IGEL Cloud Gateway (ICG)

ICG Handbuch

IGEL Cloud Gateway (ICG) erweitert die Universal Management Suite (UMS) um die Möglichkeit, Geräte außerhalb des Firmennetzwerks sicher zu verwalten.

Was ist neu in ICG 12.04.100?

Die Release Notes zu IGEL Cloud Gateway 12.04.100 finden Sie sowohl als Textdatei neben den Installationsprogrammen unter https://www.igel.com/software-downloads/cosmos/ und in der Knowledge Base unter Notes for Release ICG 12.04.100 (see page 153).

Installationsvoraussetzungen

Um eine funktionierende Umgebung mit der Universal Management Suite (UMS) und dem IGEL Cloud Gateway zu installieren und in Betrieb zu nehmen, benötigen Sie die folgenden Komponenten:

Universal Management Suite (UMS)

Für den grundlegenden Funktionsumfang ist Universal Management Suite (UMS) 5.06.100 oder höher erforderlich. Wenn Spiegeln (Shadowing) oder Sicheres Spiegeln (Secure Shadowing) benötigt wird, ist Version 6.02.110 oder höher erforderlich.

Geräte mit IGEL OS Firmware

Für den grundlegenden Funktionsumfang ist IGEL OS 10.02.100 oder höher erforderlich. Wenn Spiegeln (Shadowing) oder Sicheres Spiegeln (Secure Shadowing) benötigt wird, ist Version 11.02.100 oder höher erforderlich.

Wenn Sie ausschließlich IGEL OS 12-Geräte verwalten, benötigen Sie möglicherweise kein IGEL Cloud Gateway (ICG) zwischen Ihrer UMS 12 und Ihren Geräten, unabhängig davon, ob sich die Geräte innerhalb oder außerhalb des Unternehmensnetzwerks befinden. Ob ein ICG erforderlich ist oder nicht, hängt von Ihrem speziellen Anwendungsfall oder Ihrer Richtlinie ab. Siehe IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.
Wenn Sie entfernte IGEL OS 11-Geräte verwalten und auch Ihre entfernten IGEL OS 12-Geräte über ICG verwalten möchten, ist ICG 12 erforderlich.
Wenn Sie Ihre entfernten IGEL OS 12-Geräte ohne ICG verwalten möchten und zugleich entfernte IGEL OS 11-Geräte verwalten, können Sie ICG 12 oder ICG 2.x verwenden.

Bitte beachten Sie das Folgende, besonders wenn Sie spezielle Richtlinien oder andere Komponenten zwischen den Geräten und der IGEL Universal Management Suite (UMS) oder dem IGEL Cloud Gateway (ICG) verwenden:

- IGEL OS 12-Geräte verwenden TLS 1.3
- IGEL OS 11-Geräte verwenden TLS 1.2

Linux-Host

Hardware

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

Der ICG-Dienst selbst benötigt mindestens 4 GB RAM, 2 CPUs, 2 GB freier Speicherplatz (hängt stark von der Anzahl der zu verwaltenden Geräte ab).

Betriebssystem

Die folgenden Linux-Distributionen (64-Bit-Variante) werden unterstützt:

- Amazon Linux v2
- Debian 11
- Debian 10
- Ubuntu 22.04
- Ubuntu 20.04
- 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

Zertifikate

Für die Kommunikation zwischen dem ICG und den Geräten muss eine Zertifikatskette bereitgestellt werden. Die Anforderungen sind unter Zertifikatsanforderungen und -empfehlungen für IGEL Cloud Gateway (ICG) (see page 14) beschrieben. Die verschiedenen Methoden zur Beschaffung der Zertifikatskette sind unter Bestehende Zertifikatskette installieren (see page 16), Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (see page 27) und Zertifikat mit der UMS erstellen (see page 35) beschrieben.

> Beachten Sie bitte auch unsere Leitlinien zu Installation und Größenbestimmung im UMS Handbuch.

Wann sollte ICG verwendet werden

Typische Szenarien

Das IGEL Cloud Gateway (ICG) ist erforderlich, wenn sich die UMS und die Geräte nicht im selben Netzwerk befinden. Die folgenden Szenarien sind typische Anwendungsfälle für das ICG:

- Die Endgeräte (IGEL UD, UD Pocket oder mit UDC3/OSC konvertierte Geräte) aller geografisch verteilten Niederlassungen eines Unternehmens sollen von einer zentralen UMS verwaltet werden.
- UD Pocket oder mit UDC3/OSC konvertierte Geräte sollen von der UMS verwaltet werden, die sich "on premises" befindet.

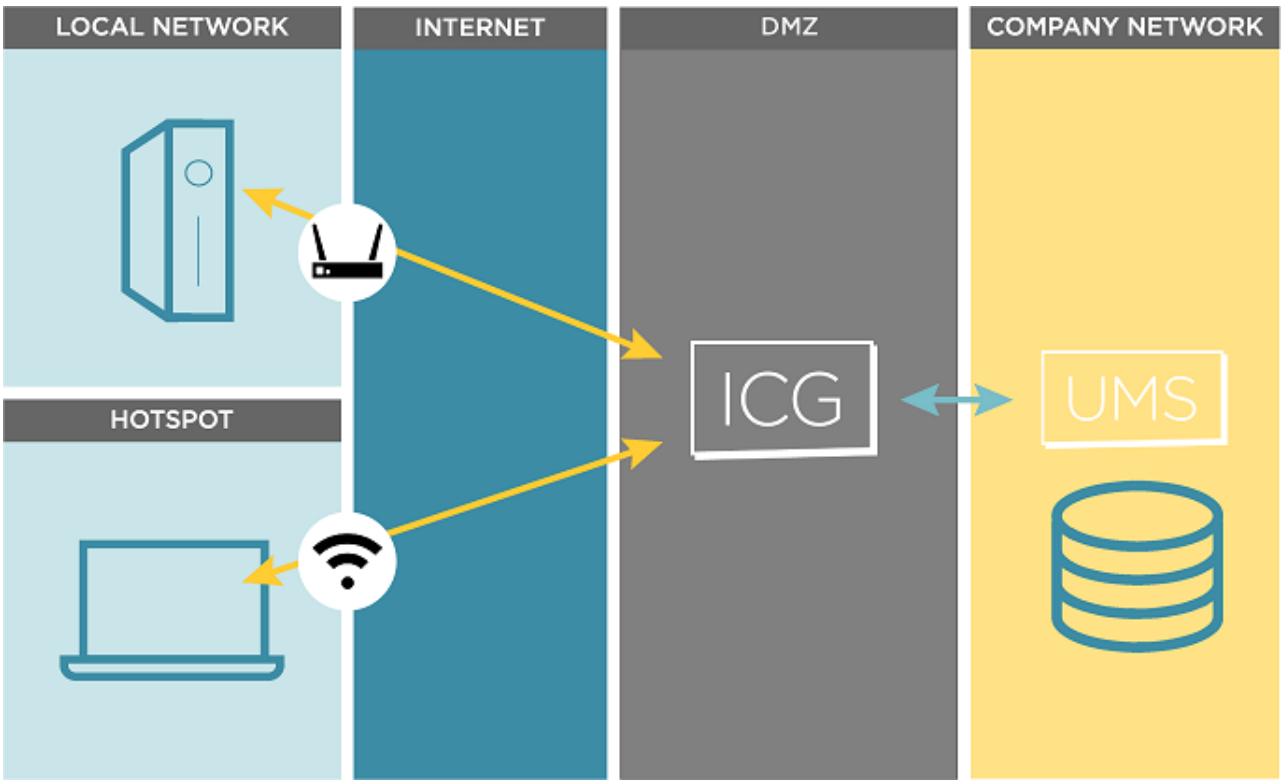
Detaillierte Informationen zu UMS Installationsszenarien finden Sie unter Leitlinien zur Installation und Größenbestimmung der IGEL UMS.

Die möglichen Netzwerktopologien sind unten aufgeführt.

Siehe auch IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.

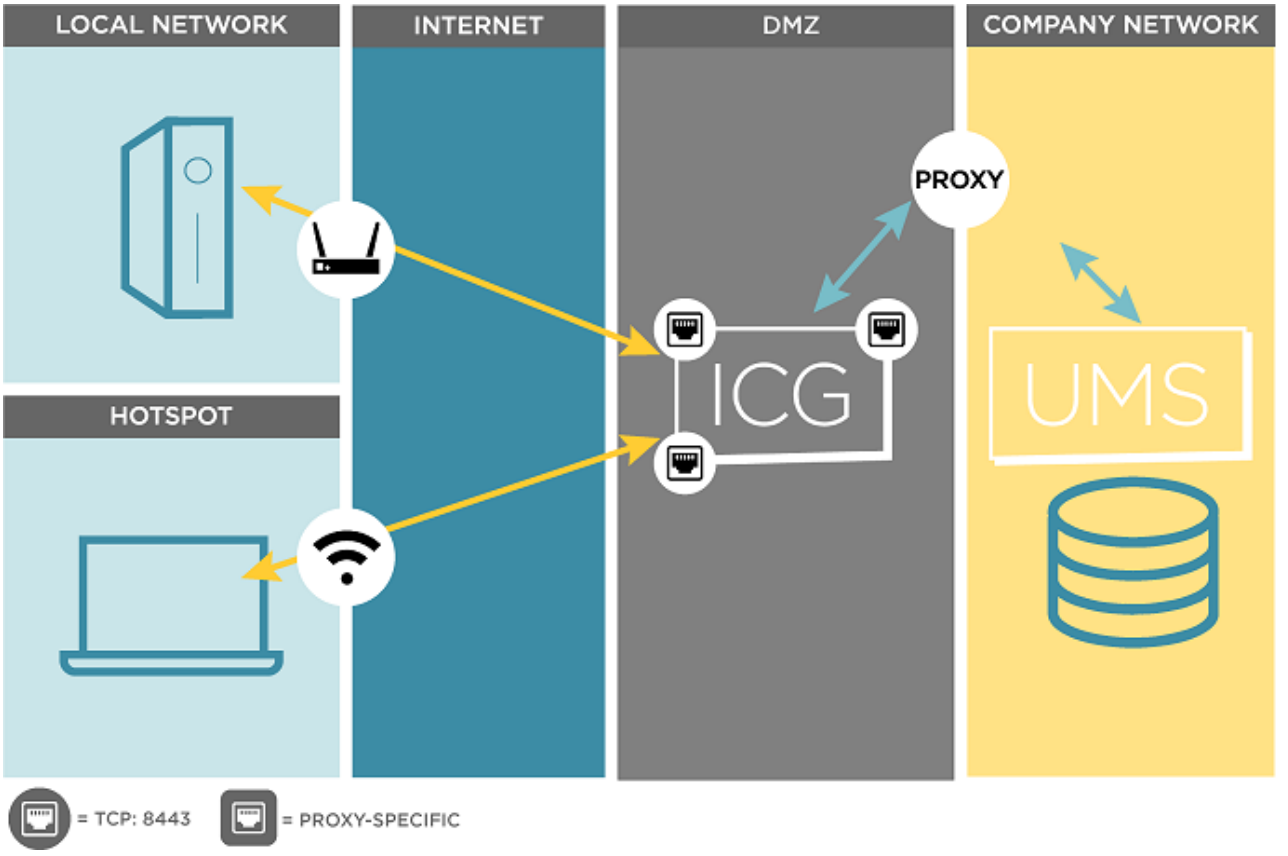
Netzwerktopologien

ICG in der Demilitarized Zone (DMZ) des Unternehmensnetzwerks

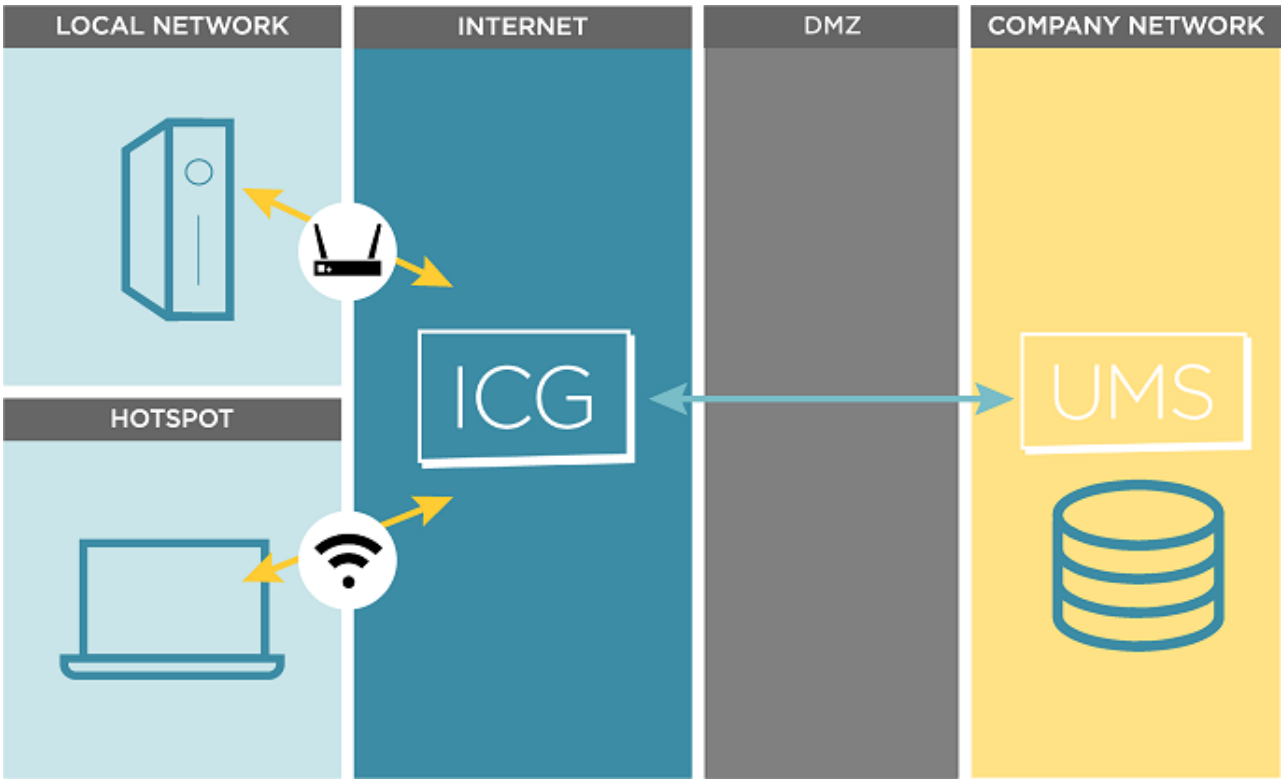


ICG in der Demilitarized Zone (DMZ) des Unternehmensnetzwerks und Proxy

Dieses Szenario wird ab UMS Version 5.08 unterstützt.

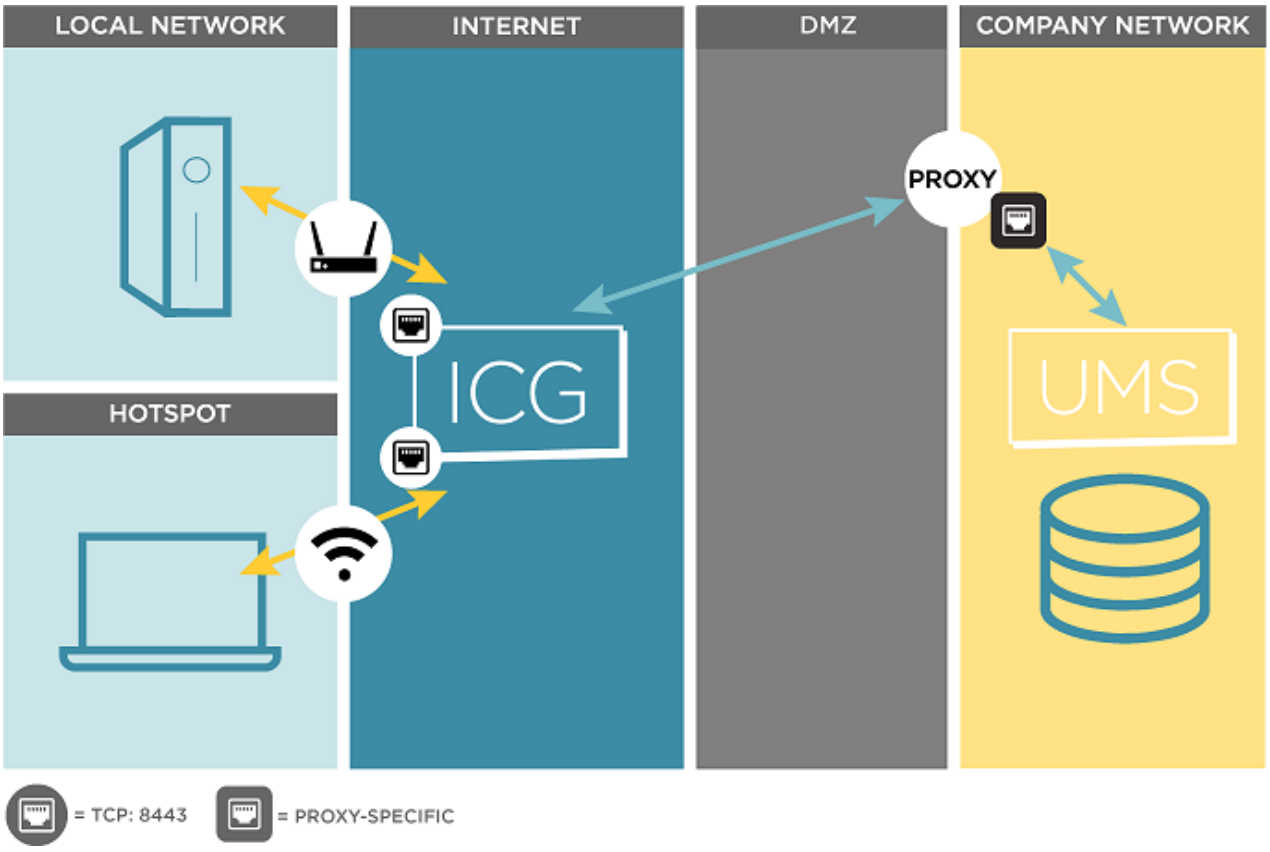


ICG im Internet (z.B. bei einem Cloud-Dienstleister)



ICG im Internet mit Proxy (z.B. bei einem Cloud-Dienstleister)

Dieses Szenario wird ab UMS Version 5.08 unterstützt.


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

Einschränkungen

Der IGEL Cloud Gateway (ICG) unterstützt alle Funktionen der Universal Management Suite (UMS) außer den folgenden:

- Universal Firmware Update über die WebDav-Funktionalität der UMS; als Alternative kann FTP verwendet werden. Weitere Informationen finden Sie unter Universal Firmware Update.
- Custom Partition über die WebDav-Funktionalität der UMS; als Alternative kann FTP verwendet werden.

Sicheres Spiegeln über ICG wird mit UMS 6.03.100 oder höher und IGEL OS 11.02.100 oder höher unterstützt.

Sicheres Terminal über ICG wird mit UMS 6.04.100 oder höher und IGEL OS 11.02.100 oder höher unterstützt.

Mit ICG Version 2.x oder 12.01.x und UMS Version 6.x oder 12.01.x ist es nicht möglich, den TLS-Verkehr zwischen den Komponenten zu untersuchen. Die Inspektion würde TLS brechen und die Kommunikation zwischen den Produkten unterbrechen.
Ab UMS Version 12.02 können Sie den TLS-Verkehr untersuchen, siehe IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading.

Installation und Einrichtung

Dieser Artikel beschreibt die Installation und Einrichtung des IGEL Cloud Gateway (ICG).

1. Rechner für die Installation des ICG vorbereiten:
   - Using IGEL Cloud Gateway on Azure Marketplace (see page 95)
   - Linux-Rechner für die Installation von IGEL Cloud Gateway (ICG) vorbereiten (see page 96) (Beispiel für einen lokalen Rechner)
2. Bereitstellung der geeigneten Zertifikate; siehe Zertifikatsanforderungen und -empfehlungen für IGEL Cloud Gateway (ICG) (see page 14). Wählen Sie einen der folgenden Abschnitte, je nach Ihren Bedürfnissen und Ihrer Umgebung:
   - Bestehende Zertifikatskette installieren (see page 16)
   - Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (see page 27)
   - Zertifikat mit der UMS erstellen (see page 35)
3. Installation des IGEL Cloud Gateway mit dem ICG Remote Installer; siehe IGEL Cloud Gateway installieren (see page 40). Dies ist der empfohlene Weg; es ist jedoch möglich, das ICG manuell zu installieren; siehe auch ICG ohne Remote Installer installieren (see page 103).

Zertifikate bereitstellen

Zertifikatsanforderungen und -empfehlungen für IGEL Cloud Gateway (ICG)

Für einen erfolgreichen Einsatz des IGEL Cloud Gateway (ICG) muss eine Zertifikatskette für die Kommunikation mit den Geräten bereitgestellt werden. Diese Zertifikatskette muss einige Anforderungen erfüllen. Außerdem sollte die Gültigkeitsdauer des Stammzertifikats so lang wie möglich sein.

Empfehlung: Gültigkeitsdauer des Root-Zertifikats

Der Gültigkeitszeitraum des Root-Zertifikats sollte so lang wie möglich sein. Wenn das Root-Zertifikat abläuft, müssen alle Zertifikate ausgetauscht und alle Geräte neu registriert werden.

Anforderung: BasicConstraint für CA-Zertifikate

Das Root-Zertifikat und jedes Zwischenzertifikat müssen als CA-Zertifikat gemäß der Definition in X509v3-Erweiterungen gekennzeichnet sein: 2.5.29.19. Dies ist der Fall, wenn die BasicConstraint-Erweiterung "is_ca" auf "true" gesetzt ist. Wenn es auf "false" gesetzt ist, kann das Zertifikat nicht zum Signieren anderer Zertifikate verwendet werden.

Anforderung: Wenn ein CA-Zähler vorhanden ist, muss er korrekt gesetzt werden

Einige CA-Zertifikate haben einen CA-Zähler, der in X509v3-Erweiterungen definiert ist: 2.5.29.19. Der CA-Zähler beschreibt, wie viele Mitglieder der Zertifikatskette hinzugefügt werden können. Wenn beispielsweise der CA-Zähler des aktuellen Zertifikats 1 ist, ist es möglich, ein Zertifikat zu signieren, mit dem ein weiteres Zertifikat signiert werden kann. Der CA-Zähler dieses Zertifikats ist 0, so dass er nur Endzertifikate signieren kann.

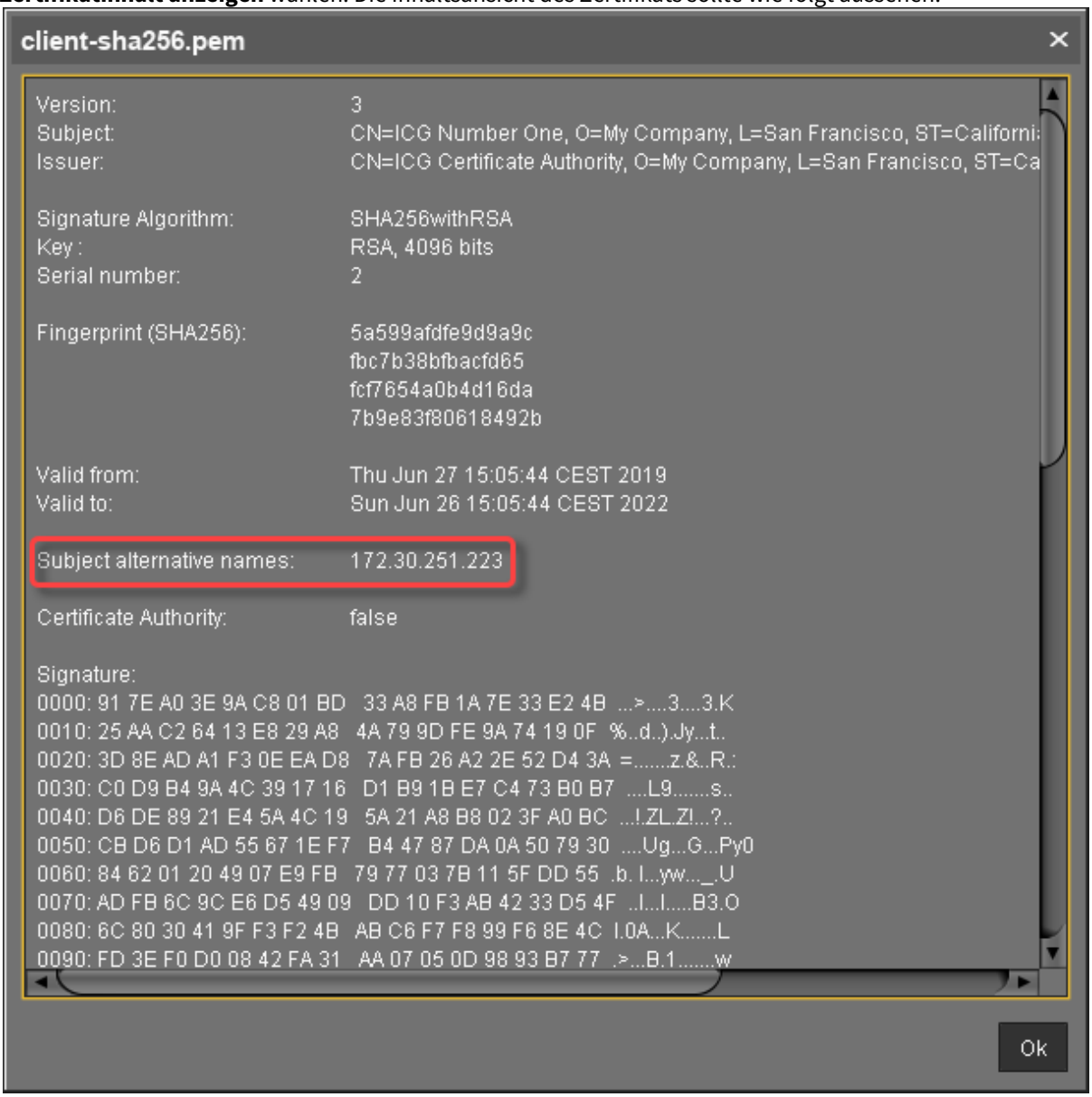
Mit der UMS 6.02 oder höher können Sie den CA-Zähler eines Zertifikats überprüfen, indem Sie das Kontextmenü auswählen und dann **Zertifikatinhalt anzeigen** wählen.

Anforderung: Endzertifikat muss gekennzeichnet sein und einen korrekten Subject Alternative Name haben

Das Zertifikat, das auf dem IGEL Cloud Gateway installiert werden soll, muss als Endzertifikat gekennzeichnet sein.

Das Endzertifikat muss einen Subject Alternative Name (X509v3-Erweiterungen 2.5.29.17) haben, der alle Hostnamen oder IP-Adressen enthält, über die die UMS und die Geräte das IGEL Cloud Gateway kontaktieren. Wildcards werden unterstützt.

Mit der UMS 6.02 oder höher können Sie dies überprüfen, indem Sie das Kontextmenü auswählen und dann **Zertifikatinhalt anzeigen** wählen. Die Inhaltsansicht des Zertifikats sollte wie folgt aussehen:



Bestehende Zertifikatskette installieren

Übersicht

Sie können eine Zertifikatskette verwenden, die bereits in Ihrer Arbeitsumgebung verwendet wird. Die Zertifikatskette muss ein CA-Stammzertifikat und ein Endzertifikat enthalten und kann ein oder mehrere Zwischenzertifikate enthalten.

Um sicherzustellen, dass Ihre Zertifikate von Ihrer IGEL Cloud Gateway-Installation verwendet werden können, lesen Sie bitte Zertifikatsanforderungen und -empfehlungen für IGEL Cloud Gateway (ICG) (see page 14) .

In dem hier beschriebenen Beispiel wird die folgende Zertifikatskette verwendet:

- Stammzertifikat
- Zwischenzertifikat
- Endzertifikat

Wenn die Zertifikatskette vorhanden ist, können Sie mit IGEL Cloud Gateway installieren (see page 40) fortfahren.

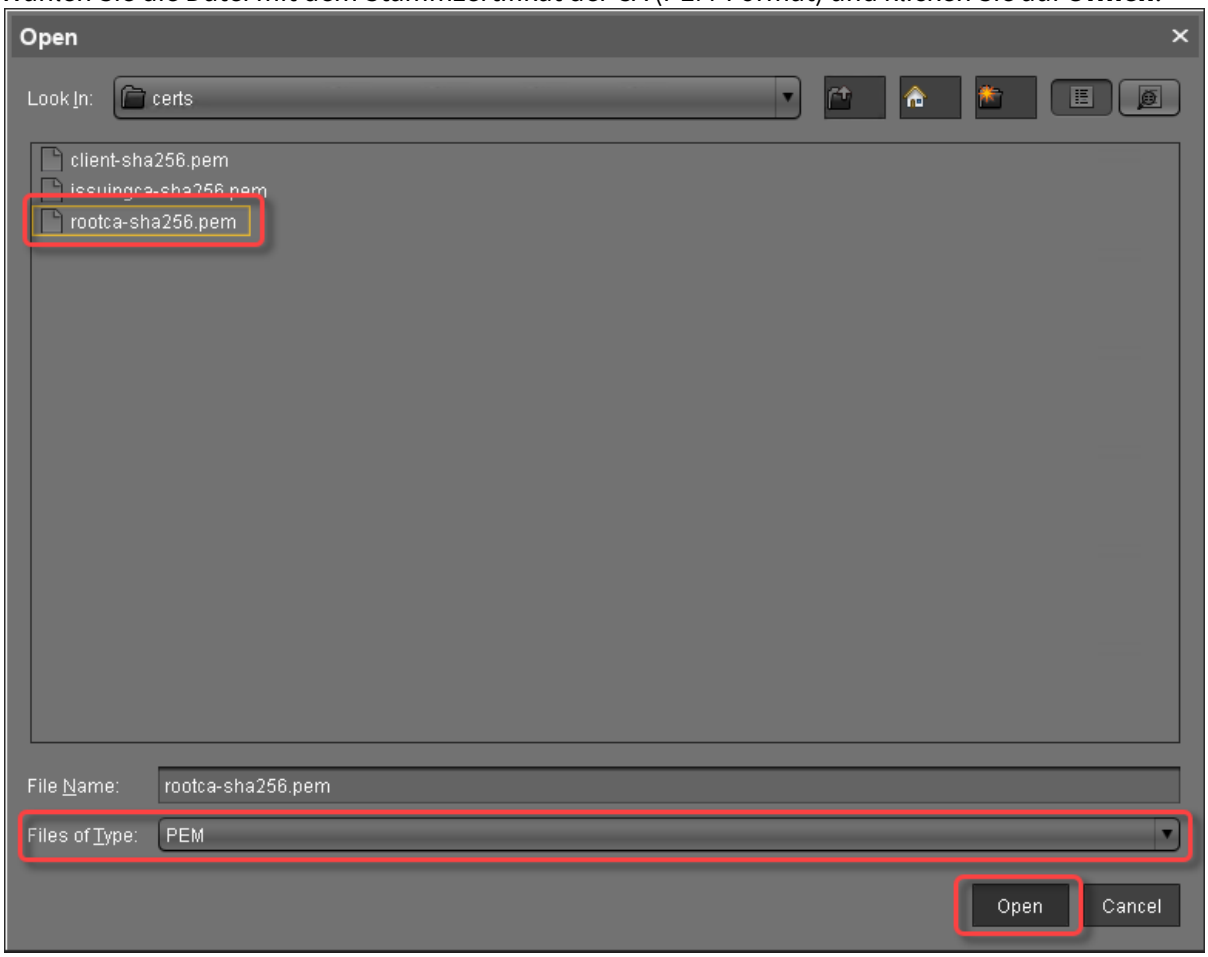
Mit UMS 6.03 oder höher können Sie den ICG Remote Installer zum Installieren von Zertifikaten verwenden. Diese Vorgehensweise wird hier beschrieben. Die Vorgehensweise für UMS 6.02 oder niedriger finden Sie im How-To Bestehende Zertifikatskette installieren (UMS 6.02 oder Älter) (see page 124).

Stammzertifikat importieren

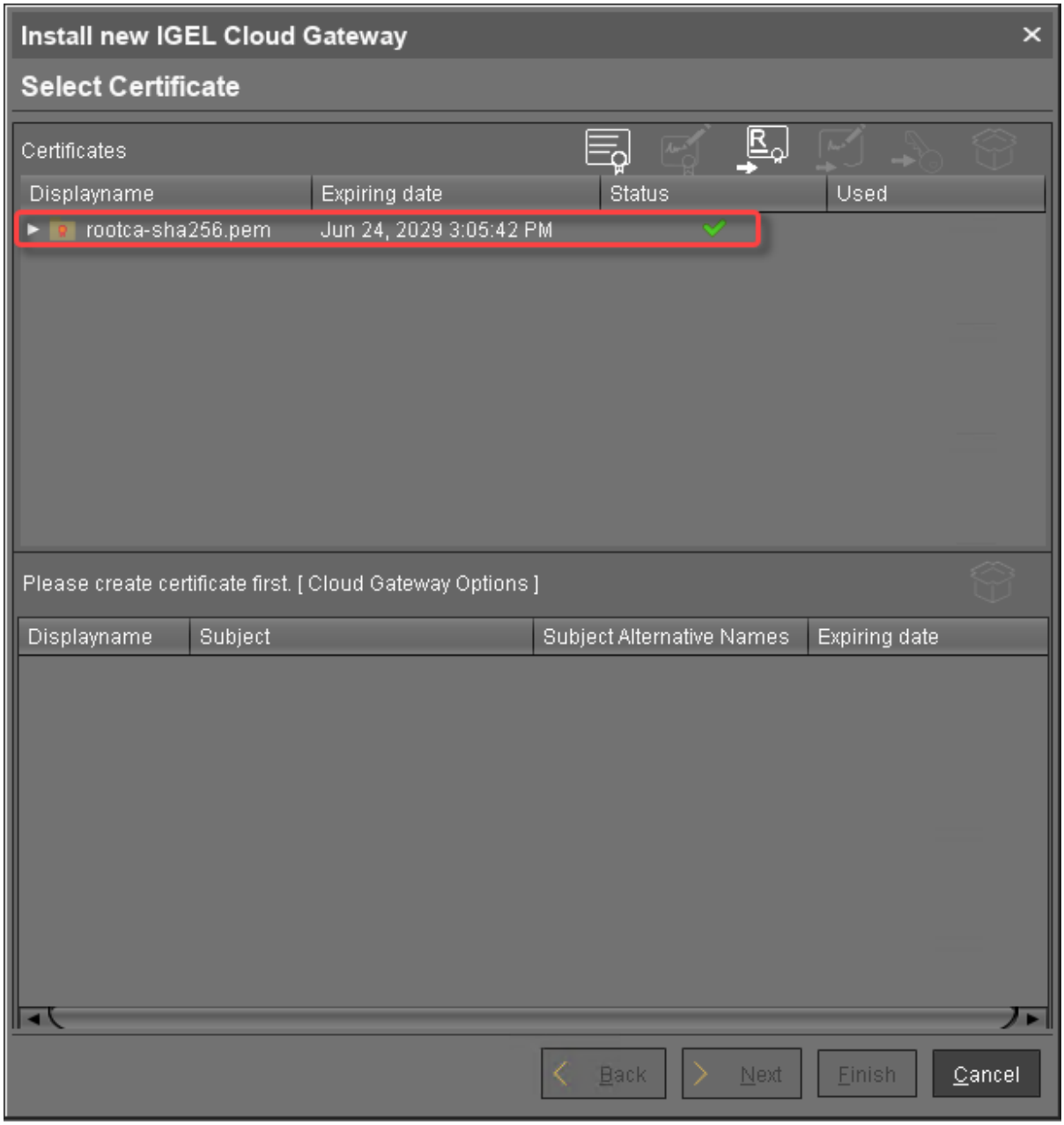
> ⓘ Der Gültigkeitszeitraum des Stammzertifikats sollte so lang wie möglich sein. Nach Ablauf des Stammzertifikats müssen alle Zertifikate ausgetauscht und alle Geräte erneut registriert werden.

1. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.
2. Klicken Sie oben rechts in der Werkzeugleiste auf  (**Neues IGEL Cloud Gateway installieren**).
3. Der ICG Remote Installer öffnet sich. Sämtliche vorhandene ICG-Zertifikate werden im Bereich **Zertifikate** angezeigt.
4. Klicken Sie  , um das Stammzertifikat zu importieren.

5. Wählen Sie die Datei mit dem Stammzertifikat der CA (PEM-Format) und klicken Sie auf **Öffnen**.

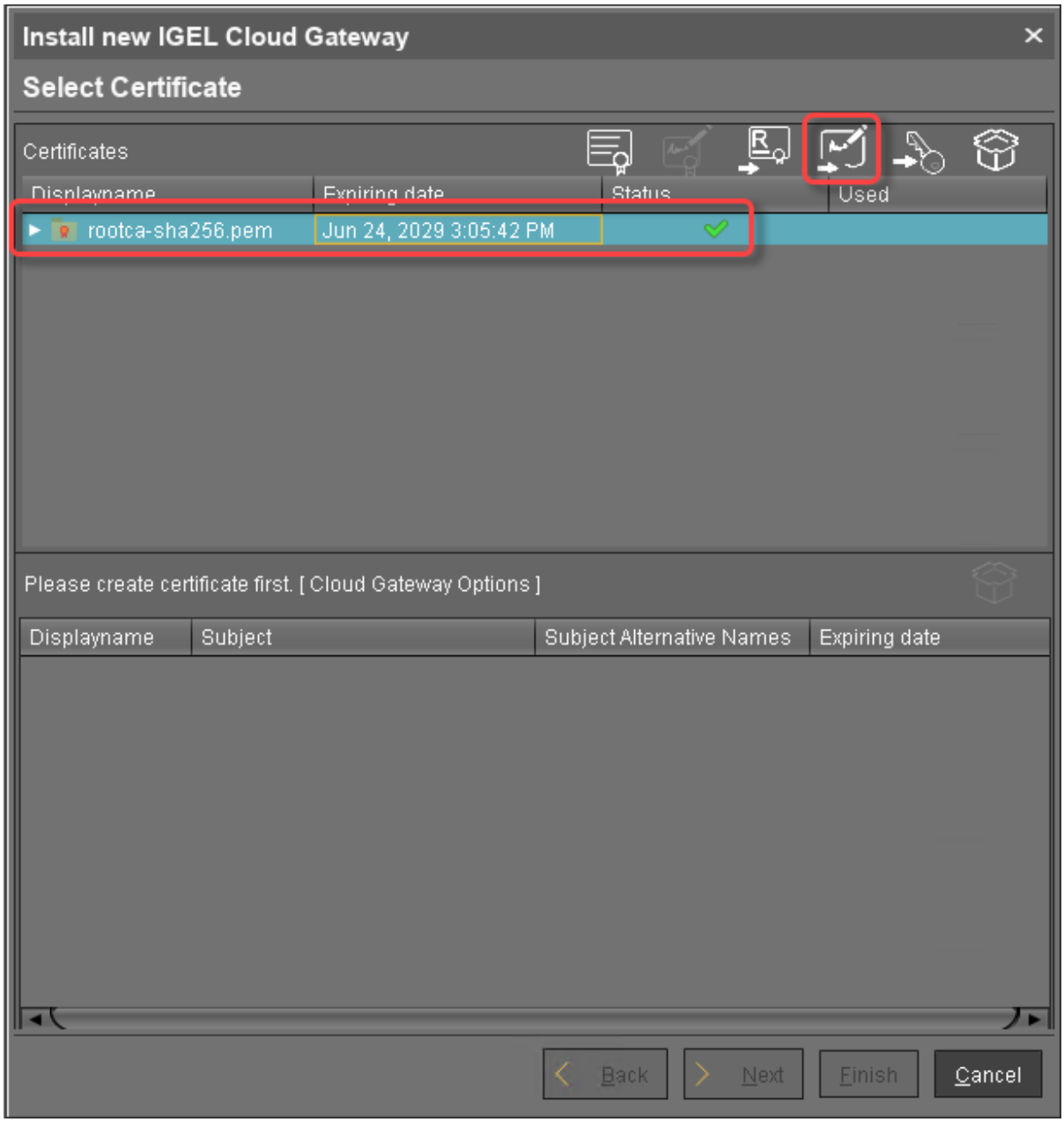


Das Stammzertifikat der CA erscheint in der Liste.

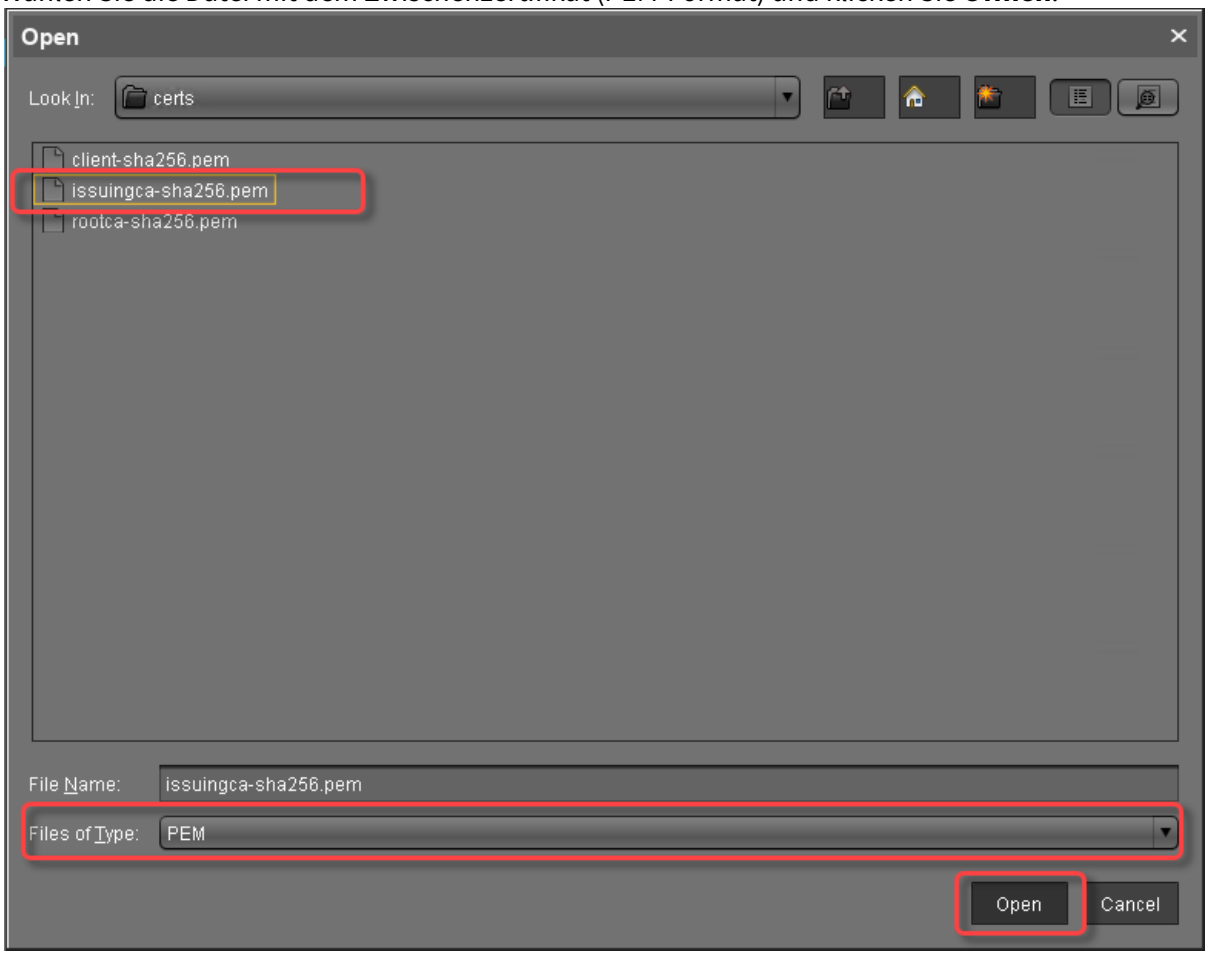


Zwischenzertifikat importieren

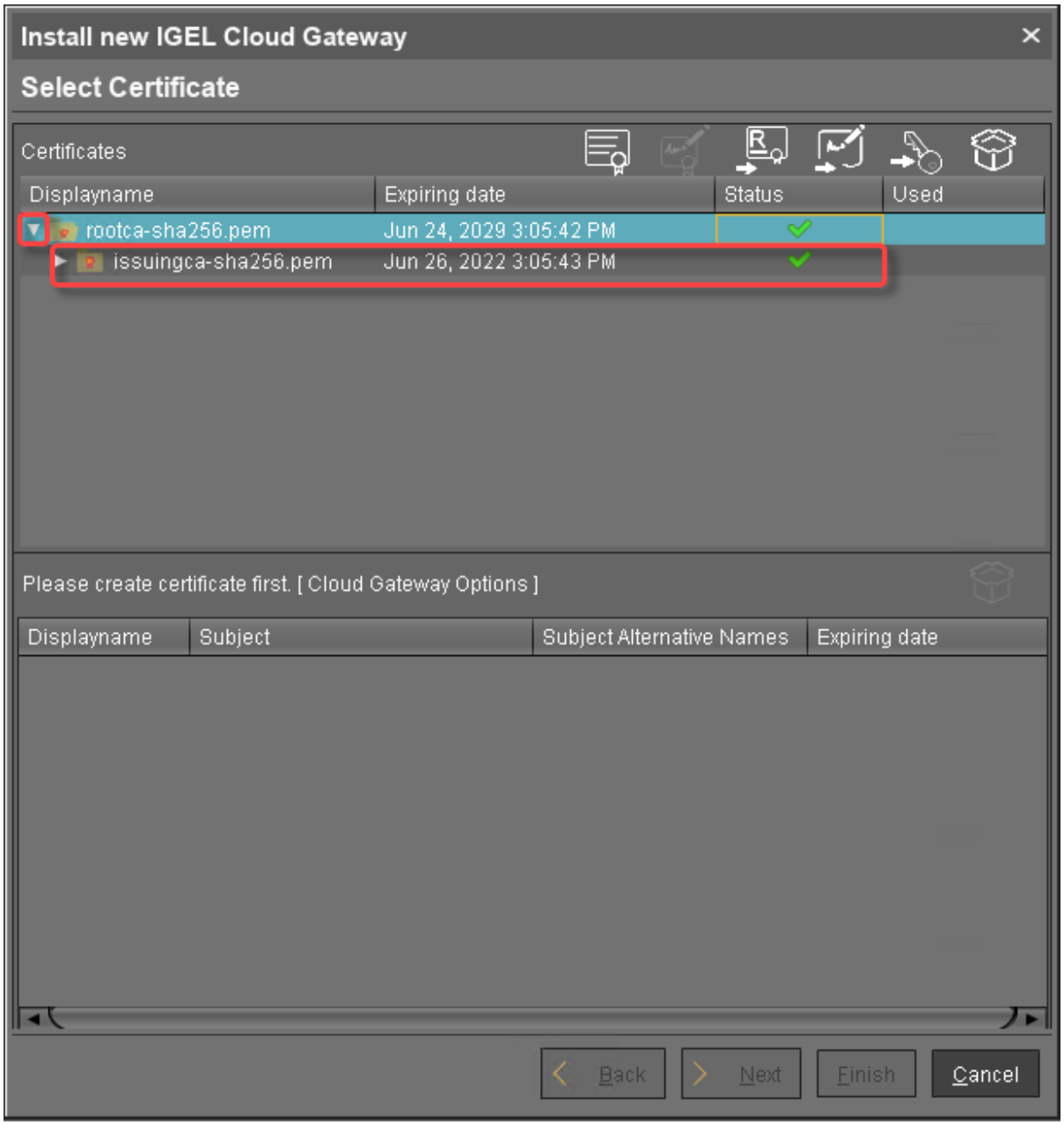
1. Wählen Sie im ICG Remote Installer das CA-Zertifikat und klicken Sie  , um das Zwischenzertifikat. das mit dem CA-Zertifikat signiert ist, zu importieren.


