and encounter `OutOfMemory` errors in the ICG log files (`usg.log`).

Problem

The default Java heap size may be insufficient for the ICG. This usually happens if you have

- a large number of devices connected to the ICG
- many files of medium or large size transferred to the devices (background images, screensavers, etc.)

Solution: Change Java Heap Size for the IGEL Cloud Gateway

This is how you can modify the heap size for the ICG version 2.01 and higher:

1. Stop the ICG server service.
2. Edit `/opt/IGEL/icg/usg/webapps/usg.conf`
3. Change the `-Xmx` value in the following line according to your needs:
   ```
   JAVA_OPTS='-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom -Xms512M -Xmx1024m -server -XX:+UseParallelGC'
   ```
4. Reboot the server.

> The Java heap size must always be defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but it must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[8]; see also the `-Xmx` option there.
> Note also the following:

8 https://docs.oracle.com/cd/E15523_01/web.1111/e13814/jvm_tuning.htm#PERFM150

- All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the ICG server will be unable to run.
- Reducing the memory may affect the function of the ICG and is NOT recommended.
- During the ICG update, the heap size value is set to the default. Therefore, you have to adapt it again.

Related Topics

How to Configure Java Heap Size for the UMS Server

How to Configure Java Heap Size for the UMS Console

Installation of IGEL Cloud Gateway (ICG) on a SELinux System Failed

Symptom

When you try to install the IGEL Cloud Gateway (ICG) on a system on which SELinux is active, you run into an error like:

```
Error:
stderr: Python 2.7.18
Command 'systemctl --quiet enable icg-server' returned non-zero exit status 1
```

Problem

The ICG service cannot be started because it is not allowed to access the necessary system resources.
The appropriate SELinux policy is missing.

For more information on SELinux, see https://www.redhat.com/en/topics/linux/what-is-selinux

Environment

- ICG 2.04.100 and ICG 2.05.100 (tested; the solution should also work with higher versions)
- Red Hat Enterprise Linux 8.5 with kernel 4.18.0-348.el8.x86_64 (tested; the solution might also work with other Linux systems)
- The Prerequisites(see page 5) must be met
- Python must be installed
- Firewall Configuration: The port that will be used by the ICG for incoming connections must be open. By default, this is port 8443; for further information, see Network Ports Used(see page 87).

Solution

We will define an SELinux policy in a file and install it with a script in the following.

Writing the SELinux Policy

1. Login to the machine that will host your ICG and go to a directory where your user is allowed to create files.

2. Open the text editor of your choice, e.g. vi, and create a file named `icg.te`

   ```
   vi icg.te
   ```

3. Enter the following content into the file and save it as `icg.te` (in vi, the file is saved with `:wq`):

```
module icg 1.0;

require {
        type init_t;
        type user_home_t;
        class file { execute execute_no_trans ioctl open read };
}

#============= init_t ==============
allow init_t user_home_t:file { execute execute_no_trans ioctl open read };
```

Installing the SELinux Policy

1. Create another file named `icg sh`; this will be the install script.

```
vi icg.sh
```

2. Enter the following content into the file and save it as `icg.sh`:

```
#!/bin/bash
checkmodule -M -m -o icg.mod icg.te
semodule_package -o icg.pp -m icg.mod
semodule -i icg.pp
```

3. Run the install script.

```
chmod +x icg.sh
sudo ./icg.sh
```

Now that the security policy is installed, you can install the ICG on your system.

ICG Release Notes

- Notes for Release 2.05.110(see page 162)
- Notes for Release 2.05.100(see page 167)
- Notes for Release 2.04.100(see page 172)
- Notes for Release 2.03.120(see page 177)
- Notes for Release 2.03.100(see page 181)
- Notes for Release 2.02.100(see page 186)
- Notes for Release 2.01.100(see page 191)
- Notes for Release 1.04.110(see page 196)
- Notes for Release 1.04.100(see page 200)
- Notes for Release 1.03.120(see page 205)
- Notes for Release 1.03.100(see page 209)
- Notes for Release 1.02.100(see page 212)
- Notes for Release 1.01.100(see page 217)

Notes for Release 2.05.110

Version:	2.05.110
Release Date:	13.12.2022

- Important Information 2.05.110(see page 163)
- Supported Environment 2.05.110(see page 164)
- New Features 2.05.110(see page 165)
- Resolved Issues 2.05.110(see page 166)

