UMS Articles

Devices Supported by IGEL Universal Management Suite (UMS)

Question

Which devices are supported by IGEL Universal Management Suite (UMS)?

Answer

> ⚠ To ensure that you can use all new features of IGEL OS:
>
> ▶ Update your UMS to the current version.
>
> ▶ For all relevant OS 11 profiles, set **Based on** to the appropriate firmware version.
>
> ▶ For OS 12 profiles, note the following: An OS 12 profile configures ALL versions of an app, unless a specific version is set under **Show Versions**.

The latest UMS version supports

- all IGEL devices that have not yet reached their end of maintenance
- devices converted with IGEL OS Creator (OSC)

Older UMS releases support

- IGEL devices that were released before the UMS release
- and that had not reached their end of maintenance at the time of the UMS release

IGEL UMS Communication Ports

The following table shows the default ports which are used by the components of the IGEL Universal Management Suite (UMS) and a UMS infrastructure. Some of these ports are configurable, e.g. web server port 8443, device communication port 30001 for IGEL OS 11 devices, etc. (see Settings - Change Server Settings in the IGEL UMS Administrator).

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
443 (TCP)	IGEL App Portal https://app.igel.com/	Cloud Service	UMS Server	The UMS Server imports apps from the IGEL App Portal.
443 (TCP)	IGEL Onboarding Service https://obs.services.igel.com[1]	Cloud Service	UMS Server	The UMS Server validates the onboarding token.
443 (TCP)	IGEL Insight Service https://insight.services.igel.com	Cloud Service	UMS Server	The UMS Server transfers analytical and usage data to IGEL.
443 (TCP)	Automatic License Deployment (ALD)	IGEL licensing server (at susi.igel.com)	UMS Server	The UMS Server requests licenses; see UMS Contacting the Licensing Server (see page 130).
443 (TCP)	Automatic License Deployment (ALD)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	The UMS Server requests the connection details required for connecting to the IGEL license server (at susi.igel.com). See UMS Contacting the Licensing Server (see page 130).

[1] https://obs.services.igel.com/

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
8443 (TCP)	Core	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Console / UMS Web App	See UMS with Internal Database (see page 91) or UMS with External Database (see page 92).
8443 (TCP)	Unified Protocol	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device opens a WebSocket for data exchange (all communication incl. registration via IGEL Onboarding Service or One-Time Password method, file transfer, firmware customization and license transfer, secure shadowing, secure terminal) For more information on Unified Protocol, see Overview of the IGEL UMS.
8443 (TCP)	UMS as an Update Proxy	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device contacts the UMS Server to download app updates.
30002 (TCP)	Core (directly, without ICG)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	HA Load Balancer	If the UMS Server and the HA Load Balancer are running on the same host, the UMS Server will use port 30002 instead of 30001, and the HA Load Balancer will use port 30001 (relevant for IGEL OS 11 only).

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
30001 (TCP)	Unified Protocol (automatic registration or registration after scanning)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 12 device	The device requests a registration token if the UMS Server was detected in the company network (see Registering Devices Automatically on the IGEL UMS and Importing Devices) or the device received a registration request after it was scanned (see Scanning the Network for Devices and Registering Devices on the IGEL UMS).
30001 (TCP)	Core (direct device communication, not used with communication via ICG)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	See Devices Contacting UMS (see page 99).
8443 (TCP)	Core (file transfer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device requests a file from the UMS; see UMS and Devices: File Transfer (see page 122).
8443 (TCP)	Core (firmware customization)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The UMS provides files for customizing the look and feel of the device's GUI; see UMS and Devices: File Transfer (see page 122).

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
88 (TCP/UDP)	Core (if Active Directory is used), Shared Workplace	MS Active Directory Service	UMS Server	The UMS Server sends a Kerberos request to MS Active Directory.
389 (TCP)	Core (if Active Directory is used), Shared Workplace	MS Active Directory Service	UMS Server	The UMS Server sends an LDAP request to MS Active Directory.
1527 (TCP)	Core (if Apache Derby is used)	Apache Derby database (Derby Network Server)	UMS Server	See UMS with External Database (see page 92).
636 (TCP)	Core (if LDAPS server is used)	LDAPS server (other than MS Active Directory)	UMS Server	The UMS Server sends an LDAP request over SSL.
1433 (TCP)	Core (if MS SQL Server is used)	Microsoft SQL Server database	UMS Server	See UMS with External Database (see page 92).
1521 (TCP)	Core (if Oracle is used)	Oracle database	UMS Server	See UMS with External Database (see page 92).
5432 (TCP)	Core (if PostgreSQL is used)	PostgreSQL database	UMS Server	See UMS with External Database (see page 92).
8443 (TCP)	Core (licenses)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The UMS provides license files for the devices; see UMS and Devices: File Transfer (see page 122).
Auto ("high port") (UDP)	Core (online check)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device responds to a message sent by the UMS to check if the device is online. The port number to be used is contained in the UDP packet sent by the UMS.

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
30005 (TCP/ UDP)	Core (scanning for device)	Device (OS 12 & OS 11) (UMS agent)	Device (OS 12 & OS 11)	The device responds to a broadcast sent by the UMS during a scan. The port number to be used is contained in the UDP packet sent by the UMS. See UMS Server.
Auto ("high port") (UDP)	Core (scanning for device)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	Device (OS 12 & OS 11)	The device responds to a broadcast sent by the UMS during a scan. The port number to be used is contained in the UDP packet sent by the UMS.
30022 (TCP)	Core (secure terminal)	IGEL OS 11 device (UMS agent)	UMS Server	See UMS and Devices: Secure Terminal (see page 117).
5900 (TCP)	Core (shadowing)	IGEL OS 11 device (UMS agent)	UMS Console	The UMS Console initiates a VNC session for shadowing; see UMS and Devices: Shadowing (see page 103).
5900 (TCP)	Core (shadowing) via UMS Web App	IGEL OS 11 device (UMS agent)	UMS Server	The UMS Web App triggers the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; see UMS and Devices: Shadowing (see page 103).

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
9080 (TCP)	Core (unencrypted, no SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	The device requests a file from the UMS (regular file transfer or Universal Firmware Update). This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.
Auto ("high port")	Core (unencrypted, no SSL)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Console	The GUI is started via Java Webstart console. This port is only used if **Allow SSL Connections only** is deactivated in the UMS Administrator. If **Allow SSL Connections only** is activated, port 8443 is used for firmware updates and file transfer.
443 (TCP)	Core (Universal Firmware Update)	IGEL download server (HTTP server at fwus.igel.com)	UMS Server	See UMS Contacting the Download Server to Check for New Updates (see page 124).
8443 (TCP)	Core (Universal Firmware Update)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	IGEL OS 11 device	In the course of a Universal Firmware Update, the device requests a file from the UMS; see UMS and Devices: File Transfer (see page 122).
9 (UDP)	Core (Wake on LAN)	Device (OS 12 & OS 11)	UMS Server	The UMS Server sends magic packets to the devices.

Port (Protocol)	Required by UMS Feature	Who is Listening? Applications/ Service Binding to Port	Who is Talking? Applications /Services Initiating Communications	Description
8443 (TCP)	Core (with ICG)	ICG (IGEL Cloud Gateway)	UMS Server	See Devices and UMS Server Contacting Each Other via ICG (see page 96) or UMS Server.
8443 (TCP)	Core (with ICG)	ICG (IGEL Cloud Gateway)	Device (OS 12 & OS 11)	See Devices and UMS Server Contacting Each Other via ICG (see page 96).
6155 (UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 6155 and use it for communication.
8443 (TCP)	High Availability (HA) and Distributed UMS	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	File synchronization between UMS Servers
61616 (TCP/ UDP)	High Availability (HA)	HA Load Balancer UMS Server	HA Load Balancer UMS Server	Both HA Load Balancer and UMS Server listen on port 61616 and use it for communication.
8443 (TCP)	IMI	UMS Server (Windows: service IGELRMGUIServer; Linux: daemon igelRMServer)	3rd party component using IMI (IGEL Management Interface)	See IGEL Management Interface (IMI) (see page 94).

- IGEL Universal Management Suite Network Configuration (see page 12)

IGEL Universal Management Suite Network Configuration

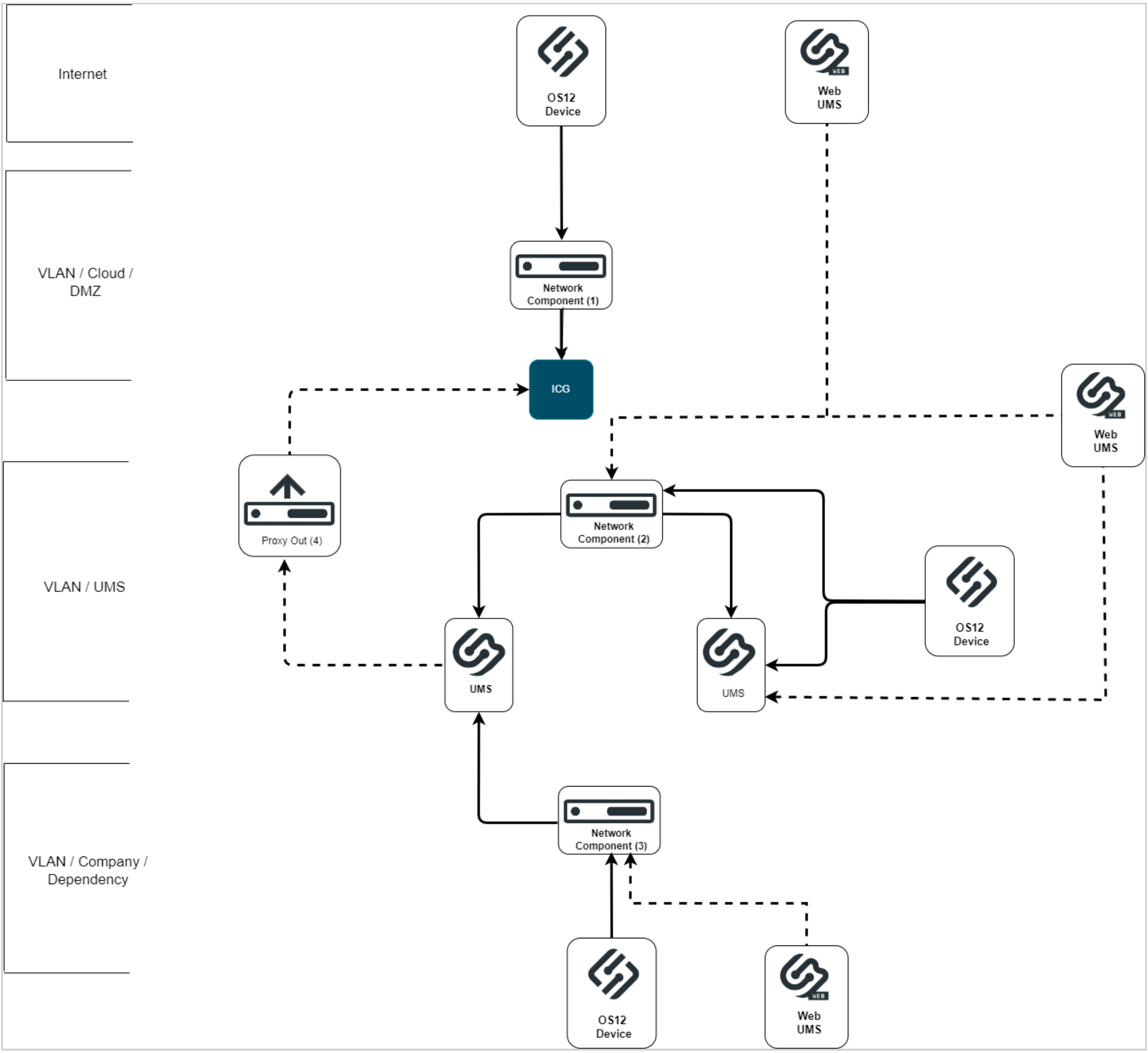
This article describes the Universal Management Suite (UMS) and IGEL Cloud Gateway (ICG) Integration with Network components like Firewalls and Reverse Proxies.

For Reverse Proxy configuration examples, see:

- NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading (see page 21)
- F5 BIG IP: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 38)
- Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading (see page 61)

UMS Network Configurations

The diagram shows a network configuration with possible network boundaries where network components like Reverse Proxies, Proxies, Firewalls and Loadbalancer can be placed.

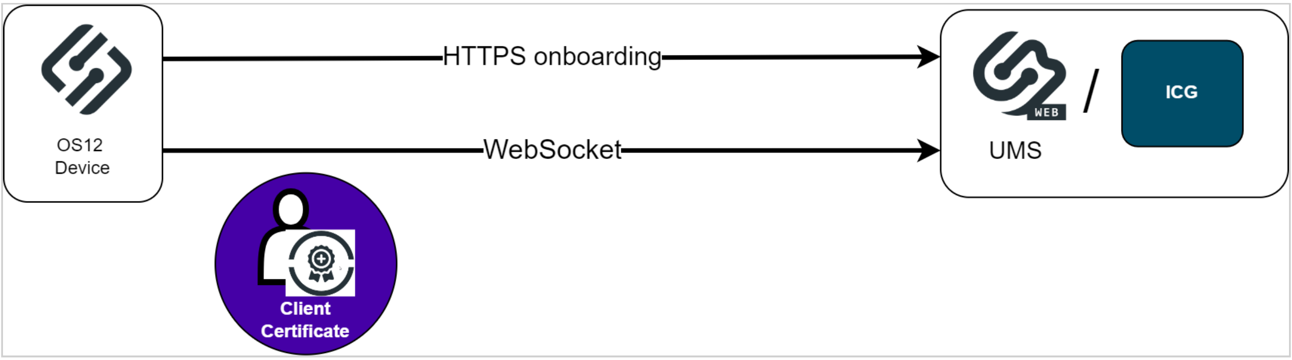


There are typically three different positions for these components:

- Device and ICG Server
- Device and UMS Server
- ICG and UMS Server

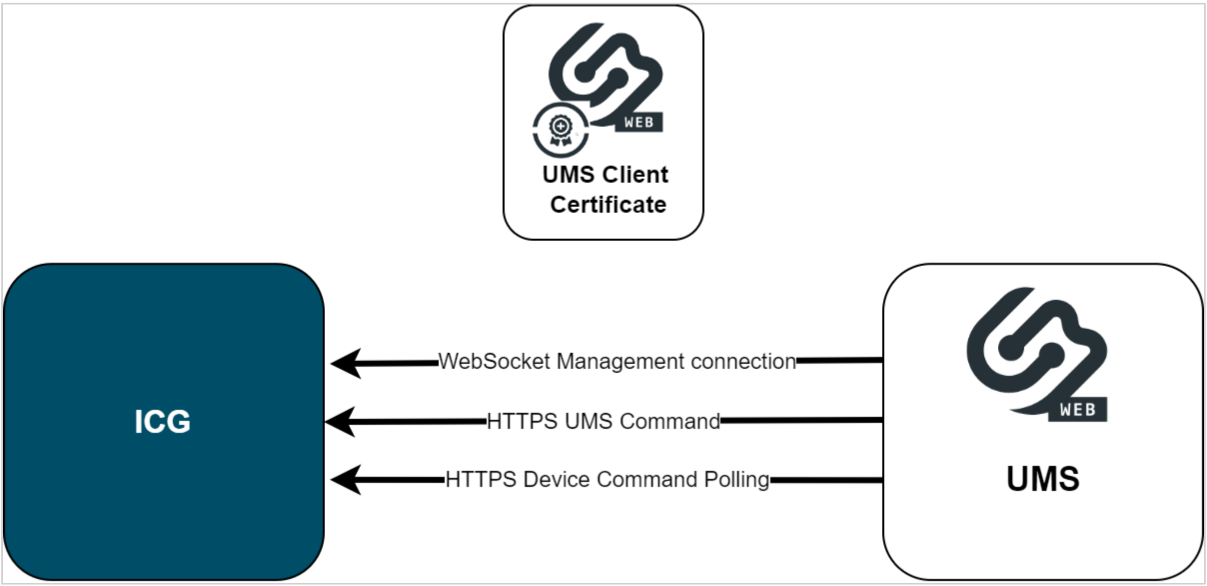
Device to ICG / UMS Communication

The communication of the devices to UMS or ICG consists of two different types. Regular HTTPS calls for the device registration and a WebSocket connection with Mutual TLS for device management. These must be considered for Proxy, Reverse Proxy and Firewall configuration.



ICG UMS Communication

The communication of the UMS to the ICG is also based on WebSocket and regular HTTPS calls. Every request is initialized by the UMS and uses Mutual TLS. A HTTPS Proxy can be configured for these connections in the UMS.



In case a Network Component is placed between these servers be aware of these connections. Connection problems could be observed when Deep Packet Inspection (DPI) is activated on a Firewall. The chapter SSL Offloading is only applicable for device to UMS / ICG connections. It is not supported for the communication between ICG and UMS.

SSL Passthrough

SSL Passthrough passes encrypted HTTPS traffic from a client to the server and back again without any decryption or deep packet inspection. The HTTPS traffic is not manipulated so this configuration of network components shouldn't have any impact on the ICG or UMS functionality. Please refer to the documentation of your Web Component for the appropriate settings.

Example

nginx – one possible configuration of passthrough:

```
## tcp LB and SSL passthrough for backend ##
stream {
    upsream umsserver{
        server 192.168.1.100:8443 max_fails=3 fail_timeout=10s;
        server 192.168.1.100:8443 max_fails=3 fail_timeout=10s;
    }
    server{
        listen 443;
        proxy_pass umsserver;
        proxy_next_upstream on;
    }
}
```

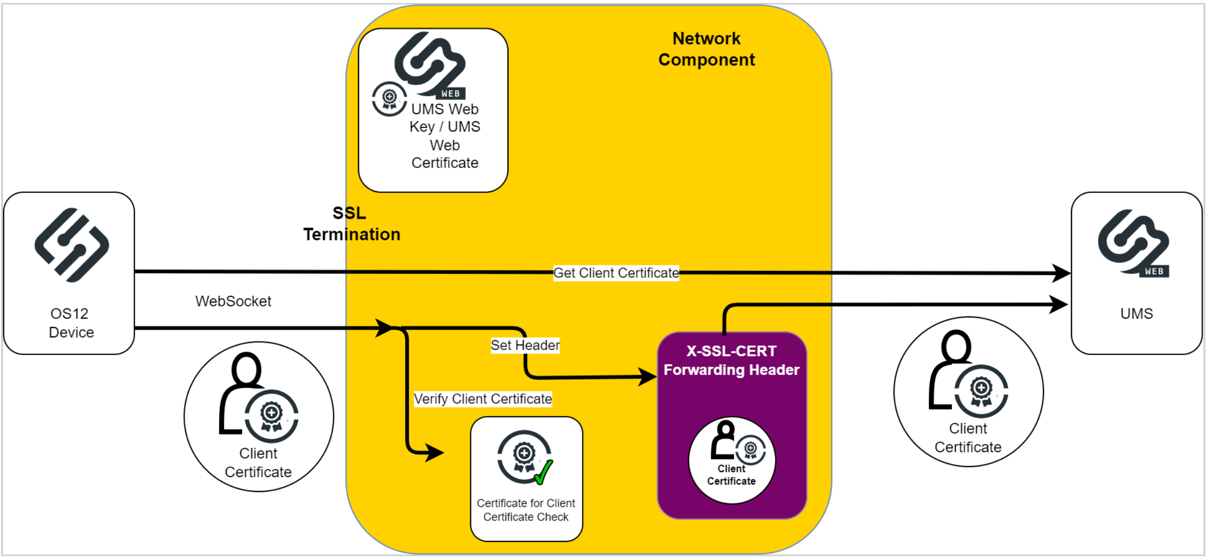
The configuration must be added to the nginx config file:

```
user nginx;
worker_process auto;
error_log /var/log/nginx/error.log warn;
pid       /var/run/nginx.ped;
events{
    worker_connections 1024;
}
http {
    include     /etc/nginx/mime.types;
    default_type application/octet-stream;
    sendfile    on;
    #tcp_nopush     on;
    keepalive_timeout 65;
    #gzip on;
    include/etc/nginx/conf.d/*.conf;
}
include/etc/nginx/passthrough.conf;
```

SSL Offloading

SSL Offloading means that the network component terminates the SSL connection and decrypts the data. This decrypted data could be sent directly to the Server which also sends decrypted data to the network component which handles the encryption.

The Network component could also inspect the decrypted traffic und encrypt it again before sending it to the server. The UMS supports only this type of communication with encrypted data until now. The diagram shows the required tasks for SSL Offloading on the Network Component for the device to UMS direction.



The Steps to configure SSL Offloading of a Network Component:

- Configure Listener for SSL Termination. This includes:
  - **Port**: UMS Web Port
  - Key and Certificate: UMS Web Key and UMS Web Certificate
- Configure Client Certificate Check and Client Certificate Forwarding. This includes:
  - SSL Client Certificate Check
  - Read SSL Client Certificate and add it to a Forwarded Header
- If necessary, configure the WebSocket Upgrade Header

The processing of forwarded Client Certificates must be activated on UMS side. The configuration file is `(Install Dir)/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml.`

```
igel:
 client-cert-forwarding:
    enabled: false
    client-cert-forwarded-header: X-SSL-CERT
```

Set client-cert-forwarding -> enabled to true.

The forwarding Header can be configured. The X-SSL-CERT Header value can be changed but be aware to change the corresponding value in the network component configuration.
The ICG configuration is analog except for the ICG Port, ICG KEY and ICG Certificate parameters.
The processing of forwarded Client Certificates must also be activated on ICG side.
The configuration file is (Install Dir)/IGEL/icg/usg/conf/application-prod.yml

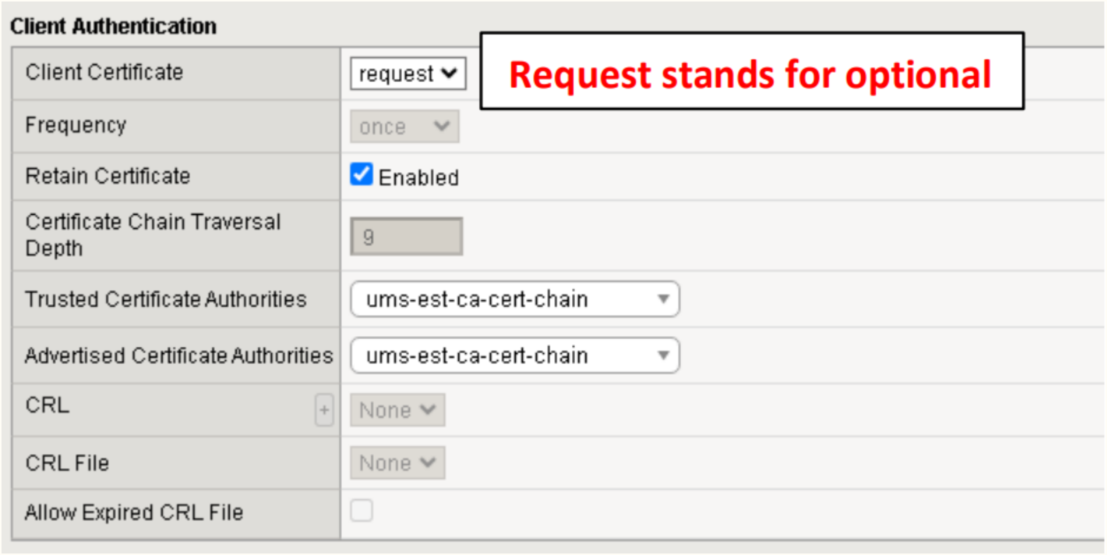
Required Features of the Network Component

Client Certificate check and forwarding

The OS12 device uses two types of connections to the UMS. One is a direct https connection to onboard the device and get a Client Certificate. The other one is a WebSocket connection for managing the device with mutual TLS. So, the used Reverse Proxy must at least implement one of the following configuration options:

1. The **Client Certificate check is optional**, so the connection will always be forwarded but the certificate is only added when a valid certificate has been sent. Additionally, the WebSocket Upgrade must be supported.

F5 Big-IP Example



Client Authentication

Client Certificate	request
Frequency	once
Retain Certificate	☑ Enabled
Certificate Chain Traversal Depth	9
Trusted Certificate Authorities	ums-est-ca-cert-chain
Advertised Certificate Authorities	ums-est-ca-cert-chain
CRL	None
CRL File	None
Allow Expired CRL File	☐

Request stands for optional

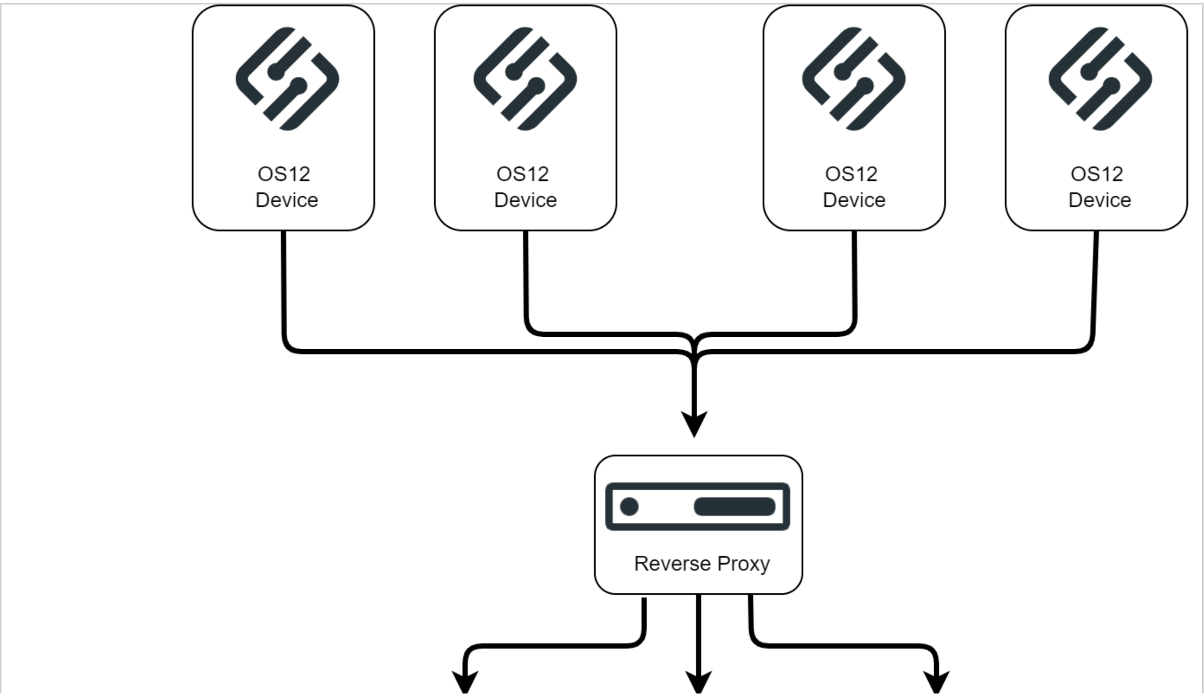
2. **Path dependent forwarding** configuration must be supported. The nginx Reverse Proxy supports this type. The listing shows a configuration for the WebSocket endpoint which requires the Client Certificate, add it to the http header and add the WebSocket Upgrade header. See also, IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading
The other configuration is required for the onboarding endpoint:

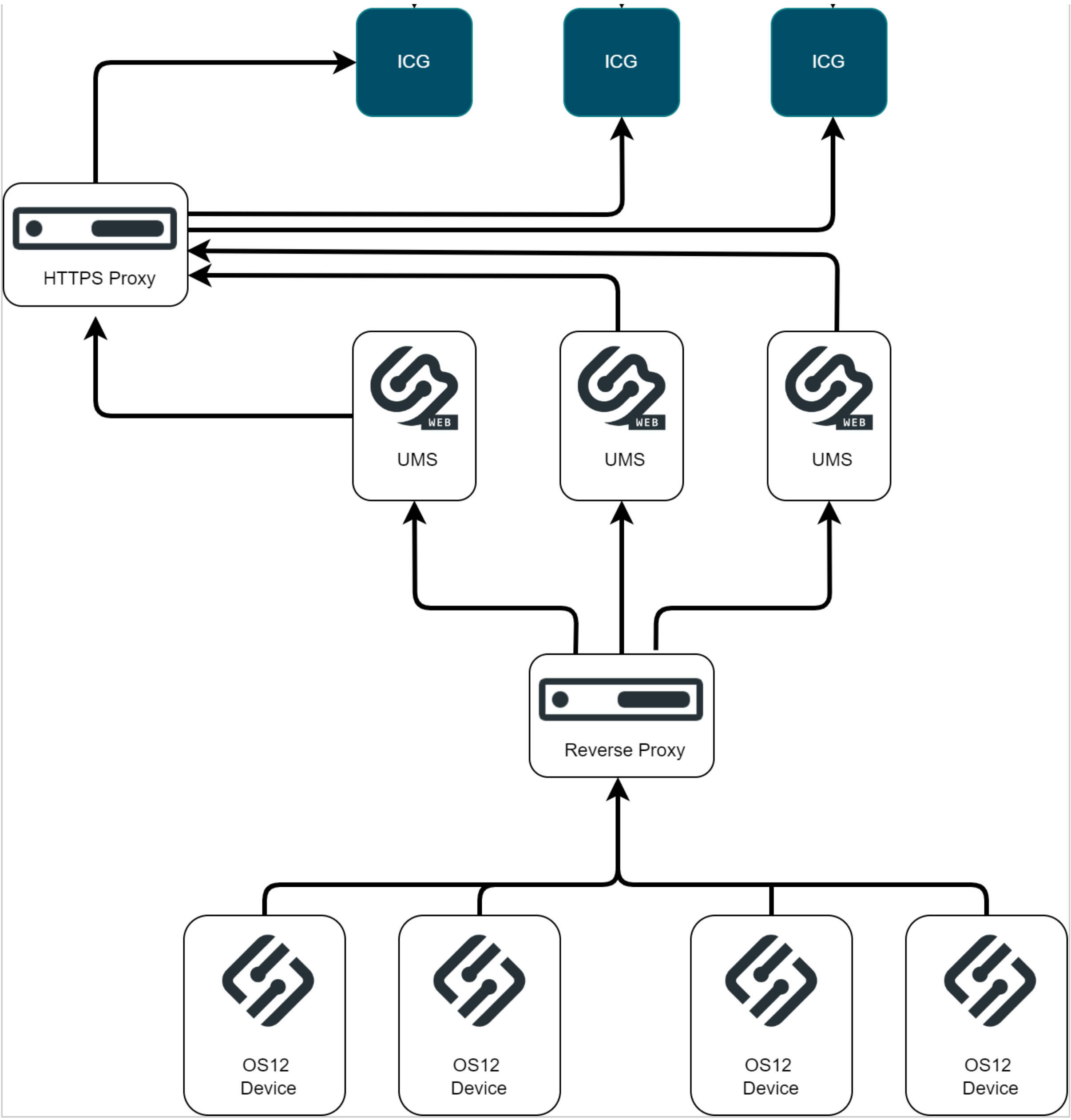
```
# Configuration for WebSocket Endpoints
 location~/device-connector/device/(ws-connect|portforwarding) {
    proxy_pass https://umsserver;
    proxy_set_header X-SSL-CERT $ssl_client_escaped_cert;# client certificate
in current connection
    proxy_set_header Upgrade $http_upgrade; #Set upgrade header
    proxy_set_header Connection $connection_upgrade;
}
#Configuration for all other endpoints
 location / {
    proxy_pass https//umsserver;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    proxy_ssl_protocols TLSv1.3;
}
```

UMS HA environment with Reverse Proxy, Loadbalancer

The device to UMS / ICG connection can be load balanced.
The UMS Web certificate and ICG certificate must correspond to the IP or Fully Qualified Domain Name of the servers and configured network component. Consider the Subject Alternative Names of the certificate. Wildcard certificates are possible. Be aware to set the UMS cluster address and the UMS public address.
The example shows a nginx upstream server configuration with multiple UMS server entries.

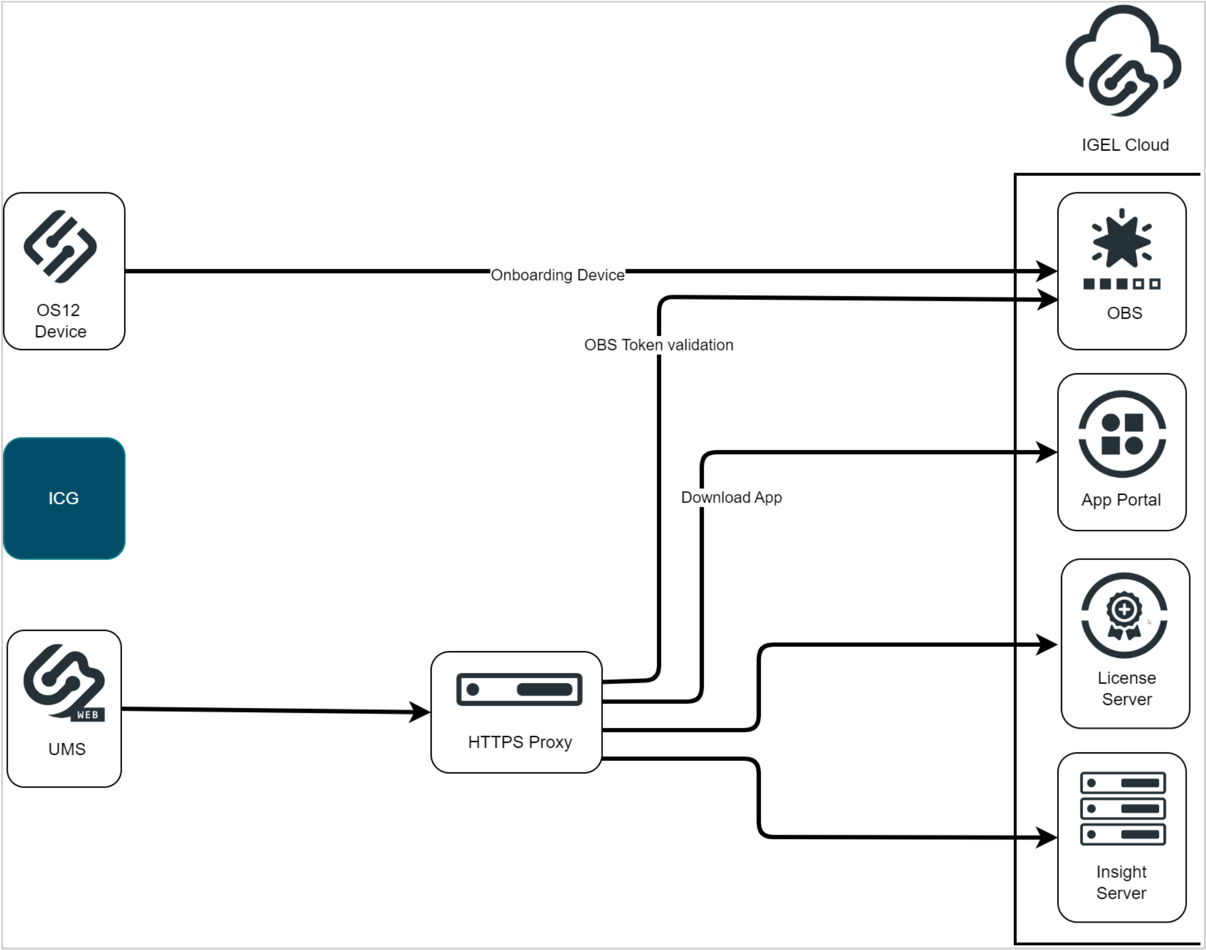
```
upstream umsserver {
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
    server 192.168.27.96:8843 max_fails=3 fail_timeout=10s;
 }
```





IGEL Cloud Service Configuration

The communication to the IGEL Cloud might be influenced also by network components. In case of the device onboarding via the Onboarding Service the OBS must be reachable for the device. The UMS server also connects to the IGEL Cloud Services. Here the required reachable services are the Onboarding Service (OBS), the License Portal, the App Portal and the Insight Service. These connections can go over a Proxy but must be configured in the UMS. A network component like a firewall with Deep Packet Inspection could result in connection problems.


IGEL Cloud
OS12 Device
Onboarding Device
OBS
OBS Token validation
ICG
App Portal
Download App
License Server
UMS
HTTPS Proxy
Insight Server

NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading

This article describes the configuration of the IGEL Universal Management Suite (UMS) and NGINX for SSL offloading. You can use this document when you want the SSL to be terminated not at the UMS Server, but at the load balancer / reverse proxy. The article is based on the example of NGINX. For more information on NGINX, see https://www.nginx.com/resources/glossary/nginx/.

⚠ General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
As the reverse proxy is an external software we cannot provide full support for each version.

ⓘ A reverse proxy / external load balancer can be used if you manage IGEL OS 12 devices only. See IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.

The tasks to be done involve:

- Configuring the Cluster Address and checking UMS web certificates
- Exporting the UMS web certificate chain
- Extracting the private key and certificate chain
- Exporting the client certificate chain
- Installing NGINX (example based on Ubuntu)
- Configuring NGINX
- Configuring the UMS
- Configuring the IGEL Cloud Gateway (ICG) if used

Requirements

- IGEL UMS version 12.02.100 or higher
- If the ICG is used: ICG version 12.02.100 or higher
- In the case of the Distributed UMS or High Availability installations, the time on all servers must be synchronized.

ⓘ For extracting keys and certificate chains, you will require a suitable tool like "Keystore Explorer". Please use the latest version of such tools.
Please also make sure that you use Java 17.

Limitations

- The scan and register command can only be used when an endpoint device can open a direct connection to the UMS. Thus, when an external load balancer / reverse proxy is configured, the scan and register feature might not be usable.

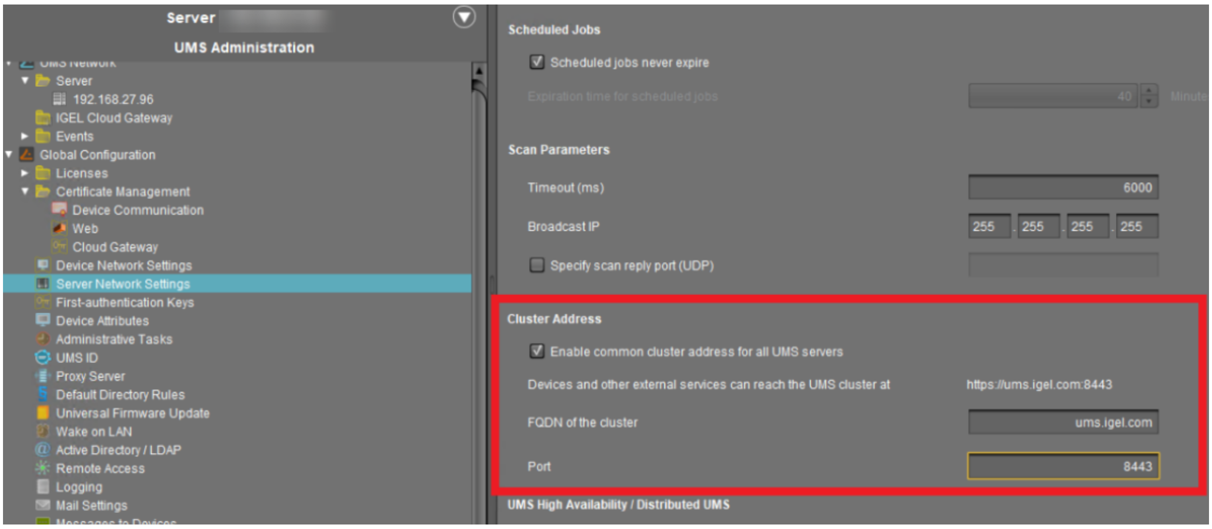
Configuring the Cluster Address and Checking UMS Web Certificates

If you are using an external load balancer / reverse proxy, you have to update the FQDN of the UMS cluster as an external address. This FQDN of the UMS cluster must be included into your web certificate, and the corresponding certificate must be assigned to all UMS servers:

1. In the UMS Console, set the Cluster Address under **UMS Administration > Global Configuration > Server Network Settings > Cluster Address** and configure a web certificate for all servers. For detailed information, see Server Network Settings in the IGEL UMS.

   For information on hostnames, Cluster Address, FQDNs, see also Troubleshooting: Error 38 during the Onboarding of an IGEL OS 12 Device. For general information on web certificates, see Web.

   > Use subject alternative names (SAN) if the IP addresses or hostnames that are used for the UMS and your load balancer / reverse proxy are different.



Scheduled Jobs

☑ Scheduled jobs never expire

Expiration time for scheduled jobs: 40 Minute

Scan Parameters

Timeout (ms): 6000

Broadcast IP: 255 . 255 . 255 . 255

□ Specify scan reply port (UDP)

Cluster Address

☑ Enable common cluster address for all UMS servers

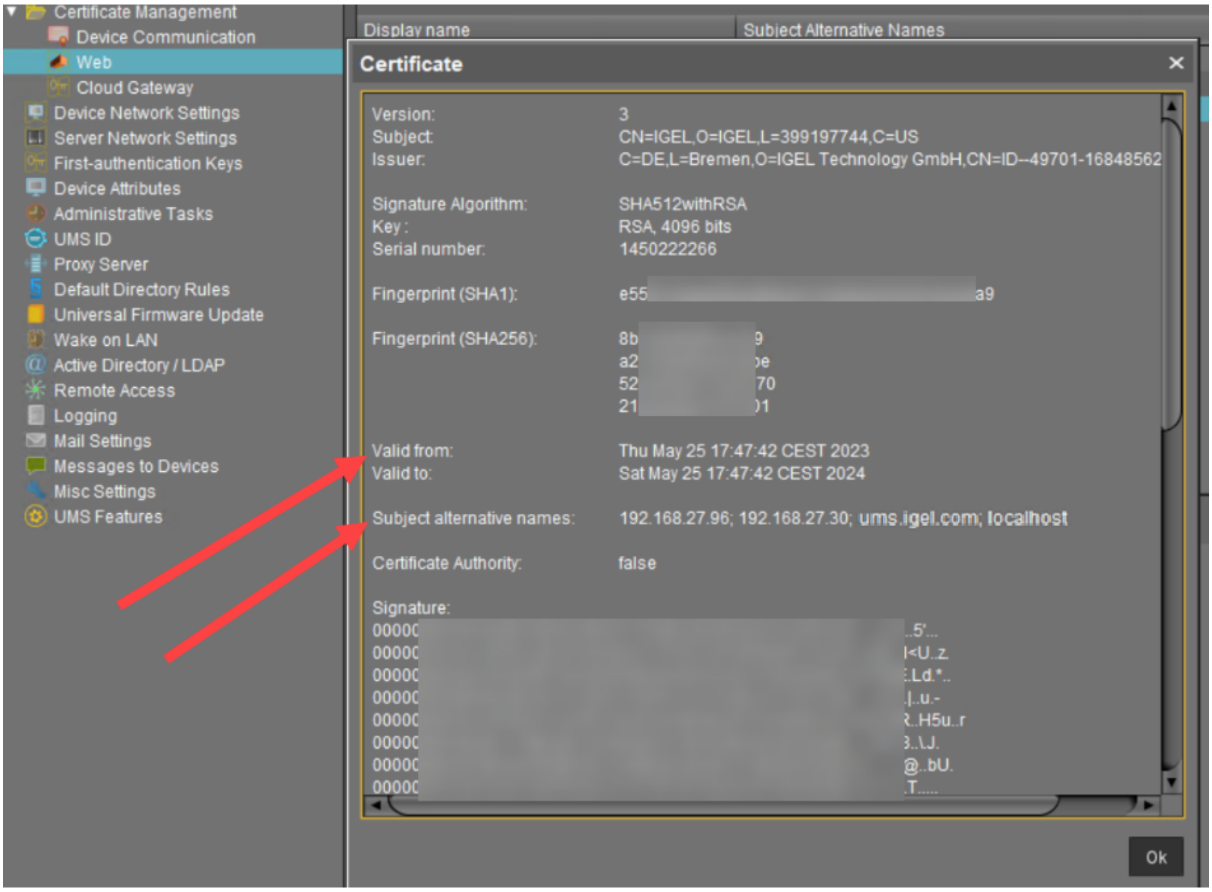
Devices and other external services can reach the UMS cluster at https://ums.igel.com:8443

FQDN of the cluster: ums.igel.com

Port: 8443

UMS High Availability / Distributed UMS

2. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web** and check again that you use a valid certificate for the UMS and your load balancer / reverse proxy. If not, create a valid web certificate.



Version: 3
Subject: CN=IGEL,O=IGEL,L=399197744,C=US
Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848562

Signature Algorithm: SHA512withRSA
Key : RSA, 4096 bits
Serial number: 1450222266

Fingerprint (SHA1): [redacted]

Fingerprint (SHA256): [redacted]

Valid from: Thu May 25 17:47:42 CEST 2023
Valid to: Sat May 25 17:47:42 CEST 2024

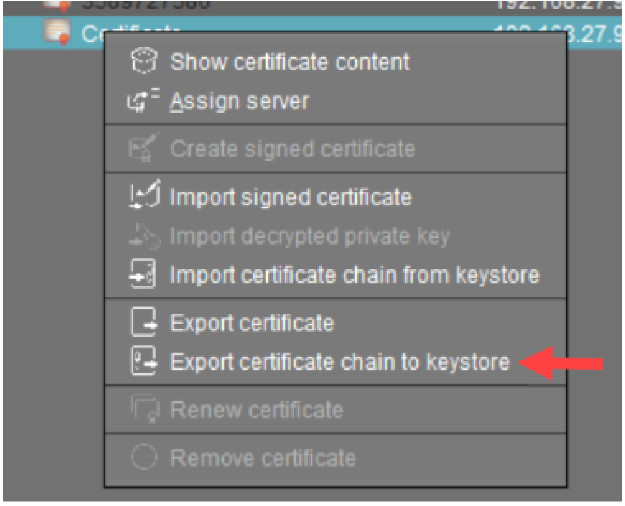
Subject alternative names: 192.168.27.96; 192.168.27.30; ums.igel.com; localhost

Certificate Authority: false

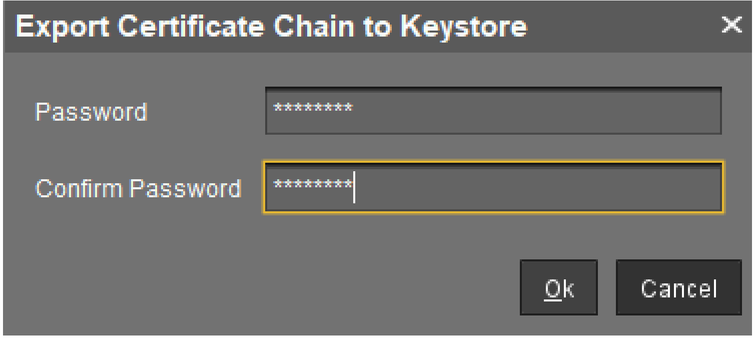
Signature: [redacted]

Exporting the UMS Web Certificate Chain

1. Select the currently used end certificate and export the certificate chain.


Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from keystore
Export certificate
Export certificate chain to keystore
Renew certificate
Remove certificate

2. Set the password.

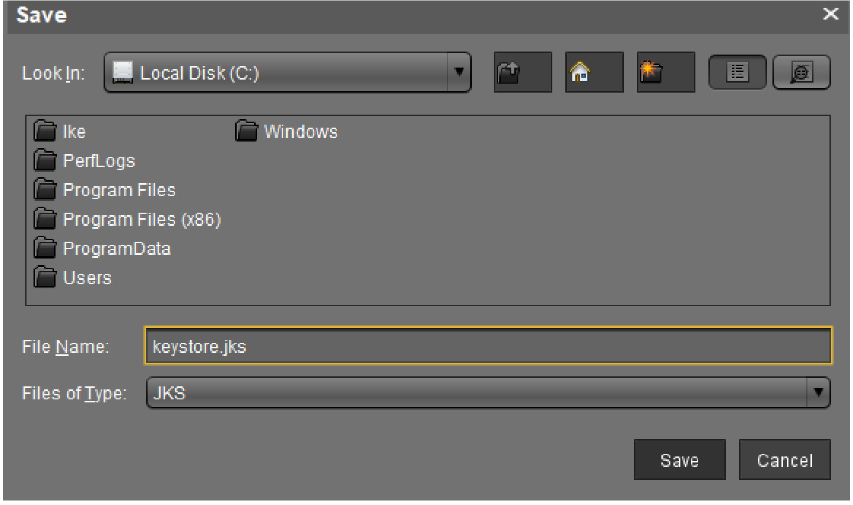


Export Certificate Chain to Keystore

Password: ********

Confirm Password: ********

3. Define the path and the file name.



Save

Look In: Local Disk (C:)

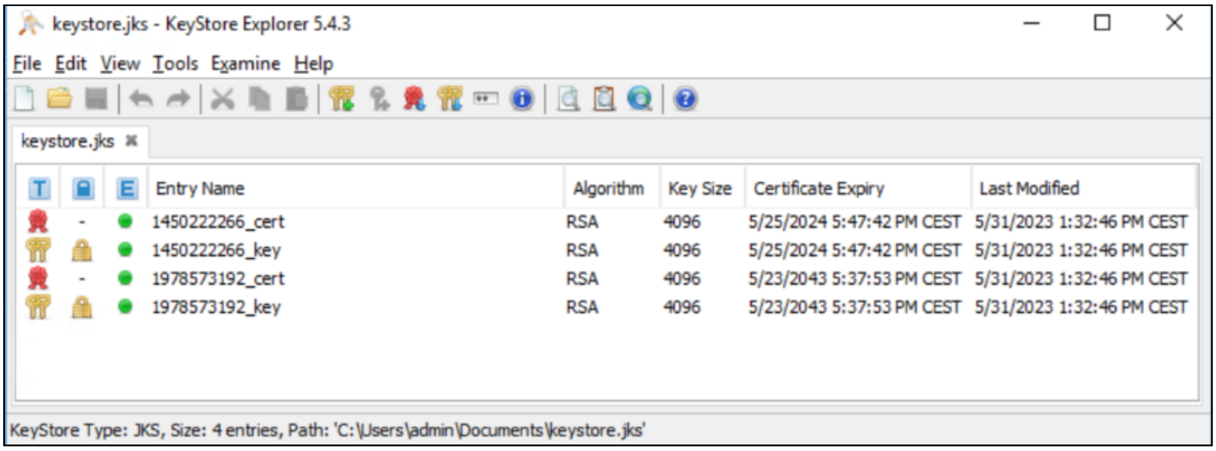
File Name: keystore.jks

Files of Type: JKS

Extracting the Private Key and Certificate Chain

The exported keystore file contains several keys and certificates, at least the root and the currently used keys and certificates. The currently used key and certificate chain must be extracted from this file. You can use any suitable tool for this, e.g. "Keystore Explorer":

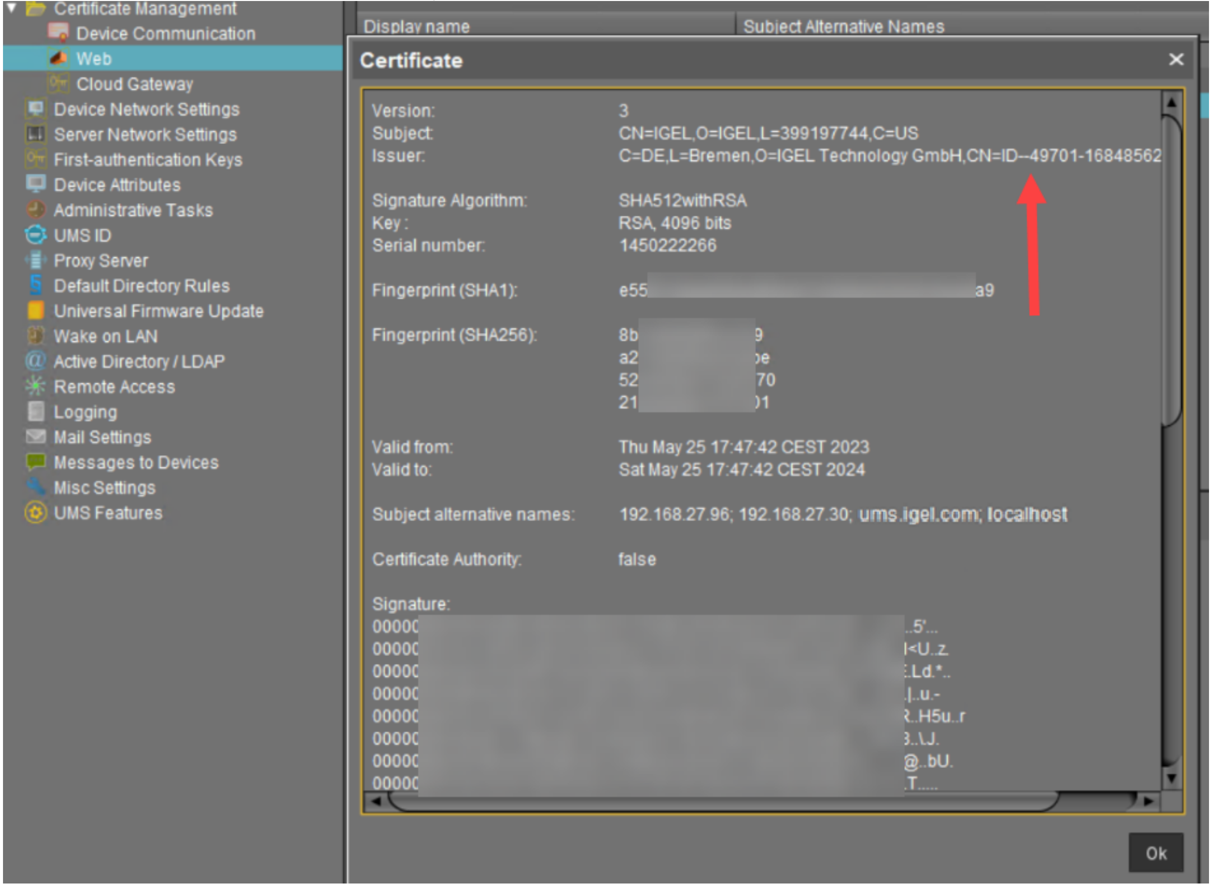
1. Open the exported file and enter the password you used in the UMS for the export.
   Several entries are shown:


keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	🔒	●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
	🔒	●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

KeyStore Type: JKS, Size: 4 entries, Path: 'C:\Users\admin\Documents\keystore.jks'

2. Find the currently used key.
   For this, you can simply compare the ID of the currently used certificate displayed in the UMS and the ID in the certificate details in Keystore Explorer.



Version: 3
Subject: CN=IGEL,O=IGEL,L=399197744,C=US
Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848562

Signature Algorithm: SHA512withRSA
Key: RSA, 4096 bits
Serial number: 1450222266

Fingerprint (SHA1): e55[redacted]a9

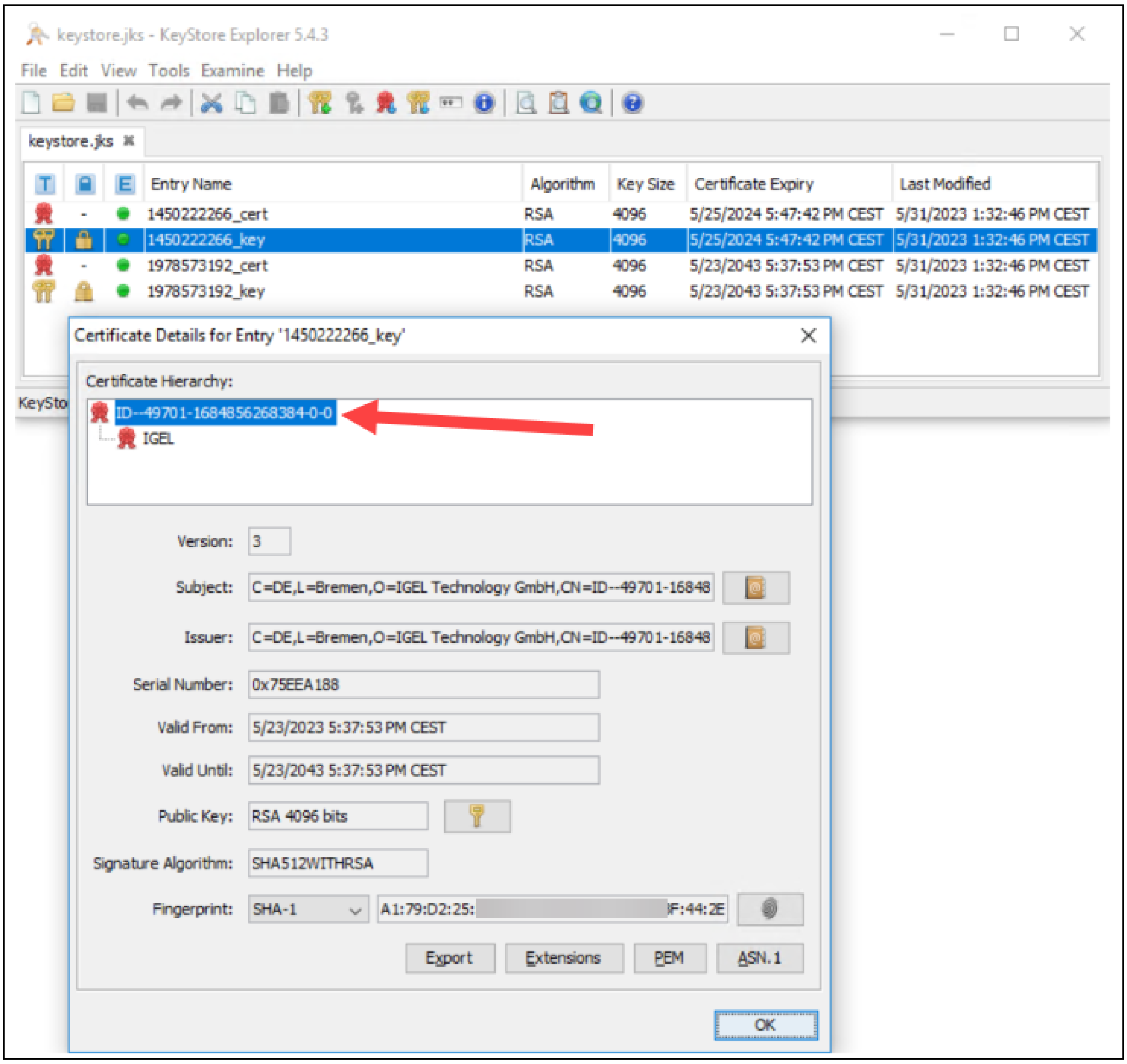
Fingerprint (SHA256): 8b[redacted]9
a2)e
52 70
21)1

Valid from: Thu May 25 17:47:42 CEST 2023
Valid to: Sat May 25 17:47:42 CEST 2024

Subject alternative names: 192.168.27.96; 192.168.27.30; ums.igel.com; localhost

Certificate Authority: false

Signature:
0000C[redacted] ..5'...
0000C |<U..z.
0000C :.Ld.*..
0000C .|..u.-
0000C R..H5u..r
0000C 3..\.J.
0000C @..bU.
0000C .T.....


keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks
KeySto

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

Certificate Details for Entry '1450222266_key'

Certificate Hierarchy:

- ID--49701-1684856268384-0-0
  - IGEL

Version: 3

Subject: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Serial Number: 0x75EEA188

Valid From: 5/23/2023 5:37:53 PM CEST

Valid Until: 5/23/2043 5:37:53 PM CEST

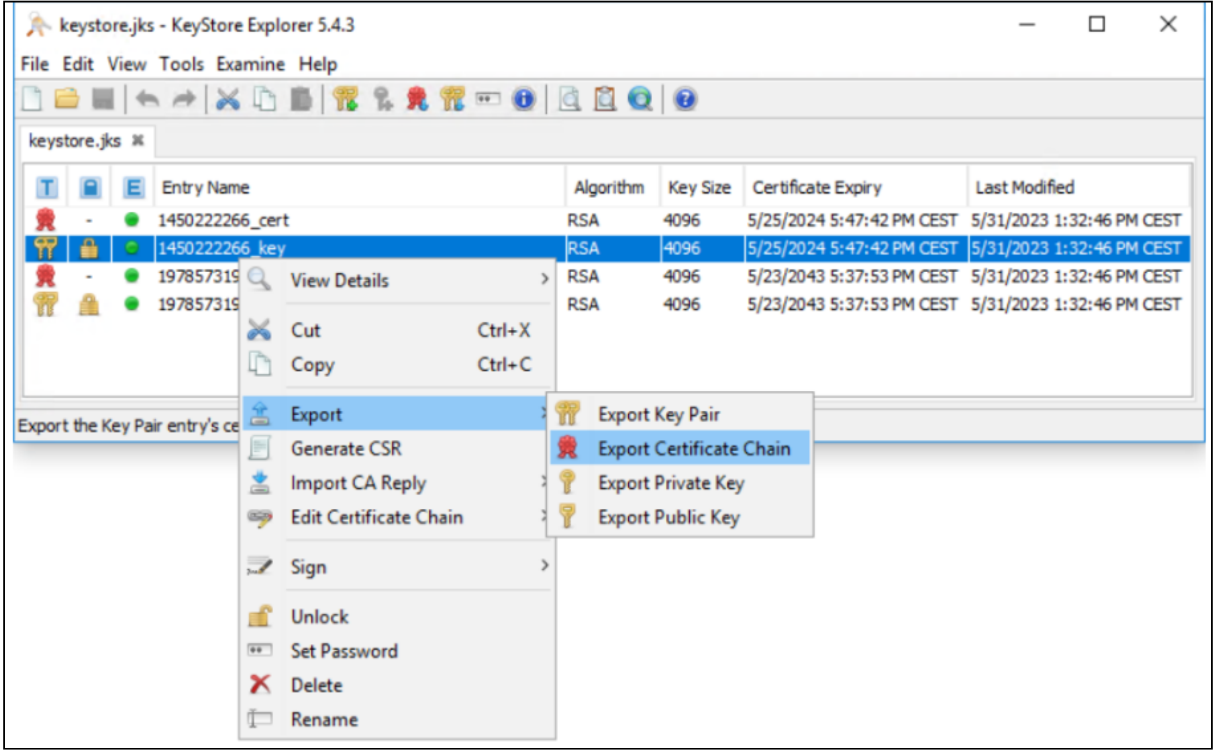
Public Key: RSA 4096 bits

Signature Algorithm: SHA512WITHRSA

Fingerprint: SHA-1 A1:79:D2:25:[redacted]F:44:2E

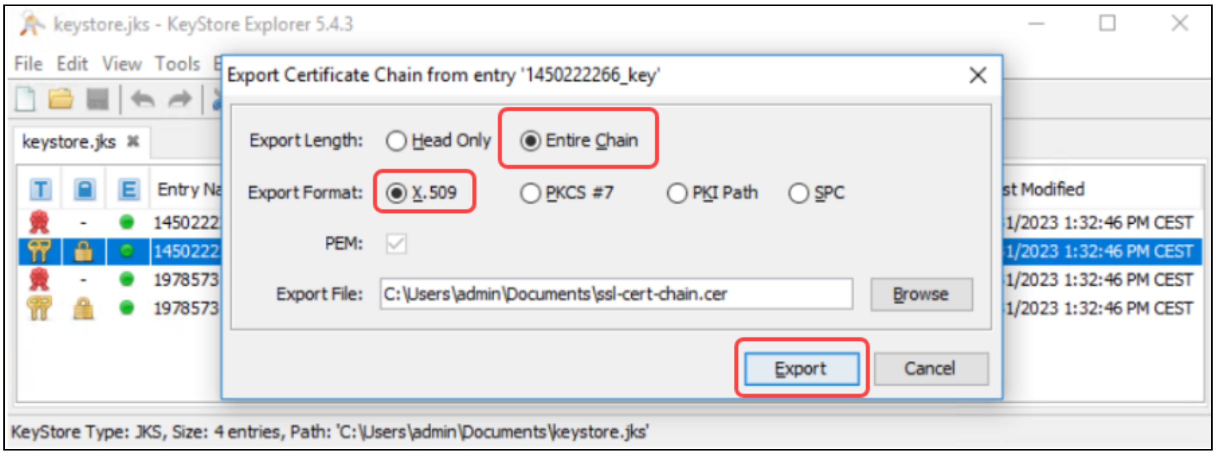
Exporting the Certificate Chain

1. Select the currently used key and export the certificate chain.



T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	197857319	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
		●	197857319	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

2. Select **Entire Chain** and **X.509** format.



Export Certificate Chain from entry '1450222266_key'

Export Length: ○ Head Only ● Entire Chain

Export Format: ● X.509 ○ PKCS #7 ○ PKI Path ○ SPC

PEM: ☑

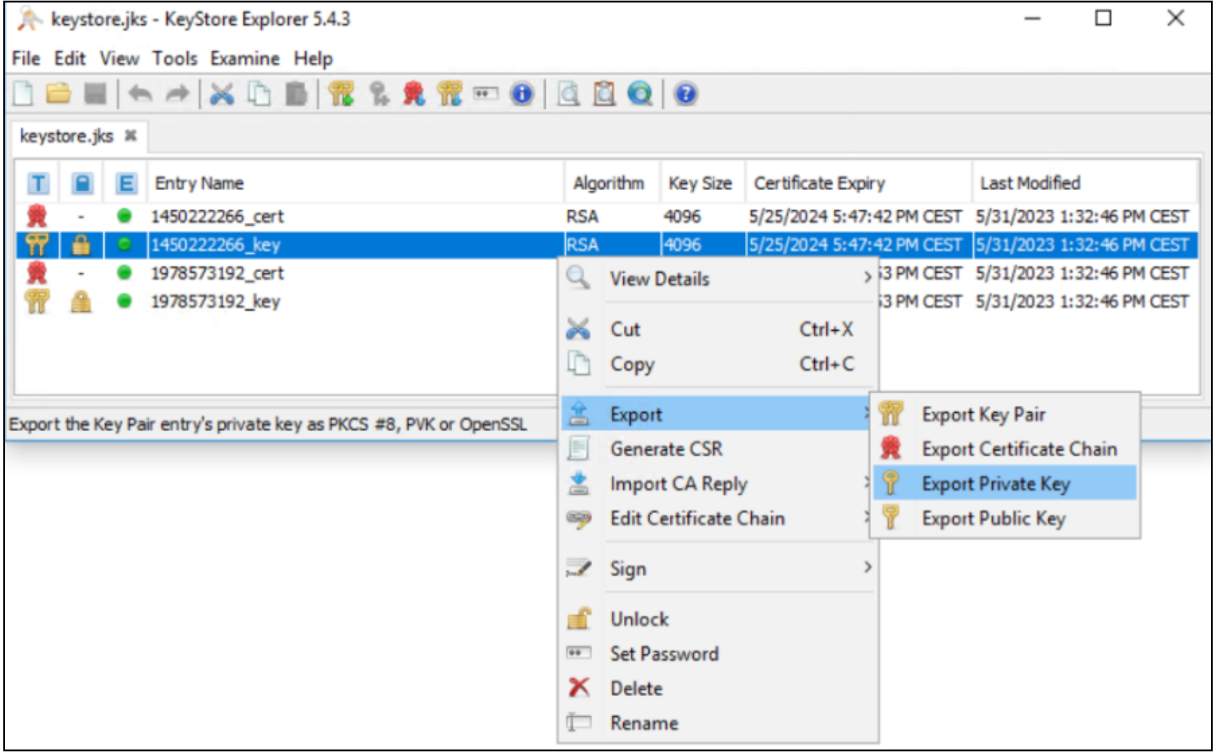
Export File: C:\Users\admin\Documents\ssl-cert-chain.cer

KeyStore Type: JKS, Size: 4 entries, Path: 'C:\Users\admin\Documents\keystore.jks'

3. Click **Export**.

Exporting the Private Key

1. Select the currently used key and export the private key.



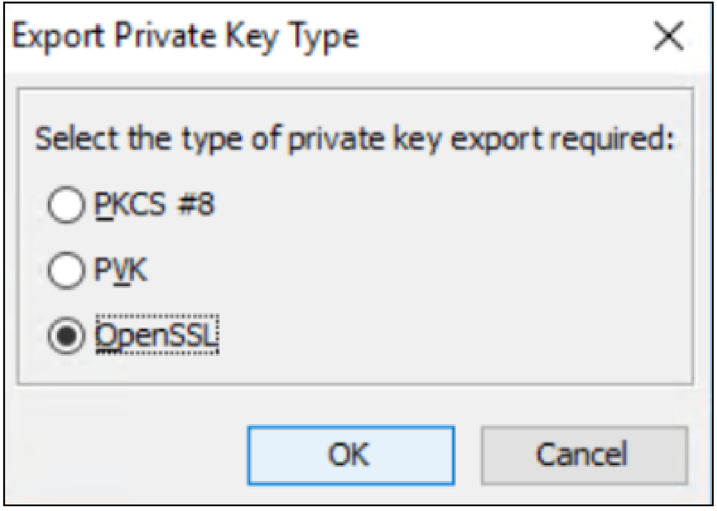
keystore.jks - KeyStore Explorer 5.4.3

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert			3 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1978573192_key			3 PM CEST	5/31/2023 1:32:46 PM CEST

Export the Key Pair entry's private key as PKCS #8, PVK or OpenSSL

2. Enter the password you used in the UMS for the export.

3. Select **OpenSSL**.



Export Private Key Type

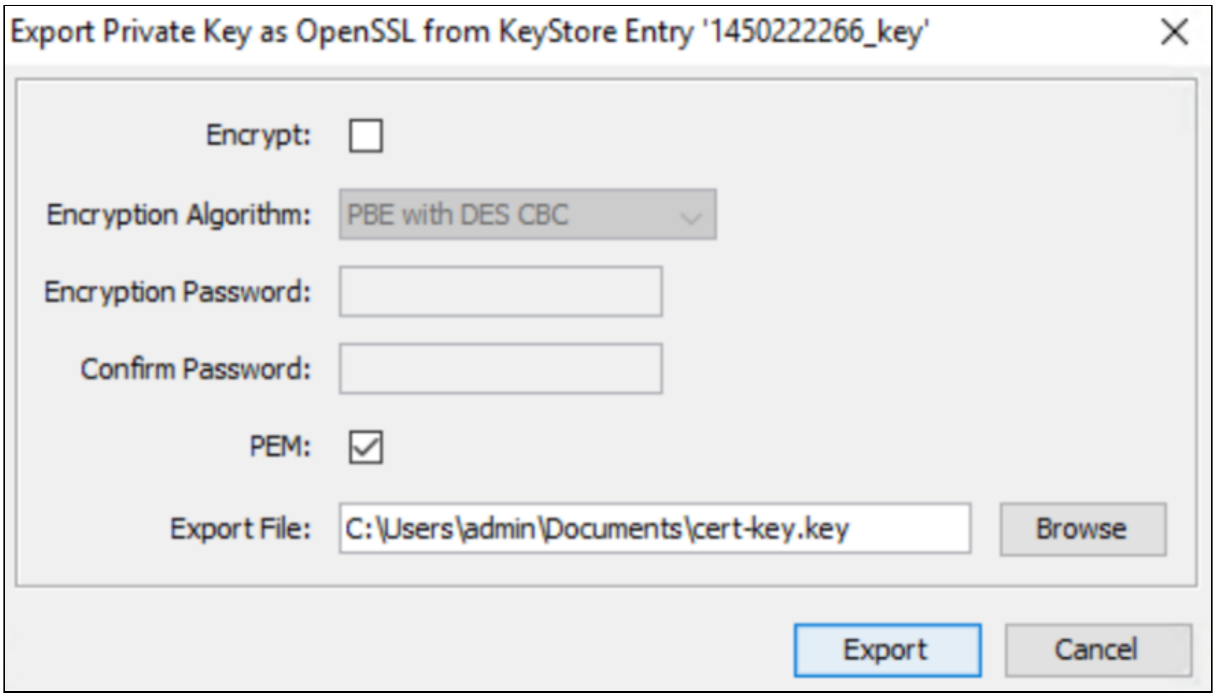
Select the type of private key export required:

○ PKCS #8

○ PVK

● OpenSSL

4. If required, select **Encrypt** and enter the corresponding data. In this example, we will use a not encrypted key file.



Export Private Key as OpenSSL from KeyStore Entry '1450222266_key'

Encrypt: ☐

Encryption Algorithm: PBE with DES CBC

Encryption Password:

Confirm Password:

PEM: ☑

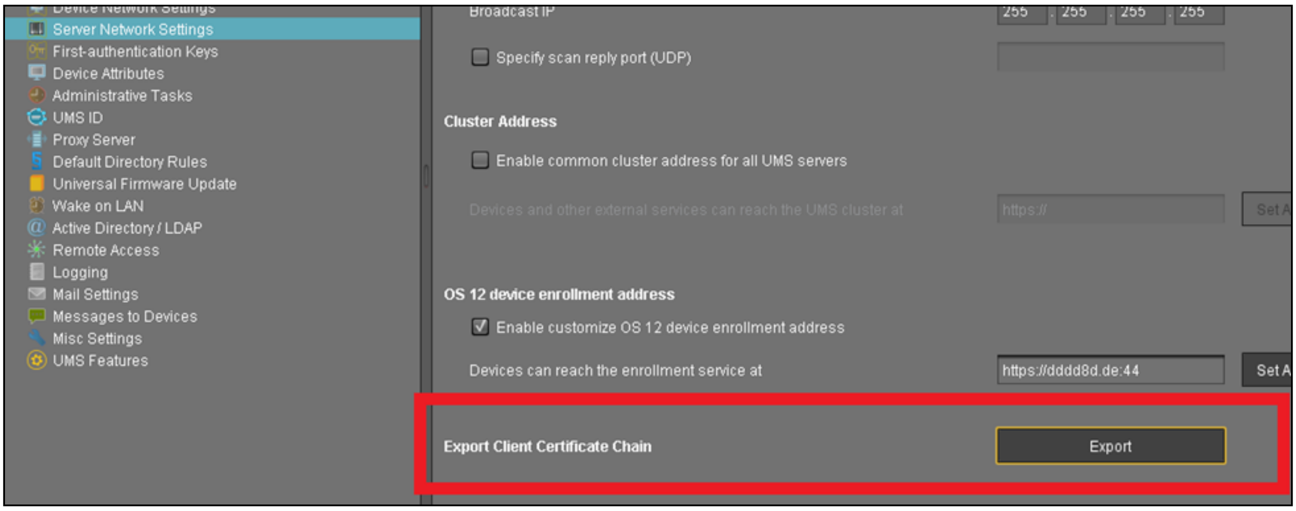
Export File: C:\Users\admin\Documents\cert-key.key

5. Click **Export**.

Export Client Certificate Chain

The EST CA Client Certificate is required for the Client Certificate check.

The Client Certificate Chain export can be found under: **UMS Administration > Global Configuration > Server Network Settings > Export Client Certificate Chain**.



Broadcast IP 255 . 255 . 255 . 255

☐ Specify scan reply port (UDP)

Cluster Address

☐ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https://

OS 12 device enrollment address

☑ Enable customize OS 12 device enrollment address

Devices can reach the enrollment service at https://dddd8d.de:44

Export Client Certificate Chain

Installing NGINX (Example Based on Ubuntu)

▶ Install NGINX on your system:

```
sudo apt update
sudo apt install nginx
```

▶ If a firewall is used, check the configuration:

1. Check the firewall configuration:

   ```
   sudo ufw app list
   ```

   The output of the command should look like this:

   ```
   Output
   Available applications:
       Nginx Full
       Nginx HTTP
       Nginx HTTPS
       OpenSSH
   ```

2. Enable 'Nginx Full':

   ```
   sudo ufw allow ‘Nginx Full’
   ```

3. Check the firewall configuration with

   ```
   sudo ufw status
   ```

4. For the UMS support, it might be necessary to open further ports. For more information on UMS ports, see IGEL UMS Communication Ports (see page 4).

5. Get the current state of NGINX:

   ```
   sudo systemctl status nginx
   ```

6. Check the current configuration of NGINX:

   ```
   sudo nginx -t
   ```

Configuring NGINX

The configuration of the server is done in configuration files. In an Ubuntu installation, the main configuration file is `/etc/nginx/nginx.conf`.

In this example, a separate configuration file `umsSSLOffloading.conf` is used. This file has to be included in the `nginx.conf` file:

```
http {

##
# Basic Settings
##
sendfile on;
        ...
##
# Virtual Host Configs
##

include /etc/nginx/conf.d/*.conf;
include /etc/nginx/sites-enabled/*;
include /etc/nginx/umsSSLOffloading.conf; # used for configuration
}
```

The extracted keys and certificates can be copied to a directory under `/etc/nginx`: for example, `/etc/nginx/ssl` – create the directory if it does not exist.

NGINX Configuration File for SSL Offloading

▶ Create a new config file `umsSSLOffloading.conf`.