Install new IGEL Cloud Gateway
Select Certificate
Certificates
Displayname
Expiring date
Status
Used
rootca-sha256.pem
Jun 24, 2029 3:05:42 PM
Please create certificate first. [Cloud Gateway Options]
Displayname
Subject
Subject Alternative Names
Expiring date
Back
Next
Finish
Cancel

2. Wählen Sie die Datei mit dem Zwischenzertifikat (PEM-Format) und klicken Sie **Öffnen**.



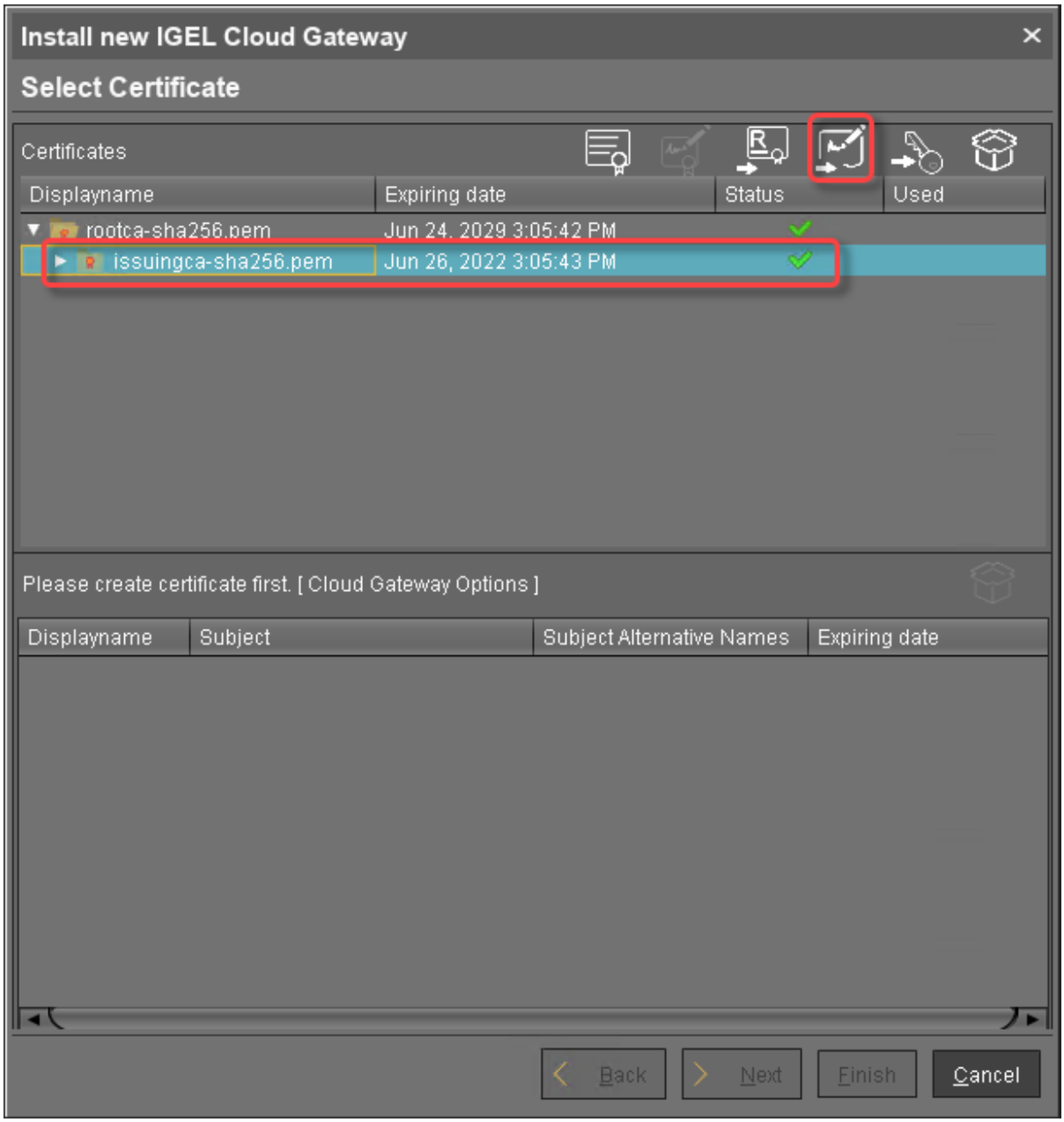
Wenn Sie den Pfeil neben dem Stammzertifikat klicken, erscheint das Zwischenzertifikat auf der Liste.



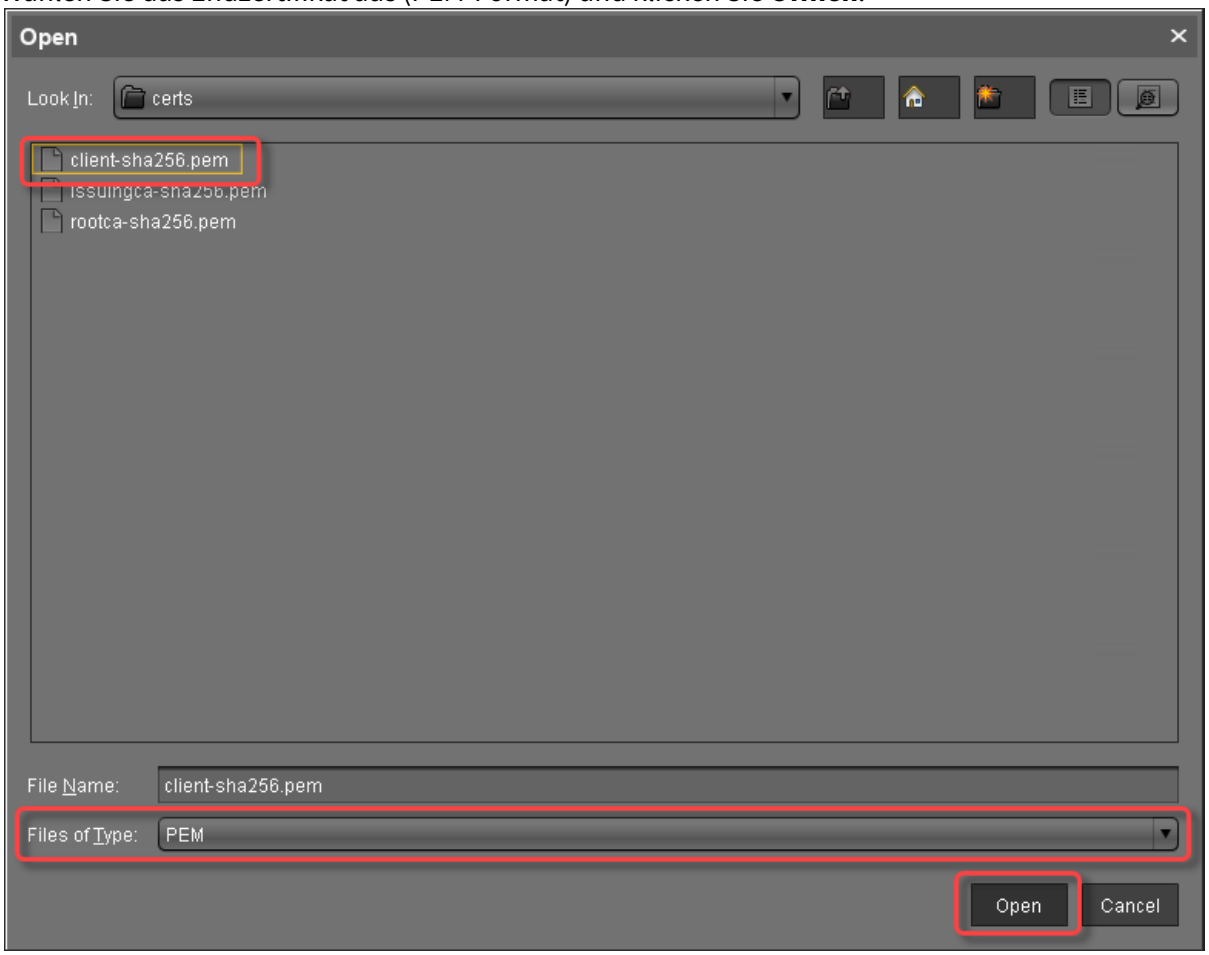
3. Fahren Sie fort, indem Sie das Endzertifikat importieren.

Endzertifikat importieren

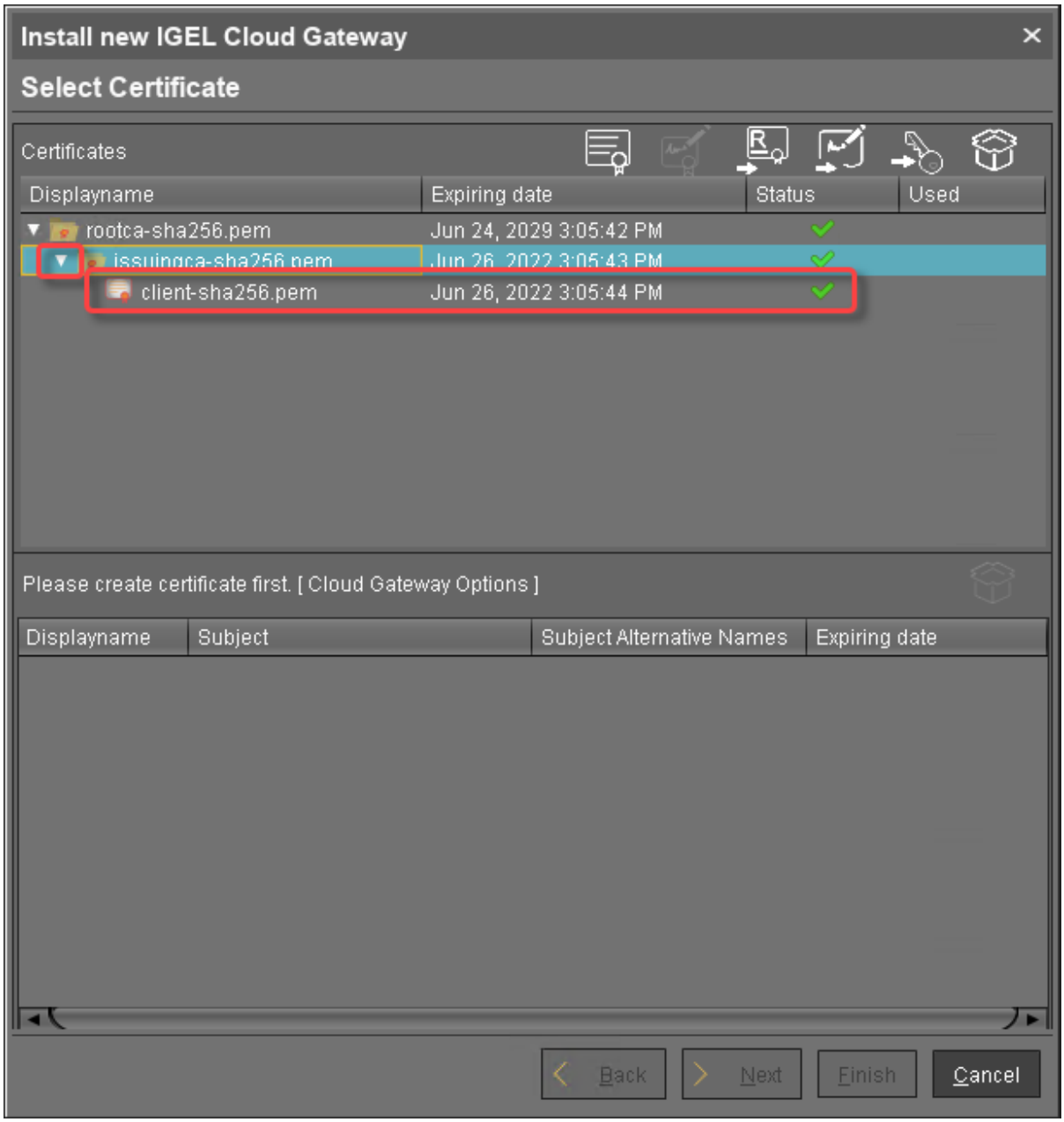
1. Wählen Sie im ICG Remote Installer das CA-Zertifikat und klicken Sie  , um das Zwischenzertifikat. das mit dem CA-Zertifikat signiert ist, zu importieren.


Install new IGEL Cloud Gateway
Select Certificate
Certificates
Displayname
Expiring date
Status
Used
rootca-sha256.pem
Jun 24, 2029 3:05:42 PM
issuingca-sha256.pem
Jun 26, 2022 3:05:43 PM
Please create certificate first. [Cloud Gateway Options]
Displayname
Subject
Subject Alternative Names
Expiring date
Back
Next
Finish
Cancel

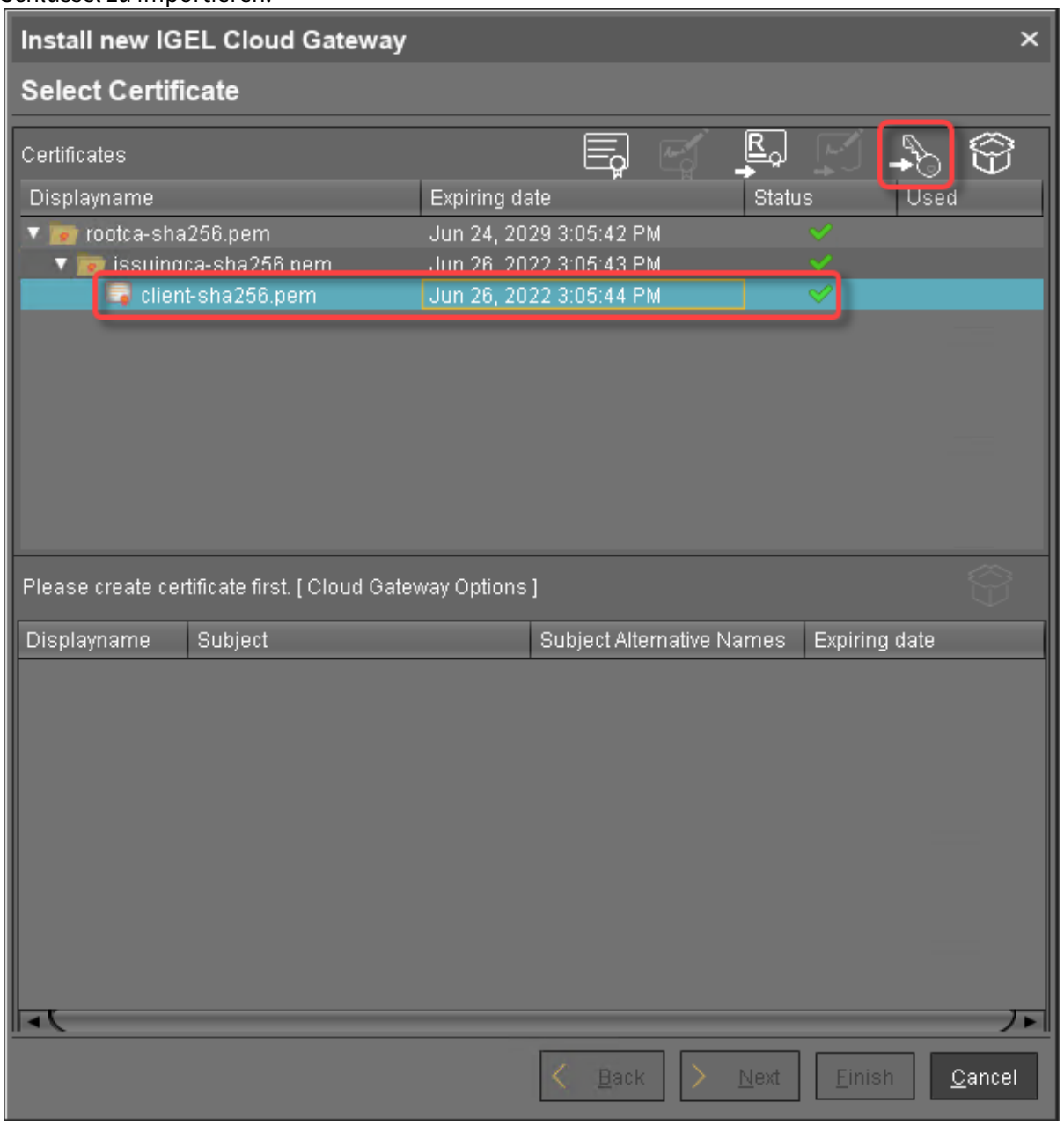
2. Wählen Sie das Endzertifikat aus (PEM-Format) und klicken Sie **Öffnen**.



3. Klicken Sie das Pfeilsymbol des Zwischenzertifikats, das dem Endzertifikat am nächsten steht, um das Endzertifikat sichtbar zu machen.

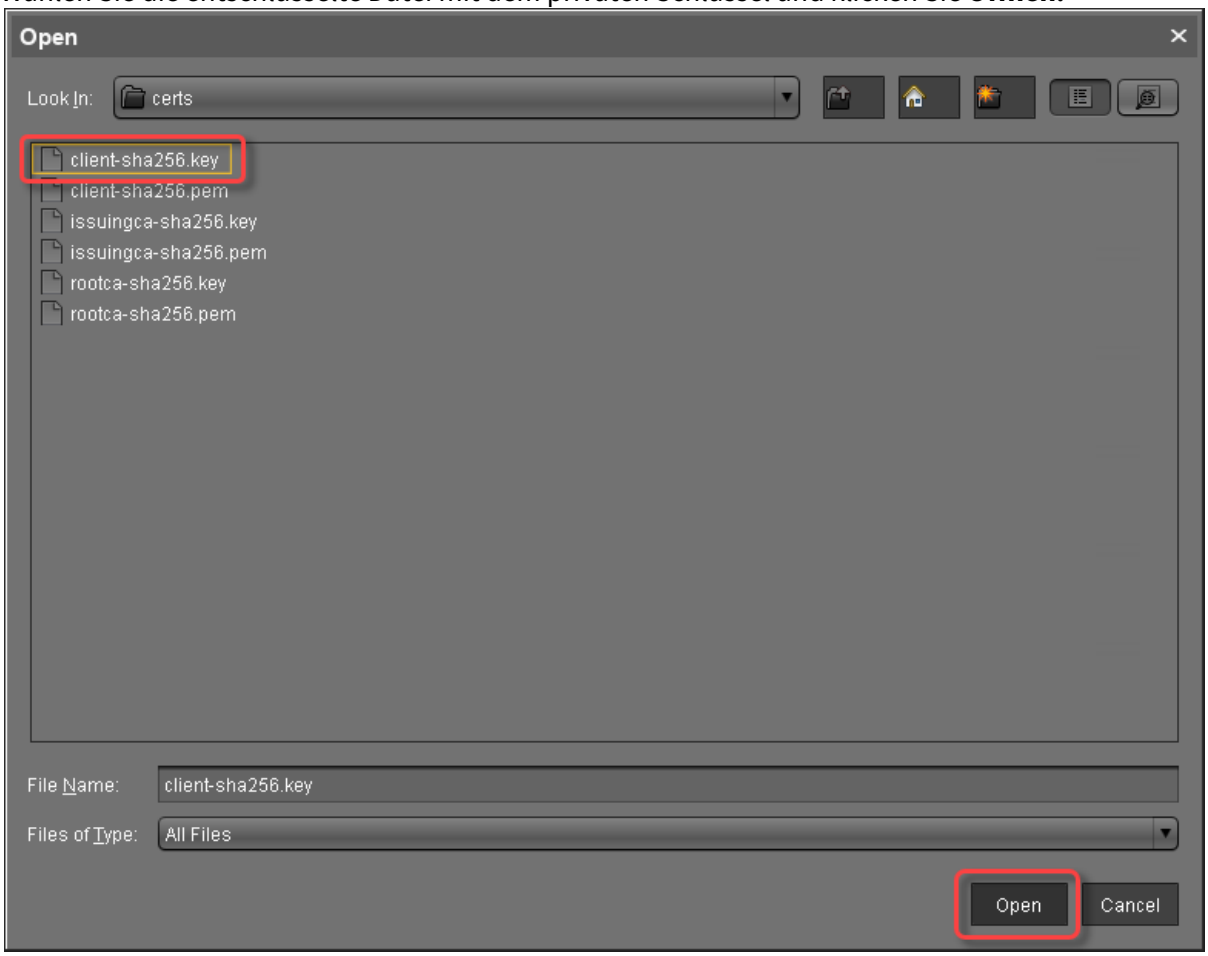

Install new IGEL Cloud Gateway
Select Certificate
Certificates
Displayname
Expiring date
Status
Used
rootca-sha256.pem
Jun 24, 2029 3:05:42 PM
issuingca-sha256.pem
Jun 26, 2022 3:05:43 PM
client-sha256.pem
Jun 26, 2022 3:05:44 PM
Please create certificate first. [Cloud Gateway Options]
Displayname
Subject
Subject Alternative Names
Expiring date
Back
Next
Finish
Cancel

4. Wählen Sie das Endzertifikat aus und klicken Sie  , um den entschlüsselten privaten Schlüssel zu importieren.

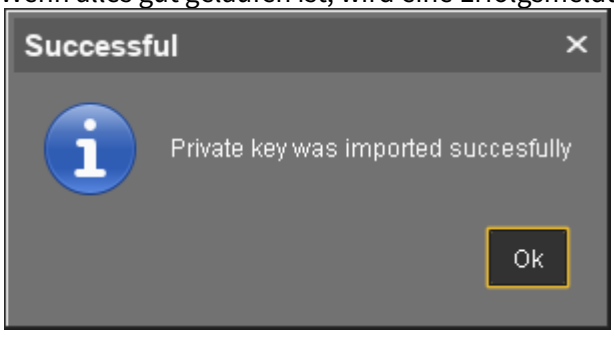


> Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn mit dem OpenSSL-Kommandozeilentool entschlüsseln: `openssl rsa -in encrypted.key -out decrypted.key`

5. Wählen Sie die entschlüsselte Datei mit dem privaten Schlüssel und klicken Sie **Öffnen.**



Wenn alles gut gelaufen ist, wird eine Erfolgsmeldung angezeigt.



6. Fahren sie fort mit IGEL Cloud Gateway installieren (see page 40).

Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen

Erforderliche Zertifikatsdateien

Die folgenden Dateien sind erforderlich:

- CA-Zertifikat
- Privater Schlüssel der CA

> Wenn Sie das Stammzertifikat und den Schlüssel der CA-Signatur von einem Microsoft CA-Server exportieren müssen, können Sie diesem Dokument von Cisco folgen: How do I export and convert a pfx CA root certificate and key from a Microsoft CA server[1]

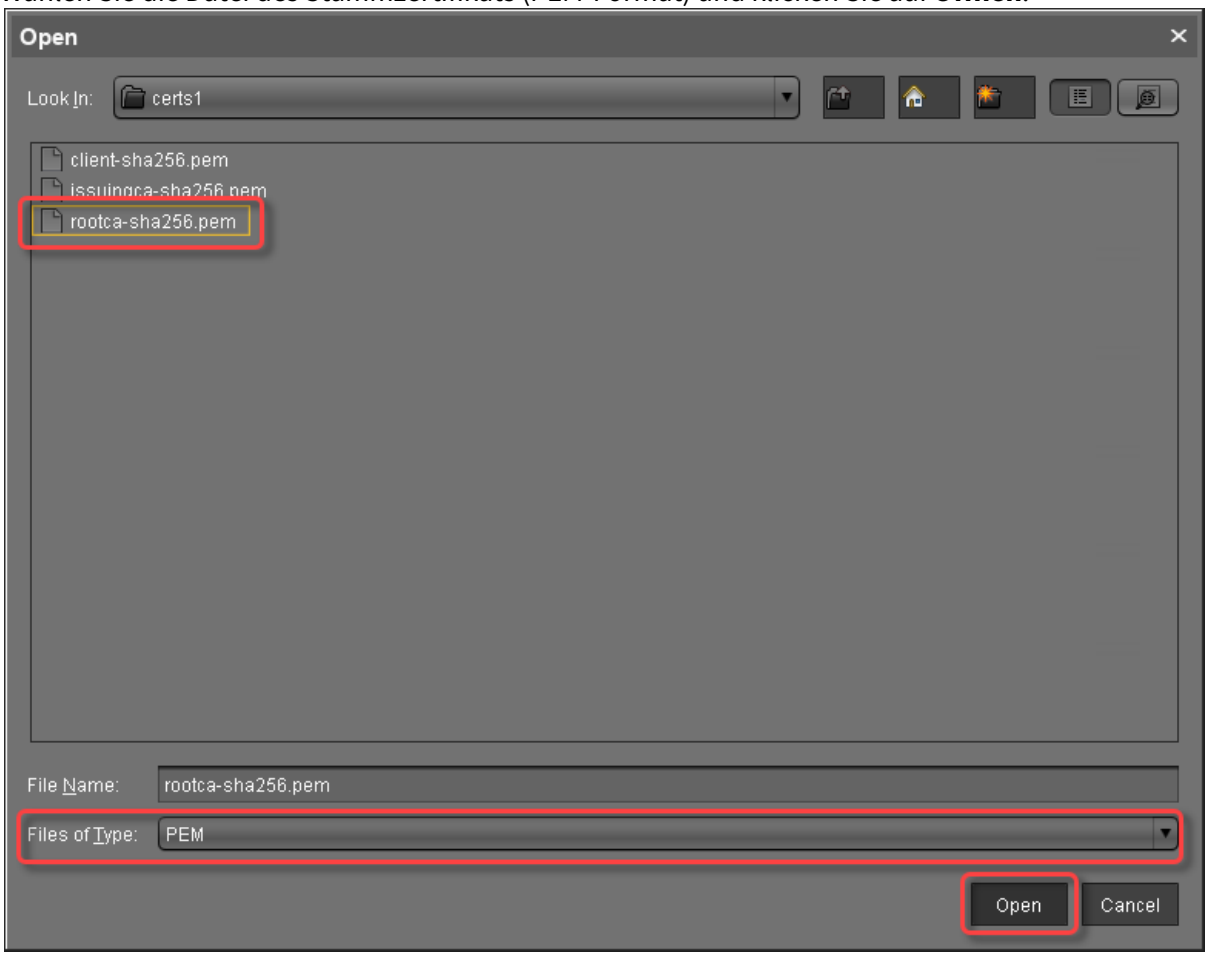
Mit UMS 6.03 oder höher können Sie den ICG Remote Installer verwenden, um Zertifikate zu installieren und zu erstellen. Diese Vorgehensweise ist hier beschrieben. Die Vorgehensweise für UMS 6.02 und niedriger finden Sie im How-To Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (UMS 6.02 oder älter) (see page 131).

Ihre vorhandenen privaten CA-Dateien in die UMS importieren

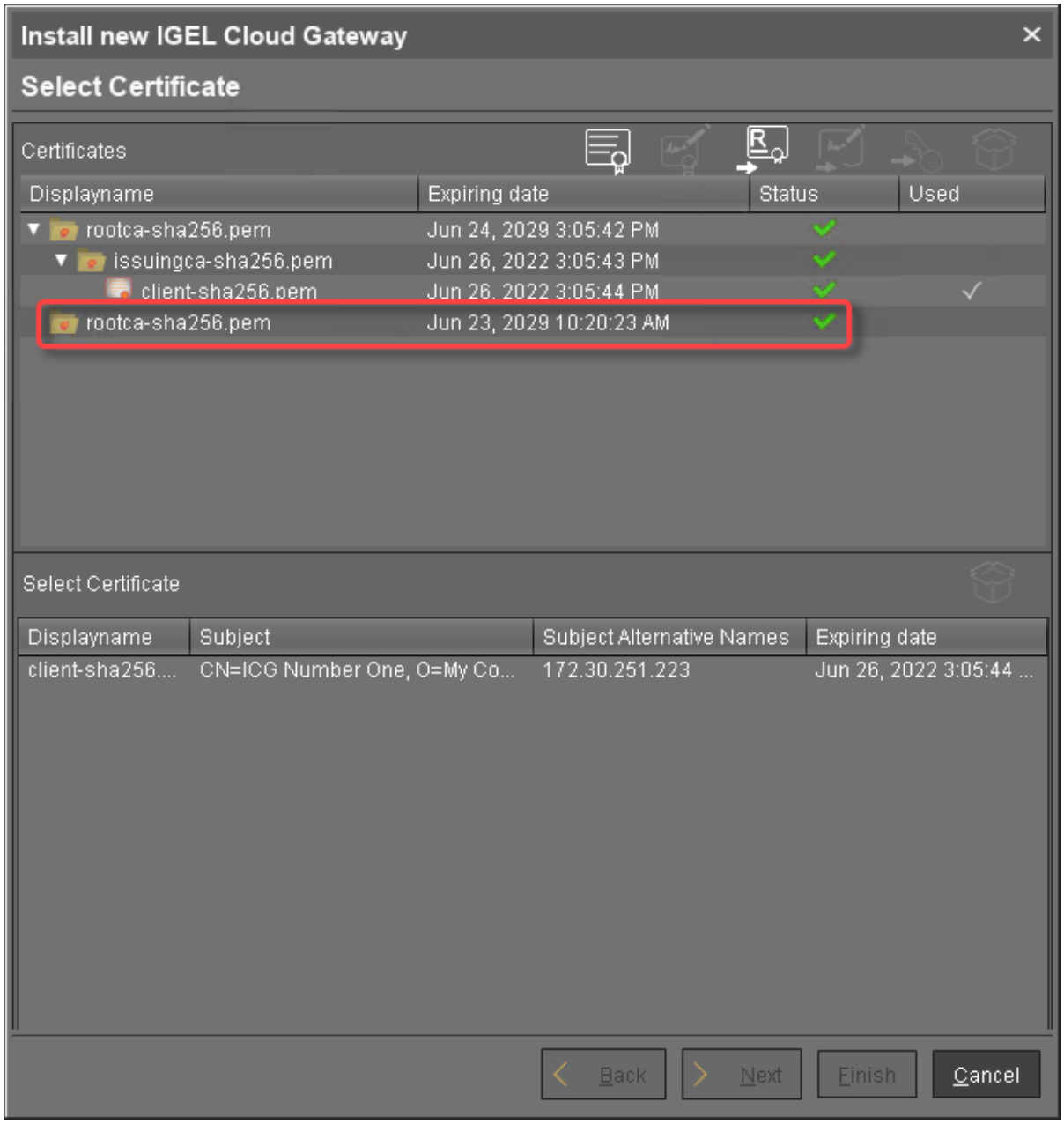
1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration.**
2. Klicken Sie oben rechts in der Werkzeugleiste auf  (**Neues IGEL Cloud Gatewas installieren**).
3. Der ICG Remote Installer öffnet sich. Sämtliche vorhandenen ICG-Zertifikate werden im Bereich **Zertifikate** angezeigt.
4. Klicken Sie im **Zertifikate** Bereich auf  , um das Stammzertifikat zu importieren.

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

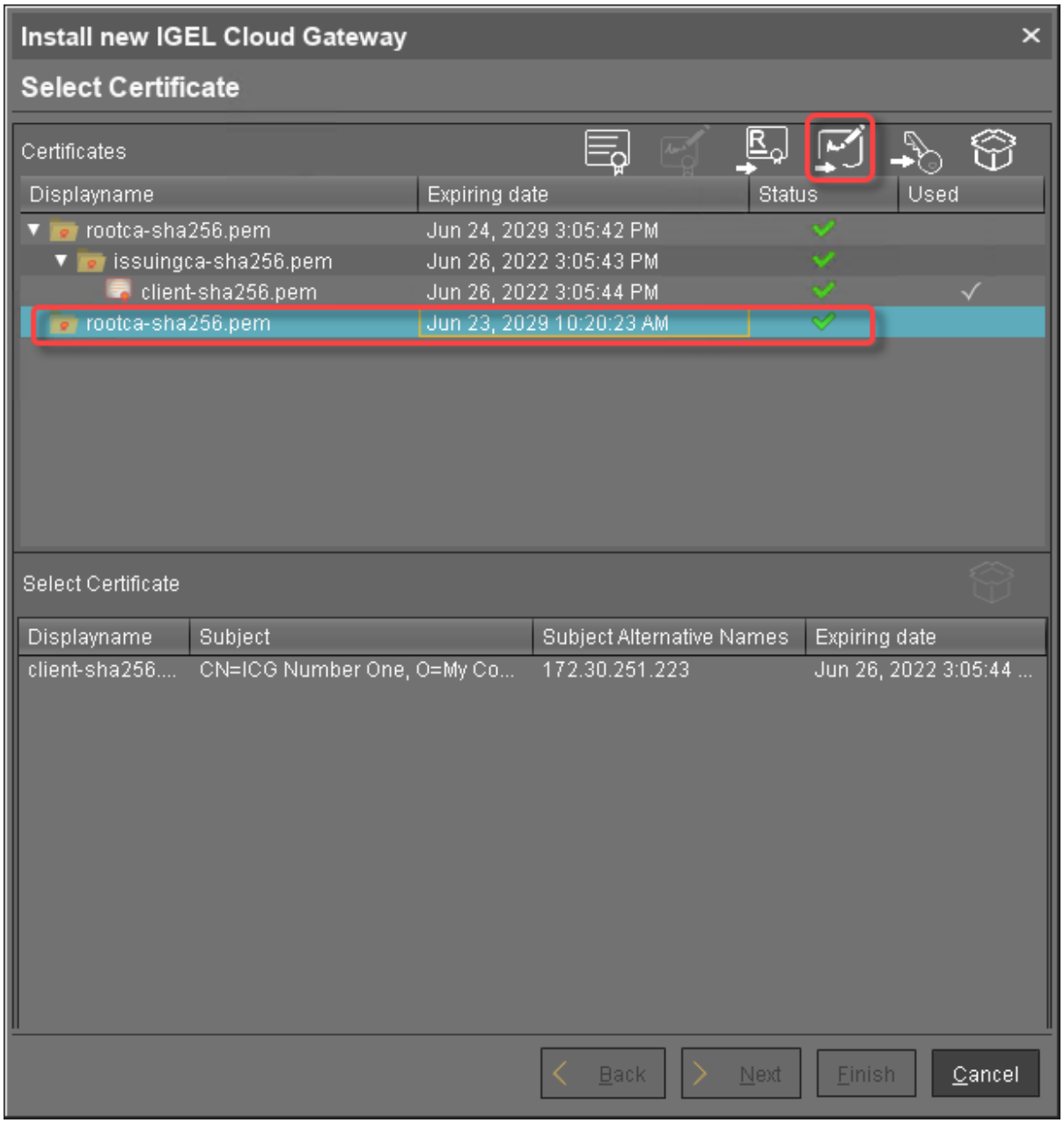
5. Wählen Sie die Datei des Stammzertifikats (PEM-Format) und klicken Sie auf **Öffnen**.



Das Stammzertifikat der CA erscheint in der Liste.

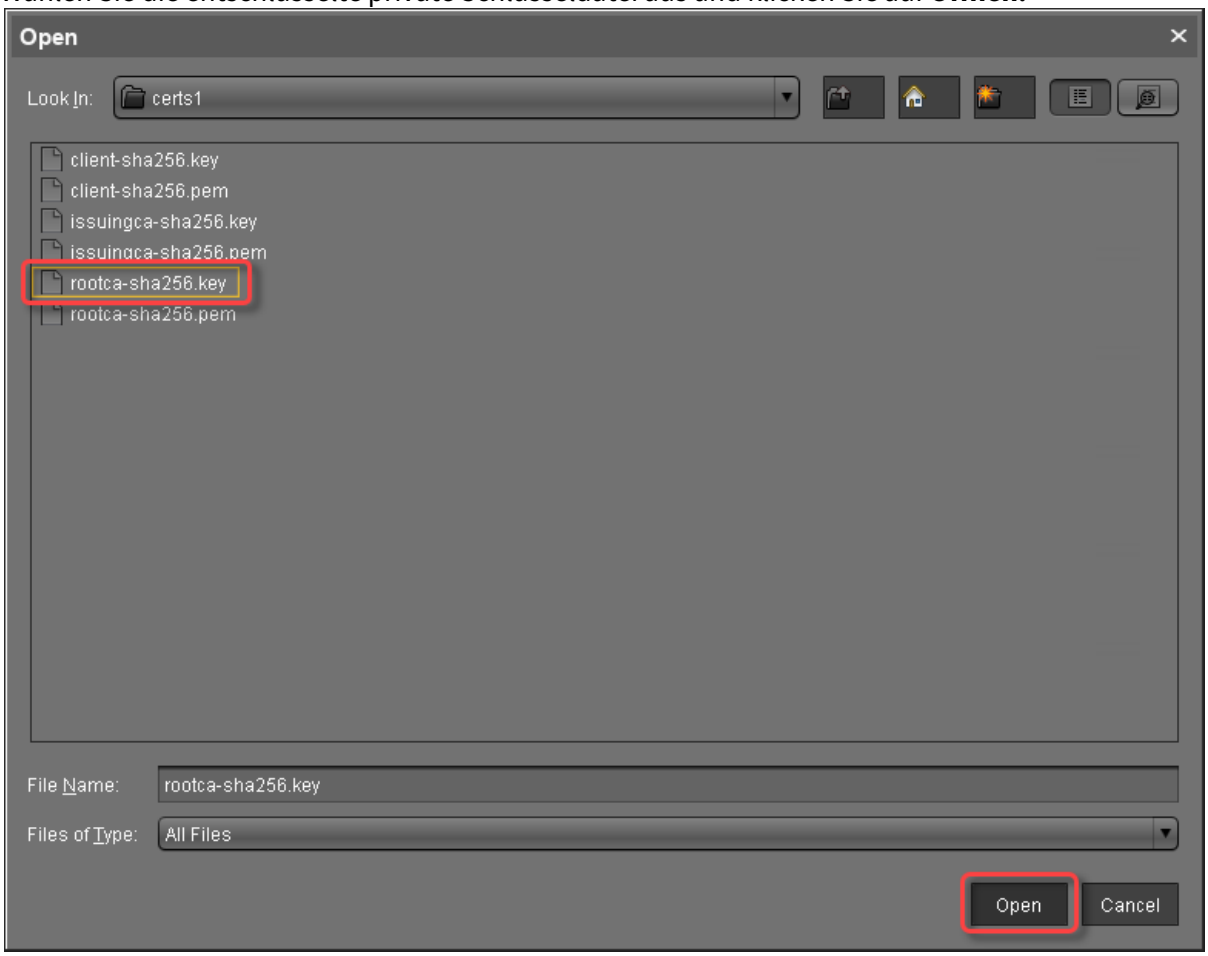


6. Wählen Sie das CA-Zertifikat und klicken Sie  , um den entschlüsselten privaten Schlüssel für das CA-Zertifikat zu importieren.

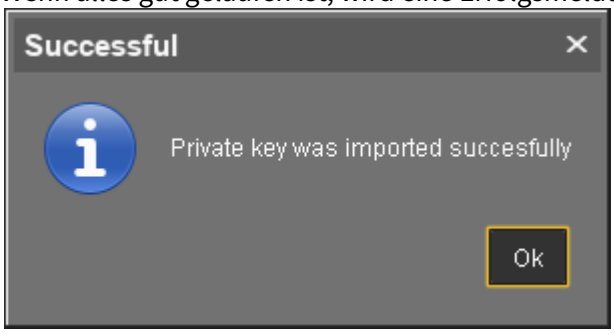


Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn mit dem OpenSSL-Kommandozeilentool entschlüsseln: `openssl rsa -in encrypted.key -out decrypted.key`

7. Wählen Sie die entschlüsselte private Schlüsseldatei aus und klicken Sie auf **Öffnen.**



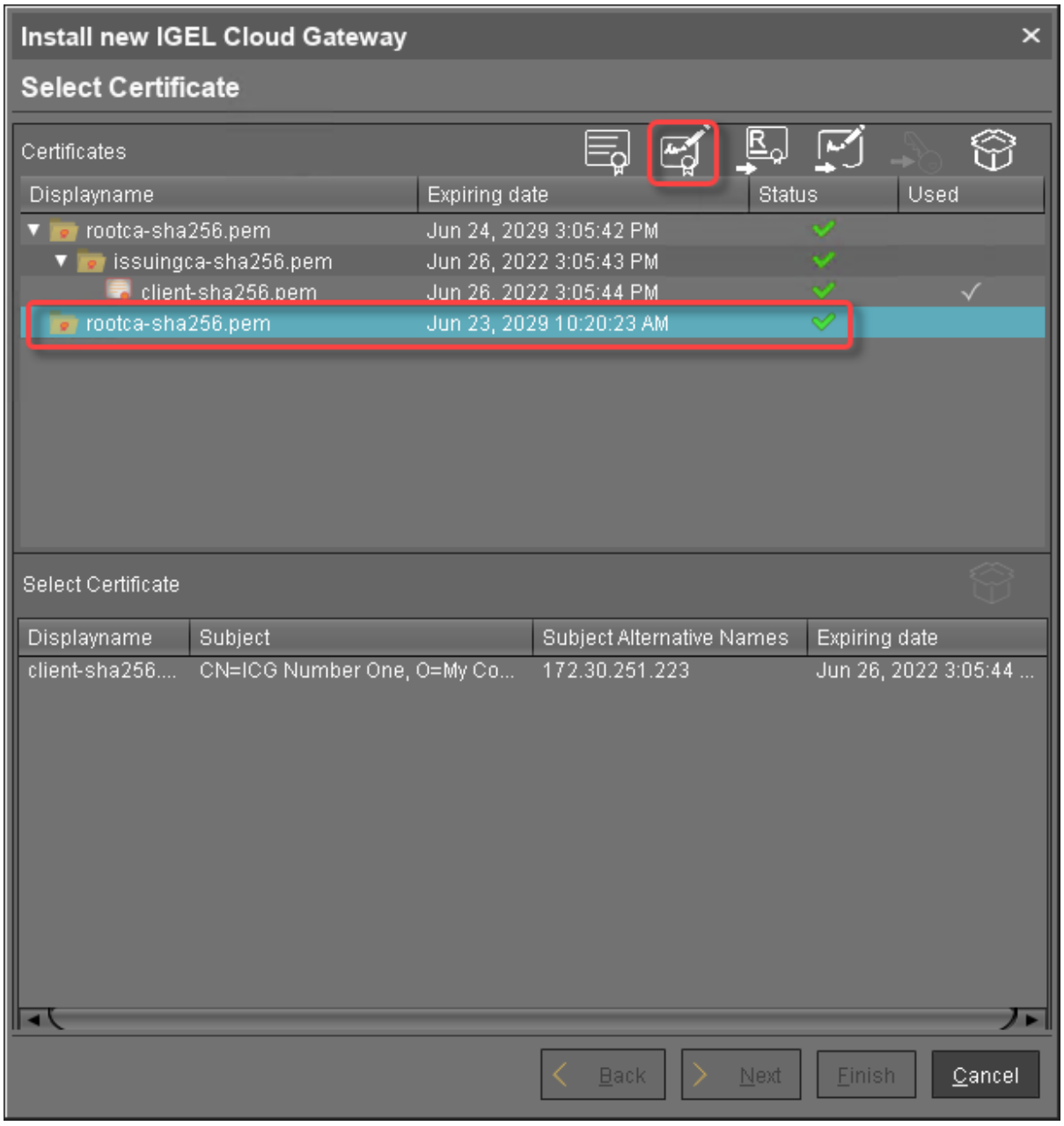
Wenn alles gut gelaufen ist, wird eine Erfolgsmeldung angezeigt.



8. Fahren Sie fort, indem Sie ein signiertes Zertifikat erstellen.

Signiertes Zertifikat erstellen

1. Wählen Sie das Stammzertifikat der CA und klicken Sie  , um ein signiertes Zertifikat zu erstellen.



2. Füllen Sie die Zertifikatsfelder aus:
   - **Name:** Name des Zertifikats
   - **Ihr Vor- und Nachname:** Name des Zertifkatsinhabers
   - **Ihre Organisation:** Organisation oder Firmenname
   - **Ihre Stadt oder Gemeinde:** Standort
   - **Ihr Ländercode (zwei Buchstaben):** ISO 3166 Ländercode, z. B. `US`, `UK` oder `ES`

- **Hostname und/oder IP des Zielservers für das Zertifikat:** Hostname(n) oder IP-Adresse(n), für die das Zertifikat gültig ist. Mehrere Eingaben sind erlaubt, getrennt durch Semikolon.

  > Alle IP-Adressen und Hostnamen, unter denen der ICG von innerhalb des Firmennetzwerks oder von außerhalb erreichbar ist, müssen hier angegeben werden.

- **Gültig bis:** Lokales Datum, an dem dieses Zertifikat abläuft. (Standard: ein Jahr ab jetzt)
- **Zertifikats-Typ:** Wählen Sie "End Entity".

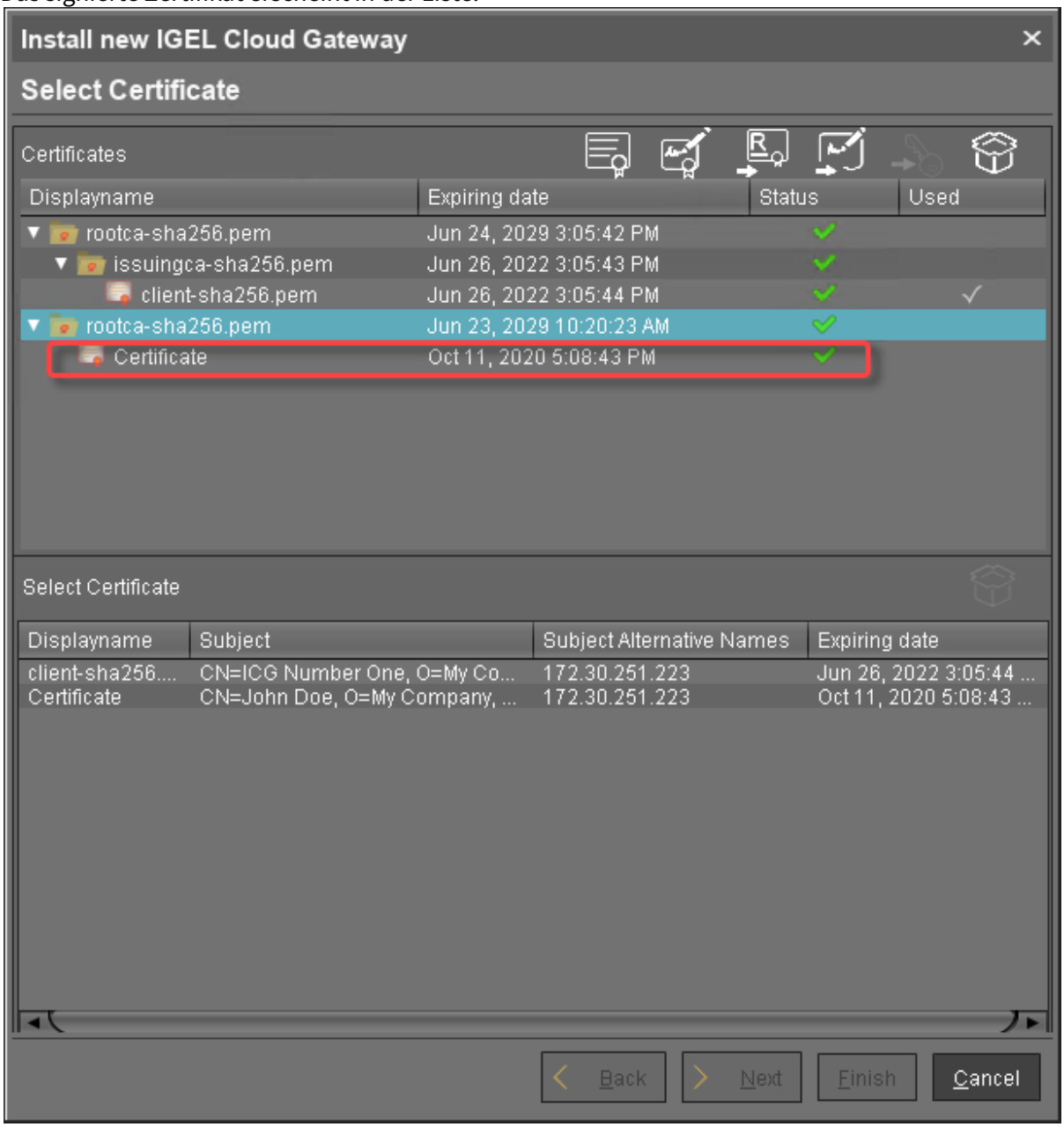
3. Klicken Sie **OK.**

Es wird ein Schlüsselpaar und ein Zertifikat erzeugt.