Important Information 2.05.110

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.05.110

Debian	• Debian 10 • Debian 9
Ubuntu	• Ubuntu 20.04 • Ubuntu 18.04 • Ubuntu 16.04
Oracle Linux	• Oracle Linux 8 • Oracle Linux 7
Red Hat Enterprise Linux (RHEL)	• Red Hat Enterprise Linux (RHEL) 8 • Red Hat Enterprise Linux (RHEL) 7
SUSE Enterprise Server	• SUSE Enterprise Server 15 • SUSE Enterprise Server 12
Amazon Linux	• Amazon Linux v2

New Features 2.05.110

ICG Server

- Changed: Updated **Spring Boot** to version **2.6.13** (embedded Tomcat version 9.0.68).
- Changed: Updated **Spring Security** to version **5.6.9**

Resolved Issues 2.05.110

- Fixed: **Missing keep-alives packages** between the ICG and the devices **caused** that the **ICG did not detect dead websockets** in some cases. This led to **wrong online/offline states in UMS** and to **wrong command routing in ICG HA** environments.

Notes for Release 2.05.100

Version:	2.05.100
Release Date:	15.03.2022

- Important Information 2.05.100(see page 168)
- Supported Environment 2.05.100(see page 169)
- New Features 2.05.100(see page 170)
- Resolved Issues 2.05.100(see page 171)

Important Information 2.05.100

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.05.100

Debian	• Debian 10 • Debian 9
Ubuntu	• Ubuntu 20.04 • Ubuntu 18.04 • Ubuntu 16.04
Oracle Linux	• Oracle Linux 8 • Oracle Linux 7
Red Hat Enterprise Linux (RHEL)	• Red Hat Enterprise Linux (RHEL) 8 • Red Hat Enterprise Linux (RHEL) 7
SUSE Enterprise Server	• SUSE Enterprise Server 15 • SUSE Enterprise Server 12
Amazon Linux	• Amazon Linux v2

New Features 2.05.100

ICG Server

- Changed: Updated **bundled Zulu JRE** from version 8u302 to **8u322**.
- Changed: Updated **Spring Boot** to version **2.6.2** (embedded Tomcat version 9.0.56).

Resolved Issues 2.05.100

ICG Server

- Changed: Removed **unused dependency to log4j** (Version 1.2.17).
- Changed: Removed **unnecessary logging of temporary file transfers**.

Notes for Release 2.04.100

Version:	2.04.100
Release Date:	15.11.2021

- Important Information 2.04.100(see page 173)
- Supported Environment 2.04.100(see page 174)
- New Features 2.04.100(see page 175)
- Resolved Issues 2.04.100(see page 176)

Important Information 2.04.100

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.04.100

Debian	• Debian 10 • Debian 9
Ubuntu	• Ubuntu 20.04 • Ubuntu 18.04 • Ubuntu 16.04
Oracle Linux	• Oracle Linux 8 • Oracle Linux 7
Red Hat Enterprise Linux (RHEL)	• Red Hat Enterprise Linux (RHEL) 8 • Red Hat Enterprise Linux (RHEL) 7
SUSE Enterprise Server	• SUSE Enterprise Server 15 • SUSE Enterprise Server 12
Amazon Linux	• Amazon Linux v2

New Features 2.04.100

ICG Server

- Changed: **ICG sends now keep-alive packages to the devices** (only for IGEL OS firmware 11.05.131 and higher) to detect and close dead websockets and forward the offline state of the device to UMS.
- Added: REST endpoint to **test the status of the ICG**.
- Changed: Updated bundled **Zulu JRE** from version 8u282 to **8u302**.
- Changed: Updated **Spring Boot** to version **2.5.6** (embedded **Tomcat** version **9.0.54**).

Resolved Issues 2.04.100

ICG Server

- Fixed: **HTTP 404** errors on client requests for files after long online time of ICG server.
- Fixed: Some endpoints were **accessible without authentication**.

Notes for Release 2.03.120

Version:	2.03.120
Release Date:	27.07.2021

- Important Information 2.03.120(see page 178)
- Supported Environment 2.03.120(see page 179)
- Resolved Issues 2.03.120(see page 180)

Important Information 2.03.120

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.03.120

Debian	• Debian 10 • Debian 9
Ubuntu	• Ubuntu 20.04 • Ubuntu 18.04 • Ubuntu 16.04
Oracle Linux	• Oracle Linux 8 • Oracle Linux 7
Red Hat Enterprise Linux (RHEL)	• Red Hat Enterprise Linux (RHEL) 8 • Red Hat Enterprise Linux (RHEL) 7
SUSE Enterprise Server	• SUSE Enterprise Server 15 • SUSE Enterprise Server 12
Amazon Linux	• Amazon Linux v2

Resolved Issues 2.03.120

ICG Server

- Fixed: **HTTP 404 errors on client requests for files** after long online time of ICG server.