This file must contain

- **upstream server** configuration
- **server** configuration
- **location** configuration

This is an example configuration to use with UMS 12 and IGEL OS 12:

- The **upstream umsserver** block defines the UMS Server in the backend.

```
upstream umsserver {
    server 192.168.27.96:8443 max_fails=3 fail_timeout=10s;
}
```

- The **server** block contains the configuration for the NGINX listener and the location.
  The UMS web certificate and the client certificate validation should be added here.
  Server common configuration:

```
server {
    listen       8443 ssl; # 'ssl' parameter tells NGINX to decrypt the traffic
    ssl_certificate             ssl/ssl-cert-chain.cer; # The Certificate File
(Web)
    ssl_certificate_key         ssl/cert-key.key; # The Private Key File (Web)
    ssl_verify_client           optional; ## Client Certificate check must be
optional
    ssl_client_certificate      ssl/estca.cer; #certificate for Client
Certificate Check

    access_log                  /var/log/nginx/ssl-access.log;
    error_log                   /var/log/nginx/ssl-error.log;
```

- At least two **location** definitions are required:
  - Location definition for all connections via WebSocket. The WebSocket connection requires the forwarding of the client certificate within the header. A second header information to add is the upgrade header which is required for WebSockets.

```
# Configuration for connections via WebSocket, the upgrade header
information must be written by NGINX
  location ~ /device-connector/device/(ws-connect|portforwarding) {
        proxy_pass https://umsserver;
        proxy_set_header X-SSL-CERT $ssl_client_escaped_cert; # client
certificate in current connection
        proxy_set_header Upgrade $http_upgrade; # Set upgrade header
        proxy_set_header Connection $connection_upgrade;
        proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer; #trusted
Cert Chain for UMS connection

        # TLSv1.3 configuration is recommended but not necessary
        proxy_ssl_protocols TLSv1.3;
 }
```

  - Location definition for all other connections.

```
# Configuration for all other connections
  location / {
        proxy_pass https://umsserver;
        proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
        proxy_ssl_protocols TLSv1.3;
 }
```

The whole configuration file:

```
#map upgrade header
map %https_upgrade $connection_upgrade {
default upgrade;
'' close;
}

    upstream umsserver {
        server 192.168.27.96:8443 max_fails=3 fail_timeout=10s;
    }

server {
    listen      8443 ssl; # 'ssl' parameter tells NGINX to decrypt the traffic
    ssl_certificate             ssl/ssl-cert-chain.cer; # The Certificate File (Web)
    ssl_certificate_key         ssl/cert-key.key; # The Private Key File (Web)
    ssl_verify_client           optional; ## Client Certificate check must be
optional
    ssl_client_certificate      ssl/estca.cer; #certificate for Client Certificate
Check

    access_log                  /var/log/nginx/ssl-access.log;
    error_log                   /var/log/nginx/ssl-error.log;

# Configuration for connections via WebSocket, the upgrade header information must be
written by NGINX
  location ~ /device-connector/device/(ws-connect|portforwarding) {
    proxy_pass https://umsserver;
    proxy_set_header X-SSL-CERT $ssl_client_escaped_cert;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection $connection_upgrade;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    # TLSv1.3 configuration is recommended but not necessary
    proxy_ssl_protocols TLSv1.3;
 }

# Configuration for all other connections
  location / {
    proxy_pass https://umsserver;
    proxy_ssl_trusted_certificate ssl/ssl-cert-chain.cer;
    proxy_set_header Upgrade $http_upgrade;
    proxy_set_header Connection $connection_upgrade;
    proxy_ssl_protocols TLSv1.3;
  # proxy_ssl_session_reuse on;
  }
}
```

Configuring the UMS

Activate Forwarding Client Certificate Processing at the UMS

The processing of forwarded client certificates must be activated on the UMS side:

1. Open the configuration file `[UMS i nstallation directory]/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml`.
   You will see:

   ```
   igel:
       client-cert-forwarding:
           enabled: false
           client-cert-forwarded-header: X-SSL-CERT
   ```

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

   ```
   client-cert-forwarding:
       enabled: true
   ```

3. If required, the forwarding header can be configured. The `X -SSL-CERT` header value can be changed but be aware to change the corresponding value in the NGINX configuration, see above Location definition for all connections via WebSocket (see page 32).

4. Save the configuration changes and restart the UMS Server service. For details on how you can restart the service, see IGEL UMS HA Services and Processes.

Configuring the IGEL Cloud Gateway (ICG) If Used

If you use an external load balancer / reverse proxy and the IGEL Cloud Gateway, it is necessary to configure the load balancer / reverse proxy in front of the ICG.

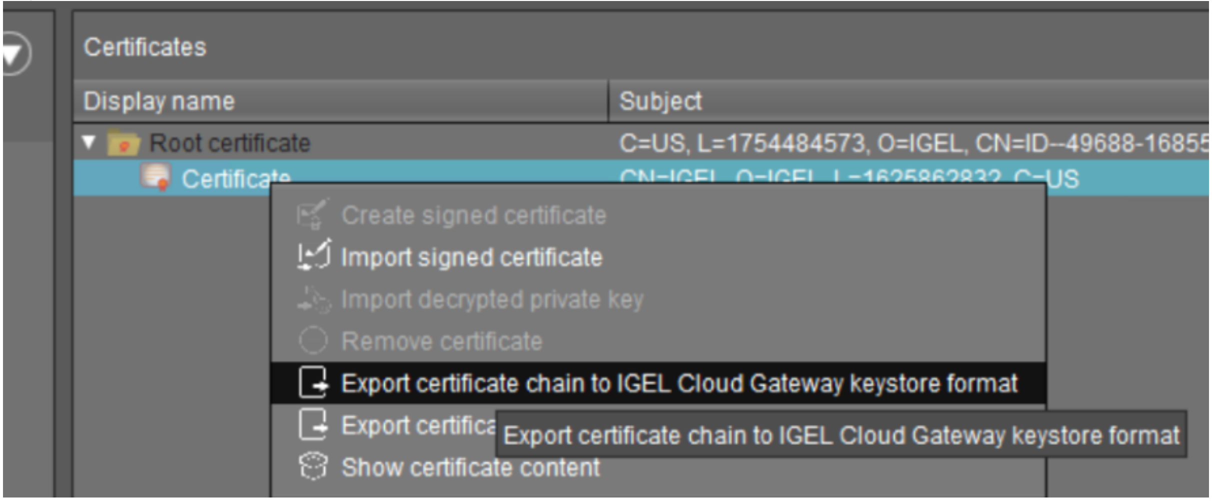
The differences in the configuration are:

- ICG certificate export (instead of the export of the UMS web certificate)
- Activate forwarding client certificate processing at the ICG (not the UMS)

> ⚠ Note that the IP or hostname of your load balancer / reverse proxy must be added when generating the ICG certificate. Use a semicolon to separate the values. For more information on ICG installation and certificates, see Installation und Einrichtung.

ICG Certificate Export

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Cloud Gateway** and export the ICG certificate chain to IGEL Cloud Gateway keystore format:



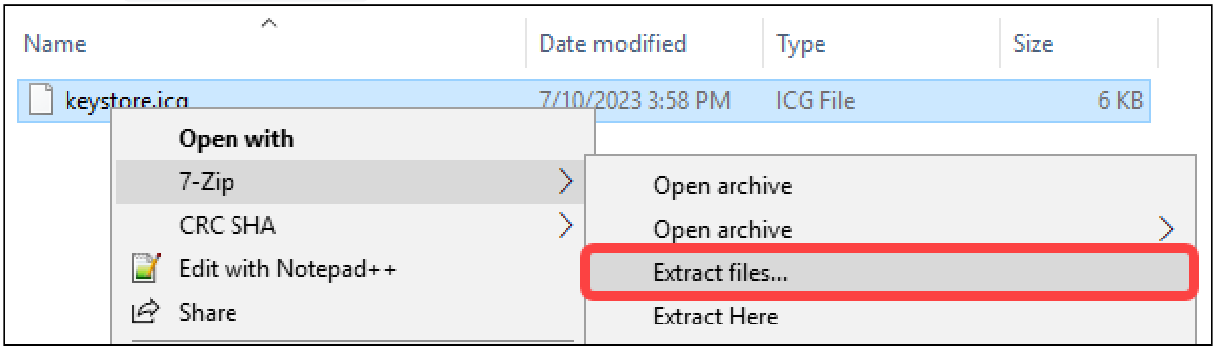
Certificates

Display name	Subject
Root certificate	C=US, L=1754484573, O=IGEL, CN=ID--49688-16855
Certificate	CN=IGEL, O=IGEL, L=1625862832, C=US

Create signed certificate
Import signed certificate
Import decrypted private key
Remove certificate
Export certificate chain to IGEL Cloud Gateway keystore format
Export certifica
Show certificate content
Export certificate chain to IGEL Cloud Gateway keystore format

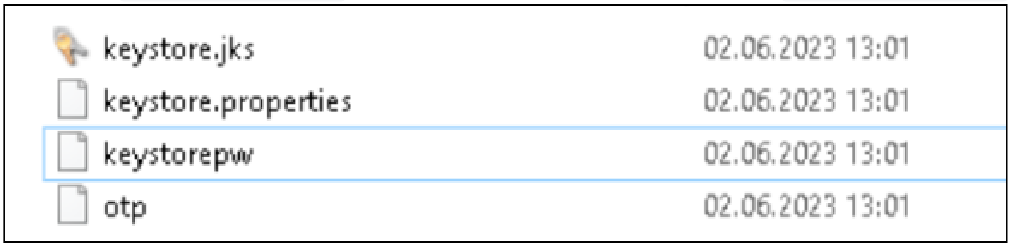
The `keystore.icg` file will be saved.

2. Unzip the `keystore.icg` file.



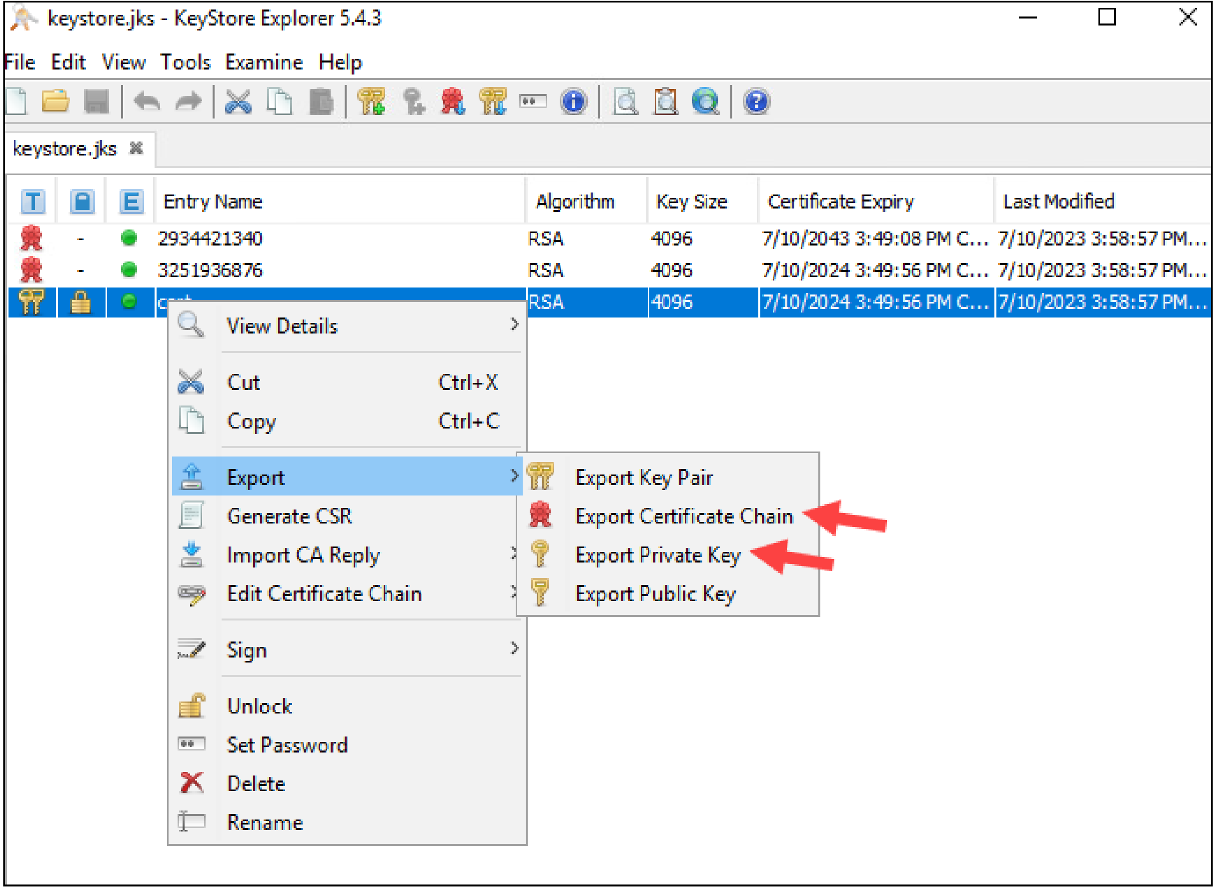
Name	Date modified	Type	Size
keystore.icg	7/10/2023 3:58 PM	ICG File	6 KB

3. Open the `keystore.jks` file and use the password from the `keystorepwd` file.



keystore.jks	02.06.2023 13:01
keystore.properties	02.06.2023 13:01
keystorepw	02.06.2023 13:01
otp	02.06.2023 13:01

4. Select the configured key entry and export the certificate chain (**Entire Chain**, **X.509** format) and the private key (**OpenSSL**).



T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	2934421340	RSA	4096	7/10/2043 3:49:08 PM C...	7/10/2023 3:58:57 PM...
	-	●	3251936876	RSA	4096	7/10/2024 3:49:56 PM C...	7/10/2023 3:58:57 PM...
		●	cert	RSA	4096	7/10/2024 3:49:56 PM C...	7/10/2023 3:58:57 PM...

5. Proceed further as described above starting with Exporting the Client Certificate Chain (https_trust.keystore) (see page 29).

Activate Forwarding Client Certificate Processing at the ICG

The processing of forwarded client certificates must be activated on the ICG side, not the UMS side:

1. Open the configuration file `[UMS i nstallation directory]/IGEL/icg/usg/conf/application-prod.yml`.
   You will see:

```
igel:
    client-cert-forwarding:
        enabled: false
        client-cert-forwarded-header: X-SSL-CERT
```

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

```
client-cert-forwarding:
    enabled: true
```

3. If required, the forwarding header can be configured. The `X` `-SSL-CERT` header value can be changed but be aware to change the corresponding value in the NGINX configuration, see above Location definition for all connections via WebSocket (see page 32).

4. Save the configuration changes and restart the ICG server.

F5 BIG IP: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

In this article. you can find an example configuration of F5 BIG IP for SSL Offloading in the IGEL Universal Management Suite (UMS).

> ⚠ General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
> As the reverse proxy is an external software we cannot provide full support for each version.

> ⓘ A reverse proxy / external load balancer can be used if you manage IGEL OS 12 devices only. See IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.

Requirements

- IGEL UMS version 12.04.100 or higher
- IGEL OS version 12.3.2 or higher
- If the ICG is used: ICG version 12.04.100 or higher
- In the case of the Distributed UMS or High Availability installations, the time on all servers must be synchronized.

> ⓘ For extracting keys and certificate chains, you will require a suitable tool like "Keystore Explorer". Please use the latest version of such tools.
> Please also make sure that you use Java 17.

Process Overview

We advise you to follow the process presented here. You will find the steps to take in detail in the sections below.

1. Configure your UMS. (Configure ICG, if used.)
   a. Activate Forwarding Client Certificate Processing
   b. Set Cluster Address
2. Create and Export Certificates
   a. Create UMS Web Certificates. (If ICG is used, create Cloud Gateway certificate.)
   b. Export UMS Web Certificate Chain and extract private key and certificate chain. (If ICG is used, export Cloud Gateway certificate chain.)
   c. Export Client Certificate Chain
3. Configure F5:
   a. UMS Certificates (Web UMS and EST CA)
   b. UMS Backend Node and Pool configuration
   c. iRule for Client Certificate Forwarding
   d. SSL Client Profile

e. SSL Server Profile
f. Virtual Server

UMS / ICG Configuration

Activate Forwarding Client Certificate Processing on UMS / ICG

If no ICG is used, the processing of forwarded Client Certificates must be activated on UMS side. In case only an ICG is used behind the Reverse Proxy, activate the processing of forwarded Client Certificates on ICG side.

To activate forwarding Client Certificate processing on UMS side:

1. Open the configuration file `[UMS i nstallation directory]/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml`.
   You will see:
   ```
   igel:
       client-cert-forwarding:
           enabled: false
           client-cert-forwarded-header: X-SSL-CERT
   ```
2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":
   ```
   client-cert-forwarding:
       enabled: true
   ```
3. If required, the forwarding header can be configured. The `X -SSL-CERT` header value can be changed but be aware to change the corresponding value in the F5 BIG IP configuration.
4. Save the configuration changes and restart the UMS Server service. For details on how you can restart the service, see IGEL UMS HA Services and Processes.

To activate the processing of forwarded Client Certificates on ICG side:

1. Open the configuration file `[UMS i nstallation directory]/IGEL/icg/usg/conf/application-prod.yml`.
   You will see:
   ```
   igel:
       client-cert-forwarding:
           enabled: false
           client-cert-forwarded-header: X-SSL-CERT
   ```
2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

```
client-cert-forwarding:
    enabled: true
```

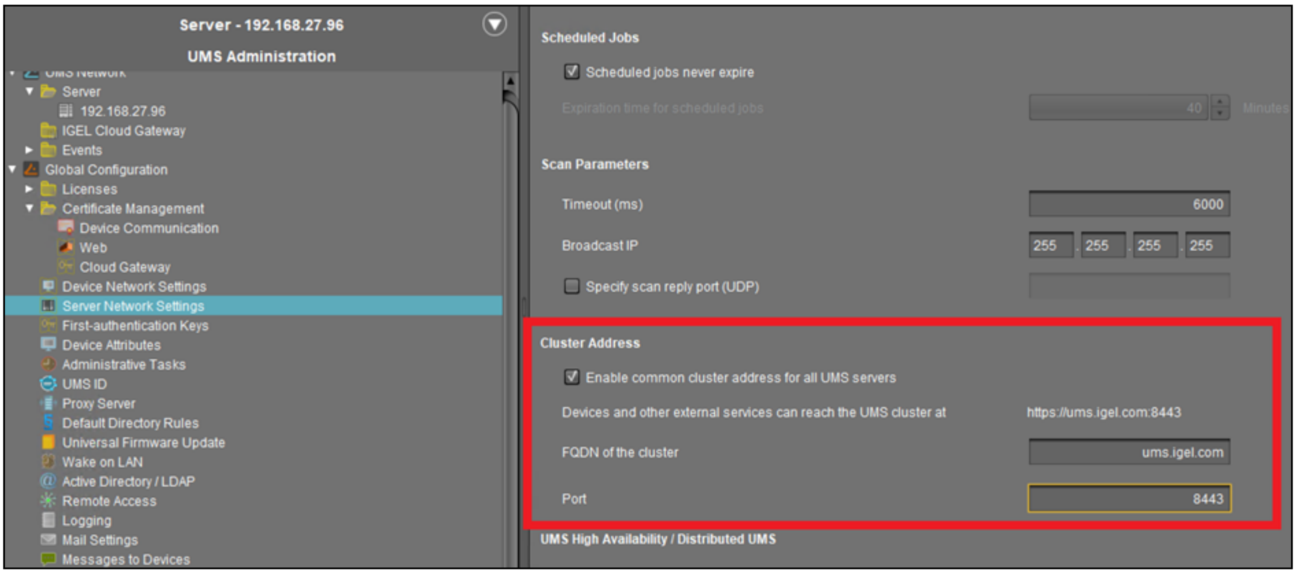
3. If required, the forwarding header can be configured. The `X -SSL-CERT` header value can be changed but be aware to change the corresponding value in the F5 BIG IP configuration.

4. Save the configuration changes and restart the ICG server.

Set Cluster Address

1. Go to **UMS Administration > Global Configuration > Server Network Settings**.

2. Set the **Cluster Address**.
   If you are using a Reverse Proxy, you will need to update the FQDN of the UMS cluster as external address.



Scheduled Jobs

☑ Scheduled jobs never expire

Expiration time for scheduled jobs 40 Minutes

Scan Parameters

Timeout (ms) 6000

Broadcast IP 255 . 255 . 255 . 255

☐ Specify scan reply port (UDP)

Cluster Address

☑ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https://ums.igel.com:8443

FQDN of the cluster ums.igel.com

Port 8443

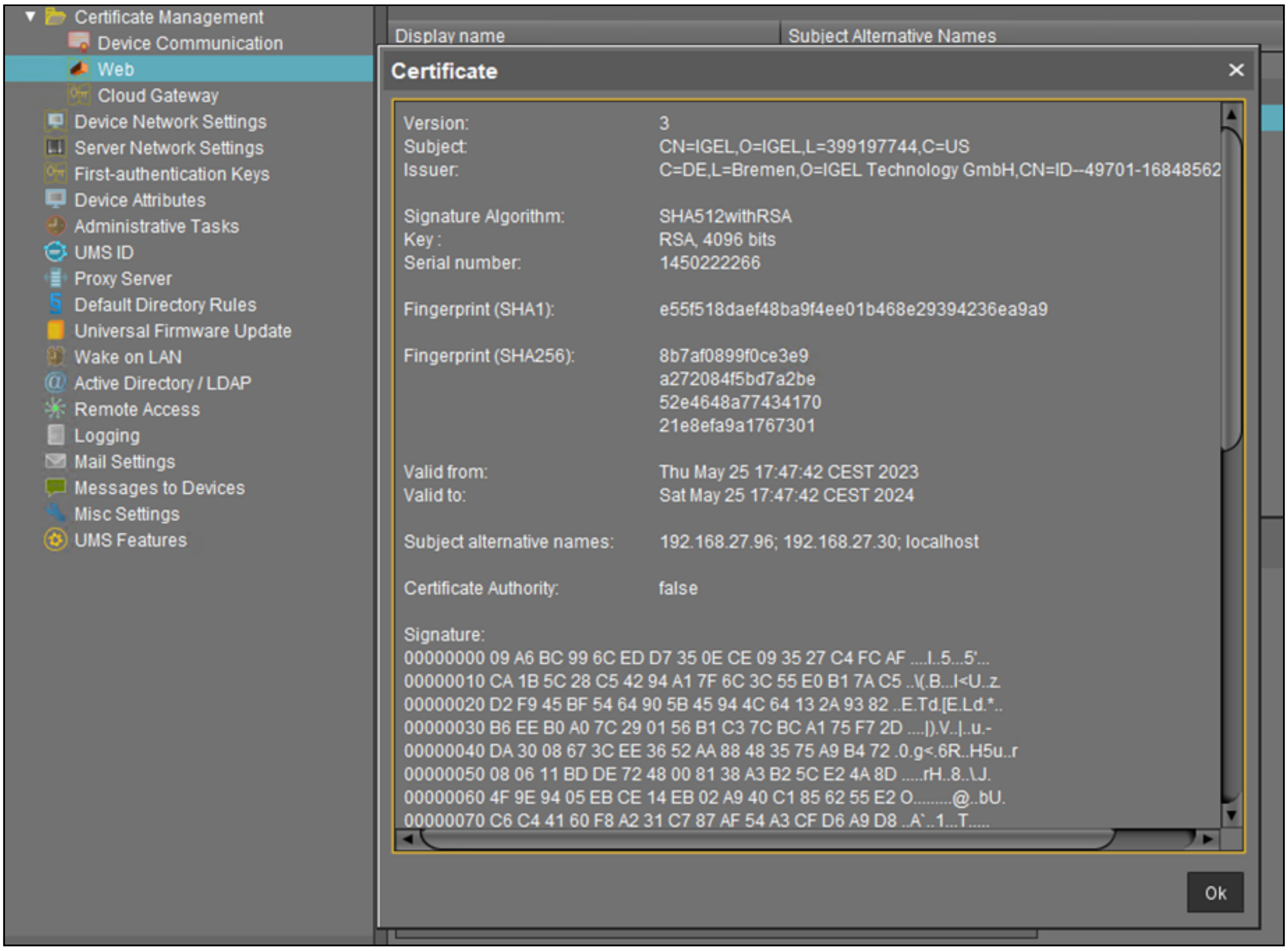
UMS High Availability / Distributed UMS

Create and Export Certificates

Create UMS Web Certificate / Cloud Gateway Certificate

You need to create and use a valid certificate for UMS and Loadbalancer.

Use Subject alternative names if the IP addresses used for UMS and Loadbalancer are different.

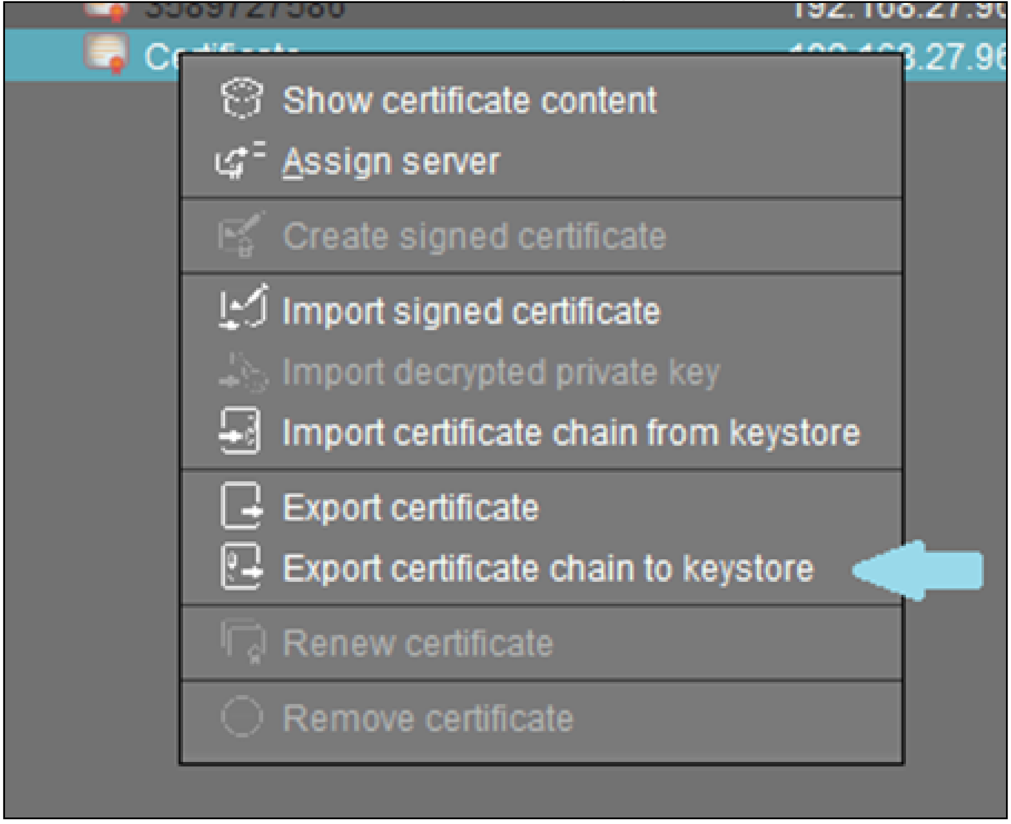


```
Version:                      3
Subject:                      CN=IGEL,O=IGEL,L=399197744,C=US
Issuer:                       C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848562

Signature Algorithm:          SHA512withRSA
Key :                         RSA, 4096 bits
Serial number:                1450222266

Fingerprint (SHA1):           e55f518daef48ba9f4ee01b468e29394236ea9a9

Fingerprint (SHA256):         8b7af0899f0ce3e9
                              a272084f5bd7a2be
                              52e4648a77434170
                              21e8efa9a1767301

Valid from:                   Thu May 25 17:47:42 CEST 2023
Valid to:                     Sat May 25 17:47:42 CEST 2024

Subject alternative names:    192.168.27.96; 192.168.27.30; localhost

Certificate Authority:        false

Signature:
00000000 09 A6 BC 99 6C ED D7 35 0E CE 09 35 27 C4 FC AF ....I..5...5'...
00000010 CA 1B 5C 28 C5 42 94 A1 7F 6C 3C 55 E0 B1 7A C5 ..\(.B...l<U..z.
00000020 D2 F9 45 BF 54 64 90 5B 45 94 4C 64 13 2A 93 82 ..E.Td.[E.Ld.*..
00000030 B6 EE B0 A0 7C 29 01 56 B1 C3 7C BC A1 75 F7 2D ....|).V..|..u.-
00000040 DA 30 08 67 3C EE 36 52 AA 88 48 35 75 A9 B4 72 .0.g<.6R..H5u..r
00000050 08 06 11 BD DE 72 48 00 81 38 A3 B2 5C E2 4A 8D .....rH..8..\.J.
00000060 4F 9E 94 05 EB CE 14 EB 02 A9 40 C1 85 62 55 E2 O.........@..bU.
00000070 C6 C4 41 60 F8 A2 31 C7 87 AF 54 A3 CF D6 A9 D8 ..A`..1...T.....
```

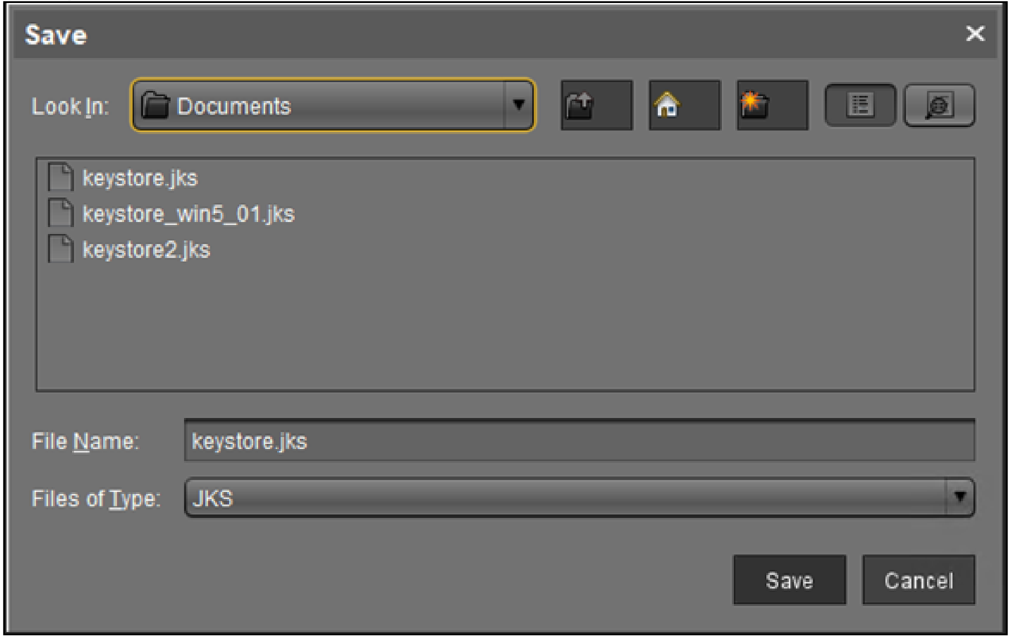
When you use the Reverse Proxy with ICG, use the **Cloud Gateway** certificate and add the IP or Hostname of the Loadbalancer at the ICG Certificate generation. Use a semicolon to separate the values.

Export UMS Web Certificate Chain and Extract Key and Certificate Chain

1. Select the current used UMS Web certificate and export the certificate chain.


Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from keystore
Export certificate
Export certificate chain to keystore
Renew certificate
Remove certificate

2. Set a password and the filename.



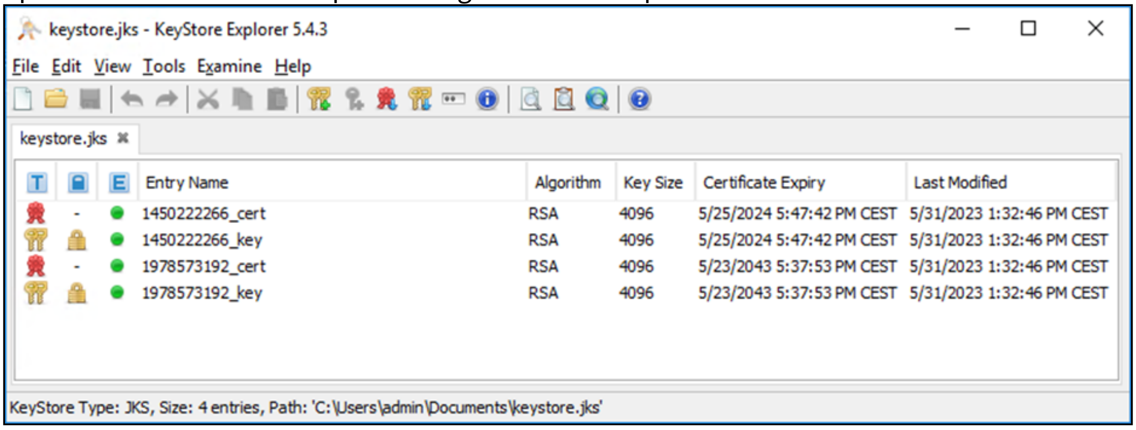
Look In: Documents

keystore.jks
keystore_win5_01.jks
keystore2.jks

File Name: keystore.jks

Files of Type: JKS

3. Identify the Web key.
   The exported keystore file contains several keys and certificates, at least the root and the currently used keys and certificates. A tool like Keystore Explorer can be used to identify the currently used Web key.
   More information with Keystore Explorer example...
   a. Open the file and enter the password given for the export. Several entries are shown:

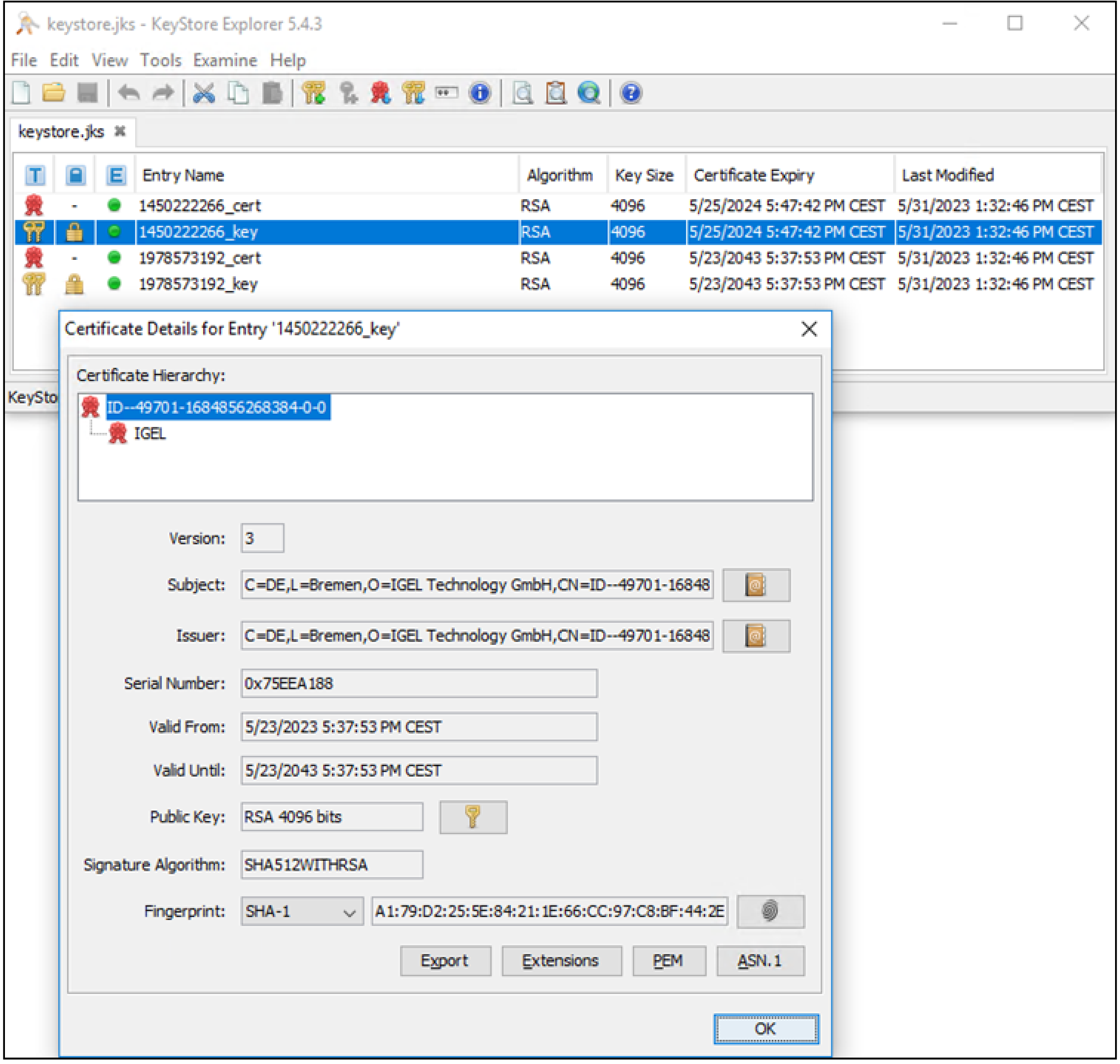


keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

KeyStore Type: JKS, Size: 4 entries, Path: 'C:\Users\admin\Documents\keystore.jks'

b. Find the currently used Web key:



keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks
KeySto

T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

Certificate Details for Entry '1450222266_key'

Certificate Hierarchy:

- ID--49701-1684856268384-0-0
  - IGEL

Version: 3

Subject: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Serial Number: 0x75EEA188

Valid From: 5/23/2023 5:37:53 PM CEST

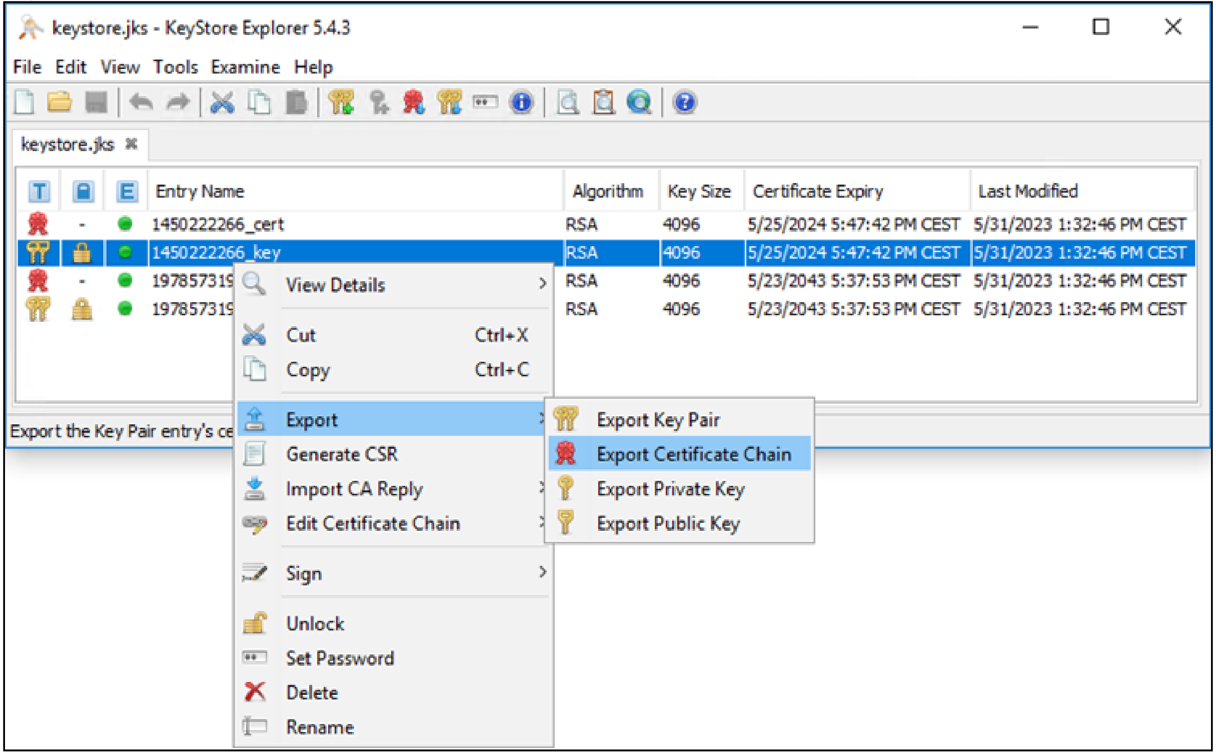
Valid Until: 5/23/2043 5:37:53 PM CEST

Public Key: RSA 4096 bits

Signature Algorithm: SHA512WITHRSA

Fingerprint: SHA-1 A1:79:D2:25:5E:84:21:1E:66:CC:97:C8:BF:44:2E

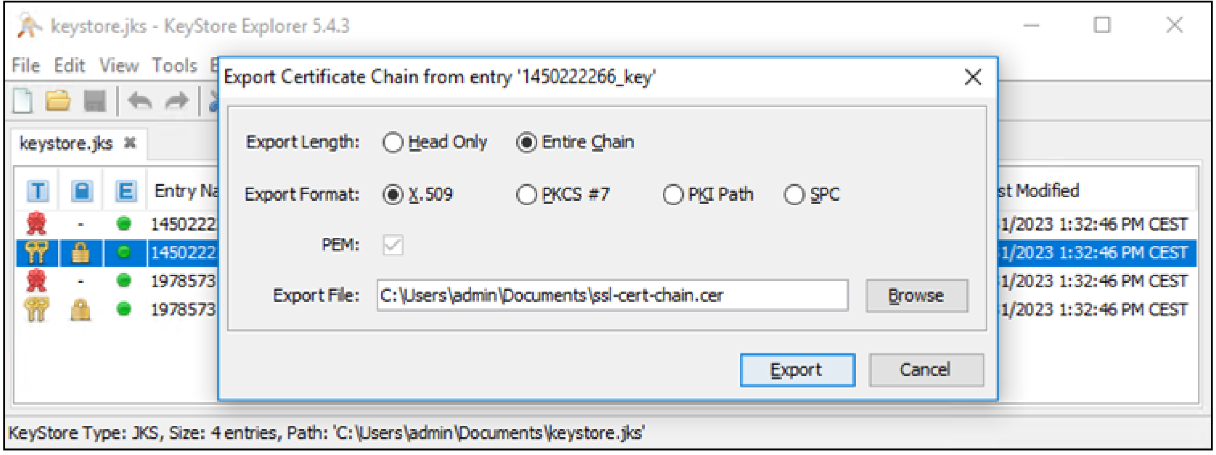
4. Export the Certificate Chain.



T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-		1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
			1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-		19785731[illegible]	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
			19785731[illegible]	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

Export the Key Pair entry's ce

5. Select **Entire Chain** and export the certificate.



Export Certificate Chain from entry '1450222266_key'

Export Length: ○ Head Only ● Entire Chain

Export Format: ● X.509 ○ PKCS #7 ○ PKI Path ○ SPC

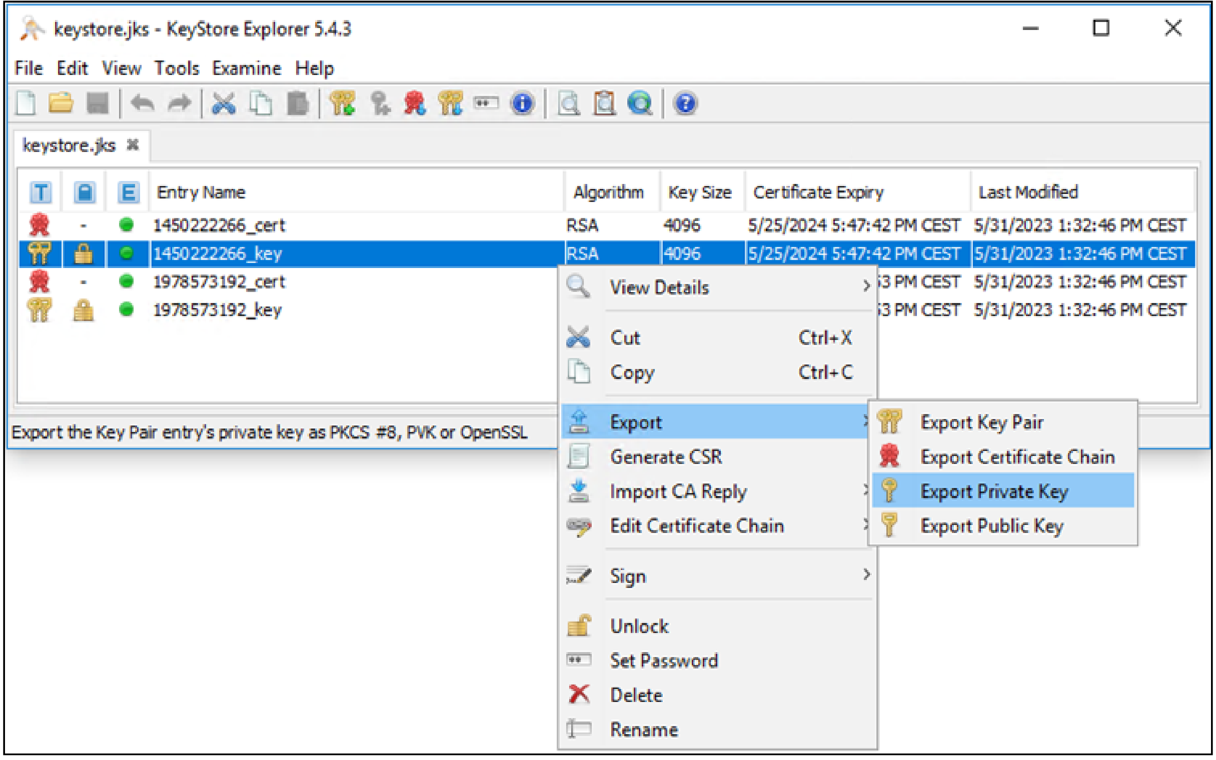
PEM: ☑

Export File: C:\Users\admin\Documents\ssl-cert-chain.cer

KeyStore Type: JKS, Size: 4 entries, Path: 'C:\Users\admin\Documents\keystore.jks'

6. Select **Head only** and export the certificate to a file for example: ssl-cert.cer.

7. Export the Private Key.

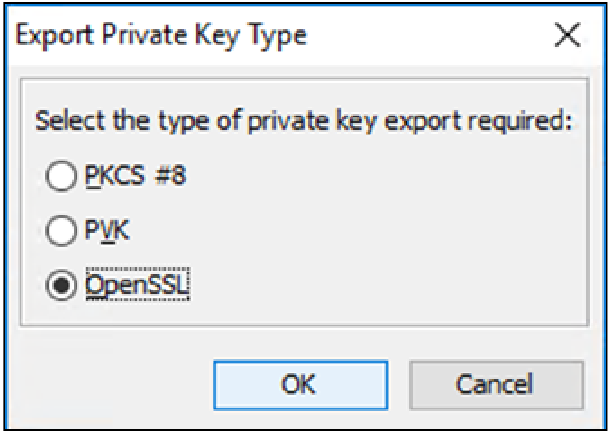


T		E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert			3 PM CEST	5/31/2023 1:32:46 PM CEST
		●	1978573192_key			3 PM CEST	5/31/2023 1:32:46 PM CEST

Export the Key Pair entry's private key as PKCS #8, PVK or OpenSSL

8. Enter the Password set at export in UMS.

9. Select **OpenSSL**.



Export Private Key Type

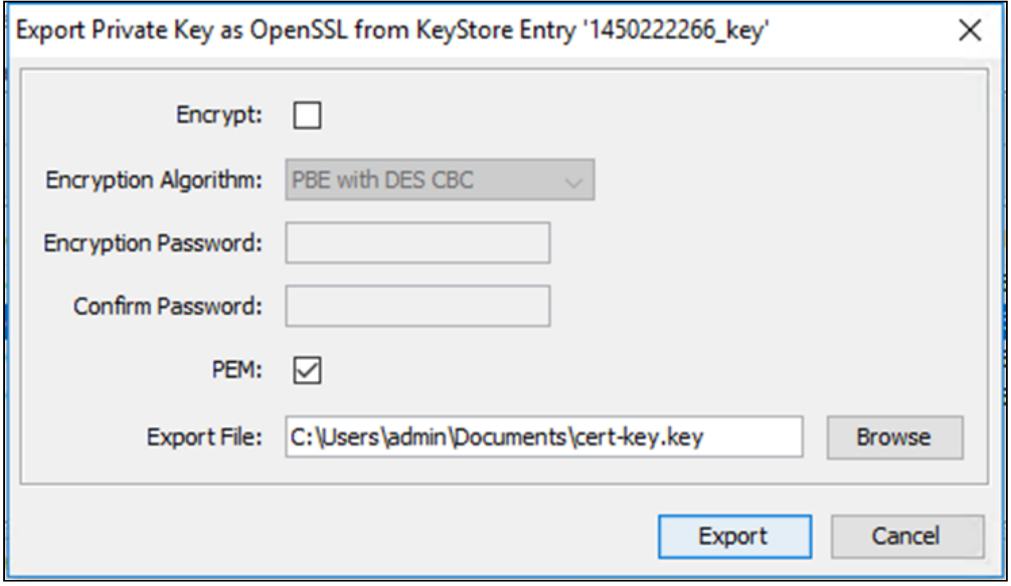
Select the type of private key export required:

○ PKCS #8

○ PVK

● OpenSSL

In this example a not encrypted key file is used.



Export Private Key as OpenSSL from KeyStore Entry '1450222266_key'

Encrypt: □

Encryption Algorithm: PBE with DES CBC

Encryption Password:

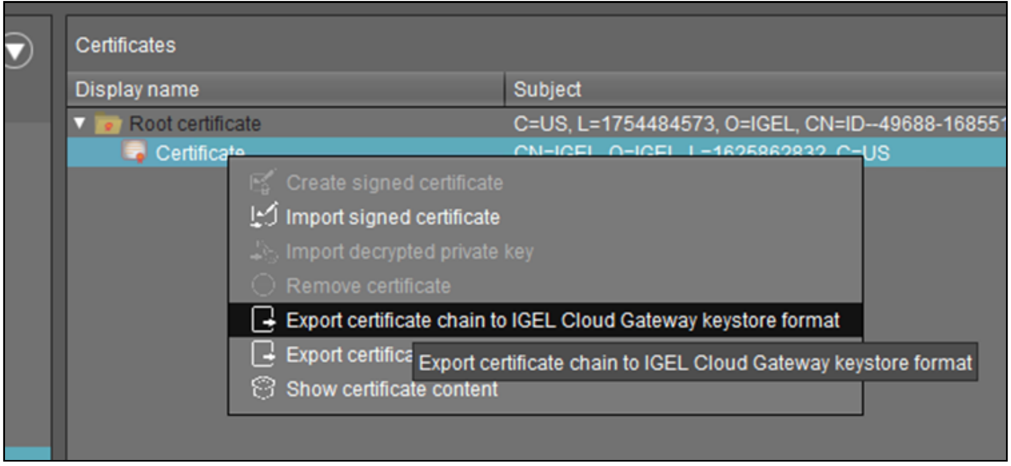
Confirm Password:

PEM: ☑

Export File: C:\Users\admin\Documents\cert-key.key

Export Cloud Gateway Certificate Chain and Extract Key and Certificate Chain

1. If the certificate was added as a Cloud Gateway certificate, export the certificate to IGEL Cloud Gateway keystore format.



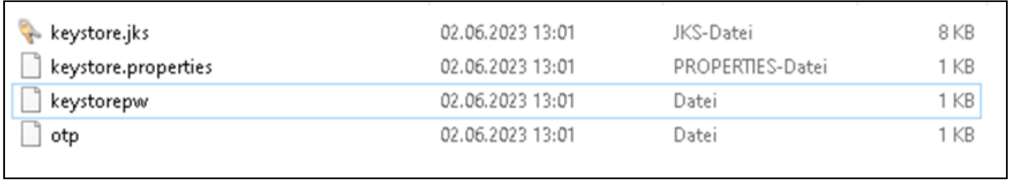
Certificates

Display name	Subject
Root certificate	C=US, L=1754484573, O=IGEL, CN=ID--49688-16855
Certificate	CN=IGEL, O=IGEL, L=1625862832, C=US

Create signed certificate
Import signed certificate
Import decrypted private key
Remove certificate
Export certificate chain to IGEL Cloud Gateway keystore format
Export certifica
Show certificate content
Export certificate chain to IGEL Cloud Gateway keystore format

2. Unzip the file.

3. Open the keystore.jks file and use the password from the keystorepwd file.



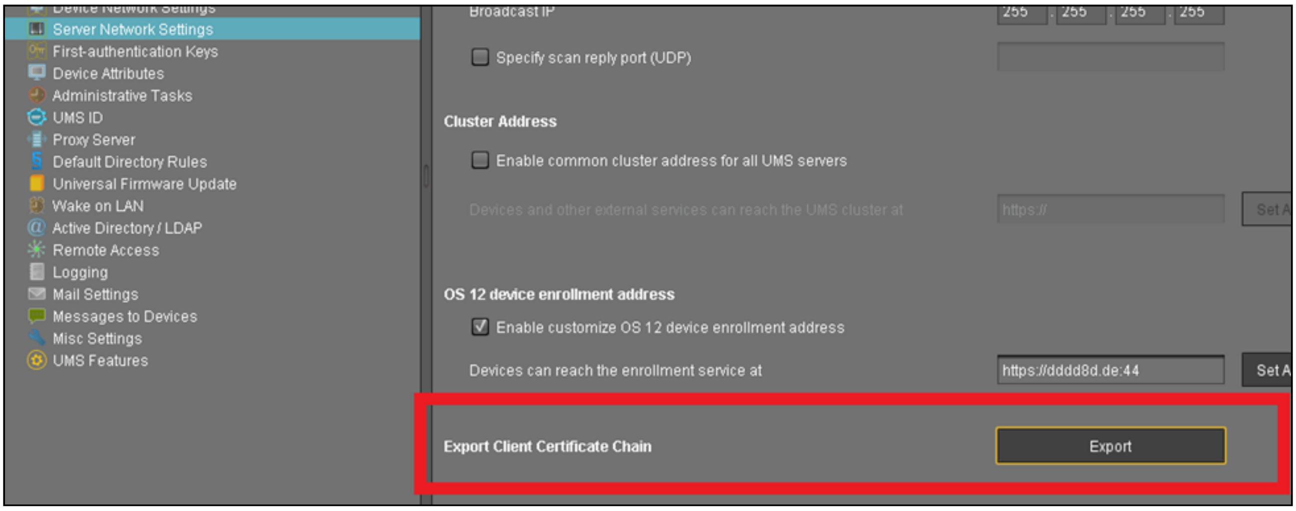
keystore.jks	02.06.2023 13:01	JKS-Datei	8 KB
keystore.properties	02.06.2023 13:01	PROPERTIES-Datei	1 KB
keystorepw	02.06.2023 13:01	Datei	1 KB
otp	02.06.2023 13:01	Datei	1 KB

4. Select the configured key entry and export the private key and certificate chain.
5. Perform the steps in the section above to extract the files.

Export Client Certificate Chain

The EST CA Client Certificate is required for the Client Certificate check.

The Client Certificate Chain export can be found under: **UMS Administration > Global Configuration > Server Network Settings > Export Client Certificate Chain**.



Broadcast IP 255 . 255 . 255 . 255

□ Specify scan reply port (UDP)

Cluster Address

□ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https://

OS 12 device enrollment address

☑ Enable customize OS 12 device enrollment address

Devices can reach the enrollment service at https://dddd8d.de:44

Export Client Certificate Chain Export

Configure F5

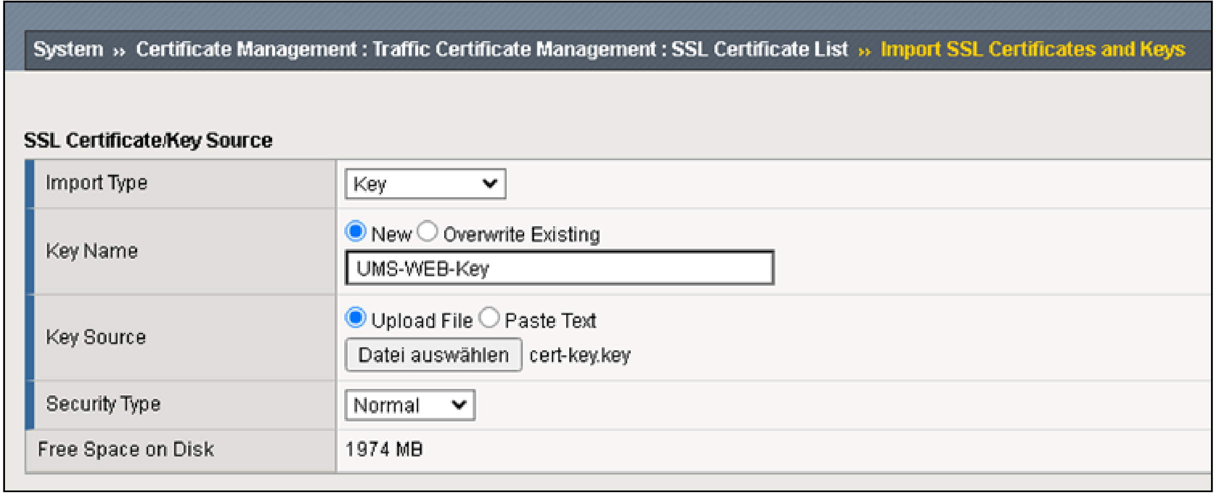
Certificate Management

The UMS Web Certificates und UMS EST CA Certificates must be added in the F5 BIG-IP application.

BIG-IP offers a common Certificate Management.

Configure the UMS Web Certificates / Key:

1. Add UMS Web Private Key.

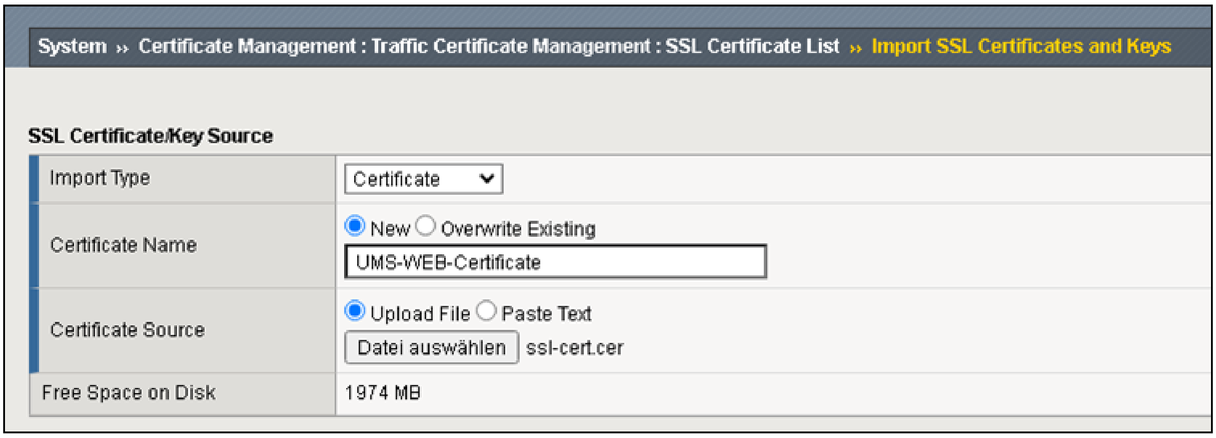


System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Key
Key Name	● New ○ Overwrite Existing UMS-WEB-Key
Key Source	● Upload File ○ Paste Text Datei auswählen cert-key.key
Security Type	Normal
Free Space on Disk	1974 MB

2. Add UMS Web Certificate.

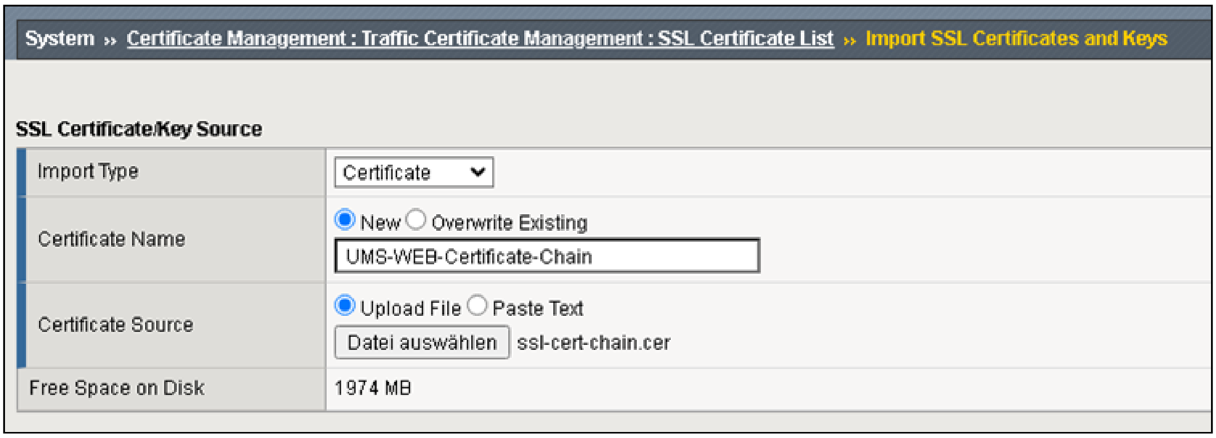


System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	● New ○ Overwrite Existing UMS-WEB-Certificate
Certificate Source	● Upload File ○ Paste Text Datei auswählen ssl-cert.cer
Free Space on Disk	1974 MB

3. Add UMS Web Certificate Chain.

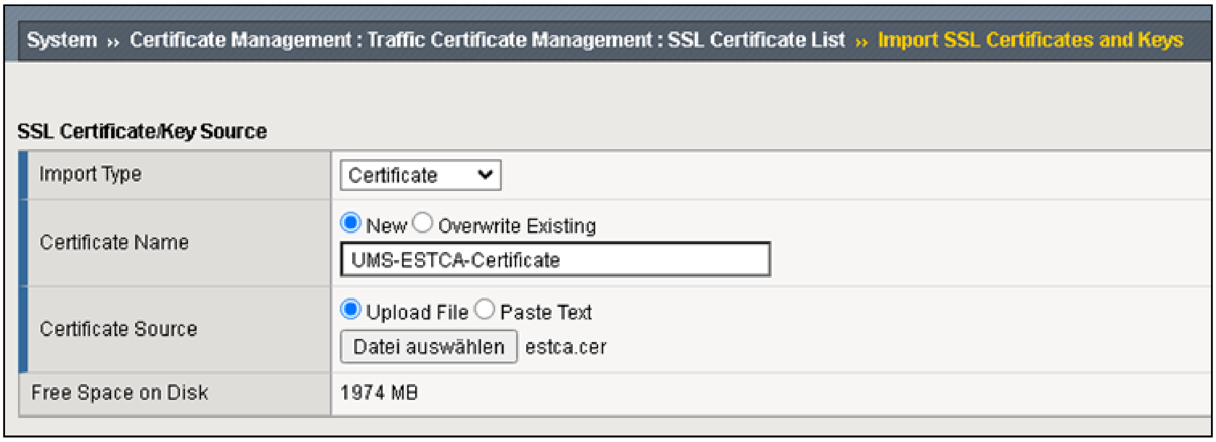


System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	● New ○ Overwrite Existing UMS-WEB-Certificate-Chain
Certificate Source	● Upload File ○ Paste Text Datei auswählen ssl-cert-chain.cer
Free Space on Disk	1974 MB

4. Add UMS EST CA Certificate

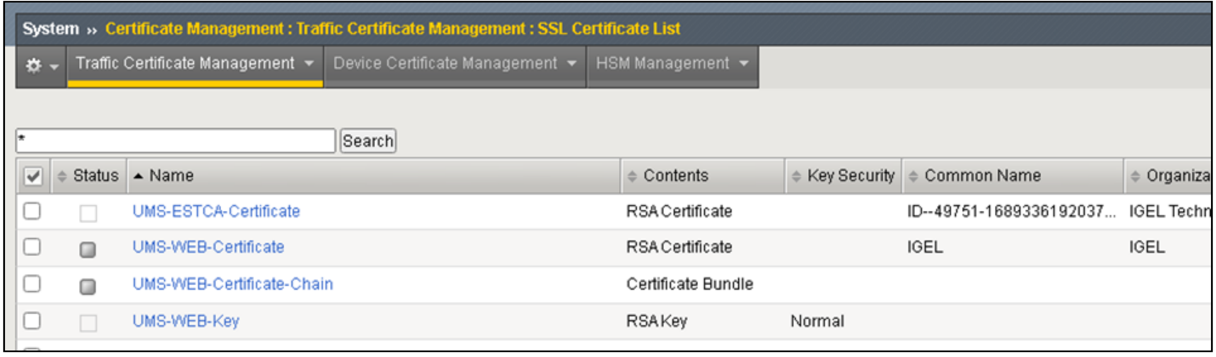


System » Certificate Management : Traffic Certificate Management : SSL Certificate List » Import SSL Certificates and Keys

SSL Certificate/Key Source

Import Type	Certificate
Certificate Name	● New ○ Overwrite Existing UMS-ESTCA-Certificate
Certificate Source	● Upload File ○ Paste Text Datei auswählen estca.cer
Free Space on Disk	1974 MB

5. Verify that you have all the imported certificates.



System » Certificate Management : Traffic Certificate Management : SSL Certificate List

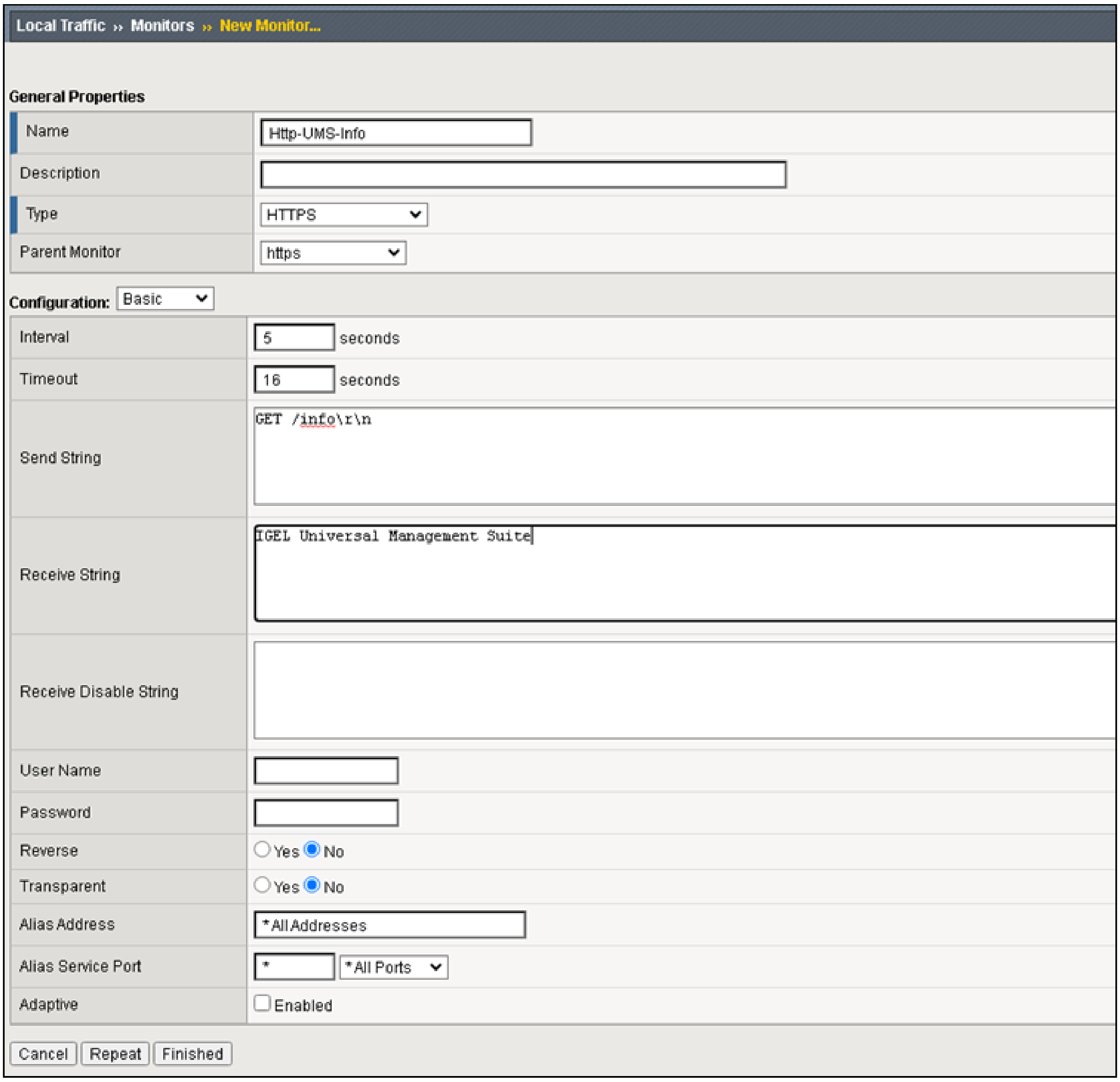
☑	Status	Name	Contents	Key Security	Common Name	Organiza
☐		UMS-ESTCA-Certificate	RSA Certificate		ID--49751-1689336192037...	IGEL Techn
☐	▨	UMS-WEB-Certificate	RSA Certificate		IGEL	IGEL
☐	▨	UMS-WEB-Certificate-Chain	Certificate Bundle			
☐		UMS-WEB-Key	RSA Key	Normal		

Backend Configuration

The UMS Server must be configured as backend server.

1. Add a Monitor and configure it for testing if the UMS info URL is online.
   The following properties must be set:

Type	HTTPS
Send String	GET /info\r\n
Receive String	IGEL Universal Management Suite



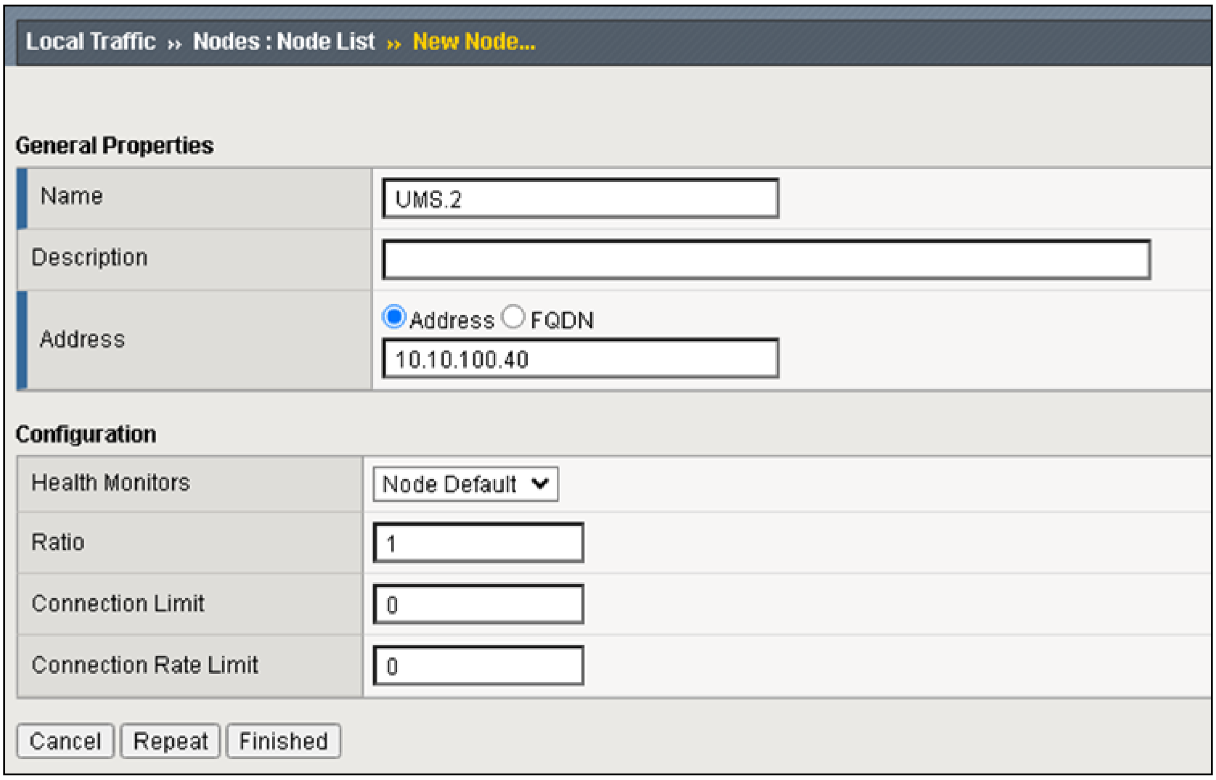
General Properties

Name	Http-UMS-Info
Description	
Type	HTTPS
Parent Monitor	https

Configuration: Basic

Interval	5 seconds
Timeout	16 seconds
Send String	GET /info\r\n
Receive String	IGEL Universal Management Suite
Receive Disable String	
User Name	
Password	
Reverse	○ Yes ● No
Transparent	○ Yes ● No
Alias Address	* All Addresses
Alias Service Port	* * All Ports
Adaptive	□ Enabled

2. Create a new Node and set the Address of the UMS Server.



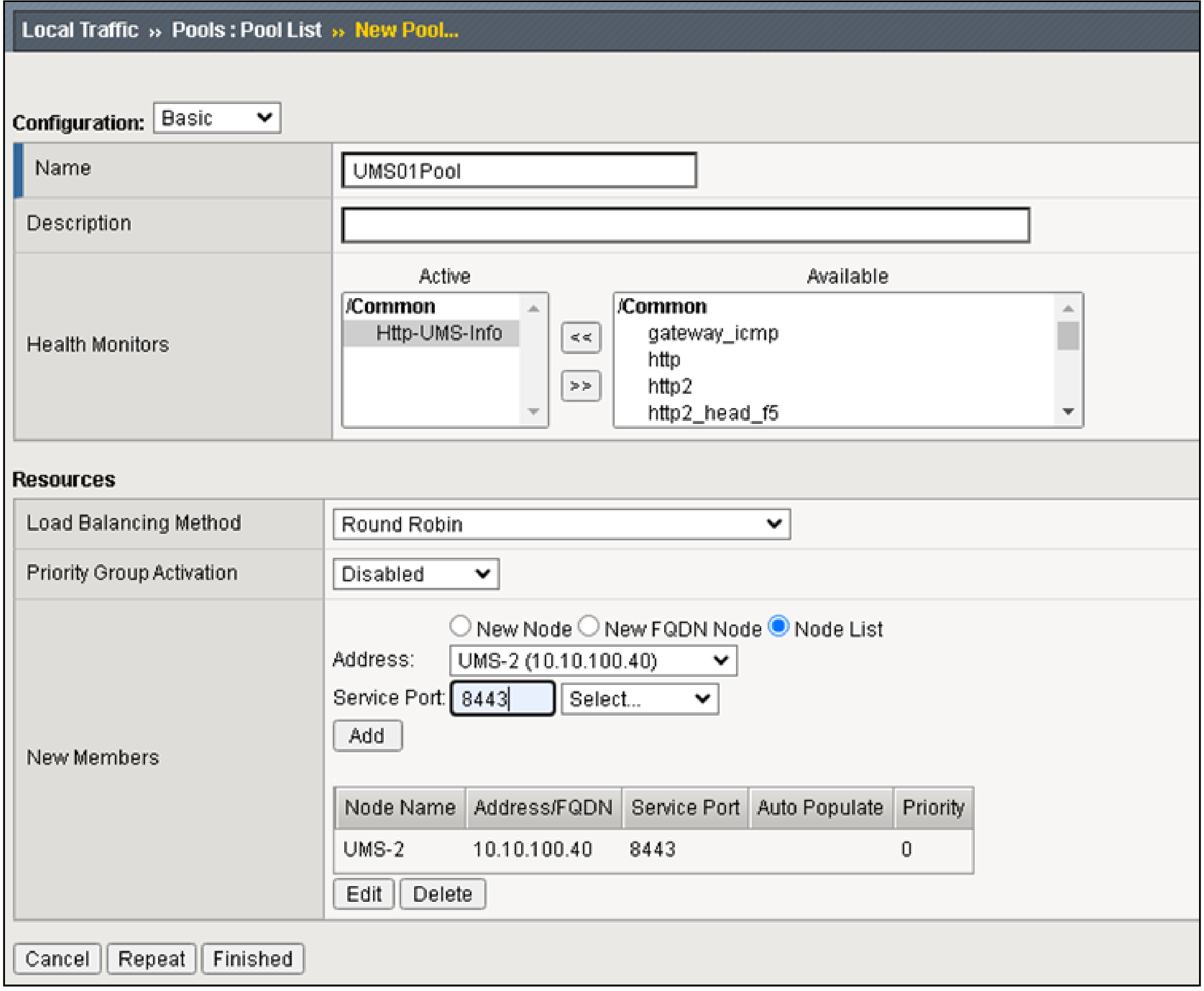
General Properties

Name	UMS.2
Description	
Address	● Address ○ FQDN 10.10.100.40

Configuration

Health Monitors	Node Default
Ratio	1
Connection Limit	0
Connection Rate Limit	0

3. Add Pool. In the pool configuration the monitor and the node server must be at least configured. There is no specific Load Balancing Method recommended.



Configuration: Basic

Name: UMS01Pool

Description:

Health Monitors: Active: /Common Http-UMS-Info; Available: /Common gateway_icmp, http, http2, http2_head_f5

Resources

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members: ○ New Node ○ New FQDN Node ● Node List

Address: UMS-2 (10.10.100.40)

Service Port: 8443 Select...