> Die Generierung von Schlüsseln kann bei virtuellen Maschinen (VMs) viel Zeit in Anspruch nehmen, da diese keine leistungsstarke (Pseudo-)Zufallszahlensquelle haben. Auf Linux-VMs kann dies durch die Installation des haveged[2] Pakets verbessert werden.

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

Das signierte Zertifikat erscheint in der Liste.



4. Fahren Sie fort mit IGEL Cloud Gateway installieren (see page 40).

Zertifikat mit der UMS erstellen

Für die Installation des IGEL Cloud Gateway (ICG) müssen Sie ein signiertes Zertifikat vorlegen. Um ein signiertes Zertifikat zu erzeugen, muss zunächst ein Root-Zertifikat generiert werden.

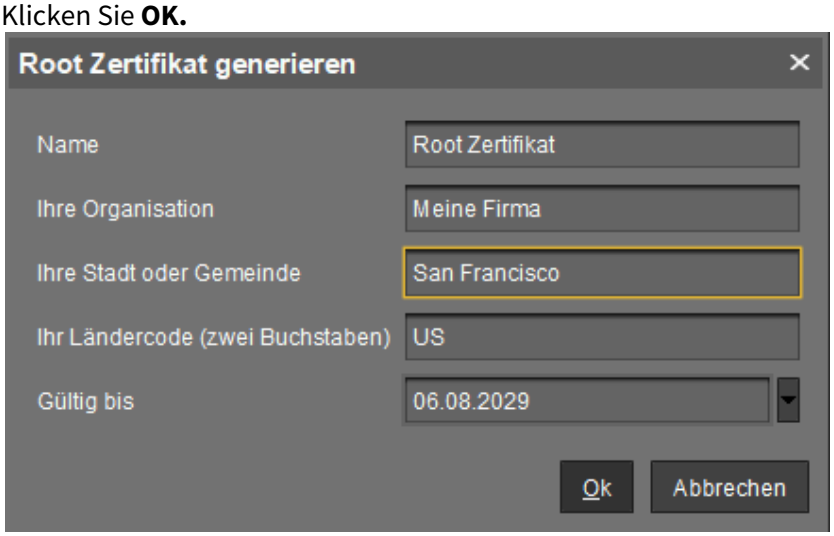
Mit UMS 6.03 oder höher können Sie den ICG Remote Installer verwenden, um Zertifikate zu erstellen. Diese Vorgehensweise wird hier beschrieben. Die Vorgehensweise mit UMS 6.02 oder niedriger finden Sie im How-To Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (UMS 6.02 oder älter) (see page 131).

Stammzertifikat erstellen

1. Gehen Sie in der UMS Konsole zu **UMS Administration > UMS Network > Cloud Gateway Konfiguration.**
2. Klicken Sie oben rechts in der Werkzeugleiste auf  (**Neues IGEL Cloud Gatewas installieren**).
3. Der ICG Remote Installer öffnet sich. Sämtliche vorhandenen ICG-Zertifikate werden im Bereich **Zertifikate** angezeigt.
4. Klicken Sie  , um das Stammzertifikat zu erstellen.
5. Füllen Sie die Zertifikatsfelder aus:
   - **Name:** Name für das Zertifikat; Freitext-Eingabe
   - **Ihre Organisation:** Organisation oder Firmenname
   - **Ihre Stadt oder Gemeinde:** Standort
   - **Ihr Ländercode (zwei Buchstaben):** ISO 3166 Ländercode, z. B. `US`, `UK` oder `ES`
   - **Gültig bis**: Lokales Datum, an dem das Zertifikat abläuft. (Standard: 10 Jahre ab jetzt)

   > Stellen Sie sicher, dass Sie eine lange Laufzeit für das Stammzertifikat definieren; 10 Jahre oder mehr werden dringend empfohlen. Nach Ablauf des Stammzertifikats müssen alle mit dem ICG verbundenen Geräte erneut registriert werden.

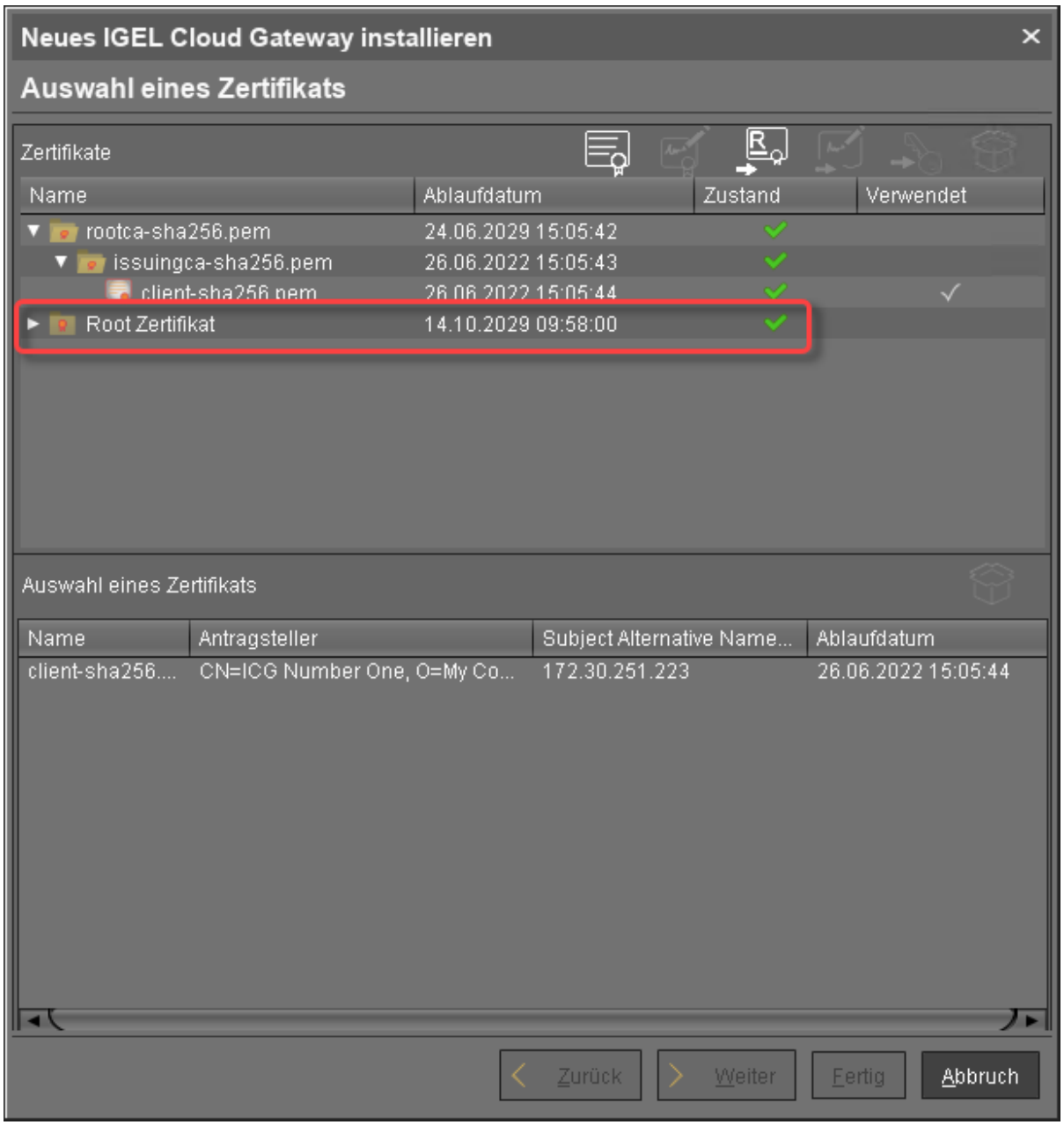
6. Klicken Sie **OK.**



Ein Schlüsselpaar und ein Zertifikat werden erzeugt.

> Die Generierung von Schlüsseln kann bei virtuellen Maschinen (VMs) viel Zeit in Anspruch nehmen, da diese keine leistungsstarke (Pseudo-) Zufallszahlensquelle haben. Auf Linux-VMs kann dies durch die Installation des haveged[3]-Pakets verbessert werden.

Das Stammzertifikat der CA erscheint in der Liste.



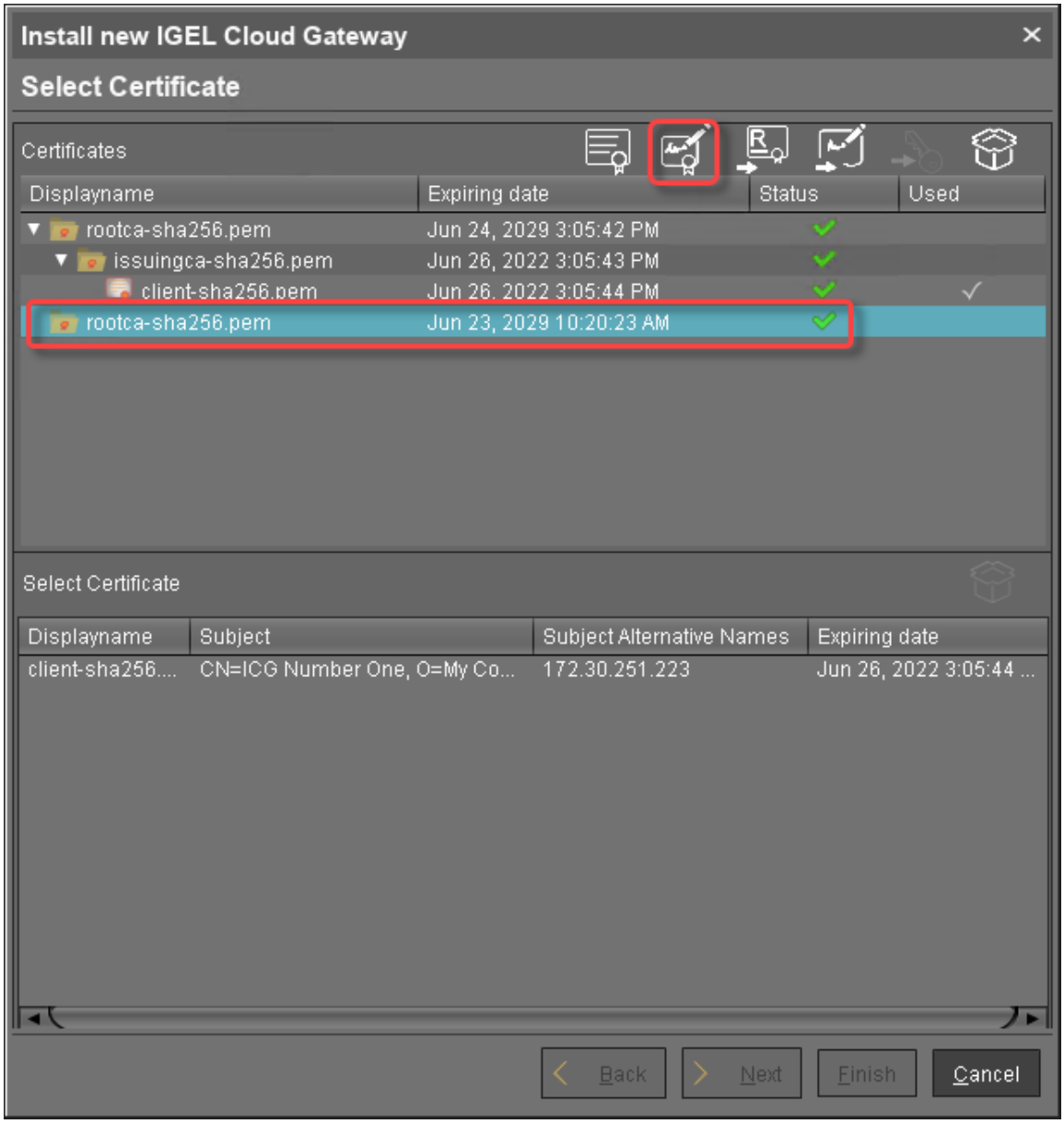
Die CA ist nun einsatzbereit.

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

Signiertes Zertifikat erstellen

Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen

1. Wählen Sie das Stammzertifikat der CA und klicken Sie  , um ein signiertes Zertifikat zu erstellen.



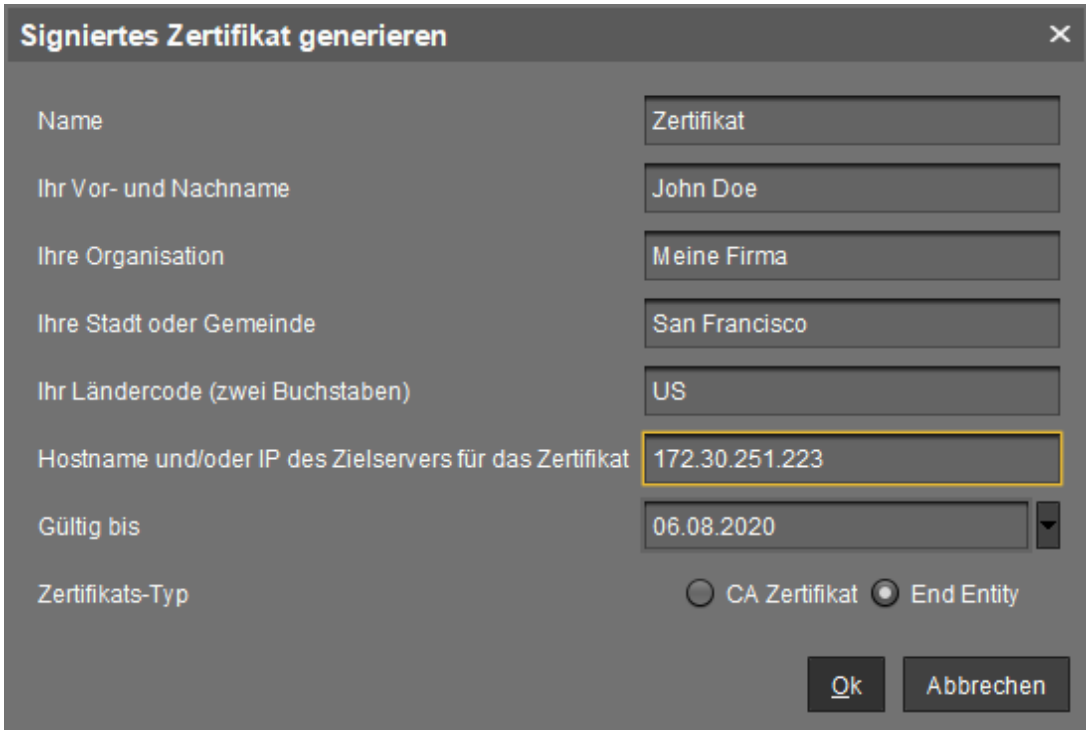
2. Füllen Sie die Zertifikatsfelder aus:

- **Name:** Name des Zertifikats
- **Ihr Vor- und Nachname:** Name des Zertifkatsinhabers
- **Ihre Organisation:** Organisation oder Firmenname
- **Ihre Stadt oder Gemeinde:** Standort
- **Ihr Ländercode (zwei Buchstaben):** ISO 3166 Ländercode, z. B. `US`, `UK` oder `ES`
- **Hostname und/oder IP des Zielservers für das Zertifikat:** Hostname(n) oder IP-Adresse(n), für die das Zertifikat gültig ist. Mehrere Eingaben sind erlaubt, getrennt durch Semikolon.

  > Alle IP-Adressen und Hostnamen, unter denen der ICG von innerhalb des Firmennetzwerks oder von außerhalb erreichbar ist, müssen hier angegeben werden.

- **Gültig bis:** Lokales Datum, an dem dieses Zertifikat abläuft. (Standard: ein Jahr ab jetzt)
- **Zertifikats-Typ:** Wählen Sie "End Entity".

3. Klicken Sie **OK.**

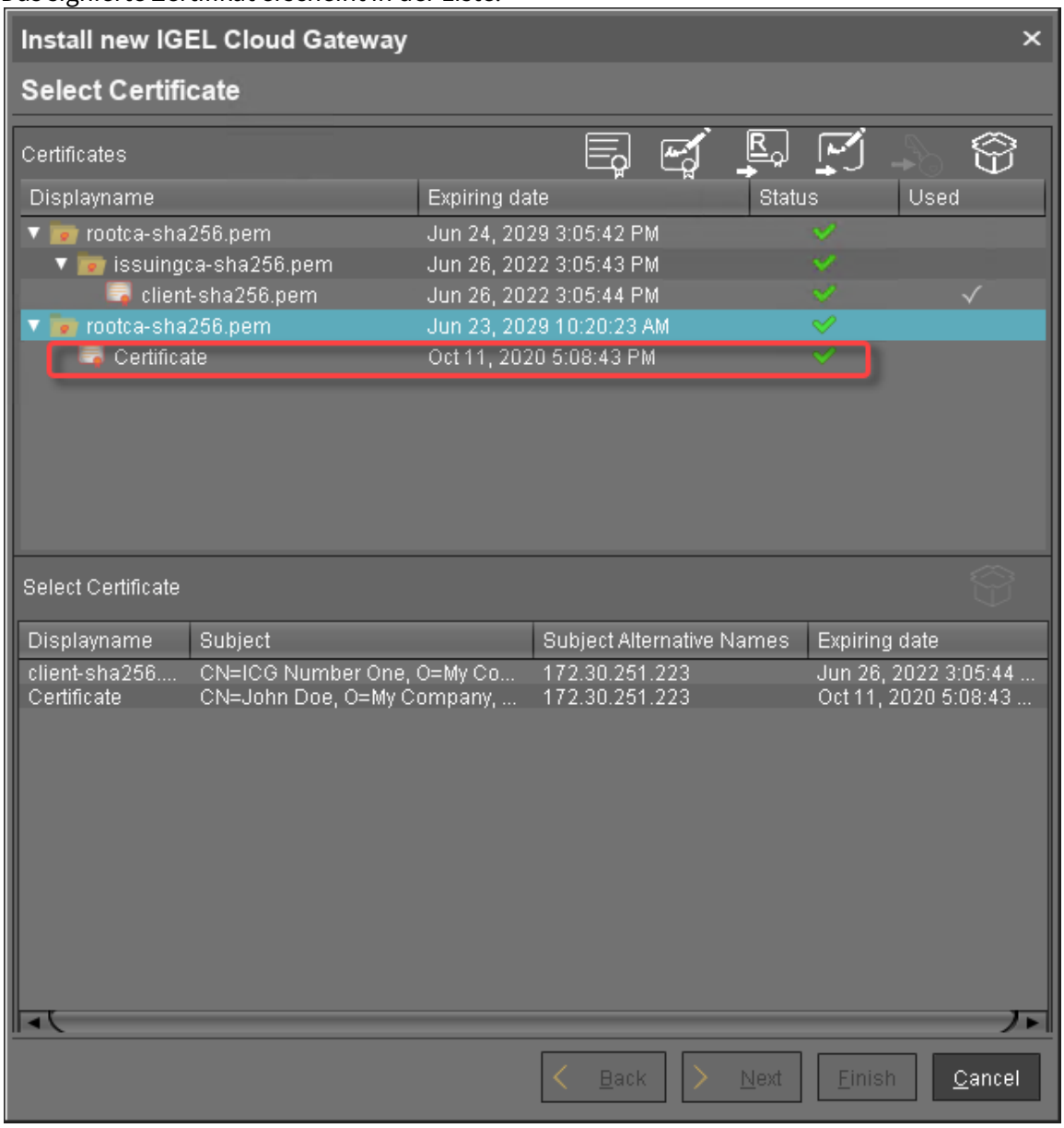


Es wird ein Schlüsselpaar und ein Zertifikat erzeugt.

> Die Generierung von Schlüsseln kann bei virtuellen Maschinen (VMs) viel Zeit in Anspruch nehmen, da diese keine leistungsstarke (Pseudo-)Zufallszahlensquelle haben. Auf Linux-VMs kann dies durch die Installation des haveged[4] Pakets verbessert werden.

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

Das signierte Zertifikat erscheint in der Liste.



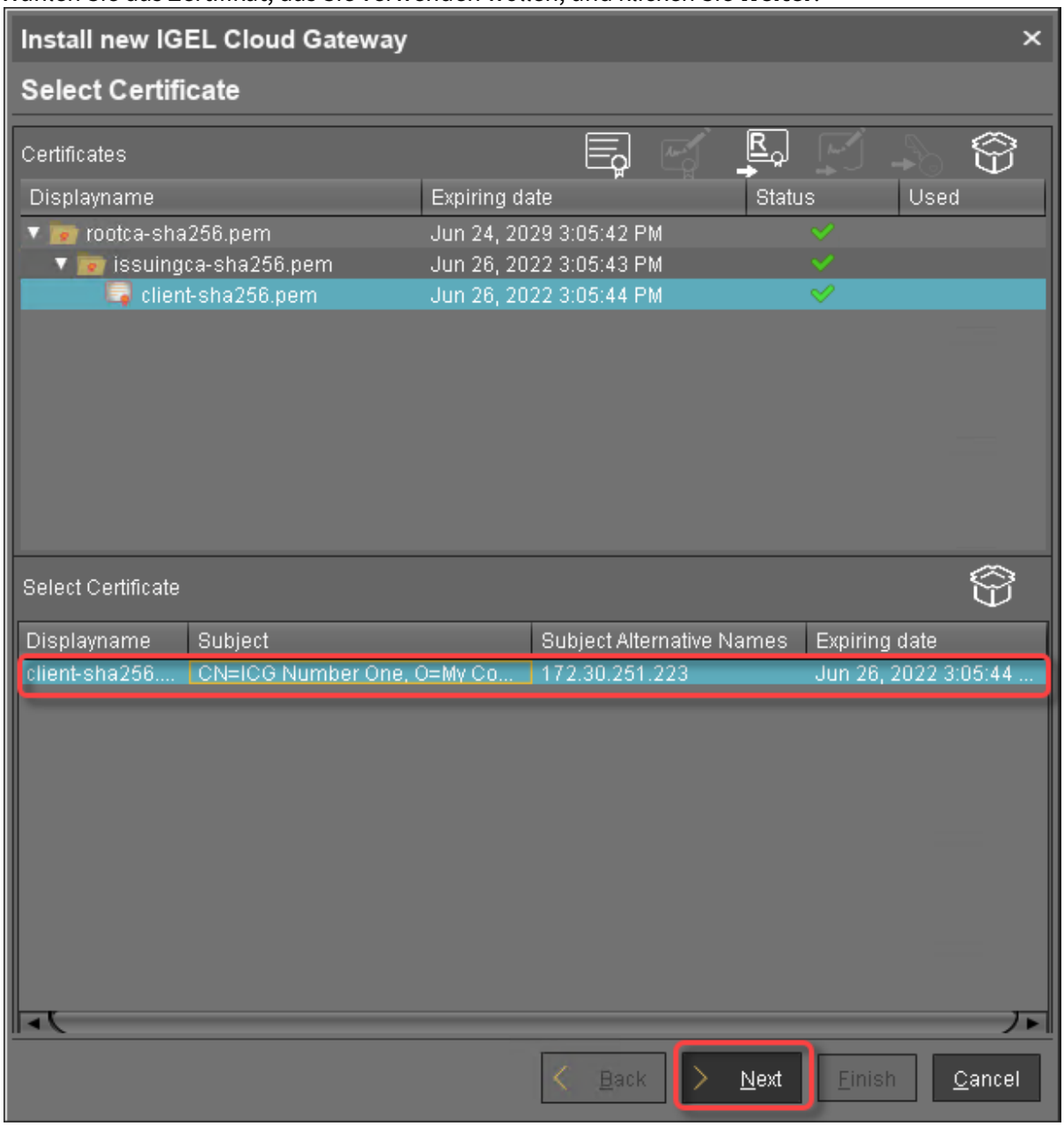
4. Fahren Sie fort mit IGEL Cloud Gateway installieren (see page 40).

IGEL Cloud Gateway installieren

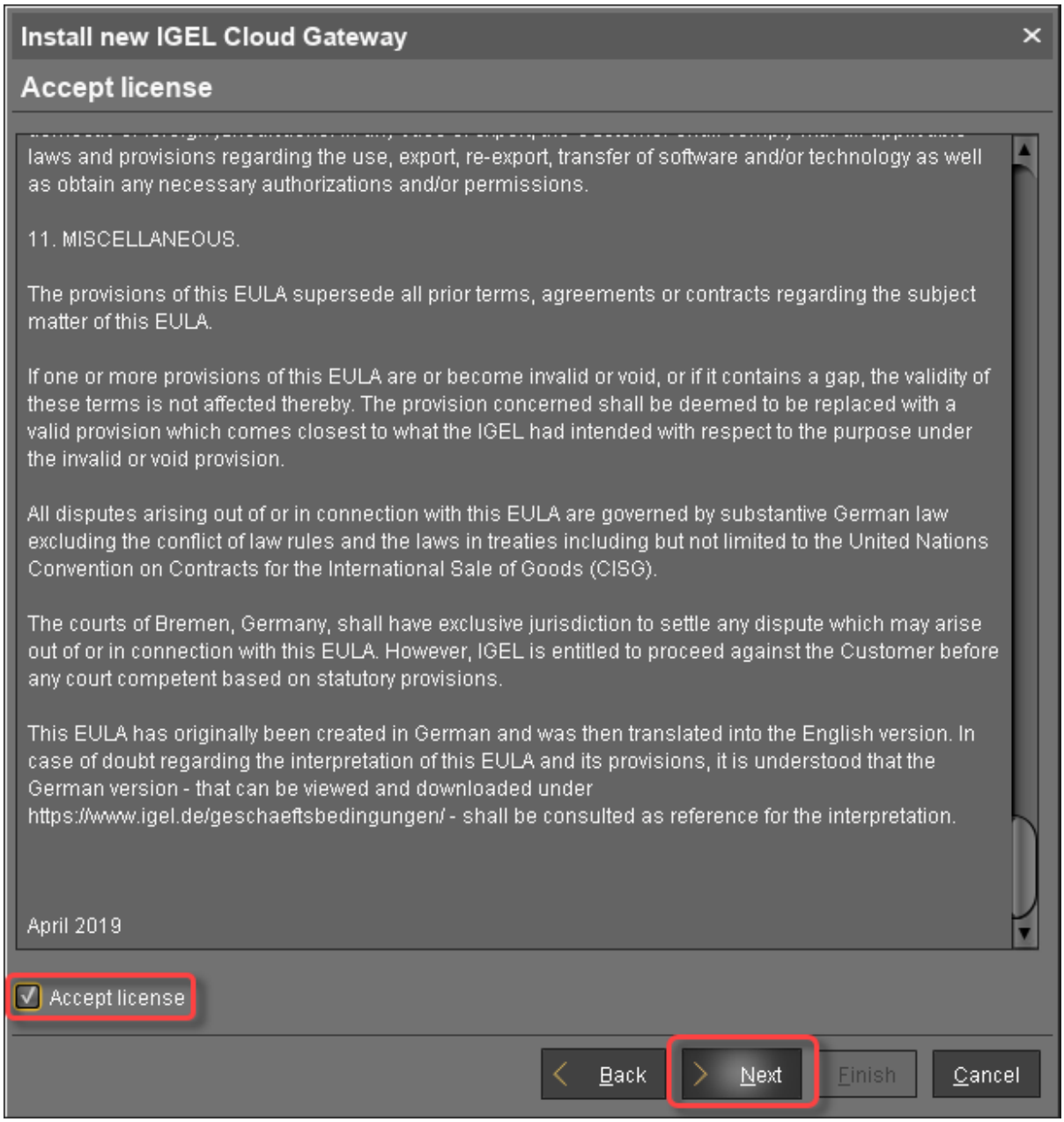
Die empfohlene Methode zur Installation des ICG ist die Verwendung des ICG Remote Installers. Wenn Sie den Remote Installer nicht verwenden können oder wollen, können Sie den ICG manuell installieren; siehe ICG ohne Remote Installer installieren (see page 103).

1. Starten Sie die UMS Konsole.
2. Gehen Sie zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.
3. Wenn der ICG Remote Installer nicht bereits läuft, gehen Sie zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway** und klicken Sie  .
   Der ICG Remote Installer öffnet sich. Im Bereich **Auswahl eines Zertifikats** sind sämtliche Zertifikate aufgelistet, die für den ICG verwendet werden können. Wenn Sie ein Zertifikat benötigen, können Sie den ICG Remote Installer verwenden, um eines zu installieren; siehe Zertifikate bereitstellen (see page 13).

4. Wählen Sie das Zertifikat, das Sie verwenden wollen, und klicken Sie **Weiter**.



5. Lesen Sie die EULA und aktivieren Sie **Lizenz akzeptieren**, wenn Sie diese akzeptieren, und klicken Sie **Weiter**.



6. Geben Sie die Installationsparameter ein:
   - **SSH Host**: Adresse des Hosts, auf dem der ICG installiert werden soll. Dieses Feld ist vorbelegt mit einem Host, der dem Zertifikat entnommen wurde. Wenn mehrere Hosts im Zertifikat spezifiziert sind, stellen Sie sicher, dass dieser derjenige Host ist, der für die Kommunikation zwischen UMS und ICG verwendet wird.
   - **SSH-Port**: SSH-Port (Standard: 22)

> Der SSH-Benutzer benötigt Root-Rechte, sonst kann der Remote Installer nicht alle notwendigen Aufgaben der Installation ausführen.
> UMS 5.09.110 oder höher: Es ist ausreichend, dass der SSH-Benutzer die sudo-Berechtigung hat.

> Root-Zugriff zum SSH-Server ist ein Sicherheitsrisiko!
> Wenn Sie die Anmeldung als Root für SSH zulassen, wird empfohlen, nach Fertigstellung der ICG-Installation die Anmeldung als Root zu deaktivieren.

> Schlüsselbasierte Authentifizierung wird vom Remote Installer nicht unterstützt. Wenn Sie schlüsselbasierte Authentifizierung verwenden wollen, müssen Sie die Installation manuell vornehmen; siehe ICG ohne Remote Installer installieren (see page 103).

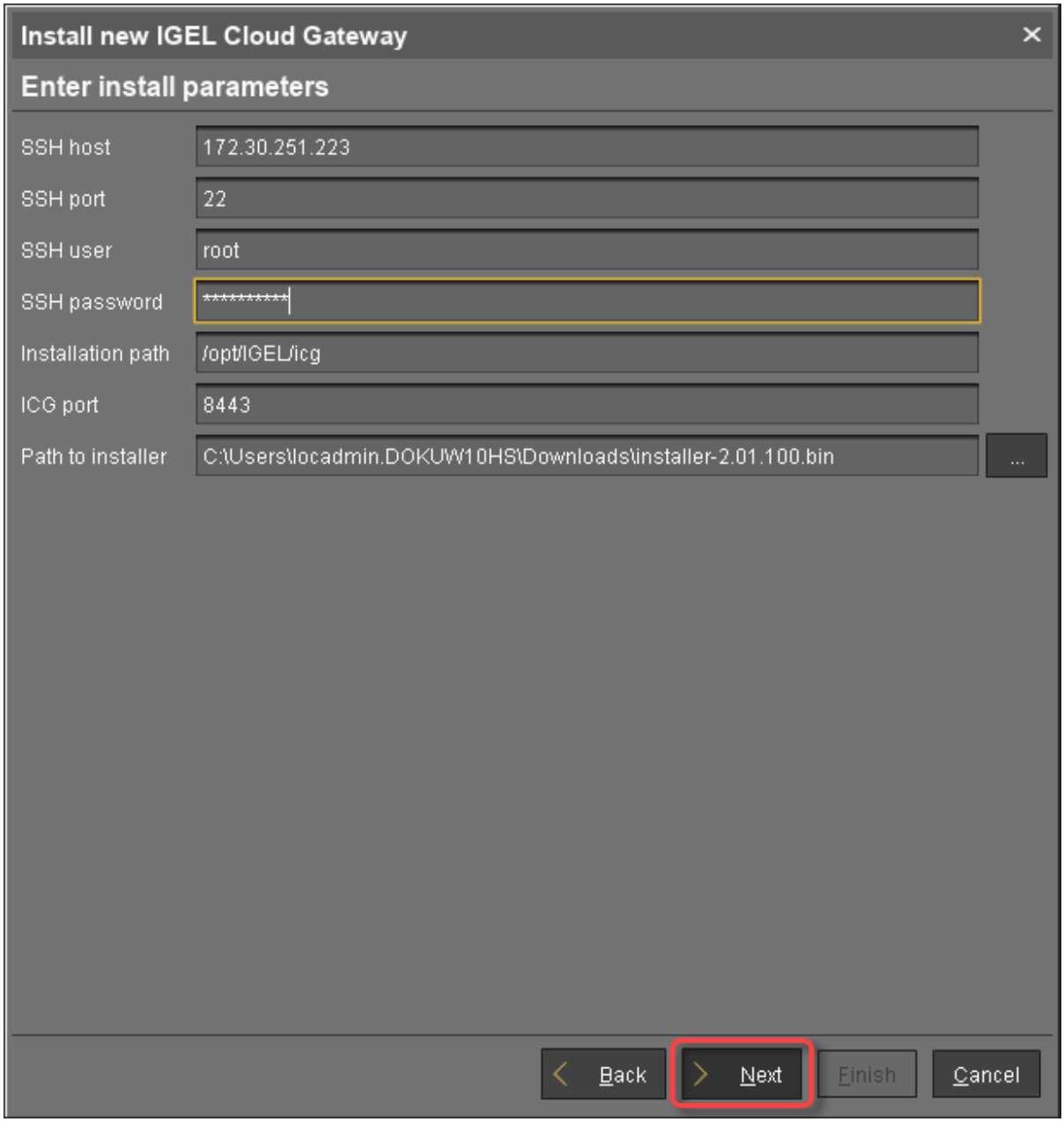
- **SSH Benutzer**: Der Benutzer, den der Remote Installer verwendet, um sich gegen den SSH-Server zu authentifizieren und den Installer auszuführen

  > **Benutzername "icg" ist reserviert**
  >
  > Verwenden Sie als Benutzernamen für den Remote Installer nicht "icg"; dies ist der Benutzername, unter dem der Tomcat-Server läuft.

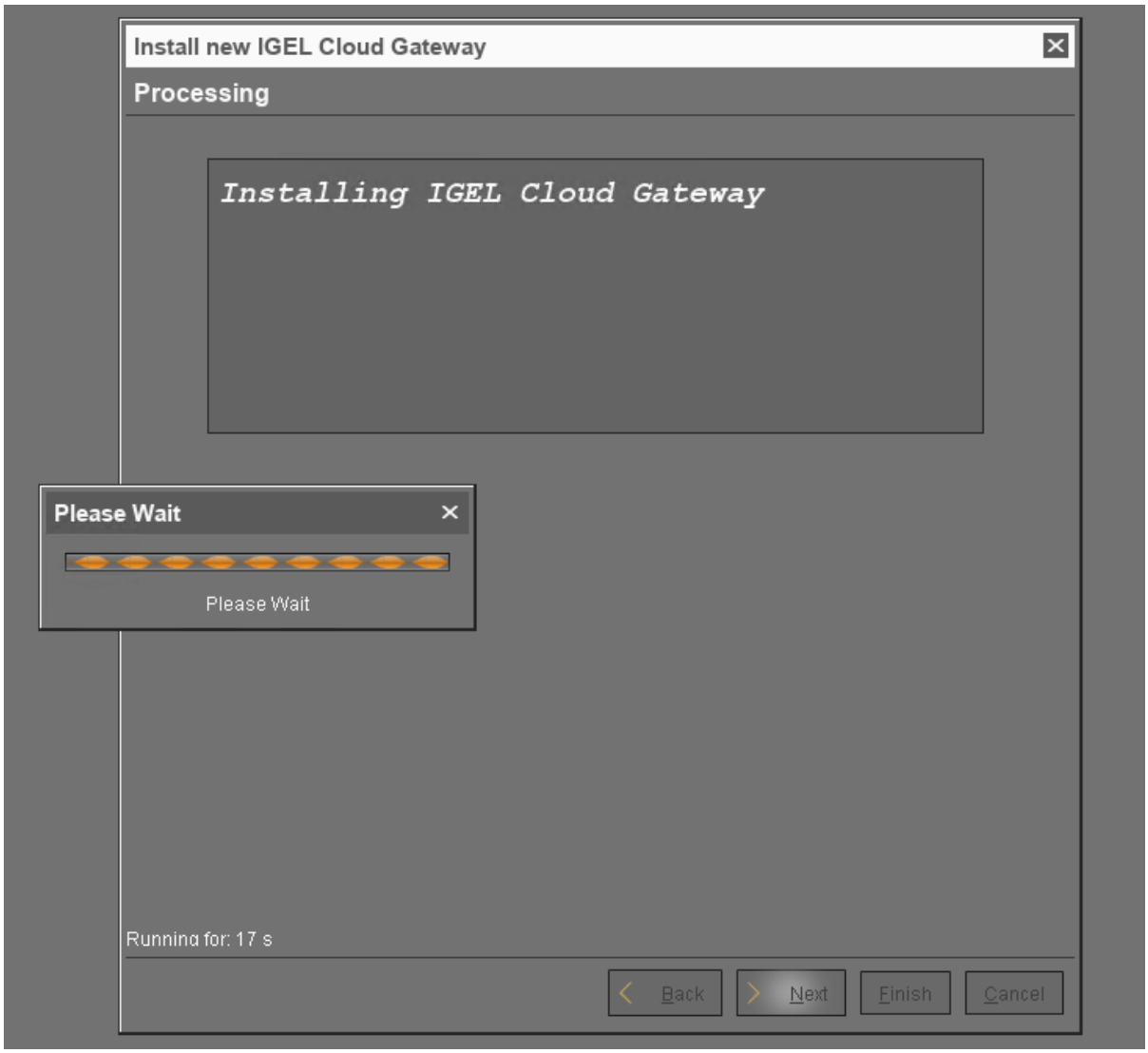
- **SSH Passwort**: Passwort für den Benutzer, der unter **SSH Benutzer** angegeben ist
- **Installationspfad**: Installationspfad auf dem Server (Standard: `/opt/IGEL/icg`)
- **ICG Port**: Nummer des Ports, auf dem der ICG lauschen wird. Privilegierte Ports können verwendet werden, z. B. Port 443. (Standard: 8443)
- **Pfad zum Installer**: Lokaler Pfad zur `.bin`-Datei, die den Installer enthält

  > Der ICG Installer ist unter https://www.igel.com/software-downloads/ verfügbar.

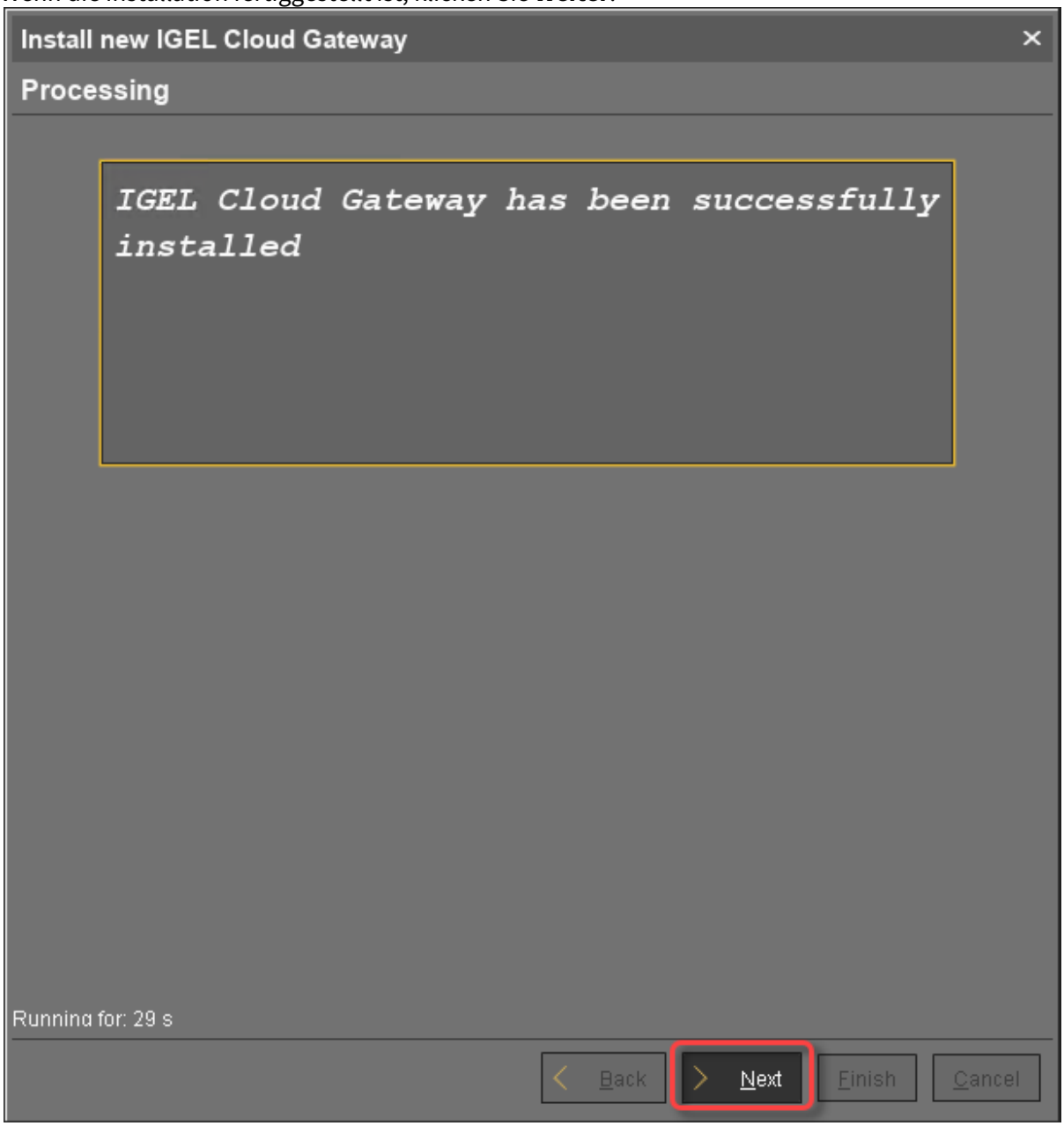
7. Klicken Sie **Weiter**.



Der ICG wird nun installiert. Das kann einige Momente dauern.


Install new IGEL Cloud Gateway
Processing
Installing IGEL Cloud Gateway
Please Wait
Please Wait
Running for: 17 s
Back
Next
Finish
Cancel

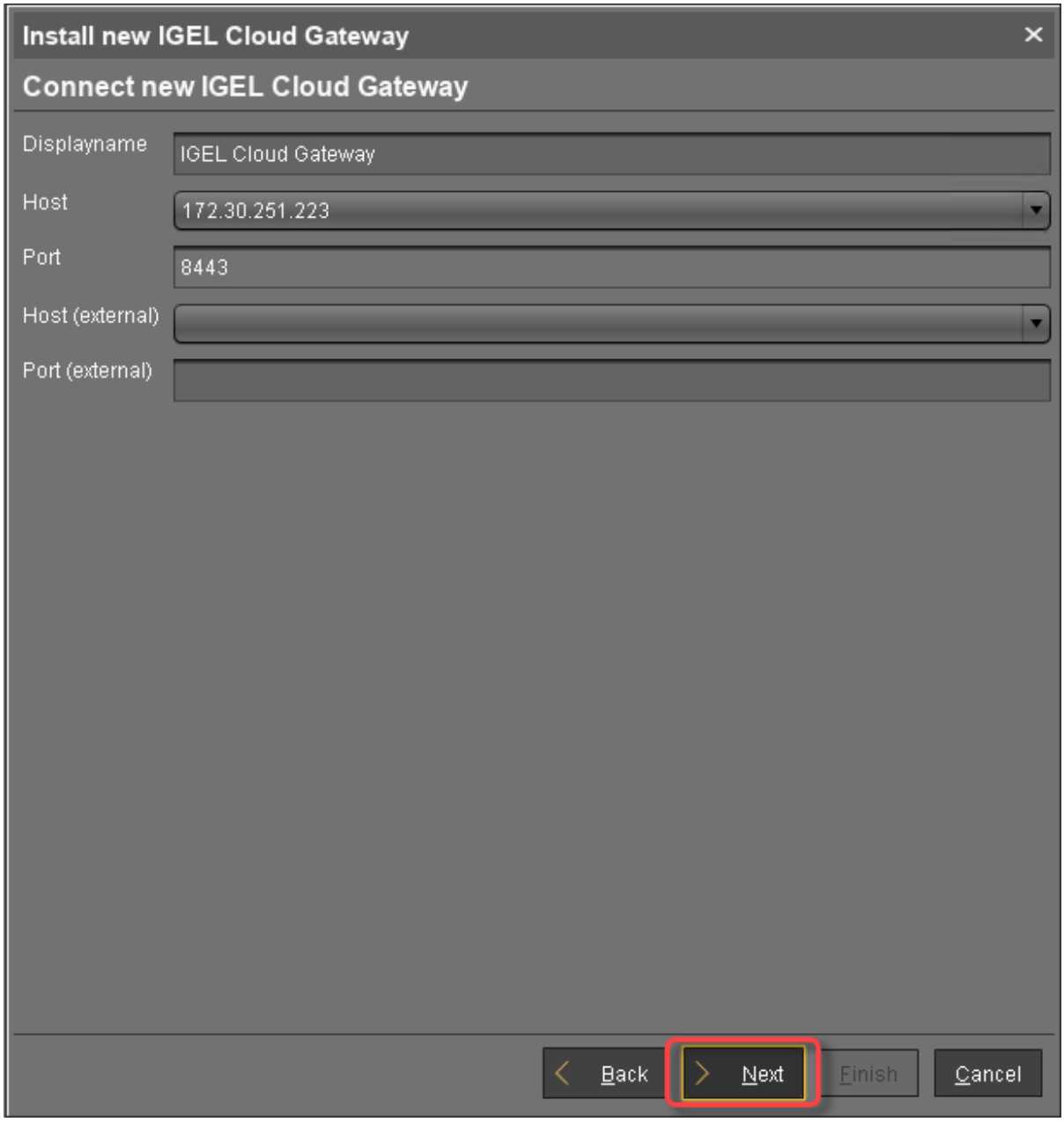
8. Wenn die Installation fertiggestellt ist, klicken Sie **Weiter**.