Notes for Release 2.03.100

Version:	2.03.100
Release Date:	29.03.2021

- Important Information 2.03.100(see page 182)
- Supported Environment 2.03.100(see page 183)
- New Features 2.03.100(see page 184)
- Resolved Issues 2.03.100(see page 185)

Important Information 2.03.100

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.03.100

Debian	• Debian 10 • Debian 9
Ubuntu	• Ubuntu 20.04 • Ubuntu 18.04 • Ubuntu 16.04
Oracle Linux	• Oracle Linux 8 • Oracle Linux 7
Red Hat Enterprise Linux (RHEL)	• Red Hat Enterprise Linux (RHEL) 8 • Red Hat Enterprise Linux (RHEL) 7
SUSE Enterprise Server	• SUSE Enterprise Server 15 • SUSE Enterprise Server 12
Amazon Linux	• Amazon Linux v2

New Features 2.03.100

ICG Server

- Changed: **Inform UMS** if a message is sent to **a device**, which is **currently not connected**.
- Changed: Improved **performance for the UMS <-> ICG synchronization**.
- Changed: Updated bundled **Zulu JRE** from version 8u265 to **8u282**.
- Changed: Updated **Spring Boot** to version **2.2.13.RELEASE** (embedded **Tomcat** version **9.0.41**).

Resolved Issues 2.03.100

ICG Server

- Fixed: **Older log files** and the **access log not** included **in ICG support information**.

Notes for Release 2.02.100

- Important Information 2.02.100(see page 187)
- Supported Environment 2.02.100(see page 188)
- New Features 2.02.100(see page 189)
- Resolved Issues 2.02.100(see page 190)

Important Information 2.02.100

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.

Supported Environment 2.02.100

Debian

- Debian 10
- Debian 9

Ubuntu

- Ubuntu 20.04
- Ubuntu 18.04
- Ubuntu 16.04

Oracle Linux

- Oracle Linux 8
- Oracle Linux 7

Red Hat Enterprise Linux (RHEL)

- Red Hat Enterprise Linux (RHEL) 8
- Red Hat Enterprise Linux (RHEL) 7

SUSE Enterprise Server

- SUSE Enterprise Server 15
- SUSE Enterprise Server 12

Amazon Linux

- Amazon Linux v2

New Features 2.02.100

ICG Server

- Added: Possibility to **limit the maximum number of device connections**. This limit can be administrated with **UMS 6.05.100 or higher**.
- Added: ICG now **reports the real name of the underlying Linux distribution to the UMS** for display in the UMS Console.
- Changed: Limited **TLS** version to **1.2** and **updated cipher suite** list.
- Changed: Updated **Spring Boot** to version **2.2.8.RELEASE** (embedded **Tomcat** version **9.0.36**).
- Changed: Updated bundled **Zulu JRE** from version 8u212 to **8u252**.

ICG Installer

- Added: **Support** for **Debian 10**, **Ubuntu 20.04**, **Red Hat Enterprise Linux 8**, **Oracle Linux 8**, and **Amazon Linux 2**.
- Added: ICG can now be **installed with port 443** (or any other privileged port).

Resolved Issues 2.02.100

ICG Server

- Fixed: The **first authentication password** of a UMS Server was **reactivated after reboot** (ISN-2020-06).
- Fixed: Reworked **authorization** concept (ISN-2020-06).
- Fixed: Secured handling of **websocket messages** (ISN-2020-06).
- Fixed: **List of connected UMS Servers** was **false** under certain circumstances. This led to a wrong view of connected UMS in UMS UI.
- Fixed: **Device connections are not accepted** if no UMS is connected to the ICG.
- Fixed: Improved performance on **UMS <-> ICG synchronization**.
- Fixed: **UMS Webdav synchronization** caused errors with deleted files.
- Changed: Removed **sensitive data** from **server status response** (ISN-2020-06).
- Changed: Removed **sensitive data** from **log files** (ISN-2020-06).
- Changed: Replaced **caching layer** to reduce memory consumption.