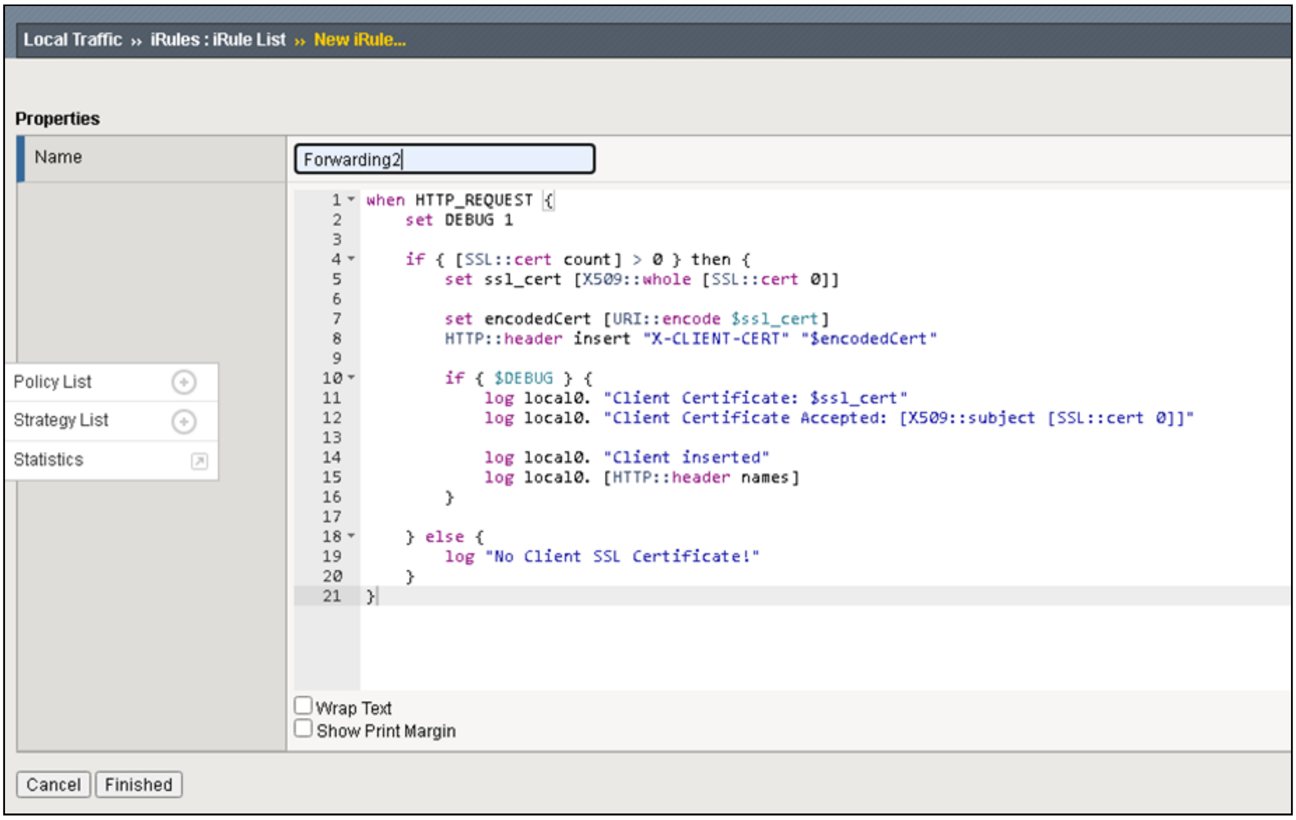
Node Name	Address/FQDN	Service Port	Auto Populate	Priority
UMS-2	10.10.100.40	8443		0

IRULE to forward the Client Certificate in HTTP Header

Irules is the Script support of F5 BIG-IP.

The Client Certificate can be read from the HTTP_REQUEST. The variable `[X509::whole [SSL::cert 0]]` contains it in `PEM` format.

The UMS expects the certificate URL Encoded so it must be encoded: `[URI::encode $ssl_cert]`



Properties

Name: Forwarding2

```
when HTTP_REQUEST {
    set DEBUG 1

    if { [SSL::cert count] > 0 } then {
        set ssl_cert [X509::whole [SSL::cert 0]]

        set encodedCert [URI::encode $ssl_cert]
        HTTP::header insert "X-CLIENT-CERT" "$encodedCert"

        if { $DEBUG } {
            log local0. "Client Certificate: $ssl_cert"
            log local0. "Client Certificate Accepted: [X509::subject [SSL::cert 0]]"

            log local0. "Client inserted"
            log local0. [HTTP::header names]
        }

    } else {
        log "No Client SSL Certificate!"
    }
}
```

□ Wrap Text
□ Show Print Margin

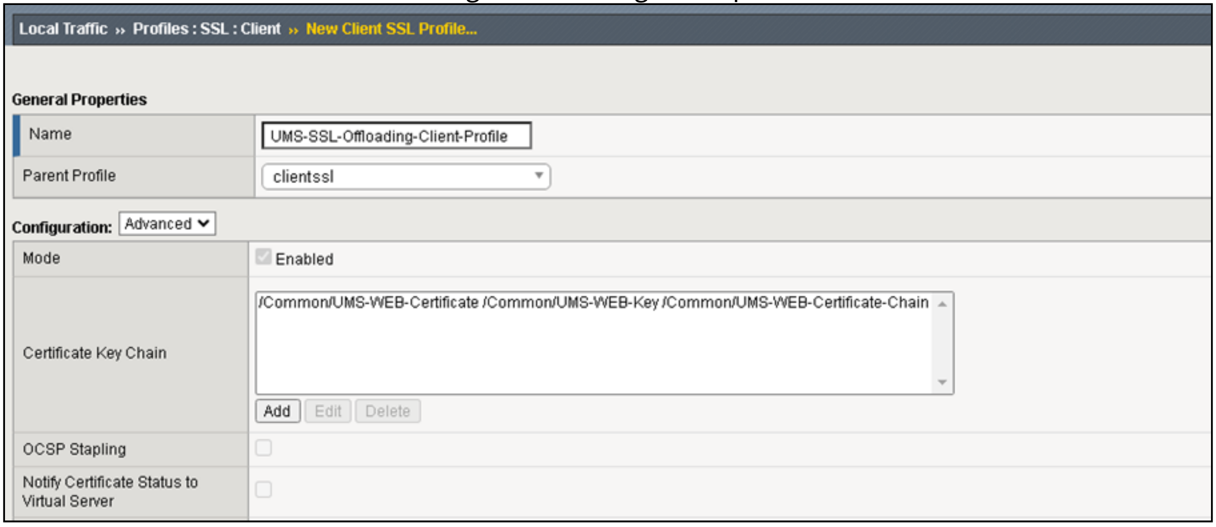
Forwarding Header Example:

```
when HTTP_REQUEST {
    set DEBUG 1

    if { [SSL::cert count] > 0 } then {
        set ssl_cert [X509::whole [SSL::cert 0]]

        set encodedCert [URI::encode $ssl_cert]
        HTTP::header insert "X-CLIENT-CERT" "$encodedCert"

        if { $DEBUG } {
            log local0. "Client Certificate: $ssl_cert"
            log local0. "Client Certificate Accepted: [X509::subject [SSL::cert 0]]"

            log local0. "Client inserted"
            log local0. [HTTP::header names]
        }

    } else {
        log "No Client SSL Certificate!"
    }
}
```

SSL Client Profile

The SSL Client Profile is used to set the SSL configuration for all incoming requests to the Virtual Servers.

1. Add a new SSL Client Profile and Configure according to the picture below.



Local Traffic » Profiles : SSL : Client » New Client SSL Profile...

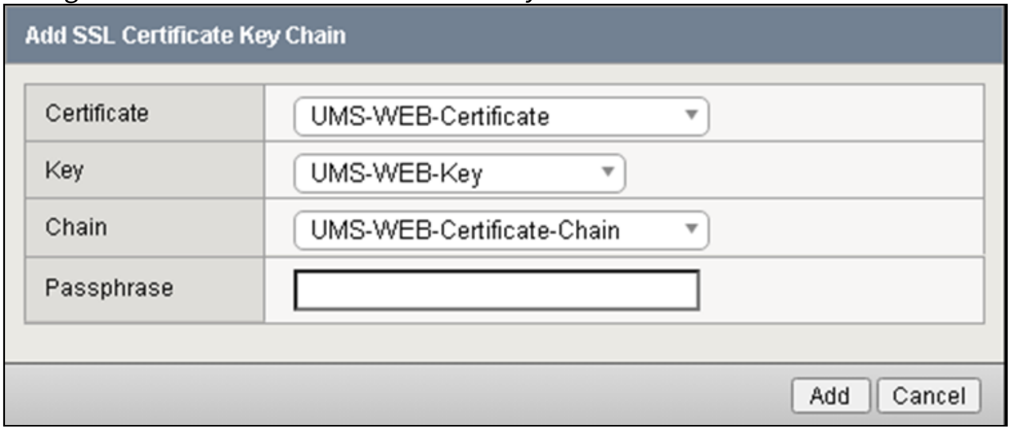
General Properties

Name	UMS-SSL-Offloading-Client-Profile
Parent Profile	clientssl

Configuration: Advanced

Mode	☑ Enabled
Certificate Key Chain	/Common/UMS-WEB-Certificate /Common/UMS-WEB-Key /Common/UMS-WEB-Certificate-Chain Add Edit Delete
OCSP Stapling	□
Notify Certificate Status to Virtual Server	□

2. Configure the UMS WEB Certificates and Key.

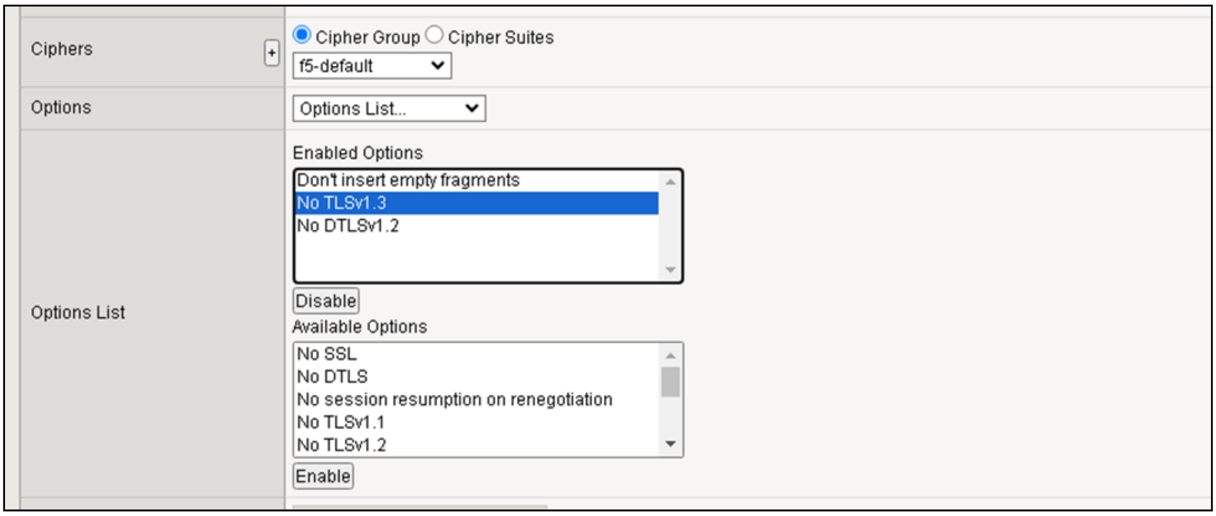


Add SSL Certificate Key Chain

Certificate	UMS-WEB-Certificate
Key	UMS-WEB-Key
Chain	UMS-WEB-Certificate-Chain
Passphrase	

3. TLSv1.3 is used in the connection from the Device to UMS so the ciphers must be customized.

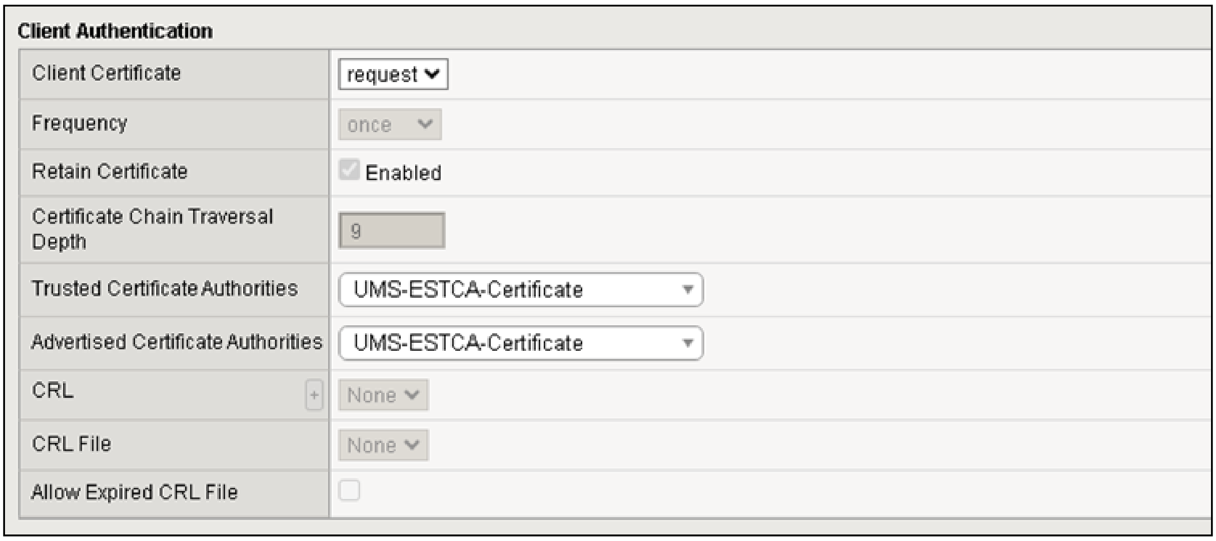
Ciphers	**f5-default** can be used as Cipher Group
Options List	disable the “No TLSv1.3” entry in the Enabled Options list



Ciphers	● Cipher Group ○ Cipher Suites f5-default
Options	Options List...
Options List	Enabled Options Don't insert empty fragments No TLSv1.3 No DTLSv1.2 Disable Available Options No SSL No DTLS No session resumption on renegotiation No TLSv1.1 No TLSv1.2 Enable

4. The necessary customizations for Client Certificate Authentication are:

Client Certificate	This value must be set to **request**
Trusted Certificate Authorities	Set to **UMS-ESTCA-Certificate**
Advertised Certificate Authorities	Can be set to **UMS-ESTCA-Certificate**



Client Authentication

Client Certificate	request
Frequency	once
Retain Certificate	☑ Enabled
Certificate Chain Traversal Depth	9
Trusted Certificate Authorities	UMS-ESTCA-Certificate
Advertised Certificate Authorities	UMS-ESTCA-Certificate
CRL	None
CRL File	None
Allow Expired CRL File	□

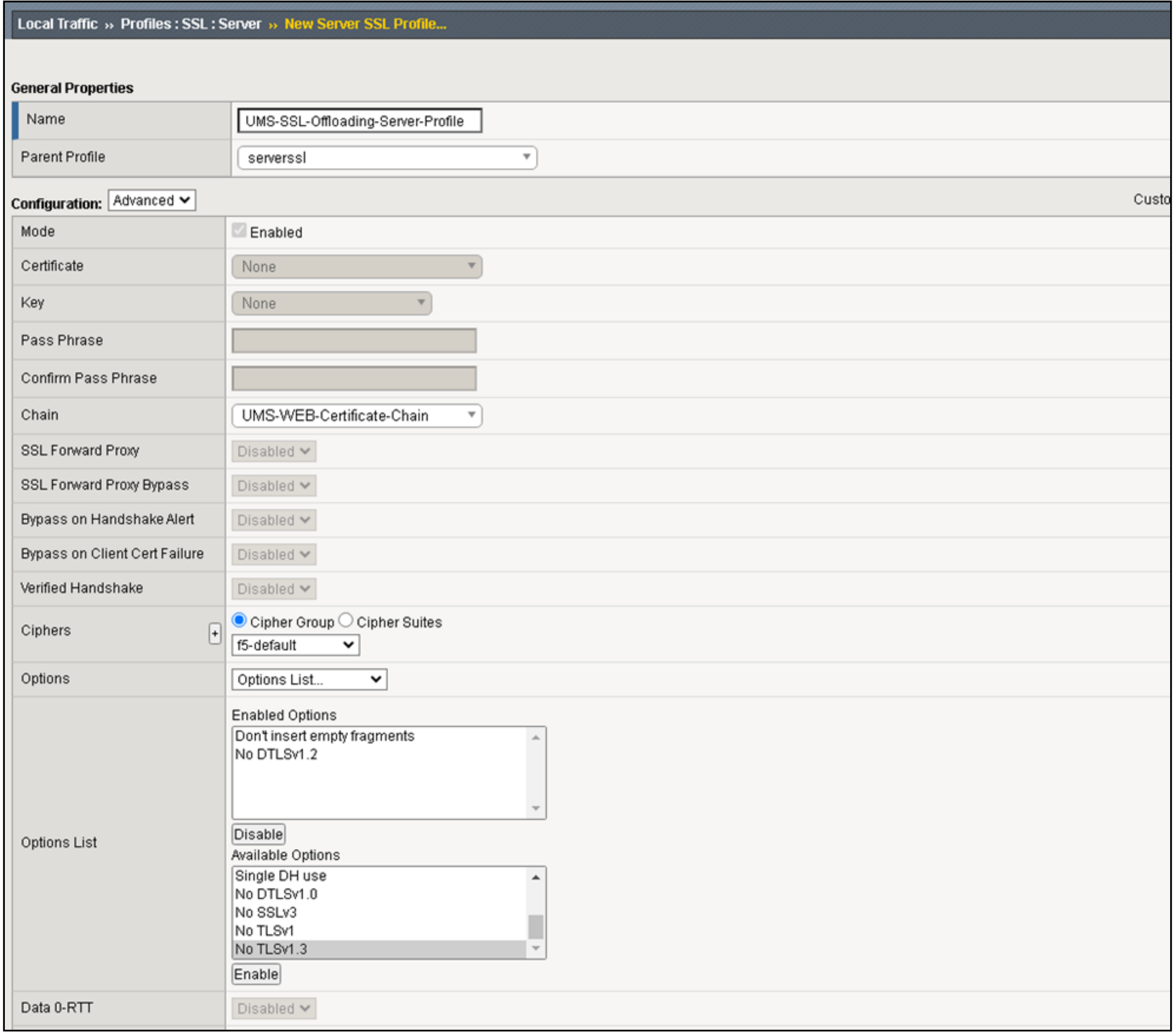
SSL Server Profile

The SSL Server Profile is used to set the SSL configuration for all requests to the Backend Servers (UMS).

1. Create a new SSL Server Profile.

2. Set the Chain value to **UMS Web Certificate Chain**.

3. Set the TLSv 1.3 configuration the same as for the SSL Client Profile above.



Local Traffic » Profiles : SSL : Server » New Server SSL Profile...

General Properties

Name	UMS-SSL-Offloading-Server-Profile
Parent Profile	serverssl

Configuration: Advanced

Custo

Mode	☑ Enabled
Certificate	None
Key	None
Pass Phrase	
Confirm Pass Phrase	
Chain	UMS-WEB-Certificate-Chain
SSL Forward Proxy	Disabled
SSL Forward Proxy Bypass	Disabled
Bypass on Handshake Alert	Disabled
Bypass on Client Cert Failure	Disabled
Verified Handshake	Disabled
Ciphers	● Cipher Group ○ Cipher Suites f5-default
Options	Options List...
Options List	Enabled Options Don't insert empty fragments No DTLSv1.2 Disable Available Options Single DH use No DTLSv1.0 No SSLv3 No TLSv1 No TLSv1.3 Enable
Data 0-RTT	Disabled

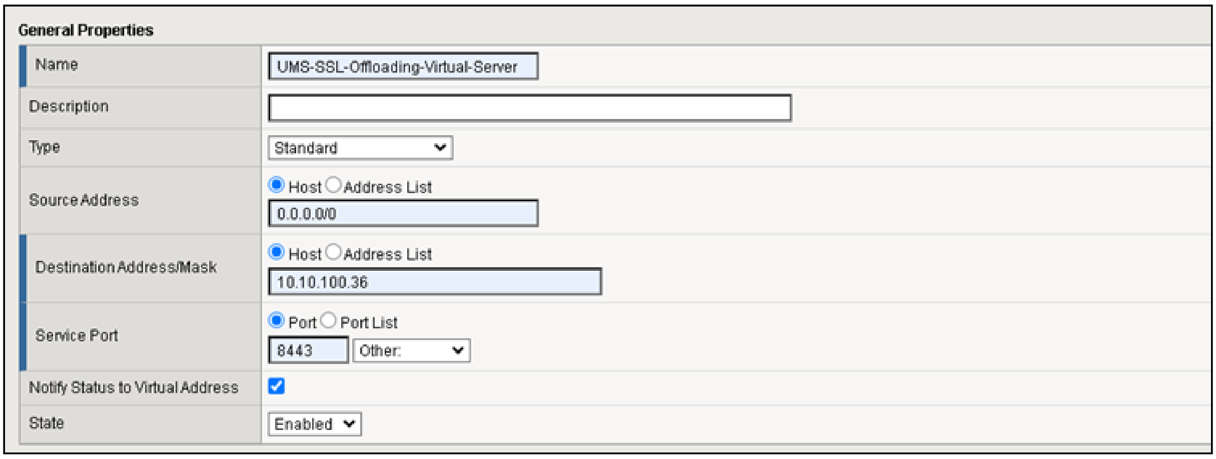
Virtual Server Configuration

The Virtual Server defines the Listener in F5 BIG-IP.

1. Set the following values:

Type	Standard
Source Address	From which IP are requests allowed. Set it to * if this shouldn't be evaluated
Destination Address	The Address under which this Virtual Server is reachable

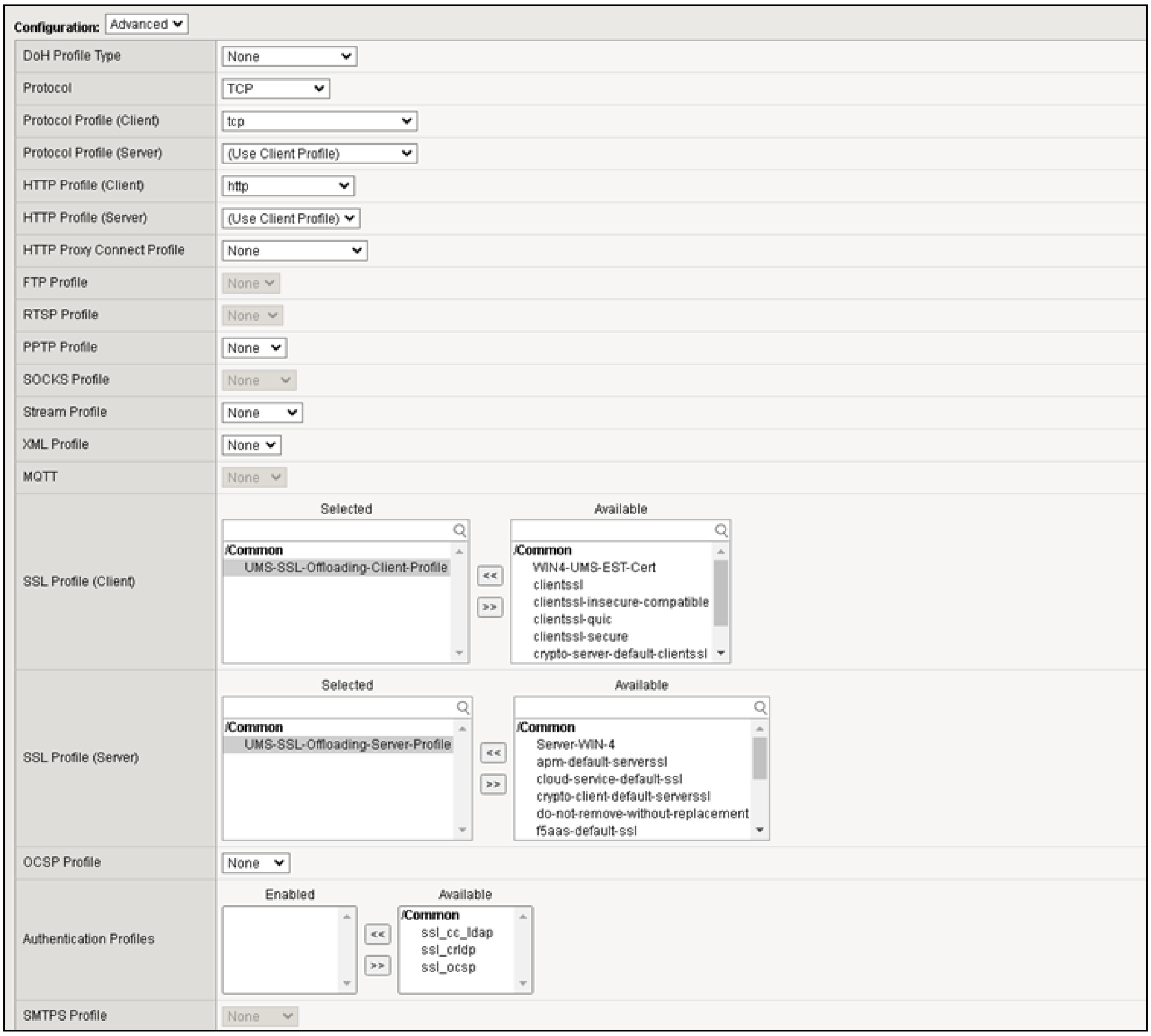
Service Port	Select the UMS Port



General Properties

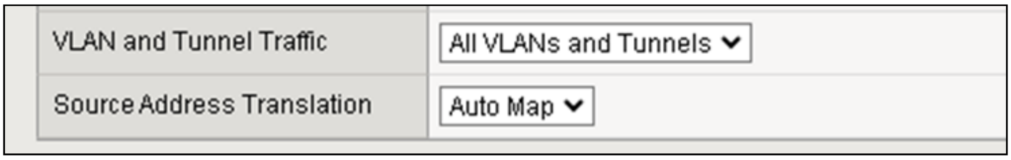
Name	UMS-SSL-Offloading-Virtual-Server
Description	
Type	Standard
Source Address	● Host ○ Address List 0.0.0.0/0
Destination Address/Mask	● Host ○ Address List 10.10.100.36
Service Port	● Port ○ Port List 8443 Other:
Notify Status to Virtual Address	☑
State	Enabled

Protocol	TCP
HTTP Profile	http, required to evaluate the HTTP Header
SSL Profile (Client)	Add the earlier created Client SSL Profile
SSL Profile (Server)	Add the earlier created Server SSL Profile
Source Address Translation	Set it to Auto Map



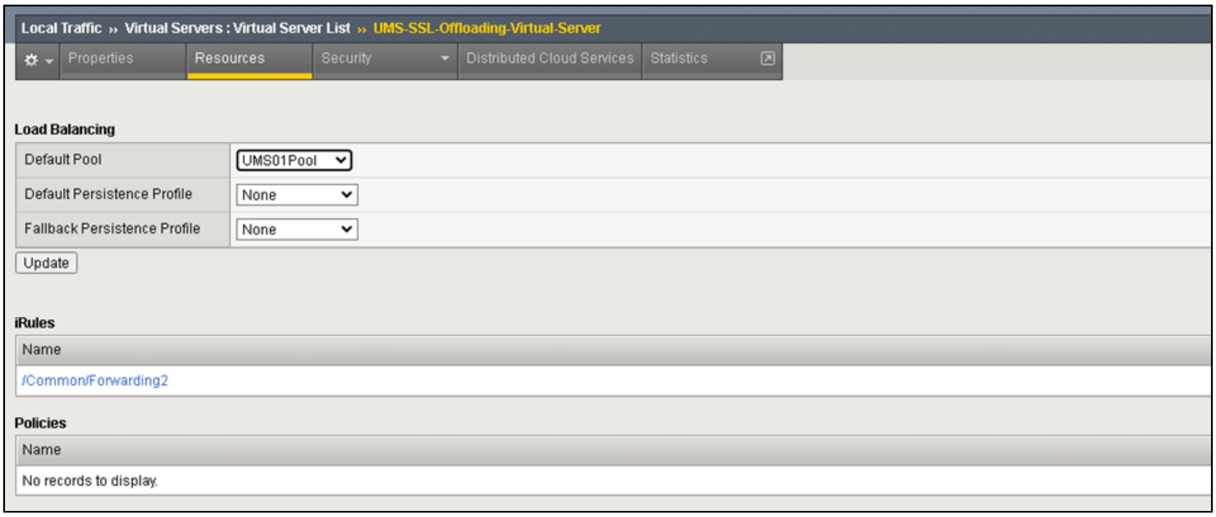
Configuration: Advanced

DoH Profile Type	None
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	http
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
PPTP Profile	None
SOCKS Profile	None
Stream Profile	None
XML Profile	None
MQTT	None
SSL Profile (Client)	Selected: /Common UMS-SSL-Offloading-Client-Profile Available: /Common WIN4-UMS-EST-Cert clientssl clientssl-insecure-compatible clientssl-quic clientssl-secure crypto-server-default-clientssl
SSL Profile (Server)	Selected: /Common UMS-SSL-Offloading-Server-Profile Available: /Common Server-WIN-4 apm-default-serverssl cloud-service-default-ssl crypto-client-default-serverssl do-not-remove-without-replacement f5aas-default-ssl
OCSP Profile	None
Authentication Profiles	Enabled: Available: /Common ssl_cc_ldap ssl_crldp ssl_ocsp
SMTPS Profile	None



VLAN and Tunnel Traffic	All VLANs and Tunnels
Source Address Translation	Auto Map

2. Add the Pool and iRule to the Virtual Server.



Local Traffic » Virtual Servers : Virtual Server List » UMS-SSL-Offloading-Virtual-Server
Properties
Resources
Security
Distributed Cloud Services
Statistics

Load Balancing

Default Pool	UMS01Pool
Default Persistence Profile	None
Fallback Persistence Profile	None

iRules

Name
/Common/Forwarding2

Policies

Name
No records to display.

Azure Application Gateway: Example Configuration as Reverse Proxy in IGEL UMS with SSL Offloading

This article describes the IGEL Unified Management Suite (UMS) configurations and the Azure Application Gateway configurations you need for SSL Offloading.

> General compatibility is tested with the configurations described in this article. There could be different ways to do the configuration.
> As the reverse proxy is an external software we cannot provide full support for each version.

> A reverse proxy / external load balancer can be used if you manage IGEL OS 12 devices only. See IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices.

Requirements

- IGEL UMS version 12.04.100 or higher
- IGEL OS version 12.3.2 or higher
- If the ICG is used: ICG version 12.04.100 or higher
- In the case of the Distributed UMS or High Availability installations, the time must be synchronized on all servers.

> For extracting keys and certificate chains, you will require a suitable tool like "Keystore Explorer". Please use the latest version of such tools.
> Please also make sure that you use Java 17.

Process Overview

We advise you to follow the process presented here. You will find the steps to take in detail in the sections below.

1. Understand different connection types.
2. Create the certificates for the Azure Application Gateway in UMS.
3. Configure your UMS:
   a. Activate Forwarding Client Certificate Processing
   b. Modify Server Network Settings
   c. Set Process Configuration
4. Export Certificates for Azure Application Gateway Configuration.
5. Configure the Azure Application Gateway:
   a. Create Azure Application Gateway
   b. Add a Routing Rule for Onboarding Connection
   c. Add a Routing Rule for the Websocket Connection
   d. Check Network Security Group

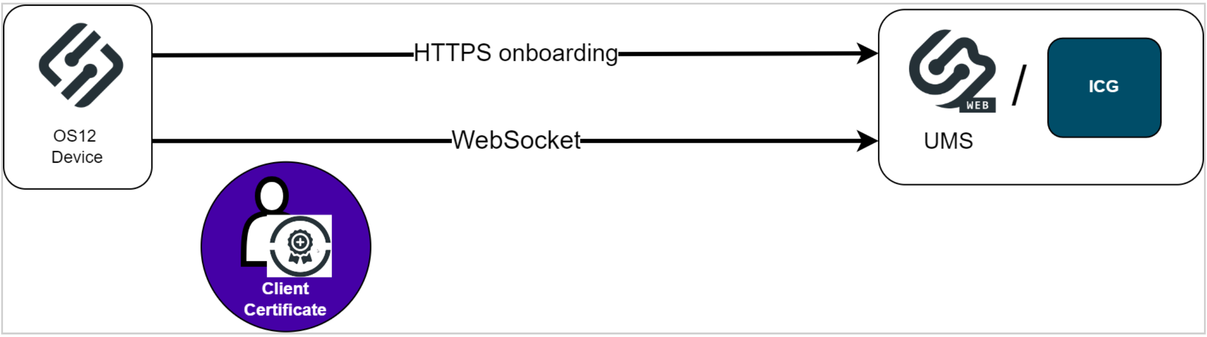
   e. Set Mutual Authentication for WebSocket Connection
   f. Add a Rewrite for Client Certificate Forwarding
6. Troubleshoot certificate error, if needed.

Connection Types Between Device and UMS

For a successful configuration it is important to understand the different connection types.

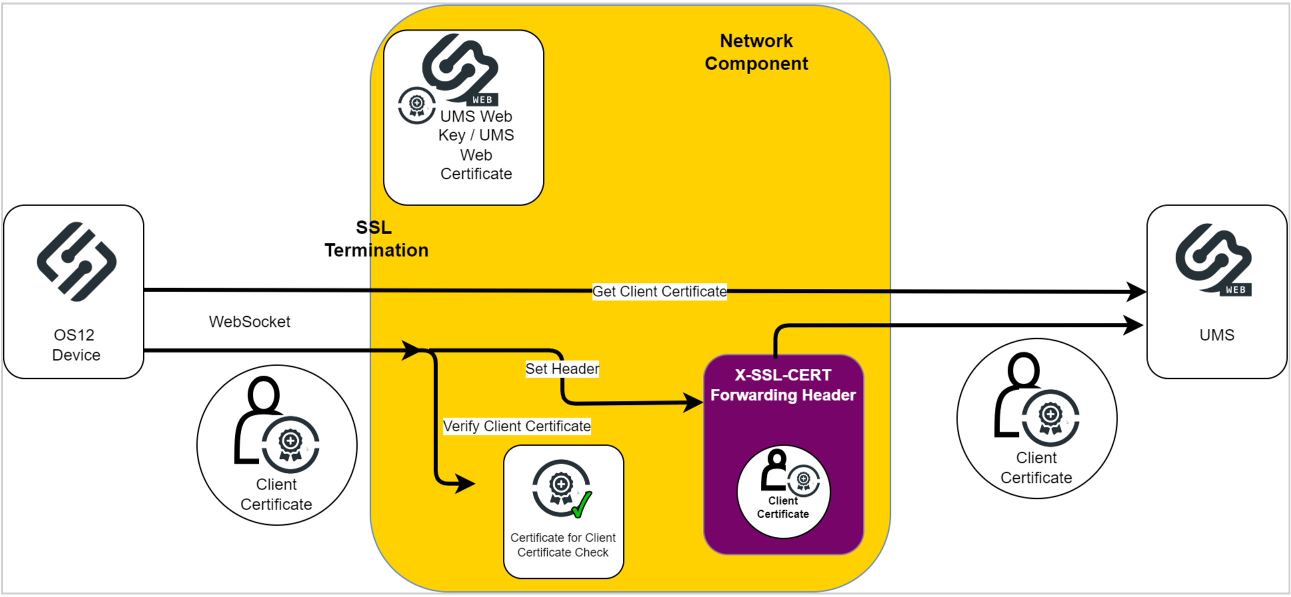
Device to ICG / UMS Communication

The communication of the devices to UMS or ICG consists of two different types. Regular HTTPS calls for the device registration and a WebSocket connection with Mutual TLS for device management.



Communication via Reverse Proxy

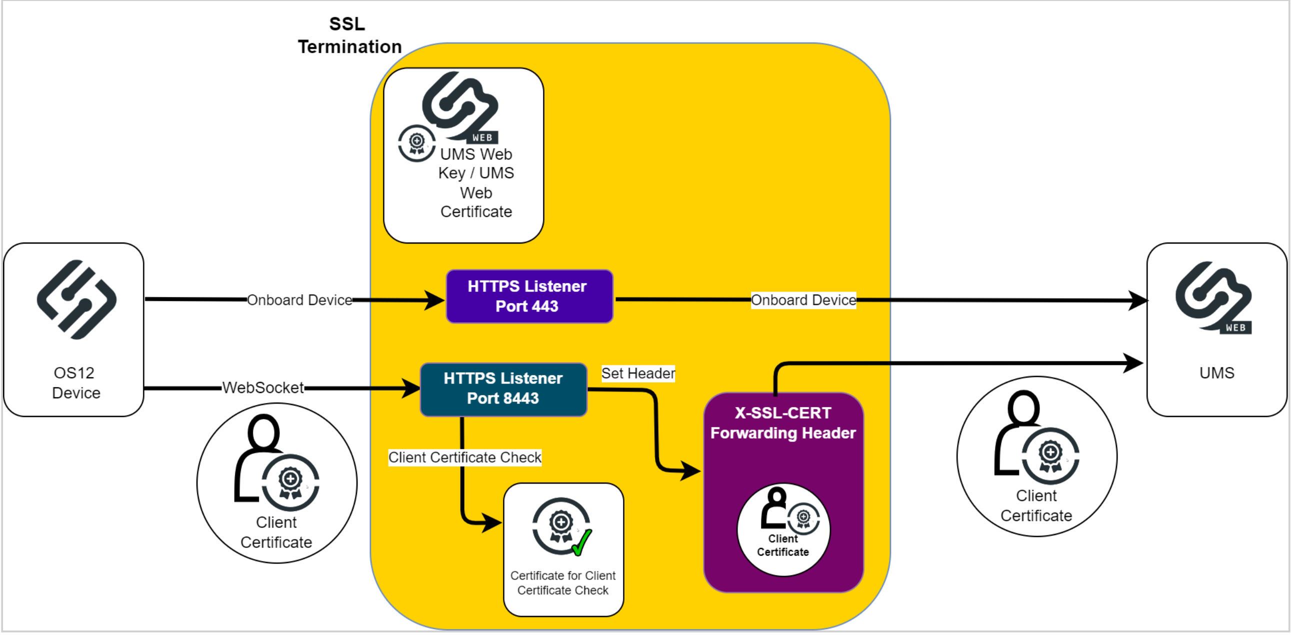
The diagram shows the device to UMS connection via a Network Component like Azure Application Gateway. The required connections are listed for SSL Offloading. The diagram shows one HTTPS connection which is necessary for device onboarding (Client Certificate request) and the following WebSocket connection where Mutual TLS and Client Certificate forwarding is required.



Communication via Azure Application Gateway

Some Reverse Proxies like NGINX support a Mutual TLS configuration with optional Client Certificate check. These Reverse Proxies can handle both required UMS connections with one configured listener. The Azure Application Gateway does not support this feature. The two types of connections used must be handled separately. According to this the Azure Application Gateway configuration must contain two separate listeners with corresponding rules.

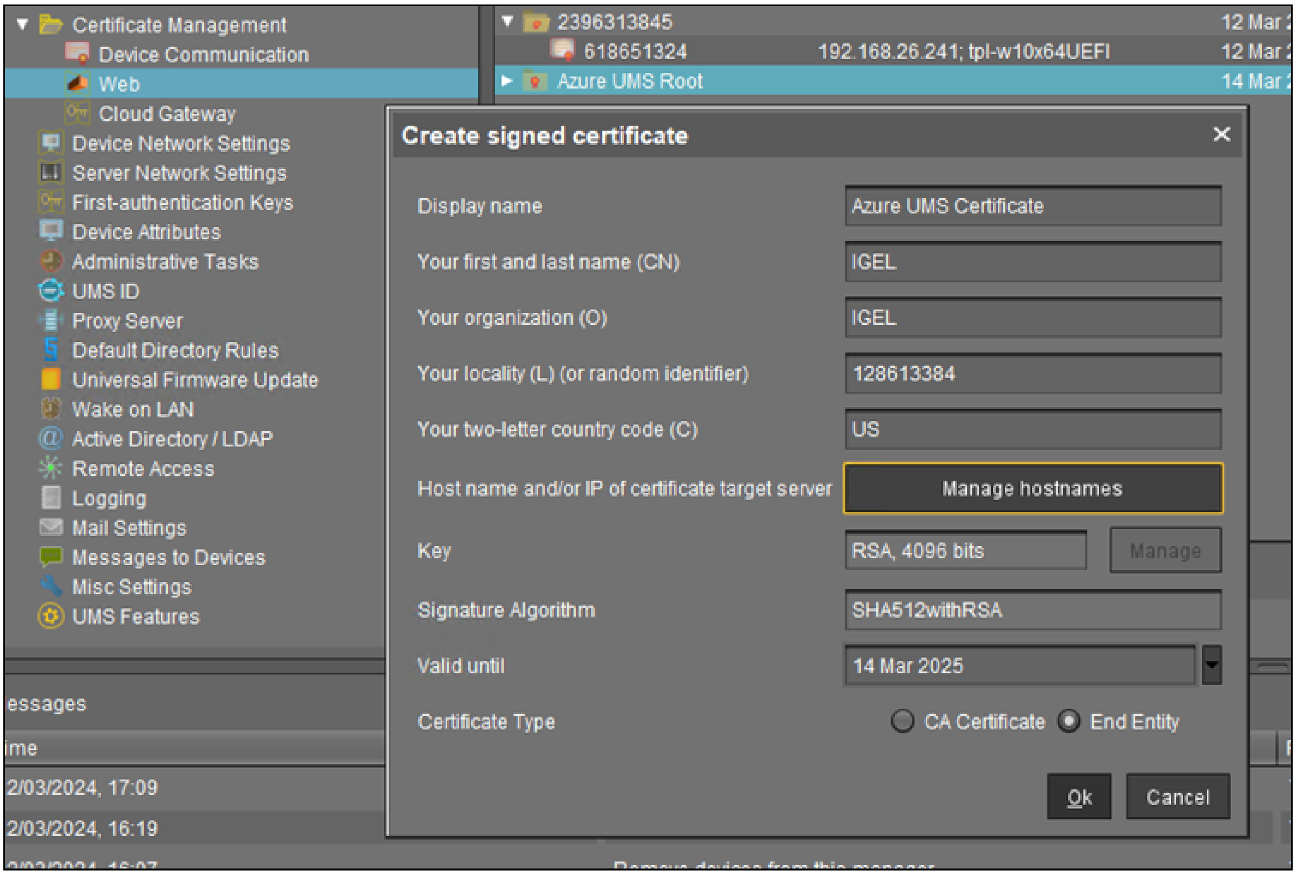
The UMS supports the separation of the Onboarding and the WebSocket connections. The following diagram shows an overview of a device to UMS connection via the Application Gateway.



The HTTPS listener for device onboarding could use the standard https Port (443) and forwards direct to UMS. In this example, the HTTPS listener for WebSocket connection listens on Port 8443 and uses mutual TLS for the Client Certificate Check and adds it to the Request Header, so that the UMS can verify it.

Create Certificate for Azure Application Gateway

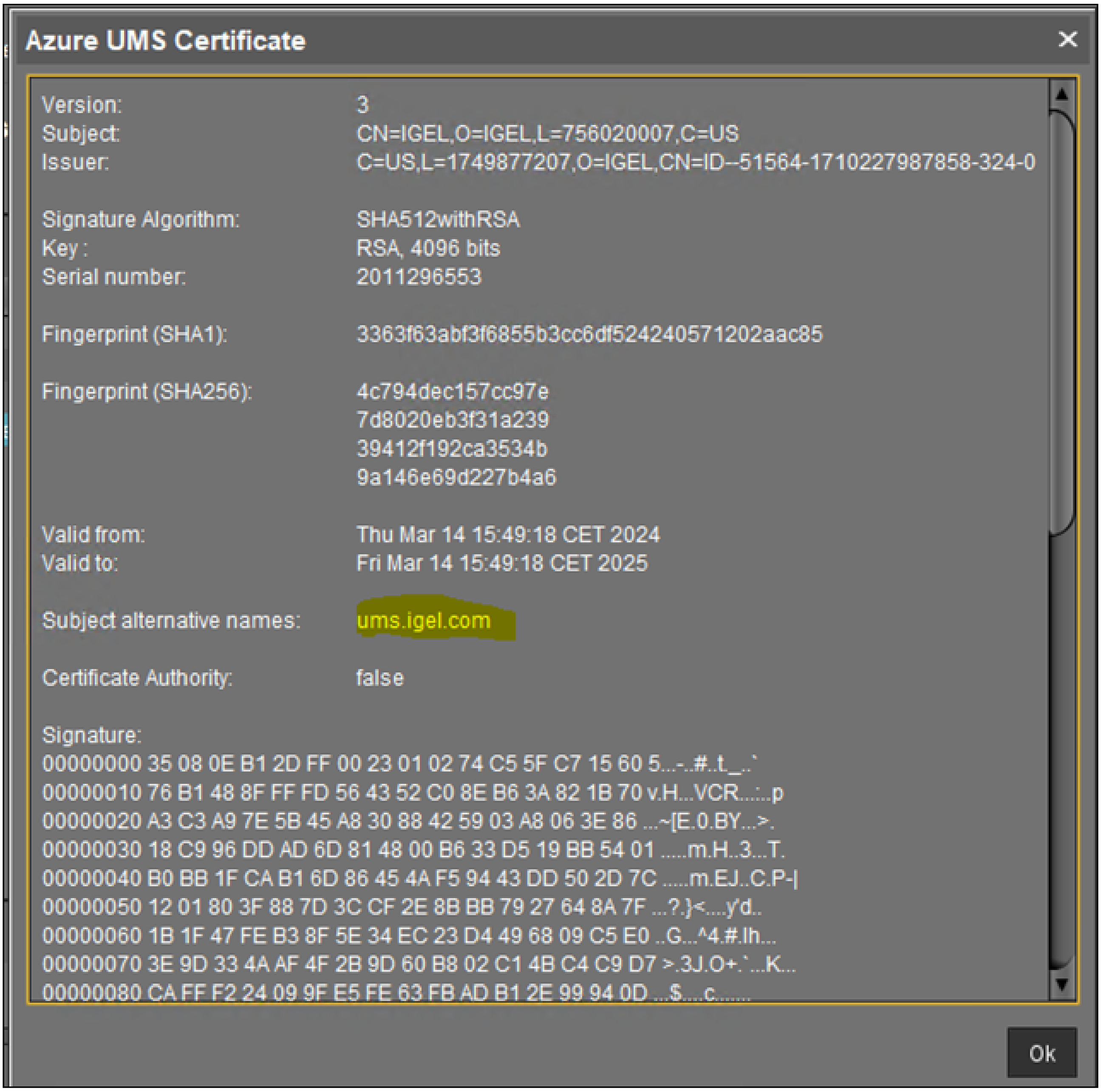
The suggested approach for Azure Application Gateway is to use an own certificate which must be added under **Certificate Management** in the UMS. This certificate can be added under **Certificate Management** either to the **Web** or **Cloud Gateway** section.



Create signed certificate

Display name	Azure UMS Certificate
Your first and last name (CN)	IGEL
Your organization (O)	IGEL
Your locality (L) (or random identifier)	128613384
Your two-letter country code (C)	US
Host name and/or IP of certificate target server	Manage hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA512withRSA
Valid until	14 Mar 2025
Certificate Type	○ CA Certificate ● End Entity

The Azure Application Gateway FQDN must be added as Hostname so that in the Certificate it is listed as a Subject Alternative Name.



Azure UMS Certificate

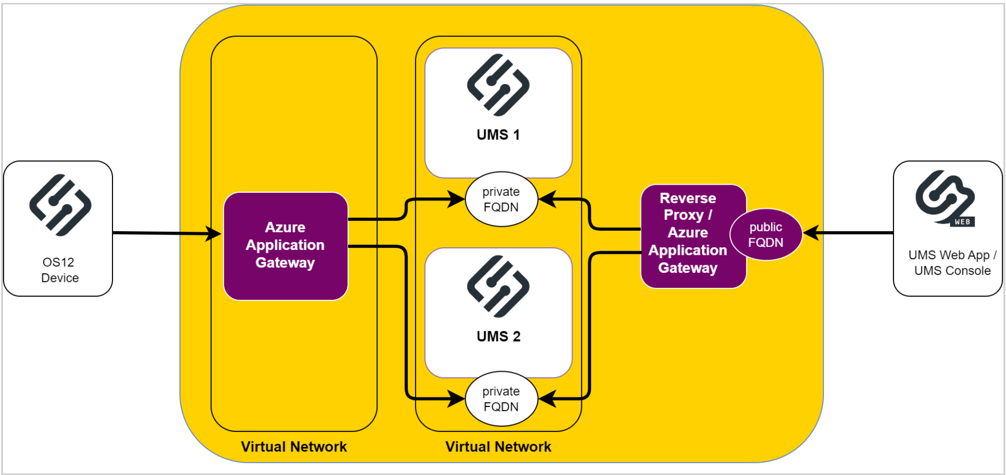
```
Version:                    3
Subject:                    CN=IGEL,O=IGEL,L=756020007,C=US
Issuer:                     C=US,L=1749877207,O=IGEL,CN=ID--51564-1710227987858-324-0

Signature Algorithm:        SHA512withRSA
Key :                       RSA, 4096 bits
Serial number:              2011296553

Fingerprint (SHA1):         3363f63abf3f6855b3cc6df524240571202aac85

Fingerprint (SHA256):       4c794dec157cc97e
                            7d8020eb3f31a239
                            39412f192ca3534b
                            9a146e69d227b4a6

Valid from:                 Thu Mar 14 15:49:18 CET 2024
Valid to:                   Fri Mar 14 15:49:18 CET 2025

Subject alternative names:  ums.igel.com

Certificate Authority:      false

Signature:
00000000 35 08 0E B1 2D FF 00 23 01 02 74 C5 5F C7 15 60 5...-..#..t_..`
00000010 76 B1 48 8F FF FD 56 43 52 C0 8E B6 3A 82 1B 70 v.H...VCR...:..p
00000020 A3 C3 A9 7E 5B 45 A8 30 88 42 59 03 A8 06 3E 86 ...~[E.0.BY...>.
00000030 18 C9 96 DD AD 6D 81 48 00 B6 33 D5 19 BB 54 01 .....m.H..3...T.
00000040 B0 BB 1F CA B1 6D 86 45 4A F5 94 43 DD 50 2D 7C .....m.EJ..C.P-|
00000050 12 01 80 3F 88 7D 3C CF 2E 8B BB 79 27 64 8A 7F ...?.}<....y'd..
00000060 1B 1F 47 FE B3 8F 5E 34 EC 23 D4 49 68 09 C5 E0 ..G...^4.#.Ih...
00000070 3E 9D 33 4A AF 4F 2B 9D 60 B8 02 C1 4B C4 C9 D7 >.3J.O+.`...K...
00000080 CA FF F2 24 09 9F E5 FE 63 FB AD B1 2E 99 94 0D ...$....c.......
```

UMS and ICG Certificates Examples

The network integration of Azure Application Gateway with the UMS and ICG is a wide area with a lot of possible network settings. Here are two examples listed with appropriate certificate details:

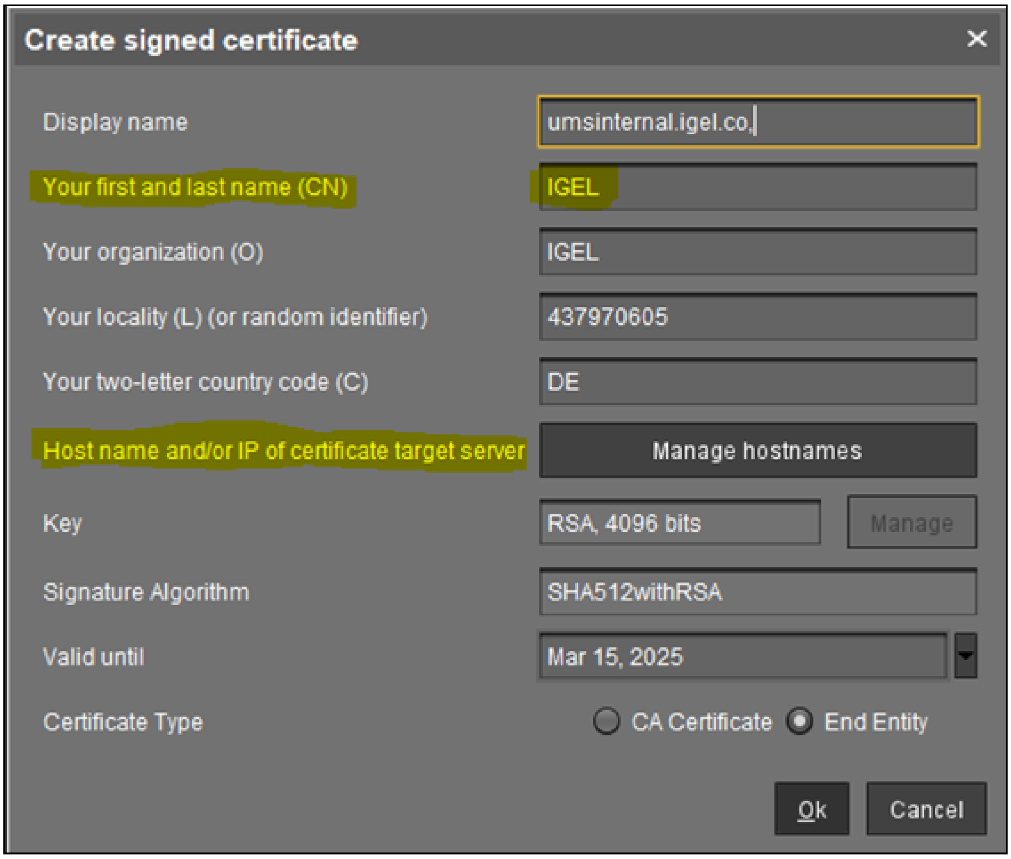
Click for the UMS Example

This diagram shows an Azure Application Gateway in front of UMS servers.

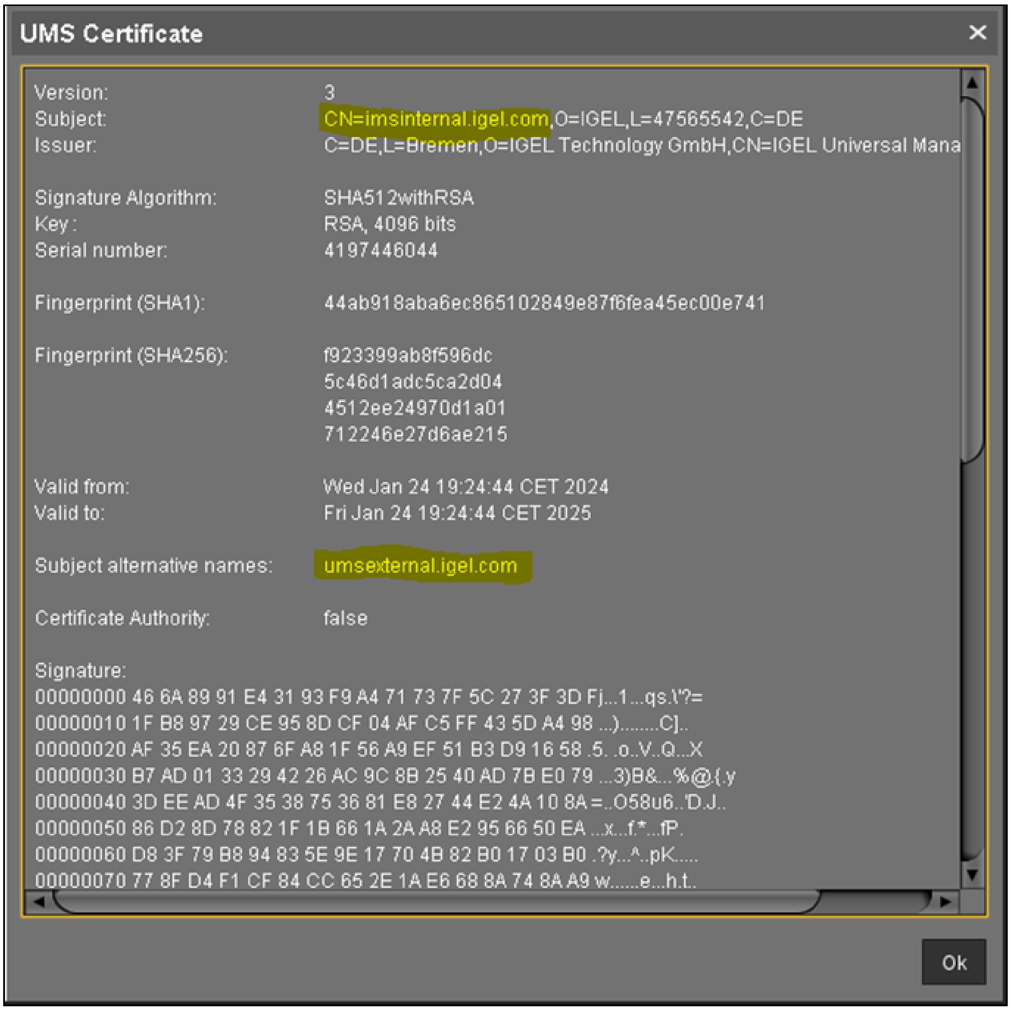


These UMS servers are within a Virtual Network and only reachable by a private FQDN. There is one Azure Application Gateway for incoming Device requests and another Reverse Proxy / Loadbalancer (Azure Application Gateway) for UMS Web App and Console requests. So the UMS server is reachable by two different addresses. This must be considered for **Web** certificate generation.

The private FQDN address is used by the Azure Application Gateway for UMS connection. This address **must be set as Common Name (CN)** to the UMS Web certificate. The public FQDN must be set for UMS Web App / Console connections to the UMS as Hostname (Subject Alternative Name).


Create signed certificate

Display name	umsinternal.igel.co
Your first and last name (CN)	IGEL
Your organization (O)	IGEL
Your locality (L) (or random identifier)	437970605
Your two-letter country code (C)	DE
Host name and/or IP of certificate target server	Manage hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA512withRSA
Valid until	Mar 15, 2025
Certificate Type	○ CA Certificate ● End Entity

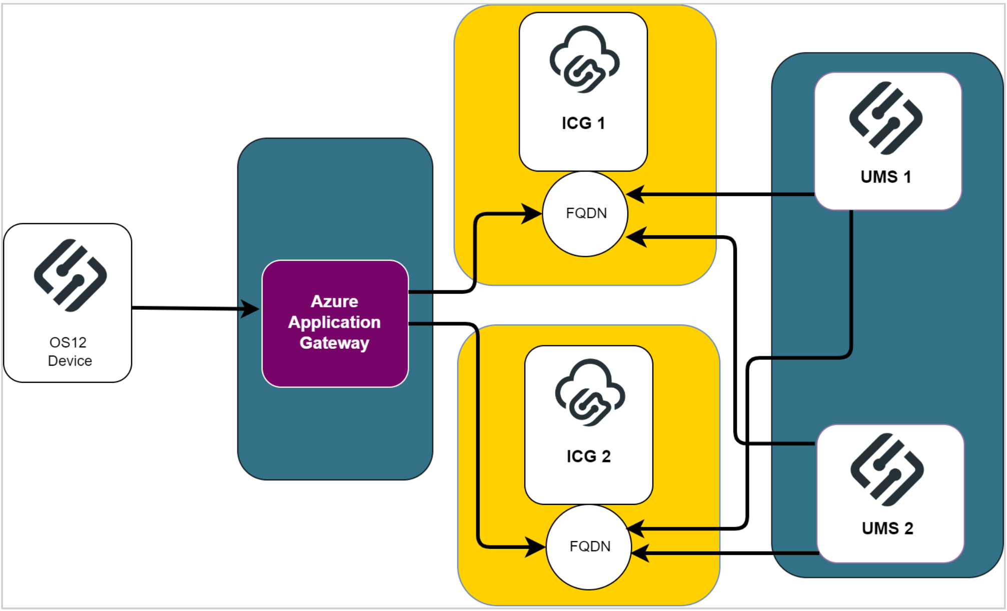


UMS Certificate

```
Version:                     3
Subject:                     CN=imsinternal.igel.com,O=IGEL,L=47565542,C=DE
Issuer:                      C=DE,L=Bremen,O=IGEL Technology GmbH,CN=IGEL Universal Mana

Signature Algorithm:         SHA512withRSA
Key :                        RSA, 4096 bits
Serial number:               4197446044

Fingerprint (SHA1):          44ab918aba6ec865102849e87f6fea45ec00e741

Fingerprint (SHA256):        f923399ab8f596dc
                             5c46d1adc5ca2d04
                             4512ee24970d1a01
                             712246e27d6ae215

Valid from:                  Wed Jan 24 19:24:44 CET 2024
Valid to:                    Fri Jan 24 19:24:44 CET 2025

Subject alternative names:   umsexternal.igel.com

Certificate Authority:       false

Signature:
00000000 46 6A 89 91 E4 31 93 F9 A4 71 73 7F 5C 27 3F 3D Fj...1...qs.\'?=
00000010 1F B8 97 29 CE 95 8D CF 04 AF C5 FF 43 5D A4 98 ...)........C]..
00000020 AF 35 EA 20 87 6F A8 1F 56 A9 EF 51 B3 D9 16 58 .5. .o..V..Q...X
00000030 B7 AD 01 33 29 42 26 AC 9C 8B 25 40 AD 7B E0 79 ...3)B&...%@.{.y
00000040 3D EE AD 4F 35 38 75 36 81 E8 27 44 E2 4A 10 8A =..O58u6..'D.J..
00000050 86 D2 8D 78 82 1F 1B 66 1A 2A A8 E2 95 66 50 EA ...x...f.*...fP.
00000060 D8 3F 79 B8 94 83 5E 9E 17 70 4B 82 B0 17 03 B0 .?y...^..pK.....
00000070 77 8F D4 F1 CF 84 CC 65 2E 1A E6 68 8A 74 8A A9 w......e...h.t..
```

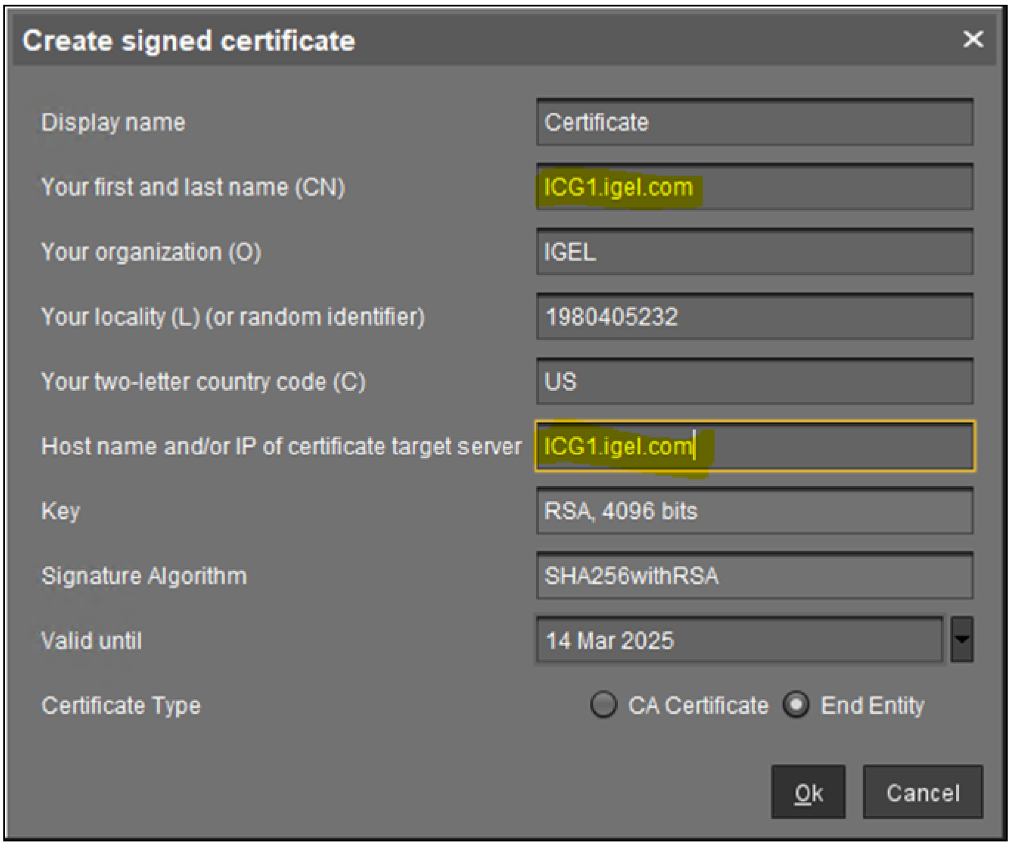
Click for the ICG Example

The diagram shows an example of Azure Application Gateway and ICG integration.



In this scenario the Azure Application Gateway connects to the ICG via the same FQDN as the UMS server. The ICG might be in a DMZ so only one FQDN is required.

The **Cloud Gateway** certificate requires the **FQDN as Common Name** and as **Subject Alternative Name** for UMS management.



Create signed certificate

Display name	Certificate
Your first and last name (CN)	ICG1.igel.com
Your organization (O)	IGEL
Your locality (L) (or random identifier)	1980405232
Your two-letter country code (C)	US
Host name and/or IP of certificate target server	ICG1.igel.com
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	14 Mar 2025
Certificate Type	○ CA Certificate ● End Entity

UMS Configurations

Activate Forwarding Client Certificate Processing on UMS / ICG

If no ICG is used, the processing of forwarded Client Certificates must be activated on UMS side. In case only an ICG is used behind an Azure Application Gateway, activate the processing of forwarded Client Certificates on ICG side.

To activate forwarding Client Certificate processing on UMS:

1. Open the configuration file: (InstallDir)/IGEL/RemoteManager/rmguiserver/conf/appconfig/application.yml
   You will see:

   ```
   igel:
       client-cert-forwarding:
           enabled: false
           client-cert-forwarded-header: X-SSL-CERT
   ```

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

   ```
   client-cert-forwarding:
       enabled: true
   ```

3. The forwarding Header can be configured. The X-SSL-CERT Header value can be changed but be aware to change the corresponding value in the Application Gateway configuration.

4. Save the configuration changes and restart the UMS Server service. For details on how you can restart the service, see IGEL UMS HA Services and Processes.

To activate the processing of forwarded Client Certificates on ICG side:

1. Open the configuration file `[UMS i nstallation directory]/IGEL/icg/usg/conf/application-prod.yml`.
   You will see:

   ```
   igel:
       client-cert-forwarding:
           enabled: false
           client-cert-forwarded-header: X-SSL-CERT
   ```

2. Activate `client-cert-forwarding` by setting "`enabled`" to "`true`":

```
client-cert-forwarding:
    enabled: true
```

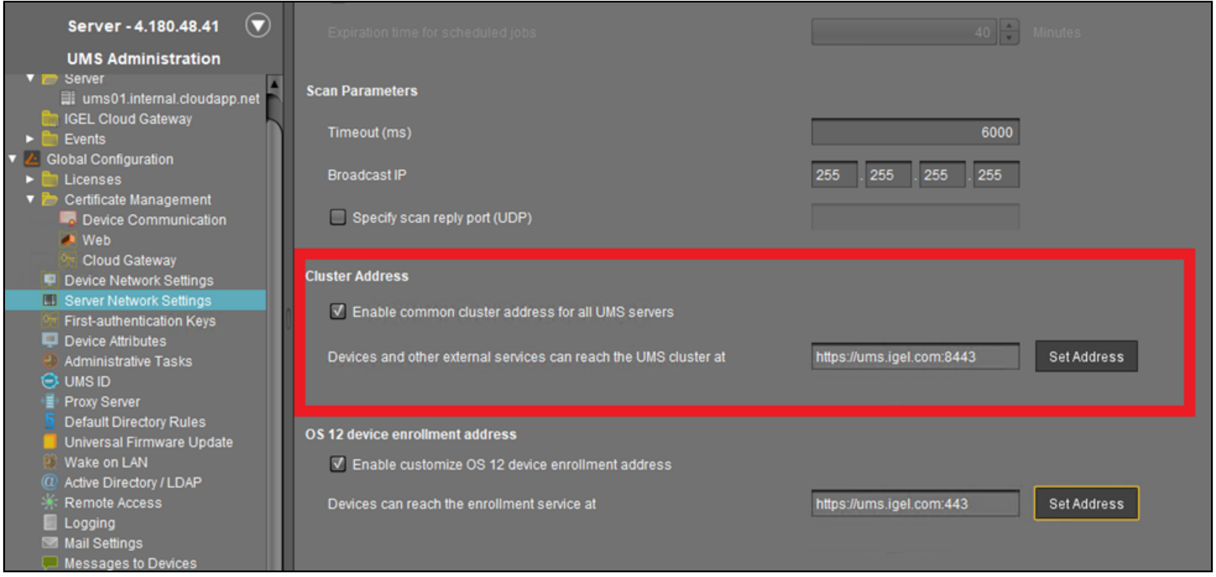
3. If required, the forwarding header can be configured. The `X -SSL-CERT` header value can be changed but be aware to change the corresponding value in the Application Gateway configuration.

4. Save the configuration changes and restart the ICG server.

Modify Server Network Settings

1. Go to **UMS Administration > Global Configuration > Server Network Settings**.

2. Set the **Cluster Address**.
   If you are using a Reverse Proxy, you will need to update the FQDN of the UMS cluster as external address. This value must be set to the FQDN and Port of the Reverse Proxy.



Expiration time for scheduled jobs: 40 Minutes

Scan Parameters

Timeout (ms): 6000

Broadcast IP: 255 . 255 . 255 . 255

□ Specify scan reply port (UDP)

Cluster Address

☑ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at: https://ums.igel.com:8443

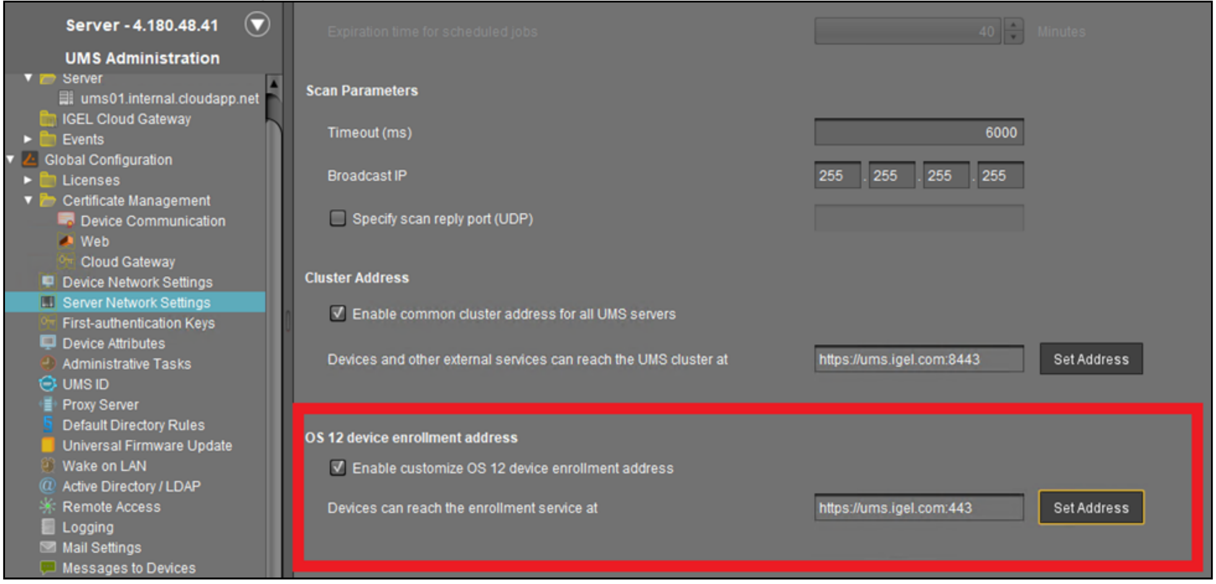
OS 12 device enrollment address

☑ Enable customize OS 12 device enrollment address

Devices can reach the enrollment service at: https://ums.igel.com:443

3. Set the **OS 12 device enrollment address** (this is the onboarding address)**.**
   This configuration must be set for Reverse Proxy without optional Client Certificate verification option like Azure Application Gateway. Set it to the FQDN / IP and Port of the configured listener

for Device onboarding.



Expiration time for scheduled jobs 40 Minutes

Scan Parameters

Timeout (ms) 6000

Broadcast IP 255 . 255 . 255 . 255

☐ Specify scan reply port (UDP)

Cluster Address

☑ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https://ums.igel.com:8443

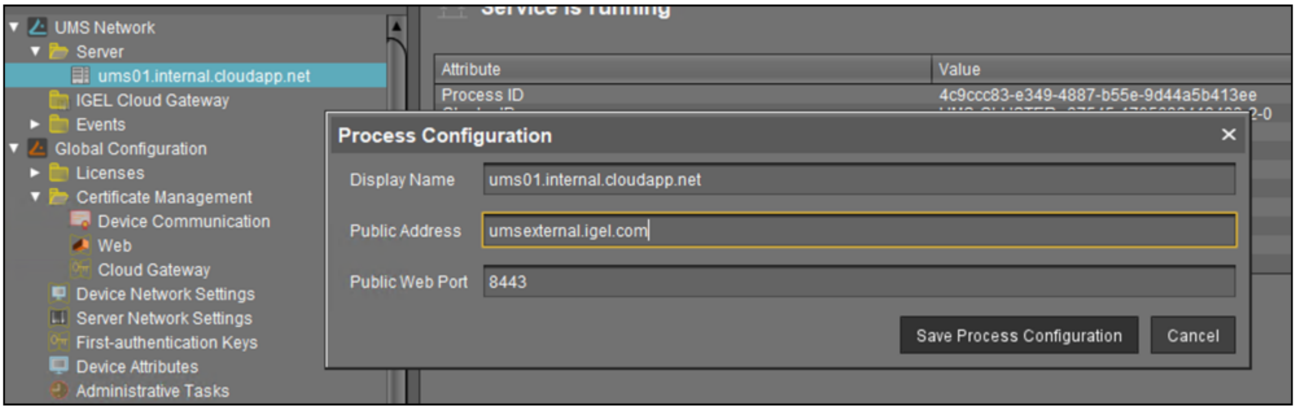
OS 12 device enrollment address

☑ Enable customize OS 12 device enrollment address

Devices can reach the enrollment service at https://ums.igel.com:443

Set Public Address and Port of the UMS Process Configuration

In case the public address of the UMS differs from the UMS address, the public address and port must be set. This option can be set under **UMS Administration > UMS Network > Server**. This is essential for device shadowing.



Attribute	Value
Process ID	4c9ccc83-e349-4887-b55e-9d44a5b413ee

Process Configuration

Display Name: ums01.internal.cloudapp.net

Public Address: umsexternal.igel.com

Public Web Port: 8443

Export Certificates for Azure Application Gateway Configuration

If no ICG is used behind an Azure Application Gateway, the following certificates have to be exported:

- UMS Web certificate chain
- UMS Web Root Certificate
- EST CA Client Certificate

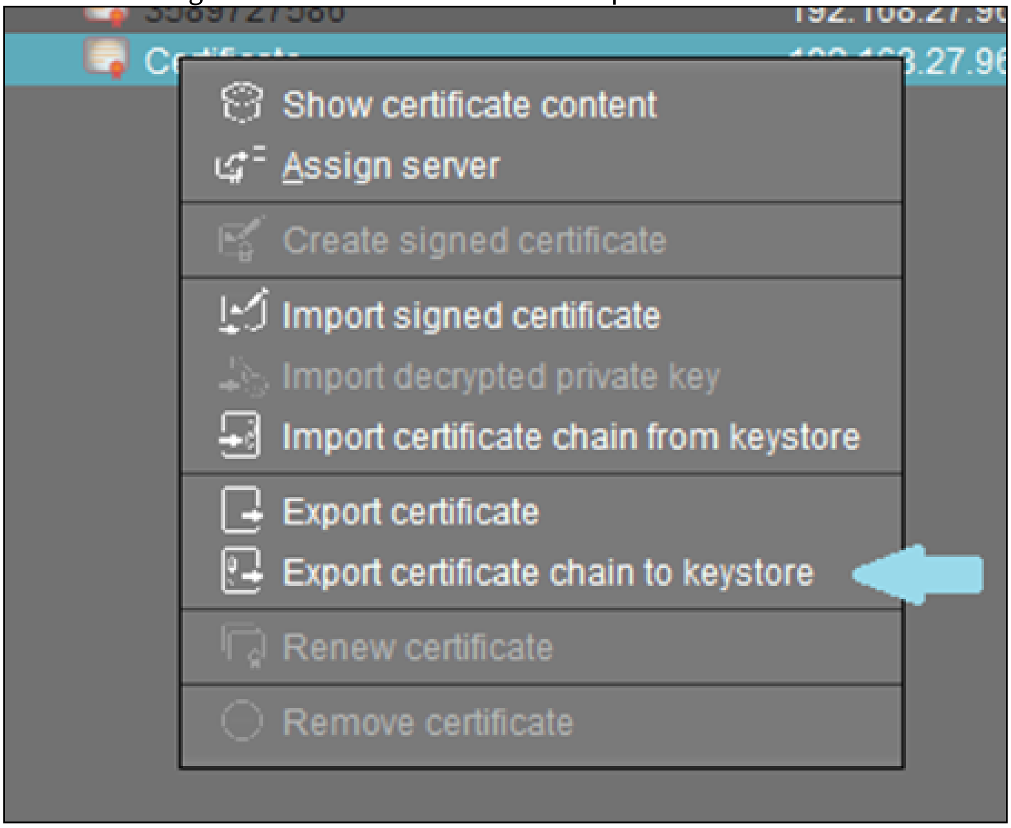
In case an ICG is used behind an Azure Application Gateway, the following certificates have to be exported:

- Cloud Gateway certificate chain
- Cloud Gateway Root Certificate for Backend Trust
- EST CA Client Certificate

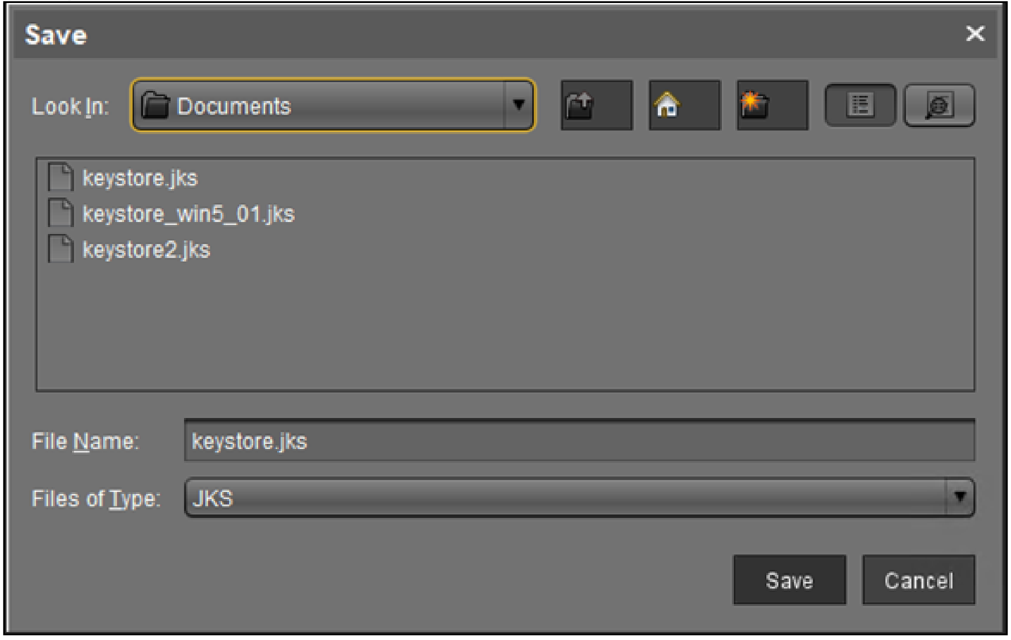
Export UMS Web Certificate Chain Used for Azure Application Gateway Listener

This certificate must be exported for use in the Listener configuration.