9. Geben Sie einen Namen für die Anzeige und die Verbindungsdaten für den ICG an:
   - **Name**: Name, unter dem der ICG unter **UMS Administration > IGEL Cloud Gateway** aufgelistet wird
   - **Host**: Interner Host, der von der UMS verwendet wird, um sich mit dem ICG zu verbinden
   - **Host (extern)**: Externer Host, der von den Geräten verwendet wird, um sich mit dem ICG zu verbinden; nur erforderlich, wenn die Geräte anstelle der unter **Host** spezifizierten Adresse eine separate Adresse verwenden

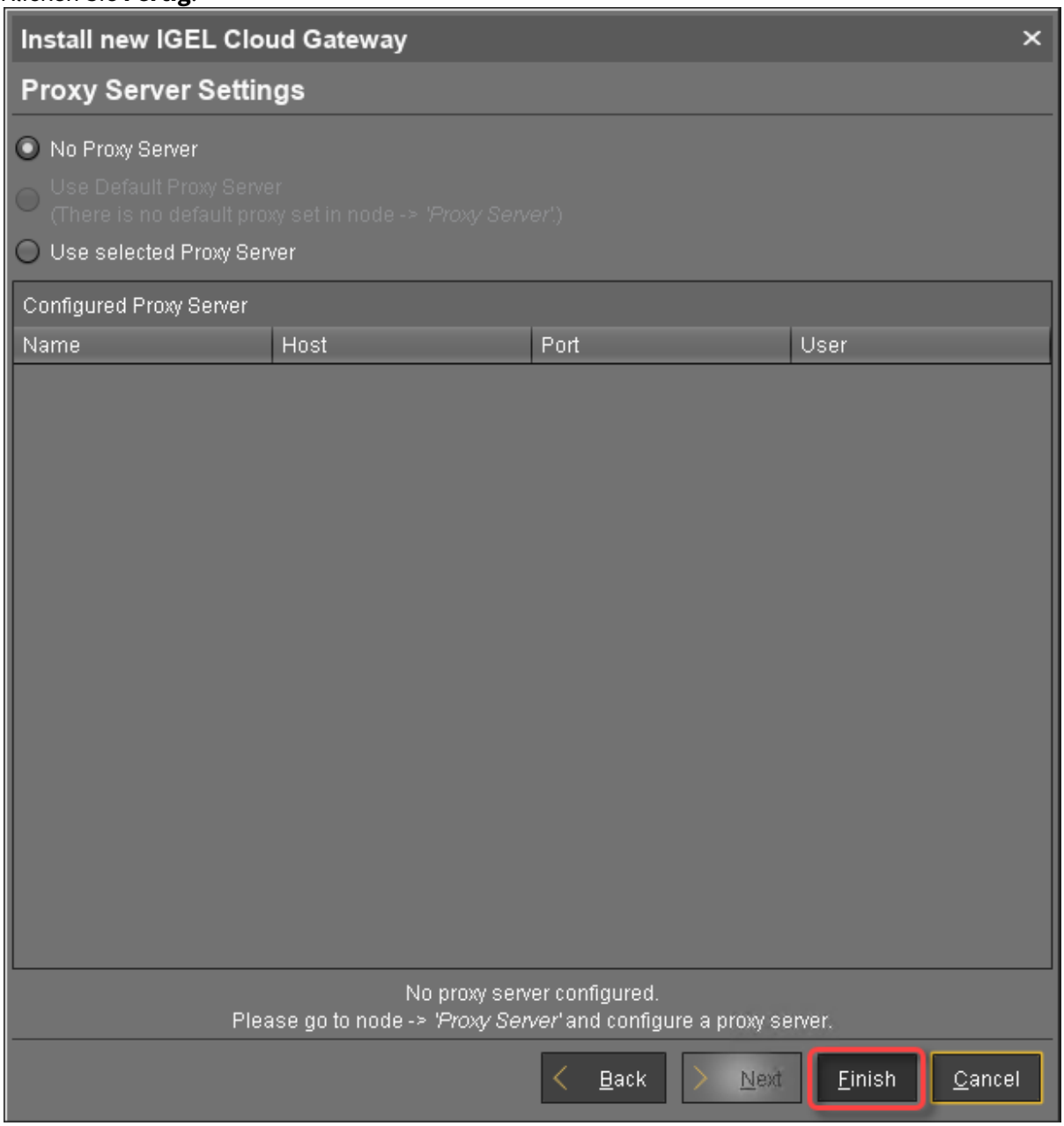
- **Port (extern)**: Port, der von den Endgeräten verwendet wird, wenn sie sich mit dem ICG über den unter **Host (extern)** angegebenen Host verbinden. Wenn die Geräte die unter Host angegebene Adresse verwenden, kann dieses Feld leer bleiben.

10. Klicken Sie **Weiter**.

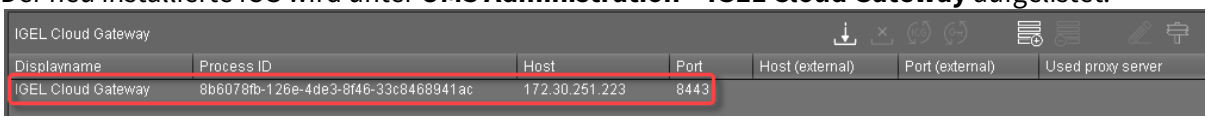


11. Wenn erwünscht, können Sie einen Proxy definieren. Legen Sie die Einstellungen entsprechend fest.

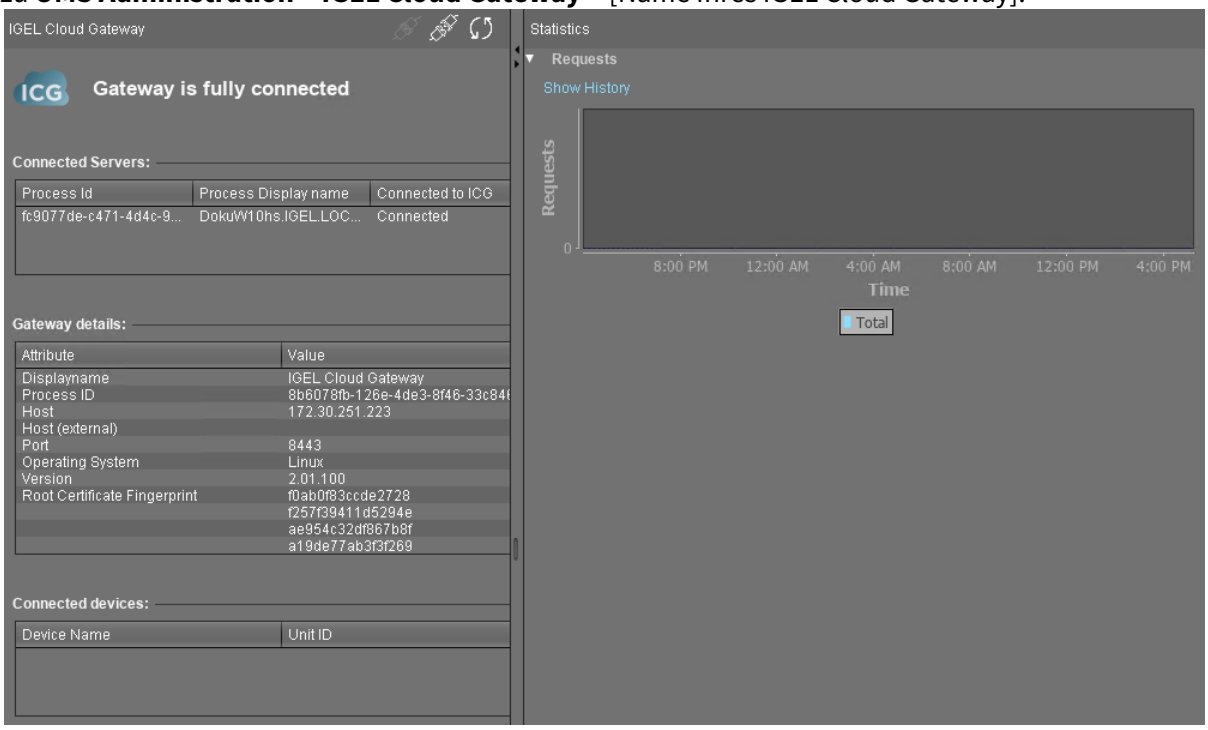
12. Klicken Sie **Fertig**.



Der neu installierte ICG wird unter **UMS Administration > IGEL Cloud Gateway** aufgelistet.



13. Um den Status des ICG und die grundlegenden Daten der Installation zu überprüfen, gehen Sie zu **UMS Administration > IGEL Cloud Gateway >** [Name Ihres IGEL Cloud Gateway].



Geräte anschließen

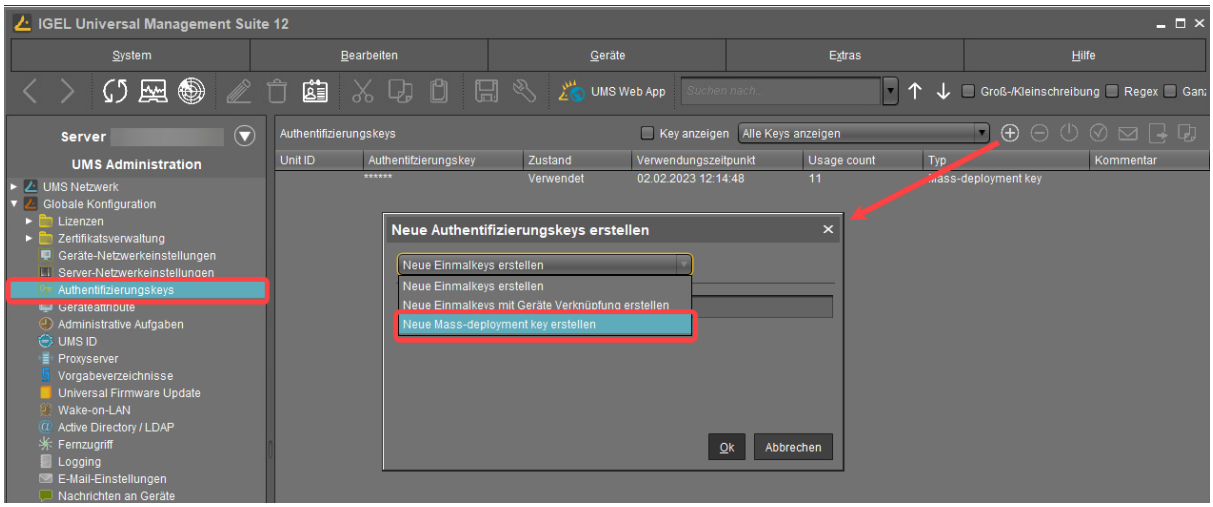
Schlüssel für die Erstauthentifizierung von Geräten generieren und verteilen

Um eine Verbindung mit dem ICG herzustellen, muss sich jedes Gerät beim ICG authentifizieren. Zu diesem Zweck muss ein Schlüssel für die Erstauthentifizierung erstellt werden. Beim ersten Kontakt mit dem ICG muss das Gerät diesen Schlüssel vorweisen.

Es gibt verschiedene Methoden, Schlüssel für die Erstauthentifizierung zu erstellen. Die gebräuchlichste Methode ist hier beschrieben; siehe Alle Methoden, um Schlüssel für die Erstauthentifizierung von Geräten zu erstellen (see page 140).

Einmalschlüssel für beliebige Geräte erstellen

1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
2. Klicken Sie  .



3. Wählen Sie **Neue Mass-deployment key erstellen**.
4. Aktivieren oder deaktivieren Sie **Zufälligen Mass-deployment key generieren**.
   ☑ Der Schlüssel wird von der UMS erstellt.
   ☐ Sie können einen im Eingabefeld einen eigenen Schlüssel eingeben.
5. Klicken Sie **Ok**.
   Ein oder mehrere Einträge erscheinen in der Liste.

Schlüssel über E-Mail oder gedruckten Brief verteilen

1. Gehen Sie unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.

2. Wählen Sie die gewünschte Passworteingabe und klicken Sie  , um die Anmeldeinformationen in die Zwischenablage zu kopieren.
   Die Daten, die für das Verbinden eines Gerätes mit dem ICG benötigt werden, befinden sich in der Zwischenablage: Host-Adresse, Fingerabdruck des ICG Serverzertifikats und Passwort.
   Der Inhalt der Zwischenablage sieht ähnlich aus wie das folgende Beispiel:

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

   Die Zwischenablage enthält Daten für alle aktiven ICGs. Im obigen Beispiel ist 1 ICG Verbindung aktiv. Wenn beispielsweise 3 ICGs aktiv wären, wären die Daten für diese 3 ICGs enthalten.

3. Um die Anmeldeinformationen per E-Mail zu senden, fügen Sie die Daten in eine verschlüsselte E-Mail ein. Um die Anmeldeinformationen in einem gedruckten Brief zu senden, fügen Sie die Daten in Ihr E-Mail-Programm oder Ihr Textverarbeitungsprogramm ein.

Gerät mit dem IGEL Cloud Gateway verbinden

Wenn die Anmeldeinformationen auf der Benutzer-/Geräteseite verfügbar sind, ist das Gerät bereit für die Verbindung mit der UMS.

Wenn das Gerät noch nicht konfiguriert ist, startet der IGEL Einrichtungsassistent (Setup Assistant) automatisch beim Systemstart.

IGEL OS 11

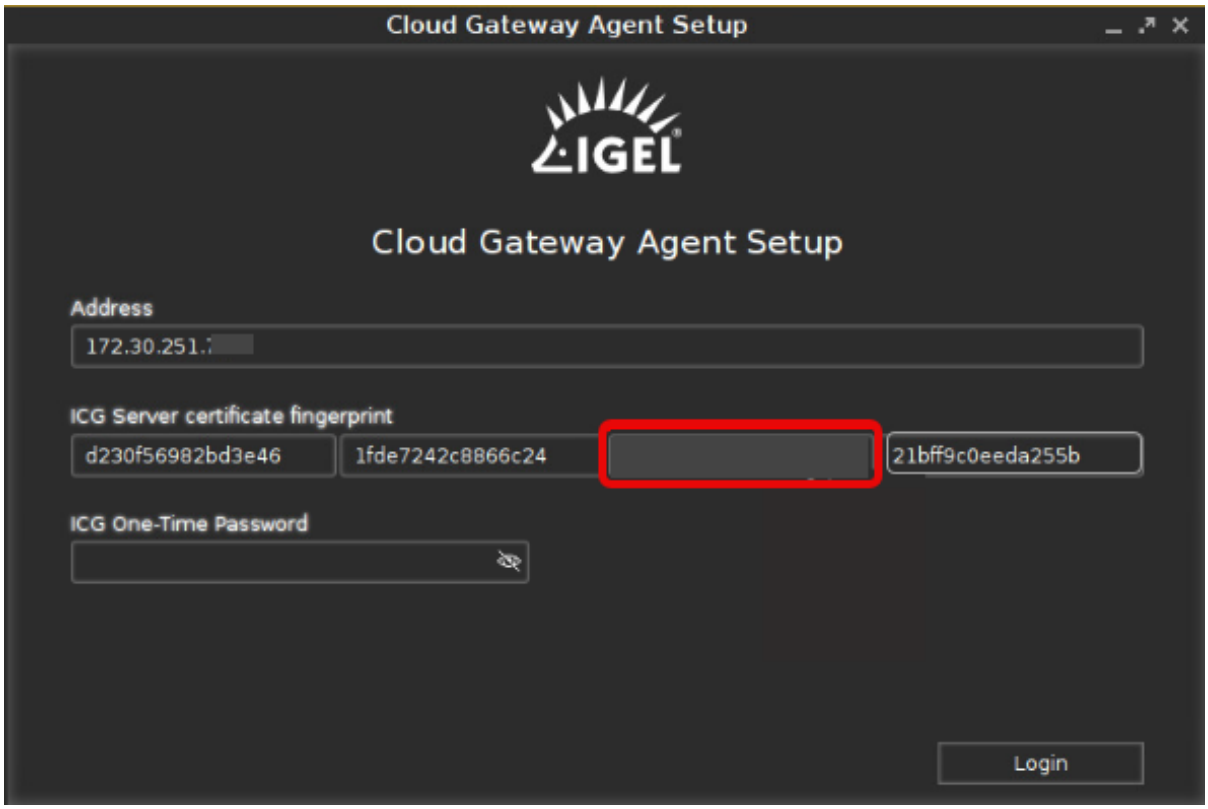
Das ICG Agent Setup, das hier beschrieben wird, ist in den Einrichtungsassistenten integriert. Die Vorgehensweise ist sowohl für das eigenständige ICG Agent Setup (kann unter **IGEL Setup > Zubehör > ICG Agent Setup** konfiguriert werden) als auch für das im Einrichtungsassistenten eingebettete Setup identisch. Nähere Informationen zum Einrichtungsassistenten in IGEL OS 11 finden Sie im Kapitel Setup Assistant im IGEL OS Handbuch.

1. Öffnen Sie unter **Startmenü >**  (System) **ICG Agent Setup**.

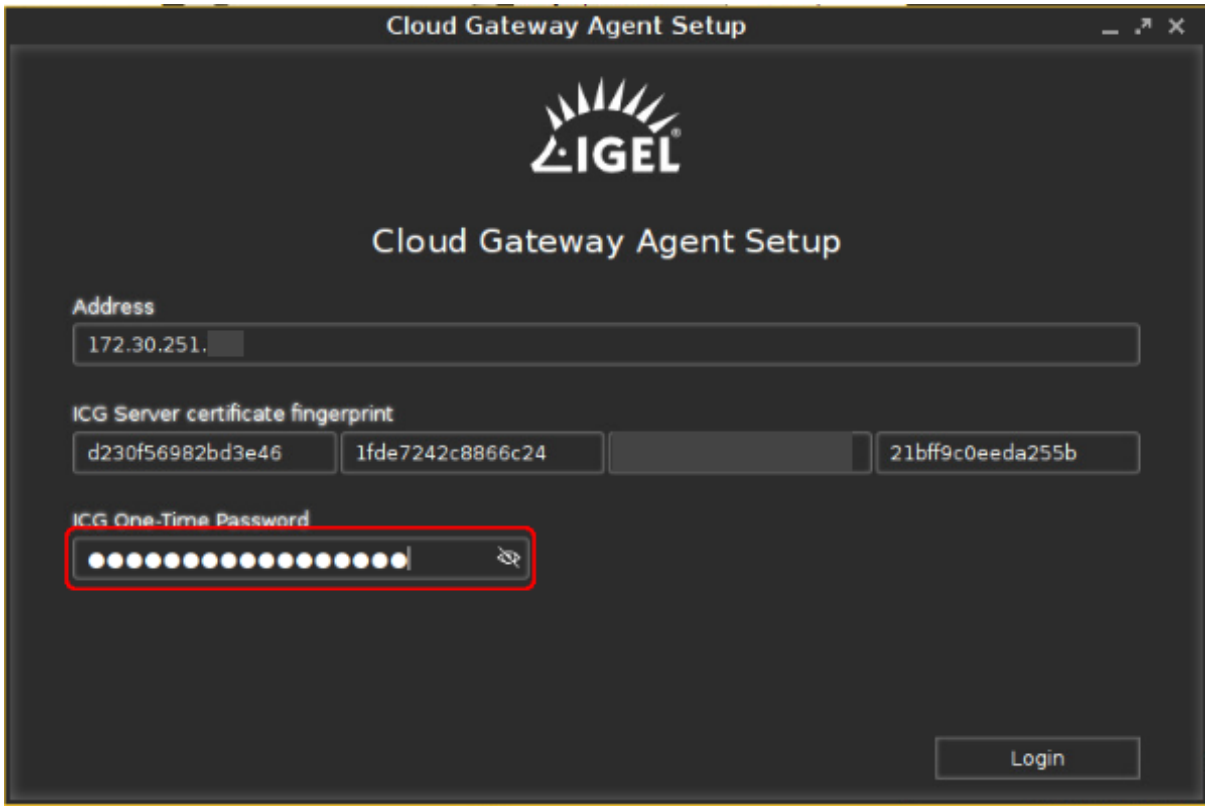
2. Geben Sie die ICG Server IP Adresse oder den DNS Name bei **Adresse** ein.
   Beispiel: `172.30.251.71` (IP Adresse), `icg.example.com` (DNS Name)

3. Klicken Sie auf **Verbinden**.
   Das Setup-Dienstprogramm überprüft die Konnektivität und zeigt 3/4 des Fingerabdrucks des ICG-Serverzertifikats an.

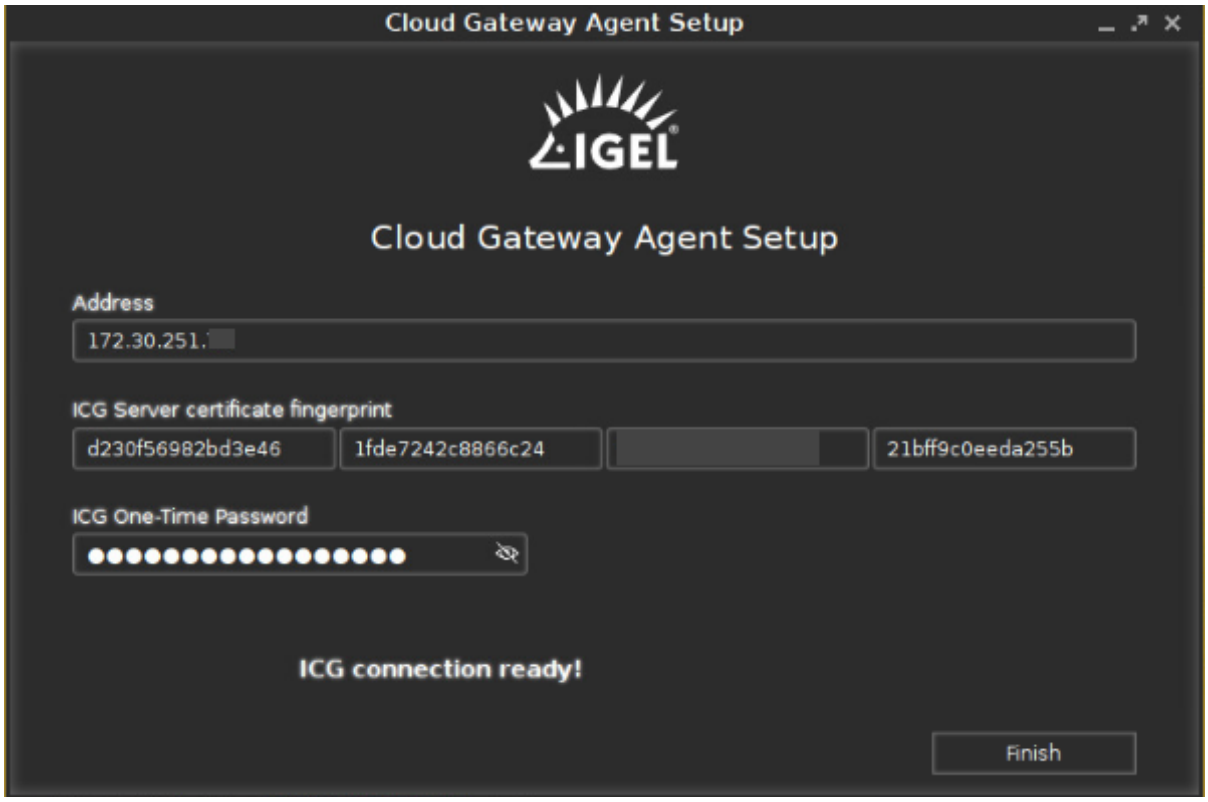
4. Geben Sie den fehlenden Teil des **Fingerabdrucks des ICG-Serverzertifikats** ein. Ein Teil des Fingerabdrucks kann fehlen; dieser wird nach dem Zufallsprinzip bestimmt.



5. Geben Sie das **ICG One-Time-Passwort** ein. Klicken Sie auf das Augensymbol, um die Sichtbarkeit des Passworts umzuschalten.



6. Klicken Sie auf **Anmelden**.
   Die Meldung **ICG-Verbindung bereit!** wird angezeigt.



7. Klicken Sie **Fertigstellen**.

   Das ICG Verbindungssymbol  wird in der Taskleiste angezeigt.

IGEL OS 12

⚠ Es ist nicht erforderlich, die ICG-Konfigurationseinstellungen manuell an OS 12 Geräte zu senden.

IGEL OS 12 Geräte kommunizieren mit der UMS 12 und dem ICG 12 über Gerätekonnektoren. Die Geräte erhalten automatisch die Gerätekonnektoren sowohl für die UMS als auch für das ICG, selbst wenn Sie die UMS innerhalb des Unternehmensnetzwerks zur Registrierung der Geräte verwenden. Sobald ein Gerät registriert ist, versucht es, sich mit einem der Geräteanschlüsse zu verbinden. Wenn die erste Verbindung nicht funktioniert, versucht es den nächsten Geräteanschluss. Befindet sich das Gerät außerhalb des Unternehmensnetzes, wird es schließlich automatisch mit dem Geräteanschluss des ICG verbunden.

ⓘ Sie können die Verbindung zwischen dem IGEL OS 12-Gerät und dem ICG überprüfen:

- in den Geräteeinstellungen der UMS Konsole. Weitere Informationen finden Sie unter Geräteinformationen in der IGEL UMS einsehen.
- im UMS Web App-Gerätekonfigurationsdialog, unter **System > Remote Management**. Weitere Informationen finden Sie unter Remote Management.

Wenn Sie remote OS 12 Geräte einbinden möchten, die sich über das ICG mit dem UMS verbinden, können Sie die Geräte mit einer der folgenden Methoden über das ICG registrieren:

- Konfigurieren Sie den IGEL Onboarding Service für das ICG. Einzelheiten finden Sie unter Initial Configuration of the IGEL Onboarding Service (OBS).
- Verwenden Sie die ICG-Anmeldeinformationen in der alternativen Onboarding-Methode. Weitere Informationen finden Sie im Abschnitt "Alternative Onboarding Method: Registering Devices with the UMS Using the One-Time Password" unter Onboarding IGEL OS 12 Devices.

Zwischen ICG und Direktverbindung umschalten

Wenn das Gerät (vorübergehend) in das lokale Netzwerk eines Unternehmens verlegt wird, wo eine direkte Verbindung zum UMS möglich ist, kann es sinnvoll sein von der ICG-Nutzung auf die direkte Verbindung umzuschalten. Dies kann mit einem Parameter in der Registry erfolgen.

Von ICG zur Direktverbindung umschalten:

1. Gehen Sie im Geräte-Setup unter **System > Registry > system > remotemanager > enable_icg** (ganzer Parametername: `system.remotemanager.enable_icg`).
2. Deaktivieren Sie **ICG aktivieren.**
3. Klicken Sie **Übernehmen** oder **Ok.**
   Das Gerät bricht die Verbindung zum ICG ab und stellt automatisch eine direkte Verbindung zur UMS her. Das Tray-Symbol ändert sich zu  .

Von der Direktverbindung zum ICG umschalten:

1. Gehen Sie im Geräte-Setup unter **System > Registry > system > remotemanager > enable_icg** (ganzer Parametername: `system.remotemanager.enable_icg`).
2. Aktivieren Sie **ICG aktivieren.**
3. Klicken Sie **Übernehmen** oder **Ok.**

   Das Gerät bricht seine Direktverbindung zur UMS ab und stellt automatisch eine Verbindung zum ICG her. Das Tray-Symbol ändert sich zu  .

Administration

IGEL Cloud Gateway (ICG) aktualisieren

Sie können Ihren IGEL Cloud Gateway (ICG) von der IGEL Universal Management Suite (UMS) aus aktualisieren.

Voraussetzungen

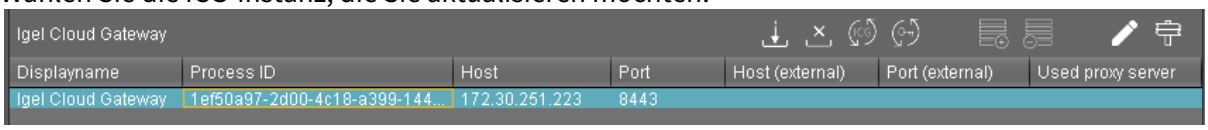
- UMS Version 5.09.100 oder höher
- Die neue Version des IGEL Cloud Gateway (ICG) wurde von https://www.igel.com/software-downloads/ heruntergeladen
- Root-Zugriff auf den Host, auf dem das ICG läuft.

> Ein Upgrade von ICG 1.x (basierend auf OVA) auf 2.x wird nicht unterstützt.
> Die unterstützte Methode ist eine Neuinstallation auf einem Linux-Server; siehe Installation und Einrichtung (see page 12).

Schritte

Um das ICG zu aktualisieren, gehen Sie wie folgt vor:

1. Starten Sie die UMS Konsole.
2. Gehen Sie unter **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway.**
3. Wählen Sie die ICG-Instanz, die Sie aktualisieren möchten.



4. Klicken Sie in der Symbolleiste oben rechts auf  .
   Der Update-Assistent öffnet sich.
5. Geben Sie die folgenden Installationsparameter ein:
   - **SSH Host:** Der Host, auf dem der ICG läuft (Standard: `localhost`)
   - **SSH Port:** SSH-Port (Standard: `22`)

   > Der SSH-Benutzer muss über einen Root-Zugang verfügen.

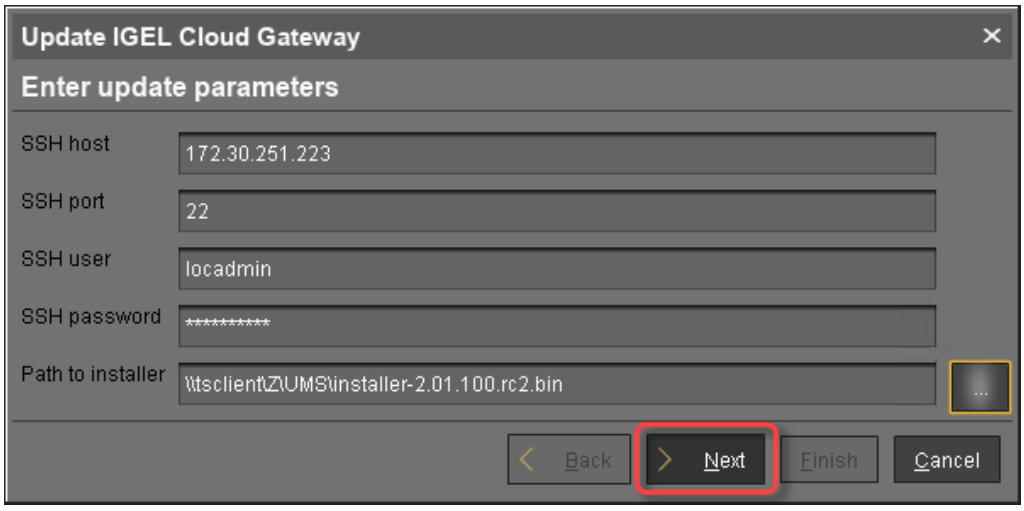
   > Der Root-Zugriff auf den SSH-Server ist ein Sicherheitsrisiko!
   > Stellen Sie sicher, dass Sie den Root-Zugriff auf den SSH-Server deaktivieren, wenn die ICG-Installation abgeschlossen ist.

> Ab UMS 5.09.110 ist es nicht mehr notwendig den Root-Benutzer zu verwenden. Es reicht aus, wenn der SSH-Benutzer über sudo-Privilegien verfügt.

- **SSH Benutzer:** SSH-Benutzer
- **SSH Passwort:** SSH-Benutzerpasswort
- **Installationspfad:** Installationspfad (Standard: `/opt/IGEL/icg`)
- **ICG Port:** ICG-Port (Standard: `8443`)
- **Installer Pfad:** Der Pfad zur `.bin`-Datei, die das Installationsprogramm enthält.

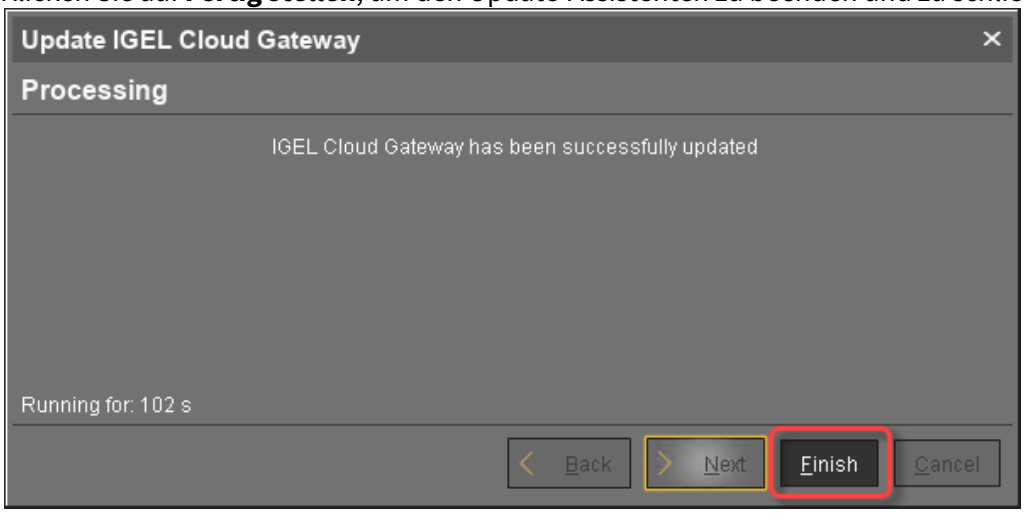
> ICG-Installer sind verfügbar unter https://www.igel.com/software-downloads/.

6. Klicken Sie **Weiter.**



Das ICG wird nun aktualisiert. Dies kann wenige Minuten dauern.
Wenn die Aktualisierung vollendet ist, zeigt der Update-Assistent eine Erfolgsmeldung an.

7. Klicken Sie auf **Fertig stellen**, um den Update-Assistenten zu beenden und zu schließen.



ICG Verbindungslimit konfigurieren

Sie können für die maximal zulässige Anzahl von Verbindungen zu Endgeräten ein Limit setzen. Dieses Limit können Sie global für alle ICG Instanzen setzen oder einzeln für jede ICG Instanz.

Wenn das Limit erreicht ist, wird das ICG alle weiteren Verbindungen zu Endgeräten zurückweisen. Die Zurückweisung der Verbindungen zu Endgeräten wird protokolliert.

Globales Verbindungslimit konfigurieren

1. Gehen Sie zu **UMS Administration > IGEL Cloud Gateway** und klicken Sie  (oben rechts).
2. Wählen Sie im Dialog **ICG Verbindungslimit** die Option **Globales Verbindungslimit**.
3. Geben Sie bei **Verbindungen begrenzen auf:** das gewünschte Limit ein.
4. Klicken Sie **Ok**.

Einzelne Limits für jede ICG Instanz konfigurieren

1. Gehen Sie zu **UMS Administration > IGEL Cloud Gateway** und klicken Sie  (oben rechts).
2. Wählen Sie im Dialog **ICG Verbindungslimit** die Option **ICG-spezifische Verbindungslimits verwenden**.
3. Geben Sie bei **Verbindungen begrenzen auf:** das gewünschte Limit für jede ICG Instanz ein oder belassen Sie **Verbindungen unbegrenzt zulassen**, je nach Ihren Bedürfnissen.
4. Klicken Sie **Ok**.

Protokoll auf zurückgewiesene Verbindungen überprüfen

Die folgenden Schritte müssen auf jedem ICG Host durchgeführt werden.

1. Öffnen Sie ein Terminal auf dem Host und melden Sie sich als der Benutzer an, der beim Installieren des ICG definiert wurde (siehe IGEL Cloud Gateway installieren (see page 40)).
2. Öffnen Sie die Konfigurationsdatei `logback-spring.xml` in einem Texteditor, z. B. vi:
   `sudo vi /opt/IGEL/icg/usg/conf/logback-spring.xml`
3. Ändern Sie das Element `<logger>` wie folgt:
   `<logger name="de.igel" level="DEBUG"/>`
4. Starten Sie das ICG neu:
   `sudo systemctl restart icg-server.service`
5. Um herauszufinden, welche Verbindungen zurückgewiesen wurden, öffnen Sie die Protokolldatei `/opt/IGEL/icg/usg/logs/usg.log` und suchen Sie nach Einträgen, die so lauten: `Max connections limit has exceeded. Device [devicename] is rejected`

Ein signiertes Zertifikat für den ICG erneuern

Wenn das signierte Zertifkat Ihrer ICG-Installation abläuft, müssen Sie es erneuern, d. h. durch ein neueres Zertifikat ersetzen, das mit dem aktuellen kompatibel ist. Das neue Zertifikat ist kompatibel, wenn folgende Voraussetzungen gegeben sind:

- Das neue Zertifikat wird von dem gleichen Root-Zertifikat wie das aktuelle ausgestellt
- Das neue Zertifikat enthält die gleiche IP-Adresse oder Hostnamen wie das aktuelle Zertifikat
- Das neue Zertifikat ist ein signiertes Zertifikat

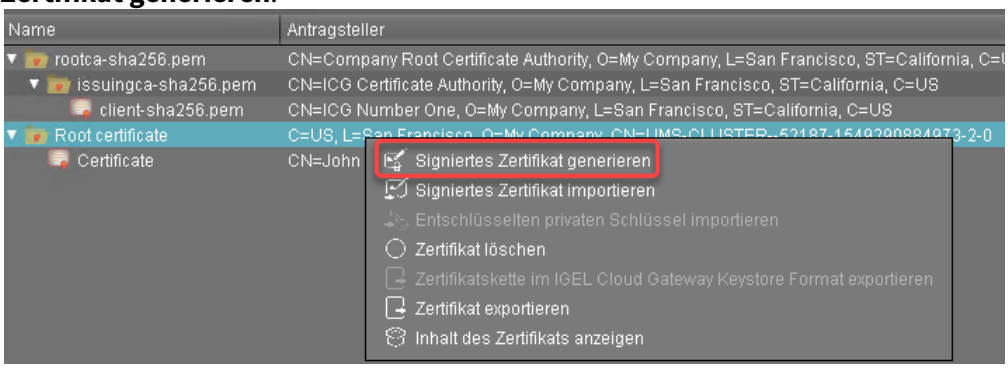
Sie können ein Zertifikat mit der Update Keystore-Funktion der UMS oder lokal auf dem Rechner, auf dem sich der ICG befindet, verlängern. Es wird die Verwendung der Update Keystore-Funktion der UMS empfohlen; diese Methode wird in diesem Kapitel beschrieben.

Ein neues Zertifikat erstellen

Wenn Sie noch kein neues Zertifikat haben:

1. Gehen Sie in der UMS Konsole auf **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway**.

2. Öffnen Sie das Kontextmenu auf dem entsprechenden Root-Zertifikat und wählen Sie **Signiertes Zertifikat generieren**.



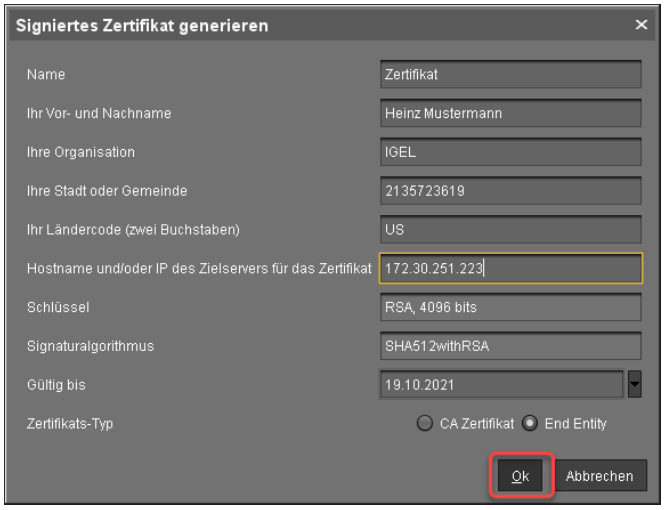
3. Füllen Sie die Felder des Zertifikats aus (wahrscheinlich sind die Daten dieselben wie de für das laufende Zertifikat):
   - **Name**: Angezeigter Name des Zertifikats

     Der angezeigte Name des Serverzertifikats darf nicht mit dem des Root-Zertifikats identisch sein.

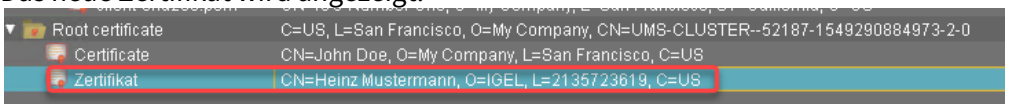
   - **Ihr Vor- und Nachname**: Name des Zertifikathalters
   - **Ihre Organisation**: Organisation oder Name der Firma
   - **Ihre Stadt oder Gemeinde**: Ortsangabe
   - **Ihr Ländercode (zwei Buchstaben)**: Ländercode nach ISO 3166, z.B. `DE`, `UK` oder `US`
   - **Hostname und/oder IP des Zielservers für das Zertifikat**: Hostname(n) oder IP-Adresse(n) wie im aktuellen Zeritifkat verwendet

- **Gültig bis**: Lokales Datum, an dem das Zertifikat abläuft. (Standard: Ein Jahr ab jetzt)

4. Klicken Sie **OK**.



Das neue Zertifikat wird angezeigt.

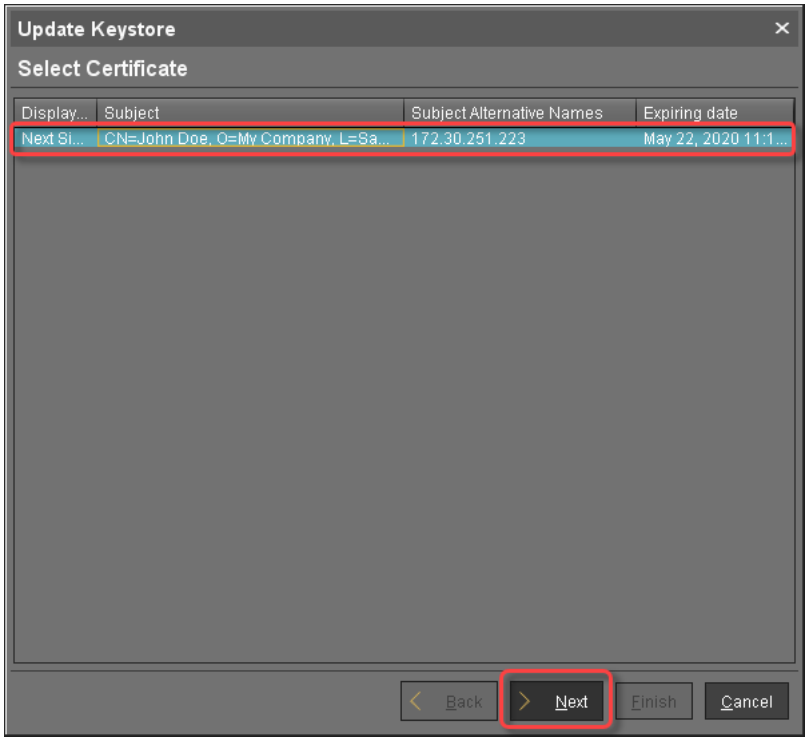


Keystore aktualisieren

1. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.

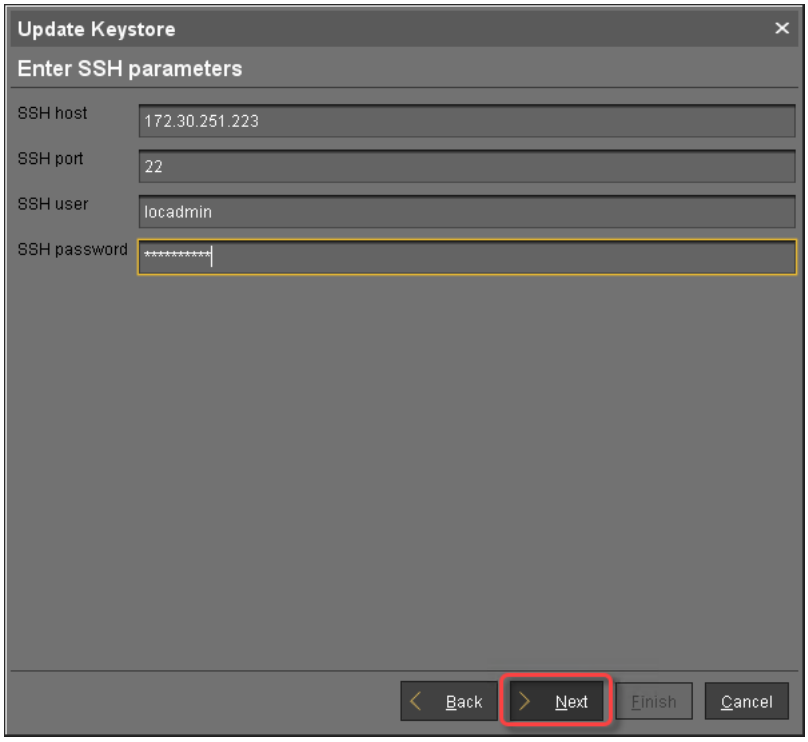
2. Wählen Sie den ICG, für den Sie das Zertifikat aktualisieren wollen, und klicken Sie  .
Der Assistent für die Aktualisierung des Keystore öffnet sich; er zeigt die Zertifikate an, die für die Erneuerung verwendet werden können.

3. Wählen Sie das neue Zertifikat aus und klicken Sie **Weiter**.



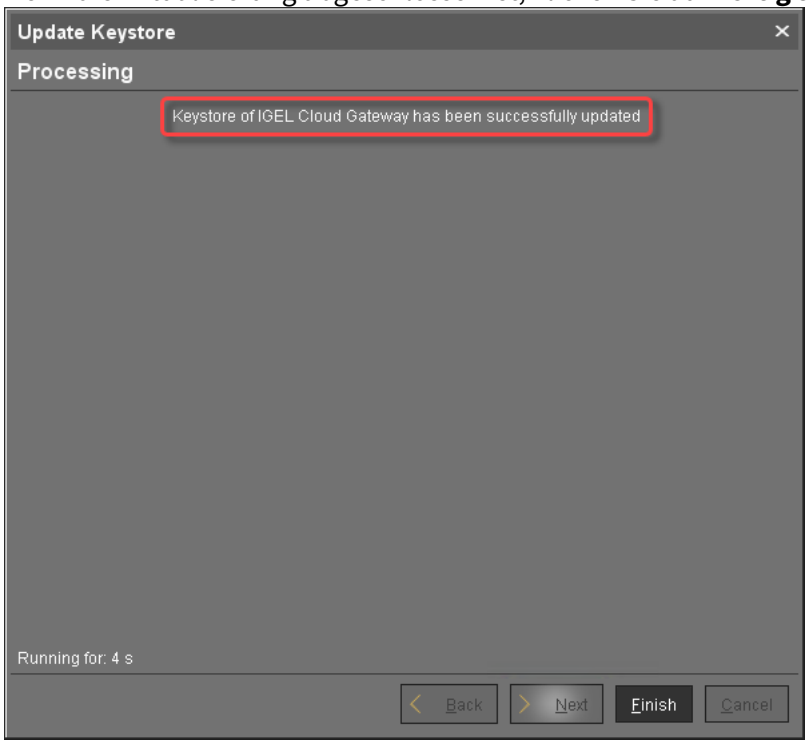
4. Geben Sie die SSH Parameter ein:
   - **SSH Host**: IP-Adresse oder Hostname, unter der die UMS den ICG erreichen kann
   - **SSH Port**: SSH Port (Standard: `22`)
   - **SSH Benutzer**: Derselbe Benutzer, der für den Remote-Installer verwendet wurde
   - **SSH Passwort**: Passwort für den als SSH-Benutzer angegebenen Benutzer

5. Klicken Sie **Weiter**.

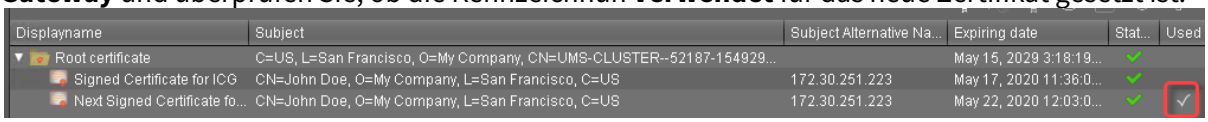


Der Keystore des ICG wird mit dem neuen Zertifikat aktualisiert.

6. Wenn die Aktualisierung abgeschlossen ist, klicken Sie auf **Fertig stellen**.



7. Gehen Sie zu **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway** und überprüfen Sie, ob die Kennzeichnun **Verwendet** für das neue Zertifikat gesetzt ist.



Stammzertifikat für ICG austauschen

Überblick

Mit UMS 6.06 oder höher können Sie das Root-Zertifikat für ein ICG austauschen, ohne die angeschlossenen Geräte manuell neu registrieren zu müssen. Allerdings kommt es zu einer kurzen Unterbrechung, wenn sich die Geräte neu verbinden, um auf das neue Zertifikat umzuschalten.

Umgebung

- ICG 2.02 oder höher
- UMS 6.06 oder höher
- IGEL OS 11.04.240 oder höher ist auf den Geräten installiert, oder die Upload-Quelle ist auf den Geräten verfügbar und konfiguriert. Weitergehende Informationen finden Sie unter Firmware-Update.

Anwendungsfälle

- Das Root-Zertifikat läuft in Kürze ab.
- Sie möchten die öffentliche CA ändern.
- Neue Sicherheitsregeln müssen implementiert werden, oder Algorithmen sind veraltet.