Notes for Release 2.01.100

- Important Information 2.01.100(see page 192)
- Supported Environment 2.01.100(see page 193)
- New Features 2.01.100(see page 194)
- Resolved Issues 2.01.100(see page 195)

Important Information 2.01.100

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions.
- ICG requires **IGEL OS** firmware **10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions.
- Due to structural changes between ICG 1.04 and ICG 2.01, **a downgrade is not possible**.
- ICG 2.01 does NOT support the following UMS functionalities yet:
    - Universal Firmware Update.

Supported Environment 2.01.100

Debian

- Debian 9 (64 bit)
- Debian 8 (64 bit)

Ubuntu

- Ubuntu 18.04 (64 bit)
- Ubuntu 16.04 (64 bit)

Oracle Linux

- Oracle Linux 7 (64 bit)

Red Hat Enterprise Linux (RHEL)

- Red Hat Enterprise Linux (RHEL) 7 (64 bit)
- Red Hat Enterprise Linux (RHEL) 6 (64 bit)

SUSE Enterprise Server

- SUSE Enterprise Server 12 (64 bit)

New Features 2.01.100

ICG Server

- Added: **Support for Shadowing** and **Secure Shadowing** from UMS (**UMS** version **6.02.110 or higher** and **IGEL OS** firmware **11.02.100 or higher** required).
- Changed: The bundled Oracle JRE has been replaced with **Azul Zulu JRE 8 Update 212**.
- Changed: Migrated from standalone Tomcat to **Spring Boot** application **with embedded Tomcat** (**Tomcat** version **9.0.14**).
- Changed: Files and credentials are now stored in an integrated **HyperSQL Database** (HSQLDB).

Resolved Issues 2.01.100

ICG Installer

- Fixed: **Update from 1.03.120 or lower to 1.04.100 or higher** was not possible.
- Fixed: Added missing **logfile symlink /var/log/icg**.
- Changed: ICG installer does now support both **Python 2** and **Python 3**.

ICG Server

- Fixed: Removed **logging of hashed passwords**.

Notes for Release 1.04.110

- Important Information 1.04.110(see page 197)
- Supported Environment 1.04.110(see page 198)
- Resolved Issues 1.04.110(see page 199)

Important Information 1.04.110

- ICG requires **UMS 5.07.100 or higher**, it is not compatible with lower UMS versions
- ICG requires I**GEL OS firmware 10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions
- The ICG v1.04 does NOT support the following UMS functionalities yet:
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
- The ICG installer requires python 2.6 or higher, Python 3.x is not supported. A symlink python2 pointing to the python 2.6+ installation is also necessary.

Supported Environment 1.04.110

Debian

- Debian 9 (64 bit)
- Debian 8 (64 bit

Ubuntu

- Ubuntu 18.04 (64 bit)
- Ubuntu 16.04 (64 bit)
- Ubuntu 14.04 (64 bit)

Oracle Linux

- Oracle Linux 7 (64 bit)

Red Hat Enterprise Linux (RHEL)

- Red Hat Enterprise Linux (RHEL) 7 (64 bit)
- Red Hat Enterprise Linux (RHEL) 6 (64 bit)

SUSE Enterprise Server

- SUSE Enterprise Server 12 (64 bit)

Resolved Issues 1.04.110

- Fixed: No feedback was sent to UMS if remote installation failed

Notes for Release 1.04.100

- Important Information 1.04.100(see page 201)
- Supported Environment 1.04.100(see page 202)
- New Features 1.04.100(see page 203)
- Resolved Issues 1.04.100(see page 204)

Important Information 1.04.100

- ICG requires **UMS 5.07.100 or higher**, it is not compatible with lower UMS versions
- ICG requires **IGEL OS firmware 10.02.100 or higher** on the endpoints, it is not compatible with lower firmware versions
- The ICG v1.04 does NOT support the following UMS functionalities yet:
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
- The ICG installer requires python 2.6 or higher, Python 3.x is not supported. A symlink python2 pointing to the python 2.6+ installation is also necessary.