1. Select the configured Azure Web certificate and export the certificate chain.


Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from keystore
Export certificate
Export certificate chain to keystore
Renew certificate
Remove certificate

2. Set a password and the filename.



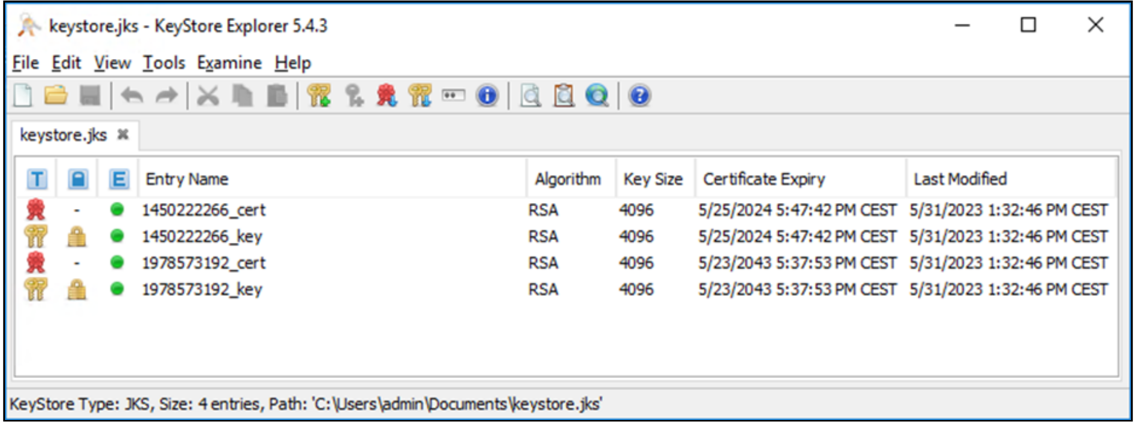
Look In: Documents

keystore.jks
keystore_win5_01.jks
keystore2.jks

File Name: keystore.jks

Files of Type: JKS

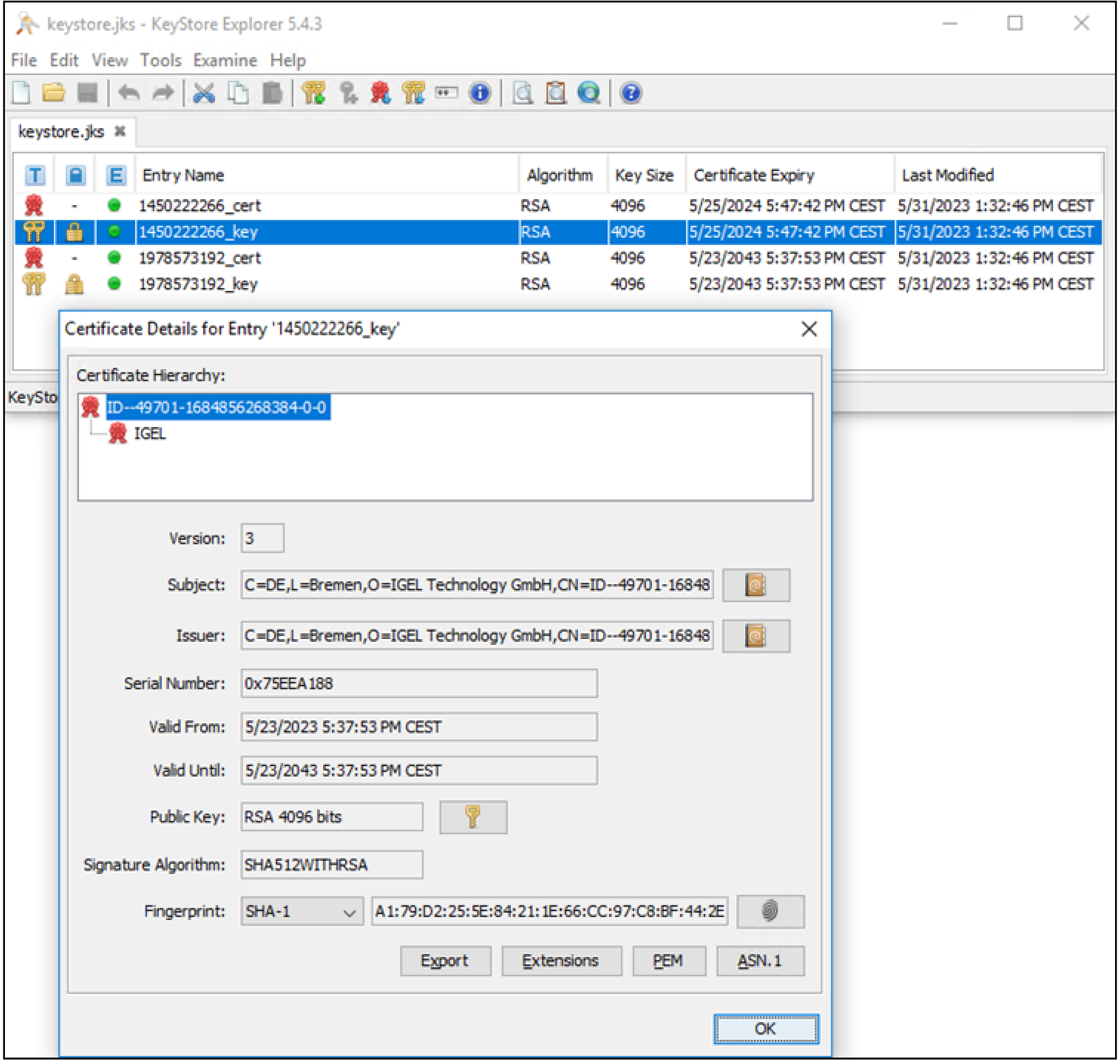
3. Identify the Web key.
   The exported keystore file contains several keys and certificates, at least the root and the currently used keys and certificates. A tool like Keystore Explorer can be used to identify the currently used Web key.
   Click for an example based on Keystore Explorer....
   a. Open the file and enter the password given for the export. Several entries are shown:


keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
🎖	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
🔑	🔒	●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
🎖	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
🔑	🔒	●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

KeyStore Type: JKS, Size: 4 entries, Path: 'C:\Users\admin\Documents\keystore.jks'

b. Find the currently used Web key:


keystore.jks - KeyStore Explorer 5.4.3
File Edit View Tools Examine Help
keystore.jks
KeySto
Export
Extensions
PEM
ASN.1
OK

T	🔒	E	Entry Name	Algorithm	Key Size	Certificate Expiry	Last Modified
	-	●	1450222266_cert	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	🔒	●	1450222266_key	RSA	4096	5/25/2024 5:47:42 PM CEST	5/31/2023 1:32:46 PM CEST
	-	●	1978573192_cert	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST
	🔒	●	1978573192_key	RSA	4096	5/23/2043 5:37:53 PM CEST	5/31/2023 1:32:46 PM CEST

Certificate Details for Entry '1450222266_key'

Certificate Hierarchy:

ID--49701-1684856268384-0-0
IGEL

Version: 3

Subject: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Issuer: C=DE,L=Bremen,O=IGEL Technology GmbH,CN=ID--49701-16848

Serial Number: 0x75EEA188

Valid From: 5/23/2023 5:37:53 PM CEST

Valid Until: 5/23/2043 5:37:53 PM CEST

Public Key: RSA 4096 bits

Signature Algorithm: SHA512WITHRSA

Fingerprint: SHA-1 A1:79:D2:25:5E:84:21:1E:66:CC:97:C8:BF:44:2E

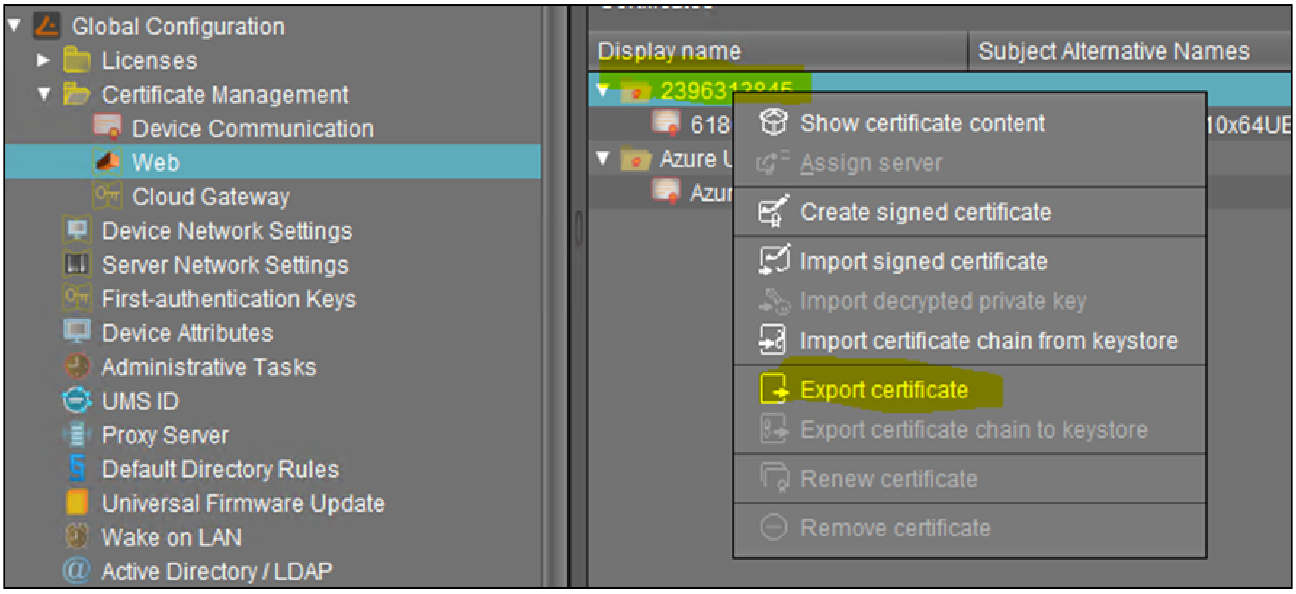
4. Parse the exported keystore file to the `PFX` format.

   Azure Application Gateway requires the key for the listener configuration in a `PFX` formatted file. The exported keystore file must be converted into this file format. The java keytool command can be used. The command line tool can be found in the UMS installation: `(Install Dir)/IGEL/RemoteManager/_jvm/bin`.
   The **key alias** must be added to the call of command.

```
keytool -v -importkeystore -srckeystore  yourkeystore.keystore -srcalias mykey
-destkeystore myp12file.pfx -deststoretype PKCS1
```

Export UMS Web Root Certificate

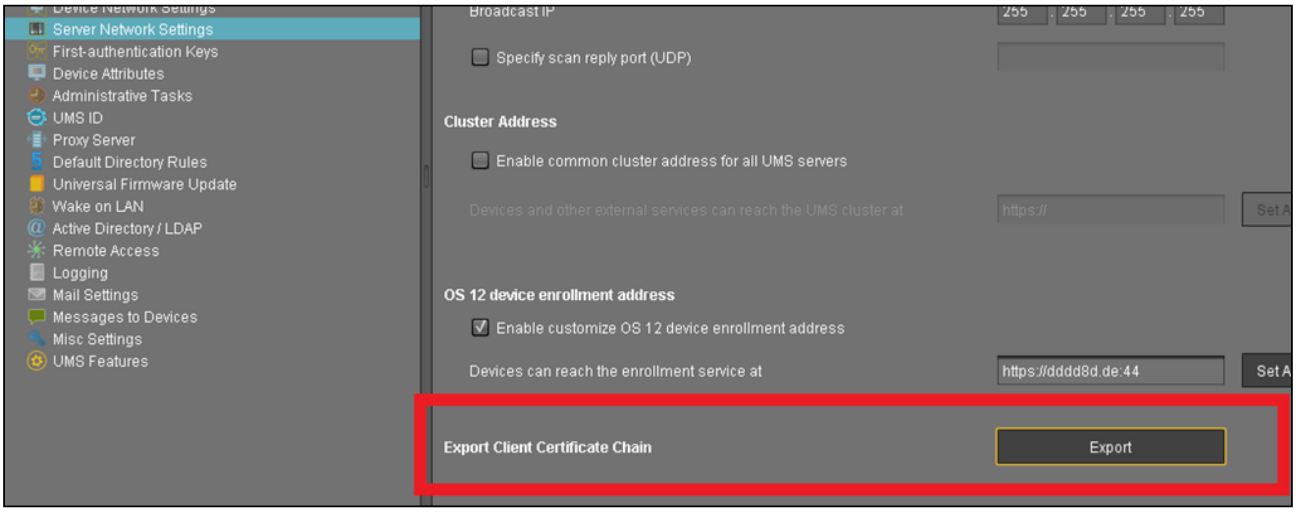
The UMS Web Root Certificate is used for the Backend Settings configuration in Azure. The root certificate of the used Web Certificate must be exported.



Export EST CA Client Certificate Chain

The EST CA Client Certificate is required for the Client Certificate check.

The Client Certificate Chain export can be found under: **UMS Administration > Server Network Settings > Export Client Certificate Chain**.



Broadcast IP 255 . 255 . 255 . 255

□ Specify scan reply port (UDP)

Cluster Address

□ Enable common cluster address for all UMS servers

Devices and other external services can reach the UMS cluster at https:// Set A

OS 12 device enrollment address

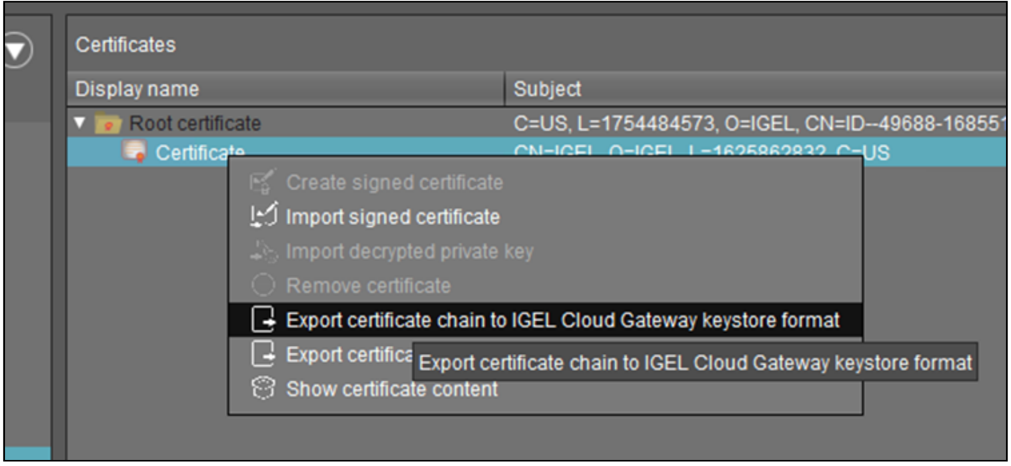
☑ Enable customize OS 12 device enrollment address

Devices can reach the enrollment service at https://dddd8d.de:44 Set A

Export Client Certificate Chain Export

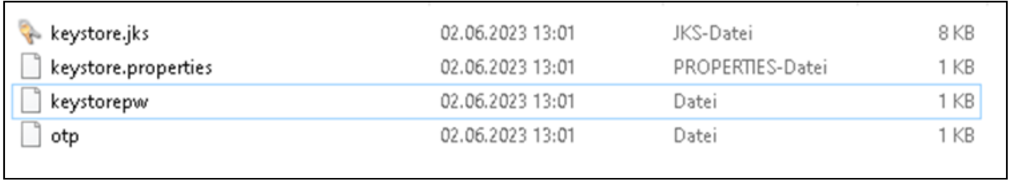
Export Cloud Gateway Certificate Chain Used for Azure Application Gateway Listener

1. If the Azure Application Gateway certificate was added as a Cloud Gateway certificate, export the certificate to IGEL Cloud Gateway keystore format.


Certificates
Display name
Subject
Root certificate
C=US, L=1754484573, O=IGEL, CN=ID--49688-16855
Certificate
CN=IGEL, O=IGEL, L=1625862832, C=US
Create signed certificate
Import signed certificate
Import decrypted private key
Remove certificate
Export certificate chain to IGEL Cloud Gateway keystore format
Export certifica
Export certificate chain to IGEL Cloud Gateway keystore format
Show certificate content

2. Unzip the file.

3. Open the keystore.jks file and use the password from the keystorepwd file.



keystore.jks	02.06.2023 13:01	JKS-Datei	8 KB
keystore.properties	02.06.2023 13:01	PROPERTIES-Datei	1 KB
keystorepw	02.06.2023 13:01	Datei	1 KB
otp	02.06.2023 13:01	Datei	1 KB

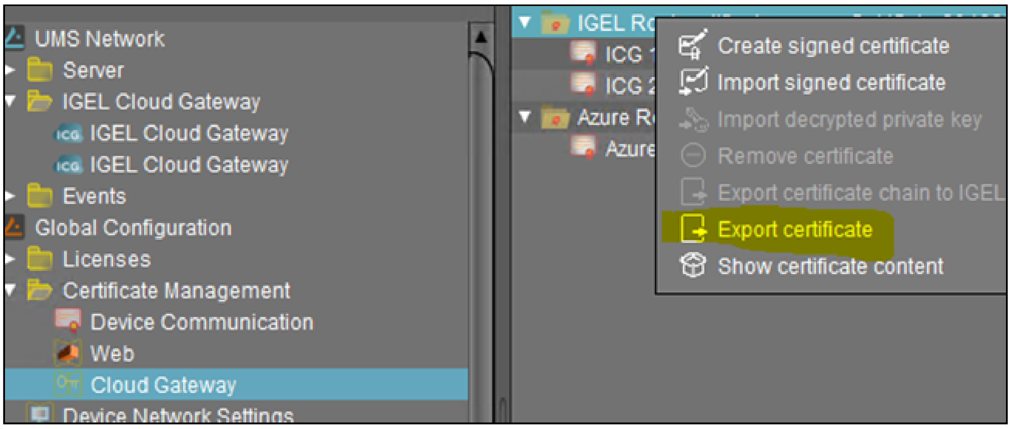
4. Identify the used key entry.

5. The Azure Application Gateway requires the key for SSL offloading in a `PFX` file. The exported keystore file can be converted into this file format:

```
keytool -v -importkeystore -srckeystore  yourkeystore.keystore -srcalias mykey
-destkeystore myp12file.pfx -deststoretype PKCS12
```

Export Cloud Gateway Root Certificate for Backend Trust

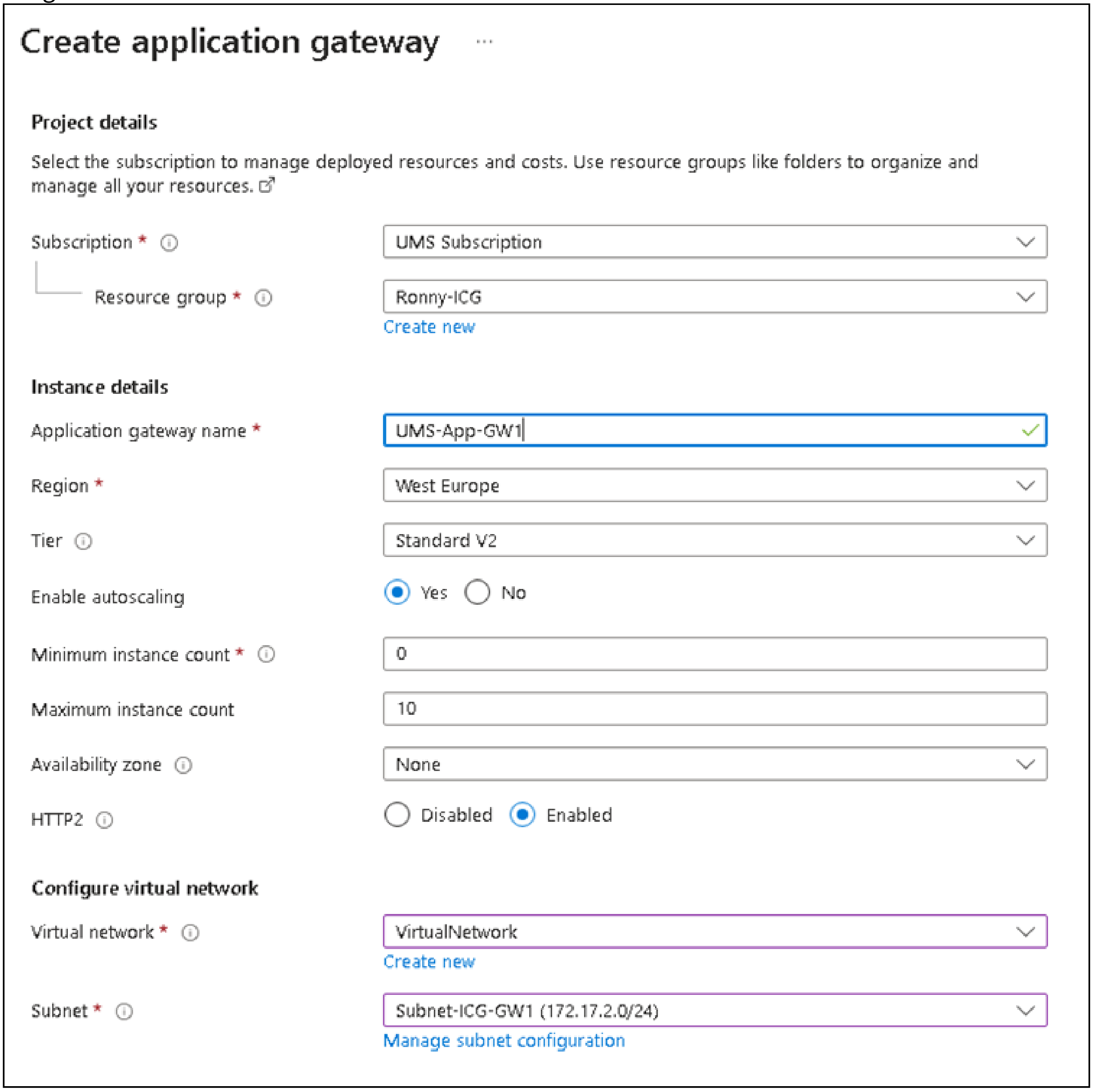
You can export the Cloud Gateway Root certificate via the GUI.


UMS Network
Server
IGEL Cloud Gateway
IGEL Cloud Gateway
IGEL Cloud Gateway
Events
Global Configuration
Licenses
Certificate Management
Device Communication
Web
Cloud Gateway
Device Network Settings
IGEL Ro
ICG 1
ICG 2
Azure R
Azure
Create signed certificate
Import signed certificate
Import decrypted private key
Remove certificate
Export certificate chain to IGEL
Export certificate
Show certificate content

Azure Application Gateway Configuration for the UMS

Create Azure Application Gateway

1. Assign correct **Virtual network** and **Subnet**.



Create application gateway ···

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : UMS Subscription

Resource group * : Ronny-ICG

Create new

Instance details

Application gateway name * : UMS-App-GW1

Region * : West Europe

Tier : Standard V2

Enable autoscaling : ● Yes ○ No

Minimum instance count * : 0

Maximum instance count : 10

Availability zone : None

HTTP2 : ○ Disabled ● Enabled

Configure virtual network

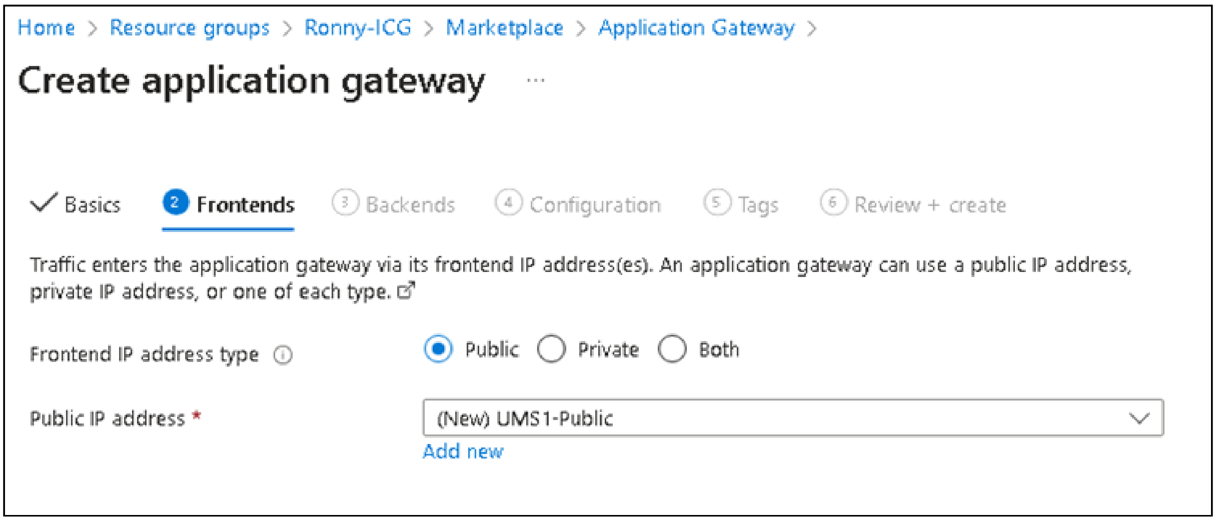
Virtual network * : VirtualNetwork

Create new

Subnet * : Subnet-ICG-GW1 (172.17.2.0/24)

Manage subnet configuration

2. Provide Frontend IP address.

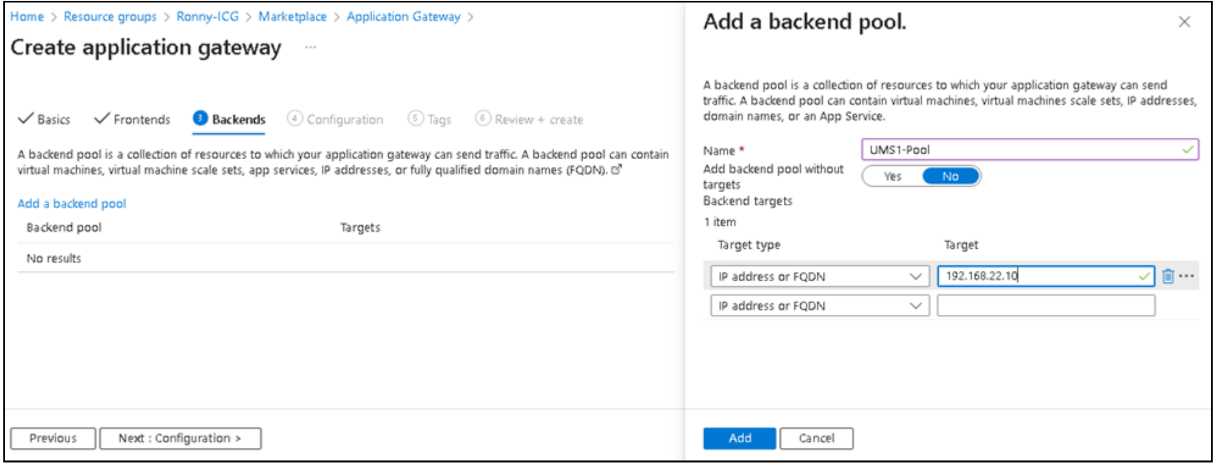

Home > Resource groups > Ronny-ICG > Marketplace > Application Gateway >
Create application gateway ...
✓ Basics
2 Frontends
3 Backends
4 Configuration
5 Tags
6 Review + create
Add new

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type: ● Public ○ Private ○ Both

Public IP address *: (New) UMS1-Public

3. Add backend pool with UMS address. Add the UMS / ICG FQDN or IP.



A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN).

Backend pool	Targets
No results	

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name *: UMS1-Pool

Add backend pool without targets: Yes [✓ No]

Backend targets

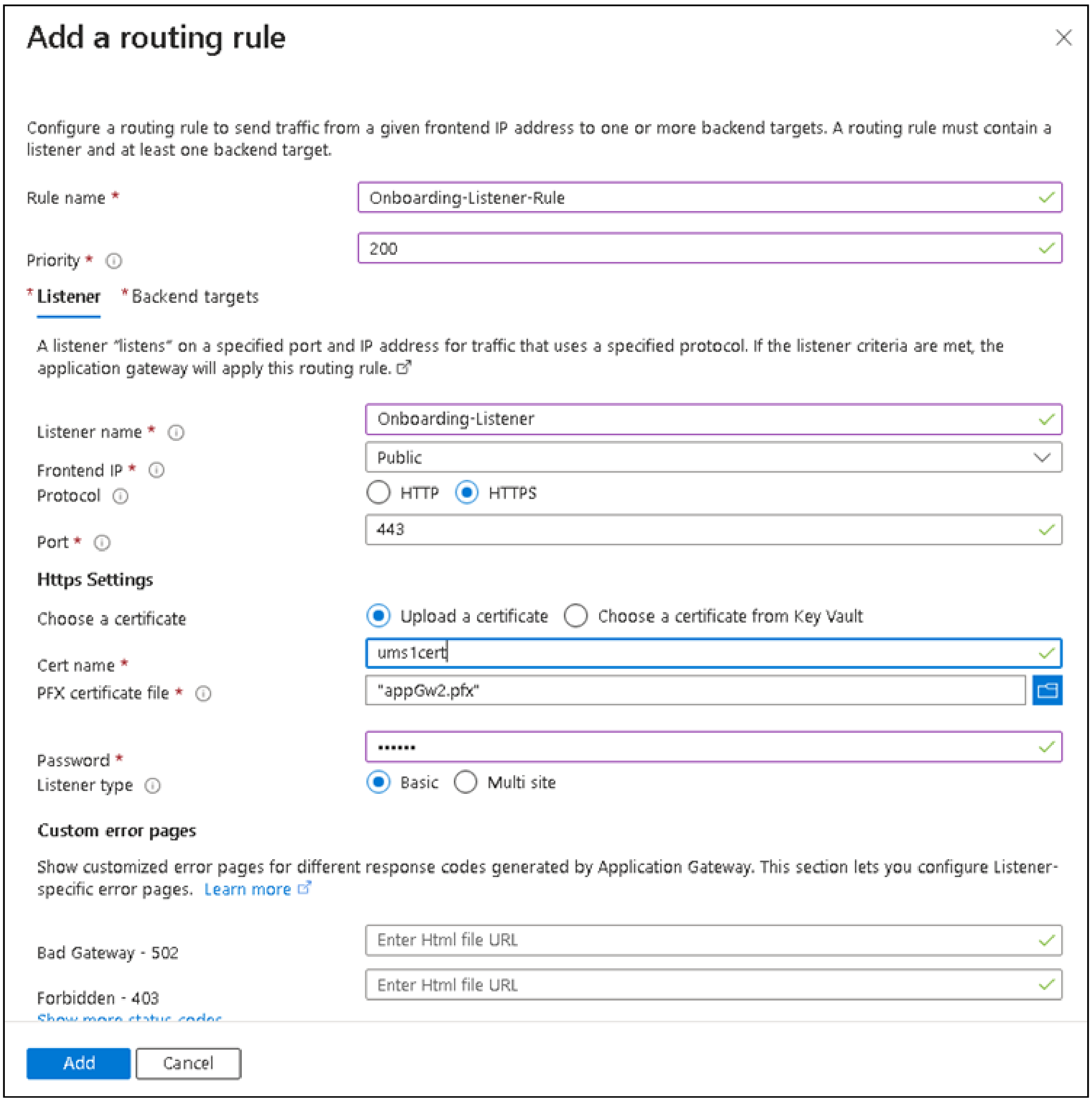
1 item

Target type	Target
IP address or FQDN	192.168.22.10
IP address or FQDN	

Add a Routing Rule for Onboarding Connection

1. Configure a listener:
    - Set the **Protocol** to **HTTPS**.
    - Set the **Public** IP address.

- The recommended **Port** value is **443**.



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name *	Onboarding-Listener-Rule ✓
Priority *	200 ✓

* Listener * Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name *	Onboarding-Listener ✓
Frontend IP *	Public
Protocol	○ HTTP ● HTTPS
Port *	443 ✓

Https Settings

Choose a certificate	● Upload a certificate ○ Choose a certificate from Key Vault
Cert name *	ums1cert ✓
PFX certificate file *	"appGw2.pfx"
Password *	•••••• ✓
Listener type	● Basic ○ Multi site

Custom error pages

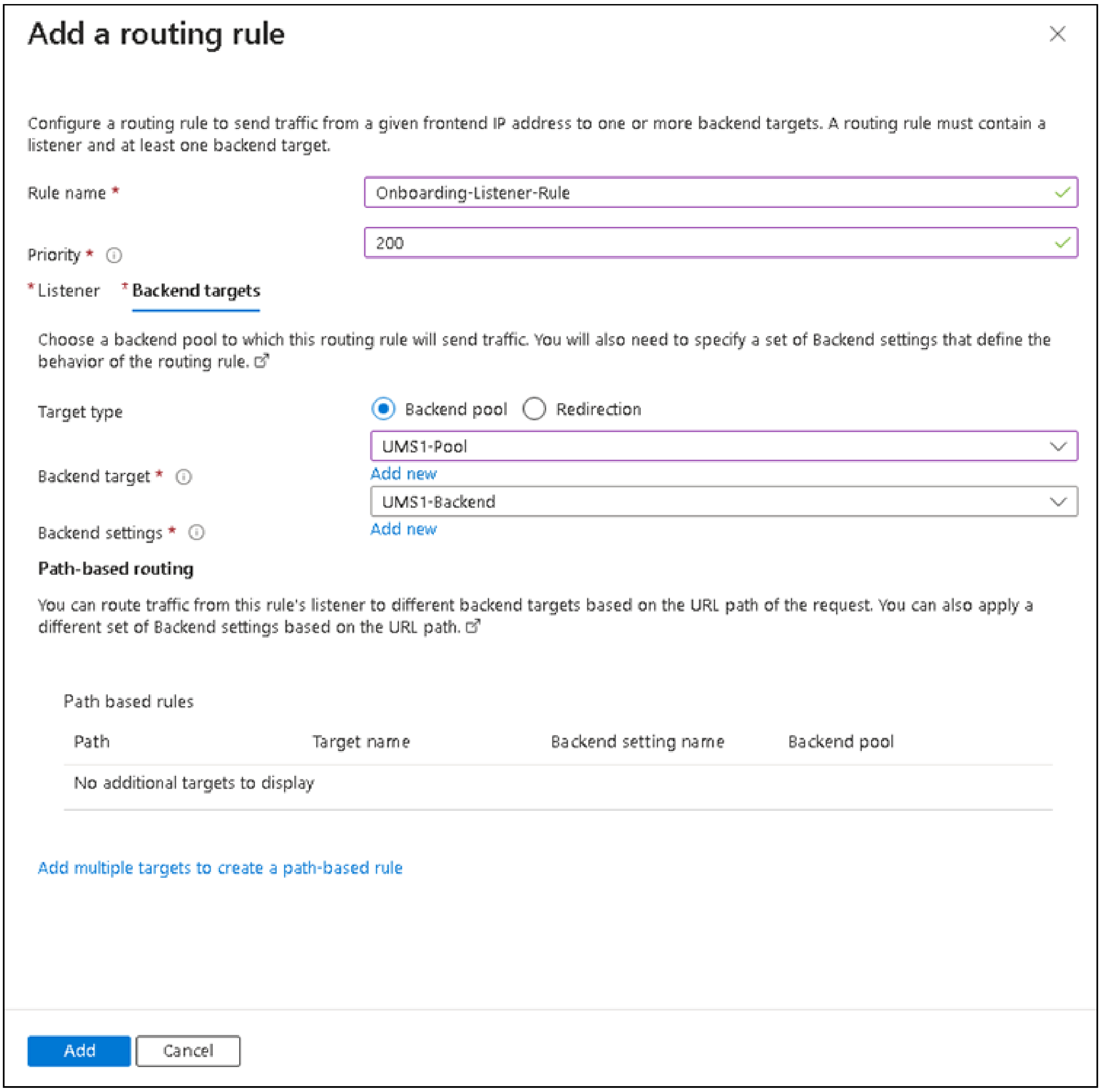
Show customized error pages for different response codes generated by Application Gateway. This section lets you configure Listener-specific error pages. Learn more

Bad Gateway - 502	Enter Html file URL ✓
Forbidden - 403	Enter Html file URL ✓

Show more status codes

2. Select the `PFX` file created in Export Cloud Gateway Certificate Chain Used for Azure Application Gateway Listener (see page 76) or Export the UMS Web Certificate Chain Used for Azure Application Gateway Listener (see page 72), and enter the appropriate password.

3. Configure **Backend targets**. The already inserted Backend pool can now be selected and the Backend settings must be added.



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * Onboarding-Listener-Rule

Priority * 200

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of Backend settings that define the behavior of the routing rule.

Target type ● Backend pool ○ Redirection

Backend target * UMS1-Pool

Backend settings * UMS1-Backend

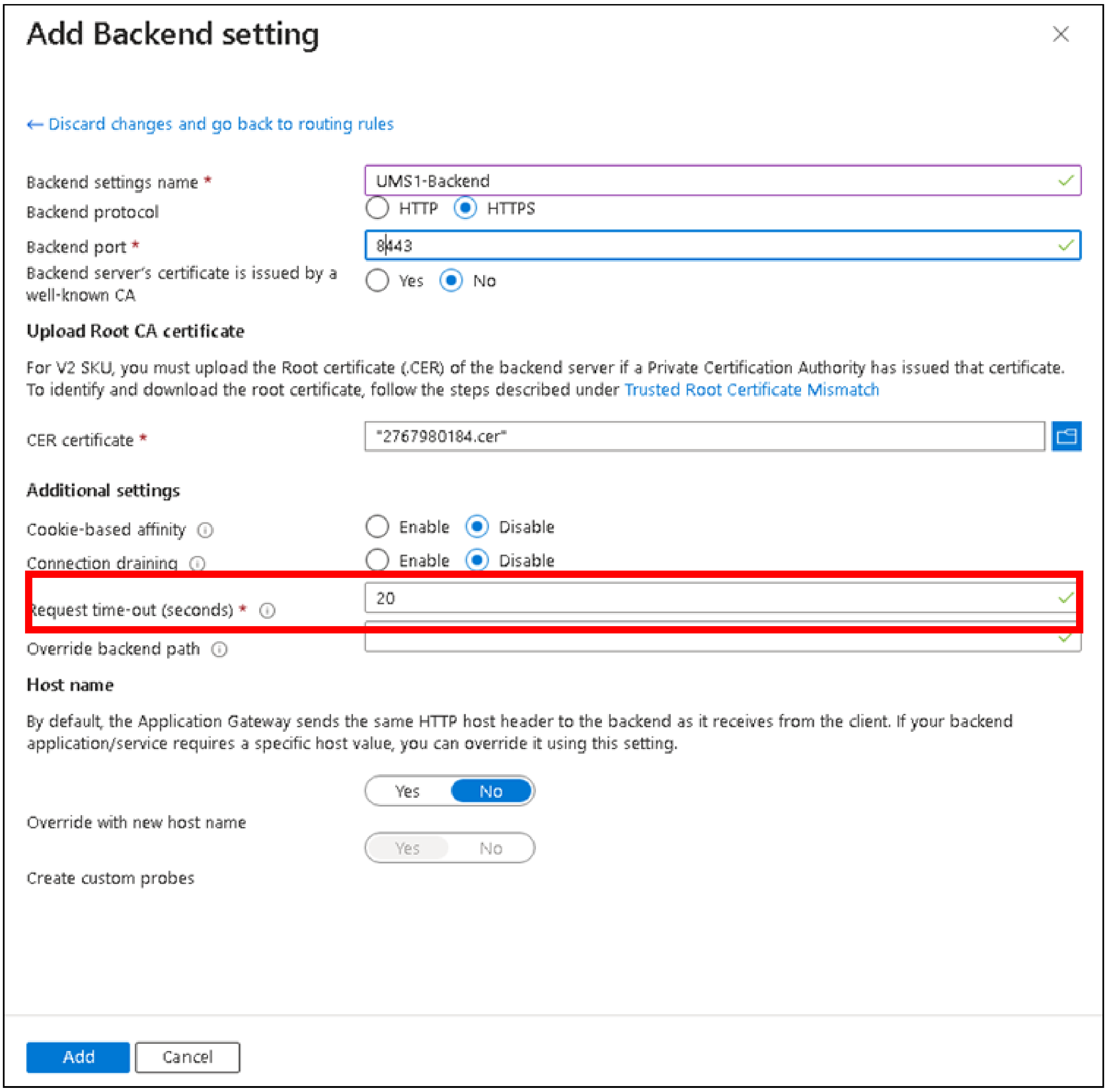
Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of Backend settings based on the URL path.

Path based rules

Path	Target name	Backend setting name	Backend pool
No additional targets to display			

4. Under **Add Backend settings**, set the **Backend protocol** to **HTTPS** and add the **UMS Web Port** as **Backend port**.



Add Backend setting

← Discard changes and go back to routing rules

Backend settings name * UMS1-Backend

Backend protocol ○ HTTP ● HTTPS

Backend port * 8443

Backend server's certificate is issued by a well-known CA ○ Yes ● No

Upload Root CA certificate

For V2 SKU, you must upload the Root certificate (.CER) of the backend server if a Private Certification Authority has issued that certificate. To identify and download the root certificate, follow the steps described under Trusted Root Certificate Mismatch

CER certificate * "2767980184.cer"

Additional settings

Cookie-based affinity ○ Enable ● Disable

Connection draining ○ Enable ● Disable

Request time-out (seconds) * 20

Override backend path

Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

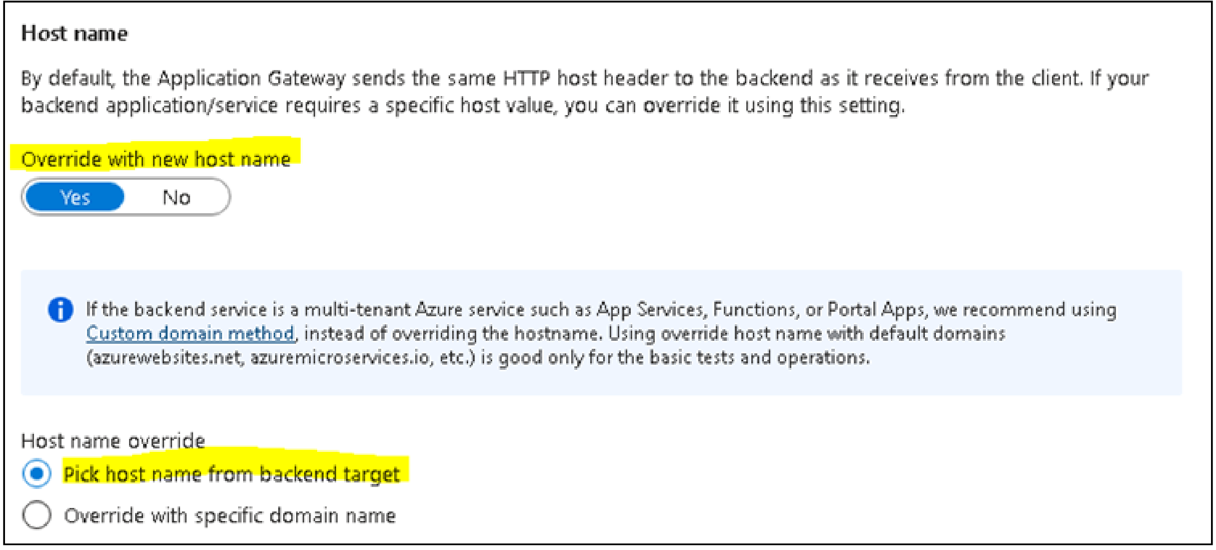
Override with new host name Yes [✓ No]

Create custom probes Yes No

5. Select the UMS Web Root Certificate exported in Export UMS Web Root Certificate (see page 75) or Export Cloud Gateway Root Certificate for Backend Trust (see page 76).

6. Set the value for **Request time-out (seconds)** to a value at least **130** seconds.

7. Verify that the **Override with new host name** is activated and set **Host name override**.



Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

Override with new host name

● Yes ○ No

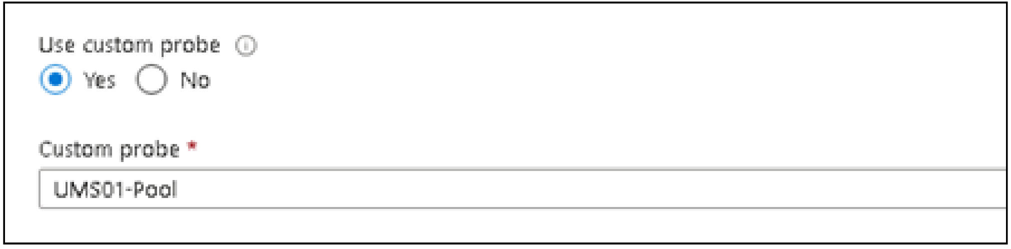
If the backend service is a multi-tenant Azure service such as App Services, Functions, or Portal Apps, we recommend using Custom domain method, instead of overriding the hostname. Using override host name with default domains (azurewebsites.net, azuremicroservices.io, etc.) is good only for the basic tests and operations.

Host name override

● Pick host name from backend target

○ Override with specific domain name

8. Set a **Custom probe**.



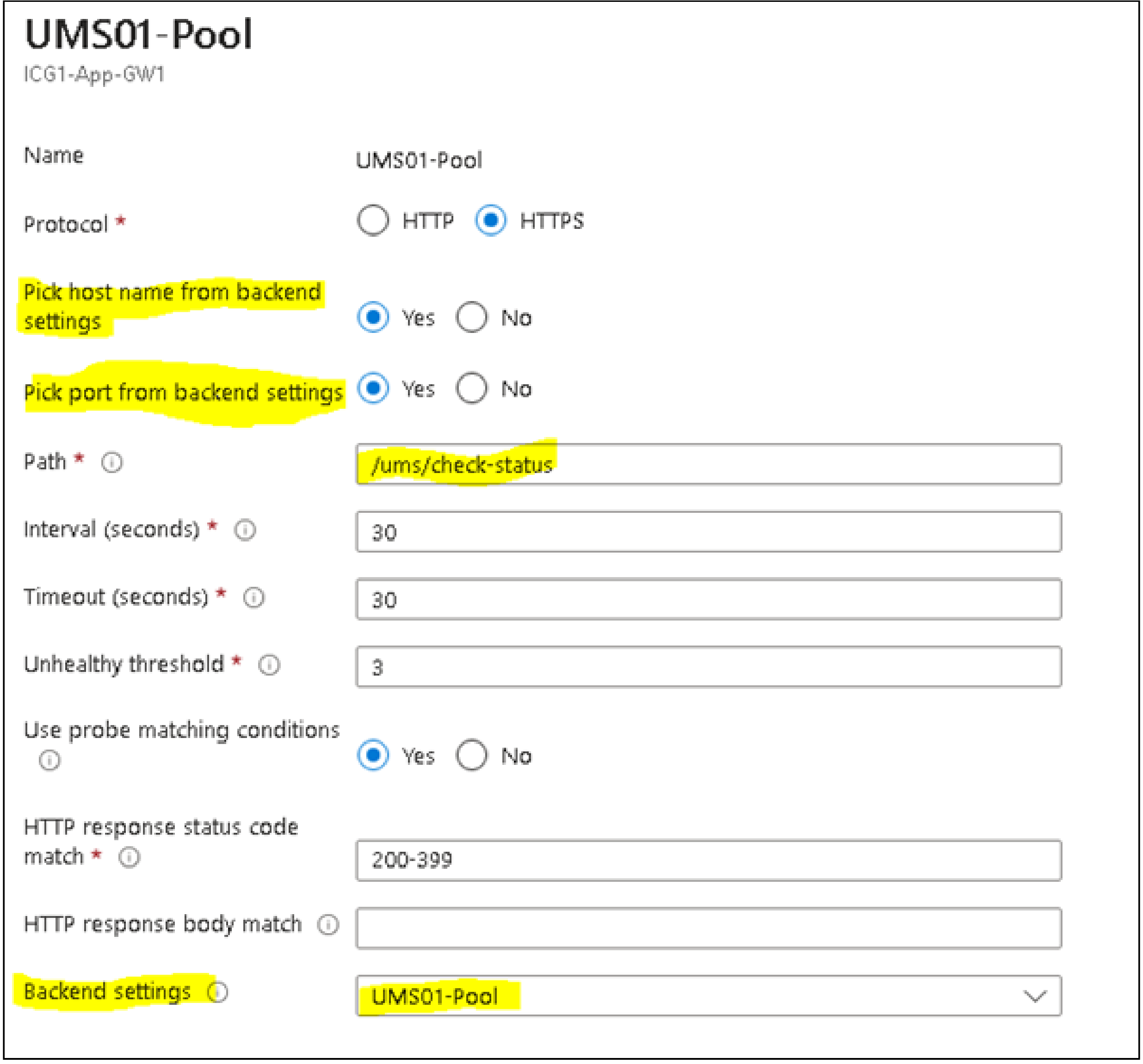
Use custom probe

● Yes ○ No

Custom probe *

UMS01-Pool

Custom Probe Settings:



UMS01-Pool

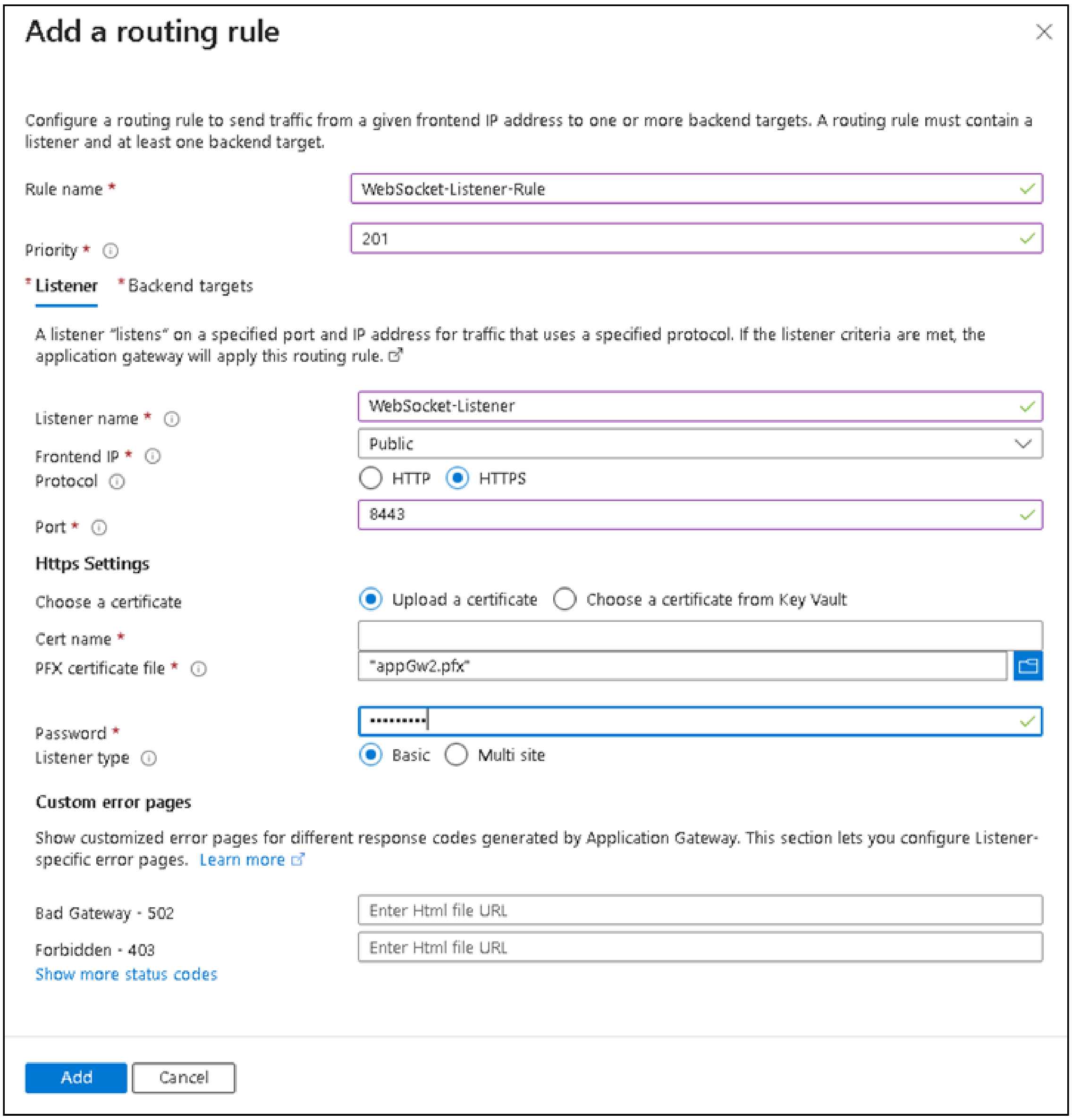
ICG1-App-GW1

Name	UMS01-Pool
Protocol *	○ HTTP ● HTTPS
Pick host name from backend settings	● Yes ○ No
Pick port from backend settings	● Yes ○ No
Path *	/ums/check-status
Interval (seconds) *	30
Timeout (seconds) *	30
Unhealthy threshold *	3
Use probe matching conditions	● Yes ○ No
HTTP response status code match *	200-399
HTTP response body match	
Backend settings	UMS01-Pool

Add a Routing Rule for the Websocket Connection

1. Configure a listener:
   - Set the **Protocol** to **HTTPS**.
   - Set the **Public** IP address.

- The recommended **Port** value is **8443**.



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name *: WebSocket-Listener-Rule

Priority *: 201

*Listener *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name *: WebSocket-Listener

Frontend IP *: Public

Protocol: ○ HTTP ● HTTPS

Port *: 8443

Https Settings

Choose a certificate: ● Upload a certificate ○ Choose a certificate from Key Vault

Cert name *:

PFX certificate file *: "appGw2.pfx"

Password *: •••••••••

Listener type: ● Basic ○ Multi site

Custom error pages

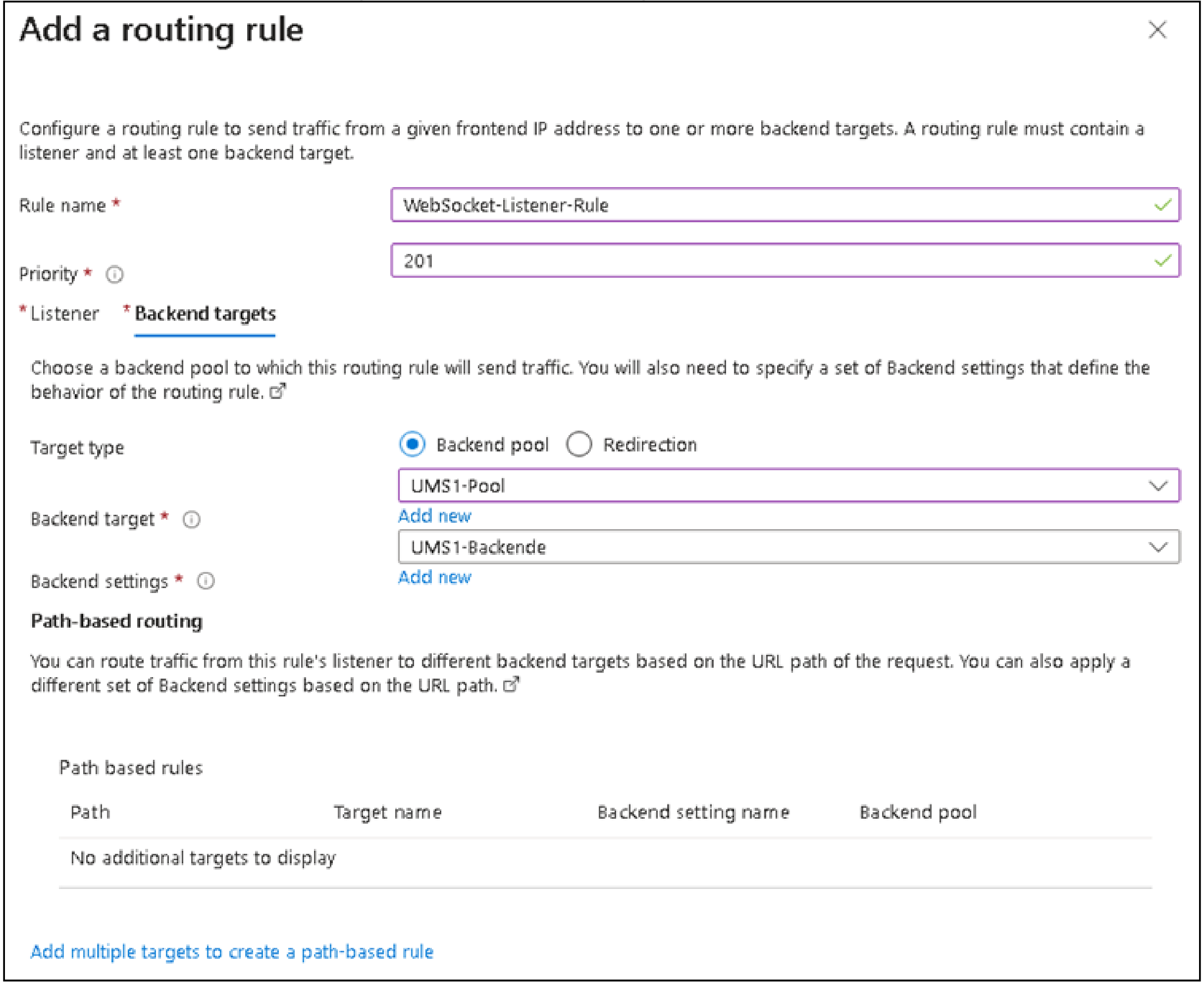
Show customized error pages for different response codes generated by Application Gateway. This section lets you configure Listener-specific error pages. Learn more

Bad Gateway - 502: Enter Html file URL

Forbidden - 403: Enter Html file URL

2. Select the `PFX` file created in Export Cloud Gateway Certificate Chain Used for Azure Application Gateway Listener (see page 76) or Export the UMS Web Certificate Chain Used for Azure Application Gateway Listener (see page 72), and enter the appropriate password.

3. Add the same Backend Settings as for the Onboarding connection.



Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * WebSocket-Listener-Rule

Priority * 201

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of Backend settings that define the behavior of the routing rule.

Target type ● Backend pool ○ Redirection

Backend target * UMS1-Pool

Backend settings * UMS1-Backende

Path-based routing

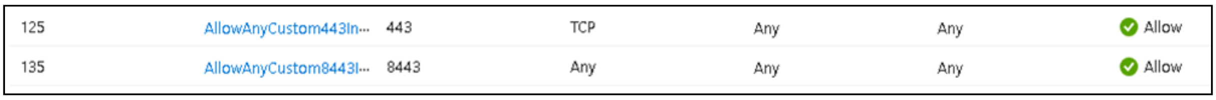
You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of Backend settings based on the URL path.

Path based rules

Path	Target name	Backend setting name	Backend pool
No additional targets to display			

Check Network Security Group

1. Open the Network Security Group used for the Gateway Network and verify if the used Ports are listed



125	AllowAnyCustom443In...	443	TCP	Any	Any	✓ Allow
135	AllowAnyCustom8443I...	8443	Any	Any	Any	✓ Allow

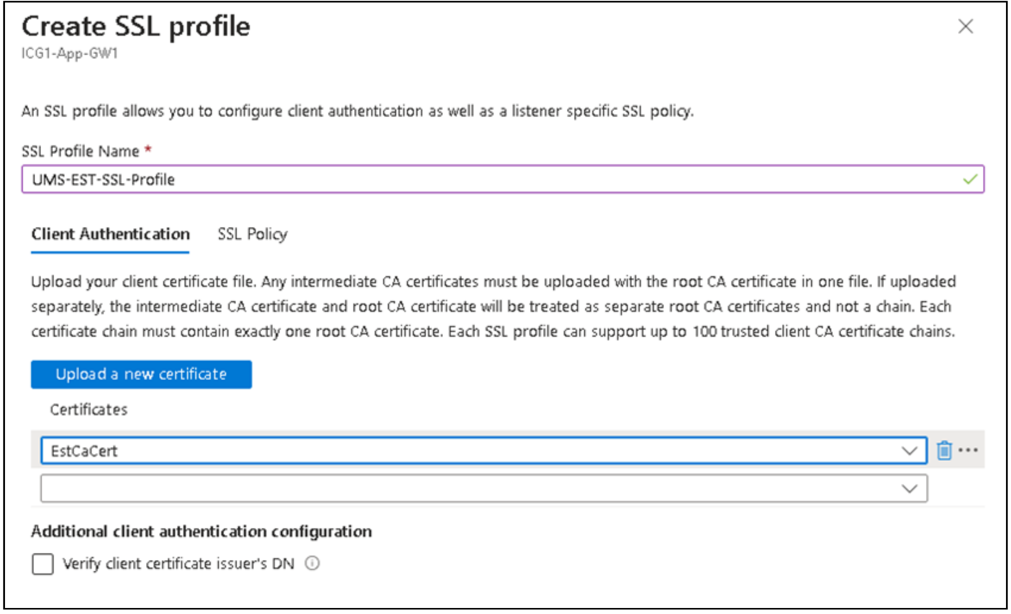
2. If they are not listed, add them.

Set Mutual Authentication for WebSocket Connection

The mutual authentication can be set in Azure Application Gateway with SSL Profiles:

1. Add an SSL Profile under SSL settings.

2. In the **Client Authentication** part of the Dialog the EST CA Certificate is required, that was exported in Export EST CA Client Certificate Chain (see page 75).



Create SSL profile

ICG1-App-GW1

An SSL profile allows you to configure client authentication as well as a listener specific SSL policy.

SSL Profile Name *

UMS-EST-SSL-Profile

Client Authentication | SSL Policy

Upload your client certificate file. Any intermediate CA certificates must be uploaded with the root CA certificate in one file. If uploaded separately, the intermediate CA certificate and root CA certificate will be treated as separate root CA certificates and not a chain. Each certificate chain must contain exactly one root CA certificate. Each SSL profile can support up to 100 trusted client CA certificate chains.

Upload a new certificate

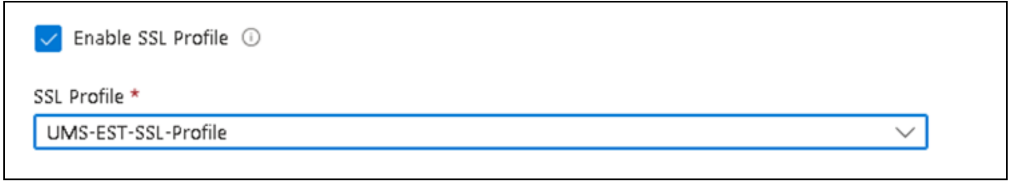
Certificates

EstCaCert

Additional client authentication configuration

□ Verify client certificate issuer's DN

3. Add the SSL profile to the WebSocket listener. **Not to the Onboarding listener!**



☑ Enable SSL Profile

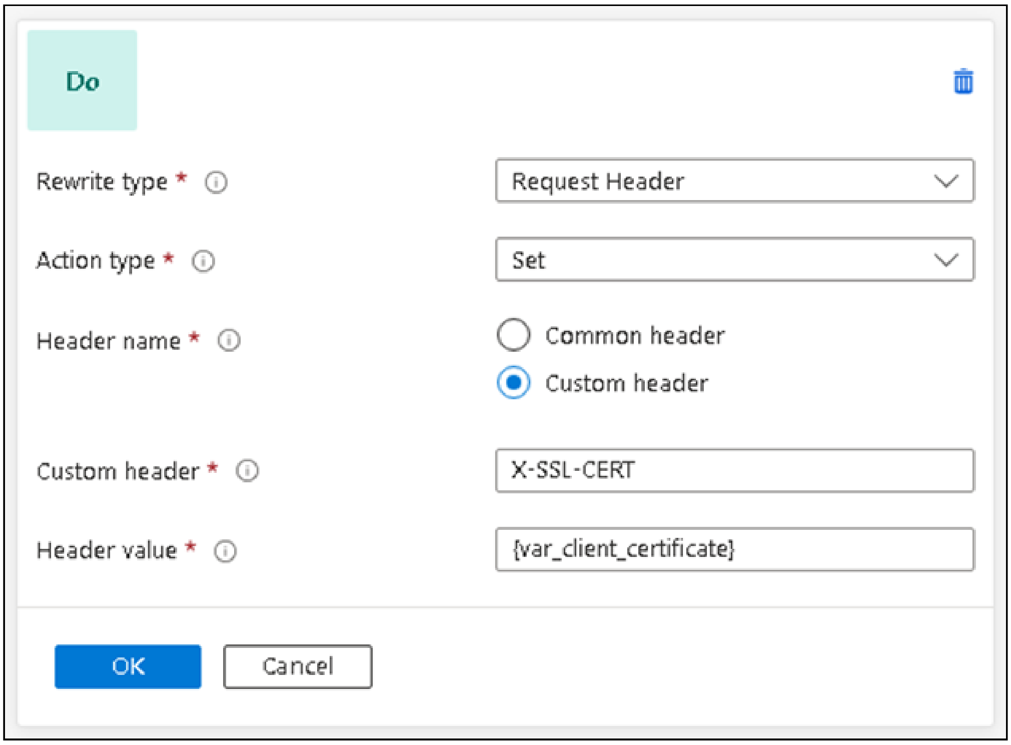
SSL Profile *

UMS-EST-SSL-Profile

Add a Rewrite for Client Certificate Forwarding

The client certificate must be forwarded to the UMS. The Application Gateway can be configured to forward it by a rewrite definition.

1. Create a rewrite set and assign it to the appropriate rule.
2. Add the following rewrite rule:



Do

Rewrite type * : Request Header

Action type * : Set

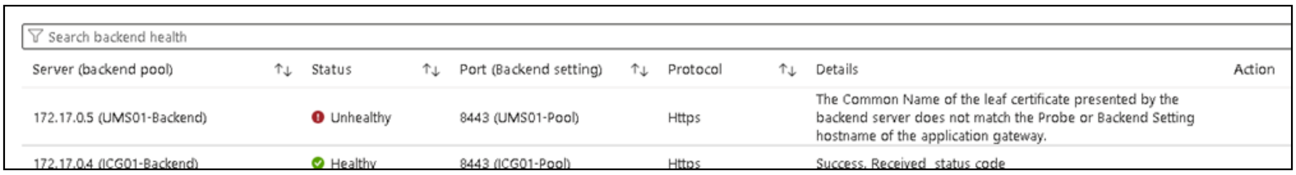
Header name * : ○ Common header ● Custom header

Custom header * : X-SSL-CERT

Header value * : {var_client_certificate}

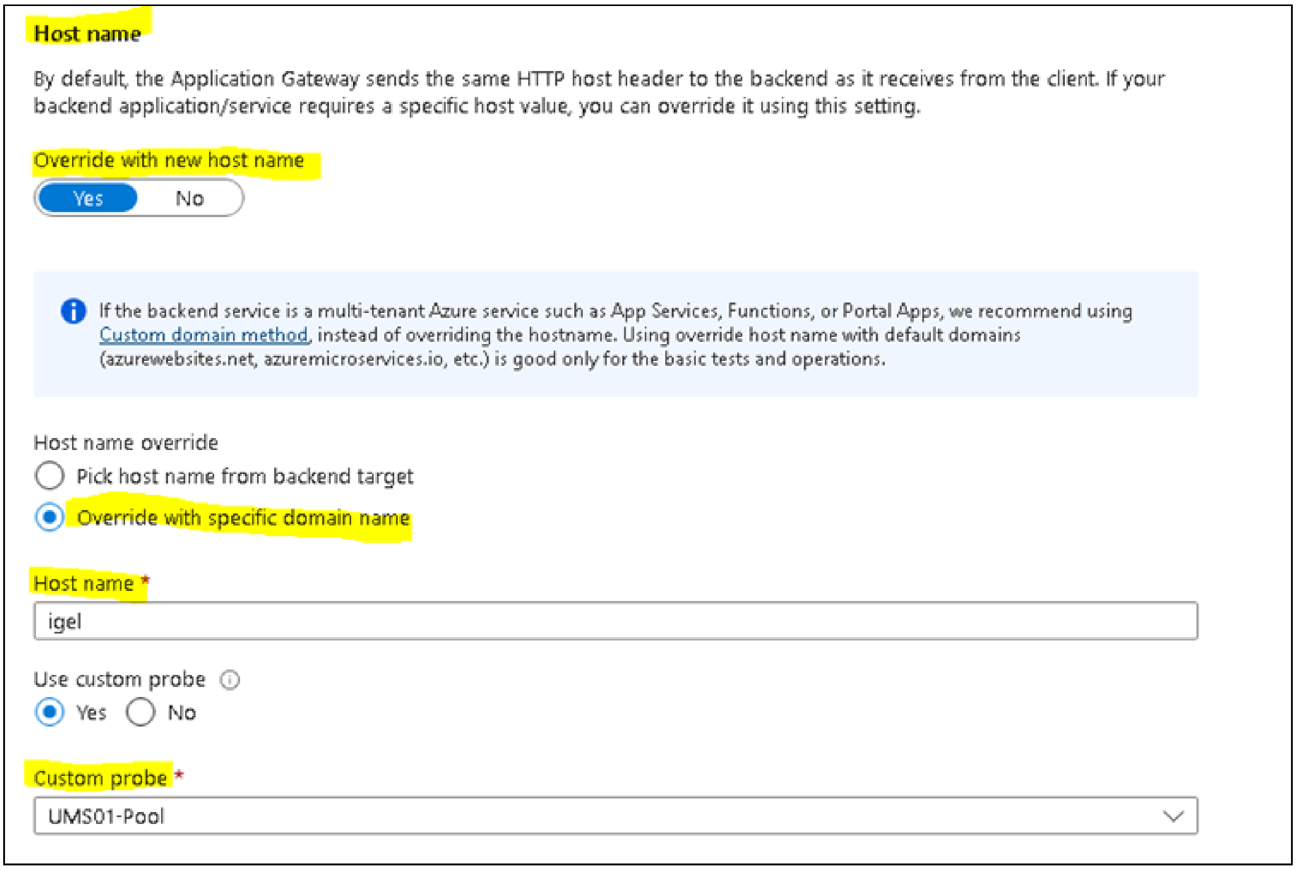
Troubleshooting Certificate Error: Common Name Does Not Match

The UMS or ICG certificate must contain the FQDN of the Backend Server as the Common Name. This value is mandatory for the Azure Application Gateway connection to the Backend. The following error occurs if the certificate is wrong.



Server (backend pool)	Status	Port (Backend setting)	Protocol	Details	Action
172.17.0.5 (UMS01-Backend)	Unhealthy	8443 (UMS01-Pool)	Https	The Common Name of the leaf certificate presented by the backend server does not match the Probe or Backend Setting hostname of the application gateway.	
172.17.0.4 (ICG01-Backend)	Healthy	8443 (ICG01-Pool)	Https	Success. Received status code	

In case the Common name cannot be adjusted, it is possible to adopt the Hostname of the UMS / ICG in the Backend Settings. In this case a custom probe must be defined with the **given Host name value**.



Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

Override with new host name

● Yes ○ No

If the backend service is a multi-tenant Azure service such as App Services, Functions, or Portal Apps, we recommend using Custom domain method, instead of overriding the hostname. Using override host name with default domains (azurewebsites.net, azuremicroservices.io, etc.) is good only for the basic tests and operations.

Host name override

○ Pick host name from backend target

● Override with specific domain name

Host name *

igel

Use custom probe

● Yes ○ No

Custom probe *

UMS01-Pool

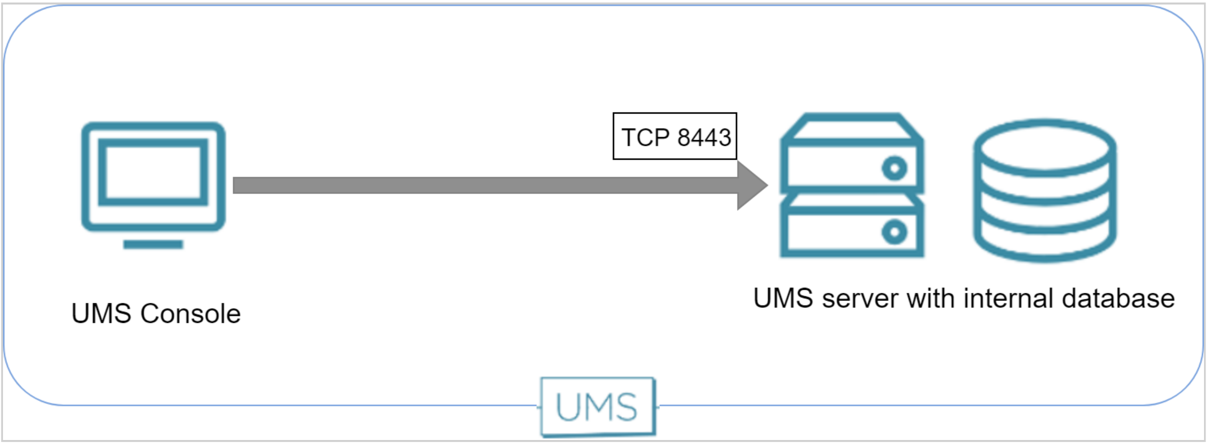
Internal Communication

UMS with Internal Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens for requests on TCP port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The port used by the UMS for internal TCP requests to the embedded database can be changed in the UMS Administrator under **Settings > Database Port (Embedded DB)**. The default port is 1528.

The following figure illustrates the communication between the UMS components:



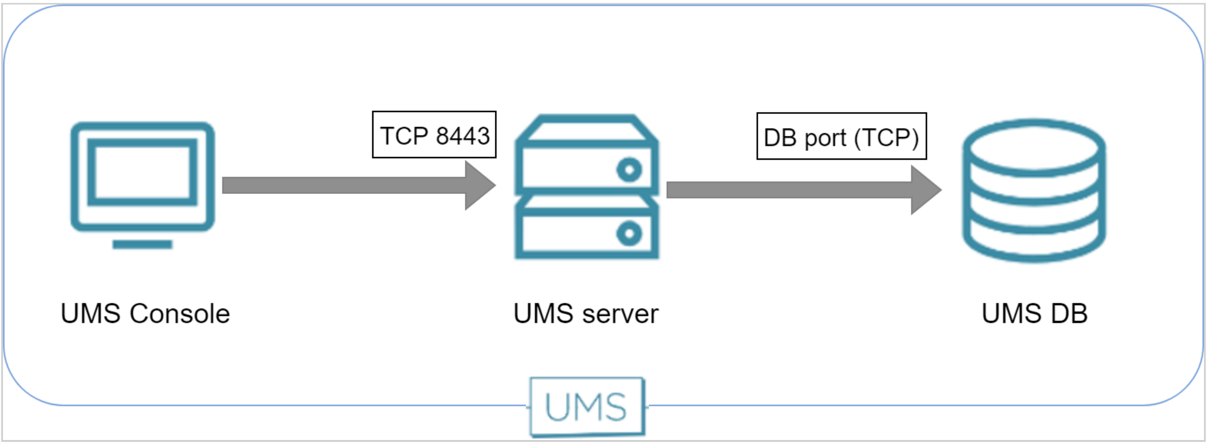
UMS with External Database

Communication between the UMS Console and the UMS server happens via HTTPS. By default, the UMS server listens to TCP requests on port 8443. The port can be changed in the UMS Administrator under **Settings > GUI server port**.