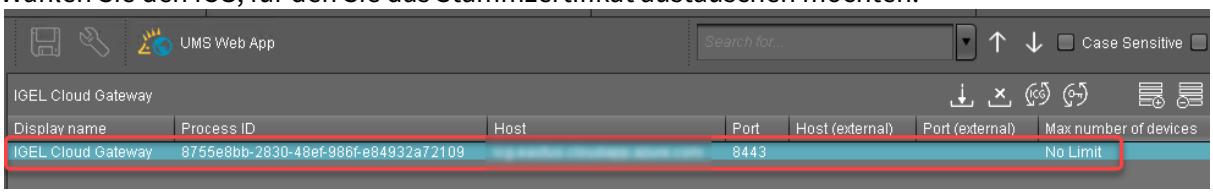
Anleitung

Der Vorgang umfasst die folgenden Schritte:

1. Gewünschtes Endzertifikat auswählen (see page 69)
2. Geräte aktualisieren (see page 71) (wo nötig)
3. Geräte neu starten (see page 76)
4. Keystore aktualisieren (see page 81)

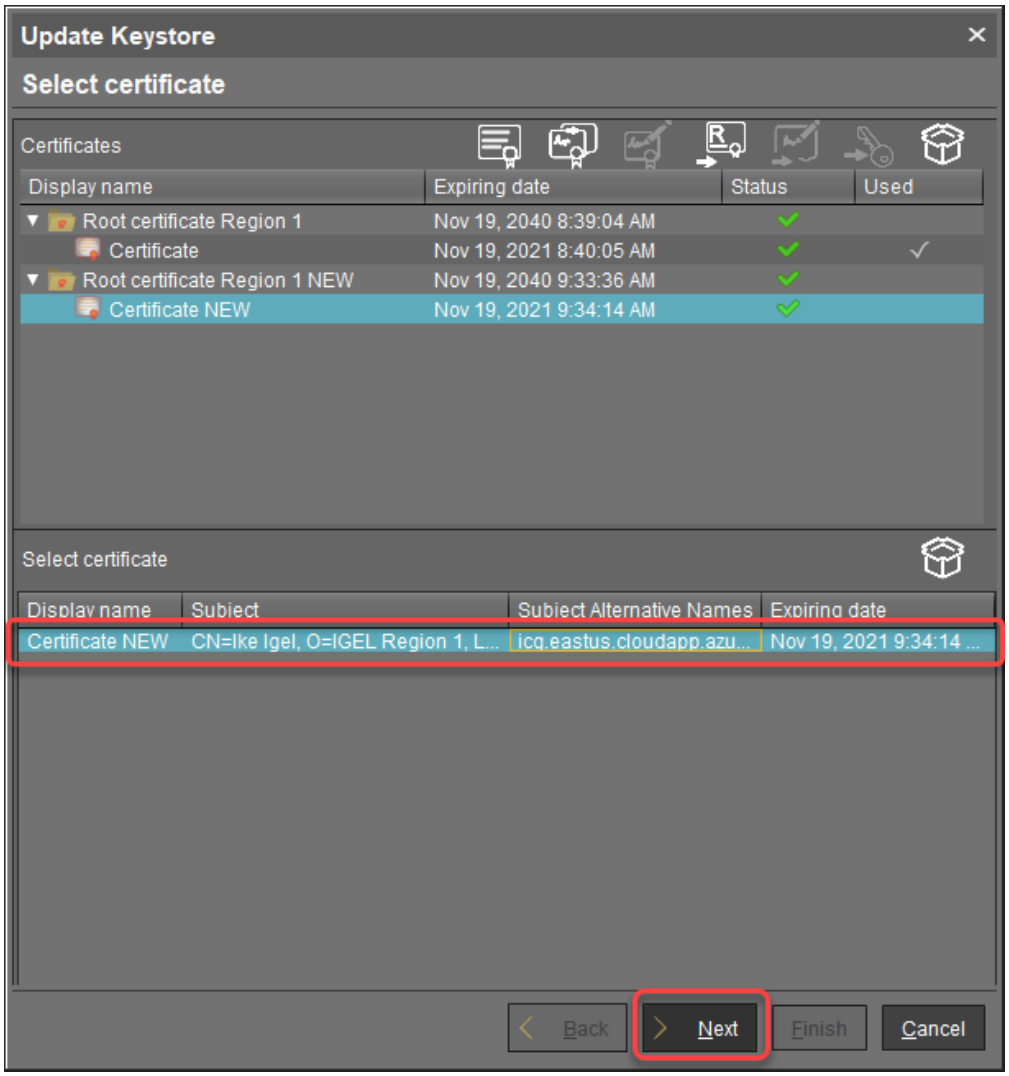
Gewünschtes Endzertifikat auswählen

1. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.
2. Wählen Sie den ICG, für den Sie das Stammzertifikat austauschen möchten.

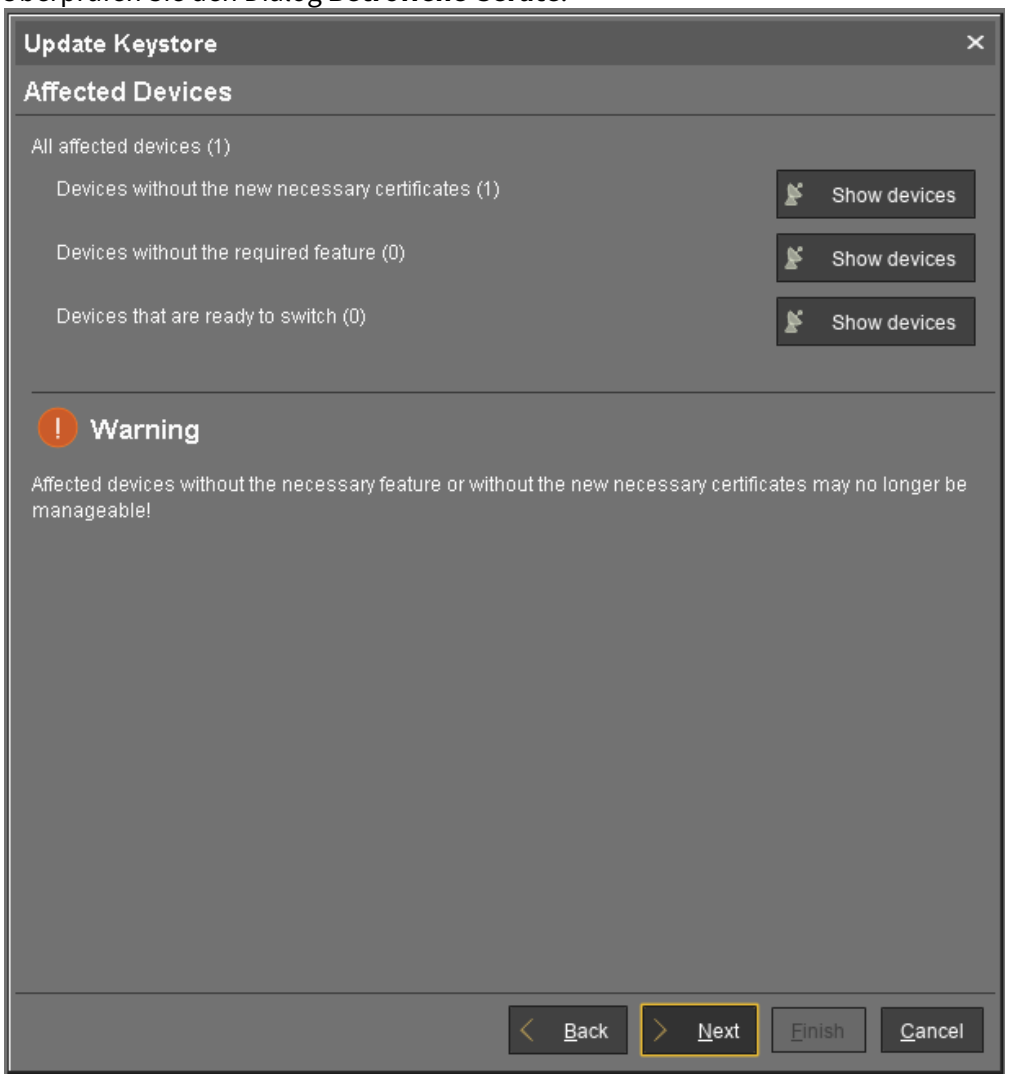


3. Klicken Sie  , um den Dialog **Keystore aktualiseren** zu öffnen.

4. Wählen Sie unter **Auswahl eines Zertifikats** das Zertifikat, das Sie in Zukunft verwenden wollen, und klicken Sie **Weiter**.



5. Überprüfen Sie den Dialog **Betroffene Geräte**.



Wählen Sie die entsprechende Methode gemäß den angezeigten Zahlen:

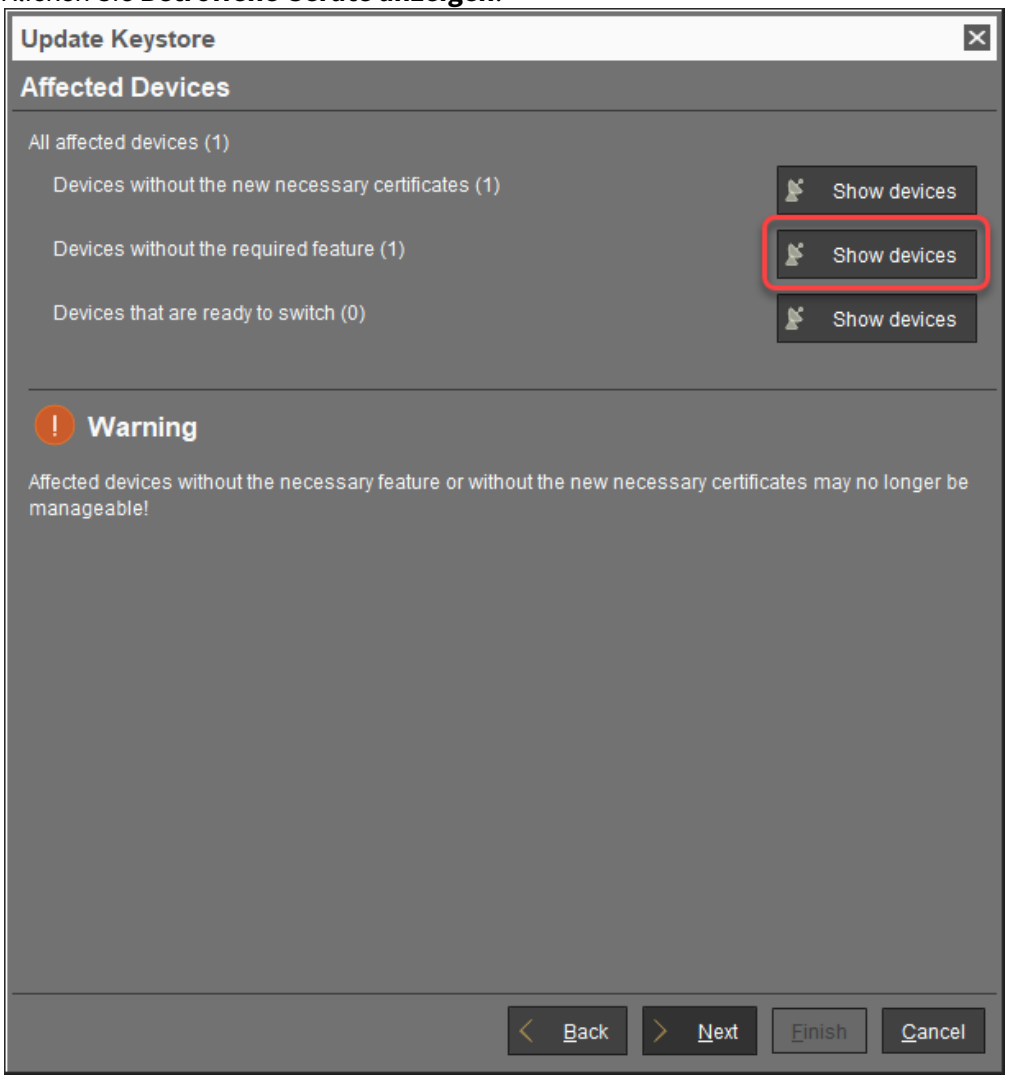
Geräte ohne die neuen benötigten Zertifikate ([Zahl])	Geräte ohne das benötigte Feature ([Zahl])	Wenn die 1. und die 2. Spalte wahr sind, fahren Sie fort mit...
≥ 1	≥ 1	Geräte aktualisieren (see page 71)
≥ 1	0	Geräte neu starten (see page 76)

Geräte aktualisieren

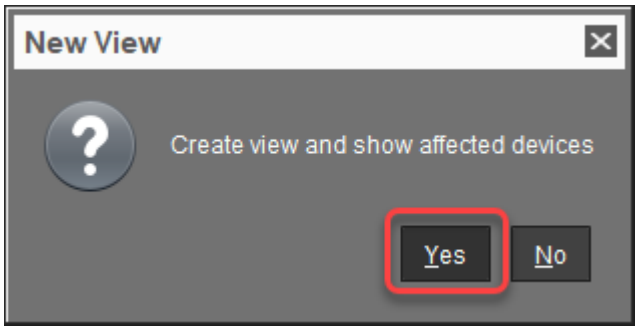
Die unter **Geräte ohne das benötigte Feature** aufgeführten Geräte sind nicht in der Lage, das ICG-Zertifikat auszutauschen und müssen auf IGEL OS 11.04.240 oder höher aktualisiert werden.

Um diese Geräte zu aktualisieren:

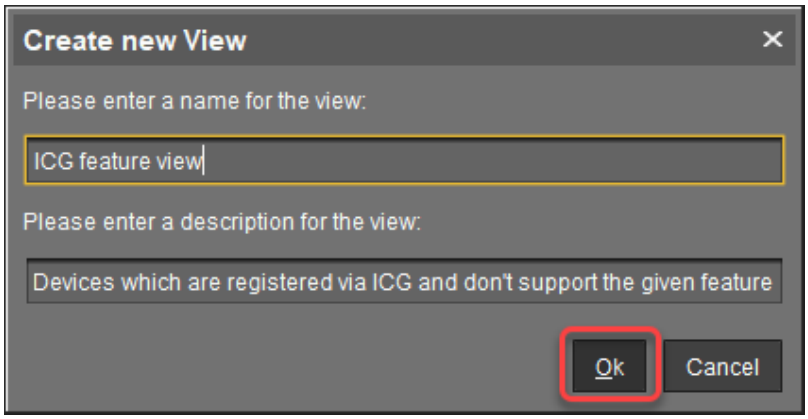
1. Klicken Sie **Betroffene Geräte anzeigen**.



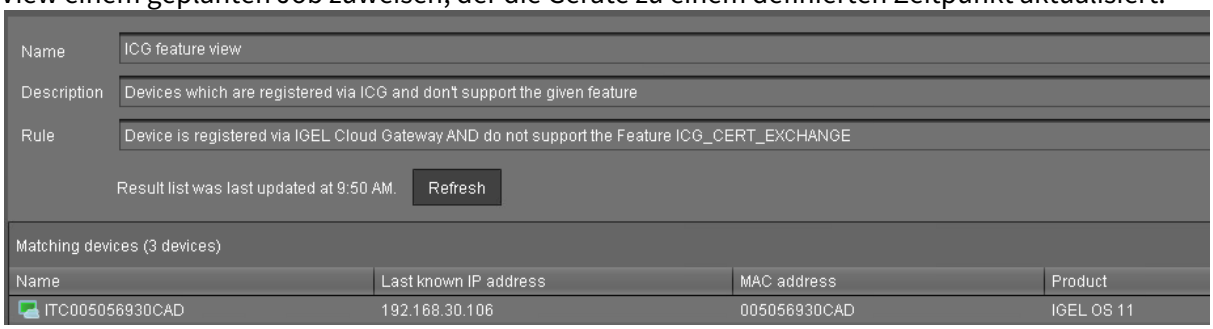
2. Klicken Sie im Bestätigungsdialog auf **Ja**, um eine View zu erstellen, die die zu aktualisierenden Geräte sammelt.



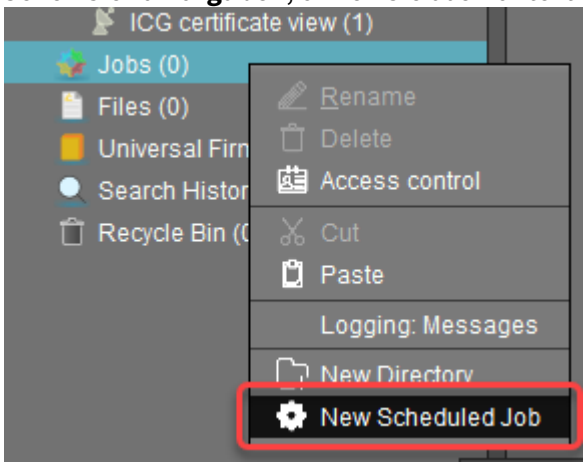
3. Überprüfen Sie im Dialog **Neue View erstellen** die vorausgefüllten Felder für Namen und Beschreibung und klicken Sie **Ok**.



Die View wird erstellt, und die UMS Konsole wechselt in die neu erstellte View. Wir werden diese View einem geplanten Job zuweisen, der die Geräte zu einem definierten Zeitpunkt aktualisiert.

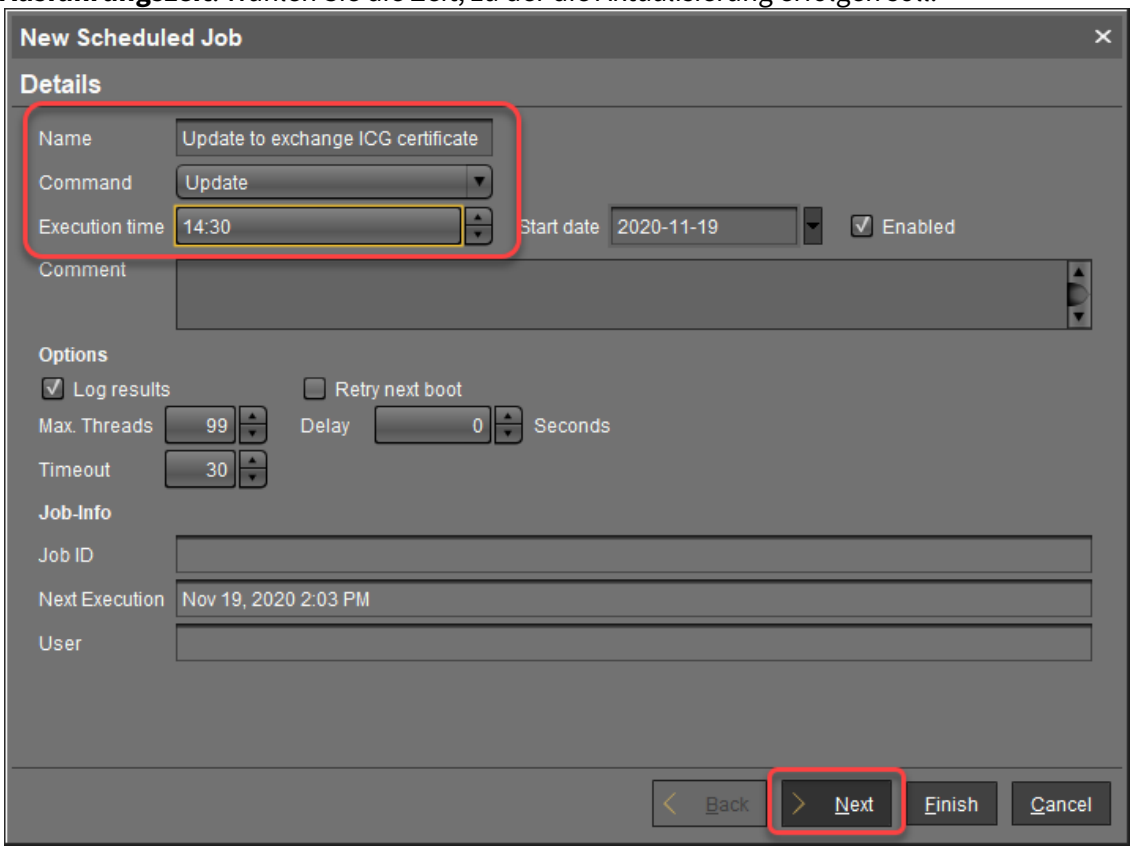


4. Gehen Sie zu **Aufgaben**, öffnen Sie das Kontextmenü und wählen Sie **Neue Aufgabe**.

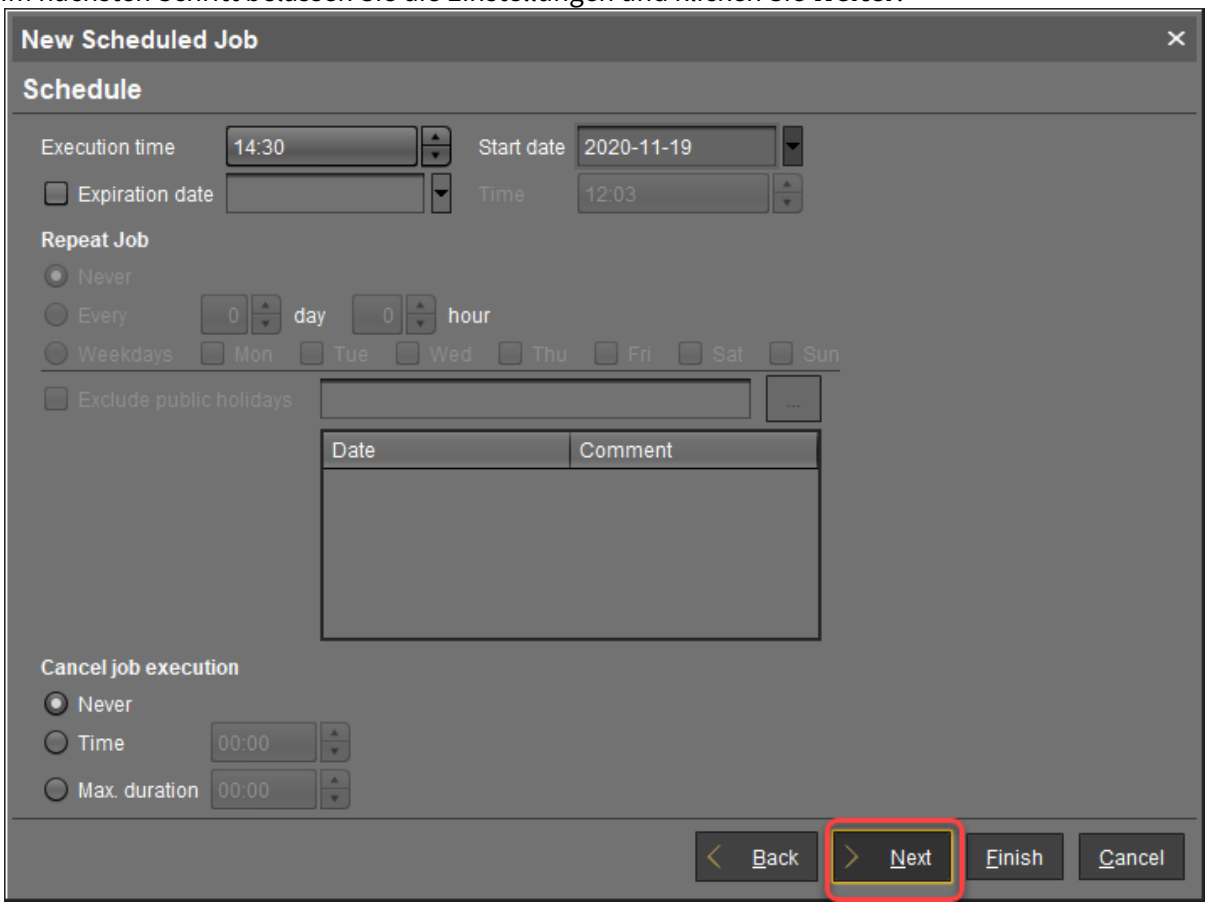


5. Ändern Sie im Fenster **Neue Aufgabe** die Einstellungen wie folgt und klicken Sie **Weiter**.
   - **Name**: Name für die Aufgabe
   - **Befehl**: Wählen Sie "Update".

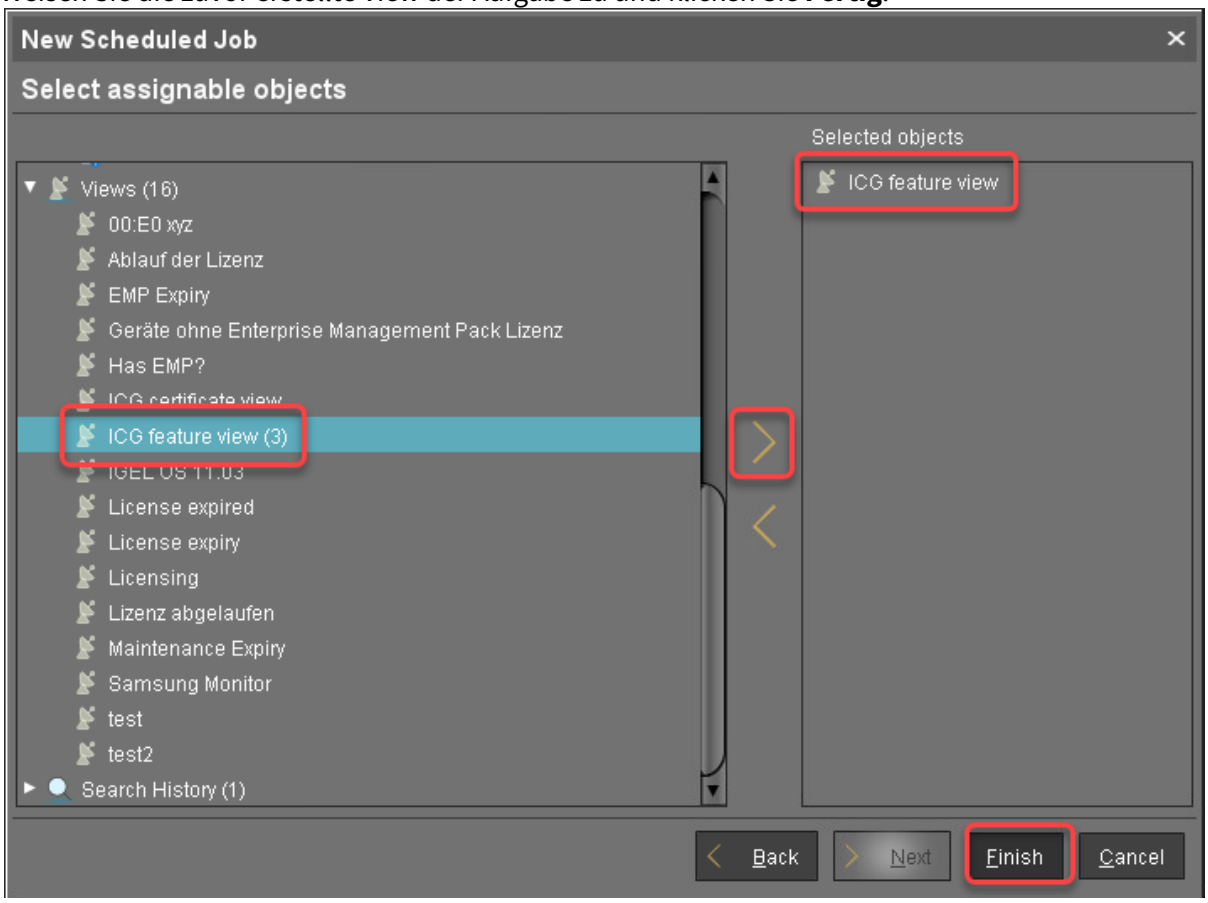
- **Ausführungszeit**: Wählen Sie die Zeit, zu der die Aktualisierung erfolgen soll.



6. Im nächsten Schritt belassen Sie die Einstellungen und klicken Sie **Weiter**.



7. Weisen Sie die zuvor erstellte View der Aufgabe zu und klicken Sie **Fertig**.



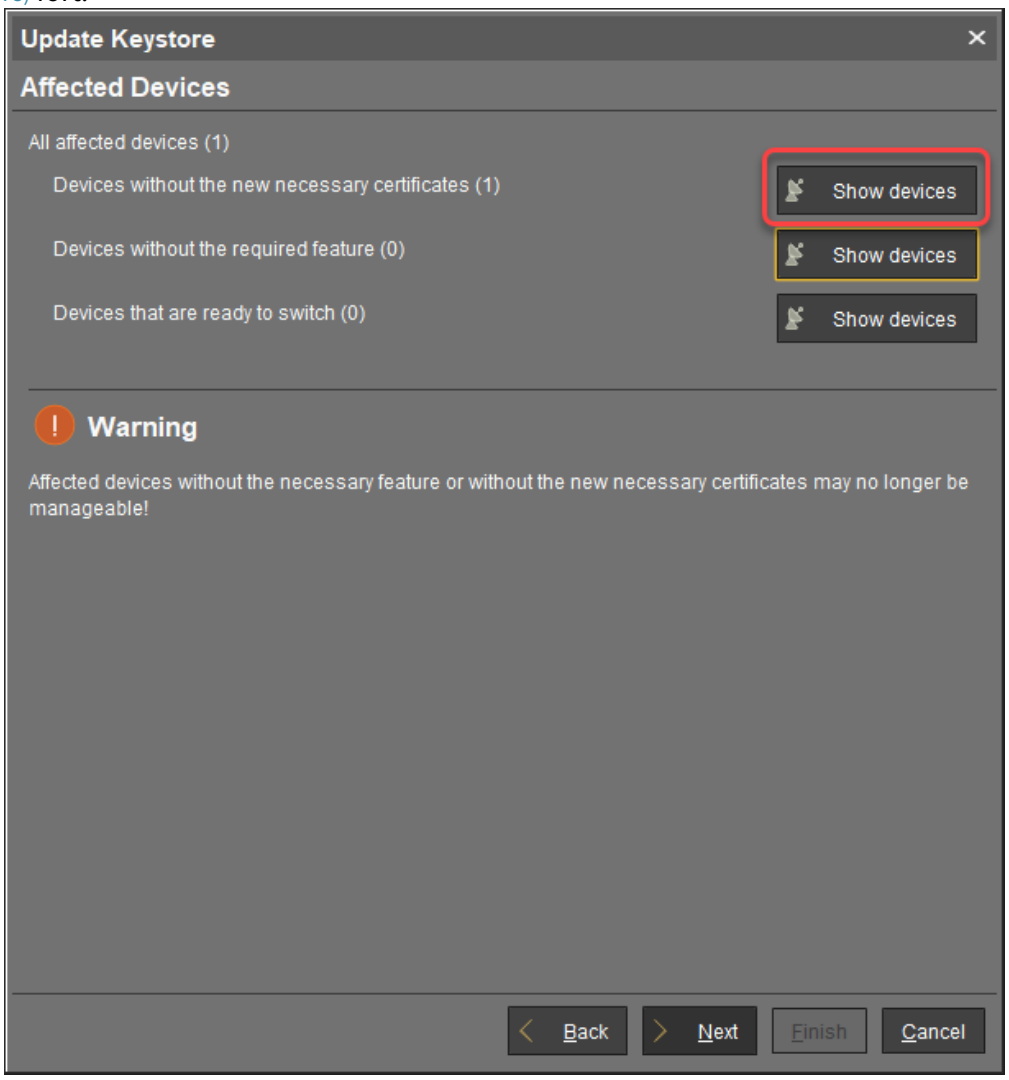
8. Stellen Sie sicher, dass IGEL OS 11.04.240 oder höher verfügbar ist und die Upload-Quelle auf den Geräten verfügbar und konfiguriert ist; weitere Informationen finden Sie unter Firmware-Update. Die Firmware wird zur angegebenen Zeit aktualisiert.
9. Wenn die Geräte aktualisiert sind, fahren Sie mit Geräte neu starten (see page 76) fort.

Geräte neu starten

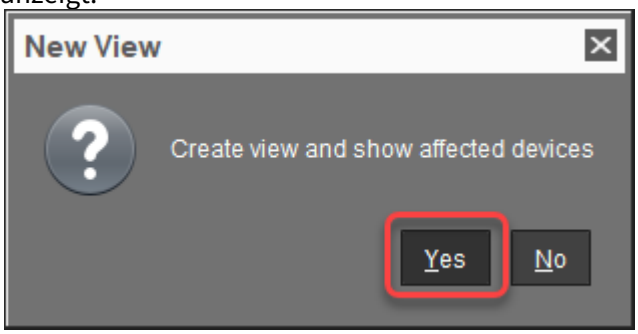
Wenn die Geräte aktualisiert sind, verfügen sie über die erforderliche Funktion, um das neue ICG-Stammzertifikat zu erhalten. Sie erhalten das neue Root-Zertifikat beim Neustart, für den wir einen geplanten Job erstellen werden.

1. Wenn Sie nicht bereits eine View angelegt haben (siehe Geräte aktualisieren (see page 71)), klicken Sie **Betroffene Geräte anzeigen**. Wenn die View bereits existiert, fahren Sie mit Schritt 4 (see page

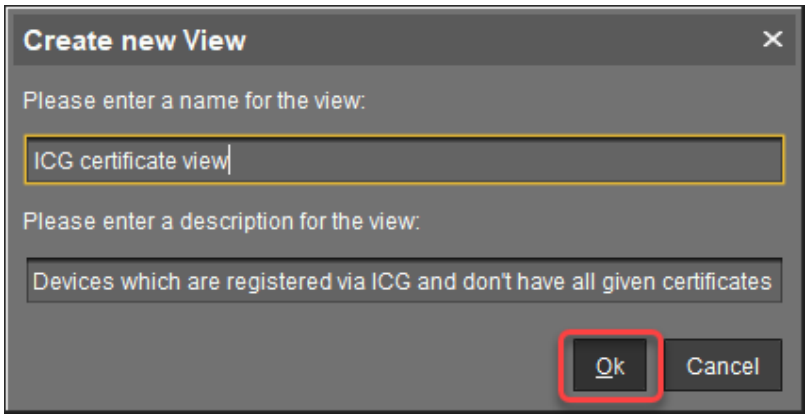
78) fort.



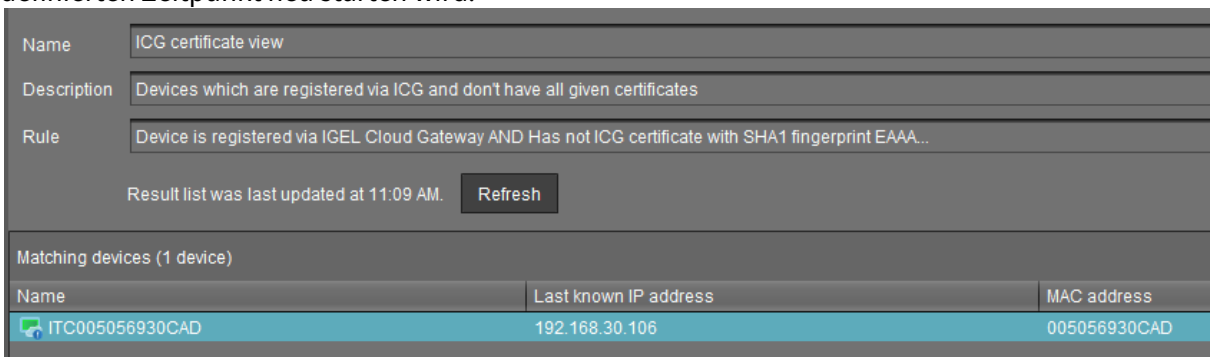
2. Klicken Sie im Bestätigungsdialog auf **Ja**, um eine View zu erzeugen, die die betroffenen Geräte anzeigt.



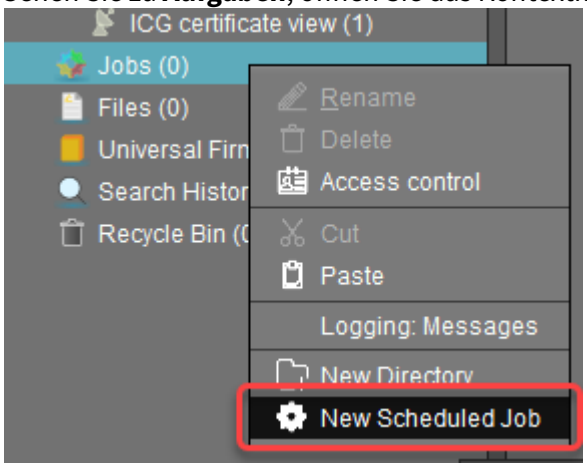
3. Überprüfen Sie im Dialogfeld **Neue View erstellen** den vorausgefüllten Namen und die Beschreibung, und klicken Sie auf **OK**.



Die View wird erstellt, und die UMS Konsole wechselt in die neu erstellte View. Wir werden diese View einem geplanten Job zuweisen, der die in dieser View gesammelten Geräte zu einem definierten Zeitpunkt neu starten wird.

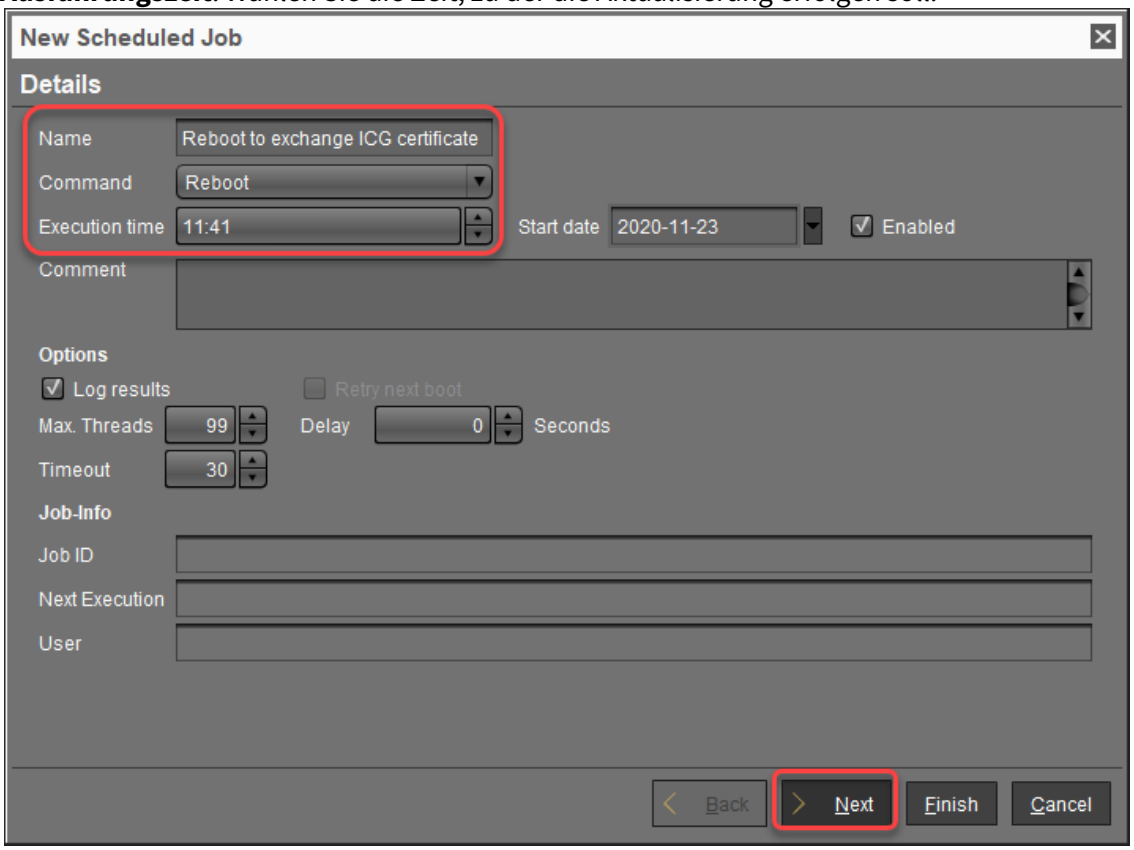


4. Gehen Sie zu **Aufgaben**, öffnen Sie das Kontextmenü und wählen Sie **Neue Aufgabe**.

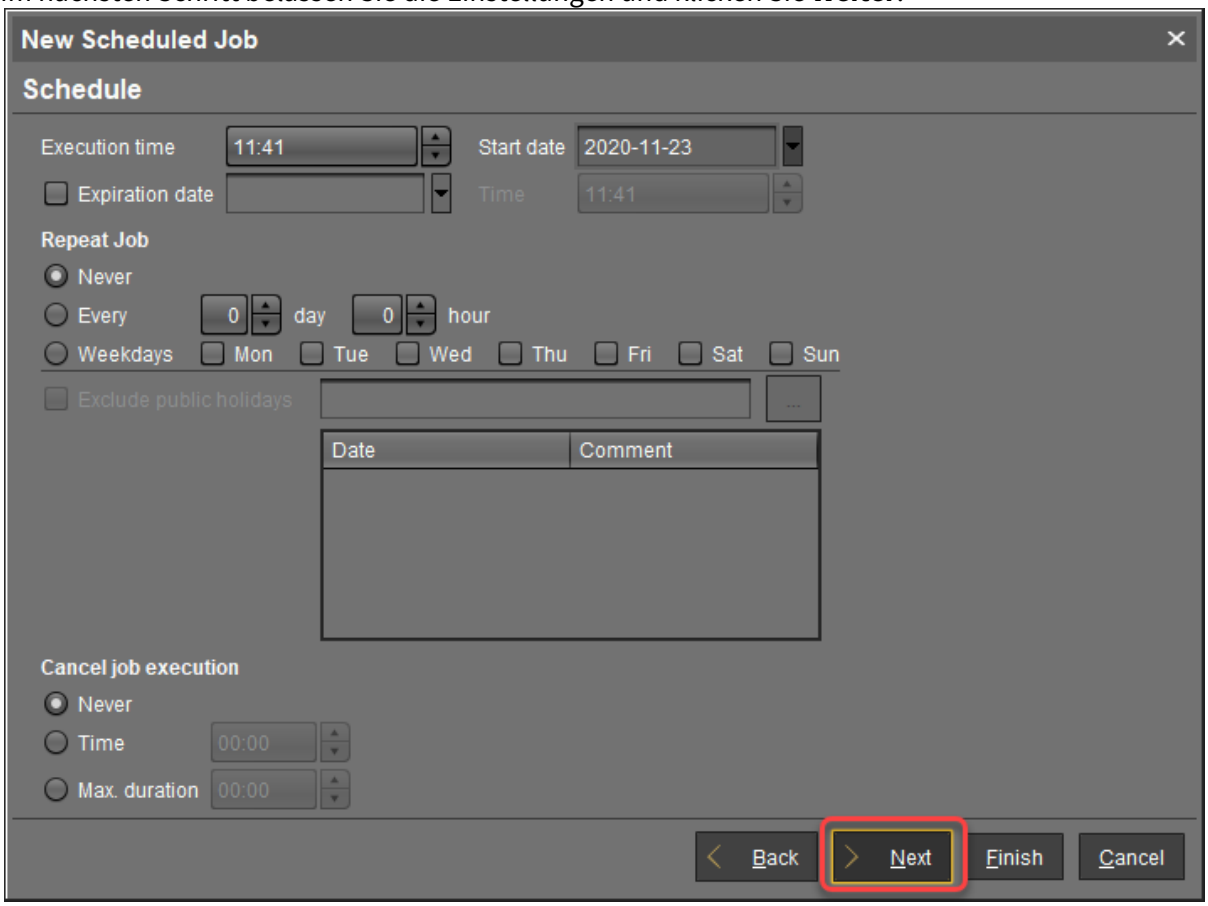


5. Ändern Sie im Fenster **Neue Aufgabe** die Einstellungen wie folgt und klicken Sie **Weiter**.
   - **Name**: Name für die Aufgabe
   - **Befehl**: Wählen Sie "Neustart".

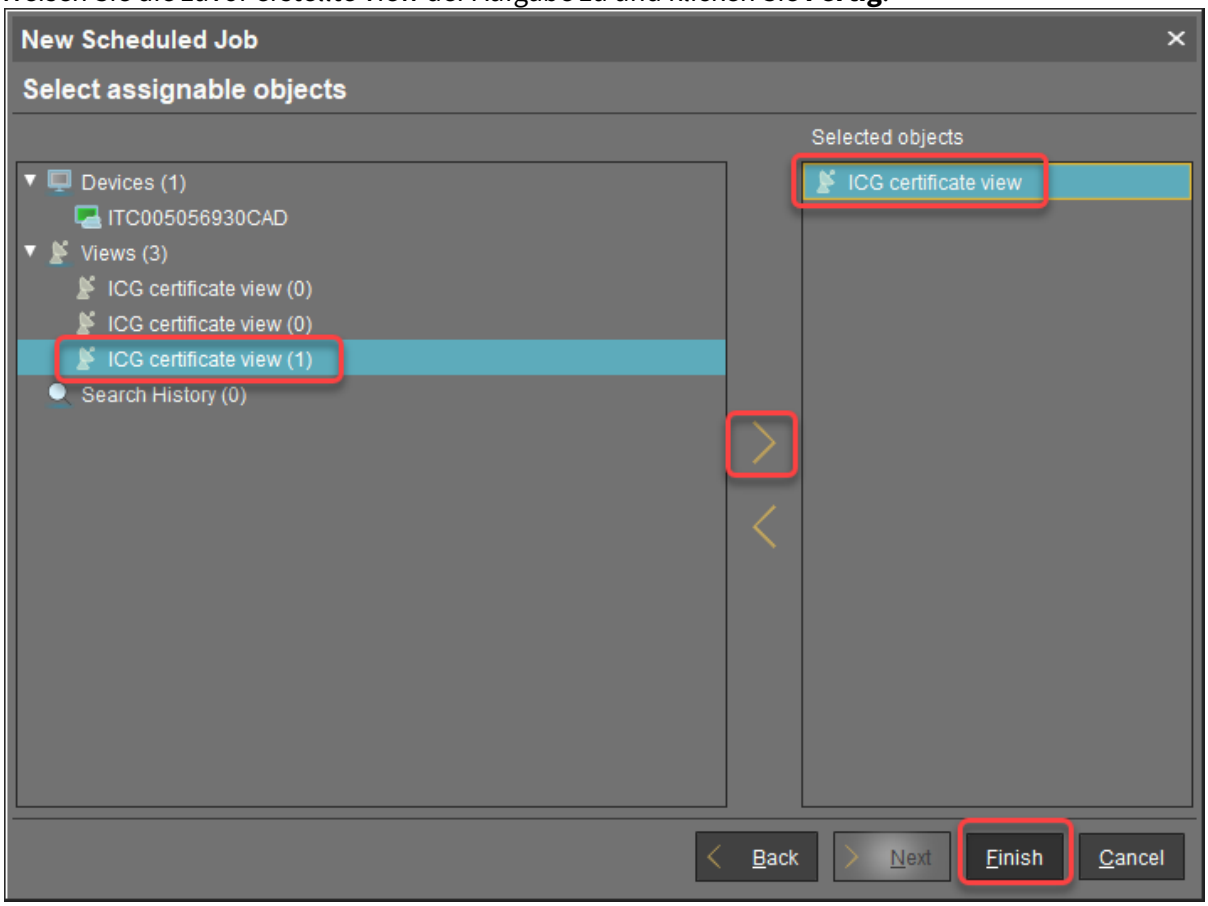
- **Ausführungszeit**: Wählen Sie die Zeit, zu der die Aktualisierung erfolgen soll.