Supported Environment 1.04.100

Debian

- Debian 9 (64 bit)
- Debian 8 (64 bit

Ubuntu

- Ubuntu 18.04 (64 bit)
- Ubuntu 16.04 (64 bit)
- Ubuntu 14.04 (64 bit)

Oracle Linux

- Oracle Linux 7 (64 bit)

Red Hat Enterprise Linux (RHEL)

- Red Hat Enterprise Linux (RHEL) 7 (64 bit)
- Red Hat Enterprise Linux (RHEL) 6 (64 bit)

SUSE Enterprise Server

- SUSE Enterprise Server 12 (64 bit)

New Features 1.04.100

ICG Server

- Changed: Because of security reasons, the **HTTPS connector** of the ICG server does now provide **TLSv1.2 only**.
- Added: Support of **UMS High Availability feature** (required **UMS version: 5.09.100 or higher**)
- Changed: UMS **one-time password** is valid until the first UMS instance has connected to the ICG
- Added: Support of UMS essentials for **Mobile Device Management (MDM)**. (required **UMS version: 5.09.100 or higher**)
- Updated: **Java** version to **1.8.0_181**
- Updated: **Apache Tomcat** from version **8.0.48 to 8.5.29**

ICG Installer

- Added: Support for **SUSE Enterprise Server**
- Added: Support for **Oracle Linux**
- Added: Support for **Red Hat Enterprise Linux**
- Added: A new dialog displaying the **EULA**
- Added: Support for the new UMS-internal **remote installer for Igel Cloud Gateway**
- Changed: The **visual presentation** of the **startup** of the IGEL Cloud Gateway after the installation step has improved.
- Changed: Simplified the **certificate update/replacement**

Resolved Issues 1.04.100

- Fixed: Disable **Apache Tomcat welcome** page

Notes for Release 1.03.120

Software:	Version	1.03.120
Release Date:	2018-05-11	
Release Notes:	Version	RN-103120-1
Last update:	2018-05-11	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

- Important Information 1.03.120(see page 206)
- New Features 1.03.120(see page 207)
- Resolved Issues 1.03.120(see page 208)

Important Information 1.03.120

- ICG requires **UMS 5.06.100 or higher**, it is not compatible with lower UMS versions
- ICG requires **Linux firmware 10.02.100 or higher**, it is not compatible with lower firmware versions
- The **ICG v1.03 does NOT support** the following UMS functionalities yet
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
- ICG **installer tested** on
    - Ubuntu 16.04
    - Debian 8.6

New Features 1.03.120

ICG Server

- Changed: Because of security reasons, the https connector of the ICG Server now **provides TLSv1.2 only**.
- Updated: **Apache Tomcat** from version 8.0.41 to **8.0.50**
- Updated: **JRE** from version 8u121 to **8u162**

ICG Installer

- A new dialog displaying the **EULA** was added.

Resolved Issues 1.03.120

ICG Server

- Fixed: Disable **Apache Tomcat welcome page**

Notes for Release 1.03.100

Software:	Version	1.03.100
Release Date:	2017-08-30	
Release Notes:	Version	RN-103100-1
Last update:	2017-08-30	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

- Important Information 1.03.100(see page 210)
- New Features 1.03.100(see page 211)

Important Information 1.03.100

- ICG requires UMS *version 5.06.100* or higher, **it is not compatible with lower UMS versions**
- ICG requires Linux firmware *version 10.02.100* or higher, **it is not compatible with lower firmware versions**
- The ICG *version 1.03* does **NOT** support the following UMS functionalities yet:
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
- ICG installer **tested on**:
    - Ubuntu 16.04
    - Debian 8.6

New Features 1.03.100

ICG Server

- Added: **Multiple-time passwords** for the first authentication of a Thin Client. This feature requires UMS *version 5.07.100* or higher.

Notes for Release 1.02.100

Software:	Version	1.02.100
Release Date:	2017-04-18	
Release Notes:	Version	RN-101100-1
Last update:	2017-04-18	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

- Important Information 1.02.100(see page 213)
- New Features 1.02.100(see page 214)
- Resolved Issues 1.02.100(see page 215)
- Known Issues 1.02.100(see page 216)

Important Information 1.02.100

- ICG requires **UMS 5.06.100** or higher, it is **not compatible with lower UMS versions**
- ICG requires **Linux firmware 10.02.120** or higher, it is **not compatible with lower firmware versions**
- The **ICG version 1.02.** does **NOT** support the following UMS functionalities yet
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
    - Firmware Customizations of type 'Wallpaper' and 'Bootsplash'
- **ICG installer tested** on
    - Ubuntu 16.04
    - Debian 8.6