The ports used by the UMS for TCP requests to the database are defined as follows:

Database Type	Database Port (default)	Configuration
Apache Derby (Derby Network Server)	1527	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **Derby**] **> Port**
MS SQL Server	1433	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **SQL Server**] **> Port**
Oracle	1521	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **Oracle**] **> Port**
PostgreSQL	5432	(UMS Administrator) **Datasource > Add... >** [as DB-Type, select **PostgreSQL**] **> Port**

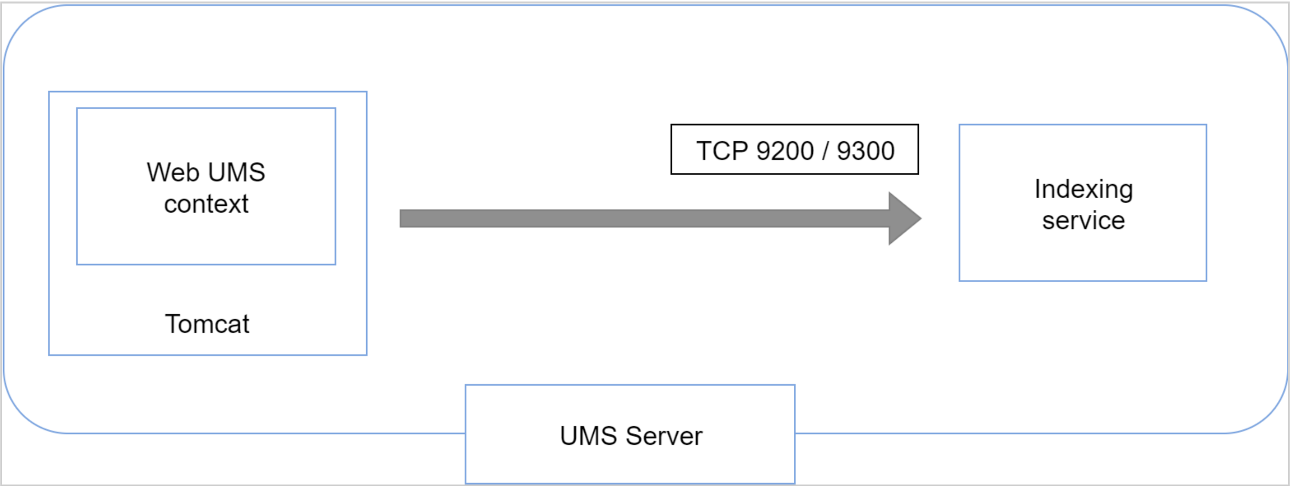
The following figure illustrates the communication between the UMS components:



Indexing for UMS Web App Search

The indexing service that is used by the search function of the UMS Web App is listening on ports 9200 and 9300. The Web UMS context reads and writes data via these ports. The ports are open internally, but cannot be reached from outside the UMS Server.

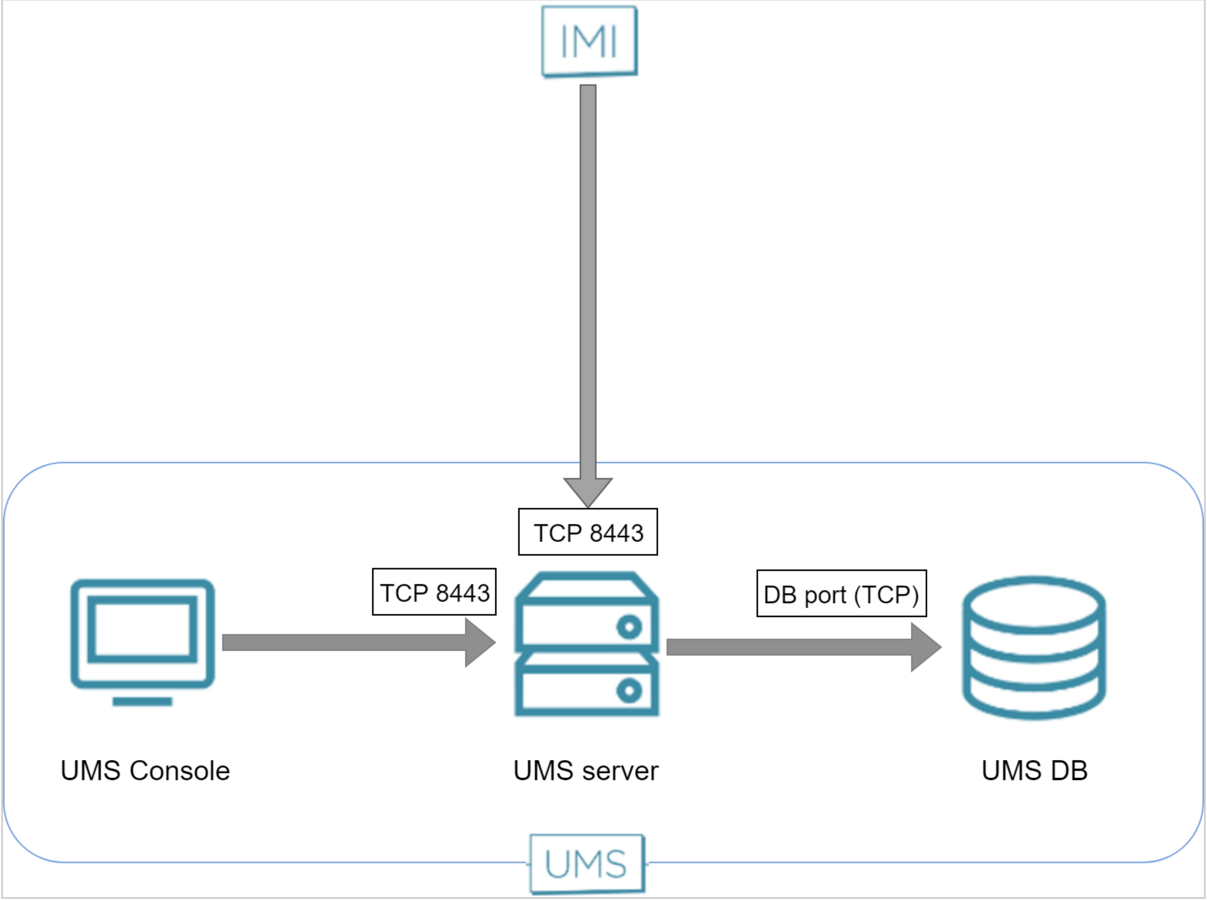
The following figure illustrates the communication within the UMS Server:



IGEL Management Interface (IMI)

The REST API provided by the IGEL Management Interface is served via HTTP on port 8443 (TCP).

The following figure illustrates the communication with the UMS server via IMI:



UMS and Devices: Settings and Control

Devices and UMS Server Contacting Each Other via ICG

To communicate with the UMS, the devices initiate a TCP connection to the ICG.

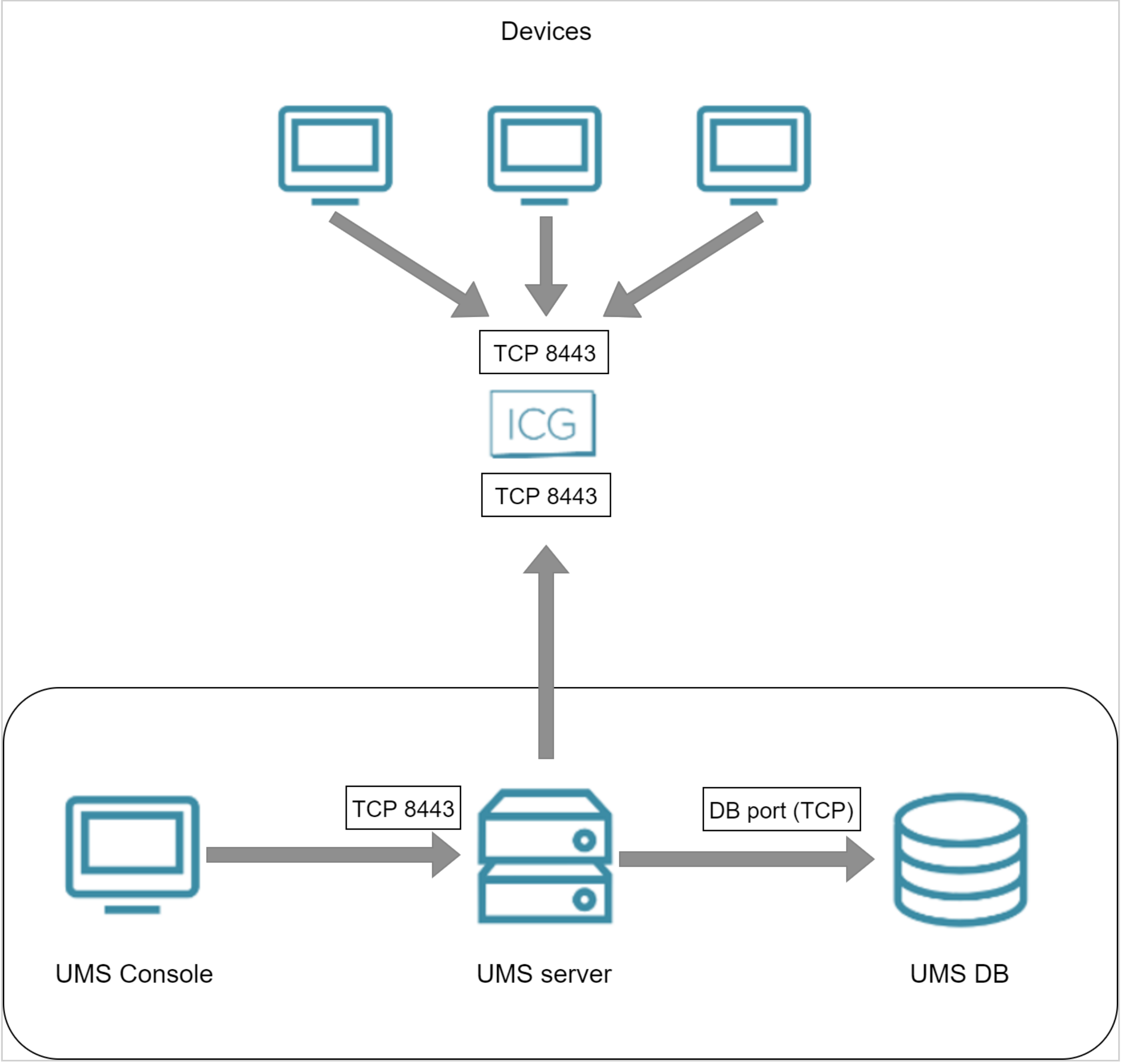
To communicate with the devices, the UMS initiates a TCP connection to the ICG.

The default port on which the ICG is listening is port 8443. It can be changed during the installation of the ICG. With ICG 2.02 or higher, a privileged port can be used, e.g. port 443. When the installation is completed, the port is fixed.

With ICG version 2.x or 12.01.x and UMS version 6.x or 12.01.x, it is not possible to inspect the TLS traffic between any of the components. The inspection would break TLS and interrupt communication between the products.
As of UMS version 12.02, you can inspect the TLS traffic, see IGEL UMS Configuration for the External Load Balancer / Reverse Proxy: Example for NGINX with SSL Offloading.

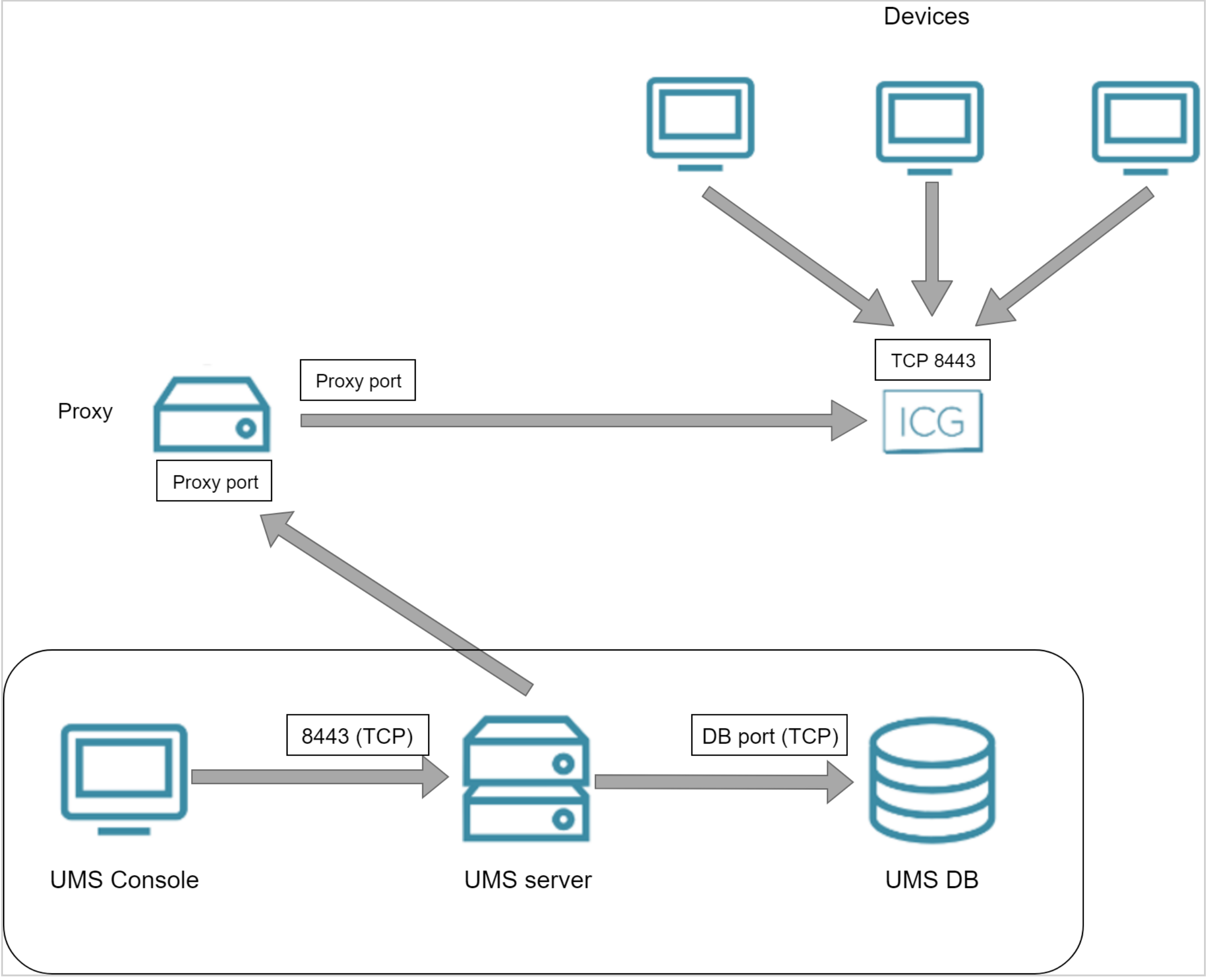
Direct Connection

The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG:



Via Proxy

The following figure illustrates the communication between the devices (thin clients) and the UMS via ICG and a proxy:

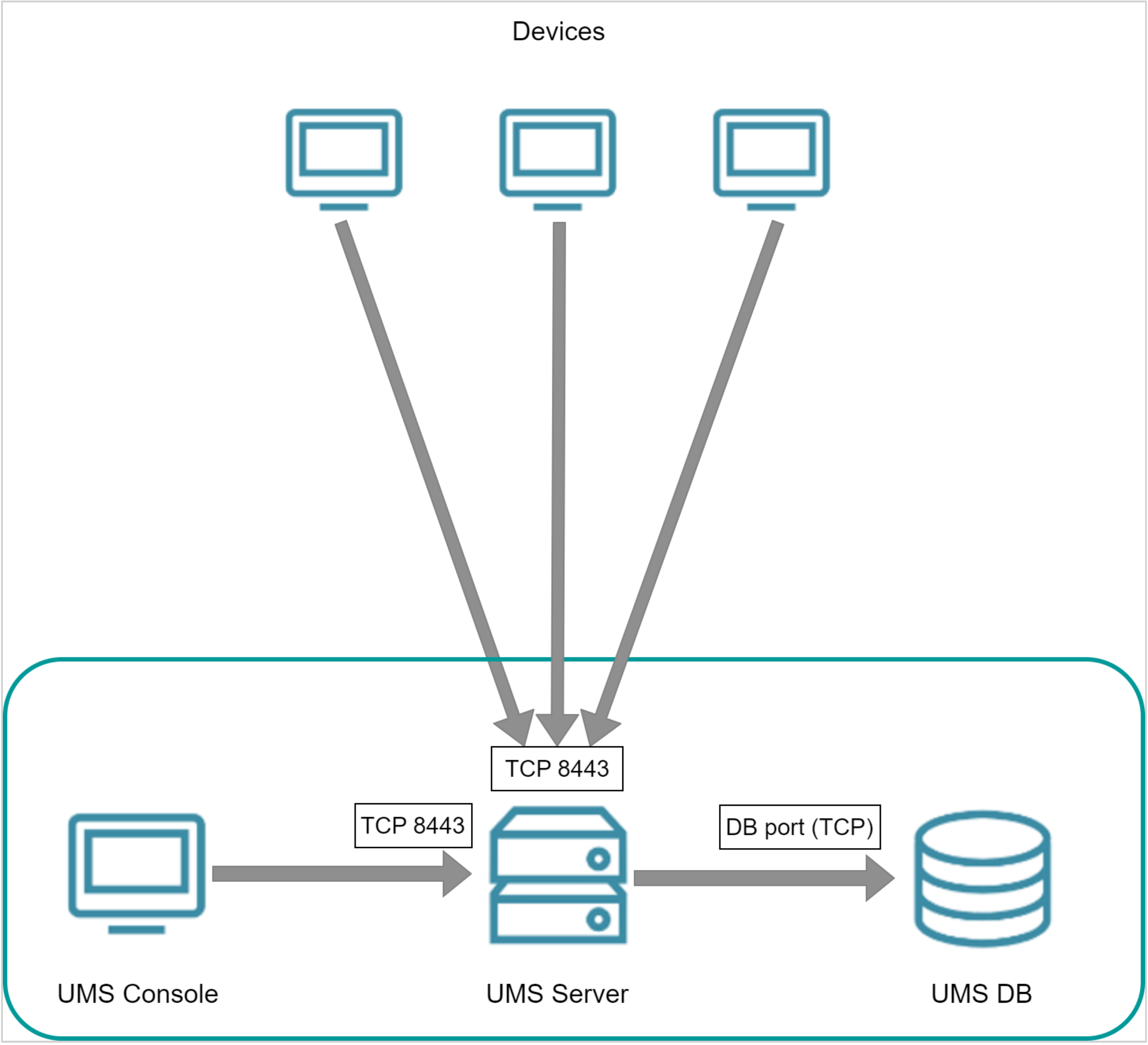

Devices
TCP 8443
ICG
Proxy
Proxy port
Proxy port
8443 (TCP)
DB port (TCP)
UMS Console
UMS server
UMS DB

Devices Contacting UMS

The following figures illustrate the communication between the endpoint devices and the UMS.

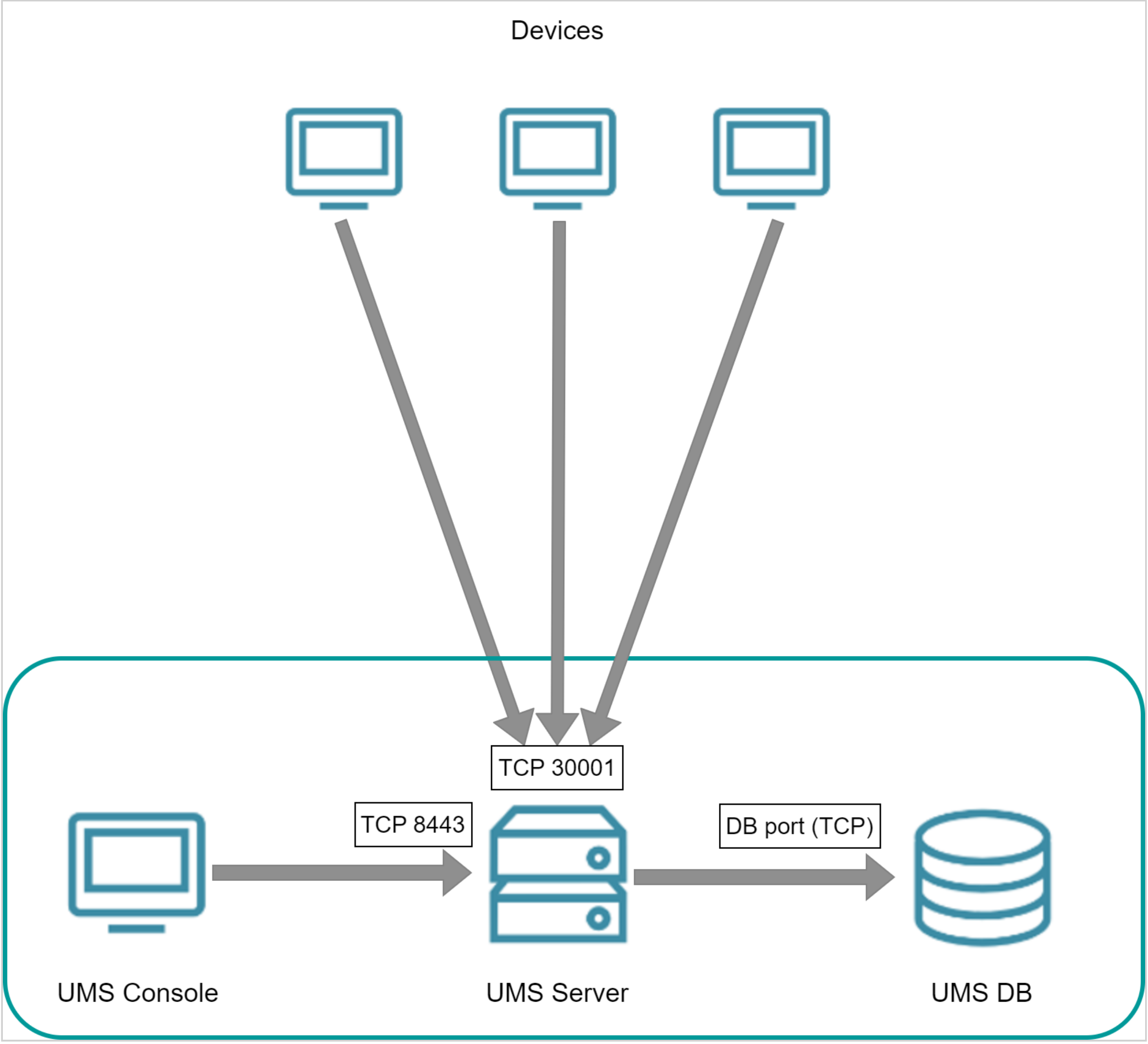
IGEL OS 12

To communicate with the UMS, the devices initiate a TCP connection to the UMS Server using port 8443.



IGEL OS 11 or Earlier

To communicate with the UMS, the devices initiate a TCP connection to the UMS Server using port 30001.


Devices
TCP 30001
TCP 8443
DB port (TCP)
UMS Console
UMS Server
UMS DB

UMS Contacting Devices

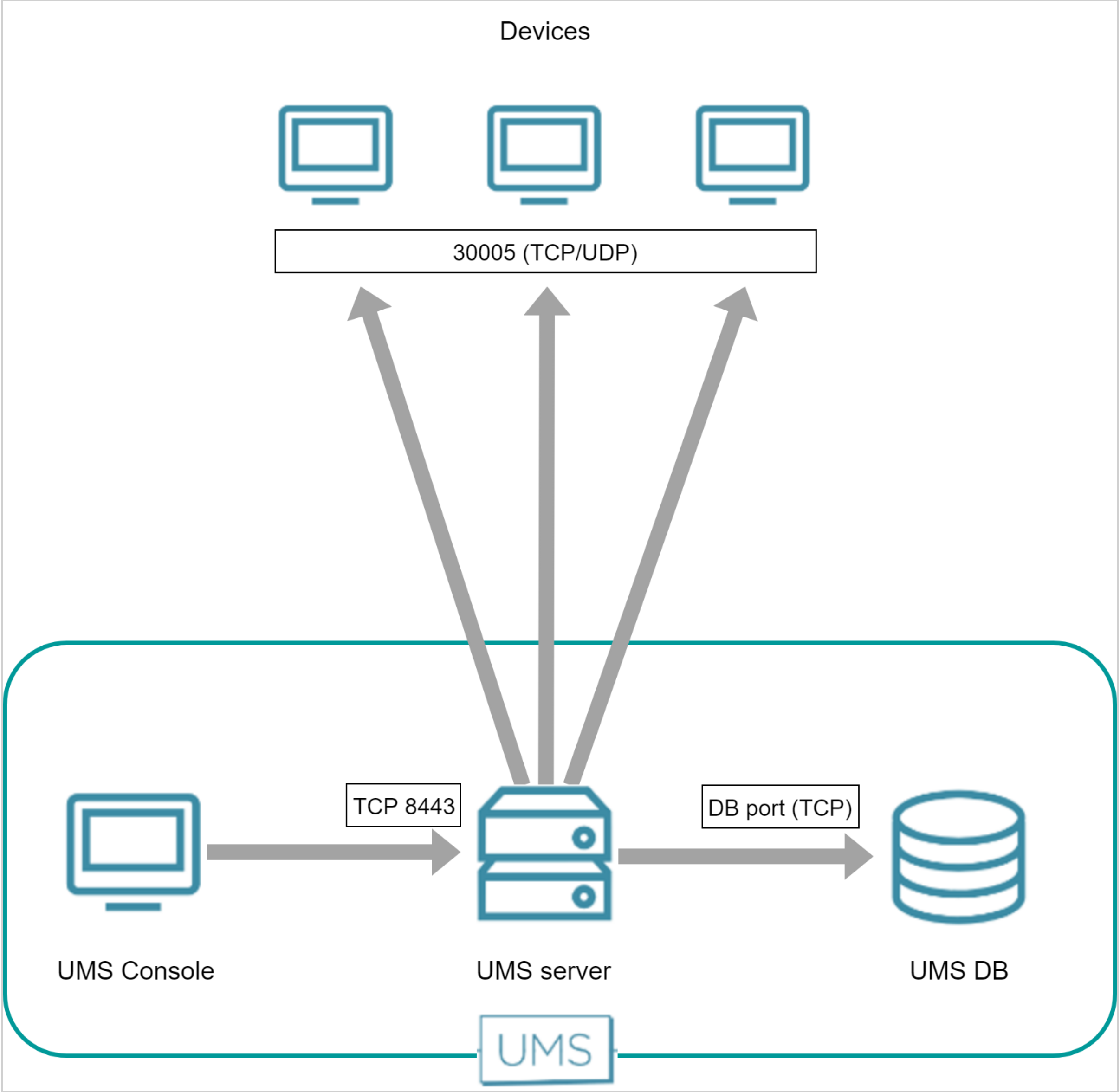
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

To communicate with IGEL OS 11 devices, the UMS initiates a TCP connection to the device's UMS agent using port 30005.

The following figure illustrates the communication between the UMS and the devices:


Devices
30005 (TCP/UDP)
TCP 8443
DB port (TCP)
UMS Console
UMS server
UMS DB
UMS

UMS and Devices: Shadowing

IGEL OS 12

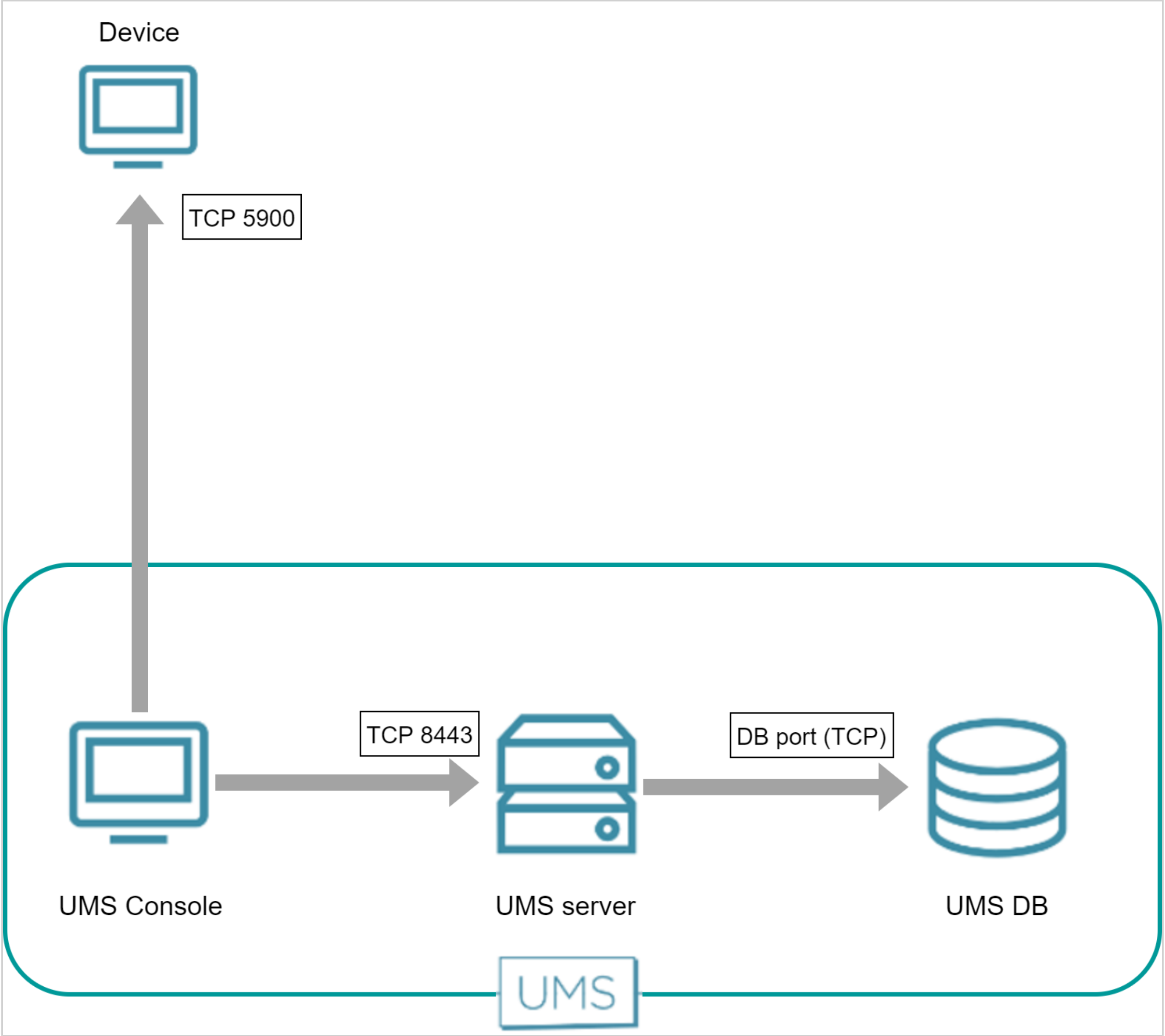
Shadowing of IGEL OS 12 devices is always secure, i.e. via the Unified Protocol. The communication is always encrypted. See UMS and Devices: Secure Shadowing (see page 106).

IGEL OS 11 or Earlier

UMS Console

The UMS Console initiates a VNC session with the device. The standard port is 5900 (TCP); the port can be changed per session.

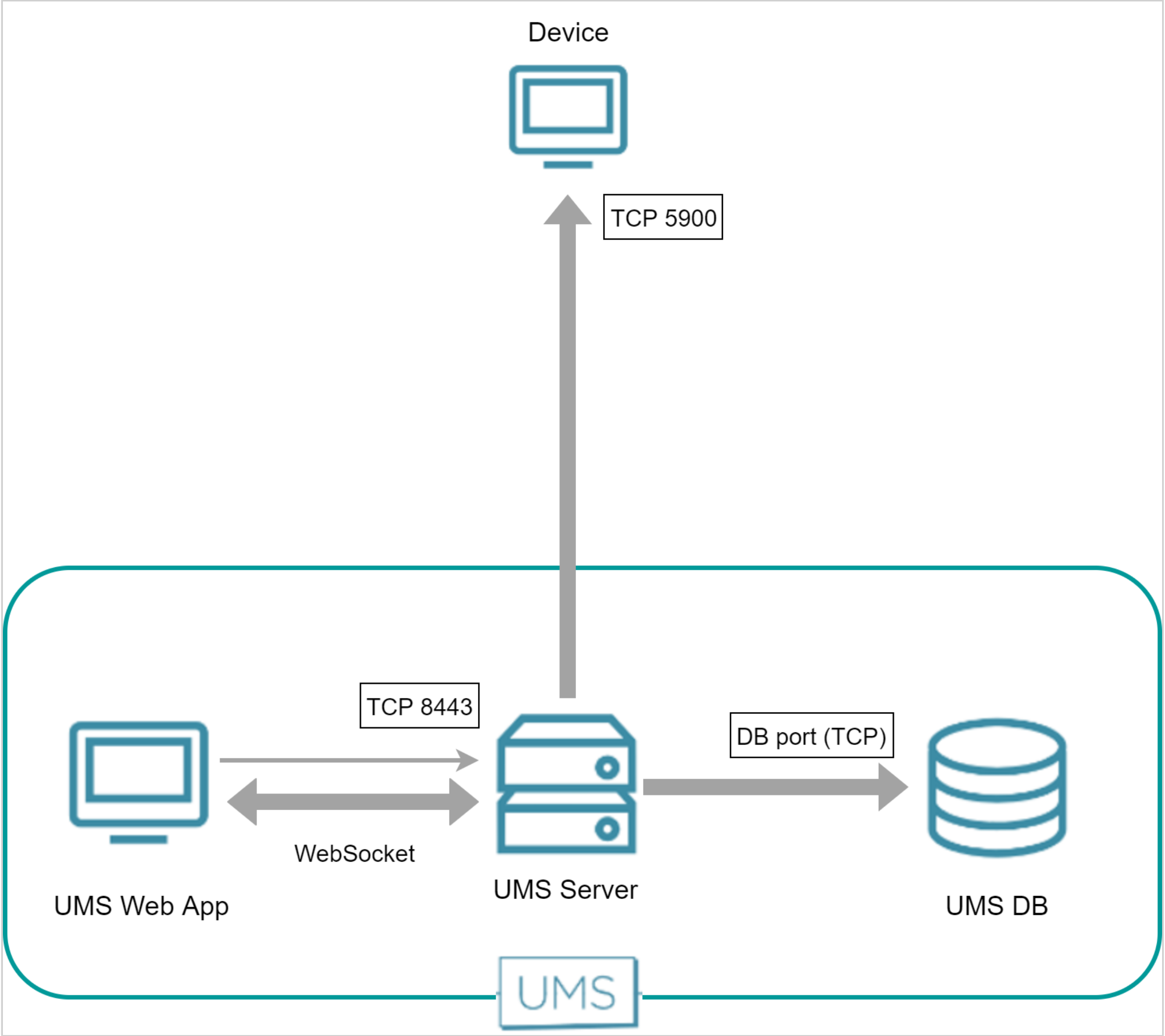
The following figure illustrates the communication between the UMS Console and a device:



UMS Web App

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The VNC session is routed through the UMS Server; between the UMS Web App and the UMS Server, the data is transferred via WebSocket. The default port for the communication between the UMS Server and the devices is 5900 (TCP).

The following figure illustrates the communication between the UMS Web App, the UMS Server, and a device:


Device
TCP 5900
TCP 8443
WebSocket
DB port (TCP)
UMS Web App
UMS Server
UMS DB
UMS

UMS and Devices: Secure Shadowing

This article describes the communication flow of a secure shadowing session in the IGEL Universal Management Suite (UMS) environment.

IGEL OS 12

Shadowing of IGEL OS 12 devices is always secure, i.e. via the Unified Protocol. The communication is always encrypted.

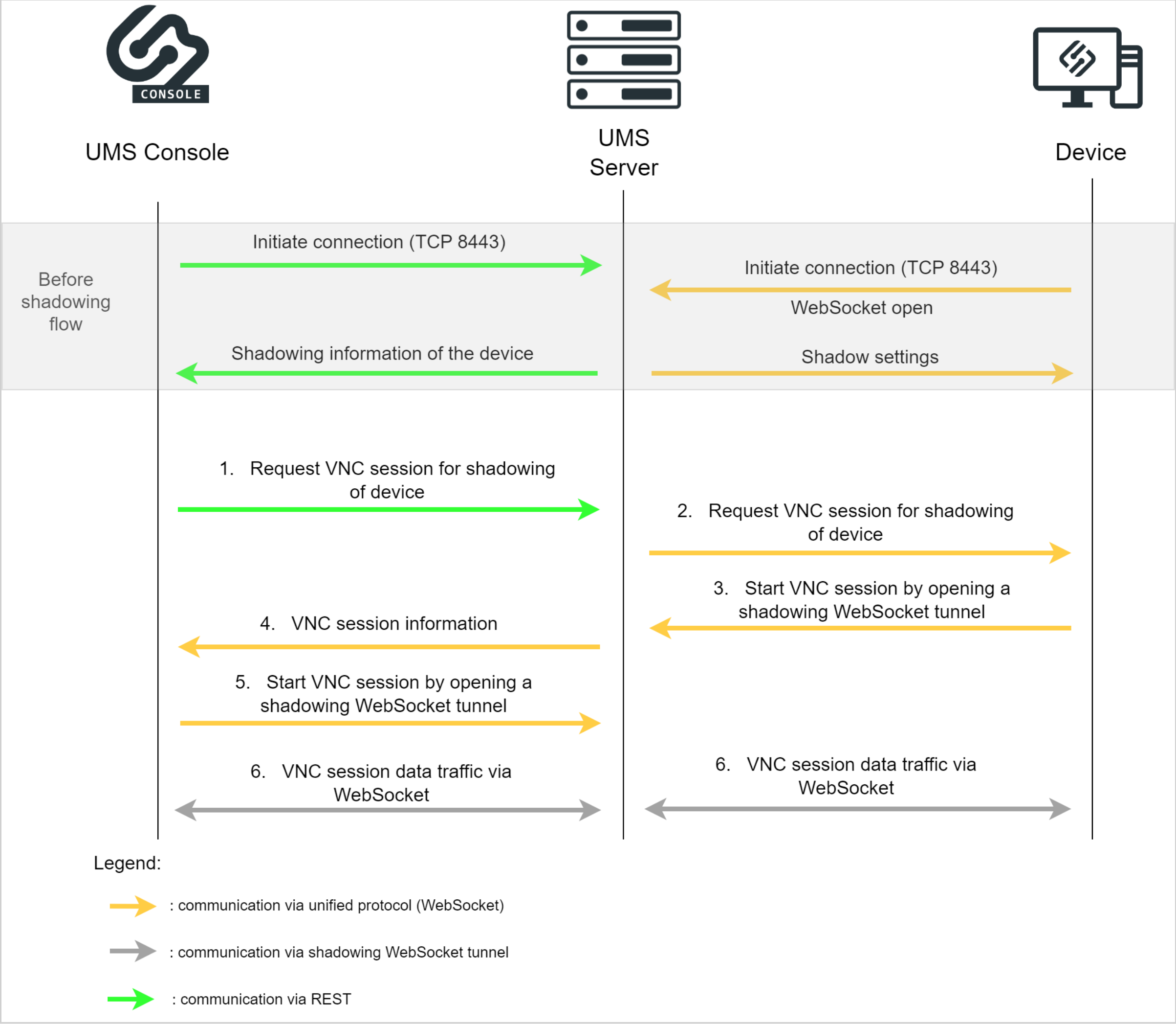
Direct Connection - UMS Console (Internal / External VNC Viewer)

Before the shadowing communication flow:

- REST connection is initiated between the Console and the UMS Server
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Shadow settings and information are forwarded

Shadowing flow:

1. The UMS Console requests the UMS Server to initiate a VNC session for shadowing.
2. The UMS Server requests the device to open a VNC session for shadowing.
3. The device opens the shadowing WebSocket tunnel to the UMS Server and starts the VNC session.
4. The UMS Server forwards the VNC session information to the UMS Console.
5. The UMS Console opens the shadowing WebSocket tunnel and starts the VNC session.
6. The VNC data is sent through the opened WebSocket tunnels between the UMS Console and the UMS Server and between the UMS Server and the Device.


CONSOLE
UMS Console
UMS Server
Device
Before shadowing flow
Initiate connection (TCP 8443)
Initiate connection (TCP 8443)
WebSocket open
Shadowing information of the device
Shadow settings
1. Request VNC session for shadowing of device
2. Request VNC session for shadowing of device
3. Start VNC session by opening a shadowing WebSocket tunnel
4. VNC session information
5. Start VNC session by opening a shadowing WebSocket tunnel
6. VNC session data traffic via WebSocket
6. VNC session data traffic via WebSocket
Legend:
: communication via unified protocol (WebSocket)
: communication via shadowing WebSocket tunnel
: communication via REST

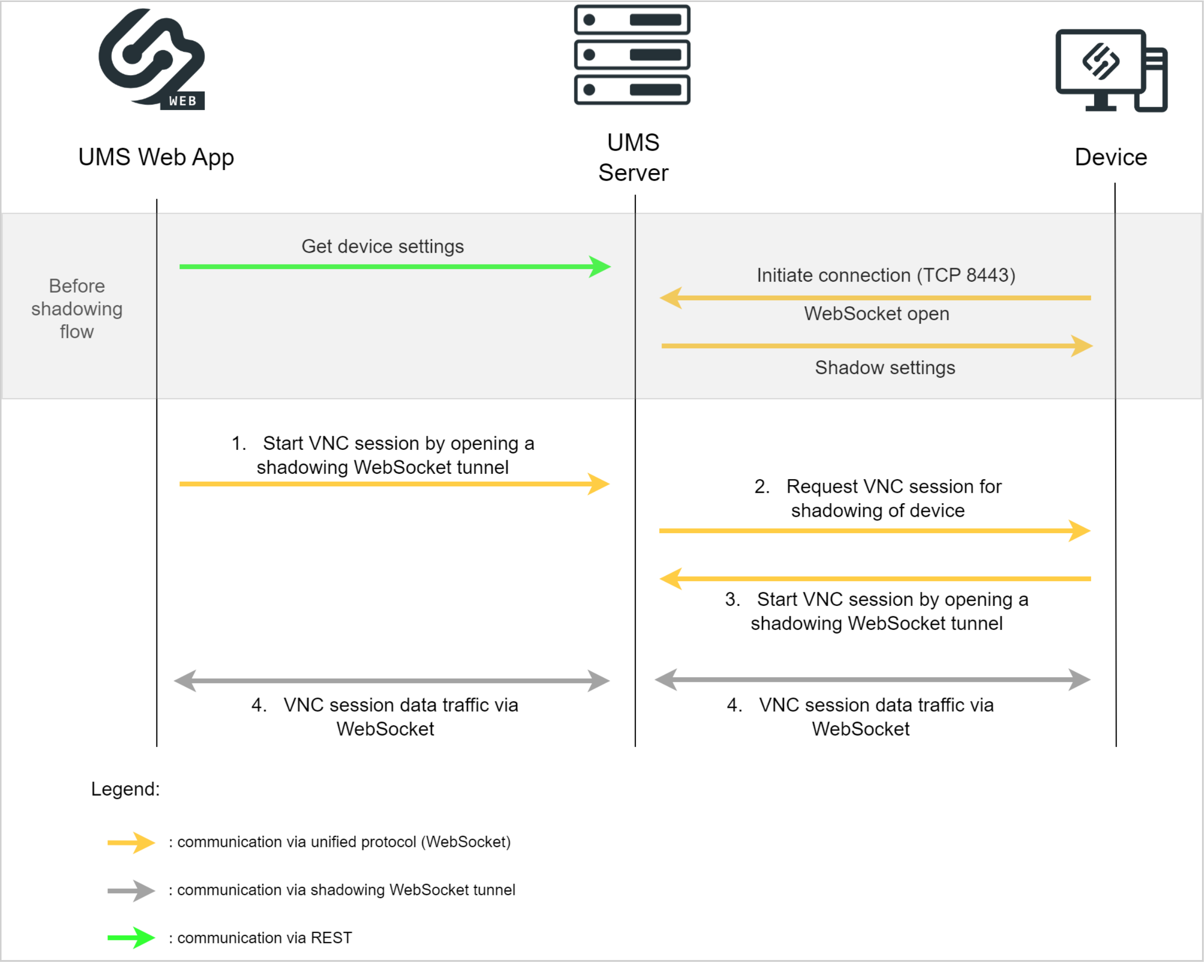
Direct Connection - UMS Web App

Before the shadowing communication flow:

- Device settings are sent to the UMS Server through REST
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Shadow settings are forwarded

Shadowing flow:

1. The UMS Web App starts the VNC session by opening the shadowing WebSocket tunnel to the UMS Server with information on the device to be shadowed.
2. The UMS Server requests the device via the Unified Protocol WebSocket to open a VNC session for shadowing.
3. The device opens the shadowing WebSocket tunnel to the UMS Server and starts the VNC session.
4. The VNC data is sent through the opened WebSocket tunnels.


UMS Web App
UMS Server
Device
Before shadowing flow
Get device settings
Initiate connection (TCP 8443)
WebSocket open
Shadow settings
1. Start VNC session by opening a shadowing WebSocket tunnel
2. Request VNC session for shadowing of device
3. Start VNC session by opening a shadowing WebSocket tunnel
4. VNC session data traffic via WebSocket
4. VNC session data traffic via WebSocket
Legend:
: communication via unified protocol (WebSocket)
: communication via shadowing WebSocket tunnel
: communication via REST

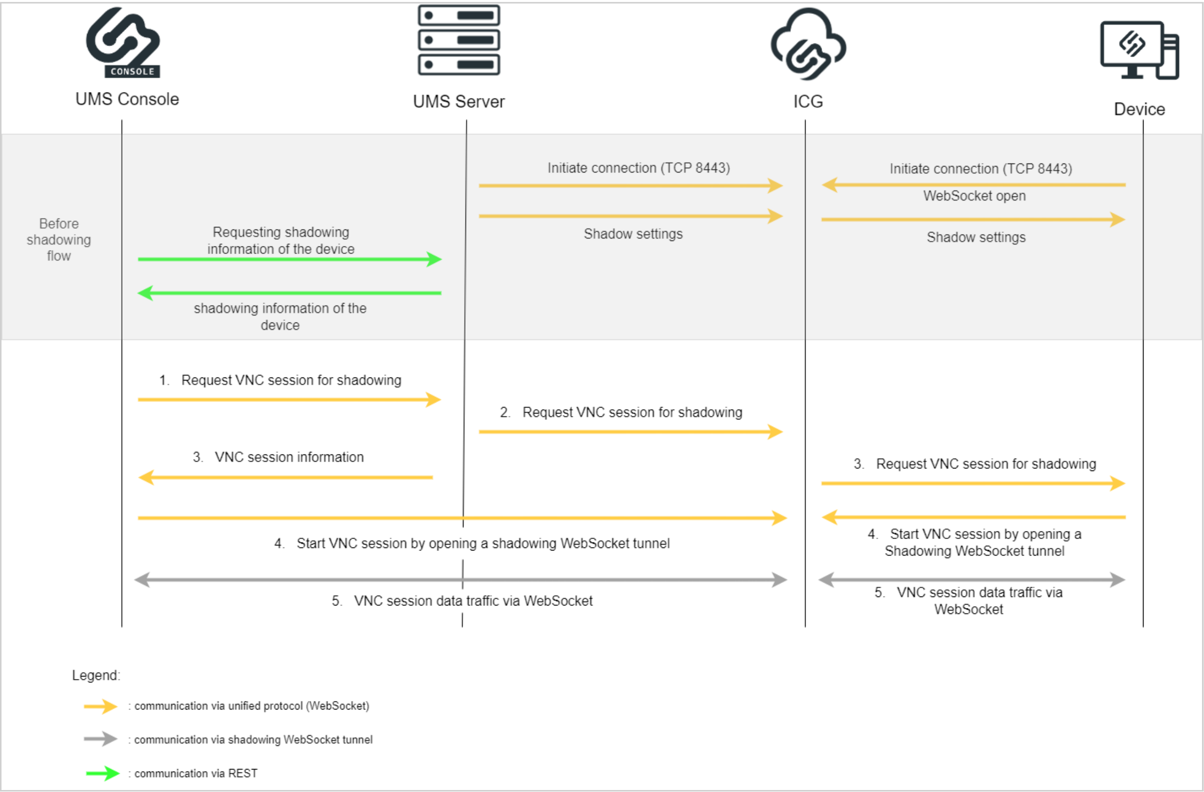
Over ICG - UMS Console (Internal / External VNC Viewer)

Before the shadowing communication flow:

- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Shadow settings are forwarded
- UMS Server sends shadowing information through REST to the UMS Console

Shadowing flow:

1. The UMS Console requests the UMS Server to initiate a VNC session for shadowing.
2. The UMS Server requests the ICG to open a VNC session for shadowing.
3. The UMS Server sends the VNC information to the UMS Console and the ICG requests the device to open a VNC session for shadowing.
4. The device opens the shadowing WebSocket tunnel to the ICG and starts the VNC session and the UMS Console opens the shadowing WebSocket tunnel to the ICG and starts the VNC session.
5. The VNC data is sent through the opened WebSocket tunnels.


UMS Console
UMS Server
ICG
Device
Before shadowing flow
Initiate connection (TCP 8443)
Shadow settings
Initiate connection (TCP 8443)
WebSocket open
Shadow settings
Requesting shadowing information of the device
shadowing information of the device
1. Request VNC session for shadowing
2. Request VNC session for shadowing
3. VNC session information
3. Request VNC session for shadowing
4. Start VNC session by opening a shadowing WebSocket tunnel
4. Start VNC session by opening a Shadowing WebSocket tunnel
5. VNC session data traffic via WebSocket
5. VNC session data traffic via WebSocket
Legend:
: communication via unified protocol (WebSocket)
: communication via shadowing WebSocket tunnel
: communication via REST

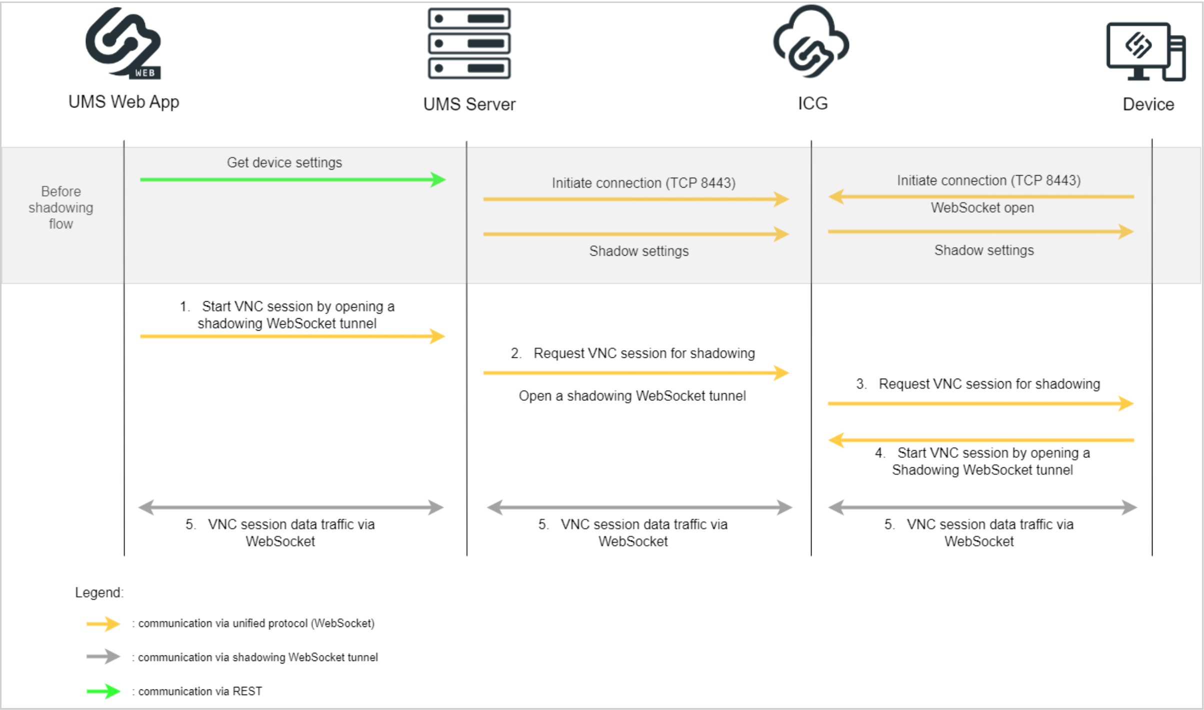
Over ICG - UMS Web App

Before the shadowing communication flow:

- Device settings are sent to the UMS Server through REST
- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Shadow settings are forwarded

Shadowing flow:

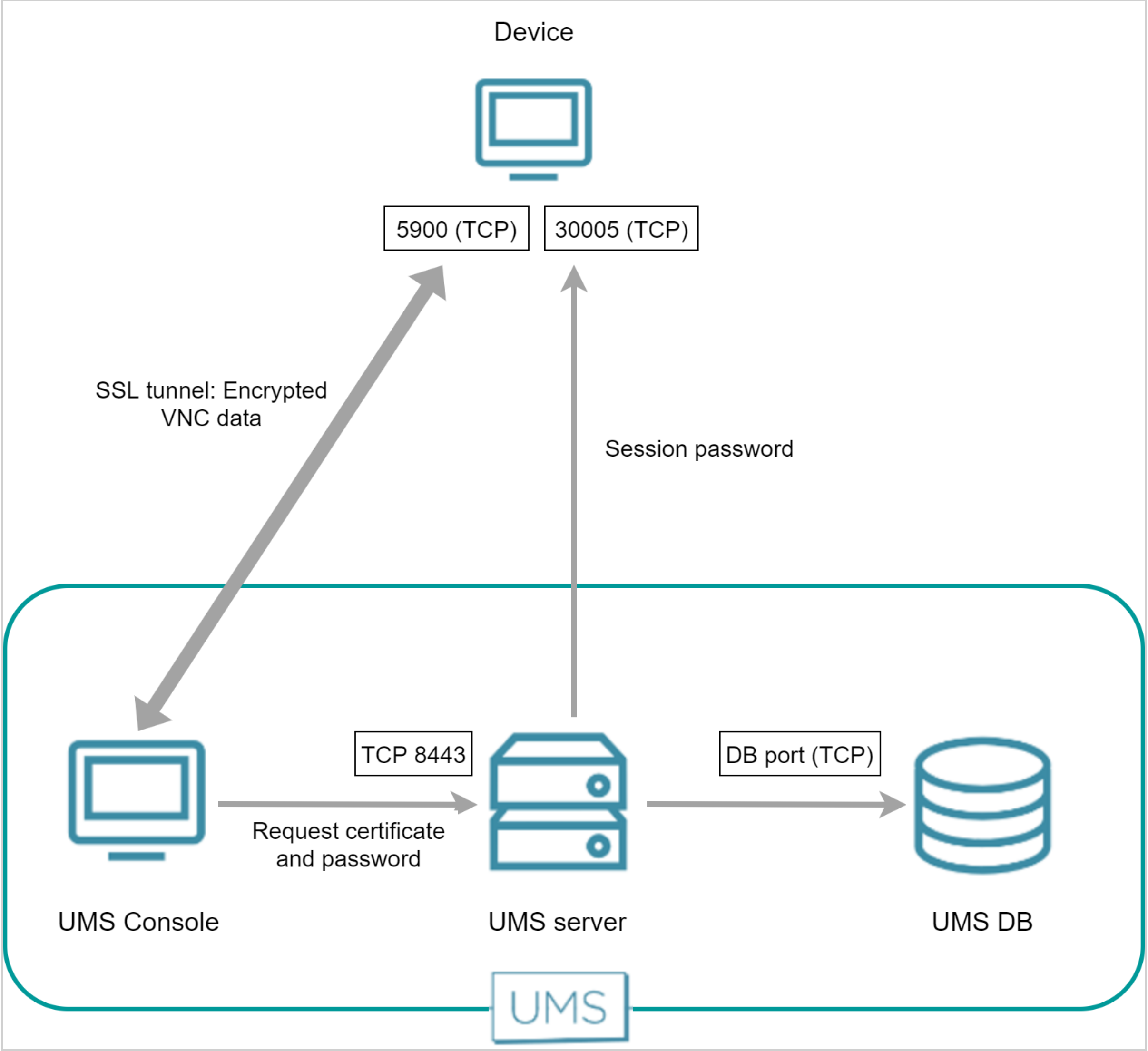
1. The UMS Web App starts the VNC session by opening the shadowing WebSocket tunnel to the UMS Server with information on the device to be shadowed.
2. The UMS Server requests the ICG to open a VNC session for shadowing and opens a WebSocket tunnel for the shadowing.
3. The ICG requests the device to open a VNC session for shadowing.
4. The device opens the Shadowing WebSocket to the ICG and starts the VNC session.
5. The VNC data is sent through these WebSockets.


UMS Web App
UMS Server
ICG
Device
Before shadowing flow
Get device settings
Initiate connection (TCP 8443)
Shadow settings
Initiate connection (TCP 8443)
WebSocket open
Shadow settings
1. Start VNC session by opening a shadowing WebSocket tunnel
2. Request VNC session for shadowing
Open a shadowing WebSocket tunnel
3. Request VNC session for shadowing
4. Start VNC session by opening a Shadowing WebSocket tunnel
5. VNC session data traffic via WebSocket
5. VNC session data traffic via WebSocket
5. VNC session data traffic via WebSocket
Legend:
: communication via unified protocol (WebSocket)
: communication via shadowing WebSocket tunnel
: communication via REST

IGEL OS 11 or Earlier

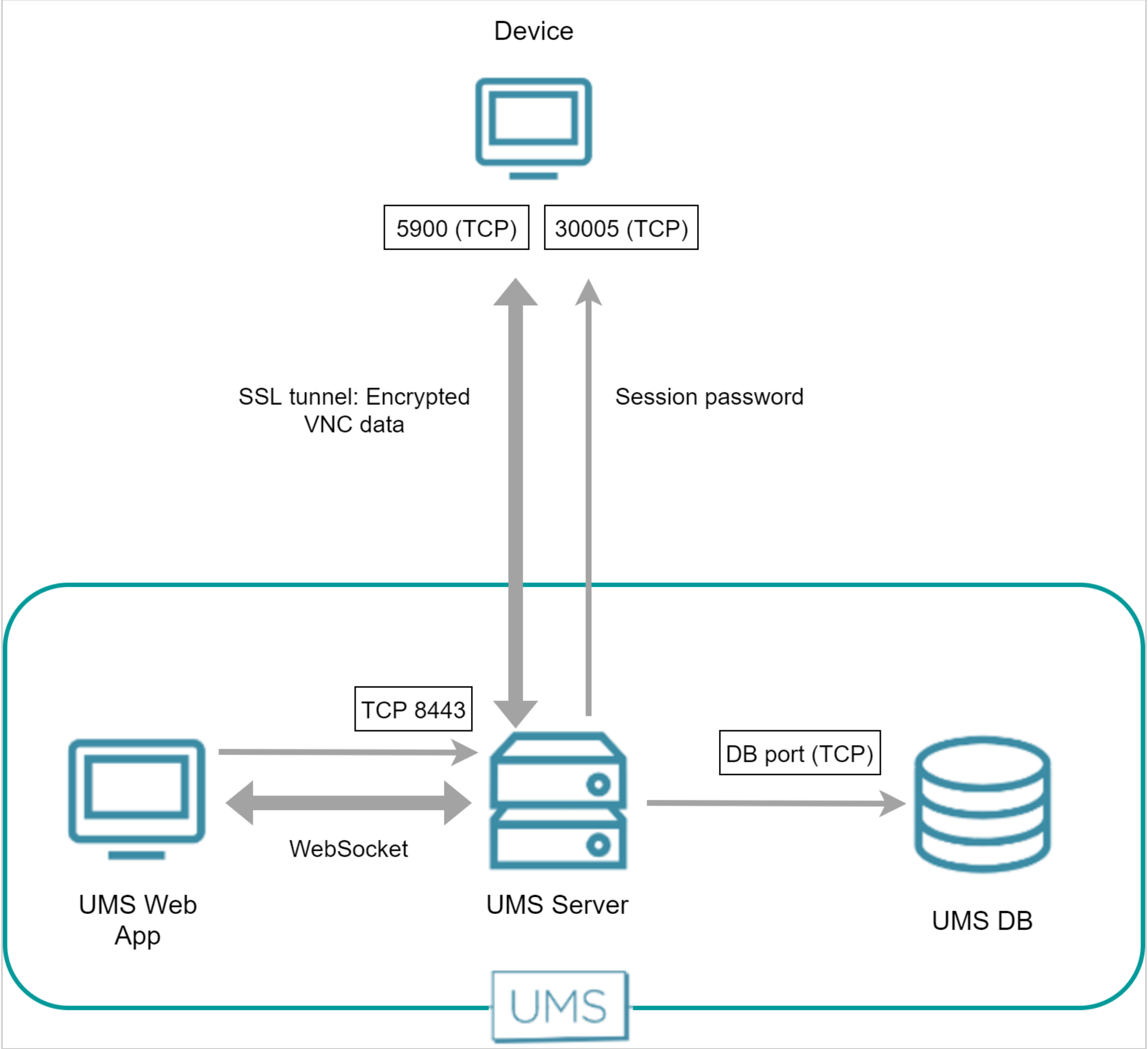
Direct Connection - Internal VNC Viewer

The UMS Console requests the device's certificate and the session password from the UMS Server. The UMS Console then establishes an SSL tunnel with the device using the session password. The device sends the certificate to the UMS Console; the UMS Console checks the certificate against the certificate it has received from the UMS Server. In return, the UMS Console sends the session password to the device. After that, the SSL tunnel between the UMS Console and device is established and can be used for exchanging VNC data.



Direct Connection - UMS Web App

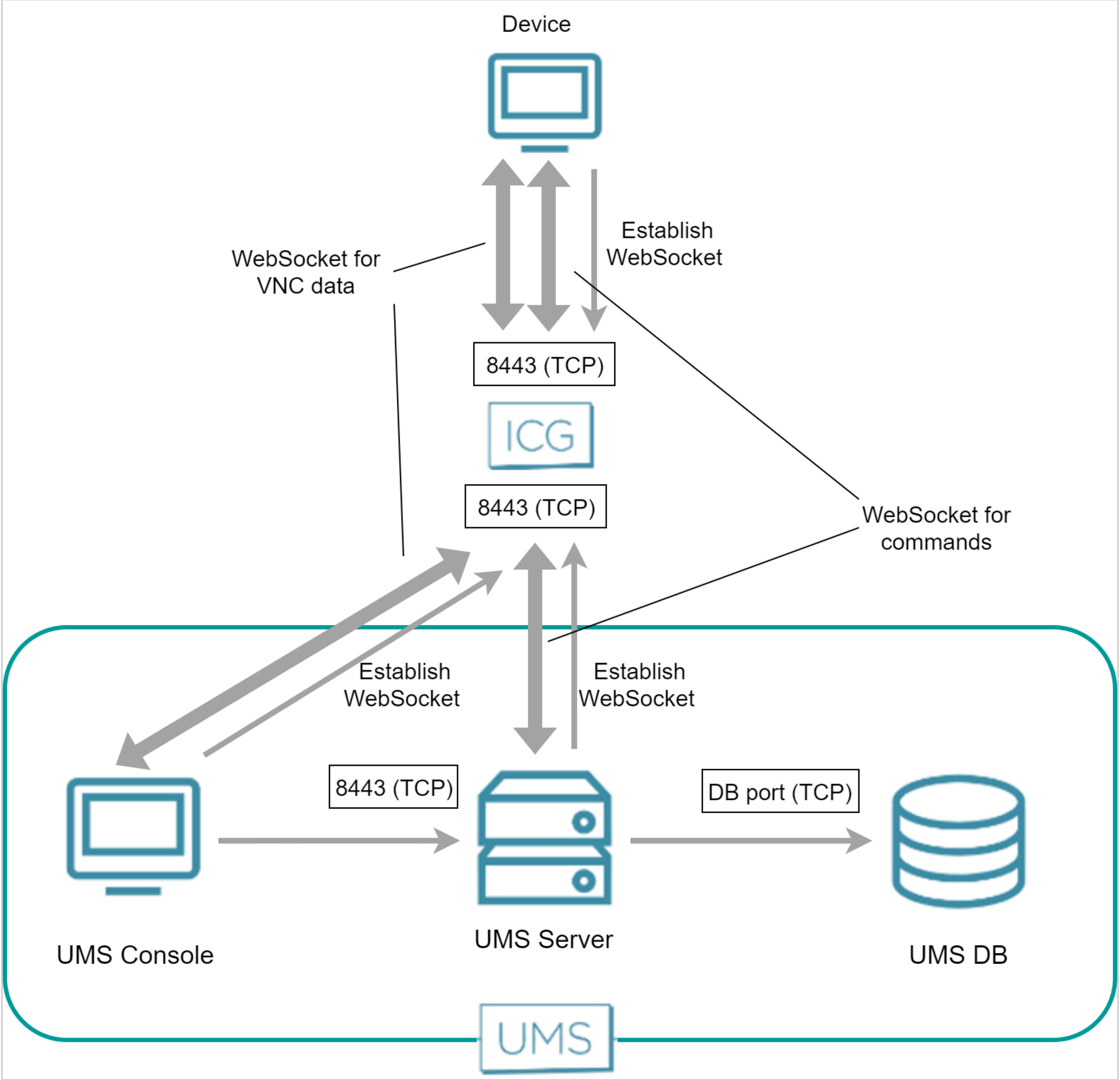
The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server establishes an SSL tunnel with the device using a session password and the device's certificate. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



Over ICG - Internal VNC Viewer

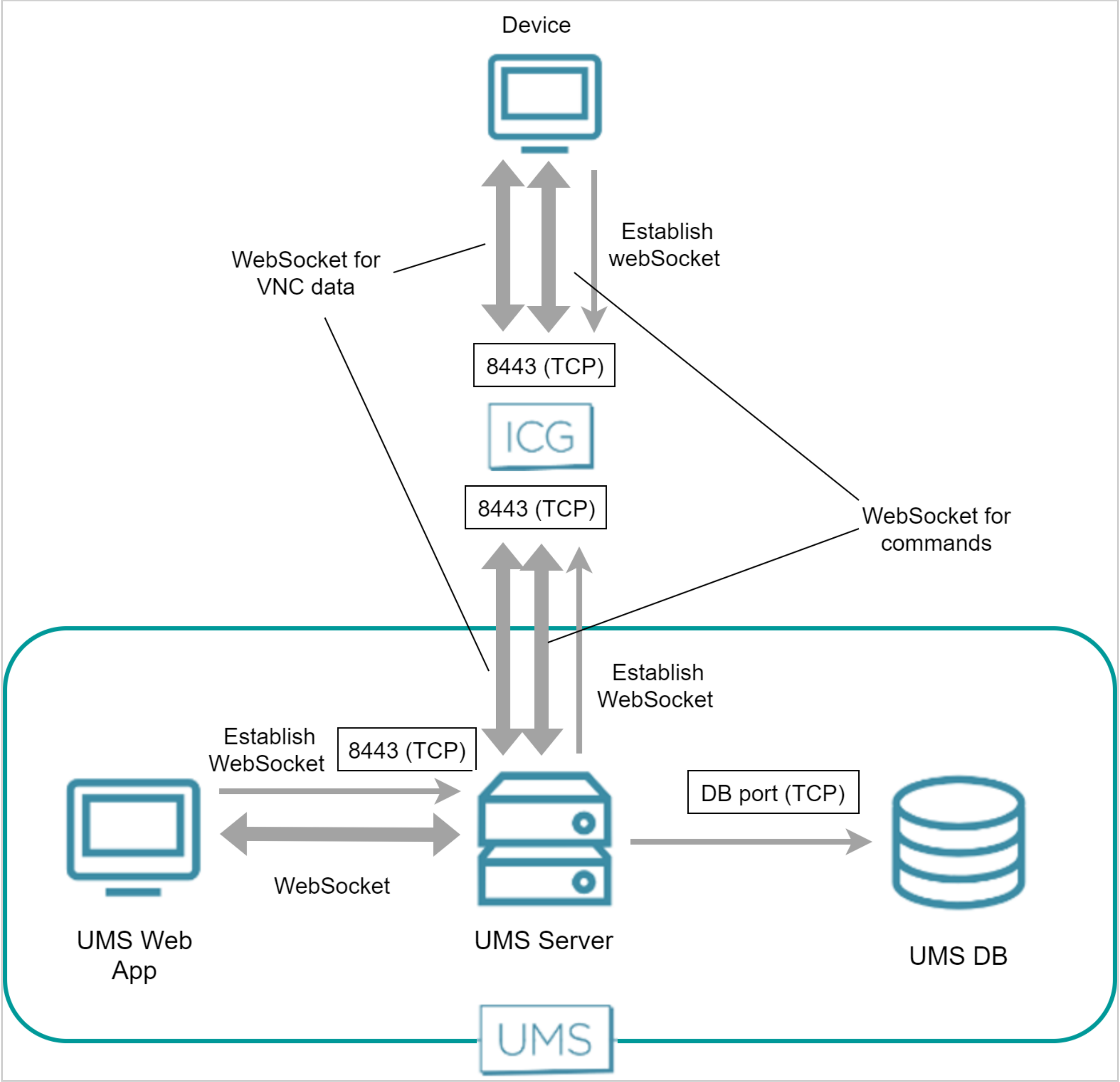
Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

The UMS Console and the device establish a dedicated WebSocket for secure shadowing with the ICG.



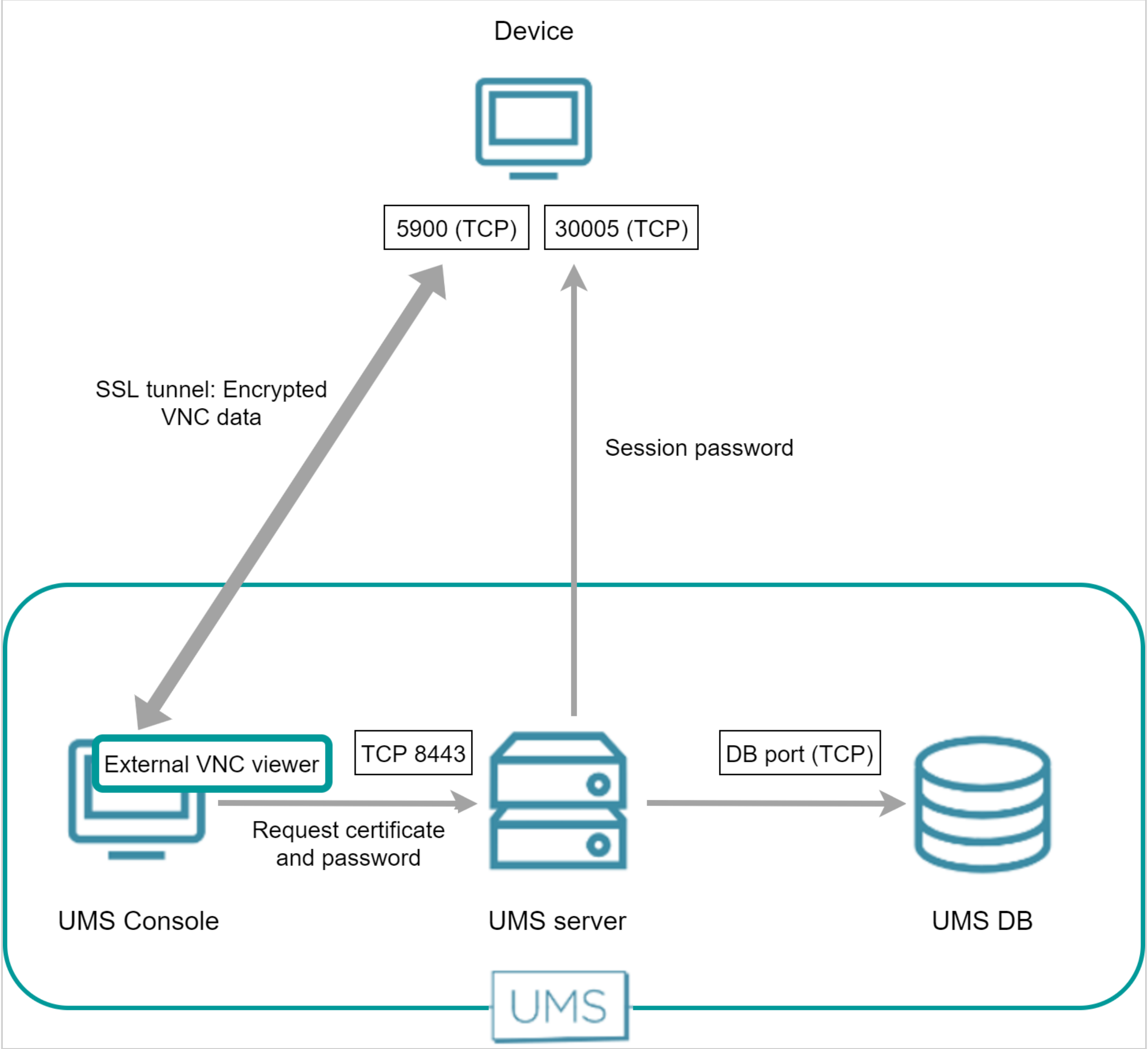
Over ICG - UMS Web App

The UMS Web App requests the UMS Server to initiate a VNC session for shadowing. The UMS Server creates an additional WebSocket connection for exchanging the VNC data. The UMS Web App and the UMS Server communicate via WebSocket, which also carries the VNC data.



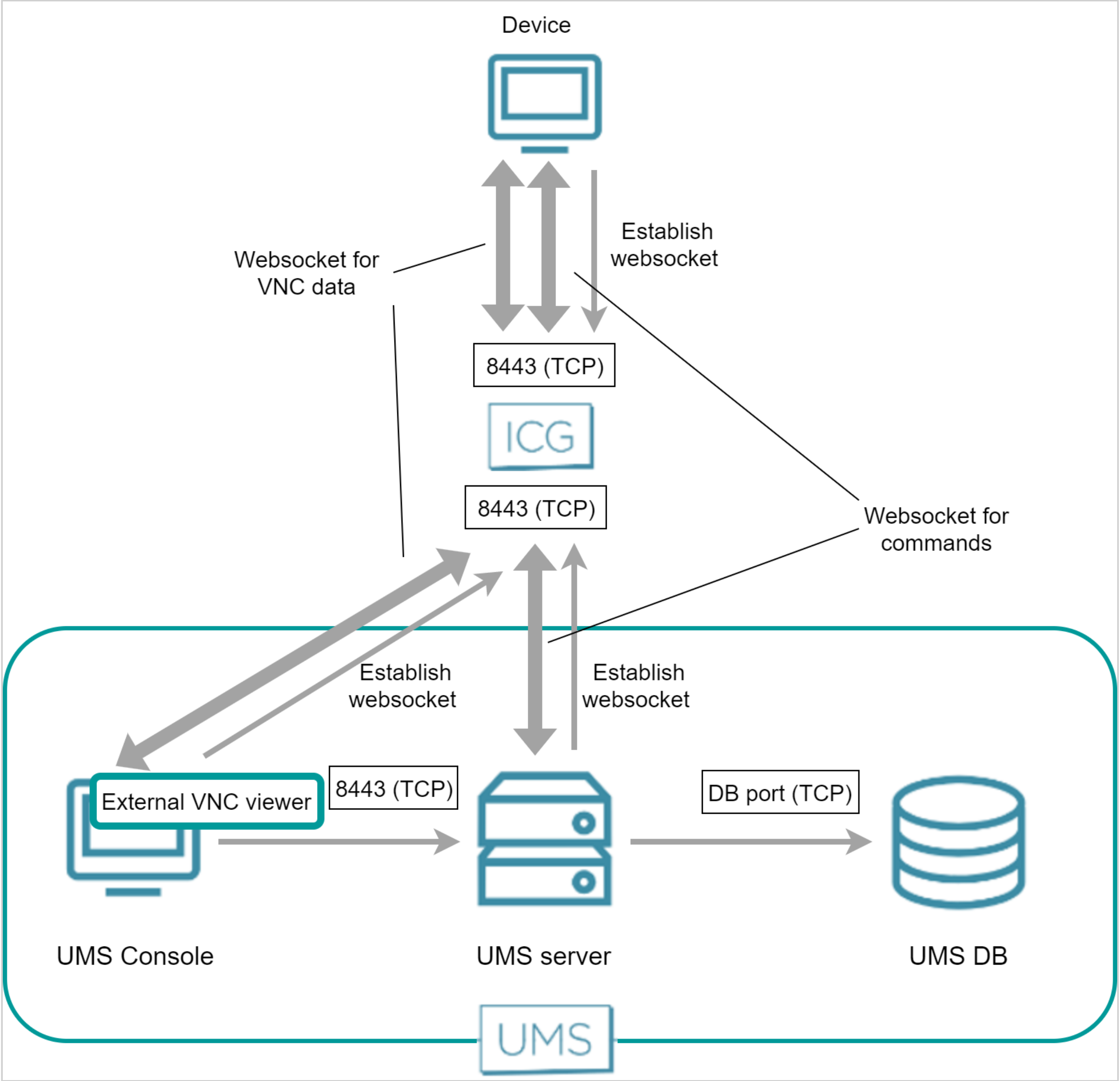
Direct Connection - External VNC Viewer

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the device and the external VNC viewer.