6. Im nächsten Schritt belassen Sie die Einstellungen und klicken Sie **Weiter**.



7. Weisen Sie die zuvor erstellte View der Aufgabe zu und klicken Sie **Fertig**.

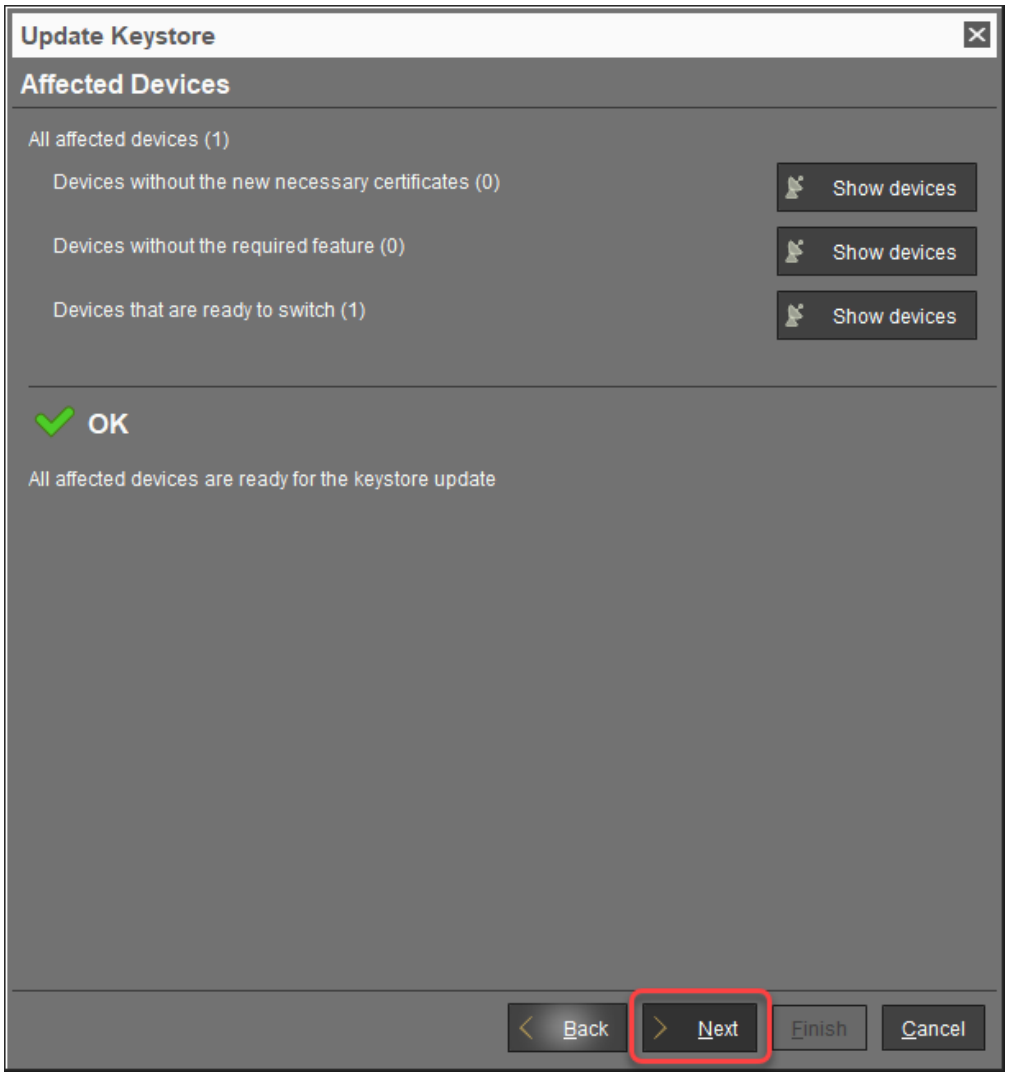


Beim Neustart erhalten die Geräte alle ICG-Zertifikate von der UMS; danach sind sie bereit, auf das neue Zertifikat umzuschalten.

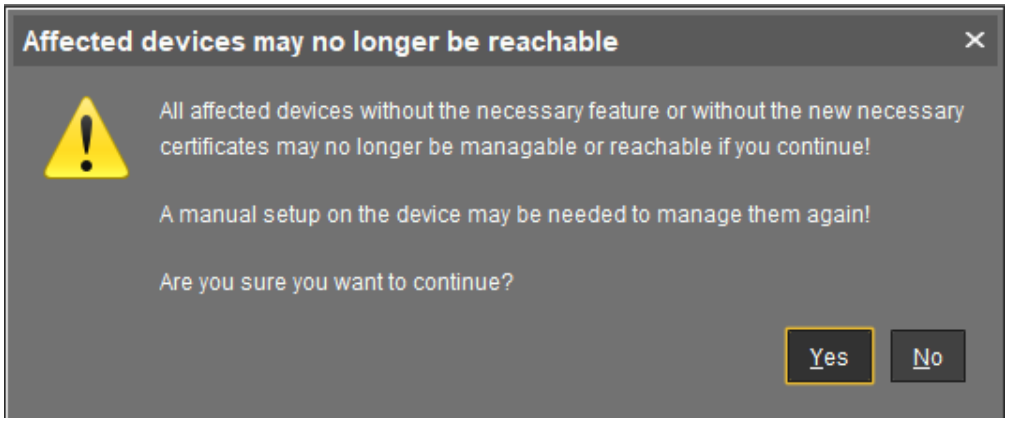
8. Fahren Sie mit Keystore aktualisieren (see page 81) fort.

Keystore aktualisieren

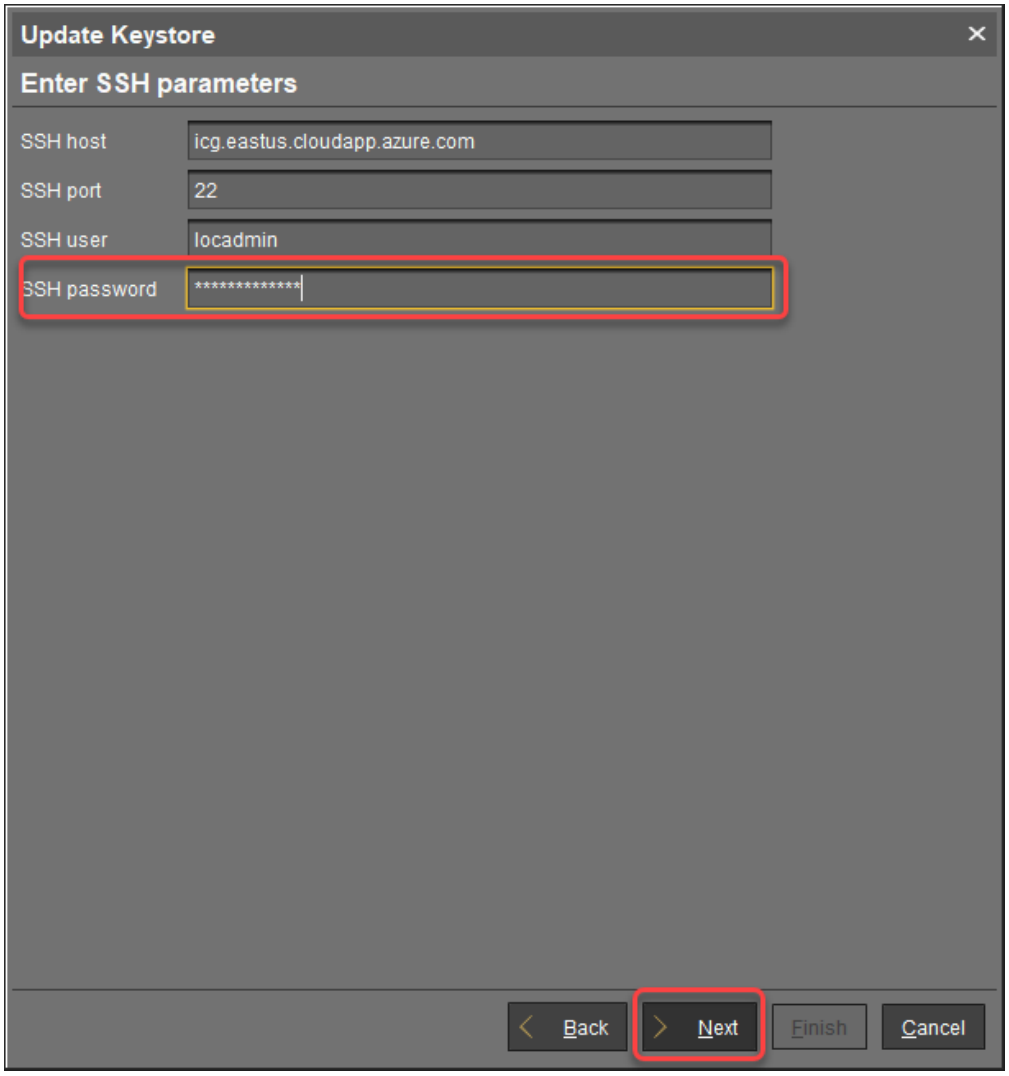
1. Um zu überprüfen, ob die Geräte bereit sind, gehen Sie zurück zu **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**, klicken Sie auf  , um den Dialog **Keystore aktualisieren** zu öffnen, wählen Sie das neue Zertifikat aus, klicken Sie auf **Weiter** und sehen Sie sich die angezeigten Zahlen an. Wenn die Ausgabe wie folgt aussieht, klicken Sie auf **Weiter**.



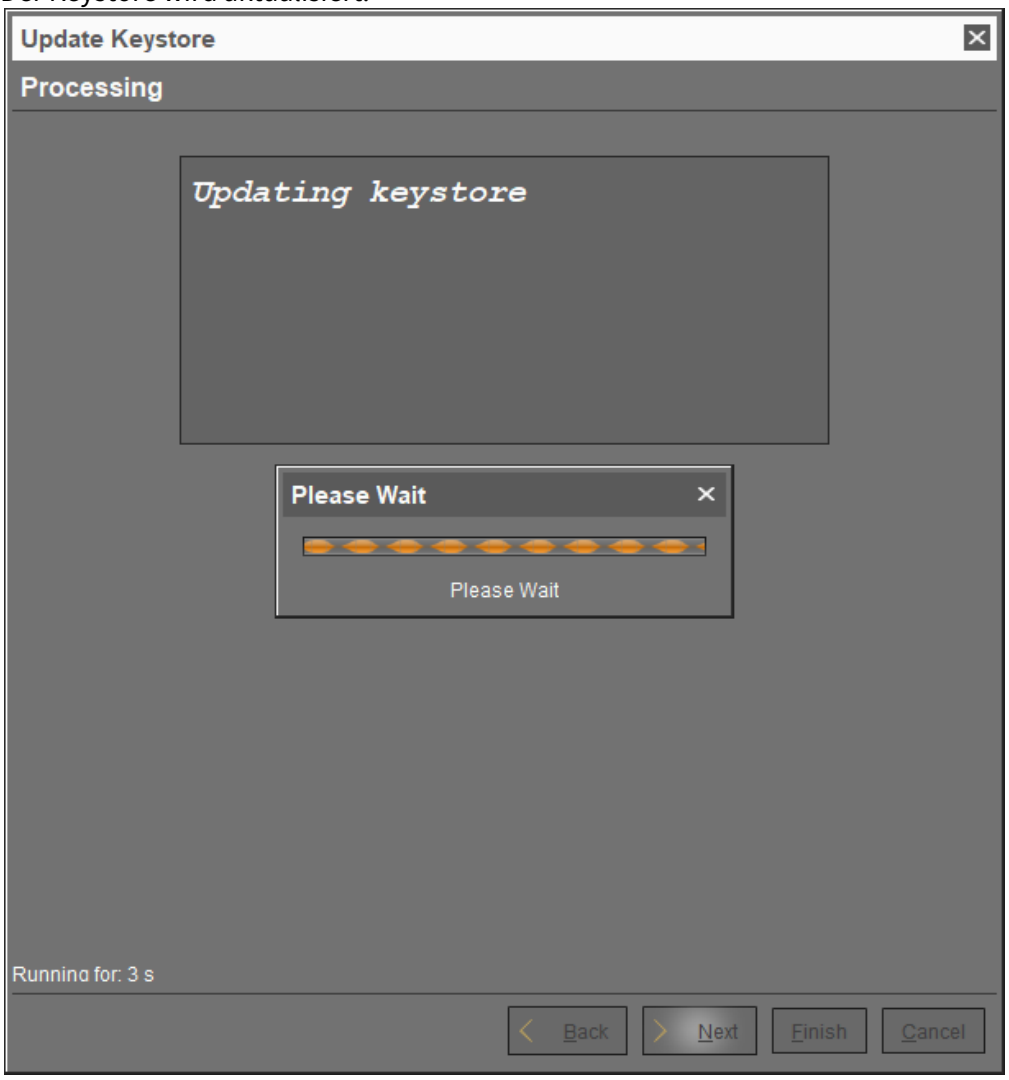
Wenn die folgende Warnmeldung erscheint, sollten Sie überprüfen, ob alle Geräte erfolgreich aktualisiert wurden. Wenn Sie auf **Ja** klicken, um fortzufahren, können die Geräte, die nicht über die erforderliche Funktion (Firmware) oder das Zertifikat verfügen, nicht mehr über ICG erreichbar sein.



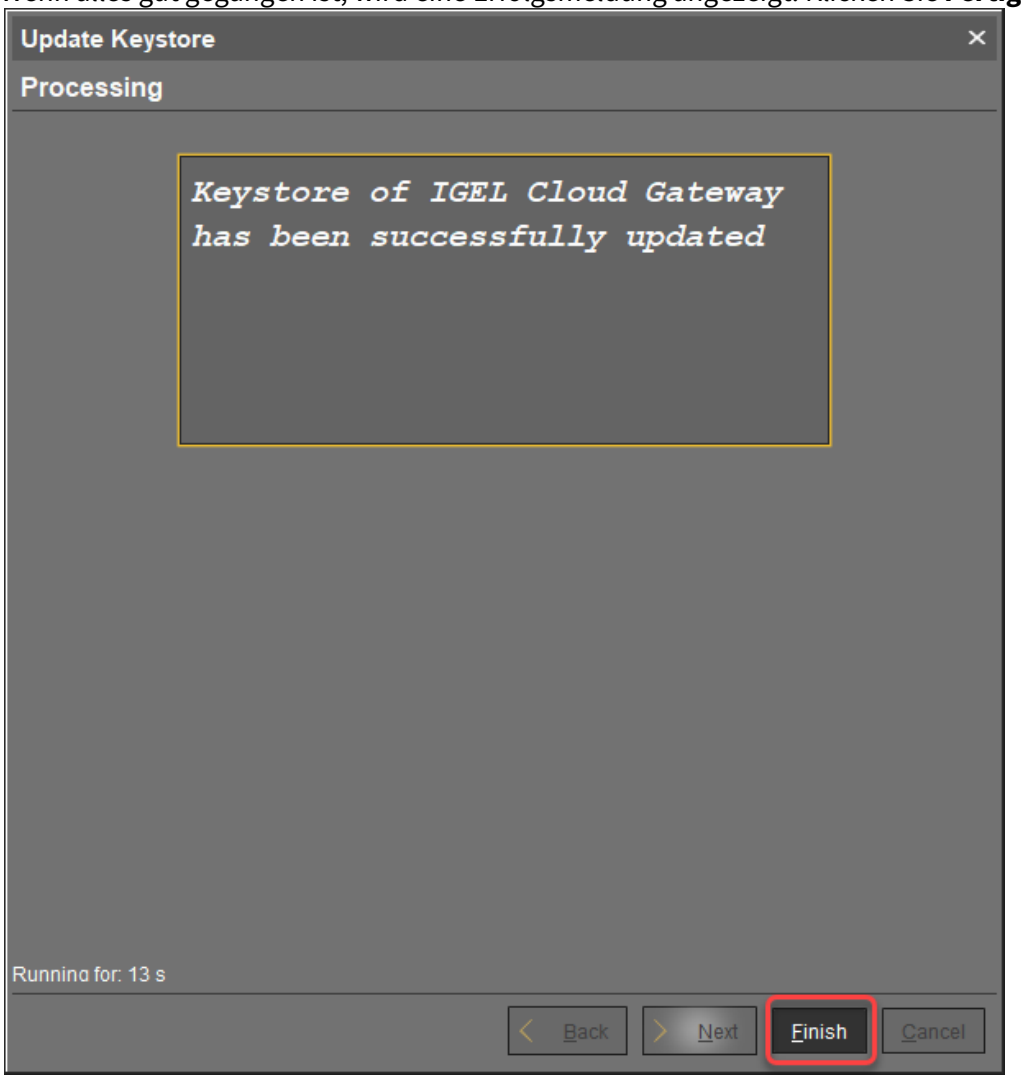
2. Geben Sie das Passwort für den **SSH-Benutzer** ein, der auf dem ICG-Server existiert. Dies ist das gleiche Passwort, das bei der Installation von ICG verwendet wurde. Klicken Sie anschließend auf **Weiter**.



Der Keystore wird aktualisiert.



3. Wenn alles gut gegangen ist, wird eine Erfolgsmeldung angezeigt. Klicken Sie **Fertig**.



Endgerät zu einem ICG verschieben

Überblick

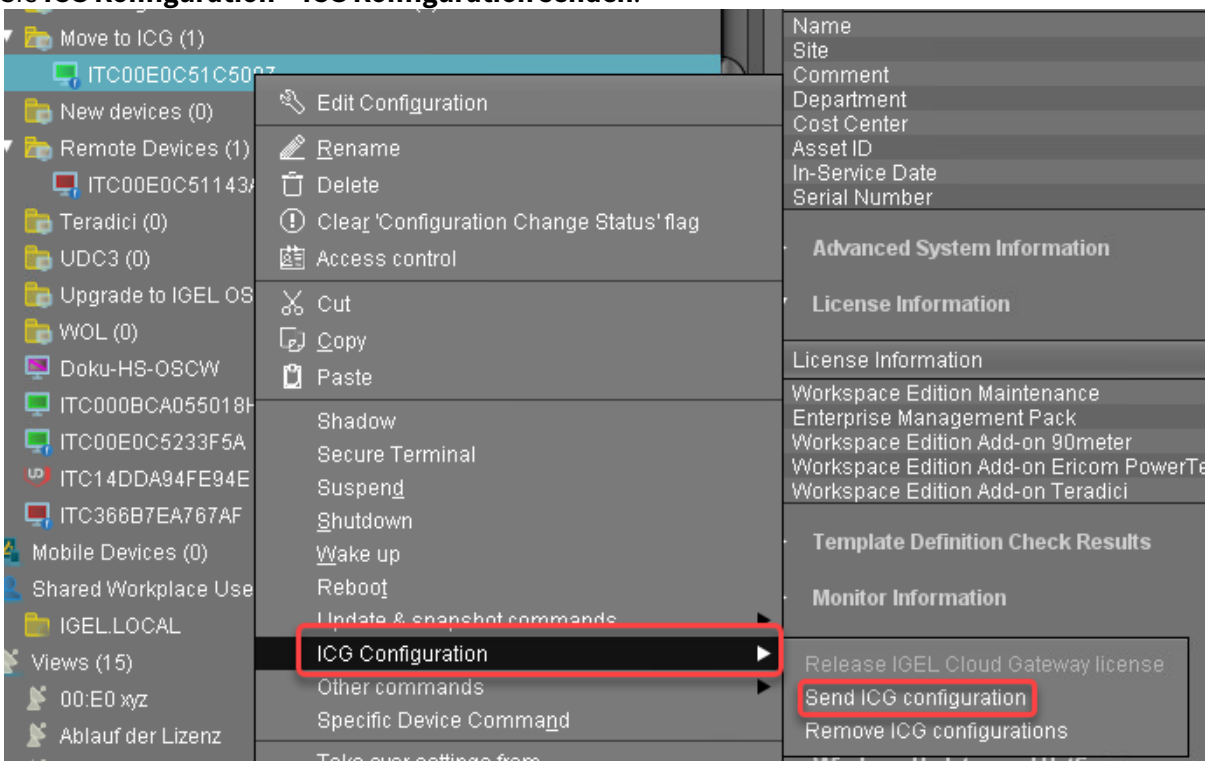
Sie können ein Endgerät aus dem lokalen Netzwerk an einen entfernten Standort verschieben, wo es über ICG verbunden wird. Außerdem können Sie ein Endgerät von einem ICG-Server auf einen anderen verschieben.

Umgebung

- UMS 6.06 oder höher
- ICG 2.02 oder höher
- IGEL OS 11.04.240 oder höher

Anleitung

1. Markieren Sie alle Geräte, die Sie verschieben möchten, öffnen Sie das Kontextmenü und wählen Sie **ICG Konfiguration > ICG Konfiguration senden**.



2. Wählen Sie im Dialog **Sende Konfigurationen eines ICG** den ICG aus, in den Sie die Geräte verschieben möchten, und klicken Sie auf **ICG auswählen**:

Wenn alles gut gegangen ist, verbinden sich die Geräte mit dem angegebenen ICG. Wenn das ICG in diesem Moment nicht erreichbar ist, bleibt die ICG-Konfiguration unverändert und die Geräte bleiben mit dem lokalen UMS-Netzwerk oder dem alten ICG verbunden.

Endgerät von ICG entfernen

Überblick

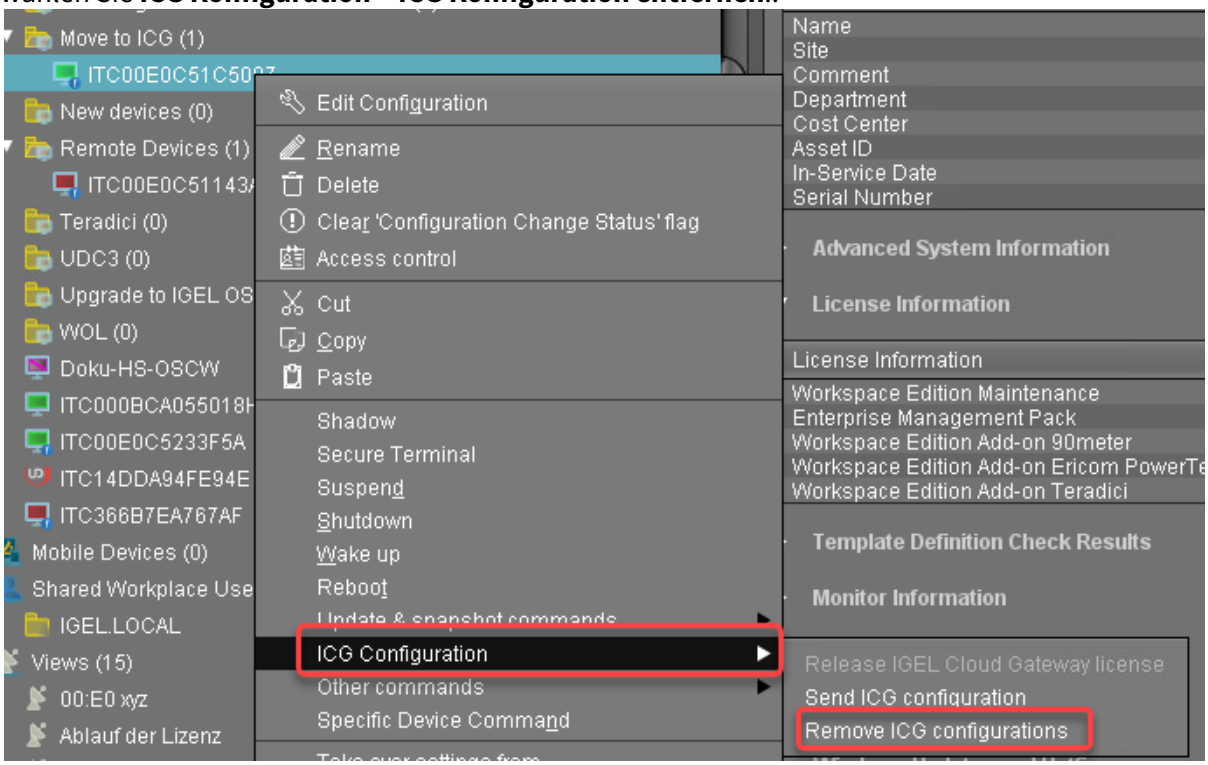
Wenn ein Endgerät mit einer ICG-Konfiguration mit dem lokalen UMS-Netzwerk verbunden wird, wechselt es automatisch zur lokalen UMS-Verbindung. Wenn Sie verhindern möchten, dass das Gerät den ICG weiterhin verwendet, können Sie seine ICG-Konfiguration entfernen.

Umgebung

- UMS 6.06 oder höher
- ICG 2.02 oder höher
- IGEL OS 11.04.240 oder höher

Anleitung

1. Stellen Sie sicher, dass alle Endgeräte mit dem lokalen UMS Netzwerk verbunden sind.
2. Wählen sie alle Geräte, die Sie von einem ICG entfernen wollen, öffnen Sie das Kontextmenü und wählen Sie **ICG Konfiguration > ICG Konfiguration entfernen**..



Das Endgerät wird vom ICG entfernt.

Verwendete Netzwerk-Ports

ICG nimmt eingehende Verbindungen auf dem TCP-Port 8443 an, sowohl von UMS als auch von Endgeräten. Dieser Port lässt sich ändern:

- auf dem ICG Server im interaktiven Installer
- in UMS unter **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.

ICG-Daemon steuern

ICG wird automatisch bei Booten des Systems gestartet sowie unmittelbar nach seiner Installation. Im Betrieb können Sie ICG mit den folgenden Kommandos steuern.

> Verwenden Sie exklusiv Systemd- oder SysVInit-Kommandos. Beispielsweise können Sie einen mit Systemd gestarteten ICG-Prozess nicht mit einem SysVInit-Kommando neu starten.

> Auch wenn die Kommandos rasch ablaufen, benötigt ICG im Hintergrund etwa 10 bis 15 Sekunden, um beispielsweise zu starten oder anzuhalten.

Auf Installationen mit Systemd (empfohlen)

Führen Sie diese Kommandos als Root aus:

- ICG-Status anzeigen: `systemctl status tomcat`
- ICG starten: `systemctl start tomcat`
- ICG neu starten (nach Konfigurationsänderungen): `systemctl restart tomcat`
- ICG anhalten: `systemctl stop tomcat`

Auf Systemen mit SysVInit

Führen Sie diese Kommandos als Root aus:

- ICG starten: `/etc/init.d/tomcat start`
- ICG neu starten (nach Konfigurationsänderungen): `/etc/init.d/tomcat restart`
- ICG anhalten: `/etc/init.d/tomcat stop`

Optional: DNS TXT Eintrag für ICG-Server

> ⚠ Diese Methode funktioniert nur bei Endgeräten mit IGEL OS 11.
> Um Geräte mit IGEL OS 12 über eine E-Mail-Adresse zu registrieren, verwenden Sie den Onboarding Service. Weitere Informationen finden Sie unter Onboarding IGEL OS 12 Devices.

Sie können dem Anwender die Eingabe des ICG-Servers erleichtern, indem Sie Ihrer Domain einen DNS TXT Eintrag für den Server hinzufügen:

▶ Fügen Sie einen TXT Eintrag `igel-cloud-gateway` mit dem Inhalt `https://[ICG IP address]:8443/usg/endpoint` hinzu.

Gibt der Anwender nun die E-Mail-Adresse `user@example.com` als Serveradresse im ICG Agent Setup an, schlägt das Setup auf dem Nameserver für `example.com` nach und findet diesen Eintrag mit der Adresse des Gateway.

ICG FAQ

Can I Use Active Directory from a Remote Device?

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

ICG How-Tos

Using IGEL Cloud Gateway on Microsoft Azure Marketplace

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Linux-Rechner für die Installation von IGEL Cloud Gateway (ICG) vorbereiten

Dieses Dokument beschreibt, wie Sie einen Host-Computer für die Installation von IGEL Cloud Gateway (ICG) vorbereiten. In diesem Beispiel wird Ubuntu-Server 18.04. LTS - 64-Bit verwendet.

Benutzer einrichten und Root werden

1. Erstellen Sie den ersten Benutzer mit einem Namen Ihrer Wahl. Der erste Benutzer, der auf dem Ubuntu-Server angelegt wird, hat die Berechtigung für `sudo.`

   > **Benutzername "icg" ist reserviert**
   >
   > Verwenden Sie als Benutzernamen für den Remote Installer nicht "icg"; dies ist der Benutzername, unter dem der Tomcat-Server läuft.

2. Geben Sie `sudo su` und das Benutzerpasswort ein, um Systemadministrator (`root)` zu werden.

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

Statische IP-Adresse festlegen

Sie können entweder DHCP verwenden, um eine statische IP-Adresse einzustellen, oder die IP-Adresse auf dem Server über Netplan mit einer YAML-Beschreibung der gewünschten Netzwerkschnittstelle konfigurieren.

Um eine statische IP-Adresse über Netplan einzustellen:

1. Geben Sie `ip addr` ein, um den Namen der Netzwerkschnittstelle herauszufinden.

```
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
```

   Im oberen Beispiel, lautet die Netzwerkschnittstelle `ens160.`

2. Um die Netzwerkkonfigurationsfähigkeiten von cloud-init zu deaktivieren, schreiben Sie eine Datei: `nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg`

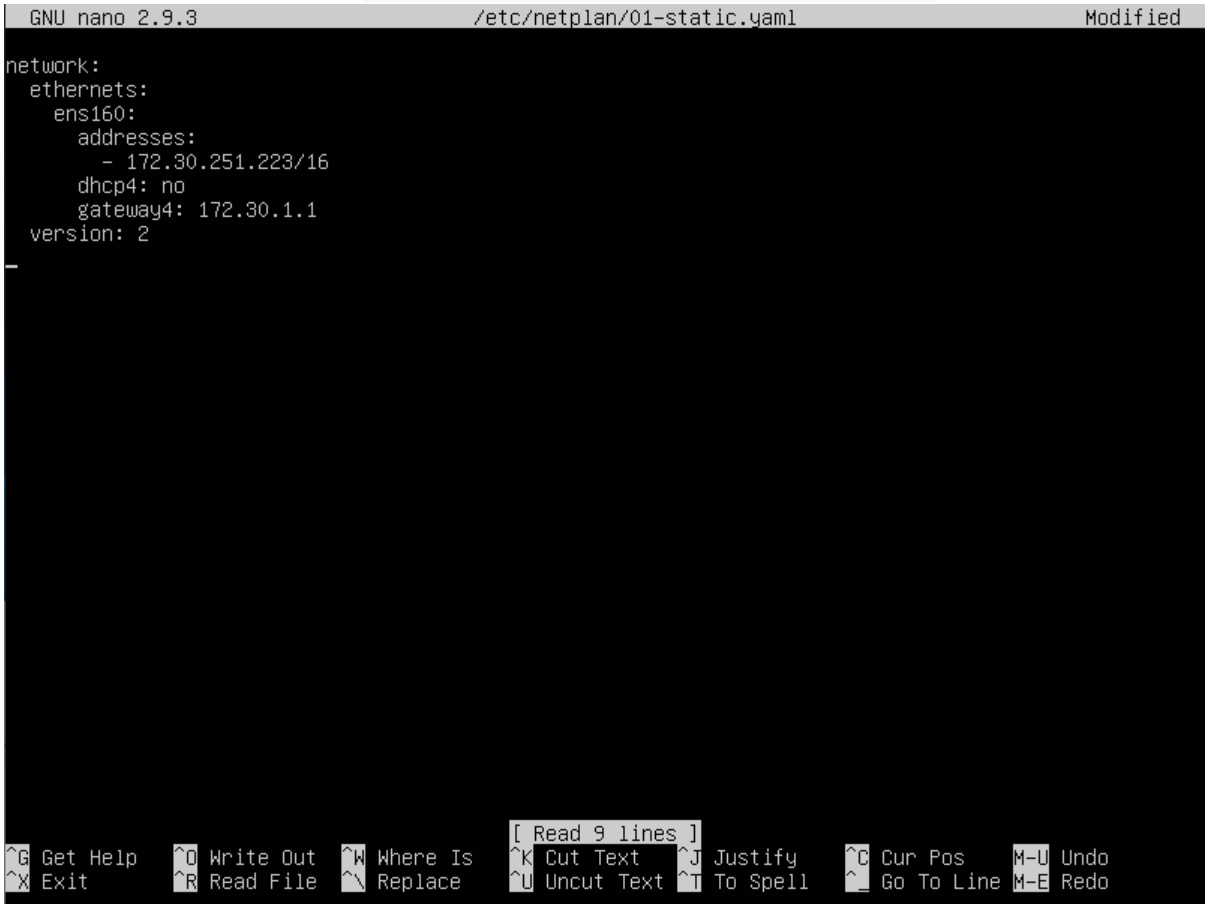
```
root@doc-hs-icg:/etc/netplan# nano /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg
```

   mit folgendem Inhalt:

```
network: {config: disabled}
```

3. Sichern Sie die Datei, in dem Sie [Strg] + [O] und dann [Enter] drücken.
4. Drücken Sie [Strg] + [X] um den Editor zu verlassen.

5. Erstellen Sie die YAML-Datei: `nano /etc/netplan/01-static.yaml`

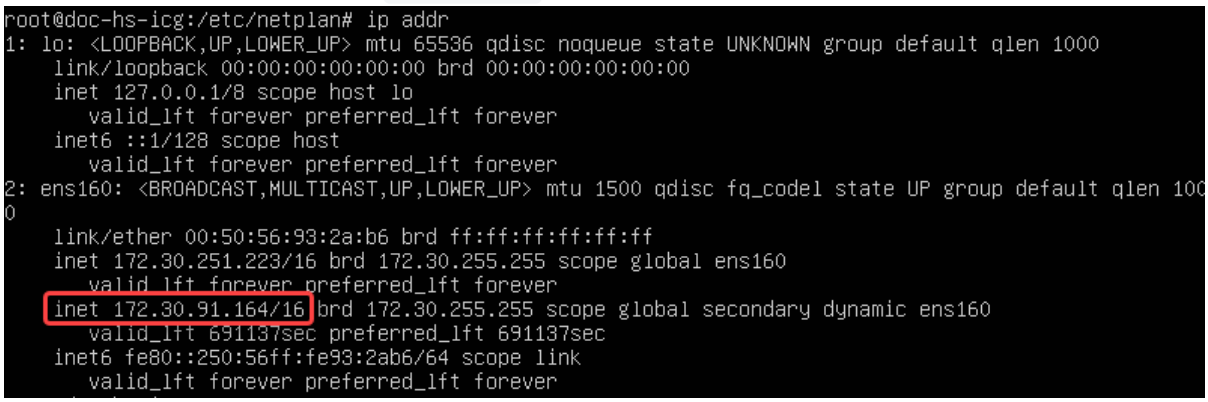


> Bei der Bearbeitung von YAML:
> - Verwenden Sie zwei Leerzeichen, um Zeilen einzurücken
> - Lassen Sie am Ende von Zeilen keine Leerzeichen oder Tabs

6. Speichern Sie die Datei und verlassen Sie den Editor.
7. Übernehmen Sie Ihre Konfiguration mit `netplan apply`. Beachten Sie eventuelle Fehlermeldungen.

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

8. Überprüfen Sie mit dem Befehl `ip addr,` ob die IP-Adresse erfolgreich eingestellt wurde.



Apache Tomcat nur für TLS 1.2 konfigurieren

Bitte beachten Sie das Folgende, besonders wenn Sie spezielle Richtlinien oder andere Komponenten zwischen den Geräten und der IGEL Universal Management Suite (UMS) oder dem IGEL Cloud Gateway (ICG) verwenden:

- IGEL OS 12-Geräte verwenden TLS 1.3. Nur TLS 1.2 ist nicht möglich.
- IGEL OS 11-Geräte verwenden TLS 1.2

Sowohl der UMS Server als auch das ICG sind standardmäßig so konfiguriert, dass sie Apache Tomcat mit TLS 1.2 und TLS 1.3 unterstützen.

Zertifikatsverwaltung

Sie können das ICG Zertifikat mit dem ICG Keystore Update Wizard verlängern.

Voraussetzungen

- UMS 5.09.100 oder höher
- Ein ICG-Keystore, den Sie aktualisieren möchten.
- SSH-Root-Zugriff auf den Host, auf dem das ICG läuft; ab UMS 5.09.110 genügt es, wenn der SSH-Benutzer über sudo-Rechte verfügt.

Der ICG Keystore Update Wizard vereinfacht das Update eines abgelaufenen ICG-Keystores auf einen neuen.

Um einen Keystore zu aktualisieren, gehen Sie wie folgt vor:

1. Starten Sie die UMS Konsole.

2. Gehen Sie unter **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway**.

3. Wenn Ihr signiertes Zertifikat abgelaufen ist, erstellen Sie ein neues signiertes Zertifikat:
   a. Wählen Sie das entsprechende Root-Zertifikat aus, öffnen Sie das Kontextmenü und wählen Sie **signiertes Zertifikat generieren**.
   b. Geben Sie die erforderlichen Daten ein und klicken Sie **Ok**.

4. Wählen Sie das signierte Zertifikat aus, das verwendet werden soll. Wenn Sie diesen Schritt weglassen, wird im nächsten Schritt eine Fehlermeldung angezeigt.

5. Gehen Sie unter **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.

6. Klicken Sie oben rechts in der Symbolleiste auf  .
   Der ICG Keystore Update Wizard wird geöffnet.

7. Wählen Sie den Keystore aus, den Sie auf den ICG-Server übertragen möchten und klicken Sie auf **Weiter**.

8. Geben Sie den SSH-Verbindungsparameter ein:
   - **SSH Host:** Der Host, auf dem das ICG läuft (Standard: `localhost`)
   - **SSH Port:** SSH Port (Standard: `22`)

   > Der SSH-Benutzer muss über einen Root-Zugang verfügen.
   > UMS 5.09.110 und höher: Es ist ausreichend, dass der SSH-Benutzer über sudo-Privilegien verfügt.

> Der Root-Zugriff auf den SSH-Server ist ein Sicherheitsrisiko!
> Stellen Sie sicher, dass Sie den Root-Zugriff auf den SSH-Server deaktivieren, wenn der Aktualisierungsprozess des Keystores abgeschlossen ist.

- **SSH Benutzer:** SSH-Benutzer
- **SSH Passwort:** SSH-Benutzerpasswort

9. Klicken Sie **Weiter** um den Update-Prozess zu starten.
   Der Keystore wird aktualisiert.

10. Klicken Sie **Fertig**.

ICG ohne Remote Installer installieren

Die empfohlene Methode zur Installation des ICG ist die Verwendung des ICG Remote Installers. Eine Anleitung finden Sie unter Installation und Einrichtung (see page 12).
Der ICG Remote Installer ist ab UMS 5.09.100 verfügbar.

Zertifikat im ICG Keystore Format erstellen und exportieren

1. Starten Sie die UMS Konsole.
2. Erstellen Sie ein signierte Zertifikat, falls Sie das nicht bereits getan haben. Wählen Sie je nach Ihren Anforderungen eine der folgenden Vorgehensweisen:
   - Zertifikat mit der UMS erstellen (see page 35)
   - Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (see page 27)
   - Bestehende Zertifikatskette installieren (see page 16)
3. Gehen Sie unter **UMS Administration** zu **Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway** (UMS 6.06 oder höher) bzw. **Globale Konfiguration > Cloud Gateway Konfiguration**. (UMS 6.05 oder niedriger).
4. Rechtsklicken Sie das Zertifikat, mit dem der ICG installiert werden soll; wählen Sie aus dem Kontextmenü **Zertifikatskette im IGEL Cloud Gateway Keystore Format exportieren**.

Keystore hochladen

Sie können SCP (Secure Copy) verwenden, um den aus der UMS exportierten Keystore auf die Maschine hochzuladen, auf der der ICG installiert wird.

Unter Windows mit WinSCP

1. Laden Sie die kostenlose WinSCP Software unter https://winscp.net[5] herunter und installieren Sie sie.
2. Konfigurieren Sie in WinSCP eine neue Sitzung mit folgenden Einstellungen:
   - **Dateiprotokoll:** SCP
   - **Hostname:** Name oder IP-Adresse Ihrer ICG Maschine
   - **Benutzername:** `sshuser`
   - **Passwort:** Das Password, welches Sie für `sshuser` gesetzt haben.
3. Klicken Sie **Anmelden.**
4. Ziehen Sie die Datei `keystore.icg` per Drag & Drop in das Heimatverzeichnis von `sshuser` auf dem ICG-Rechner.

5 https://winscp.net/

Unter Linux mit SCP

1. Wechseln Sie in einem Terminalemulator in das Verzeichnis, in dem Sie die Keystore-Datei gespeichert haben.
2. Führen Sie die folgende Befehlszeile aus:
   `scp keystore.icg sshuser@[host]:~/`
3. Geben Sie das Passwort ein, welches Sie für `sshuser` gesetzt haben.
   Die Datei wird hochgeladen.

Den ICG Installer starten

1. Melden Sie sich auf der Maschine als `root` an.
2. Kopieren Sie den hochgeladenen Keystore mit dem Befehl `cp` in das aktuelle Verzeichnis:
   `cp /home/sshuser/keystore.icg .`

   > Bitte beachten Sie, dass "." (Vollstop) ist Teil des Befehls. Der Punkt steht für das aktuelle Verzeichnis. Sie übergeben dem Befehl cp also zwei Argumente: "/home/sshuser/keystore.icg" und "." für das aktuelle Verzeichnis.

3. Machen Sie die ICG-Installationsdatei mit dem Befehl `chmod` ausführbar: `chmod u+x installer-[version].bin`
4. Starten Sie den Installer mit:
   `./installer-[version].bin keystore.icg`
5. Akzeptieren Sie den Installationspfad.
6. Akzeptieren oder ändern Sie den TCP-Port für den ICG-Service (Standard: 8443).

   > Dieser Port muss für das ICG permanent verfügbar sein.

   Das Installationsprogramm konfiguriert und startet den Tomcat-Server und druckt Umgebungsvariablen.

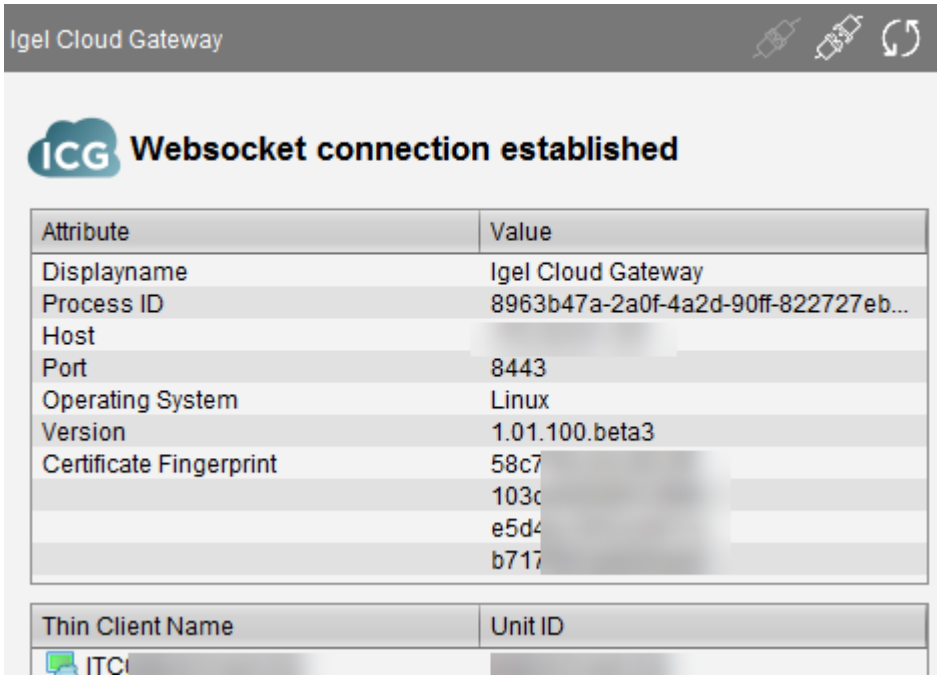
   > Starten Sie das System und den ICG-Tomcat-Server nicht neu, bevor die erste Verbindung von UMS hergestellt wurde.

Die UMS mit dem ICG verbinden

Direkt verbinden

1. Gehen Sie in der UMS Konsole unter **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.
2. Klicken Sie  , um eine neue Gateway-Instanz hinzuzufügen.
3. Geben Sie folgende Daten ein:
   - **Name**: Frei wählbarer Name
   - **Host**:IP oder DNS Name der ICG

     Diese Adresse muss auch im ICG-Zertifikat enthalten sein; sehen Sie IGEL Cloud Gateway (ICG) aktualisieren (see page 60). Andernfalls können ICG und UMS nicht mit einander kommunizieren.
   - **Port**: Der Listening Port des ICG, wie bei der Installation definiert; siehe ICG ohne Remote Installer installieren (see page 103). (Standard: 8443)
4. Klicken Sie **Fertig**.
   Die UMS ist mit dem ICG verbunden.



Über einen Proxy verbinden

Zwischen die UMS und den ICG kann ein Proxy geschaltet werden. Einzelheiten zur Kommunikation zwischen den Komponenten und den verwendeten Ports finden Sie unter Geräte und UMS Server kontaktieren sich über ICG, Abschnitt "Über Proxy"

> Der Proxy muss Websockets mit TLS unterstützen, um mit ICG arbeiten zu können.

> Die Verbindung zum ICG über einen Proxy wird von UMS Version 5.08.100 und höher unterstützt.

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Proxyserver**.
   Wie Sie einen neuen Proxy-Eintrag erstellen, erfahren Sie im UMS-Handbuch.

2. Gehen Sie in der UMS Konsole unter **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**.

3. Klicken Sie  , um eine neue Gateway-Instanz hinzuzufügen.

4. Geben Sie die folgenden Daten ein:
   - **Name**: Frei wählbarer Name
   - **Host:** IP oder DNS Name der ICG
   - **Port:** (Standard: 8443)

5. Klicken Sie **Weiter**.

6. Wählen Sie **Manuelle Proxy Konfiguration** und wählen Sie den Proxy aus, den Sie ein paar Schritte zuvor erstellt haben.

7. Klicken Sie **Fertig**.
   Die UMS ist mit dem Gateway verbunden.

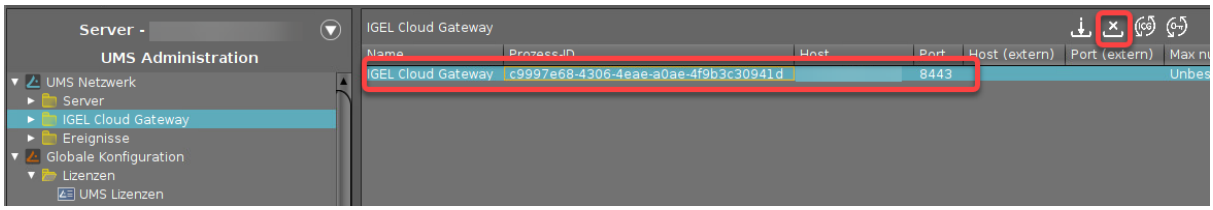
IGEL Cloud Gateway (ICG) deinstallieren

Die Standardmethode zur Deinstallation Ihres IGEL Cloud Gateway (ICG) erfolgt über die UMS Konsole; siehe Deinstallation des ICG über die UMS-Konsole (see page 107). Mit dieser Methode wird die ICG Instanz auf ihrem Hosting-Rechner deinstalliert und der entsprechende ICG Eintrag aus der UMS-Datenbank entfernt.

Alternativ können Sie auch Shell-Befehle verwenden; siehe Manuelle Deinstallation des ICG (see page 111). Wenn Sie eine ICG Instanz manuell deinstalliert haben oder der Rechner, auf dem die ICG Instanz gehostet wurde, nicht mehr existiert, müssen Sie den zugehörigen Datenbankeintrag in einem separaten Schritt entfernen; siehe Entfernen des ICG-Eintrags aus der UMS-Datenbank (see page 112).