New Features 1.02.100

ICG Installer

- Changed: Support of **Igel Cloud Gateway keystore** exported from UMS
- Added **uninstaller**

Resolved Issues 1.02.100

ICG Server

- Fixed: **Tomcat** started after reboot
- Fixed: **Connection was lost randomly**
  Added heart-beating to test healthiness of the underlying TCP connection
- Changed: **Improved performance and stability with protocol changes**

ICG installer

- Fixed: **Identifier of ICG** was not copied on update installation

Known Issues 1.02.100

Thin Clients

- **Thin Clients**, which are in the recycle bin and are registered via ICG **could not connect with ICG after reboot**.
  Workaround: Delete Thin Client from recycle bin, before register it via ICG.

Notes for Release 1.01.100

Software:	Version	1.01.100
Release Date:	2017-02-28	
Release Notes:	Version	RN-101100-1
Last update:	2017-02-28	

Following formatting is used in this document:

format type	example	use
bold and underlined	enable/disable	the default setting of a value
bold and arrow	**menu > path**	menu path in the IGEL setup
bold	**GUI** [keyboard]	elements of the graphical user interface or commands that are entered using the keyboard
within brackets	**[session name]**	variable values

- Important Information 1.01.100(see page 218)
- Known Issues 1.01.100(see page 219)

Important Information 1.01.100

- ICG requires UMS 5.05.100 or higher
- ICG requires linux firmware 10.01.310 or higher
- The ICG v1.01 does NOT support the following UMS functionality
    - Universal Firmware Update
    - Secure VNC
    - Secure Terminal
    - Firmware Customizations of type 'Wallpaper' and 'Bootsplash'

Known Issues 1.01.100

Thin Clients

- Thin Clients, which are in the **recycle bin** and are registered via ICG could not connect with ICG after reboot.
  Workaround: Delete Thin Client from bin, before register it via ICG.

ICG Field Experience

- Installing ICG on AWS and Certificate Passing Issue When Using Putty(see page 221)
- Recommendation for a Free Signed Certificate for ICG(see page 222)

Installing ICG on AWS and Certificate Passing Issue When Using Putty

Solution Based on Experience from the Field

This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Symptom

Description: When you are installing ICG in AWS and trying to get to it via Putty, you might experience a certificate transmission issue.

Environment

- UMS version: any

Problem

If you are installing the ICG into Amazon Web Services, and you are using Windows and Putty to access the Ubuntu Server in AWS, you have the problem to transmit the given .pem certificate to authenticate.

Solution

▶ Follow the instructions under https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

Recommendation for a Free Signed Certificate for ICG

> **Solution Based on Experience from the Field**
>
> This article provides a solution that has not been approved by the IGEL Research and Development department. Therefore, official support cannot be provided by IGEL. Where applicable, test the solution before deploying it to a productive environment.

Overview

This article addresses the issue when the customers need a signed cert, but don't want to use the UMS as CA.

You can use "letsencrypt" as a CA for quickly and easily grabbing a FREE certificate for your ICG server (or for any server where you need a signed cert). At this point, LetsEncrypt is trusted by all the browsers and it has a completely automated process for initially retrieving a new singed cert and also for renewing.

Environment

- UMS version: any

Instructions

Here's the process that we followed on an Ubuntu 16.04 Digital Ocean droplet. (This page is good overview: https://certbot.eff.org/lets-encrypt/ubuntuxenial-other)

1. Open up incoming port 80 (temporarily) on your server firewall to allow for automated verification that you control the domain (see below).
2. Make sure that the FQDN names that you'll be getting certs for do DNS resolve to your droplet (verification will fail if they don't).
3. Install certbot like this (from above link):
   ```
   sudo apt-get update
   sudo apt-get install software-properties-common
   sudo add-apt-repository ppa:certbot/certbot
   sudo apt-get update
   sudo apt-get install certbot
   ```
4. Run the command: `sudo certbot certonly`
5. Choose "spin up a temporary web server" (this is used for let's encrypt to fetch a page and verify that you control the domain).
6. Enter your domain names (separated by a comma) that you want to create a cert for and press "enter".
7. Finish the remaining questions.
8. If all was successful, you'll find your server certificate (cert1.pem), root CA Chain (chain1.pem), and private key (privkey1.pem) in the `/etc/letsencrypt/archive/<your domain name>` folder.
9. These files are all ready and in the right format to add to UMS and create your `keystore.icg` file.