Over ICG - External VNC Viewer

The external VNC viewer runs on the same machine as the UMS Console. The UMS Console starts the external viewer and then acts as a proxy between the ICG and the external VNC viewer.


Device
Websocket for VNC data
Establish websocket
8443 (TCP)
ICG
8443 (TCP)
Websocket for commands
Establish websocket
Establish websocket
External VNC viewer
8443 (TCP)
DB port (TCP)
UMS Console
UMS server
UMS DB
UMS

UMS and Devices: Secure Terminal

This article describes the communication flow of a secure terminal session in the IGEL Universal Management Suite (UMS) environment.

IGEL OS 12

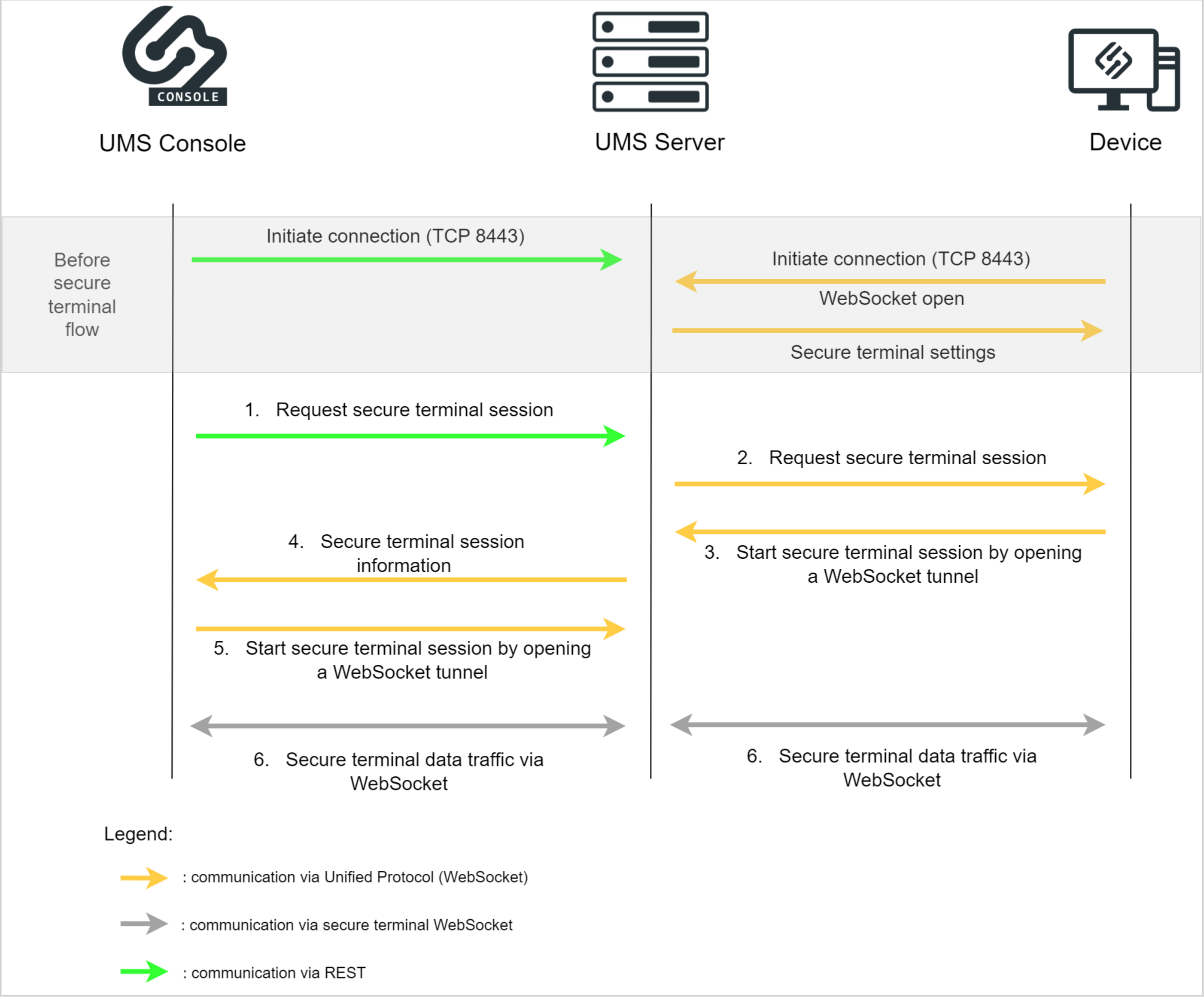
Direct Connection

Before the secure terminal flow:

- REST connection is initiated between the Console and the UMS Server
- Unified Protocol WebSocket connection is initiated between the Device and the UMS Server
- Secure terminal settings are forwarded

Secure terminal communication flow:

1. The UMS Console requests the UMS Server to initiate a secure terminal session.
2. The UMS Server requests the device via the Unified Protocol WebSocket to open the secure terminal session.
3. The device opens the WebSocket tunnel for secure terminal data to the UMS Server and starts the secure terminal session.
4. The UMS Server forwards the secure terminal session information to the UMS Console.
5. The UMS Console opens the WebSocket tunnel for secure terminal data to the UMS Server and starts the secure terminal session.
6. The terminal data is sent through the opened WebSockets.


UMS Console
UMS Server
Device
Before secure terminal flow
Initiate connection (TCP 8443)
Initiate connection (TCP 8443)
WebSocket open
Secure terminal settings
1. Request secure terminal session
2. Request secure terminal session
3. Start secure terminal session by opening a WebSocket tunnel
4. Secure terminal session information
5. Start secure terminal session by opening a WebSocket tunnel
6. Secure terminal data traffic via WebSocket
6. Secure terminal data traffic via WebSocket
Legend:
: communication via Unified Protocol (WebSocket)
: communication via secure terminal WebSocket
: communication via REST

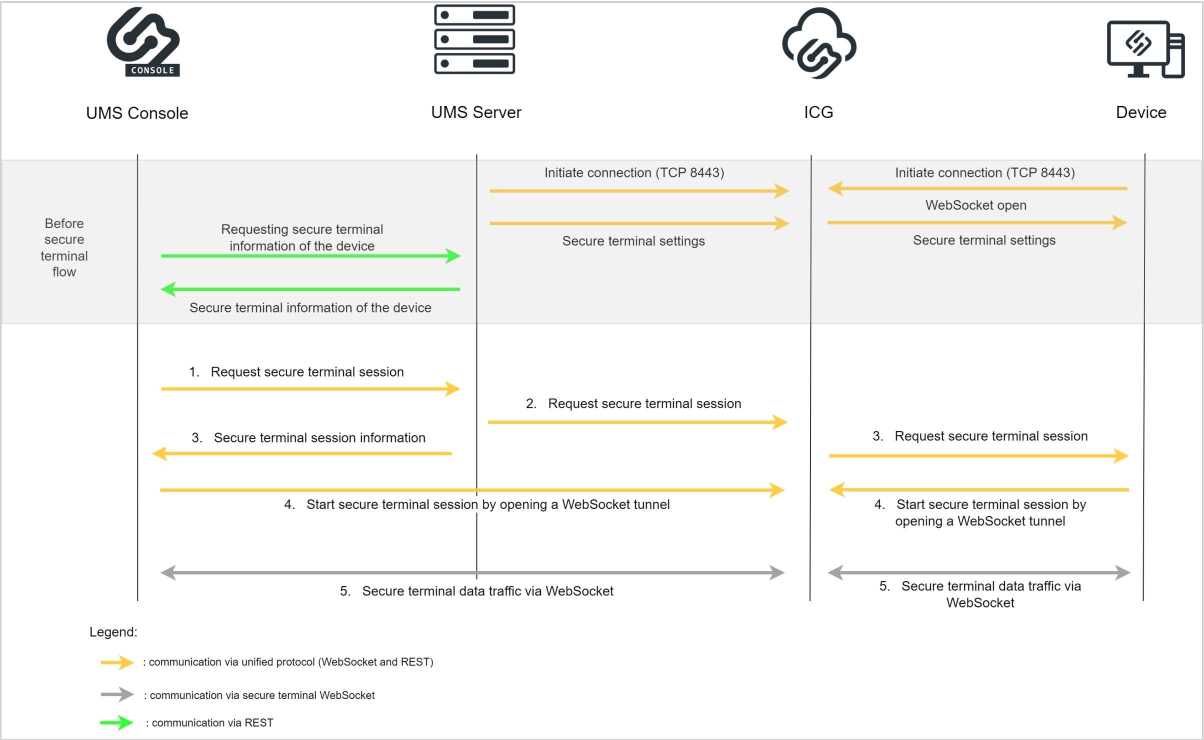
Over ICG

Before the secure terminal flow:

- Unified Protocol WebSocket connections are initiated between the UMS Server and the ICG and between the Device and the ICG
- Secure terminal settings are forwarded
- UMS Server sends the secure terminal information of the device through REST to the UMS Console

Secure terminal communication flow:

1. The UMS Console requests the UMS Server to initiate a secure terminal session.
2. The UMS Server requests the ICG to open a secure terminal session.
3. The ICG requests the device via the Unified Protocol WebSocket to open a secure terminal session and the UMS Server forwards the secure terminal session information to the UMS Console.
4. The device opens the WebSocket tunnel for secure terminal data to the ICG and starts the secure terminal session and the UMS Console opens the WebSocket tunnel for secure terminal data to the ICG and starts the secure terminal session.
5. The terminal data is sent through the opened WebSockets.

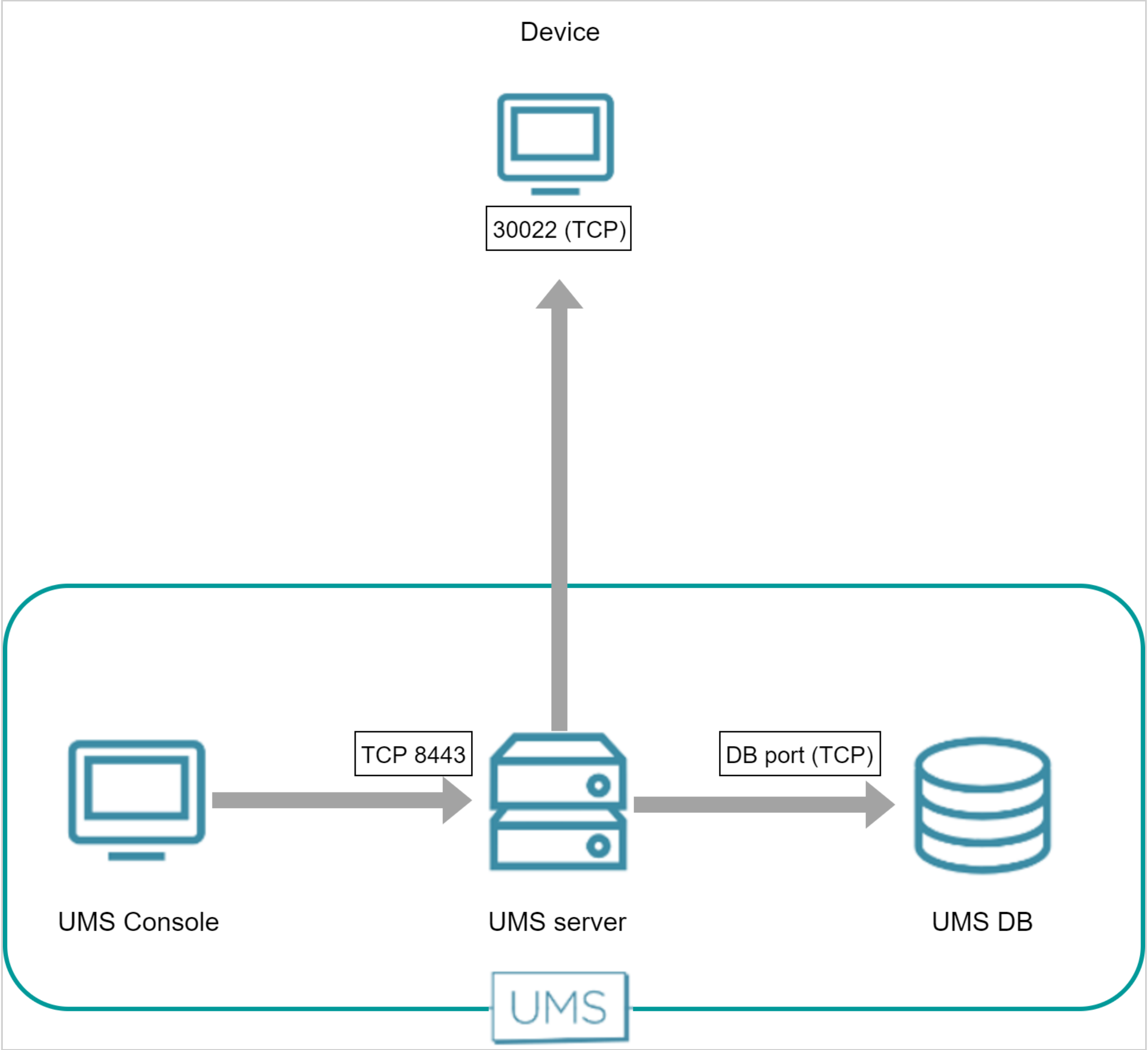

CONSOLE
UMS Console
UMS Server
ICG
Device
Before secure terminal flow
Requesting secure terminal information of the device
Secure terminal information of the device
Initiate connection (TCP 8443)
Secure terminal settings
Initiate connection (TCP 8443)
WebSocket open
Secure terminal settings
1. Request secure terminal session
2. Request secure terminal session
3. Secure terminal session information
3. Request secure terminal session
4. Start secure terminal session by opening a WebSocket tunnel
4. Start secure terminal session by opening a WebSocket tunnel
5. Secure terminal data traffic via WebSocket
5. Secure terminal data traffic via WebSocket
Legend:
: communication via unified protocol (WebSocket and REST)
: communication via secure terminal WebSocket
: communication via REST

IGEL OS 11 or Earlier

Direct Connection

The UMS Console establishes a connection to the UMS Server. The UMS Server then establishes a TLS tunnel to the device.

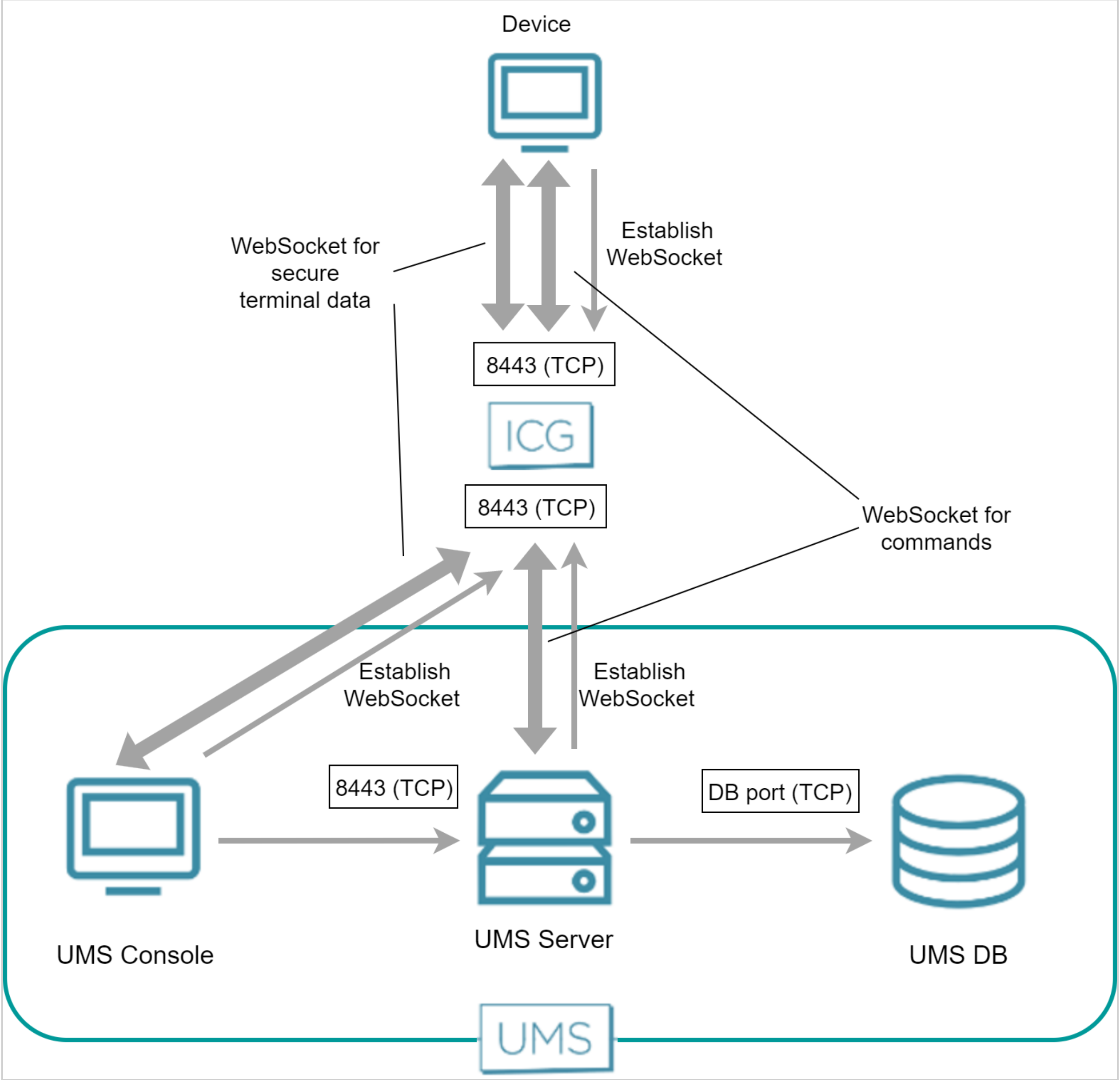
The following figure illustrates the communication between the UMS Console, the UMS Server and a device:



Over ICG

Both the UMS Server and the device have established a WebSocket connection to the ICG; this WebSocket is used for commands from the UMS and messages from the device.

The UMS Console and the device establish a dedicated WebSocket for the secure terminal with the ICG.


Device
WebSocket for secure terminal data
Establish WebSocket
8443 (TCP)
ICG
8443 (TCP)
WebSocket for commands
Establish WebSocket
Establish WebSocket
8443 (TCP)
DB port (TCP)
UMS Console
UMS Server
UMS DB
UMS

UMS and Devices: File Transfer

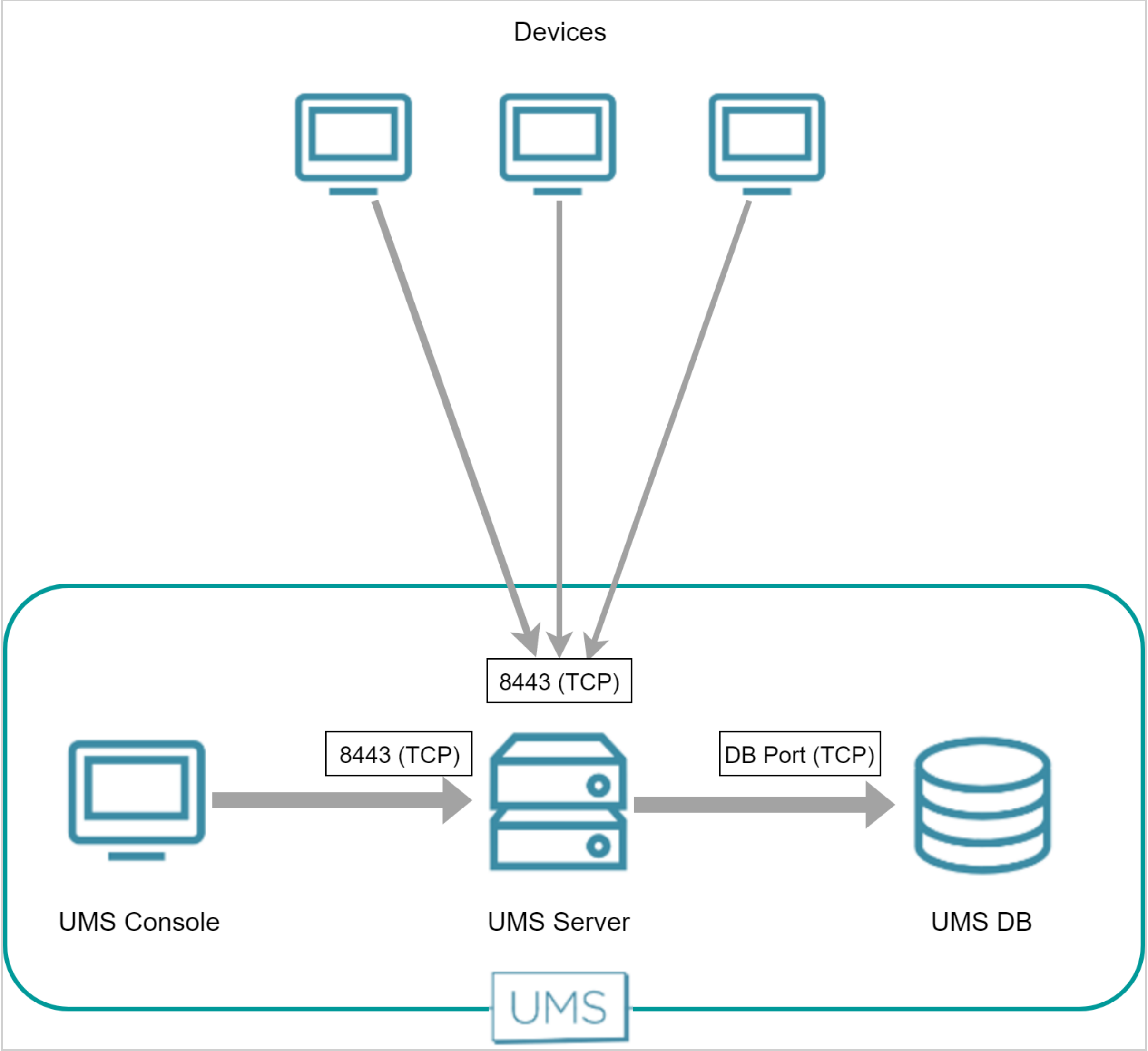
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened for the file transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

To fetch files from the UMS, e.g. a background image or log files, the devices send an HTTPS request to the UMS Server. The UMS Server is listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:



Universal Firmware Update

The Universal Firmware Update feature enables the UMS to check for new firmware updates and download the desired firmware to a WebDAV directory or FTP server. The connection to the IGEL download server can be direct or through a proxy.

For more information about this feature, see Universal Firmware Update in the UMS manual.

ⓘ The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

- UMS Contacting the Download Server to Check for New Updates (see page 124)
- UMS Downloading the Firmware (see page 127)

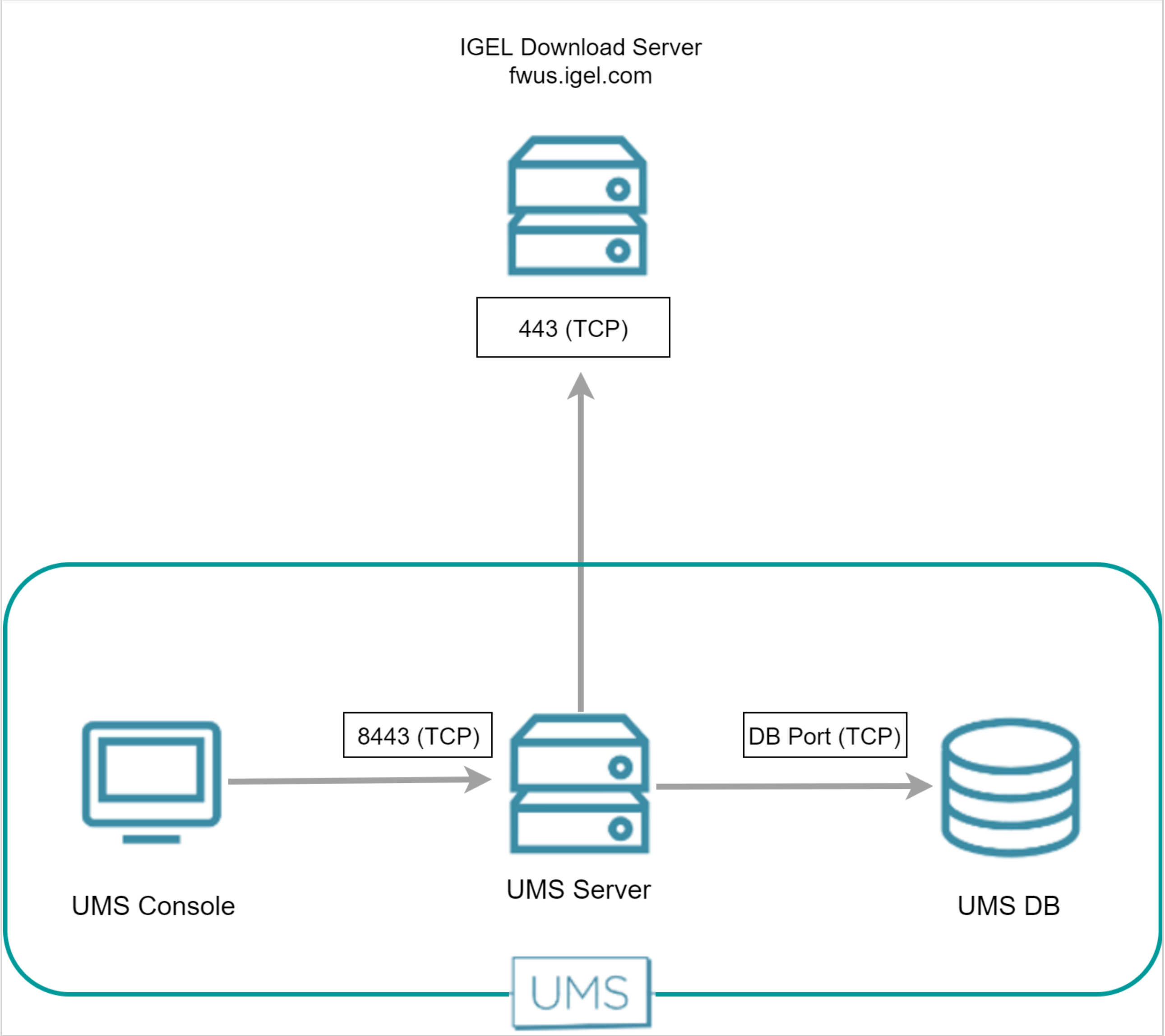
UMS Contacting the Download Server to Check for New Updates

The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

The UMS initiates a TCP connection to port 443 at fwus.igel.com. The IGEL download server will send an answer containing a list of download links that enable the UMS to download the desired firmware.

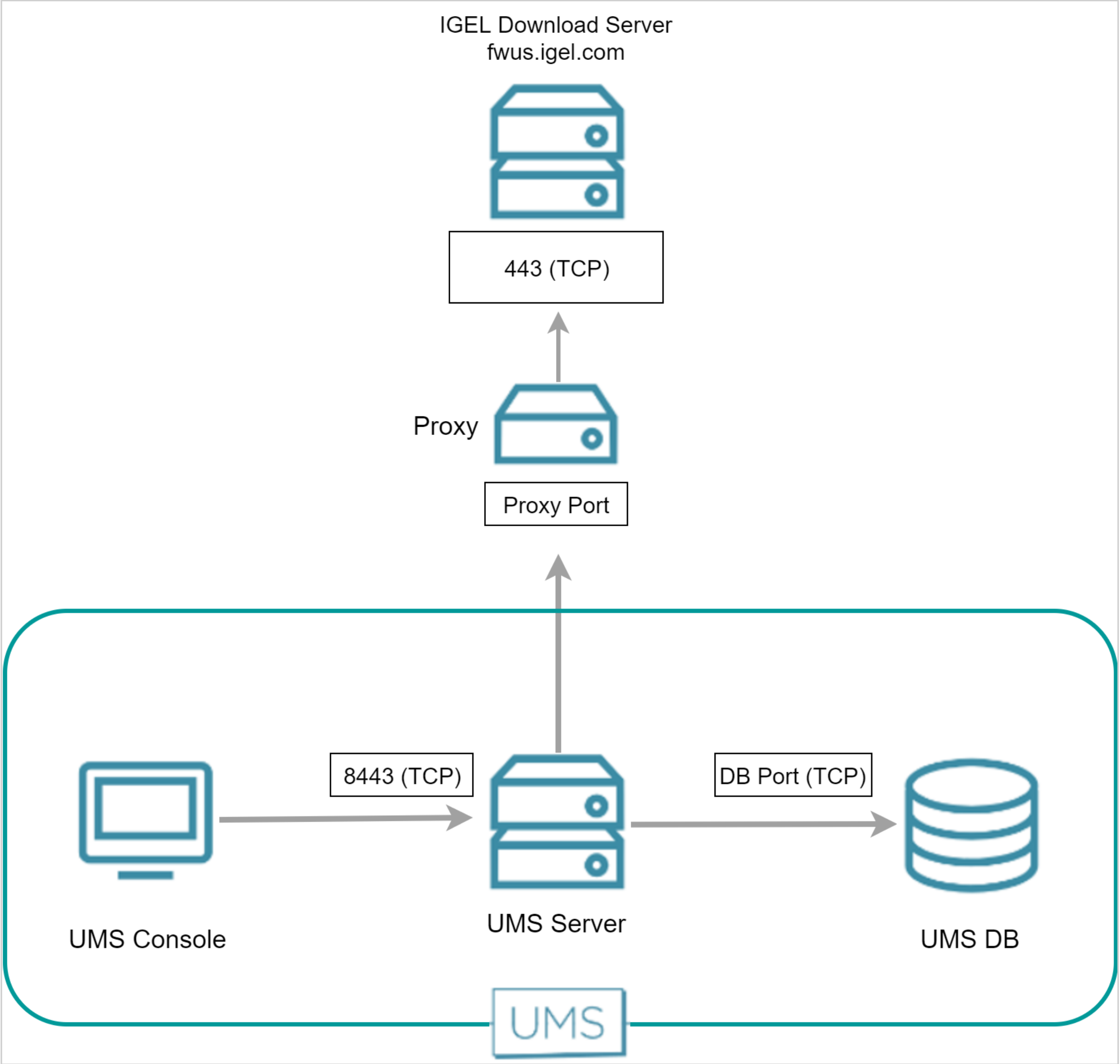
Direct Connection

The following figure illustrates the communication between the UMS server and the IGEL download servers:



Via Proxy

When a proxy is positioned between the UMS and the IGEL download servers, the port on which the proxy is listening must be specified under **UMS Administration > Global Configuration > Proxy Server**.


IGEL Download Server
fwus.igel.com
443 (TCP)
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

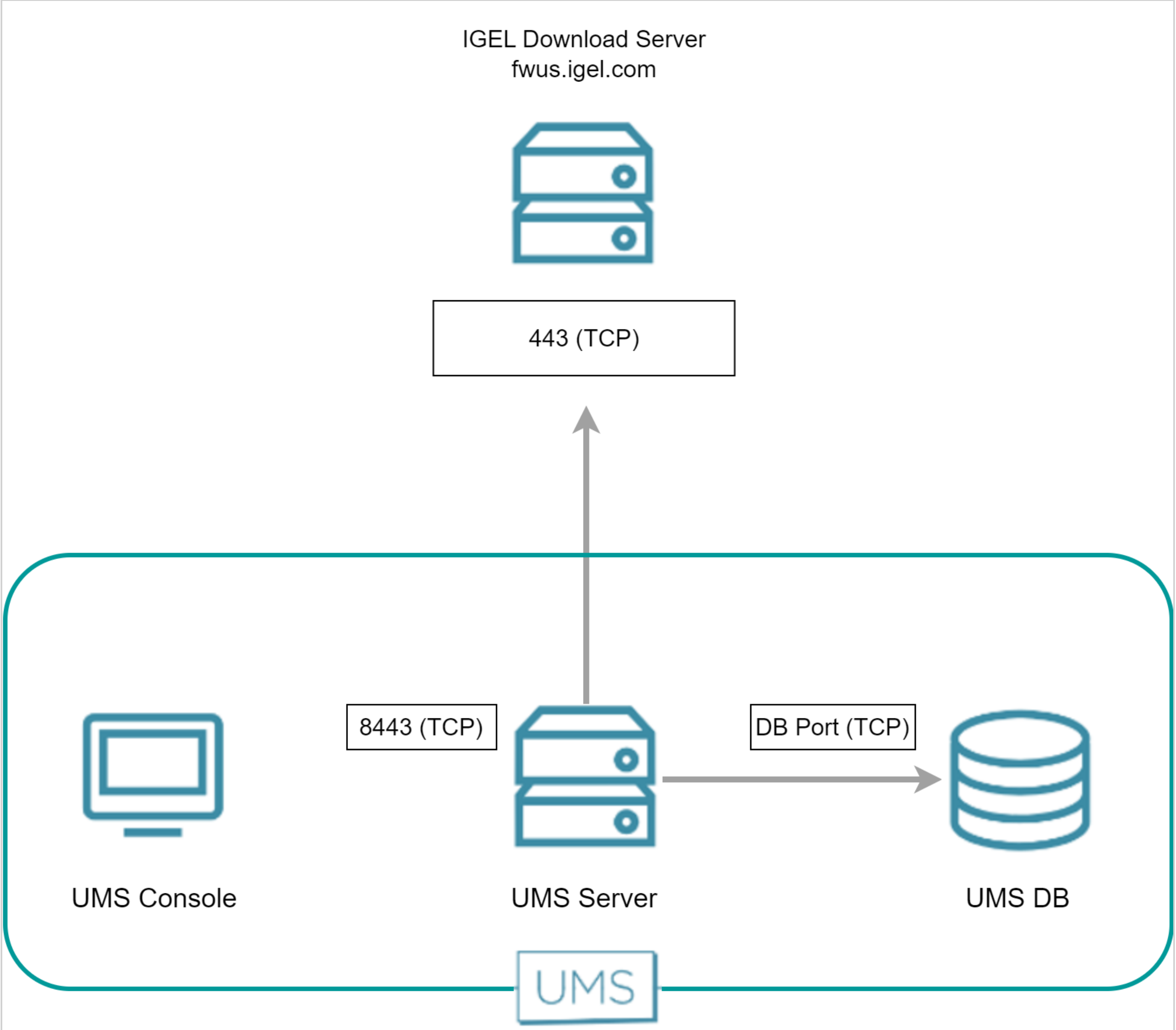
UMS Downloading the Firmware

ⓘ The Universal Firmware Update feature is relevant for IGEL OS 11 devices and earlier, not for IGEL OS 12 devices.

The UMS downloads the desired firmware using the URLs it received from the download server. The UMS uses port 443 for fwus.igel.com.

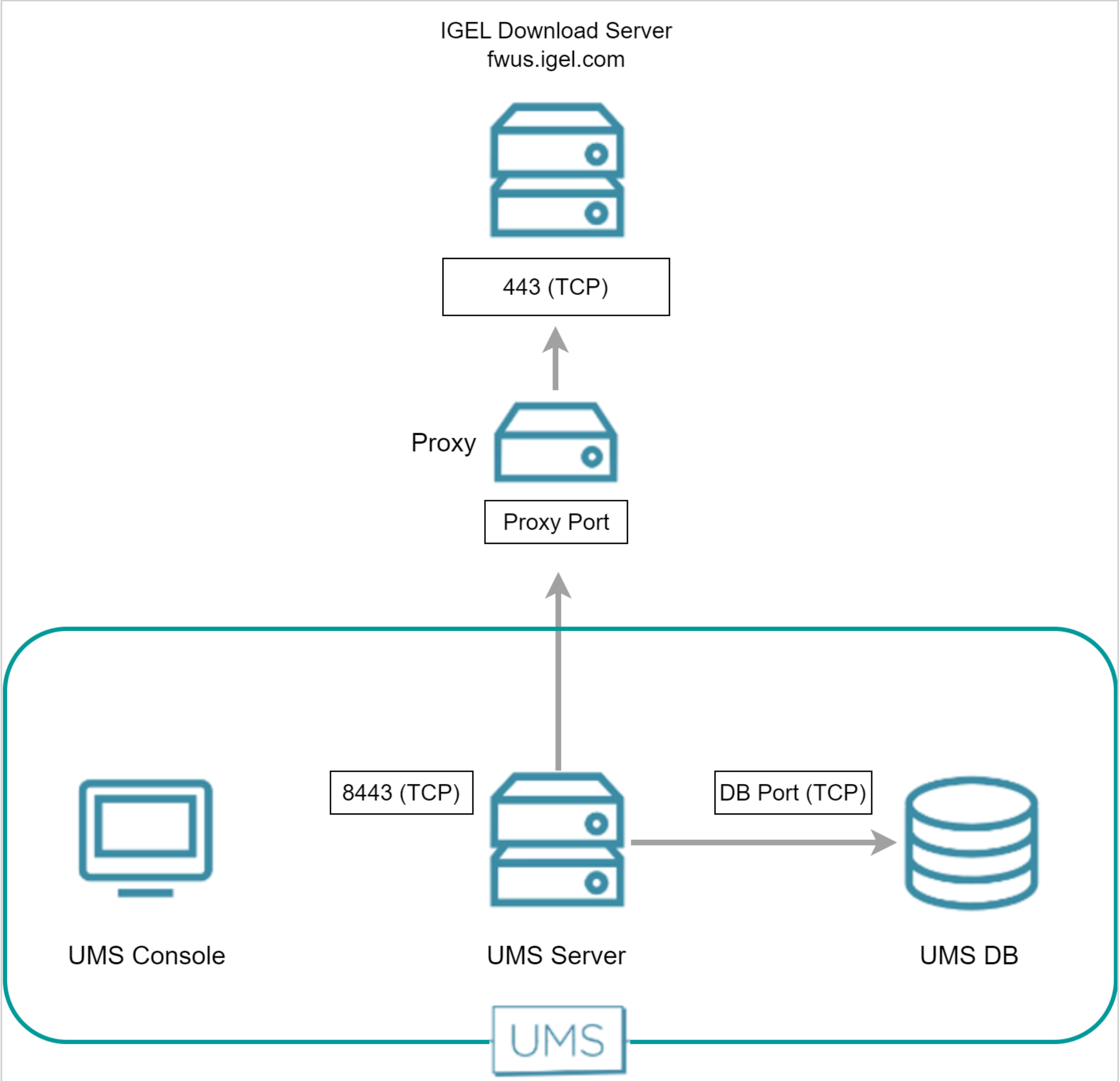
Direct Connection

The following figure illustrates the communication between the UMS Server and the IGEL download servers:



Via Proxy Server

When a proxy server is placed between the UMS Server and the IGEL download server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.



Automatic License Deployment (ALD)

The Automatic License Deployment (ALD) feature is a method to deploy licenses to devices.

For more information about this feature, see Setting up Automatic License Deployment (ALD).

Automatic License deployment can be carried out via a direct connection or via a proxy.

The steps of the procedure are described in the following sections:

- UMS Contacting the Licensing Server (see page 130)
- UMS Sending New Settings to the Devices (see page 133)
- Devices Contacting the UMS to Download License Files (see page 134)

UMS Contacting the Licensing Server

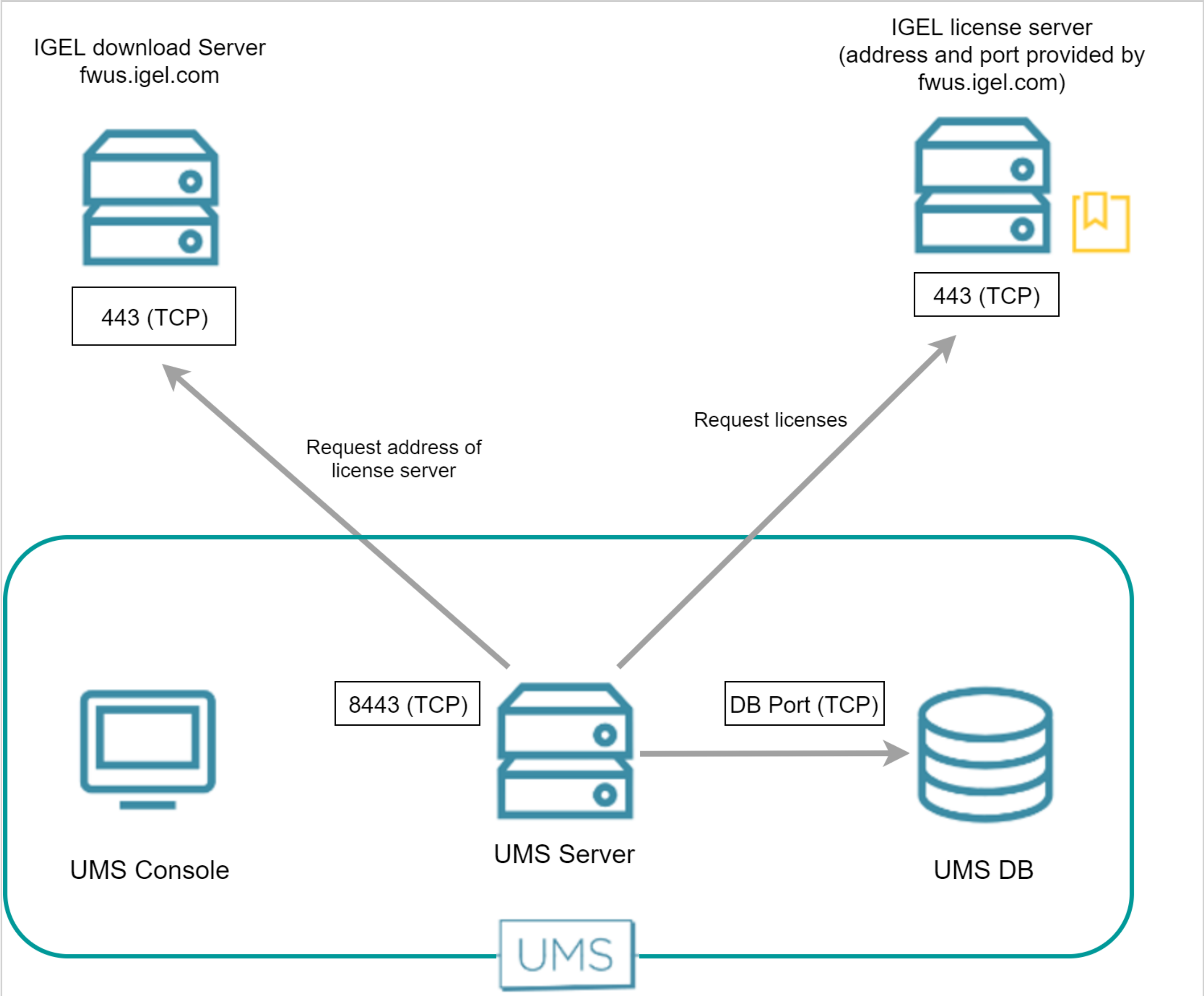
The UMS requests the connection details (URL and port) from the IGEL download server at fwus.igel.com and then contacts the IGEL licensing server. Currently, the connection details are as follows:

- URL: susi.igel.com
- Port: 443

ⓘ The connection details may be changed in the future.

Direct Connection

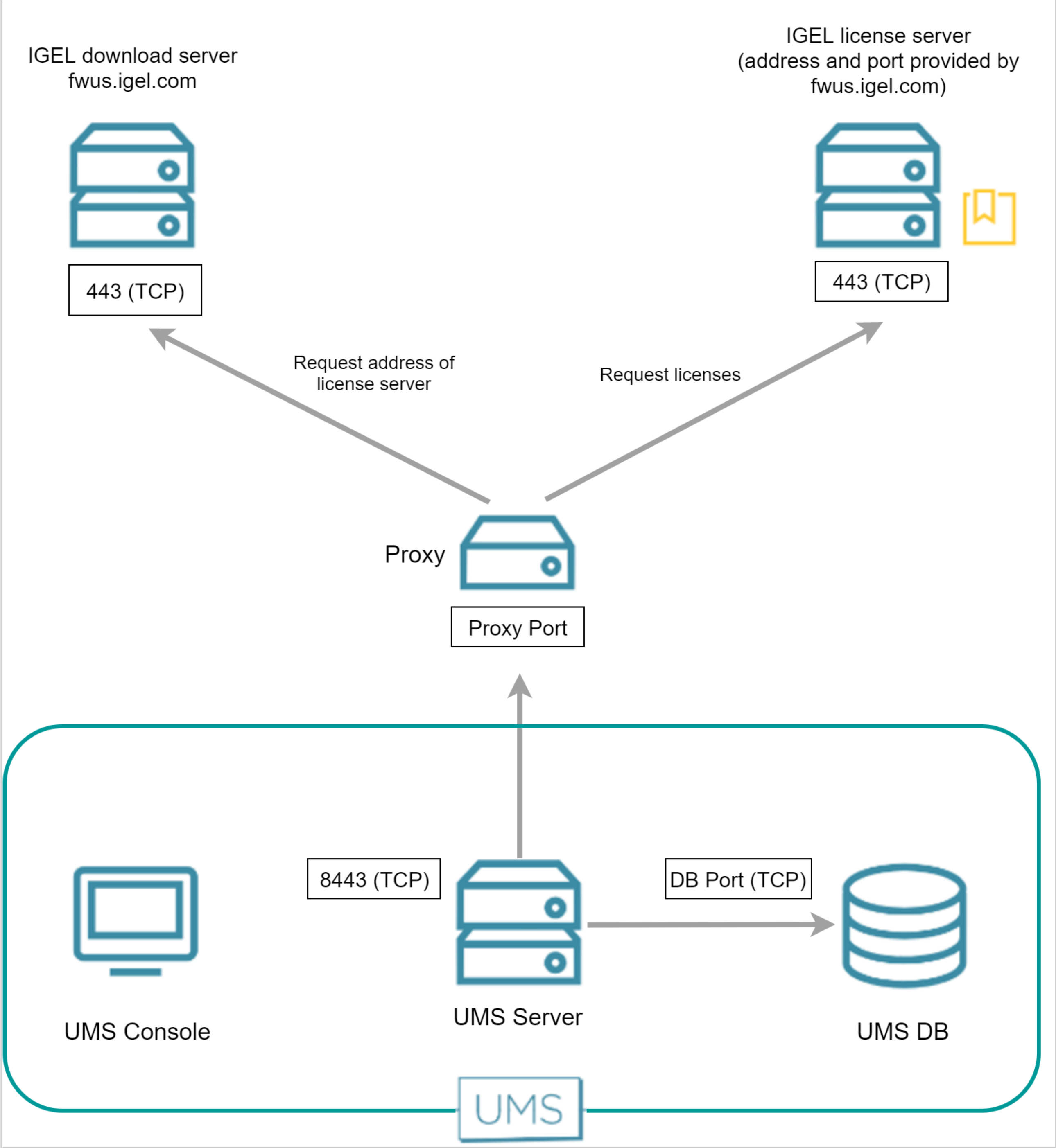
The following figure illustrates the communication between the UMS Server and the IGEL licensing server:



Via Proxy Server

When a proxy server is placed between the UMS and the IGEL licensing server, the port for the proxy server must be specified under **UMS Administration > Global Configuration > Proxy Server**.

⚠ If multiple proxies are configured, ensure to select the one that is defined for license deployment


IGEL download server
fwus.igel.com
IGEL license server
(address and port provided by
fwus.igel.com)
443 (TCP)
443 (TCP)
Request address of
license server
Request licenses
Proxy
Proxy Port
8443 (TCP)
DB Port (TCP)
UMS Console
UMS Server
UMS DB
UMS

UMS Sending New Settings to the Devices

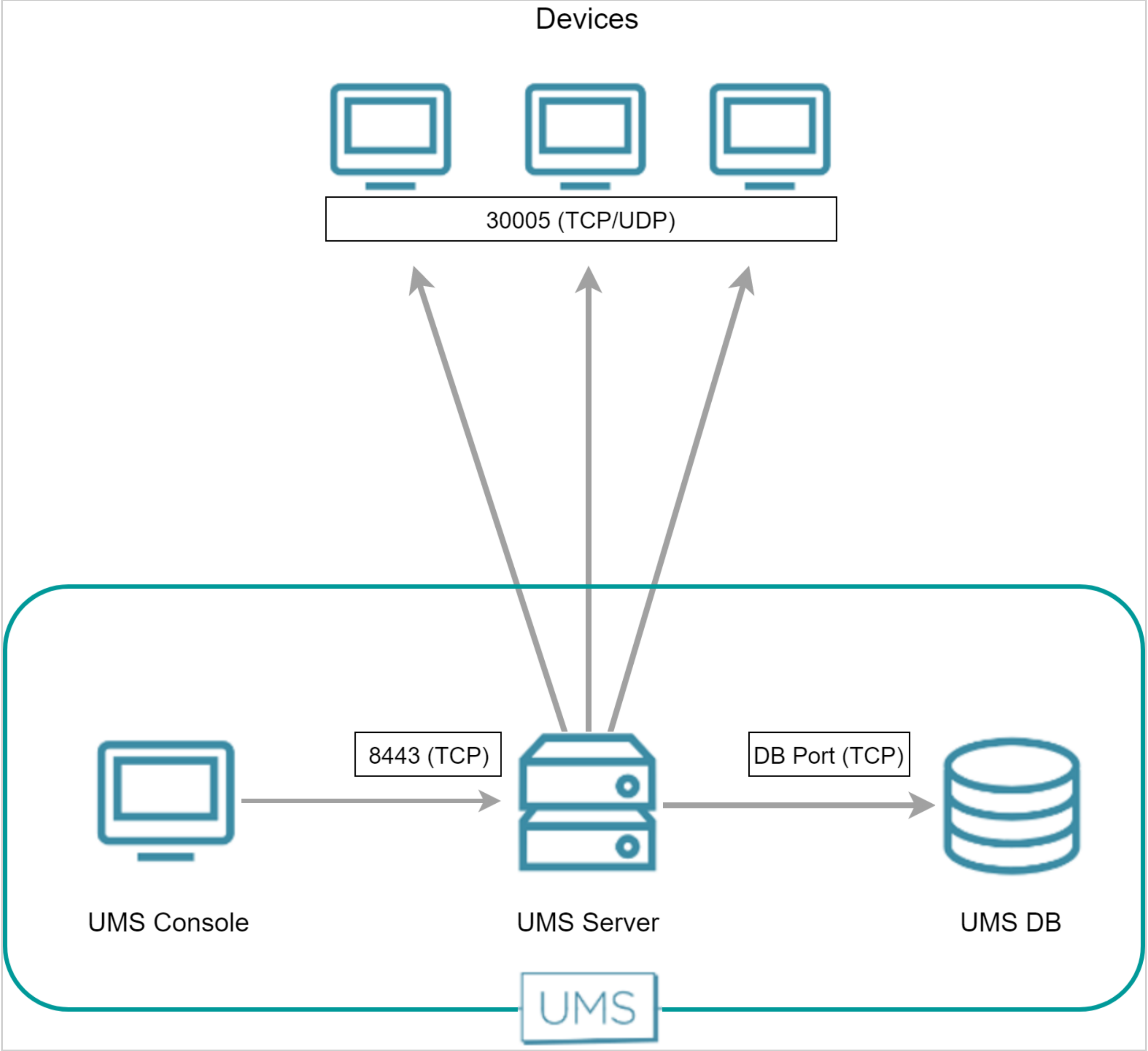
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened for the license transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

After obtaining the licenses from the license server, the UMS sends new settings to each device in question, including a download link for the license files. The device is listening on port 30005.

The following figure illustrates the communication between the UMS and the devices:



Devices Contacting the UMS to Download License Files

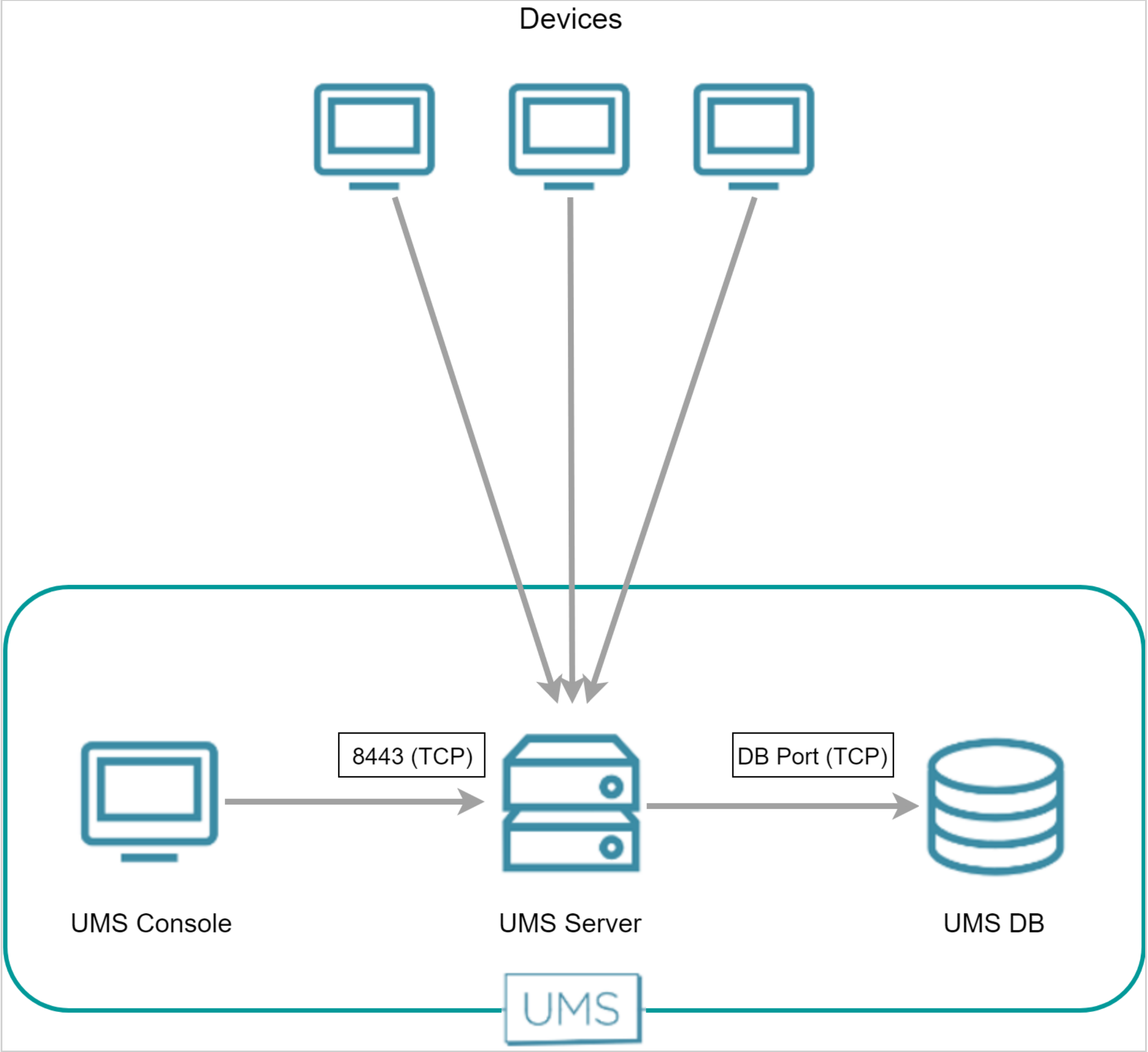
IGEL OS 12

For IGEL OS 12 devices, no additional channel is opened for the license transfer. An existing WebSocket (TCP 8443) is used.

IGEL OS 11 or Earlier

The devices have been informed by the UMS that license files are ready for download. Now, to fetch the license files from the UMS, the devices send an HTTPS request to the UMS Server. The UMS Server is listening on port 8443.

The following figure illustrates the communication between the devices and the UMS:

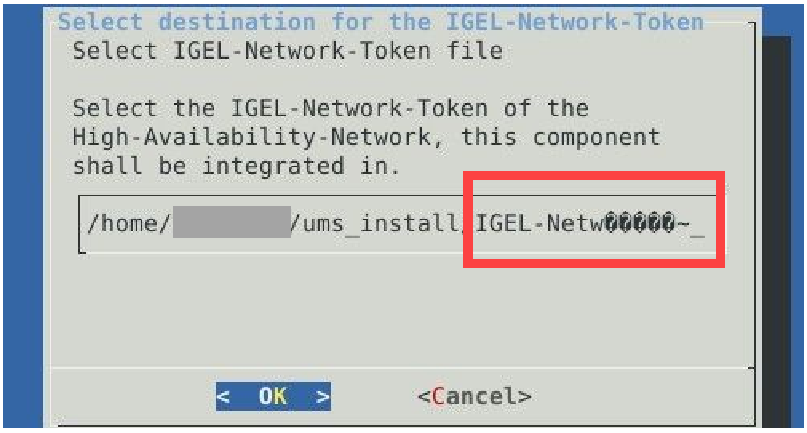


UMS Installation

Using Special Characters during the UMS Installation on Linux

Question

Why do I see strange symbols in the UMS installer on Linux, e.g. when saving / loading the IGEL network token?



Select destination for the IGEL-Network-Token

Select IGEL-Network-Token file

Select the IGEL-Network-Token of the High-Availability-Network, this component shall be integrated in.

```
/home/[redacted]/ums_install/IGEL-Netw�����~_
```

Answer

When you want to use language-specific characters, e.g. umlauts (`ä` , `ö` , etc.), for the UMS installation on Linux:

- the correct locale for the language must be set
- the system locale must also be correctly set

▶ Run the following command to list the available locales: `locale -a`

▶ If the necessary locale is not listed, you can generate and set it as the default locale for your system as follows (example for German):

```
sudo locale-gen de_DE.UTF-8
sudo update-locale LANG=de_DE.UTF-8
```

UMS Installation on 64-Bit Systems

Since version 5.09.100, IGEL UMS is 64-bit based. This article serves now for information purposes only.

Question

What are the prerequisites for the installation of IGEL Universal Management Suite on 64-bit operating systems?

Answer

Since UMS 5.09

From UMS Version 5.09, the installation of 32-bit libraries is no longer required. The necessary dependencies are automatically installed if the corresponding option has been chosen during the UMS installation procedure. For information on UMS installation, see IGEL UMS Installation.

Since UMS 5.07.100

From UMS Version 5.07.100, the required 32-bit libraries can automatically be installed by the UMS installer if the corresponding option is chosen during the UMS installation procedure.

Before UMS 5.07.100

- Windows: Use the 32-bit compatibility mode (which is activated by default) before installing IGEL UMS (e.g. on Windows Server 2008 R2).
  See also MSDN: "Running 32-bit Applications"[2]
- Linux (amd64/x86_64): Install the 32-bit compatibility packages before installing IGEL UMS.
  Examples with Ubuntu follow below, apart from that see:
  - Installing UMS on Red Hat Enterprise Linux (RHEL) 7.3
  - Installing UMS on Oracle Linux Server

Example with Ubuntu 14.04 LTS 64-bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ lib32bz2-1.0 \ libxtst6:i386 \
libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ libxrender1:i386
```

[2] https://msdn.microsoft.com/en-us/library/aa384249%28VS.85%29.aspx

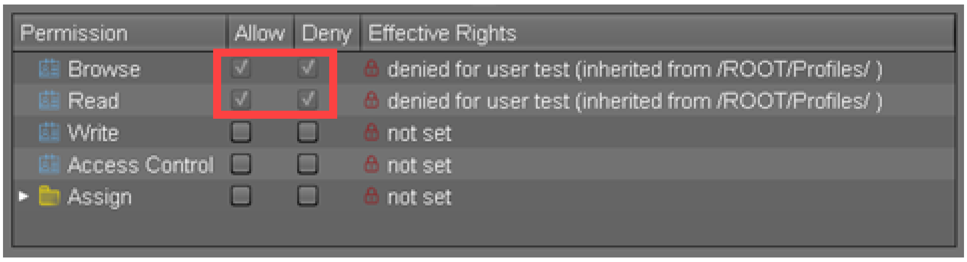
Example with Ubuntu 16.04 LTS 64-bit:

```
# add i386 support
sudo dpkg --add-architecture i386
sudo apt-get update
# install libraries
sudo apt-get install lib32z1 \ lib32ncurses5 \ libbz2-1.0:i386 \ libxtst6:i386
\ libxinerama1:i386 \ libxi6:i386 \ libxext6:i386 \ libxrender1:i386
```

No Permissions after the UMS Update

Symptom

You have updated the UMS to version 6.05.100 or higher and have no permissions for an object/tree node in the UMS anymore. In the **Access Control** dialog, both checkboxes **Allow** and **Deny** are enabled but not editable:



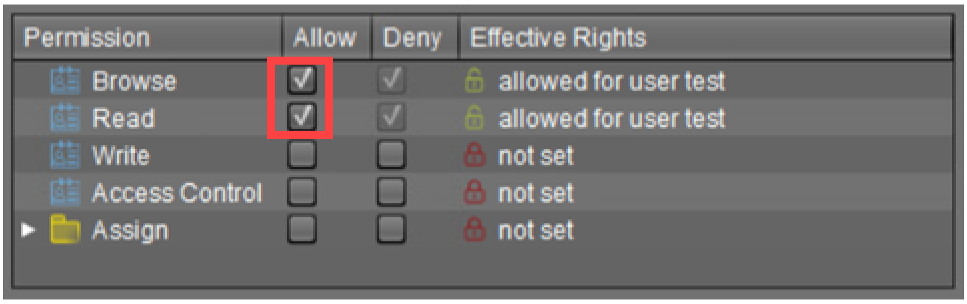
Permission	Allow	Deny	Effective Rights
Browse	☑	☑	denied for user test (inherited from /ROOT/Profiles/)
Read	☑	☑	denied for user test (inherited from /ROOT/Profiles/)
Write	□	□	not set
Access Control	□	□	not set
▸ Assign	□	□	not set

Environment

- UMS 6.05.100 or higher

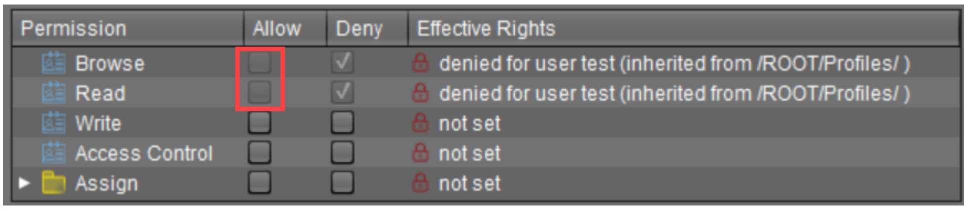
Problem

Before UMS 6.05.100, permissions could be granted for a subnode even if they were denied for a node.



Permission	Allow	Deny	Effective Rights
Browse	☑	☑	allowed for user test
Read	☑	☑	allowed for user test
Write	□	□	not set
Access Control	□	□	not set
▸ Assign	□	□	not set

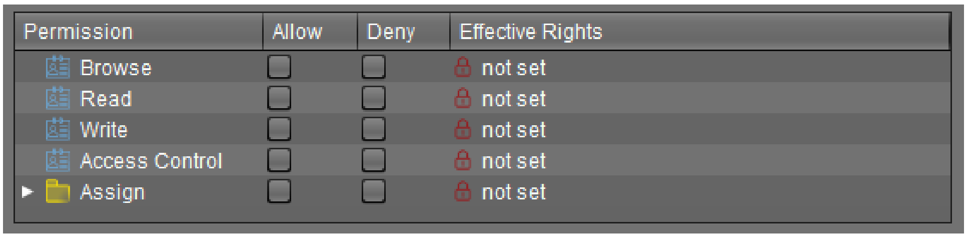
With UMS version 6.05.100, the evaluation of UMS permissions has changed: If you set **Deny** on a node, you cannot set **Allow** permission on a subnode. The **Allow** checkbox is not editable.



Permission	Allow	Deny	Effective Rights
Browse	□	☑	denied for user test (inherited from /ROOT/Profiles/)
Read	□	☑	denied for user test (inherited from /ROOT/Profiles/)
Write	□	□	not set
Access Control	□	□	not set
▸ Assign	□	□	not set

Solution

▶ Check the permissions in the **Access Control** dialog. If the **Allow** permissions should be given for a subnode, do not set any permissions for the node.



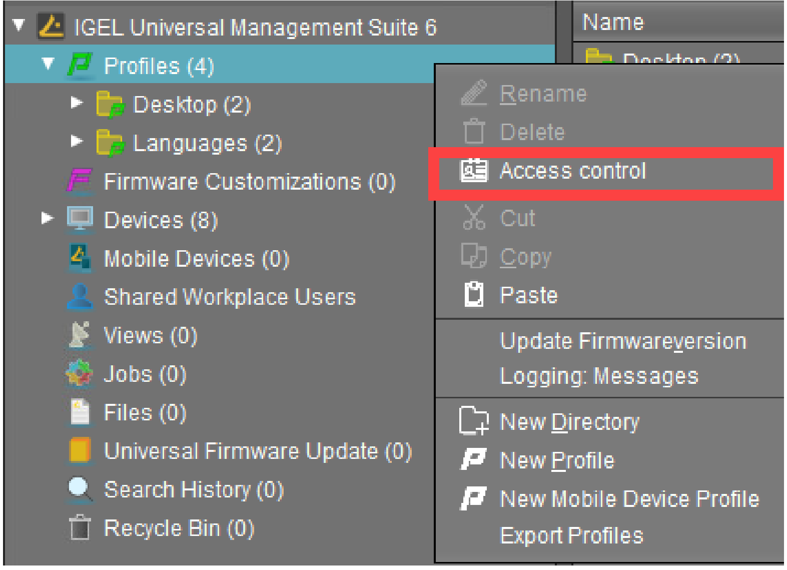
Permission	Allow	Deny	Effective Rights
Browse	☐	☐	not set
Read	☐	☐	not set
Write	☐	☐	not set
Access Control	☐	☐	not set
▶ Assign	☐	☐	not set

If the permissions are not set, the behavior is like by **Deny**. Therefore, the user will not have access rights on the node but can browse up to the subnode.

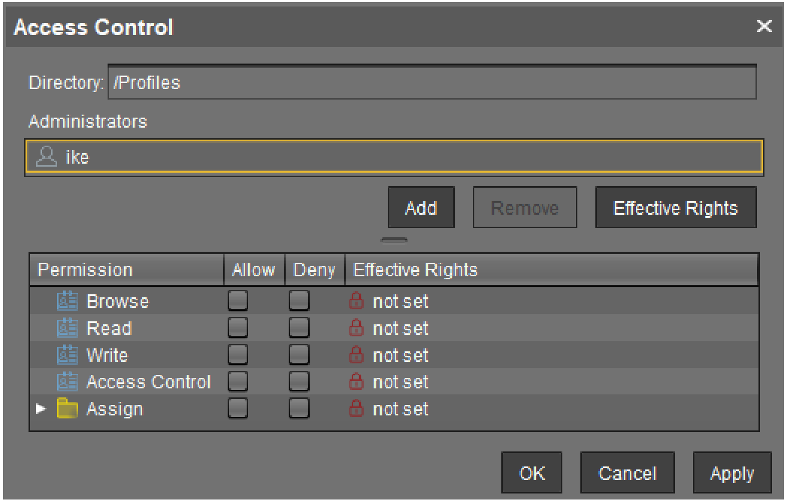
Example:

The user should have access rights only to the profile folder "Languages" and its contents:

1. Open the **Access Control** dialog for a node, **Profiles** in this case.



2. Disable checkboxes **Allow** and **Deny**.
   The **Effective Rights** read now "not set".



Access Control

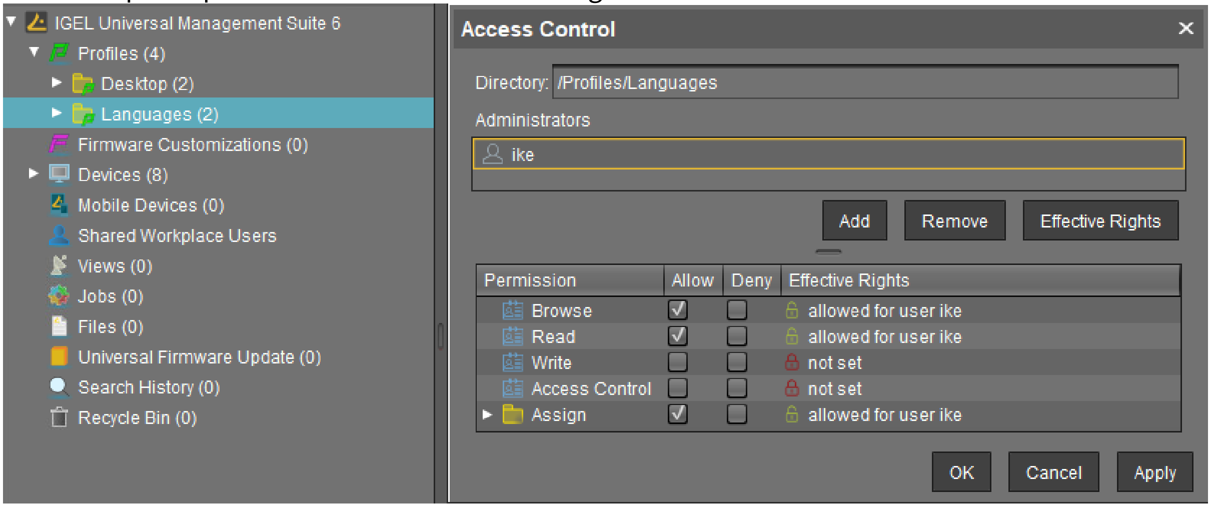
Directory: /Profiles

Administrators

ike

Permission	Allow	Deny	Effective Rights
Browse	□	□	not set
Read	□	□	not set
Write	□	□	not set
Access Control	□	□	not set
▶ Assign	□	□	not set

3. Open the **Access Control** dialog for a subnode, for which premissions should be granted. In our case, it is the folder "Languages".
4. Set the required permissions and save the settings.



Access Control

Directory: /Profiles/Languages

Administrators

ike

Permission	Allow	Deny	Effective Rights
Browse	☑	□	allowed for user ike
Read	☑	□	allowed for user ike
Write	□	□	not set
Access Control	□	□	not set
▶ Assign	☑	□	allowed for user ike

The user can only browse up to the subnode "Languages", for which the access rights have been given.

Invalid Web Certificate and Errors by Device Registration after the Installation of the IGEL UMS 12 on Linux

You have just installed IGEL Universal Management Suite (UMS) 12 or updated your existing UMS installation to UMS 12 on Linux and face now various issues, e.g. with the scanning and registration of IGEL OS 12 devices.

Symptom

After the installation of UMS 12 on Linux, you have problems with automatic or manual device registration, logging in to the UMS Web App, etc.

On the device side, you get the following error (e.g. when running the command `journalctl -f` when trying to register the device):

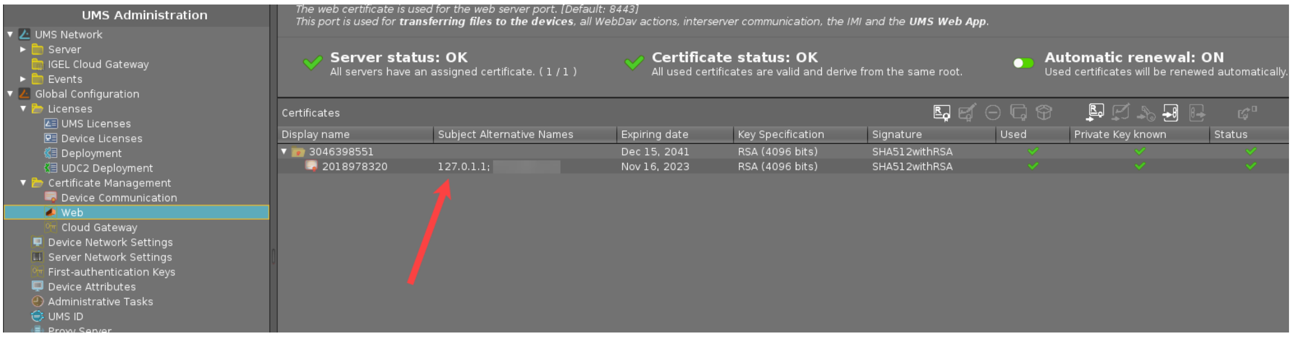
```
ERROR: Failed to verify certificate... IP address mismatch
```

Environment

- IGEL UMS 12 on Linux

Problem

For new or update installations on a Linux host, the IP address determined by the JRE can be often wrong (e.g. default IP: 127.0.1.1). If the correct IP of the UMS Server was not specified in the UMS installer during the installation / update, this will lead to invalid UMS certificates.



The web certificate is used for the web server port. [Default: 8443]
*This port is used for **transferring files to the devices**, all WebDav actions, interserver communication, the IMI and the **UMS Web App**.*

Server status: OK
All servers have an assigned certificate. (1 / 1)

Certificate status: OK
All used certificates are valid and derive from the same root.

Automatic renewal: ON
Used certificates will be renewed automatically.

Certificates

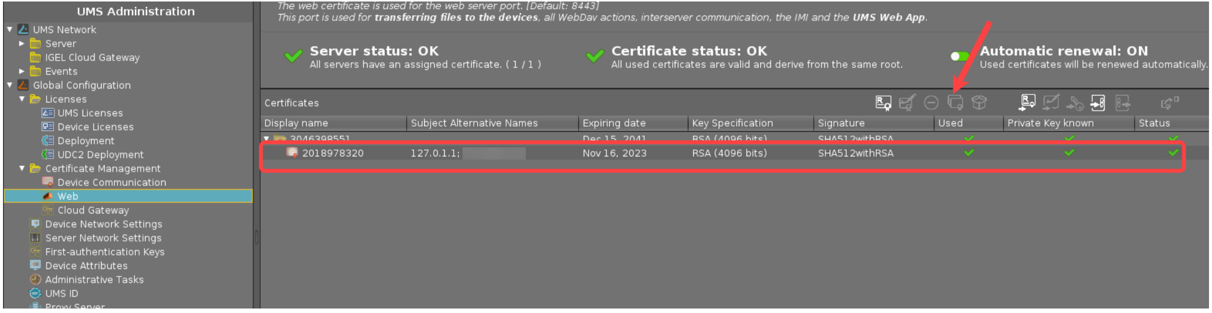
Display name	Subject Alternative Names	Expiring date	Key Specification	Signature	Used	Private Key known	Status
3046398551		Dec 15, 2041	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
2018978320	127.0.1.1; [redacted]	Nov 16, 2023	RSA (4096 bits)	SHA512withRSA	✓	✓	✓

Solution

You have to generate a new certificate:

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.

2. Select the existing certificate and click **Renew certificate** .



The web certificate is used for the web server port. [Default: 8443]
*This port is used for **transferring files to the devices**, all WebDav actions, interserver communication, the IMI and the **UMS Web App**.*

✓ **Server status: OK**
All servers have an assigned certificate. (1 / 1)

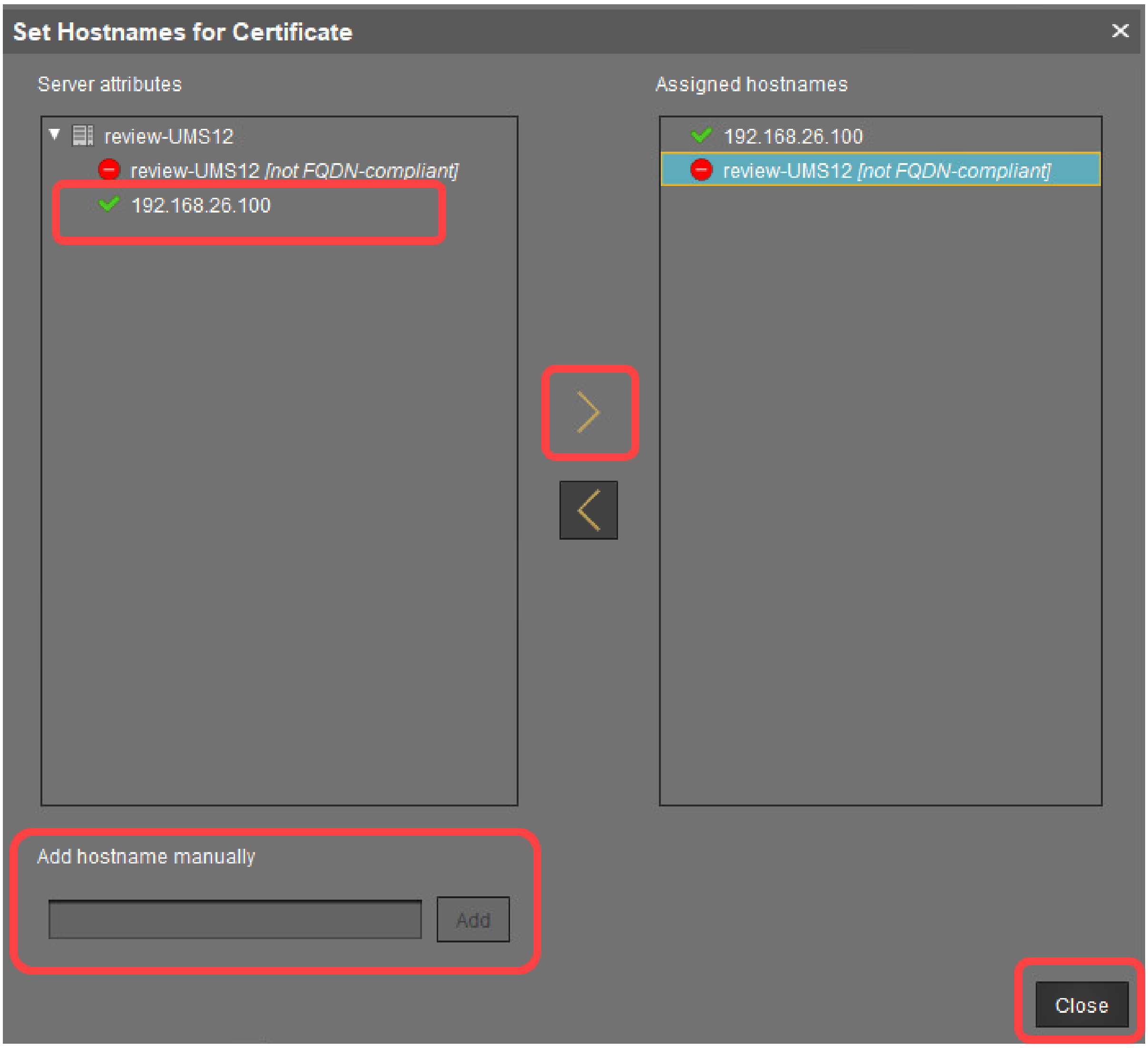
✓ **Certificate status: OK**
All used certificates are valid and derive from the same root.

Automatic renewal: ON
Used certificates will be renewed automatically.

Display name	Subject Alternative Names	Expiring date	Key Specification	Signature	Used	Private Key known	Status
3046398551		Dec 15, 2041	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
2018978320	127.0.1.1; [redacted]	Nov 16, 2023	RSA (4096 bits)	SHA512withRSA	✓	✓	✓

3. In the dialog **Create Signed Certificate**, fill in the empty fields (if there are any); all other settings can be left unchanged. Click **Manage hostnames**.

4. In the dialog **Set Hostnames for Certificate**, check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.
Note: Under **Assigned hostnames**, there must be only FQDN-compliant names. Remove all not FQDN-compliant names, if there are any, using an arrow button.


Set Hostnames for Certificate

Server attributes

- review-UMS12
  - review-UMS12 *[not FQDN-compliant]*
  - 192.168.26.100

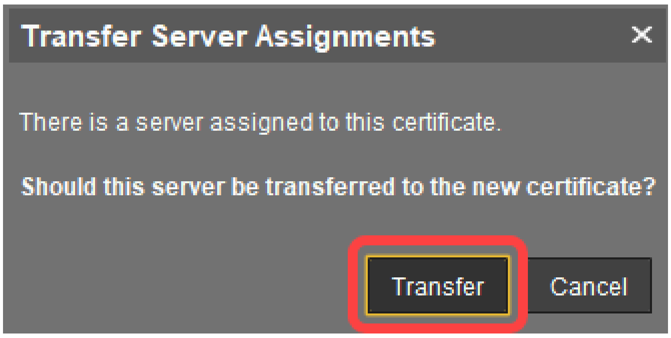
Assigned hostnames

- 192.168.26.100
- review-UMS12 *[not FQDN-compliant]*

Add hostname manually

5. Click **Ok**.

6. In the dialog **Transfer Server Assignments**, click **Transfer**.
   Note: If you are not sure, you can click **Cancel** and assign the created certificate later via **Assign server** in the context menu.


Transfer Server Assignments

There is a server assigned to this certificate.

Should this server be transferred to the new certificate?

A new certificate will be created and used for the server.

✓ It is also recommended to check the Linux OS file `/etc/hosts` and, if there are wrong entries there like 127.0.1.1, change them to the correct IP of your UMS Server and the correct server name.

Customization

User Authorization Rules

Problem

In the IGEL UMS, you want to assign permissions or roles to administrators according to various responsibilities.

Reason

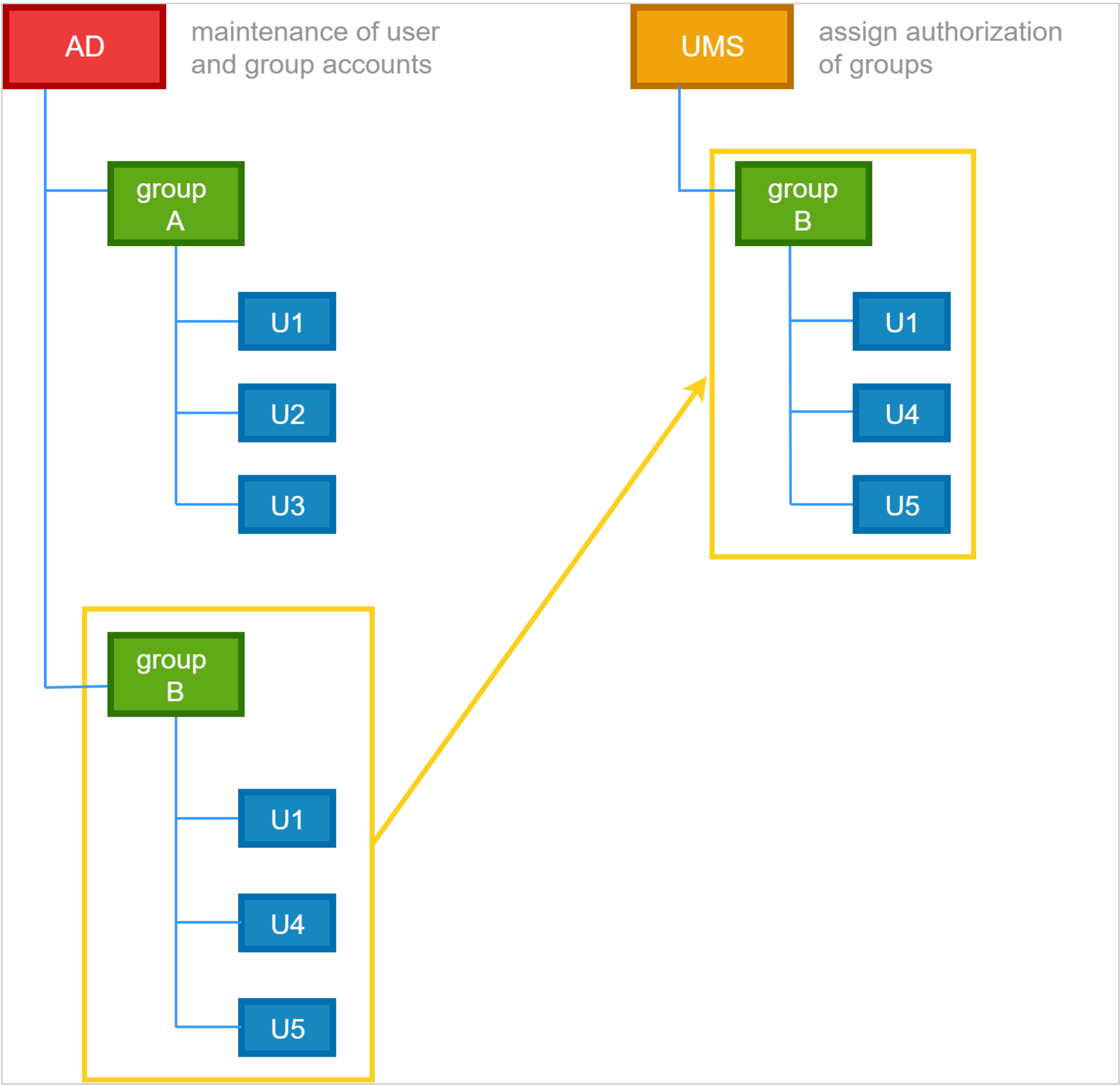
In the IGEL UMS, you can create user or administrator accounts, and you can assign rules to them, but it is not possible to assign roles.

You would like to group administrators according to their tasks in order to achieve a clearly structured management of user rights.

Within your company you already maintain employee accounts using an Active Directory or LDAP.

Solution

As best practice, we suggest connecting the UMS with the user accounts of the Active Directory. You maintain the user and group accounts in the Active Directory only. In the UMS, you assign rights to the imported groups.


AD
maintenance of user and group accounts
UMS
assign authorization of groups
group A
U1
U2
U3
group B
U1
U4
U5
group B
U1
U4
U5

Transferring Active Directory groups to the UMS and assigning permissions and roles to them:

▶ Click **UMS Administration > Global Configuration > Active Directory / LDAP** to integrate your Active Directory.

ⓘ You may import Administrative Users / UMS administrators from an Active Directory as well as from an LDAP.

▶ In the UMS console click **System > Administrator accounts > Import**, to import groups from the tree of your Active Directory.

ⓘ The successful import of a group cannot be undone. You have to manually delete the wrongly created UMS group in the "Administrator account" management. The name of the imported Active Directory group is taken from the account.

▶ Assigning roles to groups in the IGEL UMS on the basis of authorization rules:

- Click **System > Administrator accounts > Groups > Edit** to directly assign general group rights.
- Assign object-related access rights via object permissions, choosing **Access Control** in the context menu of any object.

This way, you can assign certain roles to administrators of the UMS according to their group memberships.

Please note:

- Permissions are inherited from a parent directory to a child directory or to a subordinated object.
- It is possible to change indirect rights, i.e. rights which are given by group assignment. However, directly assigned rights take precedence over indirectly assigned rights.
- An administrator can be a member of different groups and receives the corresponding rights. If they are contradictory, the deprivation of a right takes precedence over the permission. If a prohibition for an action or an object of a group is issued, it will override any number of rights from other groups.
- Click **Effective Rights** to get more details about the rules collection, for example if a permission was given directly or if it was assigned by a group or by an inheritance within a tree structure.

Managing User Permissions via UMS

Purpose

It is necessary to globally manage the permissions of the thin client users, e.g. for editing system information.

Solution

Use the **Access Control** function in the UMS.

Additional Information

There are different places where to open the **Access Control** dialog:

- In the main menu under **Edit > Access Control**
- In the symbol bar under
- In the context menu of a thin client or a thin client folder under **Access Control**

Defining end user permissions:

1. Click **Access Control** in the context menu of a thin client (folder).
   The **Access Control** dialog opens.
2. Click **Add** to select a new user/group.
3. The corresponding **Effective Rights** will be listed in the lower part of the mask.
4. **Allow** or **Deny** the permissions of the selected group or user for the selected thin clients.
5. Confirm the settings with **OK**.

6. Click the **Refresh** button of the console to apply the changes in the UMS.

   ⓘ If you have changed the rights of registered users they only take effect after a refresh.

   For further details about authorization rules see our How-To IGEL UMS: User Authorization Rules (see page 147).

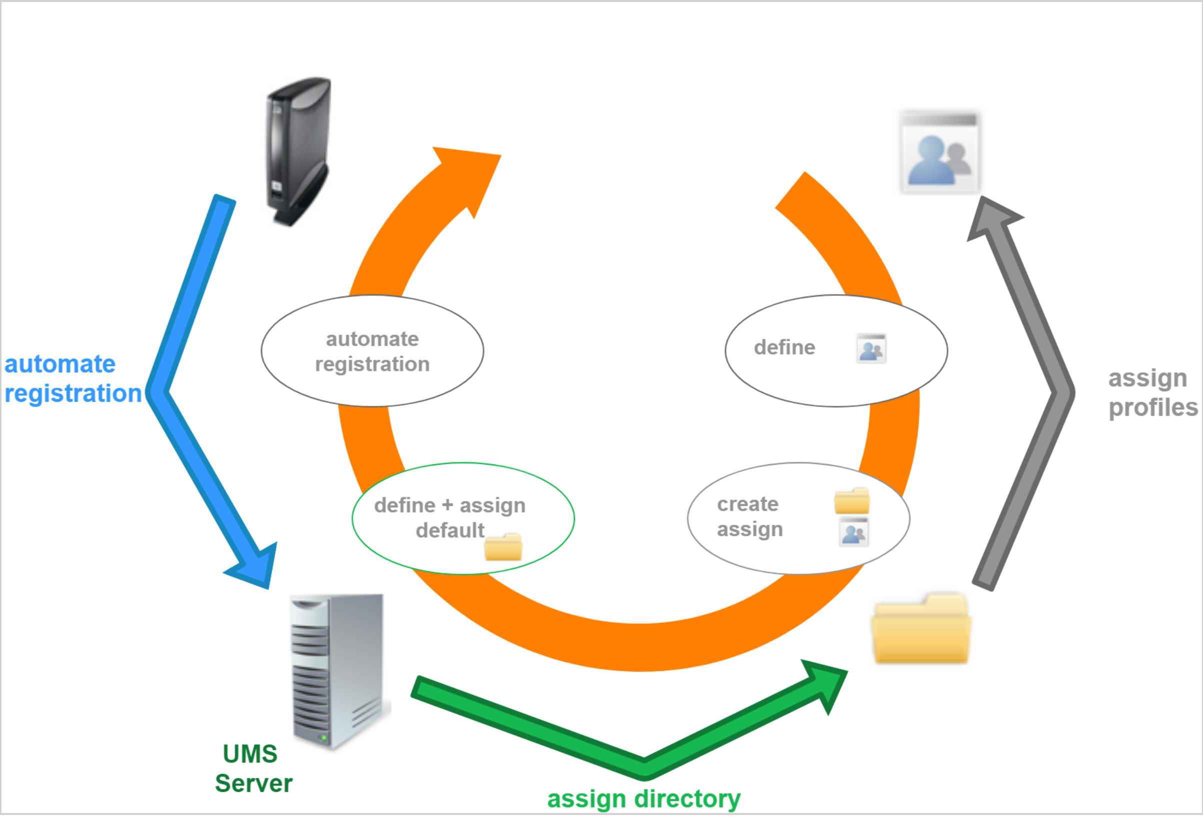
ⓘ Access rights to objects or actions within the *IGEL* UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

Automating the Rollout Process in the IGEL UMS

You want to set up the IGEL Universal Management Suite (UMS) in such a way that new devices will be stored directly in the correct directory and the right configurations will automatically be assigned to them. With Zero Touch Deployment in the rollout, devices will be configured automatically according to the profiles, with almost zero management outlay.

The idea of Zero Touch Deployment means automatic device registration with automatic assignment of profiles by default directory rules.

In the end, the device will automatically be registered in the UMS, assigned to the right directory, and related to the valid profiles. To prepare this automated process, you have to go the other way around. First, define the profiles, then assign them to the directories, then create default directory rules and automate the registration.



Preparing Automatic Rollout

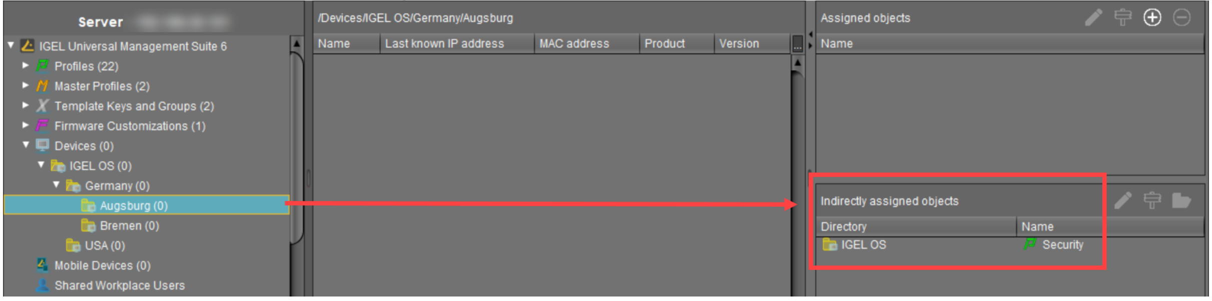
Configure your device globally, indirectly assigning profiles by a parent directory:

1. Create a new root directory, e.g. **IGEL OS**.
   For how to create a device directory, see Creating a Directory in the IGEL UMS.

2. Assign certain profiles to this root directory, e.g. **Security**.
   For how to assign profiles, see How to Allocate IGEL UMS Profiles. See also Prioritization of Profiles in the IGEL UMS.
   For detailed information on profiles, see Profiles in the IGEL UMS.

3. Move your devices or your directories containing devices to this root directory.
   These devices will inherit the profiles assigned to the root directory.

   Example: Devices that will be placed to the directory **Augsburg** during the registration will inherit the profile **Security** which is assigned to the root directory **IGEL OS**:

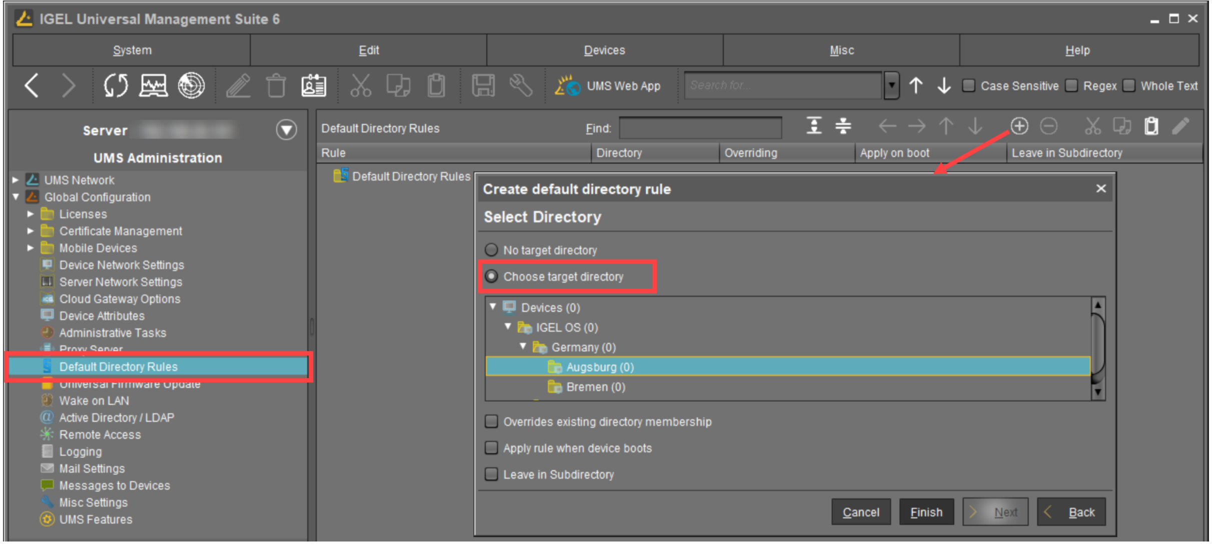


Directory	Name
IGEL OS	Security

Automating the Rollout

1. Click **UMS Administration > Global Configuration > Default directory rules** to create a new default directory rule.
   For detailed information on default directory rules, see Default Directory Rules.

2. Choose the directory in which you want to store the devices according to the rule.

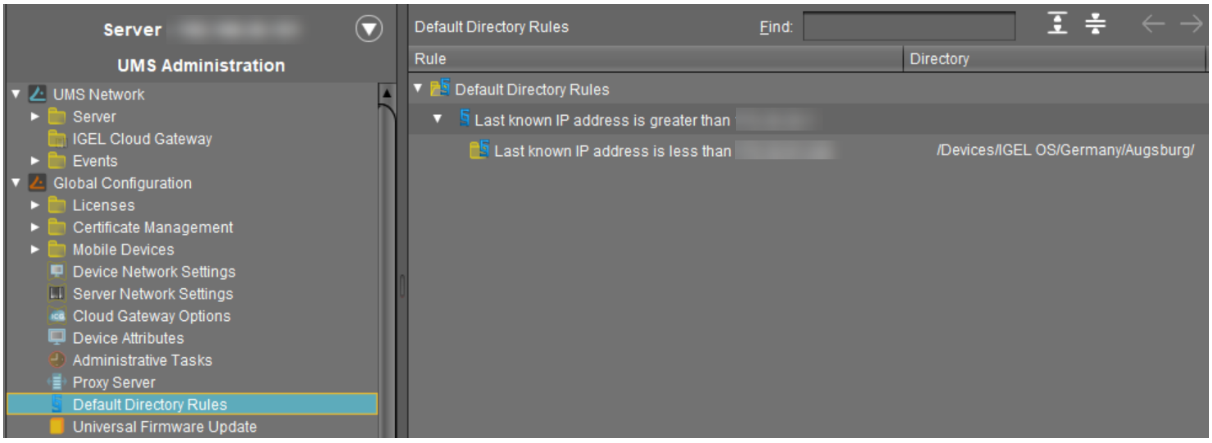


Create default directory rule

Select Directory

○ No target directory
● Choose target directory

□ Overrides existing directory membership
□ Apply rule when device boots
□ Leave in Subdirectory



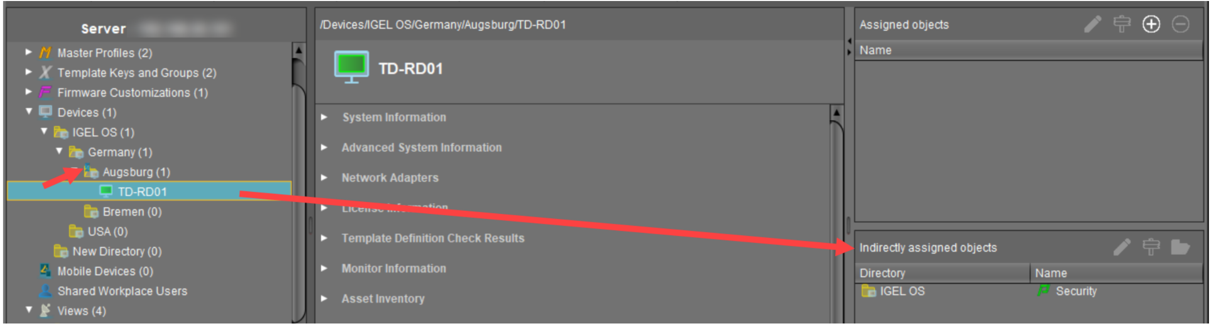
Rule	Directory
Default Directory Rules	
Last known IP address is greater than [redacted]	
Last known IP address is less than [redacted]	/Devices/IGEL OS/Germany/Augsburg/

3. Configure your DNS or DHCP server and activate the automatic registration of devices as described under Registering Devices Automatically on the IGEL UMS.

> ⓘ We recommend disabling automatic registration after the rollout, so that no unknown devices will be registered without your control and could obtain sensitive settings.

4. Start your devices. They will be automatically registered on the UMS Server.
Thanks to the default directory rule, these devices will be stored in the right directory and will automatically receive the correct profiles.

Example:



Directory	Name
IGEL OS	Security

Related Topics

If you want to use structure tags for automating the rollout: Using Structure Tags with IGEL OS 11 Devices (see page 154)

If you have problems with the device registration: Troubleshooting: Registration of a Device via Scanning for Devices Fails (see page 258)

Using Structure Tags with IGEL OS 11 Devices

Problem

When rolling out devices automatically it can be difficult to assign each to the desired folder in the Universal Management Suite (UMS).

Goal

Newly registered devices will automatically have the information where they are to be placed in the structure tree of the UMS.

The UMS will have flexible rules to place a newly registered device into a folder of the structure tree.

Solution

One solution is using a structure tag, a text string bound to the device, that is transmitted to UMS. It can be assigned to devices either via a DHCP option or in their local setup.

1. Define a Structure Tag in your Default Directory Rules under **UMS Administration > Global Configuration > Default Directory Rules**.
   Learn more in the UMS manual: Default Directory Rules.
2. Assign a structure tag to a device manually or via DHCP:
   Assigning a Structure Tag manually on the endpoint
   a. In **Setup**, go to **System > Remote Management**.
   b. Enter the structure tag value under **Structure tag**.
   c. Click **OK**.
   Assigning a Structure Tag via DHCP Server

   Use the appropriate DHCP option, depending on the IGEL OS version of your endpoint devices:

   - IGEL OS 11.03.500 or lower: Use DHCP option 226 to distribute the tag value to the devices. Set the DHCP option 226 as a string - not as a DWORD.
   - IGEL OS 11.04.100 or higher: As an alternative, you can use the DHCP option 43 (encapsulated vendor-specific options) to send the DHCP option 226 (name: "umsstructuretag") to the right endpoint devices. An endpoint device with IGEL OS 11.04.100 or higher sends option 60 (vendor class identifier) with `igel-dhcp-1` as the value.

     > ⓘ An IGEL specific DHCP option that is sent in DHCP option 43 overrides a corresponding DHCP option that is sent in the global namespace. The DHCP options 1, 224, and 226 can be embedded in option 43.
     > You can prevent a DHCP option 226 that has been sent in the global namespace from being interpreted. To achieve this, you must add option 1 (name "exclusive", type Byte, value 1) to DHCP option 43.

Deploying an IGEL made Custom Partition via UMS

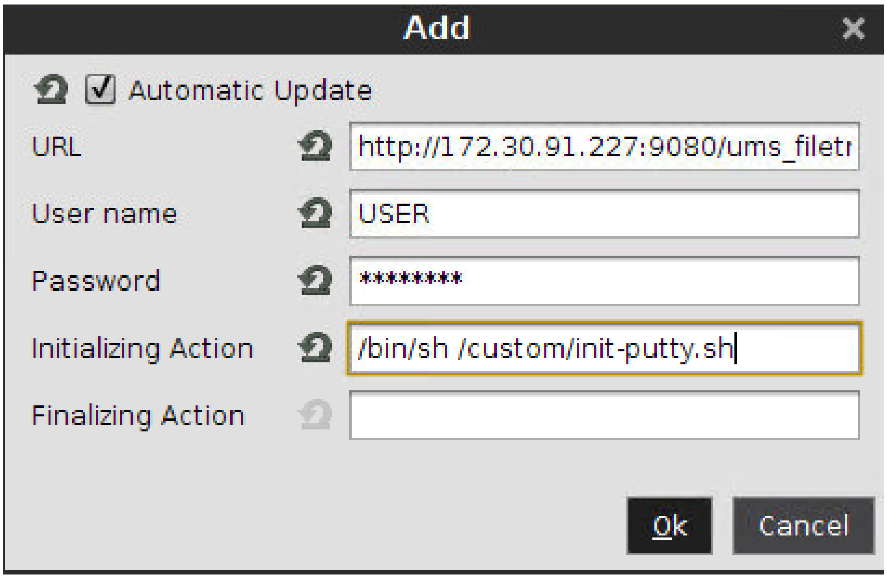
Goal

You want to deploy a custom partition that you received from IGEL to a number of thin clients via the Universal Management Suite (UMS).

Solution

> The procedure described here is only intended for installing custom partition packages that have been built by IGEL.

1. Save the `*.zip` archive you received locally and extract it.
2. Copy the contents of the directory `target` into the `ums_filetransfer` directory on the UMS Server, e.g. `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer`
3. Check the accessibility of the data by opening its address in a web browser, e.g. `http://[ums_server]:9080/ums_filetransfer/[name]/[name].inf`
   This access is password-protected, and you need to enter your UMS credentials.
4. Import the file `profiles.zip` (located in the `igel\profiles` directory of the package) into the UMS via **System > Import > Import Profiles**.
   The imported profile should now appear in the UMS Console under **Profiles**.
5. Edit the profile and adapt the settings in **System > Firmware Customization > Custom Partition > Download** to match the **URL**, **Username** and **Password** for your UMS.



☑ Automatic Update

URL: http://172.30.91.227:9080/ums_filetr

User name: USER

Password: ********

Initializing Action: /bin/sh /custom/init-putty.sh

Finalizing Action:

6. Assign the profile to one or more devices.
7. Reboot these devices.

UMS Environment

Migrate a UMS Server

If you want to migrate your IGEL Universal Management Suite (UMS) to a new server, here you find the instructions, recommendations and tips about the migration process.

Instructions for Migration Scenarios

You can find detailed instructions for the following migration scenarios:

- Migrating the UMS server and keeping the same embedded data source: Migrate a UMS Server with the Same Embedded Database (see page 160).
- Migrating the UMS server and keeping the same the external data source: Migrate a UMS Server with the Same External Database (see page 164).
- Migrating the UMS and changing the data source: Migrate a UMS Server with a Different Database (see page 168).

Recommendations and Tips

⚠ **Recommendations**

- Keep the migration and the update procedures separate. If you want to move from UMS 12.01 to 12.03, first update the UMS and migrate the server afterward, or vice versa.
- Use the same UMS ID.
  The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.
- Use the same certificate chain.
  If it must be changed, use the old chain for migration and change it after the migration successfully worked or change it before migrating.

✓ **Tip**

The move provides an opportunity to remove any UMS database data which are no longer used. For example, you can

- delete endpoint devices that no longer exist.
- delete profiles that are no longer used.
- remove files and firmware updates that are no longer needed.

It is highly recommended to create a backup before carrying out the cleanup (as a backup of the system running) and another one after the cleanup.

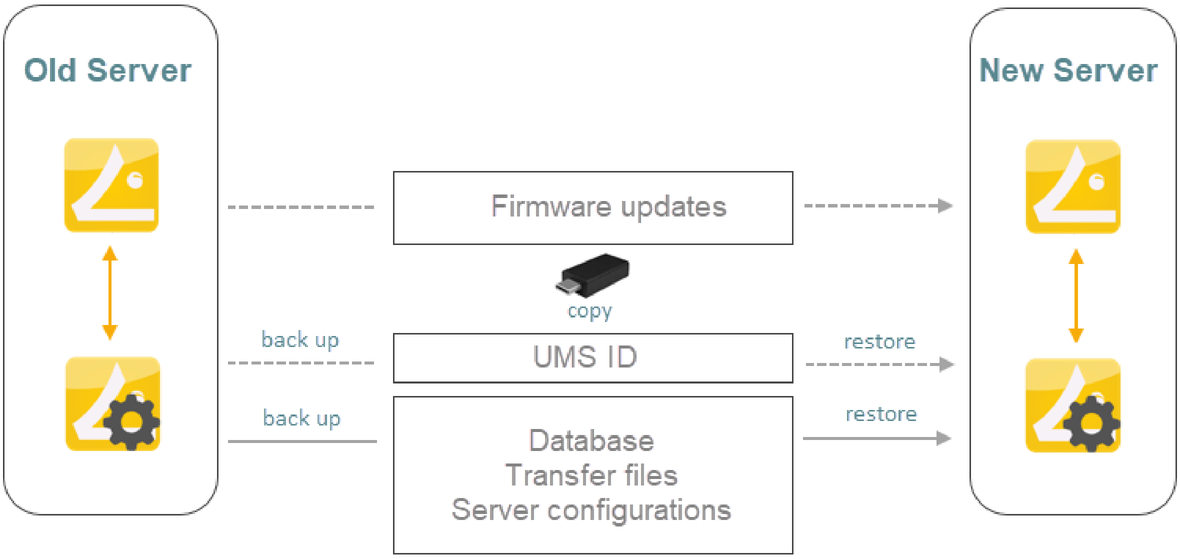
ⓘ During the migration, there will be no negative impact on your endpoint devices – they will continue to work autonomously. Exception: login via Shared Workplace (SWP). For details, see Which Features of IGEL OS Will Be Affected If the UMS Is Down?.

Migrate a UMS Server with the Same Embedded Database

Use Case

You have a UMS installation with an embedded database and want to migrate to a new UMS Server with the same embedded database.

General Overview of the Migration Procedure



The migration procedure generally involves the following steps:

1. Setting the IP address of the new server through profiles (only necessary, if devices find the UMS via IP)
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Backing up the old server. Checklist for the backups:
   ✓ **Database**
   ✓ **Transfer files**
   ✓ **Server configurations** (host-specific server configurations that differ from the defaults are noted down separately)
   ✓ **Firmware updates**
   ✓ **UMS ID**
4. Transferring the created backups to the new server
5. Adjusting DHCP tag and DNS alias on the new server (only necessary, if devices find the UMS via DNS/DHCP)

Instructions

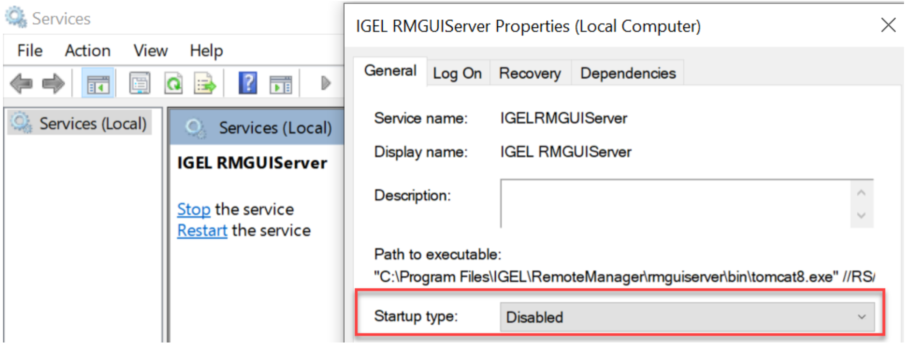
On the Old Server

1. If the devices find the UMS via the IP address, they can only connect to the new server if the IP address of the new server is set before the migration. To set the IP address:
   a. Create an OS 11 and an OS 12 profile with the new UMS server IP. The new server needs to get listed under **System > Remote Management**. For more information, see Remote Management and Remote Management.

   b. Assign the profiles.

   c. Check that all devices got their settings by creating a view with the **Last Boot Time** criterion under **Views**. For more information, see How to Create a New View in the IGEL UMS.

2. Stop the service `IGEL RMGUIServer` (for instructions, see IGEL UMS HA Services and Processes`)` and set the startup type for it to **Disabled** in order to prevent accidental parallel operation with the new UMS Server.



Service name: IGELRMGUIServer

Display name: IGEL RMGUIServer

Description:

Path to executable:
"C:\Program Files\IGEL\RemoteManager\rmguiserver\bin\tomcat8.exe" //RS/

Startup type: Disabled

3. Create a backup under **UMS Administrator > Backups** and copy it to a storage medium. Include all options in the backup. For detailed instructions, see the "Embedded Database" section under Creating a Backup of the IGEL UMS.

   ⓘ The backup of **Server configurations** includes most configurations of the **Settings** area in the UMS Administrator application. Exceptions: **Web server port**, **JWS server port**, and **ciphers** – they are host-specific, i.e. stored separately on each server and cannot be part of any backup. Therefore, you should note the values of these settings if they differ from the defaults and, in the case of recovery/migration procedure, they must be changed on each server manually.

4. Create a backup of the UMS ID in the **UMS Administrator > UMS ID Backup**. For detailed instructions, see Transferring or Registering the UMS ID (see page 169).

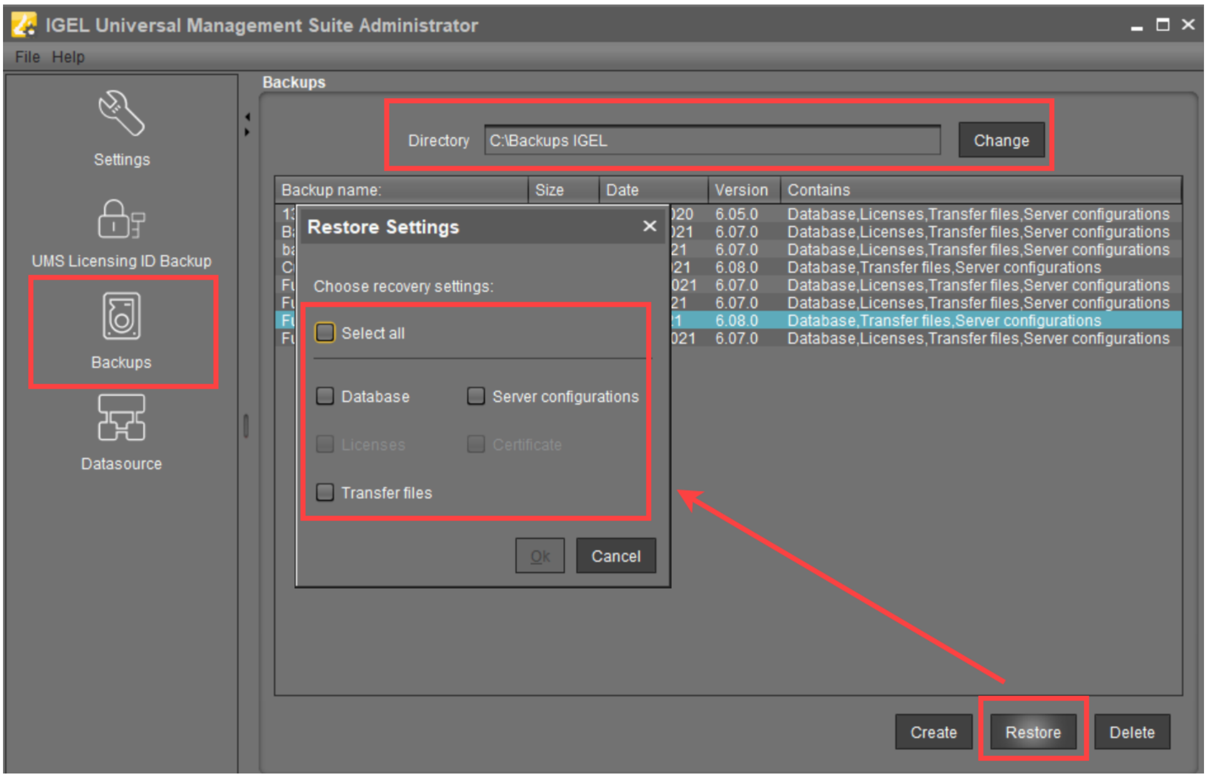
5. Create a backup of all the files in the following folder. (You will need to restore them on the new server.)
   `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

6. In the UMS Console, go to **UMS Administration > UMS Network > Server** and note the process ID of the server.

On the New Server

1. Install the UMS on the new server. If possible, use the same database user and password. For the installation instructions, see IGEL UMS Installation.

2. Under **UMS Administrator** > **Backups**, select the folder with your backup and restore the respective backup file with all options. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.



Backups

Directory C:\Backups IGEL
Change

Backup name:	Size	Date	Version	Contains
13		)20	6.05.0	Database,Licenses,Transfer files,Server configurations
B:		)21	6.07.0	Database,Licenses,Transfer files,Server configurations
ba		21	6.07.0	Database,Licenses,Transfer files,Server configurations
C		)21	6.08.0	Database,Transfer files,Server configurations
Fu		021	6.07.0	Database,Licenses,Transfer files,Server configurations
Fu		21	6.07.0	Database,Licenses,Transfer files,Server configurations
Fu		1	6.08.0	Database,Transfer files,Server configurations
Fu		021	6.07.0	Database,Licenses,Transfer files,Server configurations

Restore Settings ×

Choose recovery settings:

□ Select all

□ Database □ Server configurations

□ Licenses □ Certificate

□ Transfer files

Ok Cancel

3. Transfer the UMS ID of the previous UMS installation to the new server: **UMS Administrator > UMS ID Backup > Restore**. Alternatively, you can register the new UMS ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS ID (see page 169).

> ⚠ It is recommended to use the same UMS ID. The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.

4. If necessary, transfer host-specific server configurations to the new server.
5. Restore the files to the `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer` folder, keeping the folder structure of the old server.
6. If the ICG is used: Connect the existing ICGs as described under How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database (see page 186).
7. Restart the service `IGEL RMGUIServer`. If the devices find the UMS via the IP address, they should connect automatically.
8. If the devices find the UMS via DNS/DHCP:
   a. Adjust the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS.

      > ⓘ The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

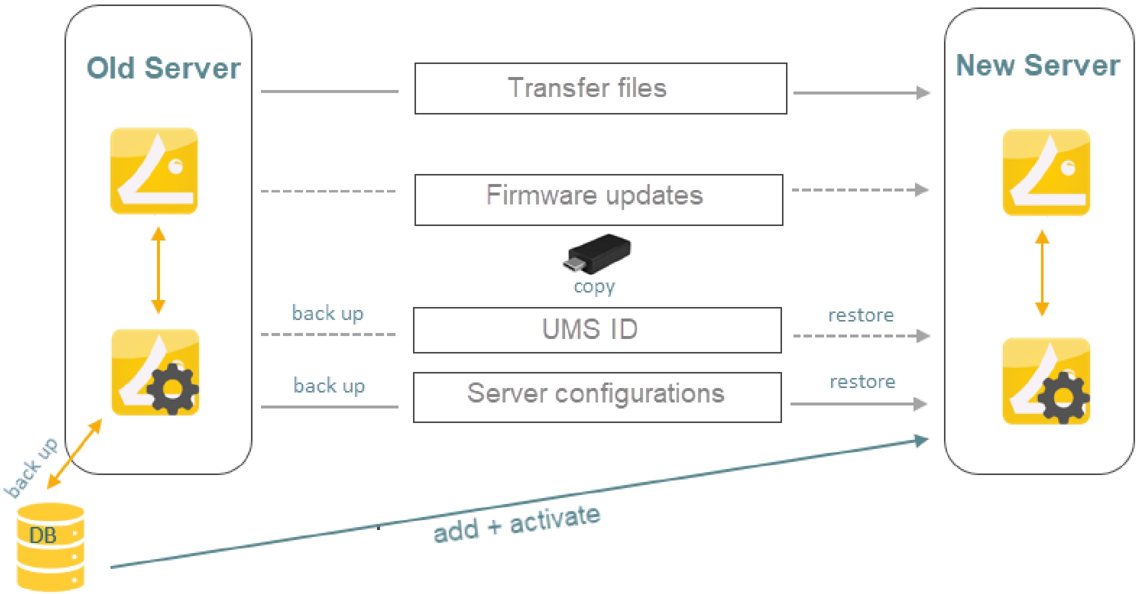
   b. Assign the new server to the old server certificate or create and assign a new certificate with the FQDN of the new server. For more information, see Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 192).
9. After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

Migrate a UMS Server with the Same External Database

Use Case

You have a UMS installation with the external database and want to migrate to a new UMS Server with the same external database.

General Overview of the Migration Procedure



The migration procedure generally involves the following steps:

1. Setting the IP address of the new server through profiles (only necessary, if devices find the UMS via IP)
2. Stopping the `IGEL RMGUIServer` service on the old server
3. Backing up the old server. Checklist for the backups:
   ✓ **Database**
   ✓ **Transfer files**
   ✓ **Firmware updates**
   ✓ **Server configurations** (host-specific server configurations that differ from the defaults are noted down separately)
   ✓ **UMS ID** (see Transferring or Registering the UMS ID (see page 169))
4. Adding the existing external database as the data source for the new server
5. Activating the data source
6. Transferring the backed-up data to the new server
7. Adjusting DHCP tag and DNS alias on the new server (only necessary, if devices find the UMS via DNS/DHCP)

Instructions

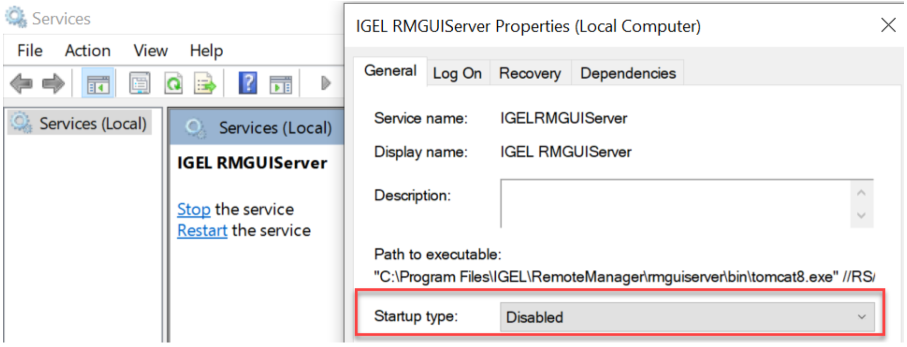
On the Old Server

1. If the devices find the UMS via the IP address, they can only connect to the new server if the IP address of the new server is set before the migration. To set the IP address:
   a. Create an OS 11 and an OS 12 profile with the new UMS server IP. The new server needs to get listed under **System > Remote Management**. For more information, see Remote Management and Remote Management.

   b. Assign the profiles.

   c. Check that all devices got their settings by creating a view with the **Last Boot Time** criterion under **Views**. For more information, see How to Create a New View in the IGEL UMS.

2. Stop the service `IGEL RMGUIServer` (for instructions, see IGEL UMS HA Services and Processes `)` and set the startup type for it to **Disabled** in order to prevent accidental parallel operation with the new UMS Server.



Service name: IGELRMGUIServer

Display name: IGEL RMGUIServer

Description:

Path to executable:
"C:\Program Files\IGEL\RemoteManager\rmguiserver\bin\tomcat8.exe" //RS/

Startup type: Disabled

3. Before the migration, make the backups as described in the "External Database" section under Creating a Backup.

4. Note the values of host-specific server settings (Web server port, JWS server port, and ciphers).

5. Create a backup of the UMS ID in the **UMS Administrator > UMS ID Backup**. For detailed instructions, see Transferring or Registering the UMS ID.

6. Create a backup of all the files in the following folder. (You will need to restore them on the new server.)
   `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer`

7. In the UMS Console, go to **UMS Administration > UMS Network > Server** and note the process ID of the server.

On the New Server

1. Install the UMS on the new server. For the installation instructions, see IGEL UMS Installation.

2. Go to **UMS Administrator > Datasource > Add** and enter the connection properties of the existing database.

3. **Activate** the data source. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.

4. In the **UMS Administrator > Backups**, restore the backup of server configurations. If necessary, transfer host-specific server configurations to the new server.

5. Transfer the UMS ID of the previous UMS installation to the new server: **UMS Administrator > UMS ID Backup > Restore**. Alternatively, you can register the new UMS ID, which was created during the installation of the new server. For detailed instructions, see Transferring or Registering the UMS ID (see page 169).

> ⚠ It is recommended to use the same UMS ID. The connection to ILP, App Portal and other services are all dependent on the UMS ID, and would be affected if it changes.

6. Restore the files to the `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer` folder keeping the folder structure of the old server.

7. If the ICG is used: Connect the existing ICGs as described under How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database (see page 186).

8. Restart the service `IGEL RMGUIServer`. If the devices find the UMS via the IP address, they should connect automatically.

9. If the devices find the UMS via DNS/DHCP:
   1. Adjust the DHCP tag and the DNS alias `igelrmserver` with the IP or FQDN of the new UMS Server. See Registering Devices Automatically on the IGEL UMS.

      > ⓘ The configuration of the DHCP tag and the DNS alias is not a setting that can be made within the IGEL software. You must configure these within your individual network environment on the corresponding DHCP and DNS servers.

   2. Assign the new server to the old server certificate or create and assign a new certificate with the FQDN of the new server. For more information, see Using Your Own Certificates for Communication over the Web Port (Default: 8443) (see page 192).

10. For HA installations only: Update the host assignment for job execution. For the instructions, see Updating Host Assignment for Job Execution (see page 172).

11. After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.

Migrate a UMS Server with a Different Database

If you want to migrate to a new UMS Server and at the same time transfer your data to a different database, you can find the instructions here.

Data transfer

Before the migration, you need to transfer the UMS data to the new database:

1. Open the the IGEL UMS Administrator of the current server.
2. Click **Data Source > Add...** to set up a data source for the new database you wish to use.
3. Click **Copy** to copy the old data source to the new one.
4. Activate the new data source.
5. Wait until the UMS Server fully starts, i.e. the UMS Console can connect with it.

ⓘ For more information on managing data sources in the IGEL UMS Administrator, see Data Source.

Migration

After the transfer of data, you can begin the migration procedure based on the database:

- If the new data source is an embedded database, follow the instructions in Migrate a UMS Server with the Same Embedded Database (see page 160).
- If the new data source is an external database, follow the instructions in Migrate a UMS Server with the Same External Database (see page 164).

Transferring or Registering the UMS ID

There are two different ways to handle the UMS ID if you migrate the UMS Server:

- Transferring the UMS ID (see page 169) (recommended): With this method, you make a backup of the old UMS ID and take it with you. The UMS ID, which is automatically created during the installation of the new UMS Server, is overwritten.
  Advantage: You do not have to reassign the license packages in the ILP and to re-register your UMS.
- Registering the New UMS ID (see page 170): With this method, you register the UMS ID of the new server in the IGEL License Portal.
  Advantage: You do not need to know the UMS ID of the old server.
  Disadvantage: To authenticate your UMS to the IGEL Cloud Services, you also have to re-register your UMS in the IGEL Customer Portal using the new UMS ID.

Transferring the UMS ID

Old Server: Create a Backup of the UMS ID

1. Open the UMS Administrator on your old server.

   > ⓘ Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

2. Go to **UMS ID Backup** and create a backup as described under UMS ID Backup in the IGEL Administrator.

3. In your file explorer, go to the folder where you saved the UMS ID backup.

4. Copy the backup (e.g. `UMS ID_backup before migration.ksbak`) to a directory of your new UMS Server environment.

New Server: Restore the UMS ID to the New Server

1. Open the **UMS Administrator** on the new server.

2. Go to **UMS ID Backup** and restore the backup as described under UMS ID Backup in the IGEL Administrator.

   The UMS ID is now stored in the new UMS environment.

Registering the New UMS ID

In the IGEL License Portal (ILP)

1. Log in to the IGEL License Portal (ILP) at https://activation.igel.com[3]. If you have not registered yet, you must register first.
   Your dashboard is shown.

2. Select **UMS ID**.
   The page **UMS ID** is shown.

3. Click **Register UMS ID**.
   The dialog **Register UMS ID** opens.

4. Under **UMS ID Name**, enter a name for the UMS ID.

5. Upload the certificate file you have exported in the UMS (see Obtaining Your UMS ID) and click **OK**.
   The UMS ID is registered. If this is the first UMS ID you registered, or if you just defined it as the default UMS ID, the dialog **Assign loose Product Packs** is shown.

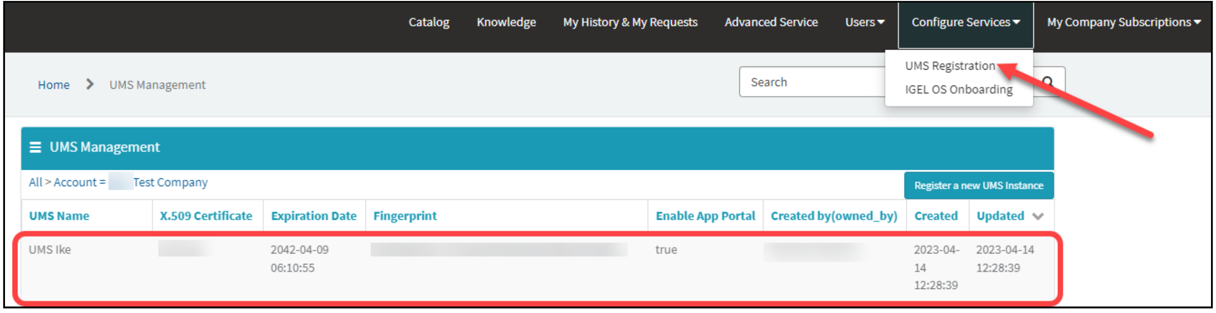
6. If the dialog **Assign loose Product Packs** is shown, click **OK** to assign Product Packs and continue with Assigning a Product Pack to the UMS ID.

For a detailed instruction with screenshots, see Registering Your UMS ID.

In the IGEL Customer Portal

1. Log in to t[4]he IGEL Customer Portal[5].

2. Go to **Configure Services > UMS Registration** and select your old UMS instance.

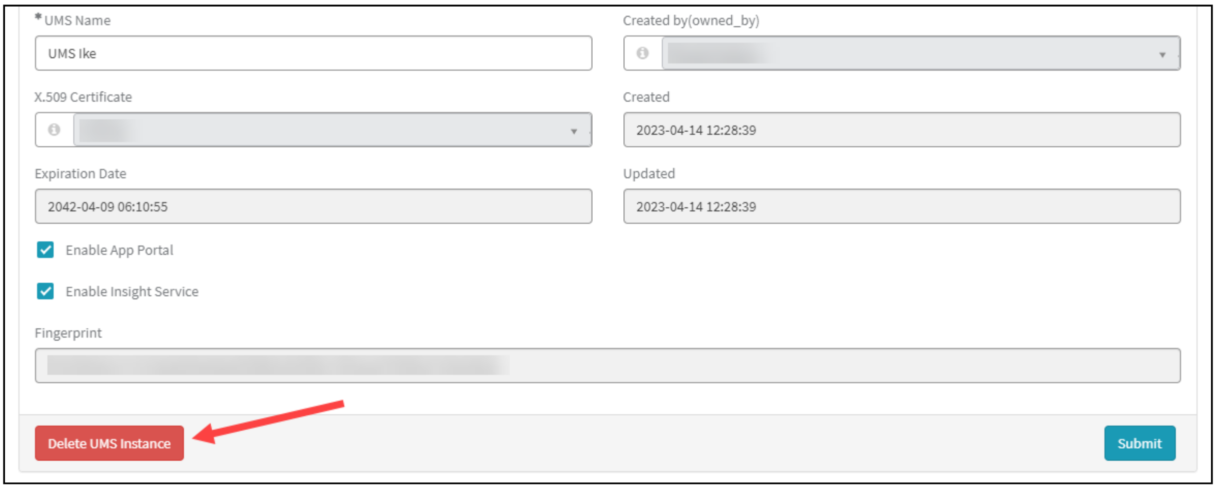


All > Account = [redacted] Test Company

UMS Name	X.509 Certificate	Expiration Date	Fingerprint	Enable App Portal	Created by(owned_by)	Created	Updated
UMS Ike	[redacted]	2042-04-09 06:10:55	[redacted]	true	[redacted]	2023-04-14 12:28:39	2023-04-14 12:28:39

[3] https://activation.igel.com/
[4] https://now.igel.com/csm
[5] https://cosmos.igel.com/

3. Click **Delete UMS Instance**.



*UMS Name: UMS Ike

Created by(owned_by):

X.509 Certificate:

Created: 2023-04-14 12:28:39

Expiration Date: 2042-04-09 06:10:55

Updated: 2023-04-14 12:28:39

☑ Enable App Portal

☑ Enable Insight Service

Fingerprint:

When you delete your UMS instance, you cannot import apps to the UMS or open the local App Portal on the IGEL OS 12 devices.

4. Register your UMS anew as described under Registering the UMS.

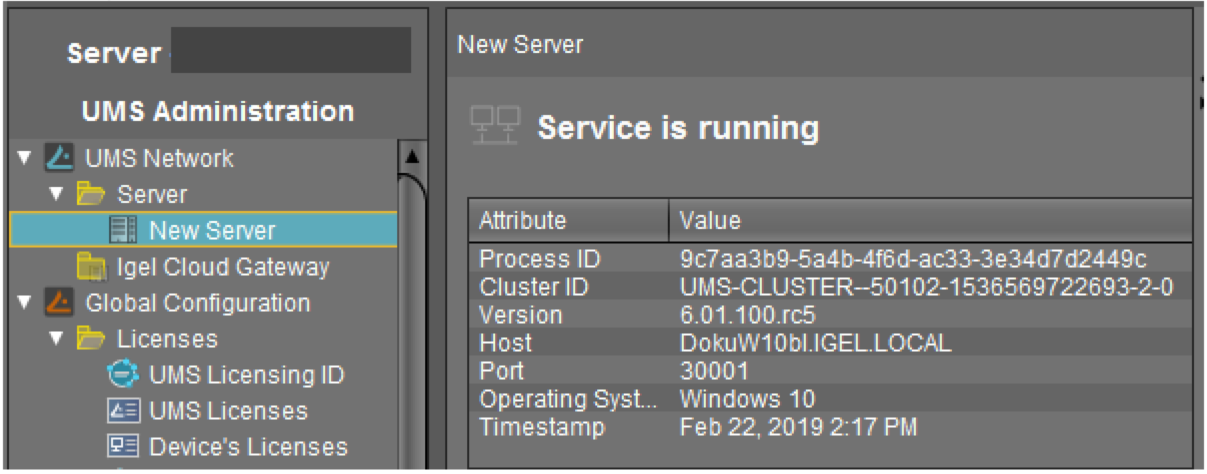
Updating Host Assignment for Job Execution

Job execution in the UMS uses a device to UMS Server mapping to avoid multiple executions of one job with the same device. If a UMS Server is migrated, this mapping needs to be adjusted.

> ⓘ The mapping is relevant for High Availability (HA) and Distributed UMS installations only. In standard (single instance) installations, the host assignments do not need to be adjusted. In HA and Distributed UMS installations, follow the steps below.

1. In the UMS Console, go to **UMS Administration > UMS Network > Server >** [new server].

2. Find the process ID of the new server.



Attribute	Value
Process ID	9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c
Cluster ID	UMS-CLUSTER--50102-1536569722693-2-0
Version	6.01.100.rc5
Host	DokuW10bl.IGEL.LOCAL
Port	30001
Operating Syst...	Windows 10
Timestamp	Feb 22, 2019 2:17 PM

3. In the menu bar of the UMS Console, select **Misc > Scheduled Jobs > Host Assignment**.

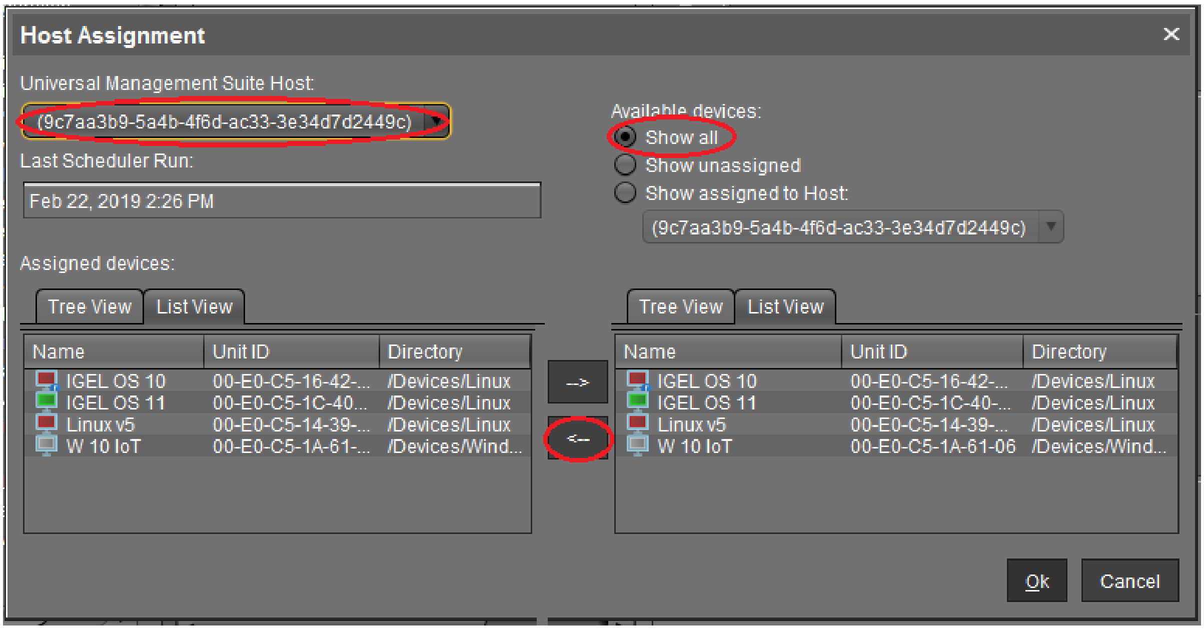
4. Select the new server and check the process ID.

5. Under **Available devices**, activate **Show all**.

6. In **List View** on the right side, select all devices.

   > ⓘ To select all devices, set the focus in the list and press [Ctrl+a].

7. Click the left arrow to assign the devices to the new host.



Host Assignment

Universal Management Suite Host: (9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c)

Last Scheduler Run: Feb 22, 2019 2:26 PM

Available devices:

● Show all

○ Show unassigned

○ Show assigned to Host: (9c7aa3b9-5a4b-4f6d-ac33-3e34d7d2449c)

Assigned devices:

Name	Unit ID	Directory
IGEL OS 10	00-E0-C5-16-42-...	/Devices/Linux
IGEL OS 11	00-E0-C5-1C-40...	/Devices/Linux
Linux v5	00-E0-C5-14-39-...	/Devices/Linux
W 10 IoT	00-E0-C5-1A-61-...	/Devices/Wind...

Name	Unit ID	Directory
IGEL OS 10	00-E0-C5-16-42-...	/Devices/Linux
IGEL OS 11	00-E0-C5-1C-40-...	/Devices/Linux
Linux v5	00-E0-C5-14-39-...	/Devices/Linux
W 10 IoT	00-E0-C5-1A-61-06	/Devices/Wind...

Migrating a UMS Database From Embedded DB to Microsoft SQL Server

This document describes how to migrate the database of a *Universal Management Suite (UMS)* installation from *Embedded DB* to a *Microsoft SQL Server*.

This is an exemplary representation. If you want to integrate the other way round or integrate other databases, the same steps are always performed. You can always use this description as a guide.

IGEL Demos Channel

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

https://www.youtube.com/watch?v=_200UQppobw

- Setting Up the SQL Database (see page 175)
- Copying Database Contents (see page 177)

Setting Up the SQL Database

The UMS supports only those standard sortings of Microsoft SQL Server which are case insensitive ("CI"). Therefore, make sure that the parameter **Collation** in MS SQL Server is set appropriately.

▶ Execute the following SQL script on the Microsoft SQL Server to create database, login, user, and schema. Replace the placeholders such as `[databasename]` with settings of your choice.

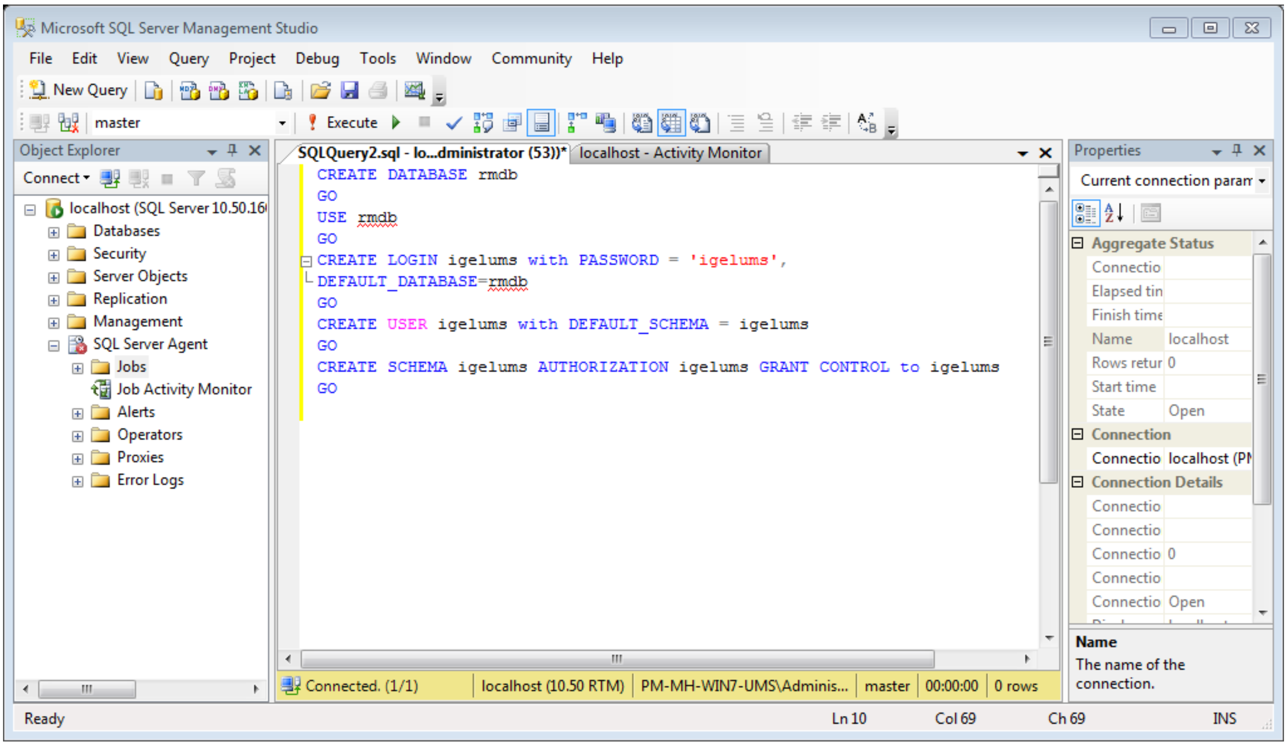
`[sql-user]` can be an SQL account or a Microsoft Active Directory (AD) account; for more information on the latter, see Connecting the UMS to an SQL Server via Active Directory (see page 175). The script uses the same string for login, user, and schema in order to simplify UMS setup.

The **user name** for the external database may only be created with the following properties:

- it consists only of **lower case** letters or **upper case** letters.
- the **low-cut character** ("_") is the only special character, which is allowed.

Do not mix upper and lower case letters. Don't use points, spaces, minus, or @ sign!

```
CREATE DATABASE [databasename]
GO
USE [databasename]
GO
CREATE LOGIN [sql-user] with PASSWORD = '[password]',
DEFAULT_DATABASE=[databasename]
GO
CREATE USER [sql-user] with DEFAULT_SCHEMA = [sql-user]
GO
CREATE SCHEMA [sql-user] AUTHORIZATION [sql-user] GRANT CONTROL to [sql-user]
GO
```