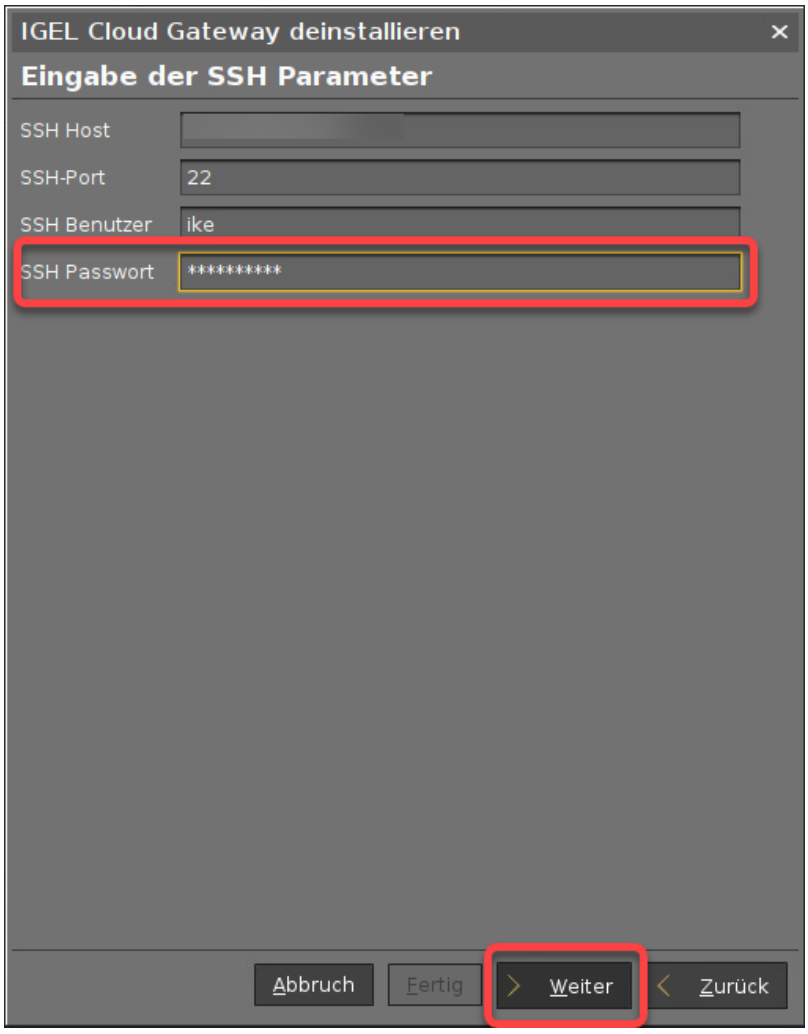
Deinstallation des ICG über die UMS-Konsole

1. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**, wählen Sie die ICG Instanz, die Sie entfernen möchten, und klicken Sie dann die Schaltfläche zur Deinstallation.



2. Bestätigen Sie den Dialog und klicken Sie **Weiter**.

3. Geben Sie das **SSH Passwort** eines SSH-Benutzers mit sudo-Berechtigung ein (typischerweise derselbe Benutzer, der den ICG installiert hat) und klicken Sie **Weiter**.



Der Deinstallationsprozess wird gestartet.

Wenn alles gut geht, wird der ICG von der Maschine deinstalliert.

4. Klicken Sie **Fertig**.

ICG manuell deinstallieren

Der ICG enthält ein Deinstallationsskript. Um den ICG vollständig vom System zu entfernen, gehen Sie wie folgt vor:

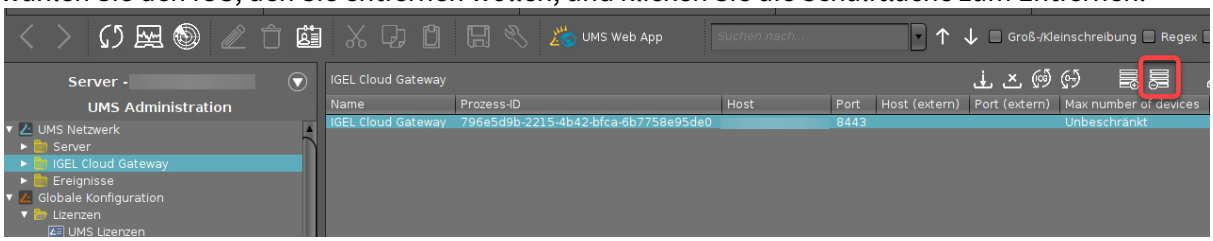
1. Melden Sie sich am ICG Host als root oder als Benutzer mit sudo-Privilegien an .
2. Wechseln Sie in das Verzeichnis, in dem Sie den ICG installiert haben (Standard: `/opt/IGEL/icg/`).
   Es enthält das Skript `uninstall.sh`
3. Um den Deinstallationsprozess zu starten, geben Sie `sudo ./uninstall.sh` ein.

4. Ein Dialog öffnet sich. Bestätigen Sie, das Sie die ICG Instanz vollständig entfernen wollen.
   Der ICG wird vollständig entfernt.

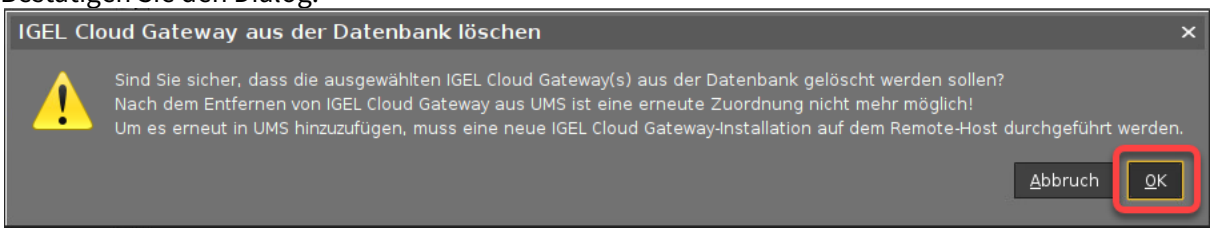
ICG Eintrag aus der UMS Datenbank entfernen

⚠ Sobald eine ICG Instanz aus der Datenbank entfernt wurde, ist es nicht mehr möglich, sie erneut mit der UMS zu verknüpfen. Wenn Sie Ihren ICG wiederherstellen möchten, müssen Sie eine neue Installation durchführen.

1. Gehen Sie in der UMS Konsole auf **UMS Administration > UMS Netzwerk > IGEL Cloud Gateway**, wählen Sie den ICG, den Sie entfernen wollen, und klicken Sie die Schalftläche zum Entfernen.



2. Bestätigen Sie den Dialog.



Die ICG Instanz wird aus der Datenbank entfernt.

ICG aktualisieren

1. Laden Sie den Installer auf Ihren ICG Server hoch, mittels WinSCP unter Windows oder mit dem Kommando `scp` unter Linux. Verwenden Sie dabei das Benutzerkonto `sshuser`.
2. Melden Sie sich auf der ICG Virtual Appliance als `root` an.
3. Kopieren Sie den hochgeladenen Installer ins das aktuelle Verzeichnis:
   `cp /home/sshuser/installer-[version].bin .`
4. Machen Sie den ICG-Installer ausführbar:
   `chmod u+x installer-[version].bin`
5. Starten Sie den Installer:
   `./installer-[version].bin`
6. Akzeptieren Sie den Installationspfad.
7. Akzeptieren oder ändern Sie den TCP-Port für den ICG Dienst (Standard: 8443).
   Der Installer konfiguriert und startet den Tomcat-Server und gibt dabei Umgebungsvariablen aus.

ICG-Zertifikate mit UMS verwalten

Die Universal Management Suite (UMS) verfügt über einen integrierten TLS/SSL-Zertifikatemanager für das IGEL Cloud Gateway (ICG). Er erzeugt Keystore-Dateien, die für den ICG-Installer geeignet sind.

Optionen für die Signierung eines Zertifikats

Die UMS unterstützt drei Optionen für die Zertifikatssignierung:

- Benutzen Sie die UMS, um eine private CA zu erzeugen (see page 35) und die ICG-Zertifikate zu signieren.
    - Vorteile: Kostenlos, unabhängig
    - Nachteile: Client-Benutzer müssen bei der ersten Verbindung mit ICG den Fingerabdruck des CA-Zertifikats überprüfen, keine erweiterten PKI-Verwaltungsfunktionen.
- Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (see page 27) und verwenden Sie das Zertifikat um ein Zertifikat des ICG zu signieren.
    - Vorteile: Kostenlos
    - Nachteile: Client-Benutzer müssen bei der ersten Verbindung mit ICG den Fingerabdruck des CA-Zertifikats überprüfen. Möglicherweise möchten Sie Ihren privaten CA-Schlüssel nicht in einer vernetzten Anwendung wie UMS speichern und es kann schwierig sein, ihn mit Ihrer privaten Haupt-CA zu synchronisieren.
- Einen öffentlichen bekannten CA in UMS verwenden (see page 116) und ein von ihm unterzeichnetes ICG-Zertifikat.
    - Vorteile: Wenn die CA eine der rund 170 von IGEL OS unterstützten CAs ist, müssen die Benutzer den Fingerabdruck des Zertifikats nicht überprüfen.
    - Nachteile: Kosten. Sie werden nicht in der Lage sein, Zertifikate selbst zu signieren.

Einen öffentlich bekannten CA in UMS verwenden

Die folgenden Dateien werden benötigt:

- CA-Root-Zertifikat
- ICG-Server-Zertifikat, das von der CA signiert wurde.
- ICG-Server privater Schlüssel

Um eine öffentlich bekannte CA im UMS zu verwenden:

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Zertifikatsverwaltung > Cloud Gateway**.
2. Klicken Sie im Bereich **Zertifikate** auf  , um das Root-Zertifikat zu importieren.
3. Wählen Sie die Root-Zertifikatedatei des CA (im PEM-Format).
   Das Root-Zertifikat des CA erscheint in der Liste.
4. Klicken Sie mit der rechten Maustaste auf das Root-Zertifikat des CA und wählen Sie **Signierte Zertifikat importieren**.
5. Klicken Sie **Ok**.
   Das signierte Zertifikat erscheint in der Liste.
6. Klicken Sie mit der rechten Maustaste auf das signierte Zertifikat und wählen Sie **Entschlüsselten privaten Schlüssel importieren**.

   > Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn mit dem OpenSSL-Kommandozeilenprogramm entschlüsseln: `openssl rsa -in encrypted.key -out decrypted.key`
7. Wählen Sie die entschlüsselte private Schlüssel-Datei aus.
   Aus den Daten kann nun eine Keystore-Datei für den ICG-Server erstellt werden.
8. Klicken Sie mit der rechten Maustaste auf das signierte Zertifikat und wählen Sie **Zertifikatskette im IGEL Cloud Gateway Keystore Format exportieren**.
   Die Datei `keysotre.icg` wird erstellt. Diese Datei wird für das Gateway benötigt.
9. Speichern Sie die `keystore.icg` Datei.

Citrix NetScaler ADC als eine SSL Bridge für ICG verwenden

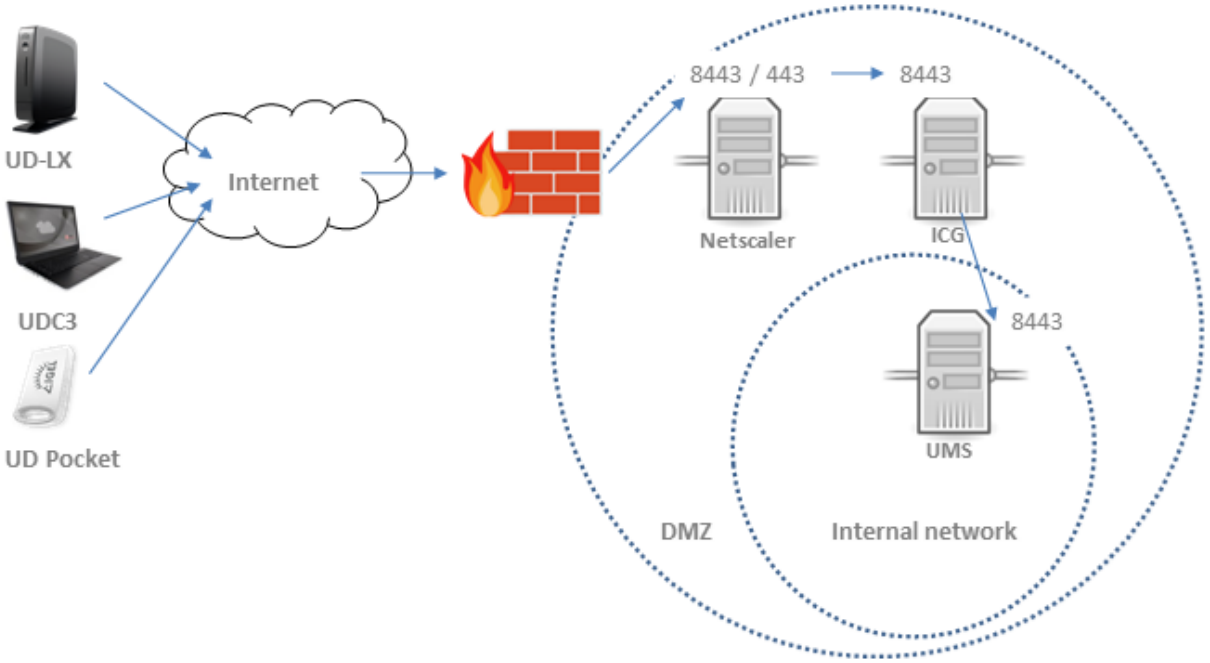
Dieses Dokument beschreibt die Verwendung von Citrix NetScaler ADC (Application Delivery Controller) zur Annahme von Anfragen von Endgeräten und deren Weiterleitung an IGEL Cloud Gateway (ICG).

> Bitte beachten Sie, dass IGEL den Einsatz von Citrix NetScaler als Load Balancer nicht unterstützt. Die Verwendung von Citrix NetScaler als SSL-Bridge hat somit keinen Einfluss auf die Verteilung von Anfragen an die ICG Instanzen.

Netzwerktopologie

Dies ist die Netzwerktopologie für Citrix NetScaler ADC zur Weiterleitung von Anfragen an ICG.

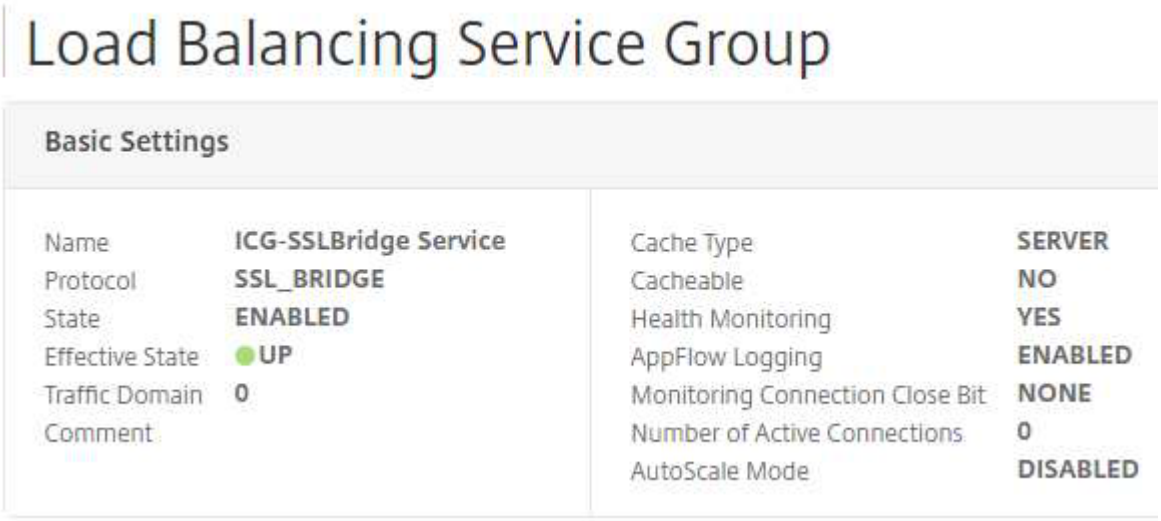
> Das TLS/SSL-Zertifikat, das Clients sehen wird dasjenige sein, das auf NetScaler installiert ist.



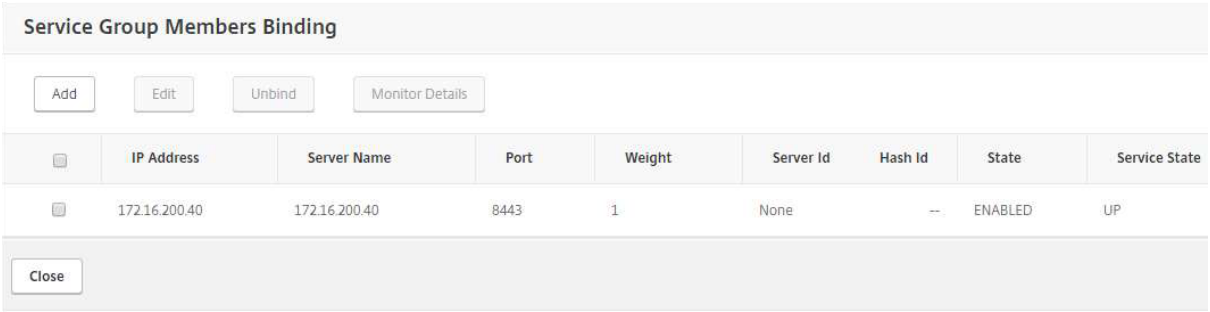
NetScaler konfigurieren

1. Konfigurieren Sie ein Serverobjekt in NetScaler unter **Load Balancing**. Wählen Sie seine IP-Adresse aus dem Subnetz, in dem sich das ICG befindet.

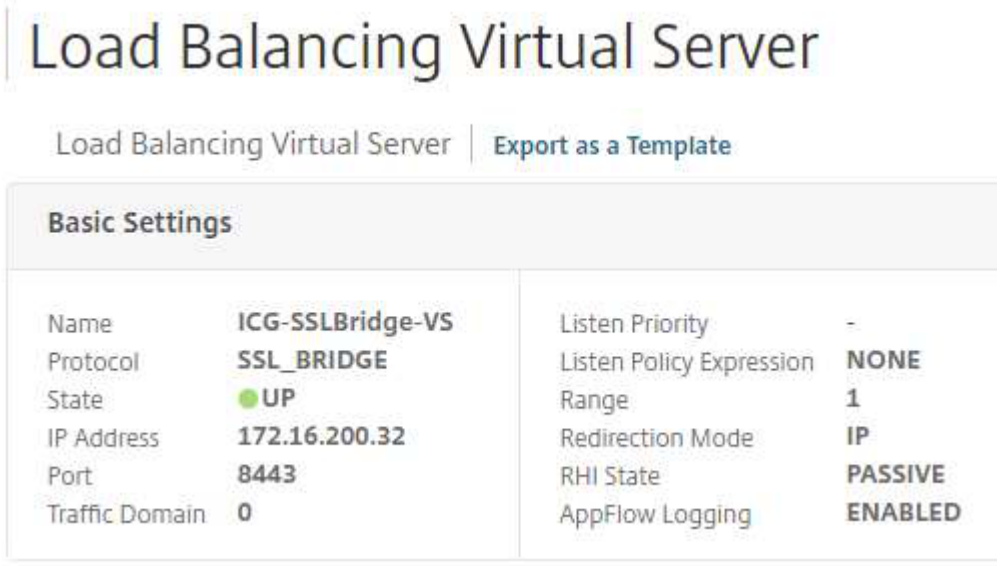
2. Erstellen Sie eine **Load Balancing Service Group** mit `SSL_Bridge` als **Protokoll.** Im Screenshot heißt er `ICG-SSLBridge` Service.



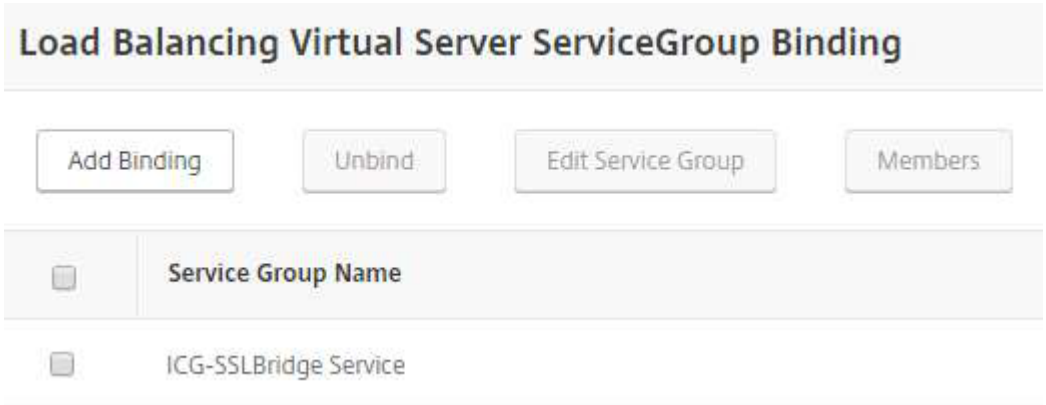
3. Fügen Sie ein **Service Group Mitglied** mit der ICG'S IP-Adresse und TCP-Port hinzu.



4. Erstellen Sie einen **virtuellen Load Balancing Server.** Die IP-Adresse und der TCP-Port, die Sie hier konfigurieren sind über das Internet zugänglich.



5. Fügen Sie der Load Balancing Server Group ein **Binding** hinzu und verbinden Sie den ICG-SSLBridge Service, den Sie in Schritt 2 angelegt haben. Der virtuelle Load Balancing Server sollte sich nun im Zustand UP befinden und die Kommunikation aus dem Internet sollte an ICG weitergeleitet werden.



Sudo-Privilegien für einen Benutzer vergeben

> Die Vergabe von Sudo-Privilegien für einen Benutzer kann ein Sicherheitsrisiko darstellen!
> Die in dieser Anleitung beschriebenen Anweisungen sollten nur von erfahrenen Benutzern ausgeführt werden.

Bei der Installation des IGEL Cloud Gateways mit dem Remote Installer (siehe IGEL Cloud Gateway installieren (see page 40)) verbindet sich der Remote Installer über SSH mit dem Bereitstellungsserver.

Damit der Installer alle erforderlichen Installationsaufgaben ausführen kann, muss der für die SSH-Anmeldung angegebene Benutzer entweder `root` oder (ab UMS 5.09.110) `sudo` -Rechte besitzen. Die folgende Tabelle zeigt, wie man einem Benutzer sudo-Privilegien auf den vom ICG unterstützten Linux-Distributionen zuweist.

Verteilung	sudo in der Standardinstallation enthalten	Befehl zum Hinzufügen eines Benutzers zur Sudoer-Liste*
Ubuntu	Ja	`usermod -aG sudo <USERNAME>`
Debian	Nein Installieren Sie mit diesem Befehl: `apt install sudo`	`usermod -aG sudo <USERNAME>`
Redhat	Ja	`usermod -aG wheel <USERNAME>`
SLES	Ja	`usermod -aG wheel <USERNAME>` Sie müssen auch das `wheel` zu `/etc/sudoers` hinzufügen.

* Root-Privilegien sind erforderlich für die Verwendung von `usermod.`

Replacing Expired ICG Certificates

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Bestehende Zertifikatskette installieren (UMS 6.02 oder Älter)

Übersicht

Sie können eine Zertifikatskette verwenden, die bereits in Ihrer Arbeitsumgebung verwendet wird. Die Zertifikatskette muss ein Stammzertifikat und ein Endzertifikat enthalten und kann ein oder mehrere Zwischenzertifikate enthalten.

Um sicherzustellen, dass Ihre Zertifikate von Ihrer IGEL Cloud Gateway-Installation verwendet werden können, lesen Sie bitte Zertifikatsanforderungen und -empfehlungen für IGEL Cloud Gateway (ICG) (see page 14).

In dem hier beschriebenen Beispiel wird die folgende Zertifikatskette verwendet:

- Root-Zertifikat
- Zwischen-CA-Zertifikat
- Endzertifikat

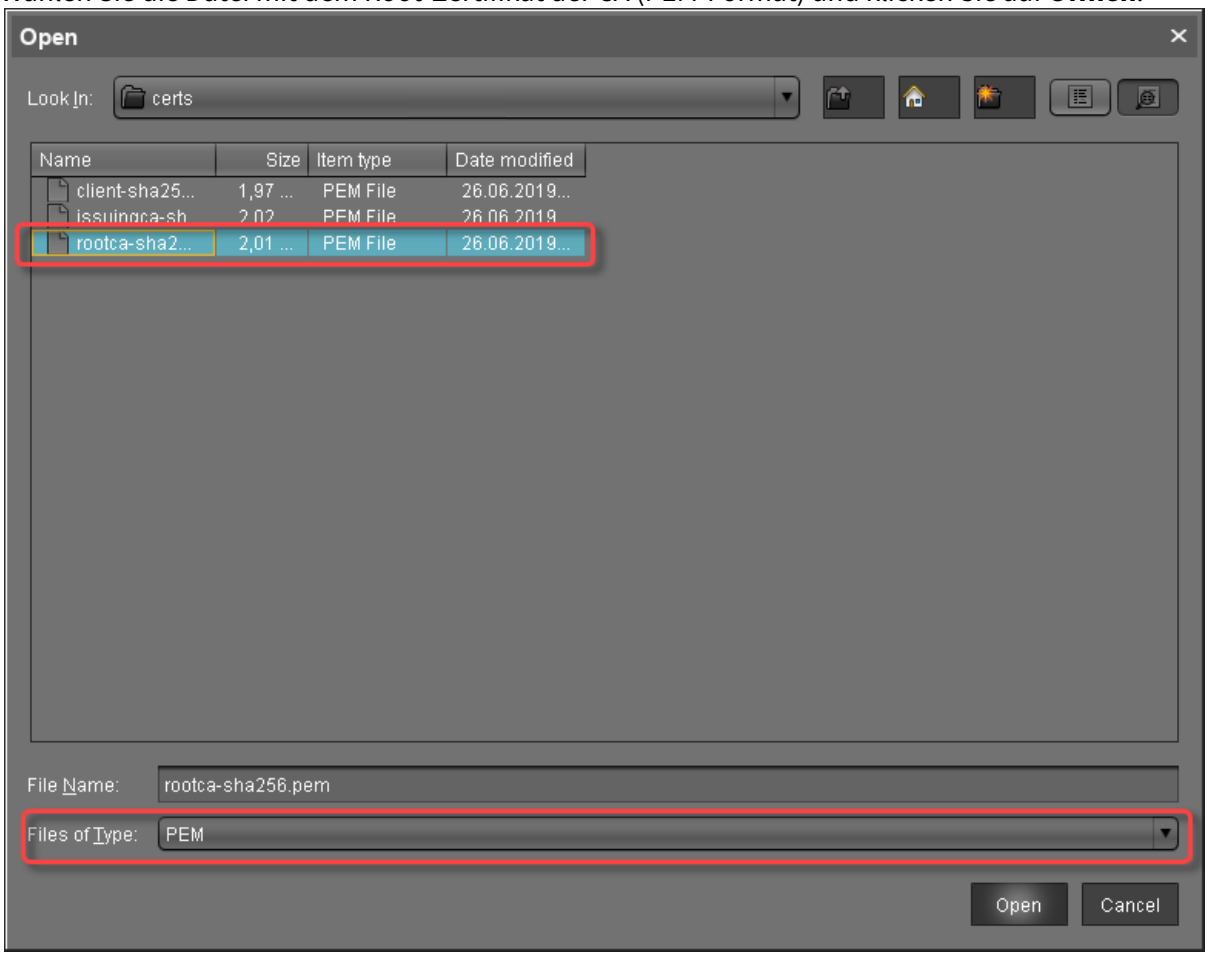
Wenn die Zertifikatskette vorhanden ist, können Sie mit der IGEL Cloud Gateway installieren (see page 40) fortfahren.

Root-Zertifikat importieren

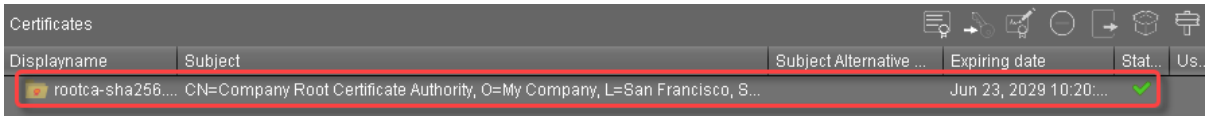
> Der Gültigkeitszeitraum des Root-Zertifikats sollte so lang wie möglich sein. Nach Ablauf des Root-Zertifikats müssen alle Zertifikate ausgetauscht und alle Geräte erneut registriert werden.

1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration.**
2. Klicken Sie im Abschnitt **Zertifikate** auf  , um das Root-Zertifikat zu importieren.

3. Wählen Sie die Datei mit dem Root-Zertifikat der CA (PEM-Format) und klicken Sie auf **Öffnen**.



Das Root-Zertifikat der CA erscheint in der Liste.

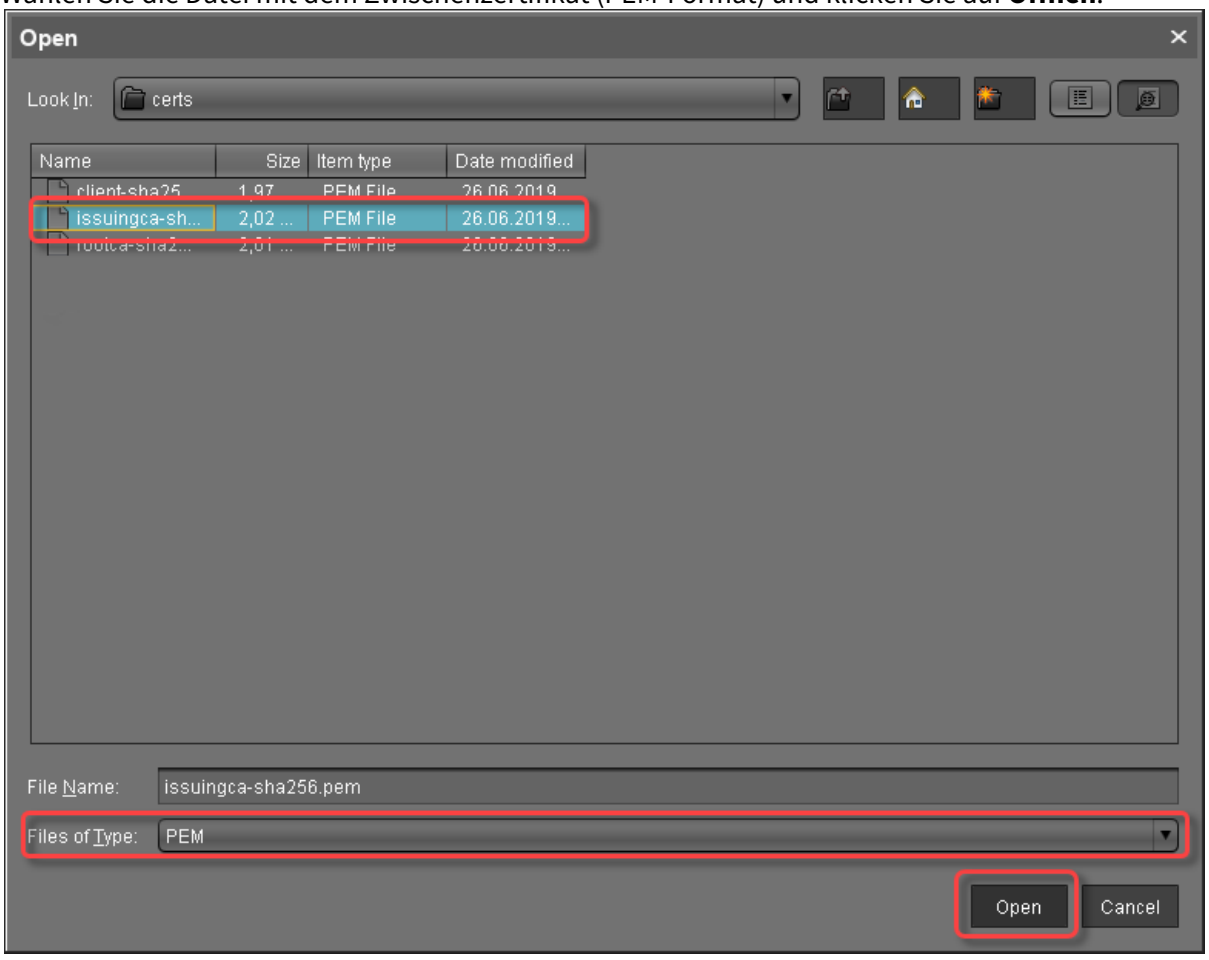


Zwischen-Zertifikat importieren

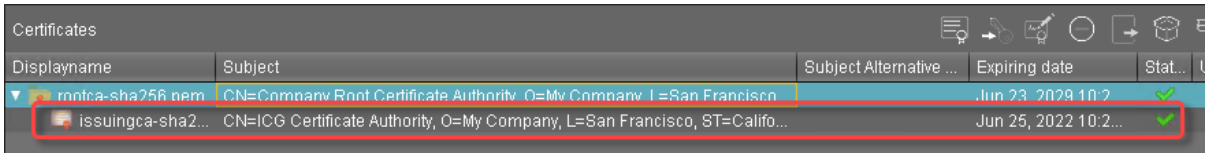
1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration.**

2. Öffnen Sie das Kontextmenü des Root-Zertifikats und wählen Sie **Signiertes Zertifikat importieren.**

3. Wählen Sie die Datei mit dem Zwischenzertifikat (PEM-Format) und klicken Sie auf **Öffnen**.

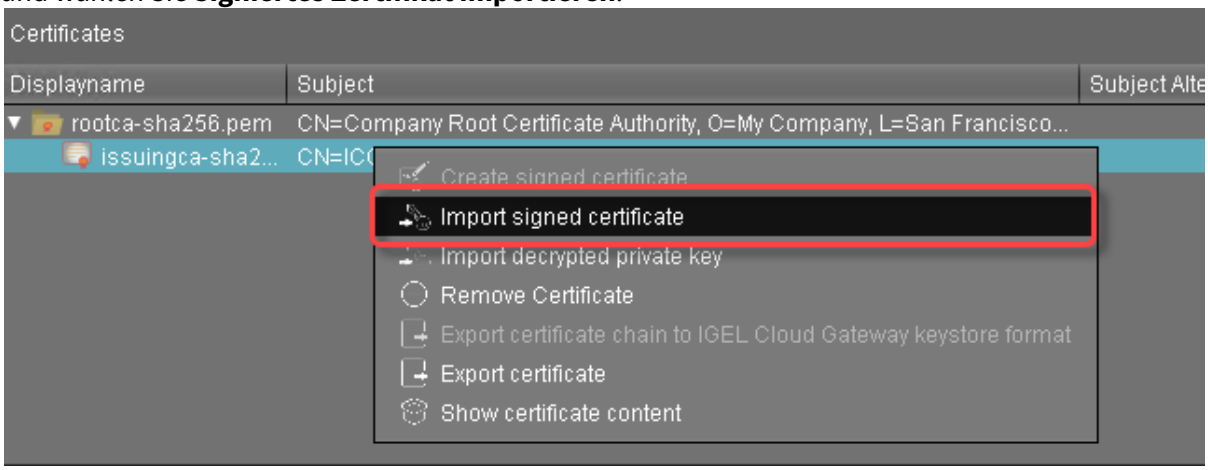


Das Zwischenzertifikat erscheint auf der Liste.

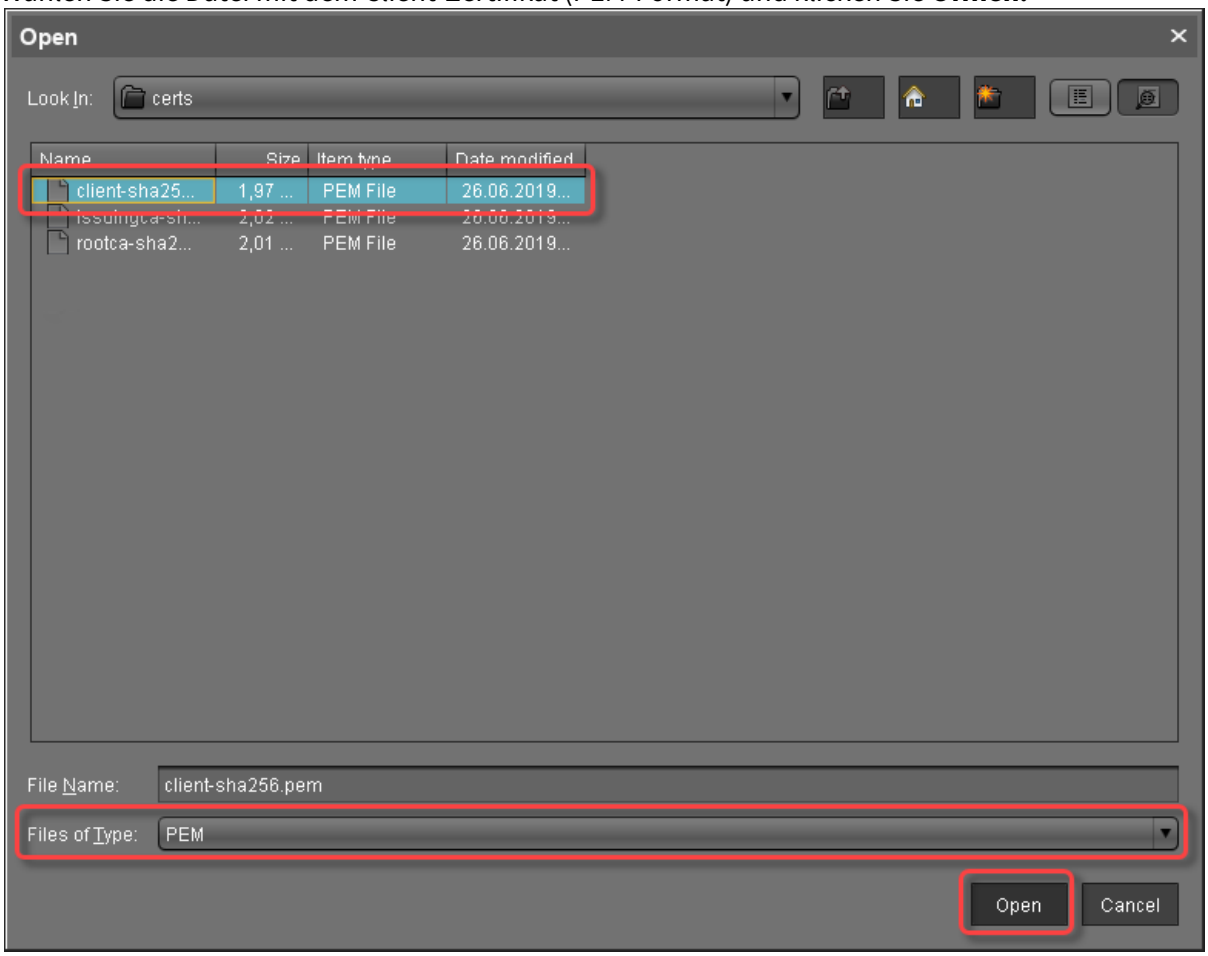


Endzertifikat importieren

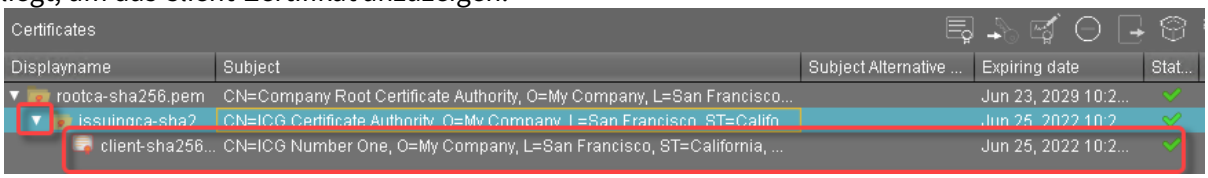
1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration.**
2. Öffnen Sie das Kontextmenü des Zwischenzertifikats, das dem Client-Zertifikat am nächsten liegt, und wählen Sie **Signiertes Zertifikat importieren**.



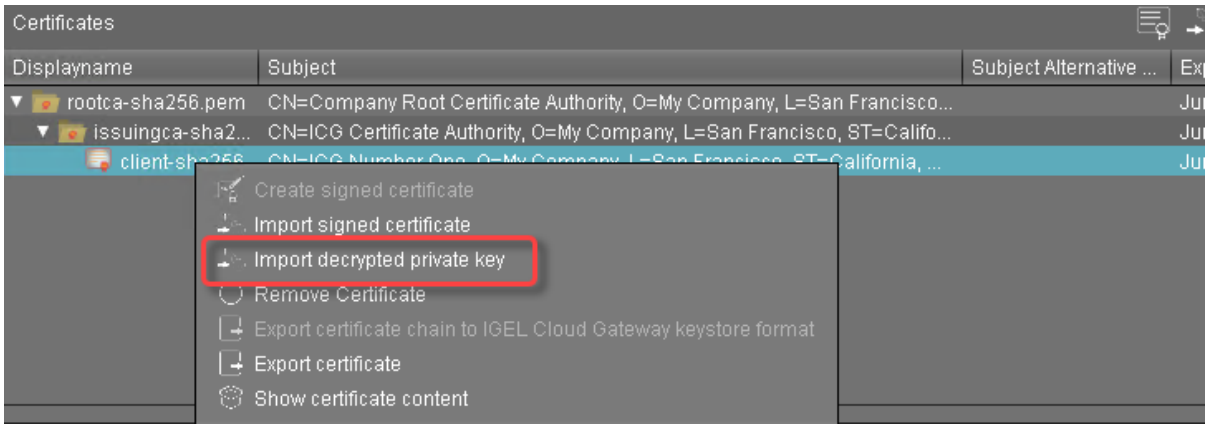
3. Wählen Sie die Datei mit dem Client-Zertifikat (PEM-Format) und klicken Sie **Öffnen.**



4. Klicken Sie auf das Pfeilsymbol des Zwischenzertifikats, das dem Client-Zertifikat am nächsten liegt, um das Client-Zertifikat anzuzeigen.

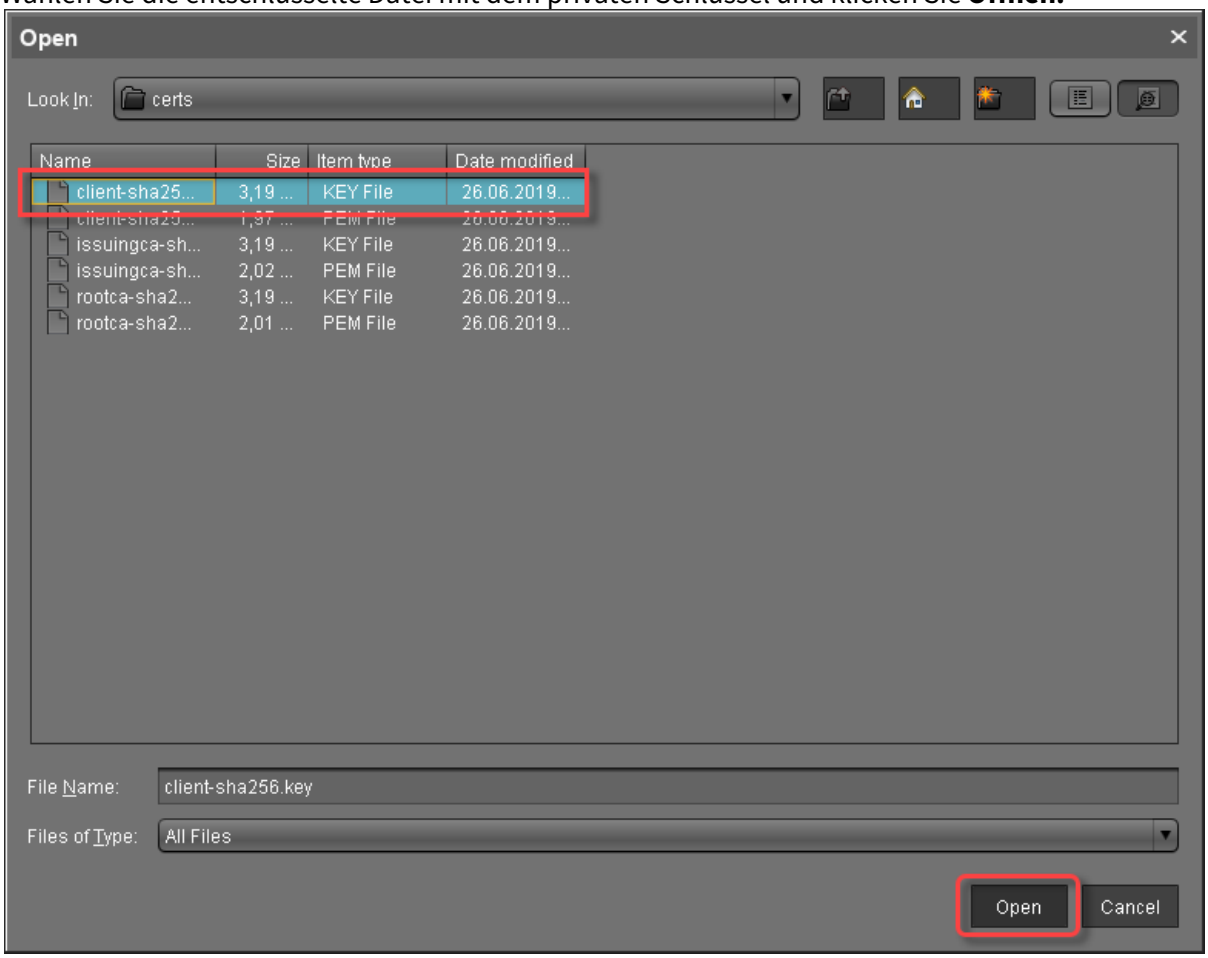


5. Klicken Sie mit der rechten Maustaste auf das Client-Zertifikat und wählen Sie **Entschlüsselten privaten Schlüssel importieren**

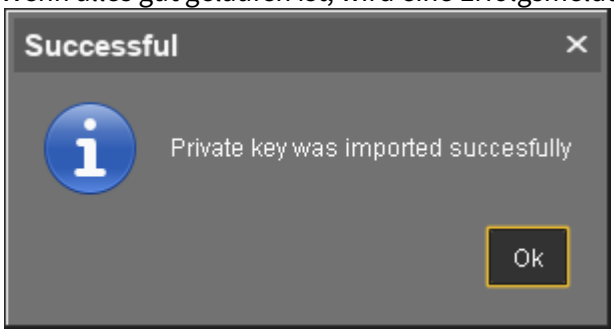


> Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn mit dem OpenSSL-Kommandozeilentool entschlüsseln: `openssl rsa -in encrypted.key -out decrypted.key`

6. Wählen Sie die entschlüsselte Datei mit dem privaten Schlüssel und klicken Sie **Öffnen.**



Wenn alles gut gelaufen ist, wird eine Erfolgsmeldung angezeigt.



Zertifikate mit einem vorhandenen Root-Zertifikat erzeugen (UMS 6.02 oder älter)

Erforderliche Zertifikatsdateien

Die folgenden Dateien sind erforderlich:

- CA-Zertifikat
- CA Privater Schlüssel

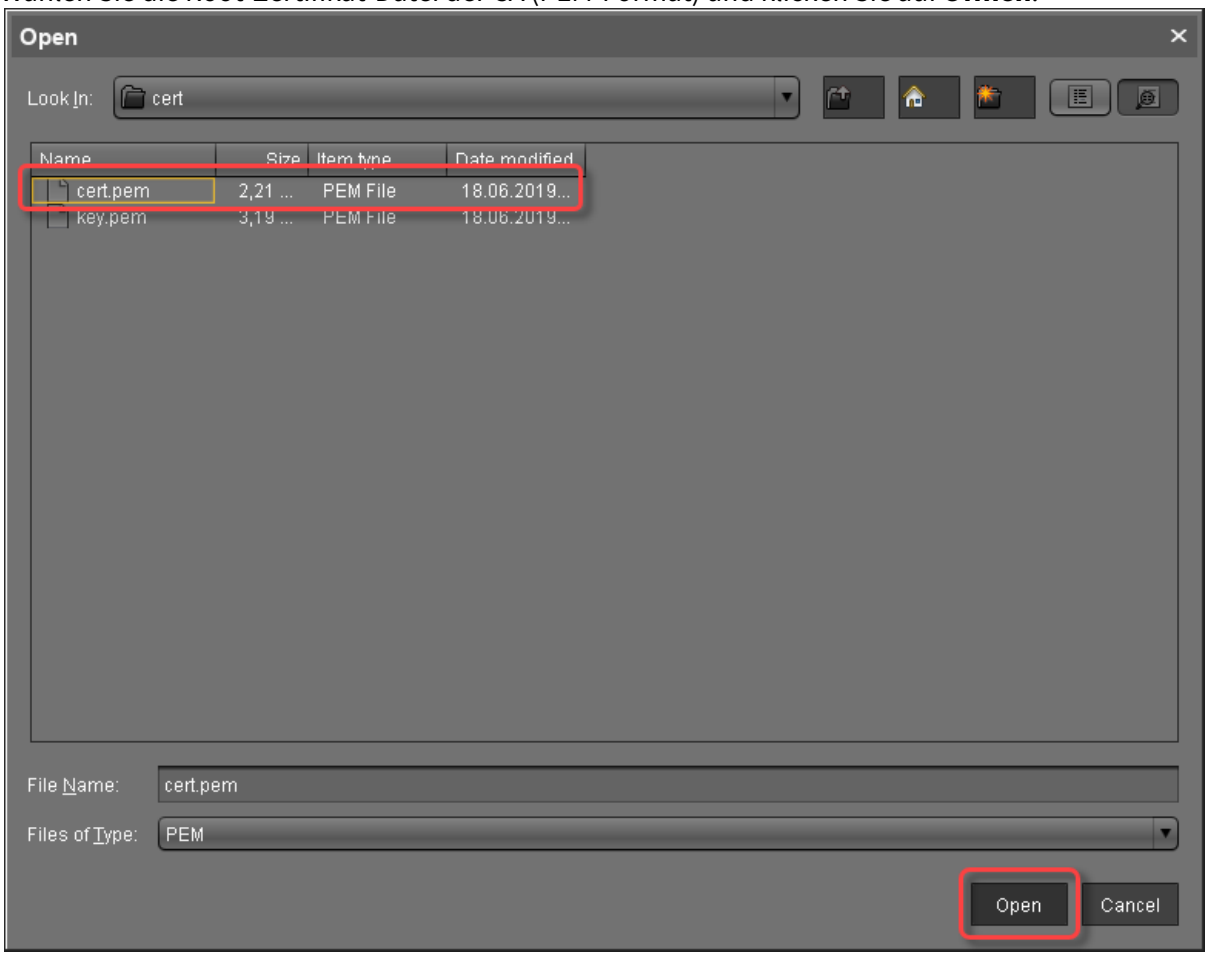
> Wenn Sie das Root-Zertifikat und den Schlüssel der CA-Signatur von einem Microsoft CA-Server exportieren müssen, können Sie diesem Dokument von Cisco folgen: How do I export and convert a pfx CA root certificate and key from a Microsoft CA server[6]

Ihre vorhandenen privaten CA-Dateien in die UMS importieren

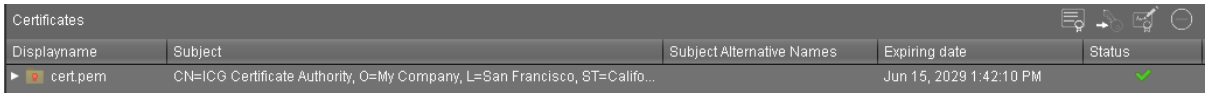
1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Cloud Gateway Konfiguration.**
2. Klicken Sie im **Zertifikate** Bereich auf  , um das Root-Zertifikat zu importieren.

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

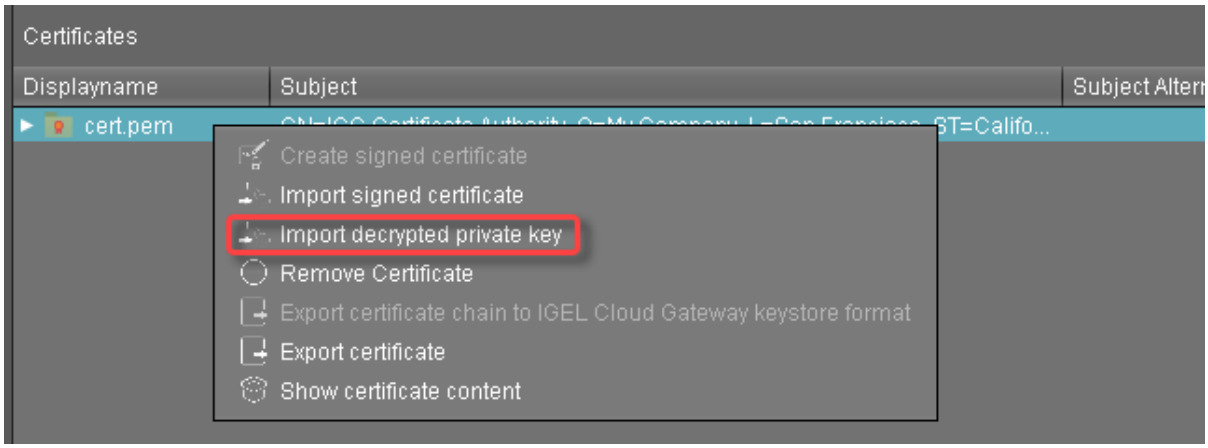
3. Wählen Sie die Root-Zertifikat-Datei der CA (PEM-Format) und klicken Sie auf **Öffnen**.



Das Root-Zertifikat der CA erscheint in der Liste.

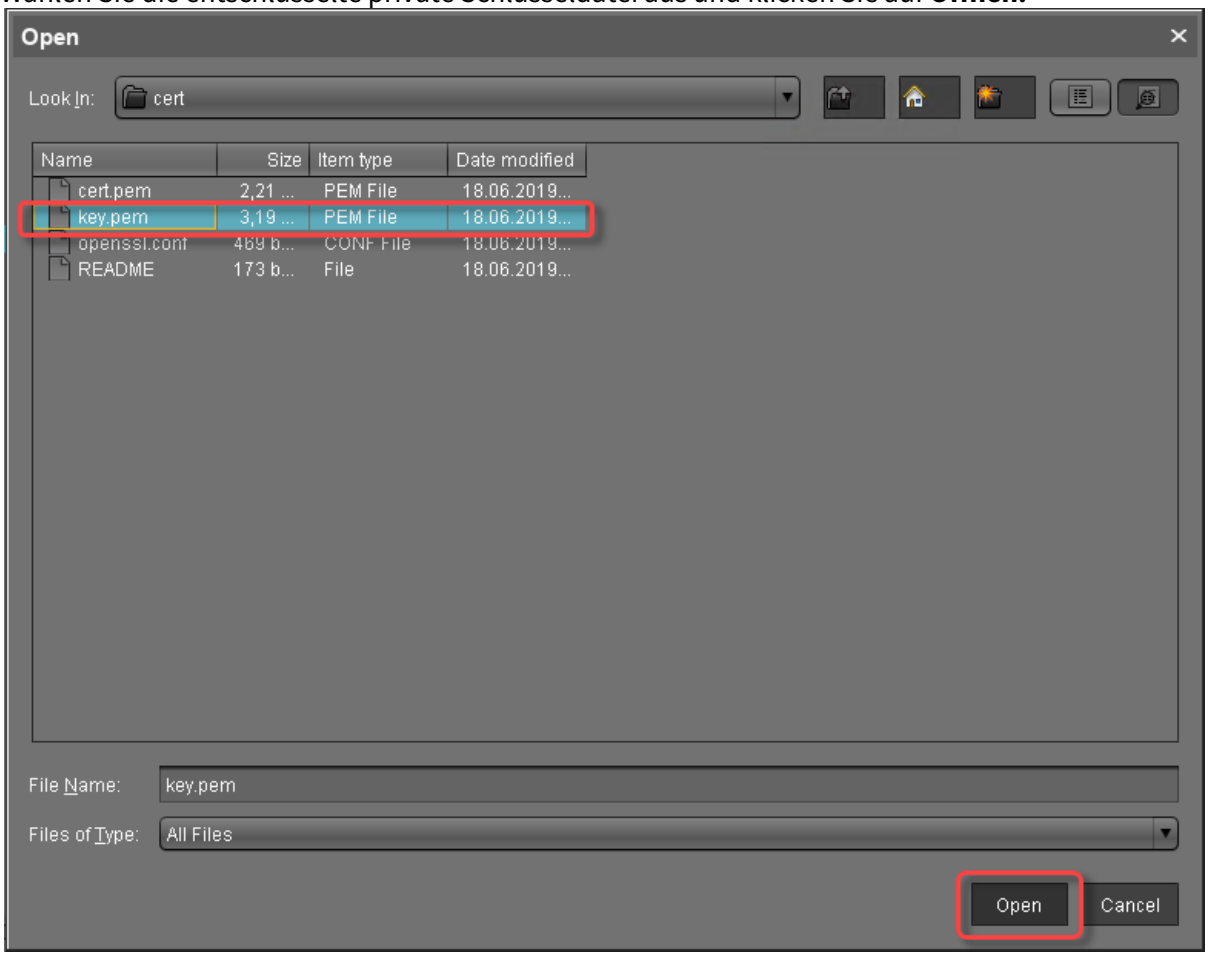


4. Klicken Sie mit der rechten Maustaste auf das Root-Zertifikat der CA und wählen Sie **Entschlüsselten privaten Schlüssel importieren.**

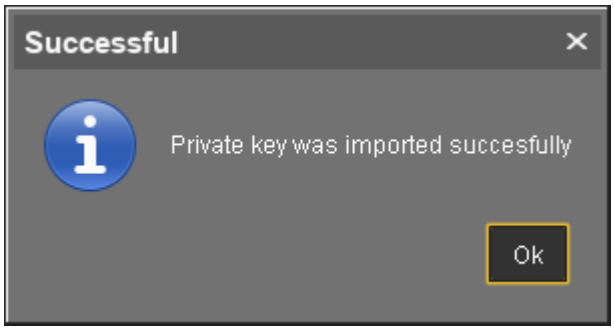


> Wenn der private Schlüssel mit einer Passphrase geschützt ist, müssen Sie ihn mit dem OpenSSL-Kommandozeilentool entschlüsseln: `openssl rsa -in encrypted.key -out decrypted.key`

5. Wählen Sie die entschlüsselte private Schlüsseldatei aus und klicken Sie auf **Öffnen.**



Wenn alles gut gelaufen ist, wird eine Erfolgsmeldung angezeigt.



Die CA ist nun einsatzbereit.

Ein signiertes Zertifikat erstellen

1. Klicken Sie mit der rechten Maustaste auf das Root-Zertifikat der CA und wählen Sie **Signiertes Zertifikat generieren.**

2. Füllen Sie die Zertifikatsfelder aus:
   - **Name:** Name des Zertifikats
   - **Ihr Vor- und Nachname:** Name des Zertifkatsinhabers
   - **Ihre Organisation:** Organisation oder Firmenname
   - **Ihre Stadt oder Gemeinde:** Standort
   - **Ihr Ländercode (zwei Buchstaben):** ISO 3166 Ländercode, z. B. `US`, `UK` oder `ES`
   - **Hostname und/oder IP des Zielservers für das Zertifikat:** Hostname(n) oder IP-Adresse(n), für die das Zertifikat gültig ist. Mehrere Eingaben sind erlaubt, getrennt durch Semikolon.

     > Alle IP-Adressen und Hostnamen, unter denen die ICG von innerhalb des Firmennetzwerks oder von außerhalb erreichbar ist, müssen hier angegeben werden.

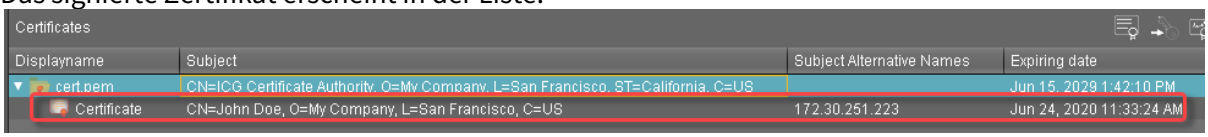
   - **Gültig bis:** Lokales Datum, an dem dieses Zertifikat abläuft. (Standard: ein Jahr ab jetzt)
   - **Zertifikats-Typ:** Wählen Sie "End Entity".

3. Klicken Sie **OK.**

Es wird ein Schlüsselpaar und ein Zertifikat erzeugt.

> ⓘ Die Generierung von Schlüsseln kann bei virtuellen Maschinen (VMs) viel Zeit in Anspruch nehmen, da diese keine leistungsstarke (Pseudo-)Zufallszahlensquelle haben. Auf Linux-VMs kann dies durch die Installation des haveged[7] Pakets verbessert werden.

Das signierte Zertifikat erscheint in der Liste.



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

Passwörter auf die Geräte übertragen

Um ein Gerät mit dem ICG zu verbinden, müssen die neu erzeugten Zugangsdaten (Fingerabdruck, Passwort) auf der Benutzer- bzw. Geräteseite verfügbar sein. In vielen Fällen befinden sich Benutzer und Gerät an einem entfernten Ort, so dass es dem Benutzer überlassen bleibt, die Verbindung zum ICG herzustellen.

Es gibt mehrere Möglichkeiten, die Zugangsdaten bereitzustellen:

- über einen USB-Stick, der die Zugangsdaten in Form einer XML-Datei enthält
- über einen USB-Stick, der die Zugangsdaten in Form einer HTML-Datei enthält
- über eine E-Mail mit den Zugangsdaten, die direkt aus der UMS erstellt und gesendet werden.
- über eine E-Mail oder gedruckten Brief mit den Zugangsdaten; die Zugangsdaten können per Copy & Paste eingefügt werden.

XML auf einem USB-Stick

Die XML-Datei aus der UMS exportieren:

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
2. Wählen Sie die gewünschte Passworteingabe und klicken Sie  , um die Passwörter zu exportieren.
3. Sichern Sie die Passwörter auf einem USB-Stick im XML-Format als `icg.xml.`

Die Anmeldeinformationen auf dem Gerät abrufen:

1. Öffnen Sie auf Ihrem Gerät das IGEL Setup und gehen Sie unter **Geräte > Speichergeräte > Hotplug-Speichergeräte**.
2. Aktivieren Sie **dynamische Laufwerkszuordnung**.
3. Klicken Sie **Übernehmen**.
4. Stecken Sie den zuvor vorbereiteten USB-Stick ein.
5. Öffnen Sie ein **lokales Terminal**.
6. Melden Sie sich als `user` an.
7. Führen Sie den Befehl `ls media` aus, um Wechselmedien anzuzeigen.
8. Wechseln Sie mit `cd media/[device label]` zu Ihrem USB-Stick.

9. Zeigen Sie die XML-Datei mit `cat icg.xml` an.
   Die XML-Datei enthält alle Daten, die für die Anbindung eines Gerätes an das ICG benötigt werden: Host-Adresse, Fingerabdruck des ICG-Server-Zertifikats und das Passwort.

Jetzt können Sie den fehlenden Teil des Zertifikat-Fingerabdrucks und das Passwort vom Terminal kopieren.

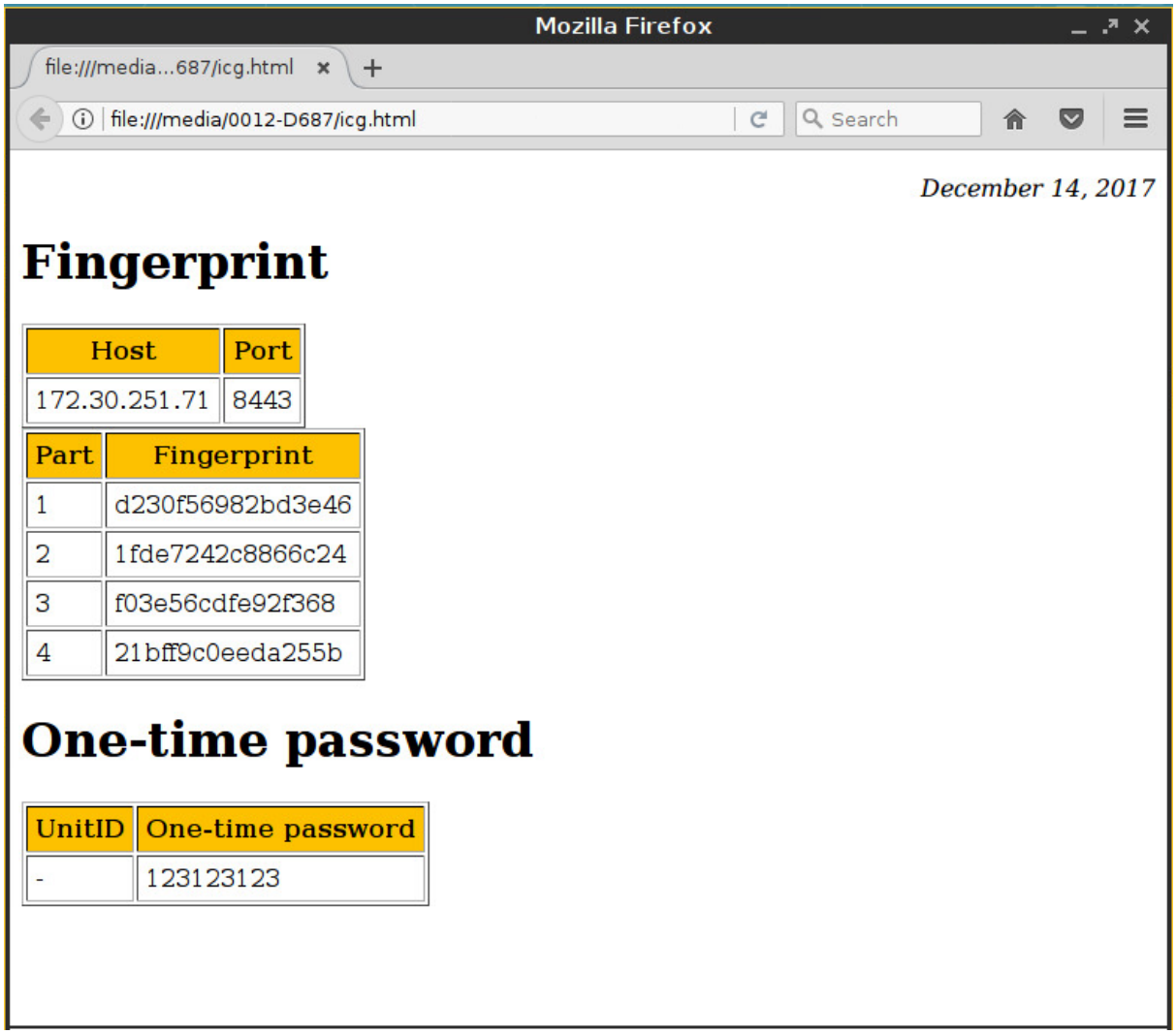
HTML-Datei auf einem USB-Stick

Die HTML-Datei von der UMS exportieren:

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
2. Wählen Sie die gewünschte Passworteingabe und klicken Sie  um die Passwörter zu exportieren.
3. Sichern Sie die Passwörter auf einem USB-Stick im XML-Format als `icg.html.`

Die Anmeldeinformationen auf dem Gerät abrufen:

1. Öffnen Sie auf Ihrem Gerät das Setup und gehen Sie unter **Geräte > Speichergeräte > Hotplug-Speichergeräte**.
2. Aktivieren Sie **dynamische Laufwerkszuordnung**.
3. Klicken Sie **Übernehmen**.
4. Stecken Sie den zuvor vorbereiteten USB-Stick ein.
5. Öffnen Sie ein **lokales Terminal**.
6. Melden Sie sich als `user` an.
7. Führen Sie den Befehl `ls media` aus, um Wechselmedien anzuzeigen.
8. Wechseln Sie mit `cd media/[device label]` zu Ihrem USB-Stick.
9. Zeigen Sie die HTML-Datei mit `firefox icg.html` an.
   Die HTML-Datei enthält alle Daten, die für die Anbindung eines Gerätes an das ICG benötigt werden: Host-Adresse, Fingerabdruck des ICG-Server-Zertifikats und das Passwort:

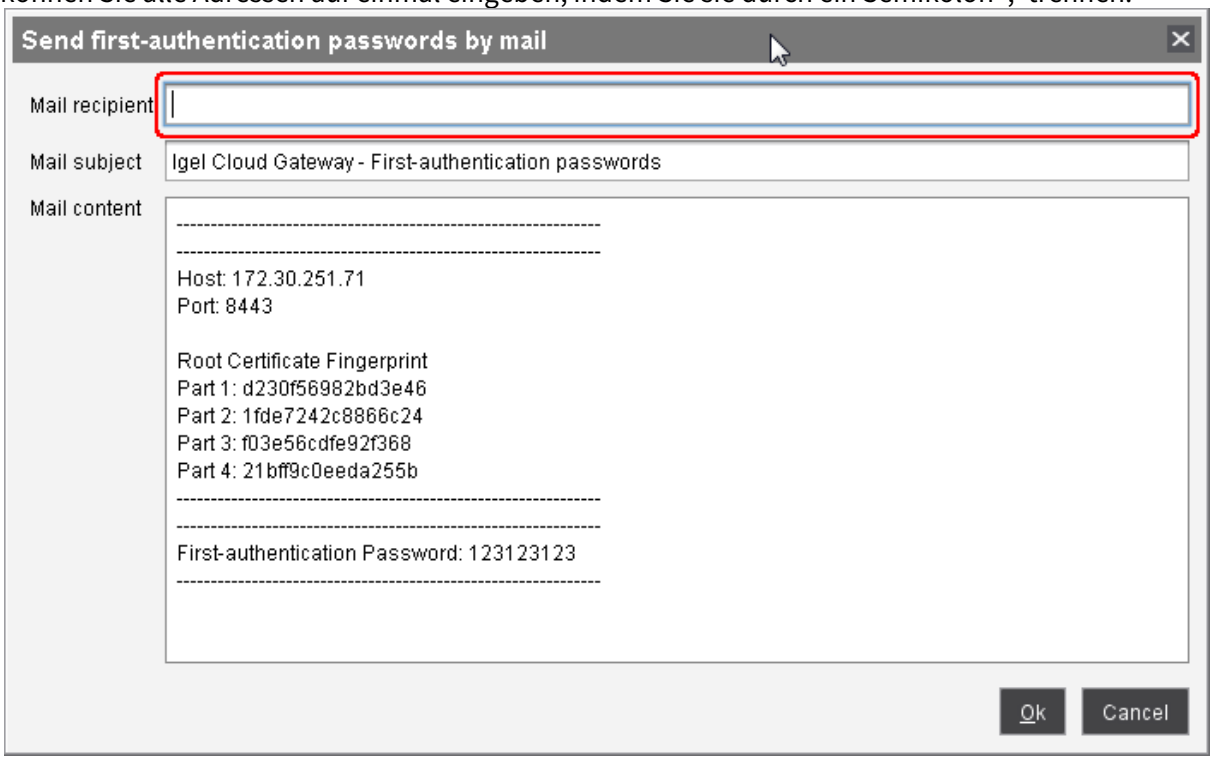


E-Mail von der UMS aus senden

Um eine E-Mail direkt von der UMS zu senden, müssen die E-Mail-Einstellungen richtig eingestellt sein. Weitere Informationen finden Sie unter E-Mail-Einstellungen im UMS-Handbuch.

1. Gehen Sie unter **UMS Administration > Globale Konfiguration > Cloud Gateway Konfigurationen.**
2. Wählen Sie in der Liste **Authentifizierungskeys** die gewünschte Passworteingabe und klicken Sie  , um eine E-Mail zu erstellen.
   Der Dialog **Authentifizierungskeys per Mail senden** öffnet sich.
   Der E-Mail-Text enthält alle Daten, die für die Verbindung eines Gerätes mit dem ICG erforderlich sind: Host-Adresse, Fingerabdruck des ICG-Serverzertifikats und Passwort.

3. Geben Sie den **Mail-Empfänger** ein. Um ein Mehrfachpasswort an mehrere Empfänger zu senden, können Sie alle Adressen auf einmal eingeben, indem Sie sie durch ein Semikolon ';' trennen.



4. Klicken Sie **Ok**, um die E-Mail zu versenden.

Manuell erstellte E-Mail oder gedruckter Brief

1. Gehen Sie in der UMS Konsole unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.

2. Wählen Sie die gewünschte Passworteingabe und klicken Sie  , um die Anmeldeinformationen in die Zwischenablage zu kopieren. Die Daten, die für die Verbindung eines Gerätes mit dem ICG benötigt werden, befinden sich in der Zwischenablage: Host-Adresse, Fingerabdruck des ICG-Serverzertifikats und Passwort.

3. Um die Anmeldeinformationen per E-Mail zu senden, fügen Sie die Daten in eine verschlüsselte E-Mail ein. Um die Anmeldeinformationen in einem gedruckten Brief zu senden, fügen Sie die Daten in Ihr E-Mail-Programm oder Ihre Textverarbeitung ein.

Alle Methoden, um Schlüssel für die Erstauthentifizierung von Geräten zu generieren

Um eine Verbindung mit dem ICG herzustellen, muss sich jedes Gerät mit dem ICG authentifizieren. Zu diesem Zweck muss ein Schlüssel für die Erstauthentifizierung generiert werden. Beim ersten Kontakt mit dem ICG muss das Gerät diesen Schlüssel vorweisen. Sie haben folgende Möglichkeiten, Schlüssel für die Erstauthentifizierung zu generieren:

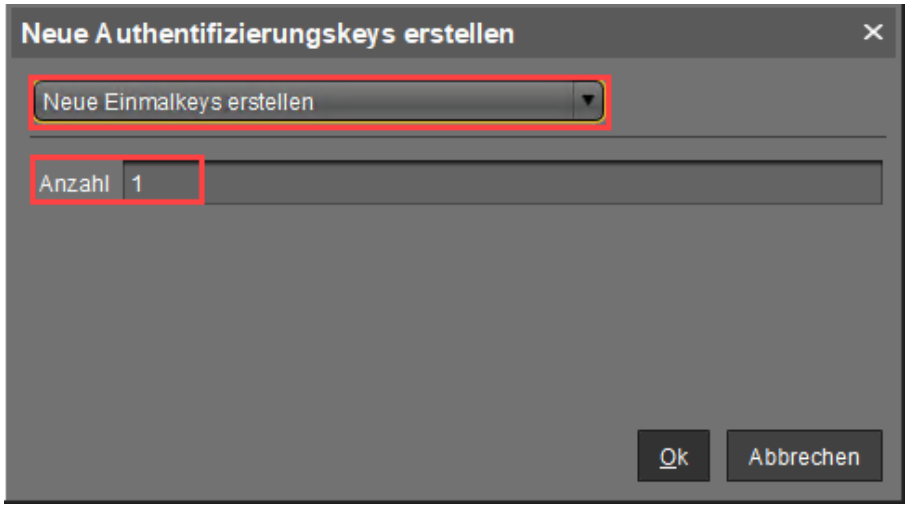
- Einmalschlüssel, die von jedem beliebigen Gerät verwendet werden können, aber nicht von einem anderen Gerät wiederverwendet werden können. Daher muss die Anzahl der Schlüssel mit der Anzahl der Geräte übereinstimmen.
- Einmalschlüssel, die nur von bestimmten Geräten verwendet werden können und nach Gebrauch ungültig werden.
- Mehrfachschlüssel, die von jedem Gerät verwendet werden können und auch nach Gebrauch gültig bleiben.

Wenn die Schlüssel für die Erstauthentifizierung angelegt sind, können Sie mit Passwörter auf die Geräte übertragen (see page 136) fortfahren.

Einmalschlüssel für beliebige Geräte erstellen

1. Gehen Sie in der UMS Konsole zu **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
2. Klicken Sie  .
3. Wählen Sie **Neue Einmalkeys erstellen**.
4. Geben Sie die **Anzahl** der Einmalpasswörter ein, die Sie generieren möchten.

5. Klicken Sie **Ok**.

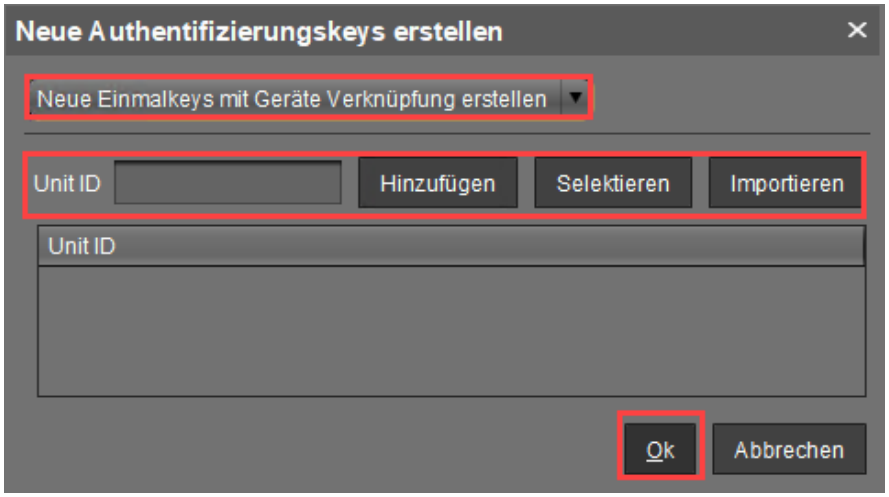


Je nach dem unter **Anzahl** eingegebenen Wert erscheinen ein oder mehrere neue Einträge in der Liste.

Einmalschlüssel für bestimmte Geräte erstellen

1. Gehen Sie unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
2. Klicken Sie  .
3. Wählen Sie **Neue Einmalkeys mit Geräte Verknüpfung erstellen**.
4. Wählen Sie eine Methode, um ein oder mehrere Unit IDs hinzuzufügen:
   - **Hinzufügen:** Geben Sie manuell eine **Unit ID** ein und klicken Sie **Hinzufügen**.
   - **Selektieren:** Klicken Sie **Selektieren** und wählen Sie Geräte mit  .
   - **Importieren:** Klicken Sie **Importieren** und wählen Sie eine CSV-Datei mit Unit IDs aus. Anweisungen zum Erzeugen einer Liste von Geräte-IDs finden Sie unter Unit-ID-Liste für IGEL OS erzeugen.

5. Klicken Sie **Ok**.



   Wenn alles gut gelaufen ist, wird eine Erfolgsmeldung angezeigt.

6. Bestätigen Sie die Meldung.
   Ein oder mehrere neue Einträge erscheinen in der Liste.

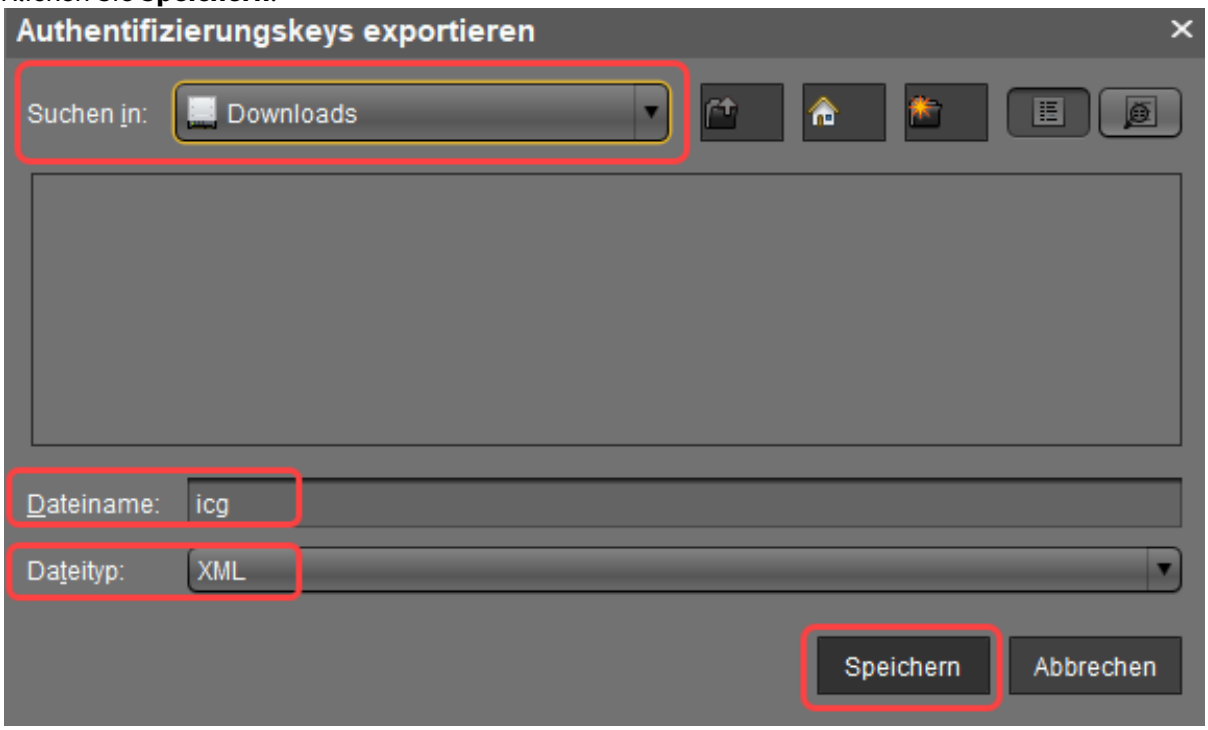
7. Wählen Sie die neuen Einträge aus und klicken Sie auf  , um die Schlüssel zu exportieren.

8. Wählen Sie unter **Suchen in** einen Dateipfad auf Ihrem USB-Stick.

9. Geben Sie einen **Dateinamen** ein, z. B. `icg.xml`

10. Wählen Sie unter **Dateityp** als Dateiformat entweder "XML" oder "HTML".

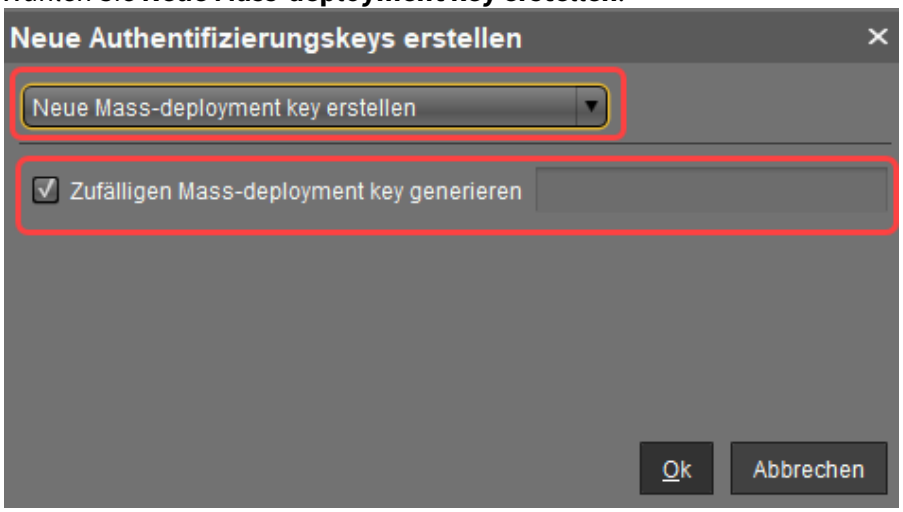
11. Klicken Sie **Speichern**.



Neuen Schlüssel für das Massen-Deployment auf beliebigen Geräte erstellen

1. Schließen Sie einen USB-Stick an den Computer an, auf dem die UMS Konsole läuft.
2. Gehen Sie zu **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.
3. Klicken Sie  .

4. Wählen Sie **Neue Mass-deployment key erstellen**.



5. Aktivieren oder deaktivieren Sie **Zufälligen Massen-deployment key generieren**, um die Methode der Schlüsselerzeugung auszuwählen:
   - ☑ Der Schlüssel wird von der UMS generiert.
   - ☐ Sie können in das Eingabefeld einen eigenen Schlüssel eingeben.

6. Klicken Sie **Ok**.
   Ein oder mehrere neue Einträge erscheinen in der Liste.

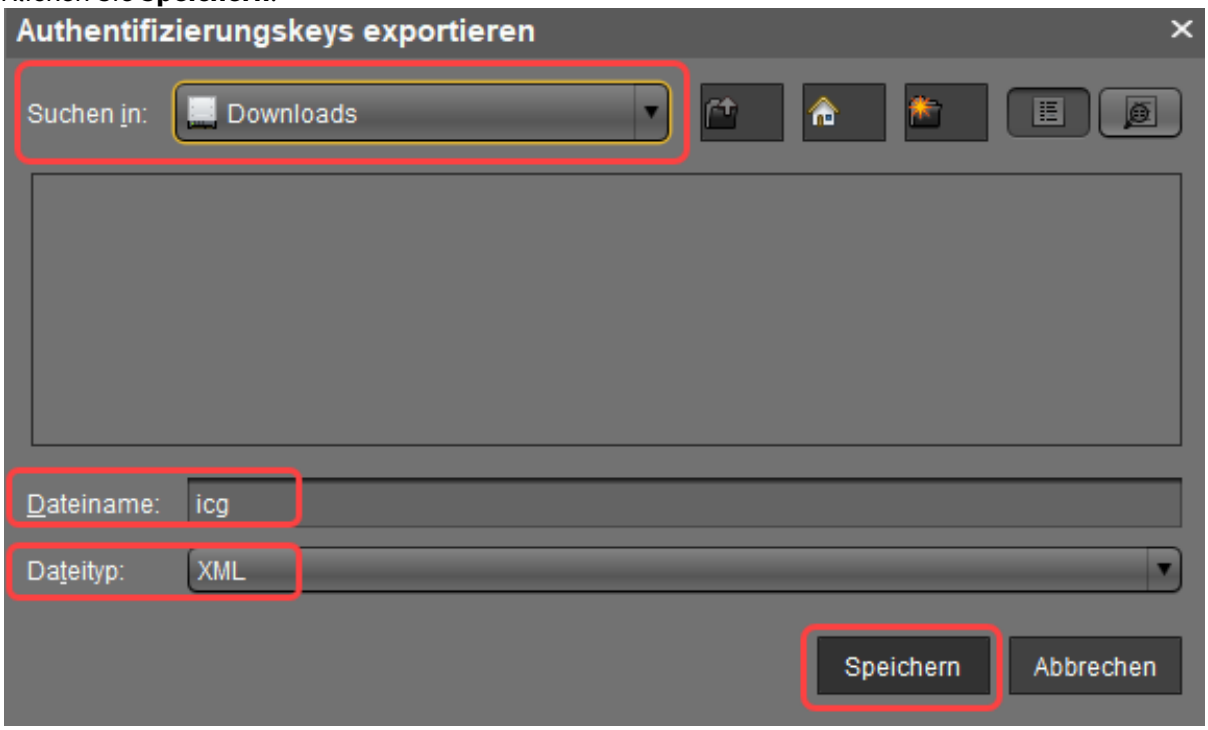
7. Wählen Sie die neuen Einträge aus und klicken Sie  , um die Schlüssel zu exportieren.

8. Wählen Sie unter **Suchen in** einen Dateipfad auf Ihrem USB-Stick.

9. Geben Sie einen **Dateinamen** ein, z. B. `icg.xml`

10. Wählen Sie unter **Dateityp** als Dateiformat entweder "XML" oder "HTML".

11. Klicken Sie **Speichern**.



Schlüssel über E-Mail oder gedruckten Brief verteilen

1. Gehen Sie unter **UMS Administration > Globale Konfiguration > Authentifizierungskeys**.

2. Wählen Sie die gewünschte Passworteingabe und klicken Sie  , um die Anmeldeinformationen in die Zwischenablage zu kopieren.
   Die Daten, die für das Verbinden eines Gerätes mit dem ICG benötigt werden, befinden sich in der Zwischenablage: Host-Adresse, Fingerabdruck des ICG Serverzertifikats und Passwort.

3. Um die Anmeldeinformationen per E-Mail zu senden, fügen Sie die Daten in eine verschlüsselte E-Mail ein. Um die Anmeldeinformationen in einem gedruckten Brief zu senden, fügen Sie die Daten in Ihr E-Mail-Programm oder Ihr Textverarbeitungsprogramm ein.

Installing IGEL Cloud Gateway (UMS 6.02 or Lower)

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

Wie überwache ich das IGEL Cloud Gateway?

IGEL Cloud Gateway (ICG) beinhaltet eine Monitoring-Endpoint-Lösung, die Sie in Ihre bestehende Monitoring-Infrastruktur (z.B. Nagios, SolarWinds, Paessler, Logic Monitor, Sensu, usw.) integrieren können. Mit dem Monitoring Endpoint können Sie die Prozess-/Servicezustände des ICG überwachen und entsprechend reagieren, falls Probleme diagnostiziert werden.

IGEL Umgebung

- ICG 2.04.100 oder höher

Den aktuellen Status des ICG abrufen

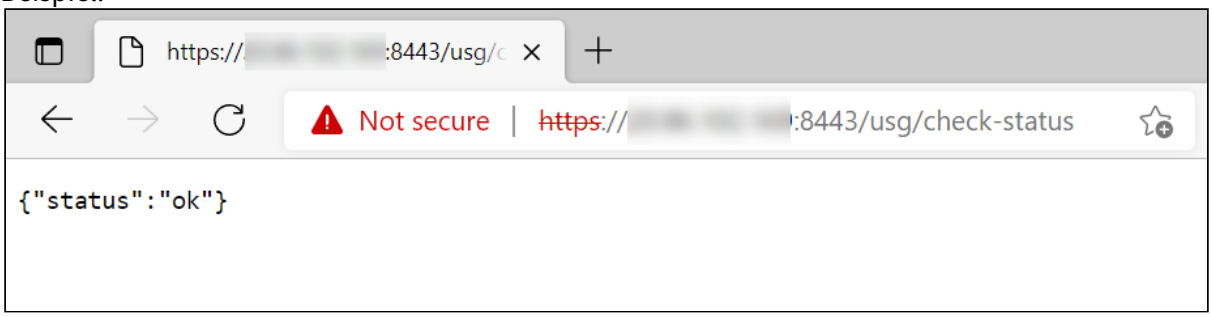
▶ Verwenden Sie die folgende Anfrage, um den Status des ICG Servers zu überprüfen: `https://[host]:8443/usg/check-status`

Wenn Sie zu diesem Zweck einen Browser verwenden und das ICG ein selbstsigniertes Zertifikat hat, kann der Browser eine Sicherheits- / Zertifikatswarnung anzeigen. Akzeptieren Sie das Risiko und fahren Sie fort, oder machen Sie das Zertifikat dem Browser bekannt.

Die folgenden Antworten sind möglich:

1. Wenn der (Prüfstatus-) Dienst läuft, wird der HTTP-Statuscode 200 zurückgesendet. Der Antwortkörper enthält ein `JSON` -Dokument mit Informationen über den ICG Status: `{“status”: ”init|ok|warn|err”}`
   Details dazu finden Sie unten unter ICG Monitoring: Mögliche Status (see page 148).

   Beispiel:

2. Wenn der Prüfstatusdienst nicht erreichbar ist, wird der HTTP-Statuscode 404 zurückgesendet.
3. Andere übliche HTTP-Statuscodes, die auf standardmäßige HTTP-Fehler hinweisen, können auftreten.

Beachten Sie, dass der Status des Servers alle 30 Sekunden aktualisiert wird. Aus Leistungsgründen wird der Status NICHT bei jeder Überwachungsanforderung neu berechnet, d. h. wenn eine Überwachungsanforderung eingeht, aber ein 30-Sekunden-Intervall noch nicht zu Ende ist, wird der zuvor gespeicherte Serverstatus angezeigt.

ICG Monitoring: Mögliche Status

ok	Der ICG Server ist betriebsbereit und läuft.
warn	Es gibt keinen angeschlossenen UMS Server, siehe Die UMS mit dem ICG verbinden (see page 105).
err	Es liegt kein gültiges Zertifikat für ICG vor. Einzelheiten zu ICG Zertifikaten finden Sie unter Installation und Einrichtung (see page 12).
init	Die Initialisierung des ICG Servers ist noch nicht abgeschlossen (z. B. Komponenten werden geladen; die Verbindung zu UMS Servern wird hergestellt). Hinweis: Wenn der Initialisierungsprozess nicht innerhalb von 30 Sekunden abgeschlossen ist, wechselt der Status automatisch zu **err**.

Ähnliche Themen

Wie überprüfe ich den aktuellen Status des IGEL UMS Servers über die vorhandene Monitoring Lösung?

Wie konfiguriere ich die Java-Heap-Größe für ICG?

Sie haben Leistungsprobleme mit dem IGEL Cloud Gateway (ICG). Die Gründe für die Leistungsverschlechterung können vielfältig sein, und es gibt verschiedene Lösungen wie z. B. die Erweiterung des physischen Arbeitsspeichers des Servers, die Aktualisierung des ICG und der UMS Komponenten usw. Der folgende Artikel befasst sich aber ausschließlich mit der Erhöhung des dem ICG zugewiesenen maximalen Speichers (Java-Heap-Größe).

Symptom

Sie haben Leistungsprobleme und es gibt `OutOfMemory` -Fehler in den ICG-Protokolldateien (`usg.log`).

Problem

Die standardmäßige Java-Heap-Größe kann für das ICG unzureichend sein. Dies geschieht normalerweise, wenn:

- eine große Anzahl von Geräten an das ICG angeschlossen ist
- viele Dateien mittlerer oder hoher Größe auf die Geräte übertragen werden (Hintergrundbilder, Bildschirmschoner usw.)

Lösung: Java-Heap-Größe für das ICG ändern

So können Sie die Heap-Größe für die ICG-Version 2.01 und höher anpassen:

1. Stoppen Sie den ICG-Serverdienst.
2. Bearbeiten Sie `/opt/IGEL/icg/usg/webapps/usg.conf`
3. Ändern Sie den Wert `-Xmx` in der folgenden Zeile entsprechend Ihren Anforderungen:
   `JAVA_OPTS='-Djava.awt.headless=true -Djava.security.egd=file:/dev/./urandom -Xms512M -Xmx1024m -server -XX:+UseParallelGC'`
4. Starten Sie den Server neu.

⚠ Die Java-Heap-Größe muss immer INDIVIDUELL, je nach Konfiguration des Servers und Ihrer UMS Umgebung, festgelegt werden, aber sie muss kleiner sein als der verfügbare physische RAM. Allgemeine Empfehlungen finden Sie im Oracle-Artikel Tuning Java Virtual Machines (JVMs)[8]; siehe dort auch die Option `-Xmx` .

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

Beachten Sie auch das Folgende:

- Alle Änderungen der Heap-Größe erfolgen auf eigenes Risiko! Ändern Sie die Heap-Größe nur, wenn Sie genau wissen, was Sie tun. Bei einer fehlerhaften Konfiguration kann es geschehen, dass der ICG Server nicht mehr läuft.
- Eine Verringerung des Speichers kann die ICG-Funktion beeinträchtigen und wird NICHT empfohlen.
- Bei einer ICG-Aktualisierung wird der Wert für die Heap-Größe auf den Standardwert gesetzt. Daher müssen Sie ihn erneut anpassen.

Ähnliche Themen

Wie konfiguriere ich die Java-Heap-Größe für den UMS Server?

Wie konfiguriere ich die Java-Heap-Größe für die UMS Konsole?

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

Zu diesem Artikel liegt noch keine deutsche Übersetzung vor. Wir arbeiten daran und bitten einstweilen um Ihr Verständnis.

ICG Release Notes

Notes for Release ICG 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment ICG 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features ICG 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues ICG 12.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release ICG 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment ICG 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features ICG 12.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release ICG 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment ICG 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features ICG 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues ICG 12.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release ICG 12.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment ICG 12.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features ICG 12.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues ICG 12.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues: Configuration of Unlimited Session Timeout for ICG 12.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.05.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.05.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 2.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 2.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 2.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 2.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 2.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 1.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 1.04.110

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Supported Environment 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 1.04.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 1.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 1.03.120

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 1.03.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

New Features 1.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Resolved Issues 1.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Known Issues 1.02.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Notes for Release 1.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Important Information 1.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Knows Issues 1.01.100

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

ICG Field Experience

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Installing ICG on AWS and Certificate Passing Issue When Using Putty

Dieser Artikel ist nur in englischer Sprache verfügbar. Wir bitten um Ihr Verständnis.

Recommendation for a Free Signed Certificate for ICG

Article Removed

Dieser Artikel wurde von der IGEL Knowledge Base entfernt. Sie finden ihn unter den Dokumenten der IGEL Community:
https://igel-community.github.io/IGEL-Docs-v02/Docs/HOWTO-ICG-Free-Signed-Certificate/