```
CREATE DATABASE rmdb
GO
USE rmdb
GO
CREATE LOGIN igelums with PASSWORD = 'igelums',
DEFAULT_DATABASE=rmdb
GO
CREATE USER igelums with DEFAULT_SCHEMA = igelums
GO
CREATE SCHEMA igelums AUTHORIZATION igelums GRANT CONTROL to igelums
GO
```

Connected. (1/1) | localhost (10.50 RTM) | PM-MH-WIN7-UMS\Adminis... | master | 00:00:00 | 0 rows

Aggregate Status	
Connectio	
Elapsed tin	
Finish time	
Name	localhost
Rows retur	0
Start time	
State	Open
Connection	
Connectio	localhost (PN
Connection Details	
Connectio	
Connectio	
Connectio	0
Connectio	
Connectio	Open

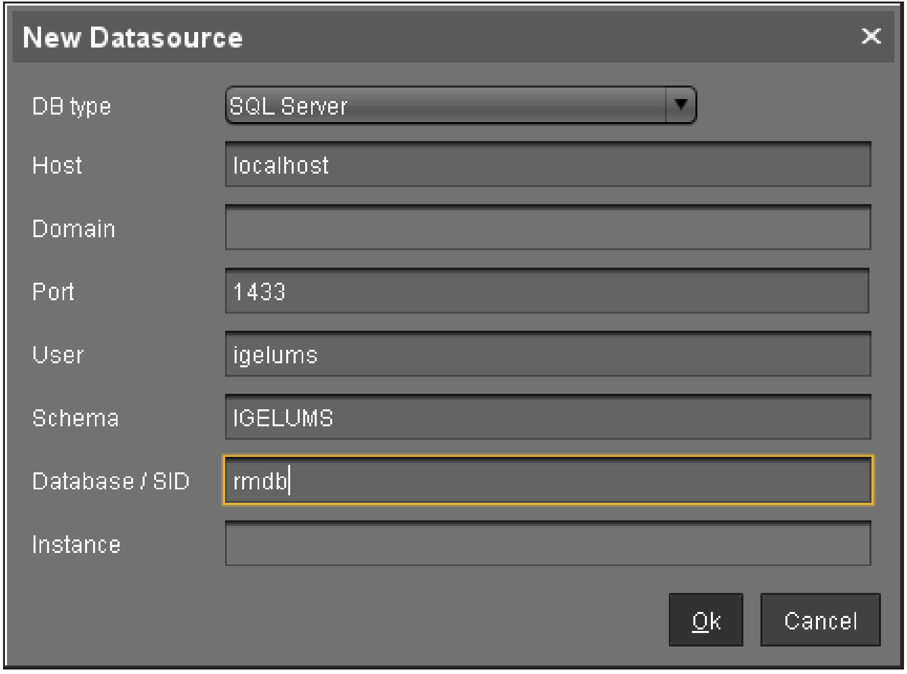
Name
The name of the connection.

Copying Database Contents

1. Start IGEL Universal Management Suite Administrator.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

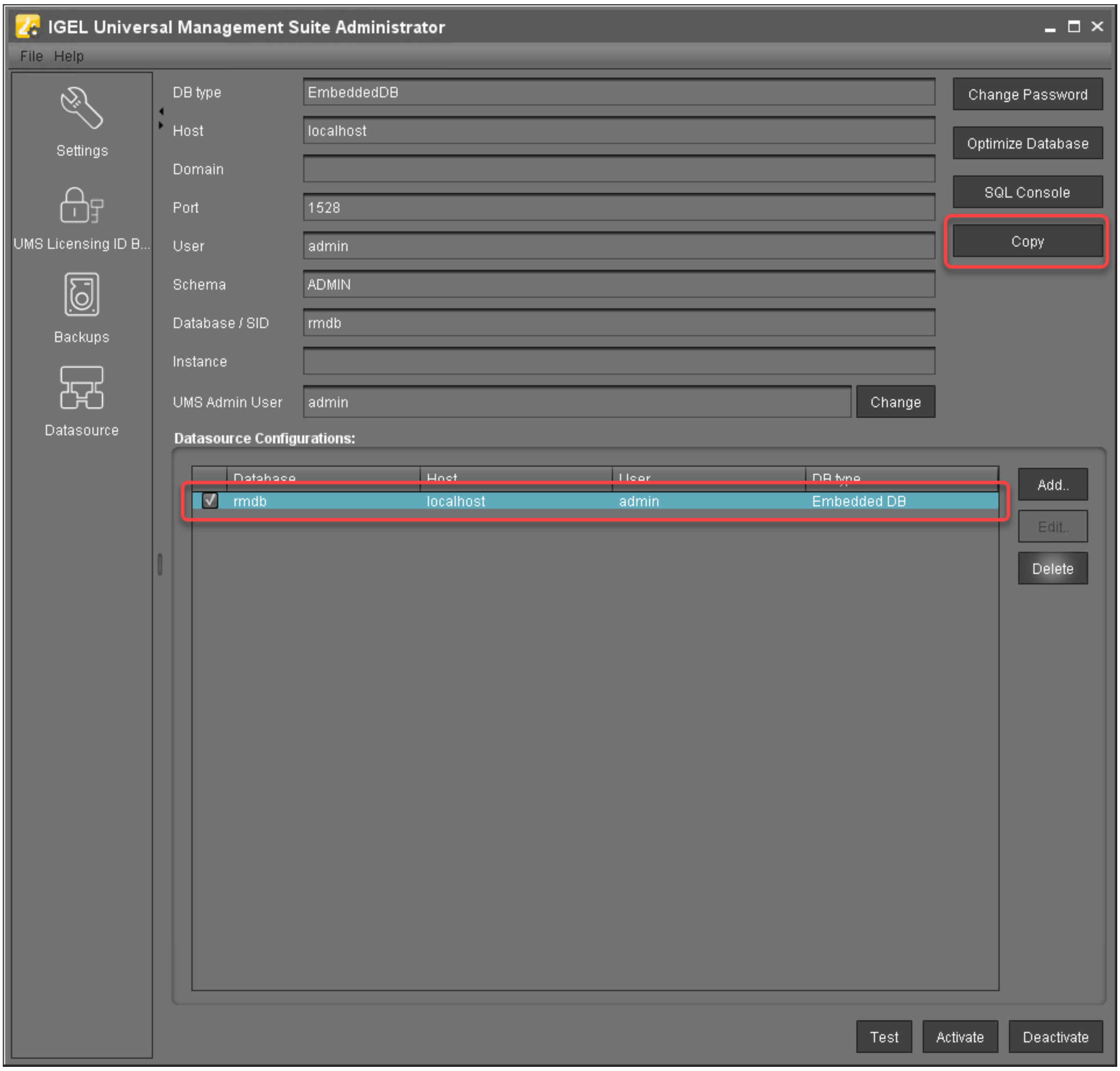
2. Go to **Datasource > Add...** to create a new SQL Server data source; use exactly the same database name and settings you have defined while setting up the SQL Database (see Setting Up the SQL Database (see page 175)).



New Datasource

DB type	SQL Server
Host	localhost
Domain	
Port	1433
User	igelums
Schema	IGELUMS
Database / SID	rmdb
Instance	

3. Select the **Embedded DB** entry and click **Copy.**



DB type: EmbeddedDB

Host: localhost

Domain:

Port: 1528

User: admin

Schema: ADMIN

Database / SID: rmdb

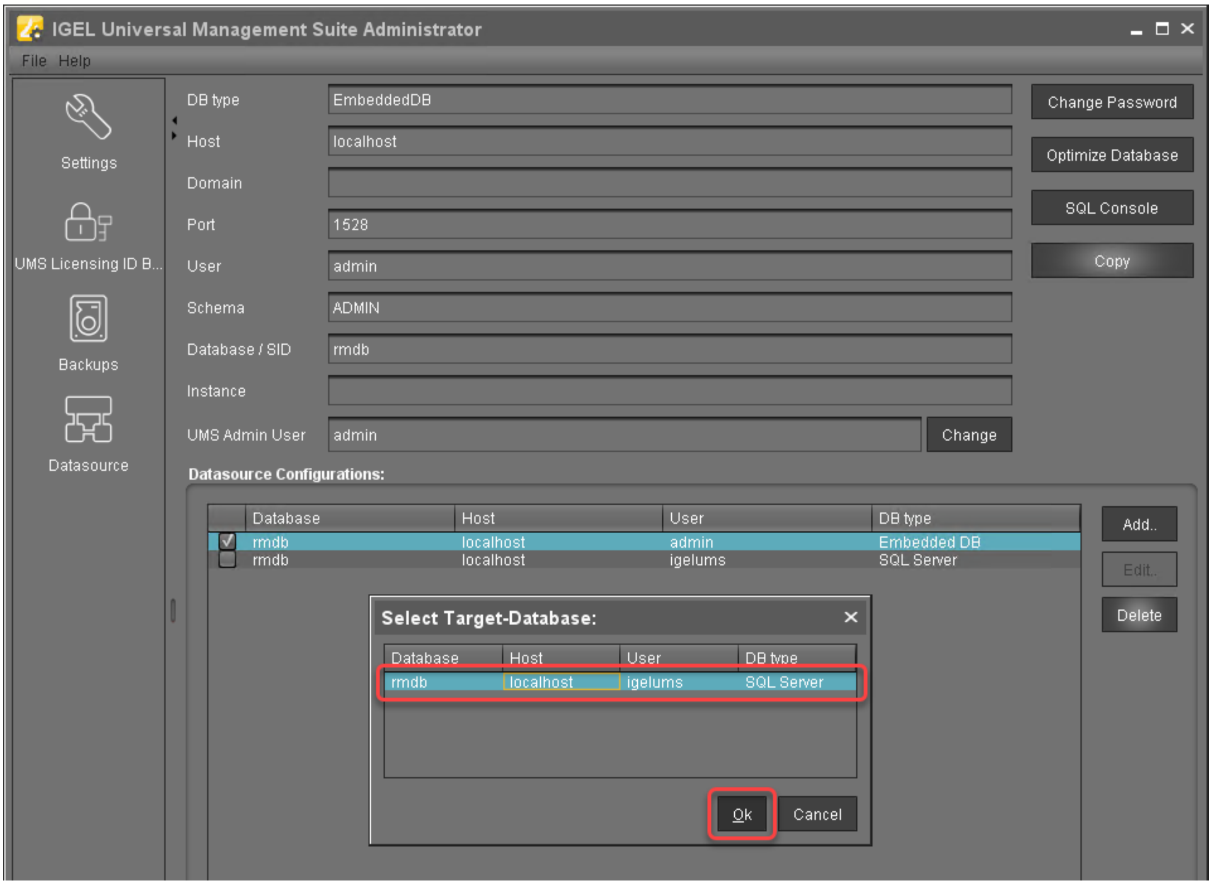
Instance:

UMS Admin User: admin

Datasource Configurations:

	Database	Host	User	DB type
☑	rmdb	localhost	admin	Embedded DB

4. Select the newly created SQL Server entry as the target and click **OK.**



DB type	EmbeddedDB
Host	localhost
Domain	
Port	1528
User	admin
Schema	ADMIN
Database / SID	rmdb
Instance	
UMS Admin User	admin

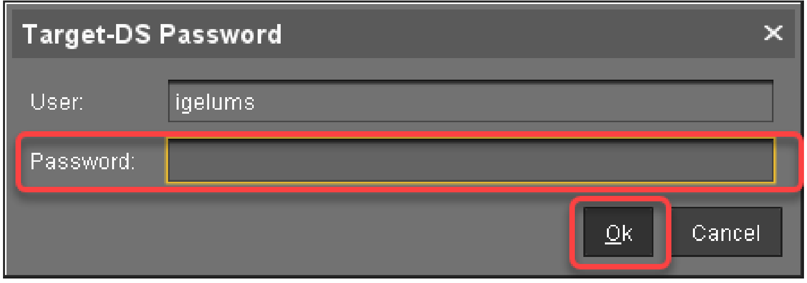
Datasource Configurations:

	Database	Host	User	DB type
☑	rmdb	localhost	admin	Embedded DB
□	rmdb	localhost	igelums	SQL Server

Select Target-Database:

Database	Host	User	DB type
rmdb	localhost	igelums	SQL Server

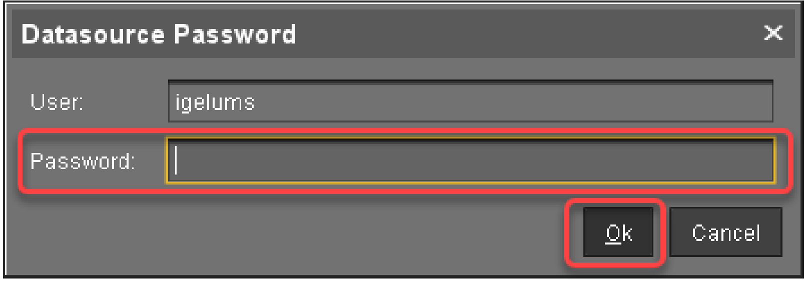
5. Enter the password and click **OK** to start the copying.



User: igelums

Password:

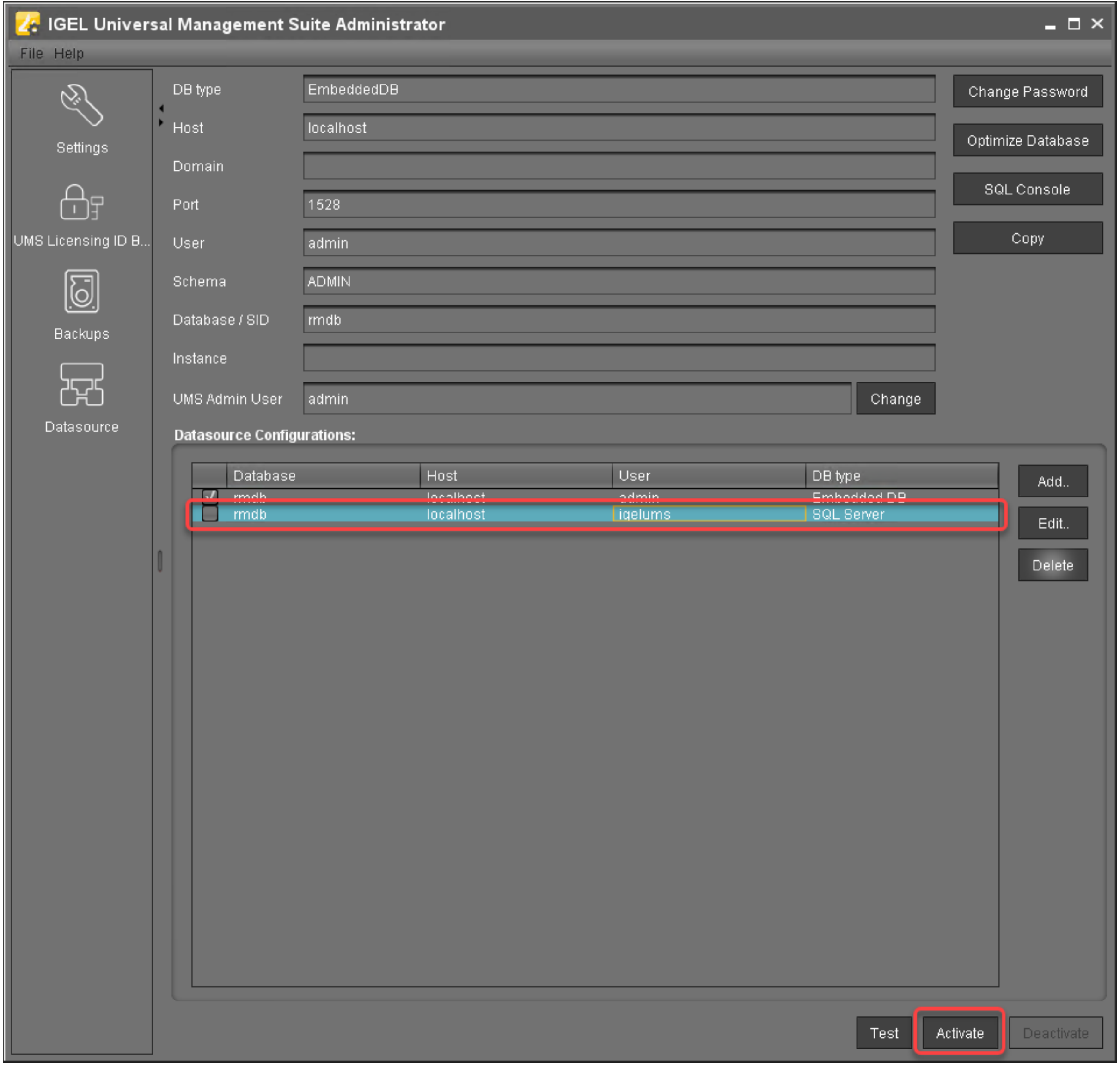
6. When the copying has completed, test the database connection by clicking **Test** and entering the password.



User: igelums

Password:

7. If the test was successful, select the **SQL Server** datasource and click **Activate.**

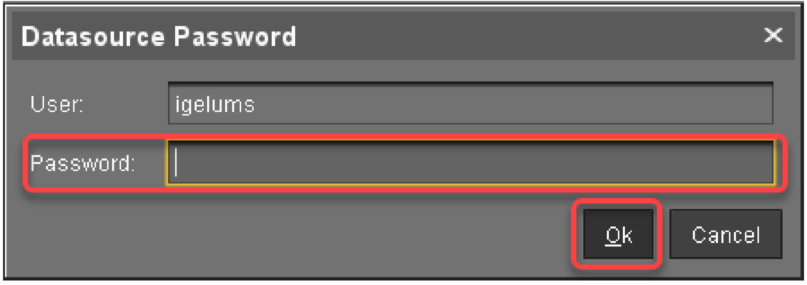


DB type: EmbeddedDB
Host: localhost
Domain:
Port: 1528
User: admin
Schema: ADMIN
Database / SID: rmdb
Instance:
UMS Admin User: admin

Datasource Configurations:

	Database	Host	User	DB type
☑	rmdb	localhost	admin	Embedded DB
□	rmdb	localhost	igelums	SQL Server

8. Enter the password to confirm the activation.



User: igelums
Password:

ⓘ Now the Microsoft SQL Server is set up as the datasource. From now on, back up the SQL Server in order to back up UMS data.

ⓘ The same way you can go back to the embedded database, if you need.

Restore and Recover Corrupted UMS Embedded DB

Environment

- UMS 6 on Windows or Linux

If the embedded database of UMS* is corrupted, try the following measures to resolve the issue.

*The underlying technology of the embedded database is Apache Derby.

Restoring a Database Backup Made with the UMS Administrator

If a backup of the embedded database is available (see Creating a Backup of the IGEL UMS), just restore the backup, see Restoring a Backup.

Restoring a File-Based Backup

If an uncorrupted copy of the database files located under `C:\Program Files...\IGEL\RemoteManager\db\rmdb` (default installation path on Windows) and/or `/opt/IGEL/RemoteManager/db/rmdb/` (default installation path on Linux) is available, you can restore the file copy. In the remainder of this how-to, the aforementioned possible paths will be referred to as `RMDB_PATH.`

To restore the backup, perform the following steps:

1. Open the UMS Administrator, and go to **Datasource** in the menu on the left.

   > Default path to the UMS Administrator:
   > Linux: `/opt/IGEL/RemoteManager/RMAdmin.sh`
   > Windows: `C:\Program Files\IGEL\RemoteManager\rmadmin\RMAdmin.exe`
   > The IGEL UMS Administrator application can only be started on the UMS Server.

2. In the **Datasource** area, delete the corrupted Derby DB.
3. Create a new embedded DB with exactly the same user name and password as you used for the deleted DB.
4. Deactivate the newly created DB.
5. Stop the UMS Server service. For details on how you can stop it, see IGEL UMS HA Services and Processes.
6. Erase all files contained in the folder at `RMDB_PATH`.
7. Copy your previously backed-up files to `RMDB_PATH`.
8. Activate the DB with the UMS Administrator under **Datasource**.
9. Wait 1 - 2 minutes, then log in to the UMS Console.

Disaster Recovery: UMS with an External Database

The following instructions require a proper backup of your environment, see the "External Database" section under Creating a Backup of the IGEL UMS.

Execution Order in Case of the Disaster Recovery

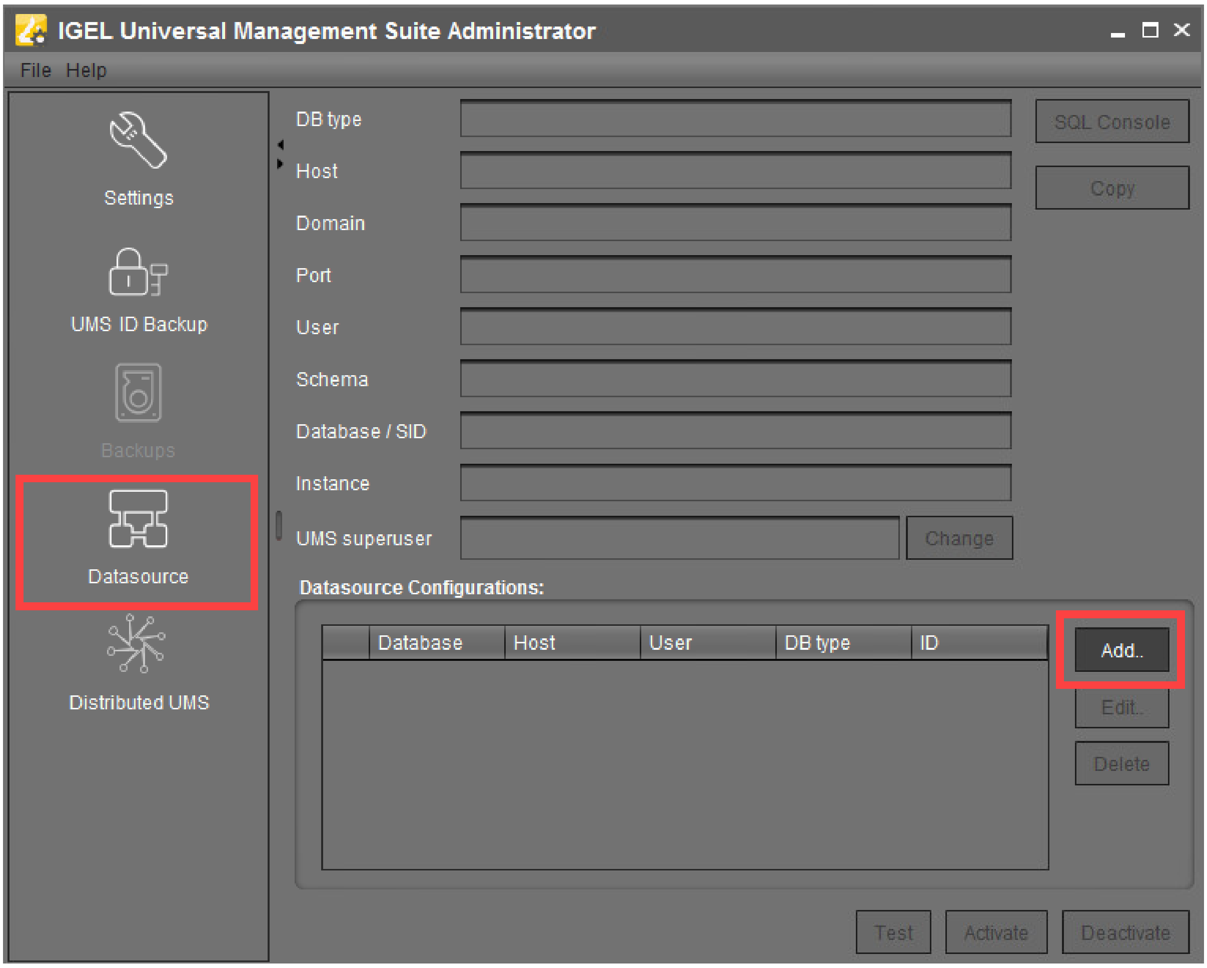
1. Install the UMS on the server, see IGEL UMS Installation. All the UMS components must be installed like before:
   a. The same UMS version
   b. The same network configuration of the host (the same IP addresses, ports)
   c. For High Availability (HA) installations only: During the installation, use the backed-up IGEL network token. See the "Starting the Installation" section under Adding Further Servers to the HA Network.

2. Stop the existing UMS Server(s). For the details on how you can do it, see IGEL UMS HA Services and Processes.

3. Copy all the saved files and firmware updates from `[IGEL installation directory]/rmguiserver/webapps/ums_filetransfer` to the new UMS Server(s) – without the `WEB-INF` folder.
   If you deploy the HA environment, see also Which Files Are Automatically Synchronized between the IGEL UMS Servers? (see page 245).

4. Restore the database backup using the procedures recommended by the DBMS manufacturer.

5. Add the database connection to your external database on each UMS Server: **UMS Administrator > Datasource > Add**.



6. Click **Activate** to enable the data source.
   The UMS Server will start automatically after that.

7. In the **UMS Administrator > Backups > Restore**, restore the backup of server configurations on each UMS Server. If necessary, transfer host-specific server configurations to the new server(s).

8. In the **UMS Administrator > UMS ID Backup > Restore**, restore the backup of the UMS ID.

9. For HA and Distributed UMS installations only: Check host assignments for job execution and, if required, adjust them. See Updating Host Assignment for Job Execution (see page 172).

ⓘ After the procedure is complete, open the UMS Console and go to **UMS Administration > UMS Network > Server** to check if there is an entry for the previous UMS Server among the listed components. If so, select the entry and click **Delete** in the context menu.
In the case of the HA installations, the same must be done for the load balancers: **UMS Administration > UMS Network > Load Balancer**.

If you have a UMS installation with an embedded database, you may find it useful to read: Restore and Recover Corrupted UMS Embedded DB (see page 182).

How to Connect to the ICG after the UMS Server Migration or New Installation with the Same Database

After you have migrated your UMS Server, or newly installed it with the same database, or restored a database backup on this reinstalled server, the server cannot connect to an already existing IGEL Cloud Gateway (ICG). This happens because the ICG credentials are bound to the old process ID.

There are two possibilities to solve the problem:

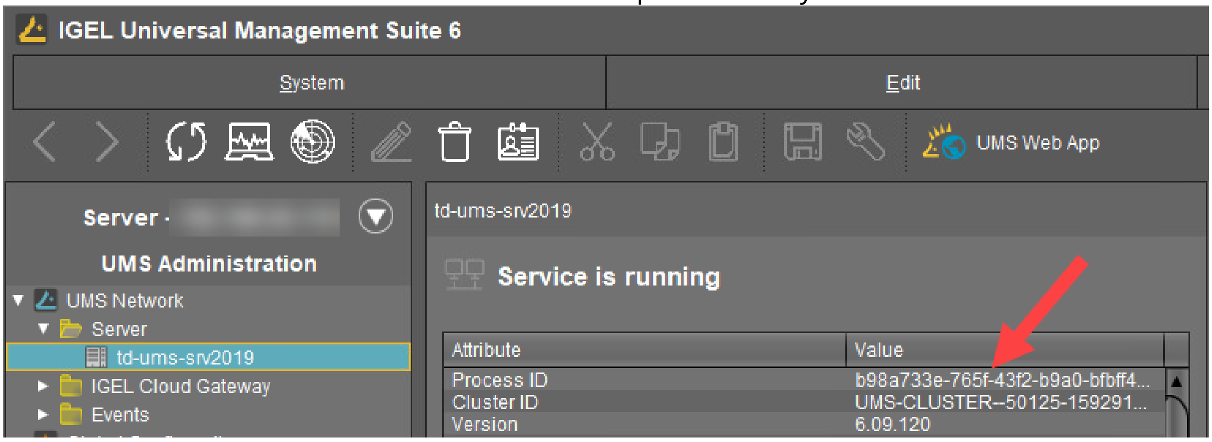
- Keeping the connection to the existing ICG (see page 186): Applicable to UMS version 6.09.100 and higher. With this method, you follow the below instructions exactly in the order given and do NOT restart the UMS Server before performing these steps. Otherwise, you cannot connect to the existing ICG and have to reinstall it.
- ICG reinstallation (see page 188): Applicable to all UMS versions. With this method, you have to uninstall the ICG and then install it again.

> ⓘ With both methods, there will be no negative impact on your endpoint devices – they will continue to work autonomously. Exception: login via Shared Workplace (SWP).

Keeping the Connection to the Existing ICG

Before UMS 6.09.100, it was always necessary to reinstall the existing ICGs after the migration of the UMS Server or reinstalling the UMS Server with the same database / backup restored. As of UMS 6.09.100, it is possible to keep the connection to the existing ICG. Proceed as follows:

1. On the old server / before the server reinstallation, open the UMS Console and go to **UMS Administration > UMS Network > Server**. Note the process ID of your UMS Server.



td-ums-srv2019

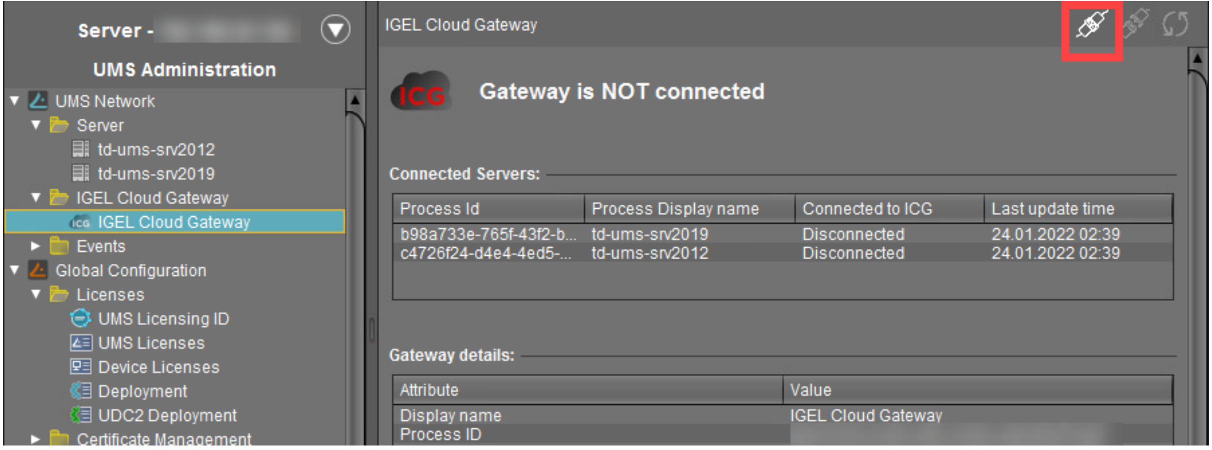
Service is running

Attribute	Value
Process ID	b98a733e-765f-43f2-b9a0-bfbff4...
Cluster ID	UMS-CLUSTER--50125-159291...
Version	6.09.120

2. Install the UMS Server. For how to install the UMS, see IGEL UMS Installation.

3. In the UMS Administrator, restore the backup (see Restoring a Backup) or, in the case of the external database, connect the existing data source and activate it (see How to Set Up a Data Source in the IGEL UMS Administrator).
   You will see the entries with the old and the new process ID in the UMS Console under **UMS Administration > UMS Network > Server** and **IGEL Cloud Gateway > [ICG name]**.

4. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway > [ICG name]** and click the **Connect** button .
   If there are several ICGs installed, perform this for each ICG.



Gateway is NOT connected

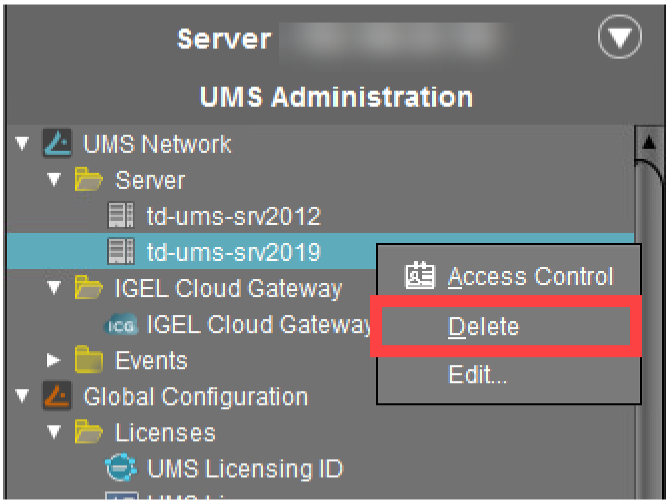
Connected Servers:

Process Id	Process Display name	Connected to ICG	Last update time
b98a733e-765f-43f2-b...	td-ums-srv2019	Disconnected	24.01.2022 02:39
c4726f24-d4e4-4ed5-...	td-ums-srv2012	Disconnected	24.01.2022 02:39

Gateway details:

Attribute	Value
Display name	IGEL Cloud Gateway
Process ID	[redacted]

5. Go to **UMS Administration > UMS Network > Server** and delete the server with the old process ID.



ⓘ After the above steps, you can restart the UMS Server at any time – you will keep the connection to the ICG. If you restart the UMS Server before performing the above steps, you will NOT be able to connect to your existing ICG and will have to reinstall it.

ICG Reinstallation

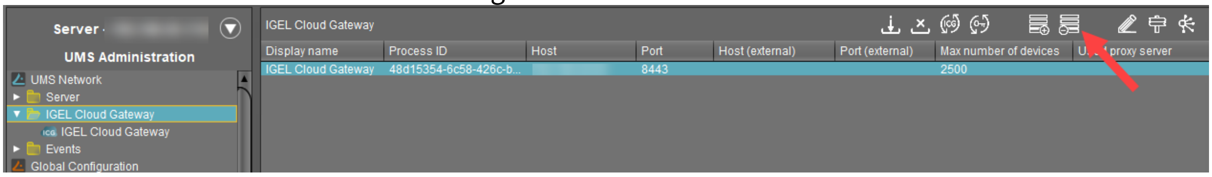
If you have migrated the UMS Server or reinstalled it with the same database / backup restored and cannot use the above-mentioned method for some reason, you will have to uninstall all the ICGs and install them again.

After you have confirmed that the new / reinstalled UMS Server is running properly, proceed as follows:

1. Log in to the ICG host and uninstall the ICG, see Uninstalling ICG.

2. Reboot the ICG server.

3. In the UMS Console, go to **UMS Administration > UMS Network > IGEL Cloud Gateway** and click **Remove Gateway from database** button ☰ to remove the ICG from the UMS Server.
   In the case of the UMS Server migration, you have to remove the ICG from both the old and the new server if the old server is still running.



Display name	Process ID	Host	Port	Host (external)	Port (external)	Max number of devices	U[illegible] proxy server
IGEL Cloud Gateway	48d15354-6c58-426c-b...	[redacted]	8443			2500	

4. Install the ICG, and in the case of the UMS Server migration, connect it only to the new UMS Server. See Installing the IGEL Cloud Gateway.

   ⚠
   - The same root certificate must be used for the installation.
   - The ICG must not move to a new server and must be reachable as before.

   ✓ **Tip**
   Check preliminarily if ICG updates are available, see IGEL Download Server[6]. It is also recommended to check time and date on all UMS and ICG servers and ports, see IGEL UMS Communication Ports (see page 4).

After the ICG reinstallation, the previously bound endpoint devices can be managed via the new ICG and do not have to be re-registered.

[6] https://www.igel.com/software-downloads/enterprise-management-pack/

UMS Does Not Connect to ICG: "TrustAnchor ...is not a CA certificate"

Symptom

The UMS fails to connect to the IGEL Cloud Gateway (ICG). The following message appears in the GUI or in the log file:

```
TrustAnchor ...is not a CA certificate
```

```
Caused by: sun.security.validator.ValidatorException: PKIX path validation
failed: sun.security.validator.ValidatorException: TrustAnchor with subject
"CN=UMS-CLUSTER--xxx, O=test, L=test, C=US" is not a CA certificate
at sun.security.validator.PKIXValidator.doValidate(PKIXValidator.java:380)
at sun.security.validator.PKIXValidator.engineValidate(PKIXValidator.java:273)
at sun.security.validator.Validator.validate(Validator.java:262)
at
sun.security.ssl.X509TrustManagerImpl.validate(X509TrustManagerImpl.java:327)
at
sun.security.ssl.X509TrustManagerImpl.checkTrusted(X509TrustManagerImpl.java:236)
at
sun.security.ssl.X509TrustManagerImpl.checkServerTrusted(X509TrustManagerImpl.java:113)
at
de.igel.apps.usg.connection.ssl.TrustedOnlyTrustManager.checkServerTrusted(TrustedOnlyTrustManager.java:74)
at
sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:1099)
at
sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1622)
... 54 more
```

Environment

- UMS 6.04 or higher
- ICG with older root certificates created with UMS 5.07 or UMS 5.08

Problem

Older ICG root certificates (created with UMS 5.07 or UMS 5.08) do not have the right CA modifier, which was never a problem with previous Java versions. But the Java version used in UMS 6.4.x onwards blocks these certificates.

To check whether you have an old ICG root certificate:

1. Open the UMS Console, go to **UMS Administration > Global Configuration > Cloud Gateway** and select your ICG root certificate.
2. Click to read the certificate content.
   If **Certificate Authority** is set to "false", you have an old ICG root certificate.

Solution

If you do not want to exchange the ICG root certificate (involves installing the ICG anew and re-registering all endpoint devices), you can add a start parameter that tells the UMS Server to ignore the CA flag in the certificate.

> ⚠ This start parameter will be overwritten on each UMS update installation, so you must set it again after the update.

Follow the instructions below, according to your operating system.

For Windows

1. Open the Windows **Services** dialog and stop the service **IGELRMGUIServer**.
2. Navigate to the directory `<UMS installation directory>\RemoteManager\rmguiserver\bin` (example: `C:\Program Files (x86)\IGEL\RemoteManager\rmguiserver\bin`)
3. Double-click on **editTomcatService**.
4. Confirm the warning dialog.
5. Select the **Java** tab.
6. Under **Java Options**, add the following entry as a new line:
   `-Djdk.security.allowNonCaAnchor=true`
7. Click **Ok** to save the changes.
8. In the Windows **Services** dialog, start the service **IGELRMGUIServer**.

For Linux

1. Stop the service `igelRMserver`
2. Navigate to the directory `/opt/IGEL/RemoteManager/rmguiserver/bin`
3. Open the file `igelRMserver`

4. Find the two entries `-Xmx4096` and add a new line before each entry with the following content: `-Djdk.security.allowNonCaAnchor=true`
5. Save the changes.
6. Start the service `igelRMserver`

Using Your Own Certificates for Communication over the Web Port (Default: 8443)

Overview

For all communication that is taking place over the Web Port (default: 8443, see also IGEL UMS Communication Ports (see page 4)), a specific self-signed certificate chain comes with the UMS on installation. Nevertheless, you can use a certificate chain of your own.

See also Web in the UMS Reference Manual.

This article describes how to deploy a certificate chain with a corporate CA certificate or a public certificate:

- Deploying a Self-Signed Corporate Certificate Chain (see page 192) (recommended)

  > ✓ We recommend using a self-signed corporate certificate chain. Of course, a self-signed certificate must be made known to the browsers first, otherwise, the browsers will display warning messages.

- Deploying a Certificate Chain with a Public Root CA (see page 203)

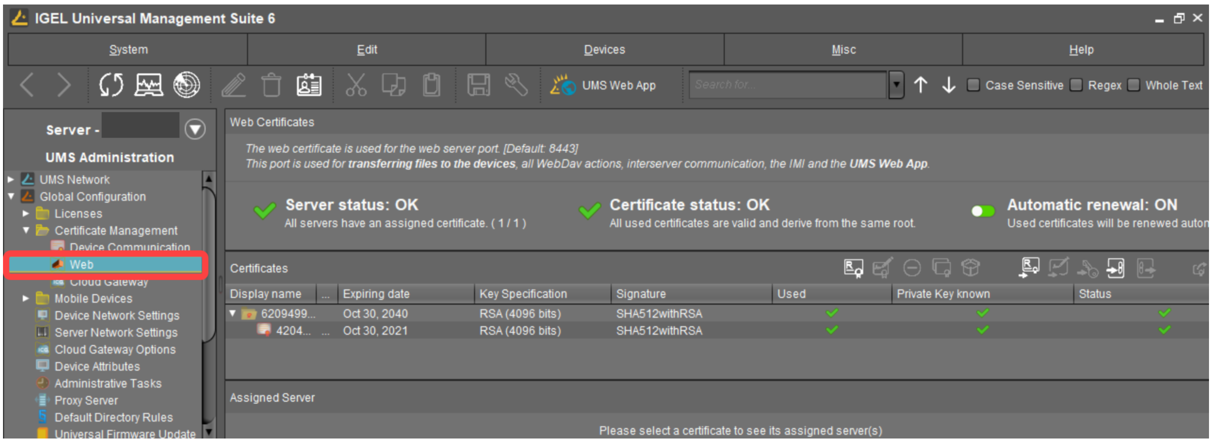
Deploying a Self-Signed Corporate Certificate Chain

Prerequisites

- You have a self-signed root CA certificate that serves as a trusted “root” certificate company-wide.
- Your self-signed root CA certificate has been applied to all relevant trust stores within your company.
- You have an intermediate CA certificate that is signed by your root CA certificate and a corresponding private key.

Importing the Root Certificate

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.



Web Certificates

The web certificate is used for the web server port. [Default: 8443]
This port is used for ***transferring files to the devices****, all WebDav actions, interserver communication, the IMI and the* ***UMS Web App****.*

✓ **Server status: OK**
All servers have an assigned certificate. (1 / 1)

✓ **Certificate status: OK**
All used certificates are valid and derive from the same root.

Automatic renewal: ON
Used certificates will be renewed auton

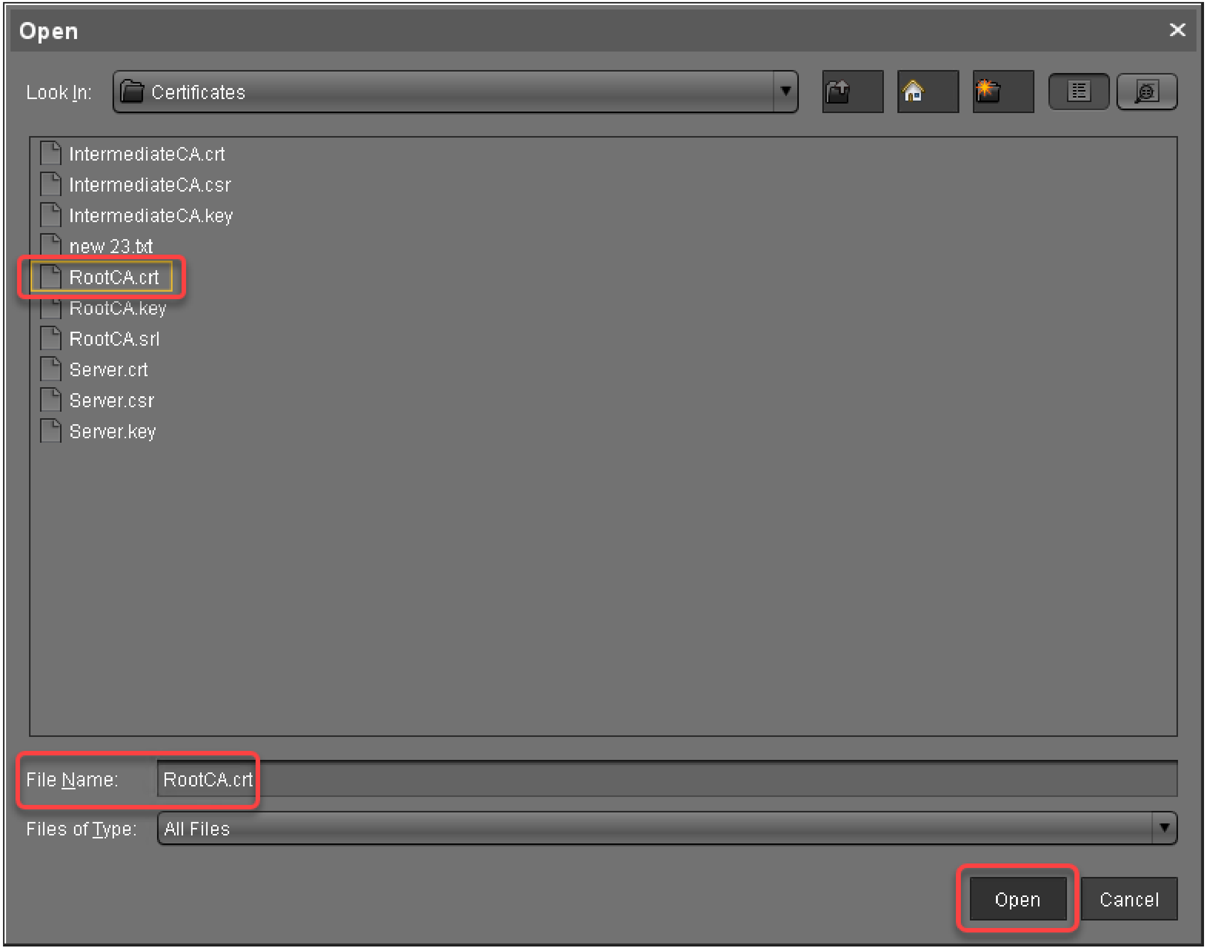
Certificates

Display name	...	Expiring date	Key Specification	Signature	Used	Private Key known	Status
▼ 6209499...		Oct 30, 2040	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
4204...	...	Oct 30, 2021	RSA (4096 bits)	SHA512withRSA	✓	✓	✓

Assigned Server

Please select a certificate to see its assigned server(s)

2. Click , select the root certificate file, and click **Open**.

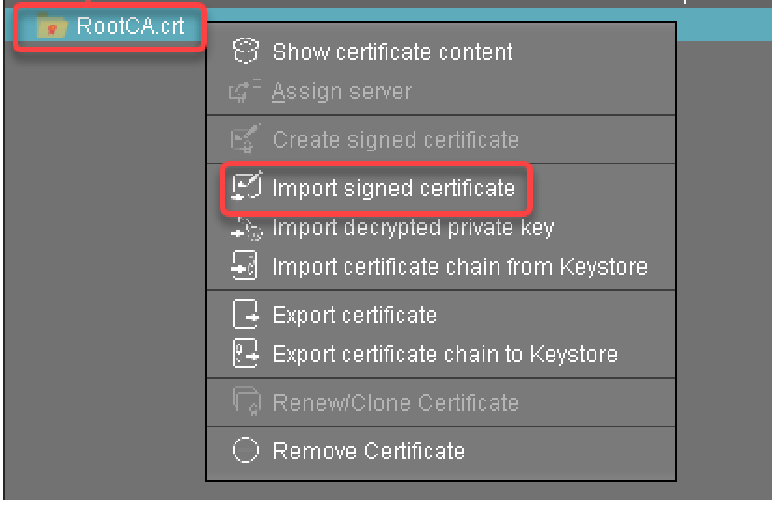


File Name: RootCA.crt

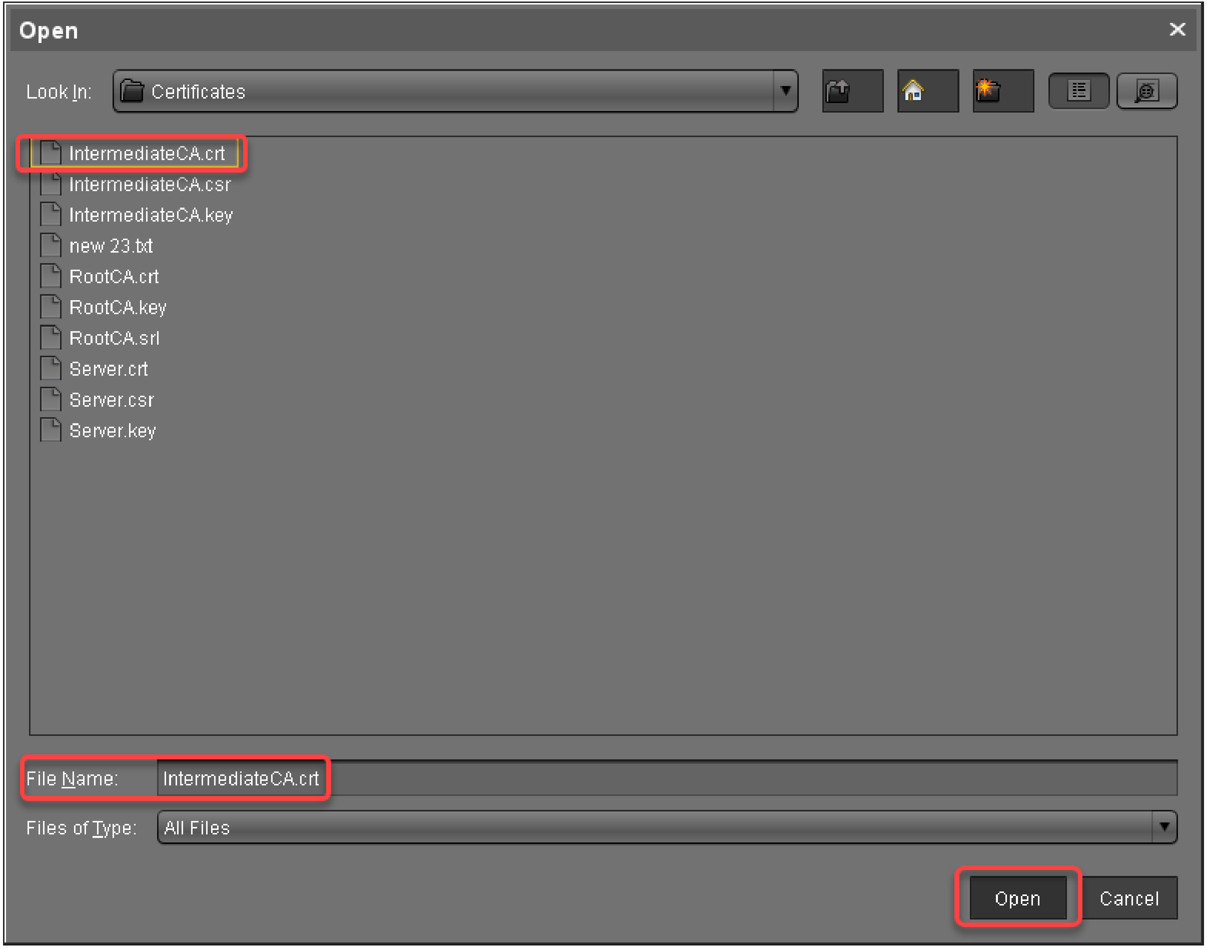
The root certificate is imported.

Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.

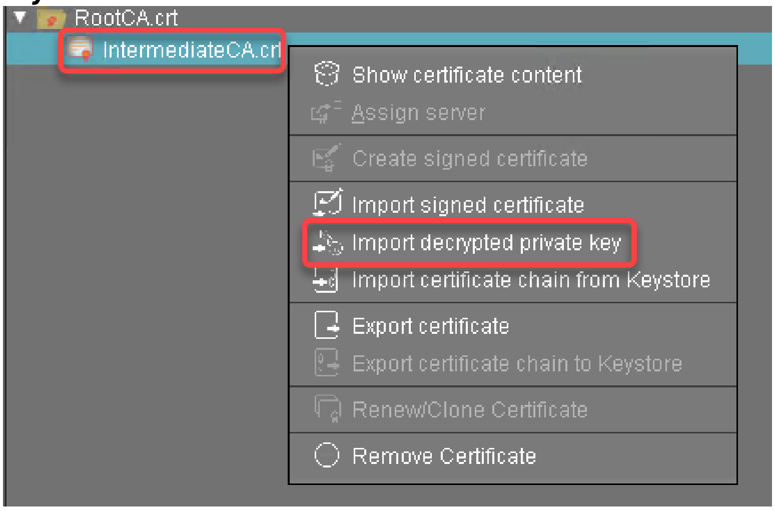

RootCA.crt
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone Certificate
Remove Certificate

2. Select the intermediate certificate file and click **Open**.

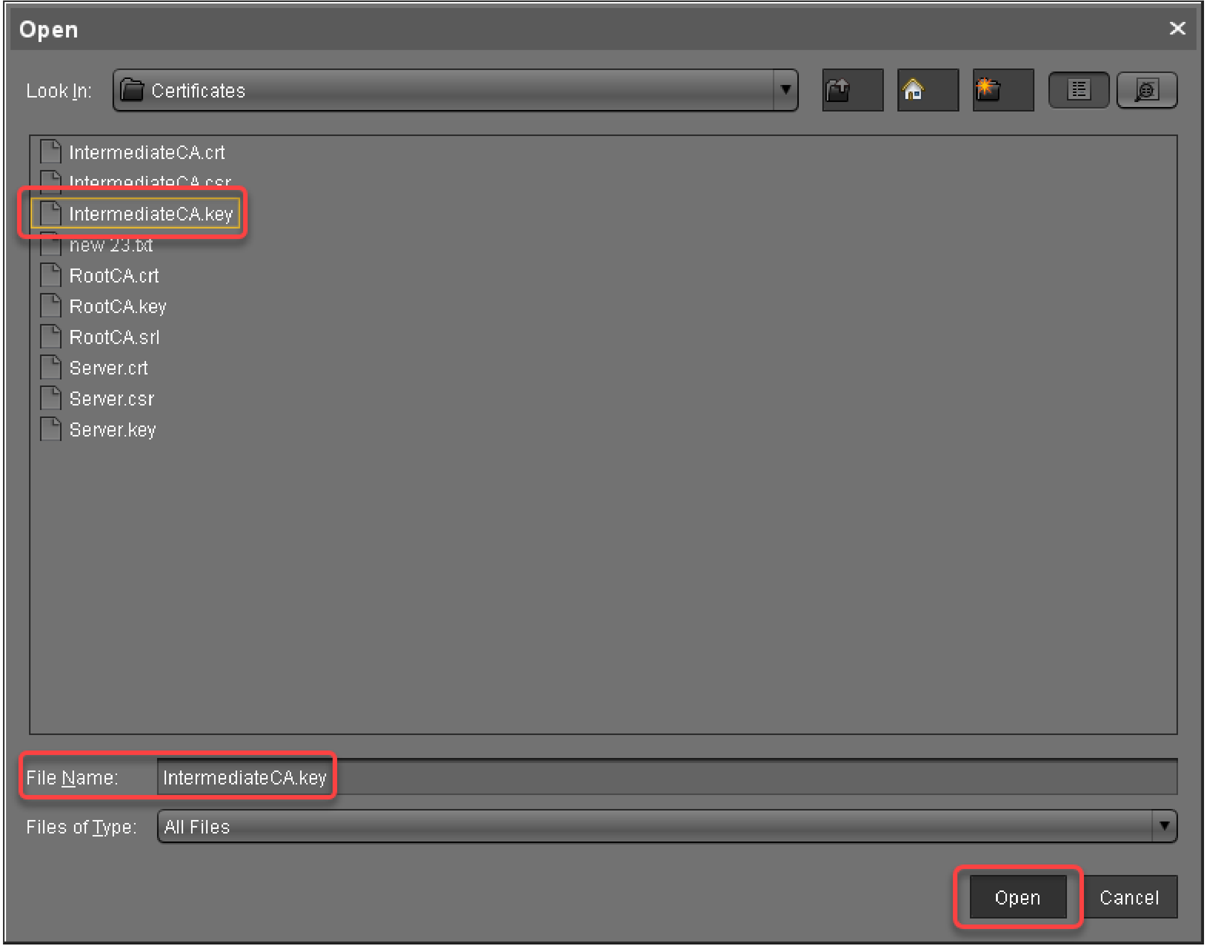


The intermediate certificate is imported.

3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.


RootCA.crt
IntermediateCA.crt
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone Certificate
Remove Certificate

4. Select the private key file of the intermediate certificate and click **Open**.



The private key of the intermediate certificate is imported.

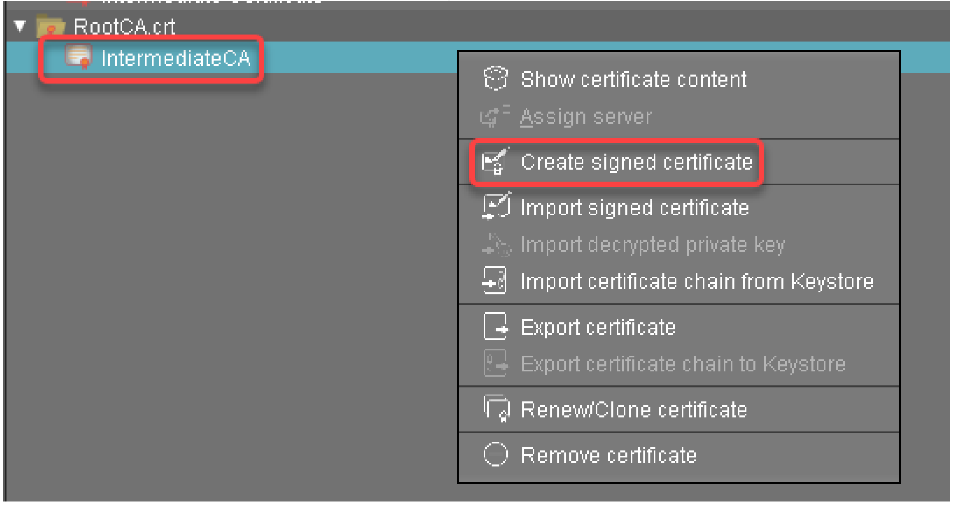
> ⚠ The private key is encrypted again when saved into the UMS Database.

5. Continue with Creating the End Certificates (see page 196).

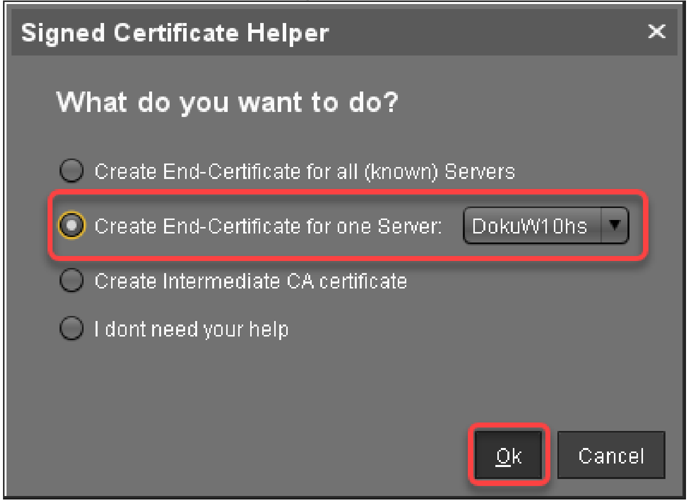
Creating the End Certificates

Repeat the following steps for each server in your UMS environment:

1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.


RootCA.crt
IntermediateCA
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone certificate
Remove certificate

2. In the **Signed Certificate Helper**, select **Create end certificate for one server** and select the server which is to be assigned to the certificate.


Signed Certificate Helper

What do you want to do?

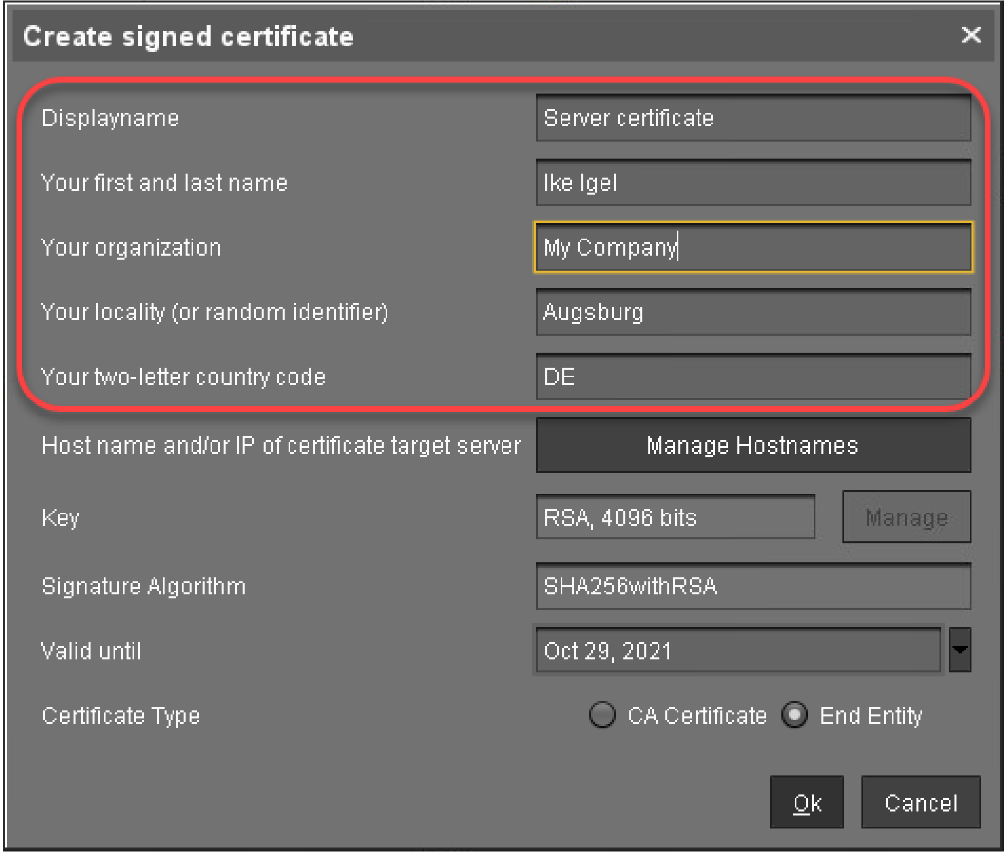
○ Create End-Certificate for all (known) Servers

● Create End-Certificate for one Server: DokuW10hs

○ Create Intermediate CA certificate

○ I dont need your help

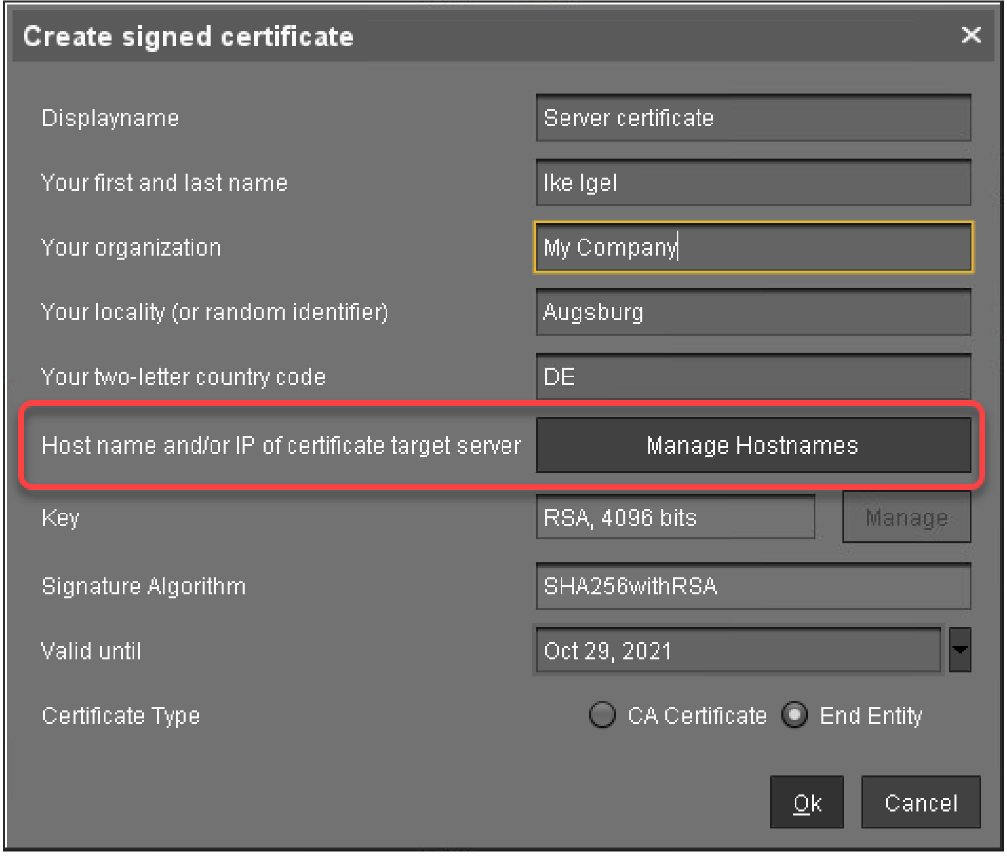
3. In the dialog **Create Signed Certificate**, fill in the data as required.



Create signed certificate

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Host name and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	○ CA Certificate ● End Entity

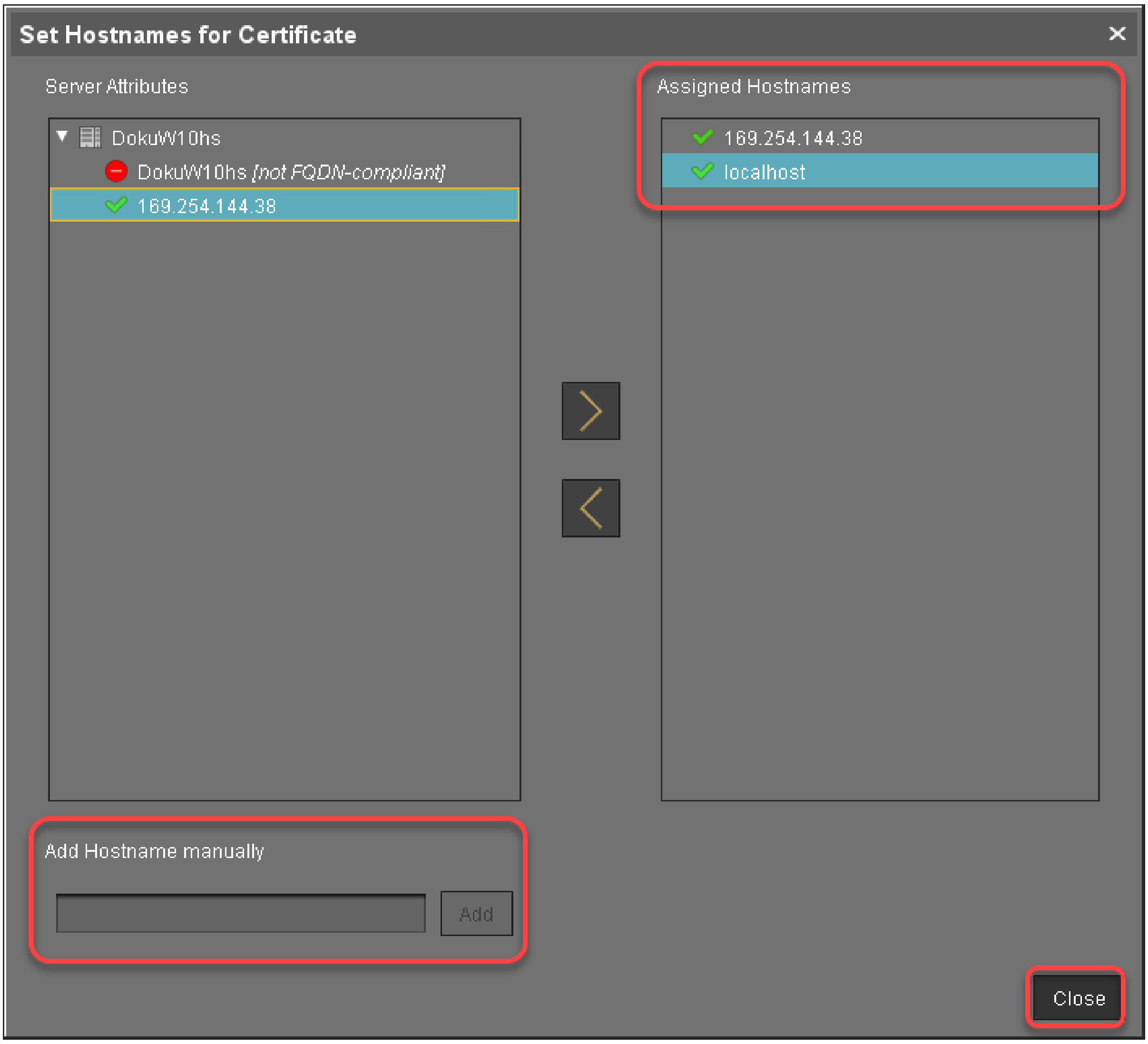
4. Click **Manage hostnames**.



Create signed certificate

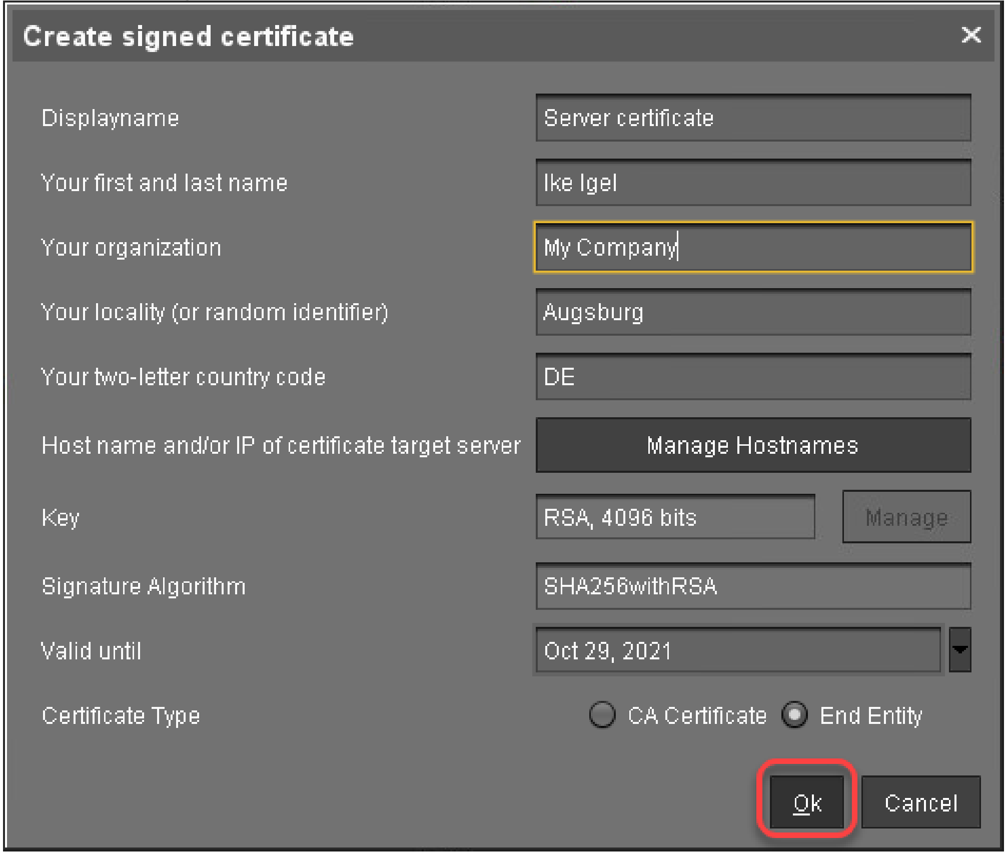
Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Host name and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	○ CA Certificate ● End Entity

5. In the dialog **Set Hostnames for Certificate**, check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.



Set Hostnames for Certificate
✕
Server Attributes
▼ DokuW10hs
DokuW10hs *[not FQDN-compliant]*
✓ 169.254.144.38
Assigned Hostnames
✓ 169.254.144.38
✓ localhost
Add Hostname manually
Add
Close

6. Close the dialog **Create Signed Certificate** with **Ok**.



Create signed certificate

Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Host name and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits Manage
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	○ CA Certificate ● End Entity

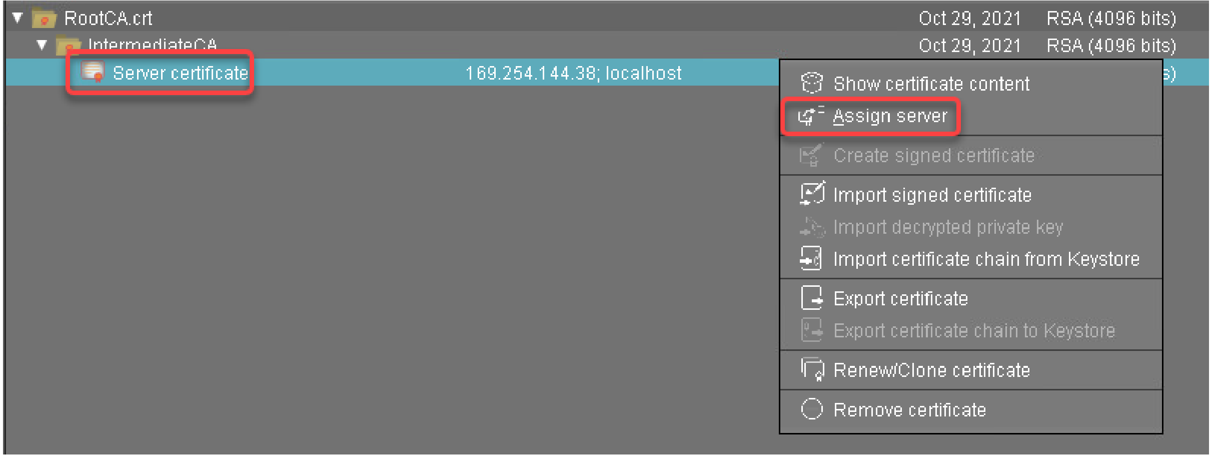
The signed server certificate is created.

7. Continue with Assigning the Certificate to All Servers (see page 201).

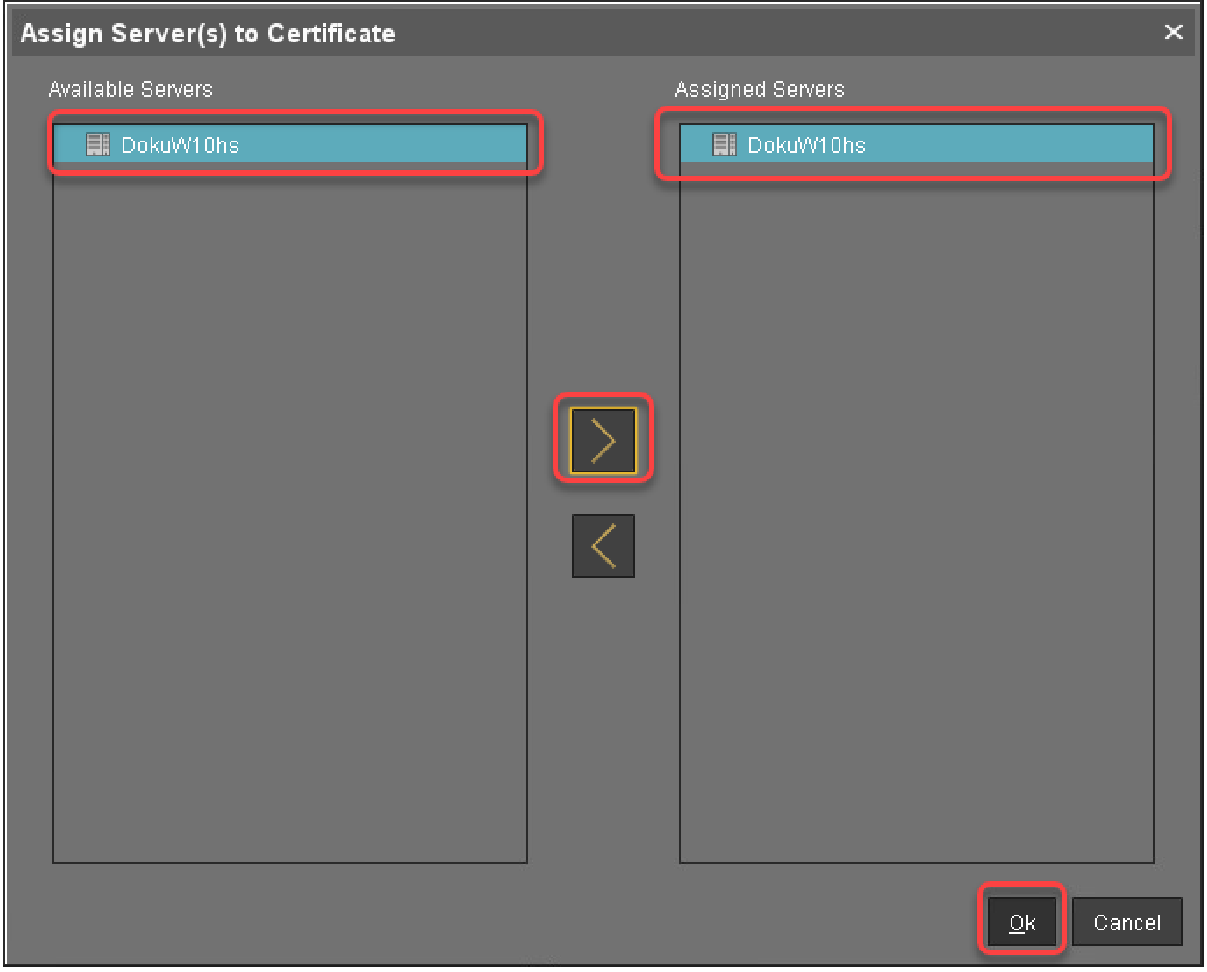
Assigning All Servers to the Certificate

Repeat the following steps for each server in your UMS environment:

1. Select the server certificate, open the context menu, and select **Assign server**.



2. Assign the server to the certificate as appropriate.



3. If you are managing IGEL OS 12 devices, see If You Exchange a Root Web Certificate for IGEL OS 12 Devices (see page 213).

4. If you are using the UMS Web App: To avoid warning messages from browsers, you must make the new certificates known to the browsers. For instructions, see UMS Web App: The Browser Displays a Security Warning (Certificate Error) (see page 286).

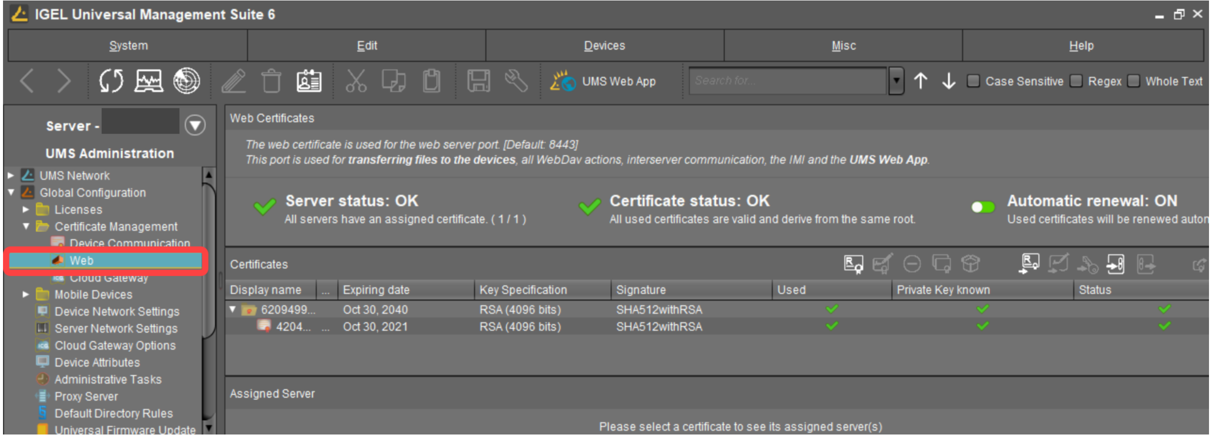
Deploying a Certificate Chain with a Public Root CA

Prerequisites

- You have a public certificate that is able to serve as a CA.
- All UMS Servers follow the same naming scheme, e.g. “something.ums.mycompany.de” if the company name is "mycompany.de".

Importing the Root Certificate

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.



The web certificate is used for the web server port. [Default: 8443]
*This port is used for **transferring files to the devices**, all WebDav actions, interserver communication, the IMI and the **UMS Web App**.*

Server status: OK
All servers have an assigned certificate. (1 / 1)

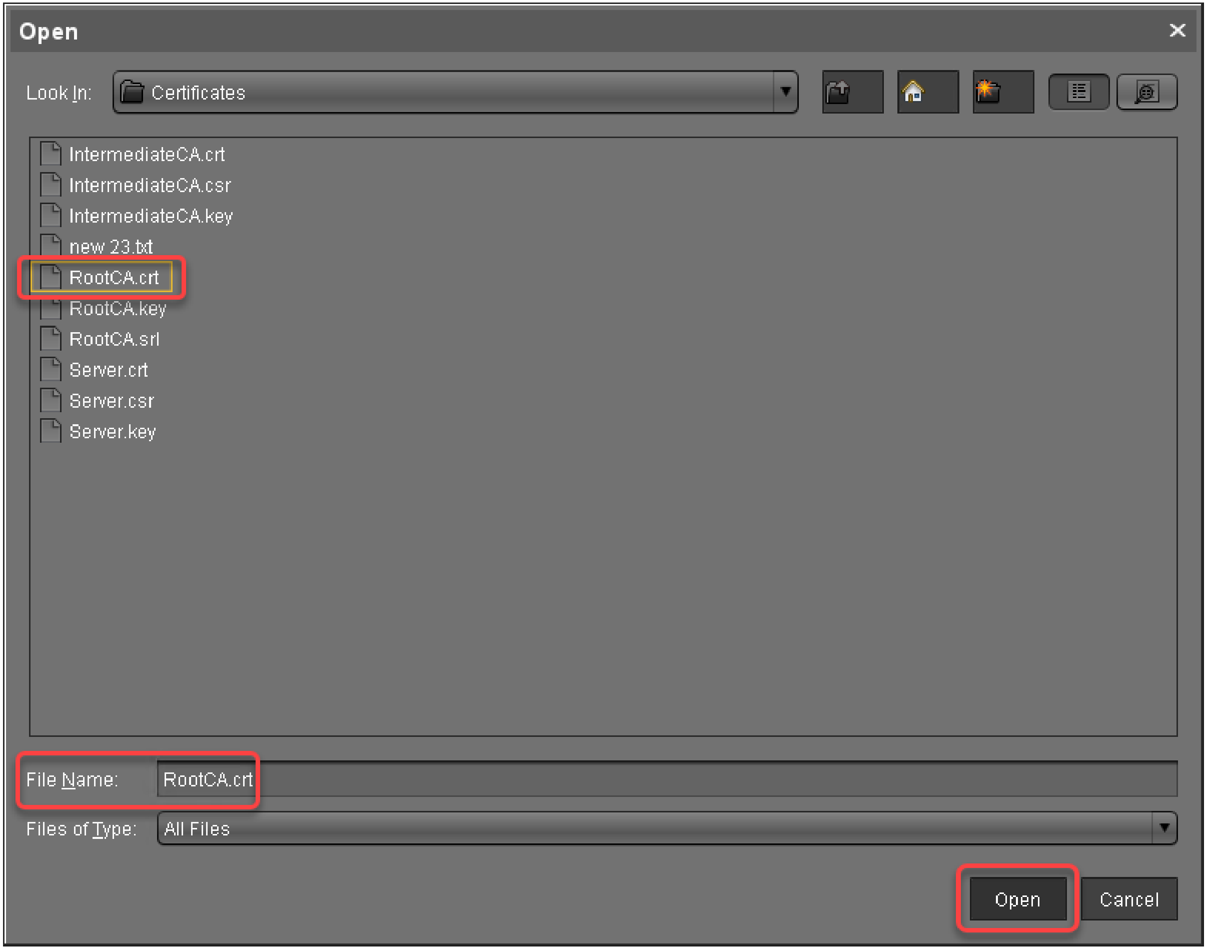
Certificate status: OK
All used certificates are valid and derive from the same root.

Automatic renewal: ON
Used certificates will be renewed auton

Display name	...	Expiring date	Key Specification	Signature	Used	Private Key known	Status
6209499...		Oct 30, 2040	RSA (4096 bits)	SHA512withRSA	✓	✓	✓
4204...	...	Oct 30, 2021	RSA (4096 bits)	SHA512withRSA	✓	✓	✓

Please select a certificate to see its assigned server(s)

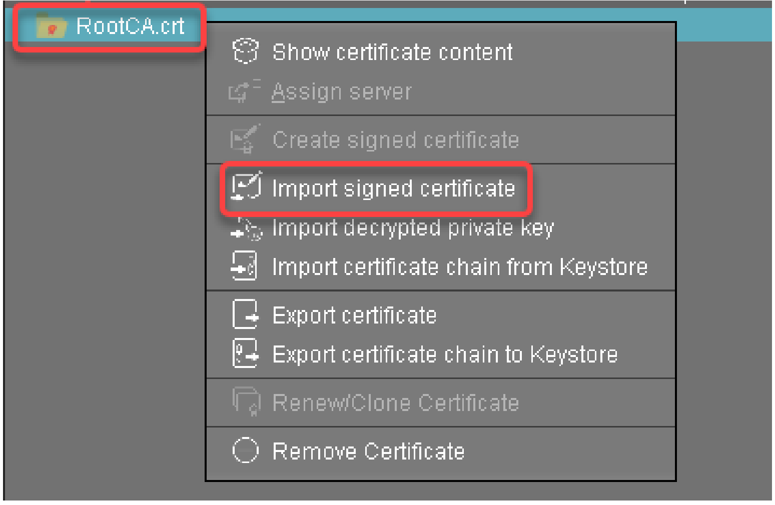
2. Click [icon], select the root certificate file, and click **Open**.



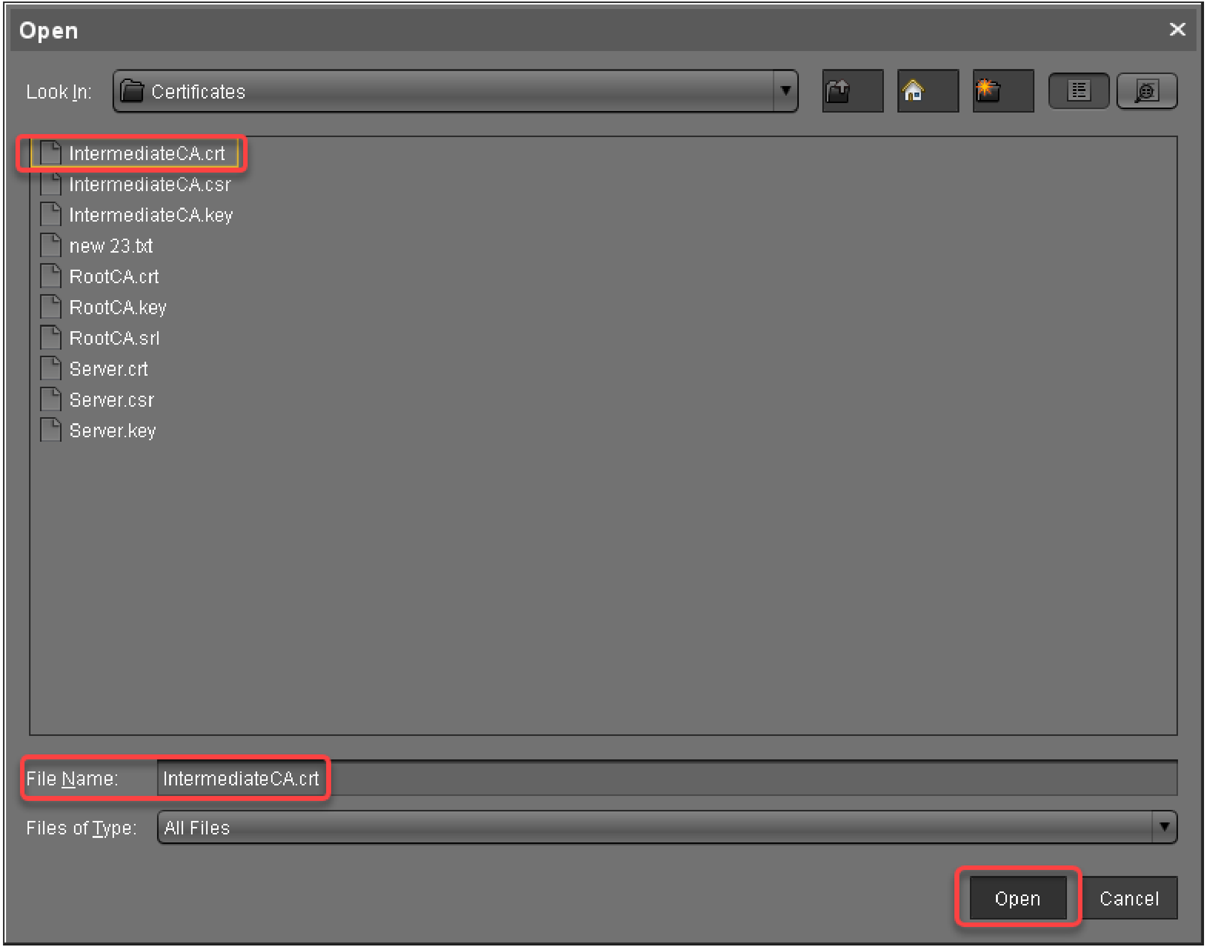
The root certificate is imported.

Importing the Intermediate Certificate

1. Select the root certificate, open the context menu, and select **Import signed certificate**.

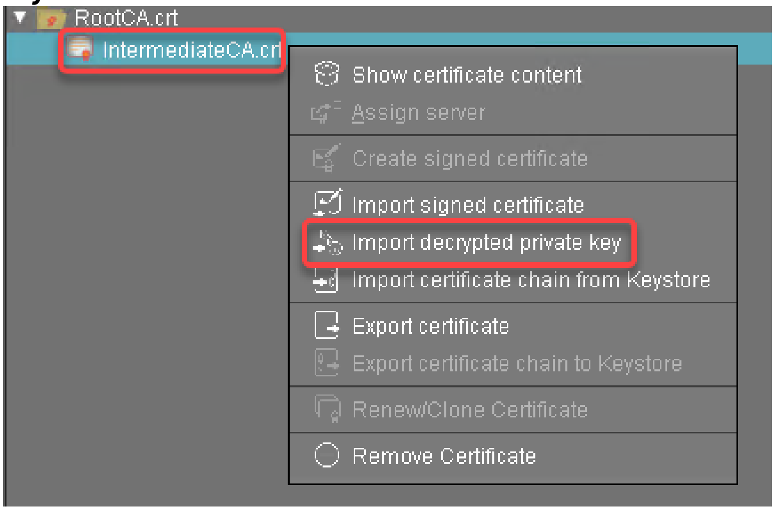

RootCA.crt
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone Certificate
Remove Certificate

2. Select the intermediate certificate file and click **Open**.

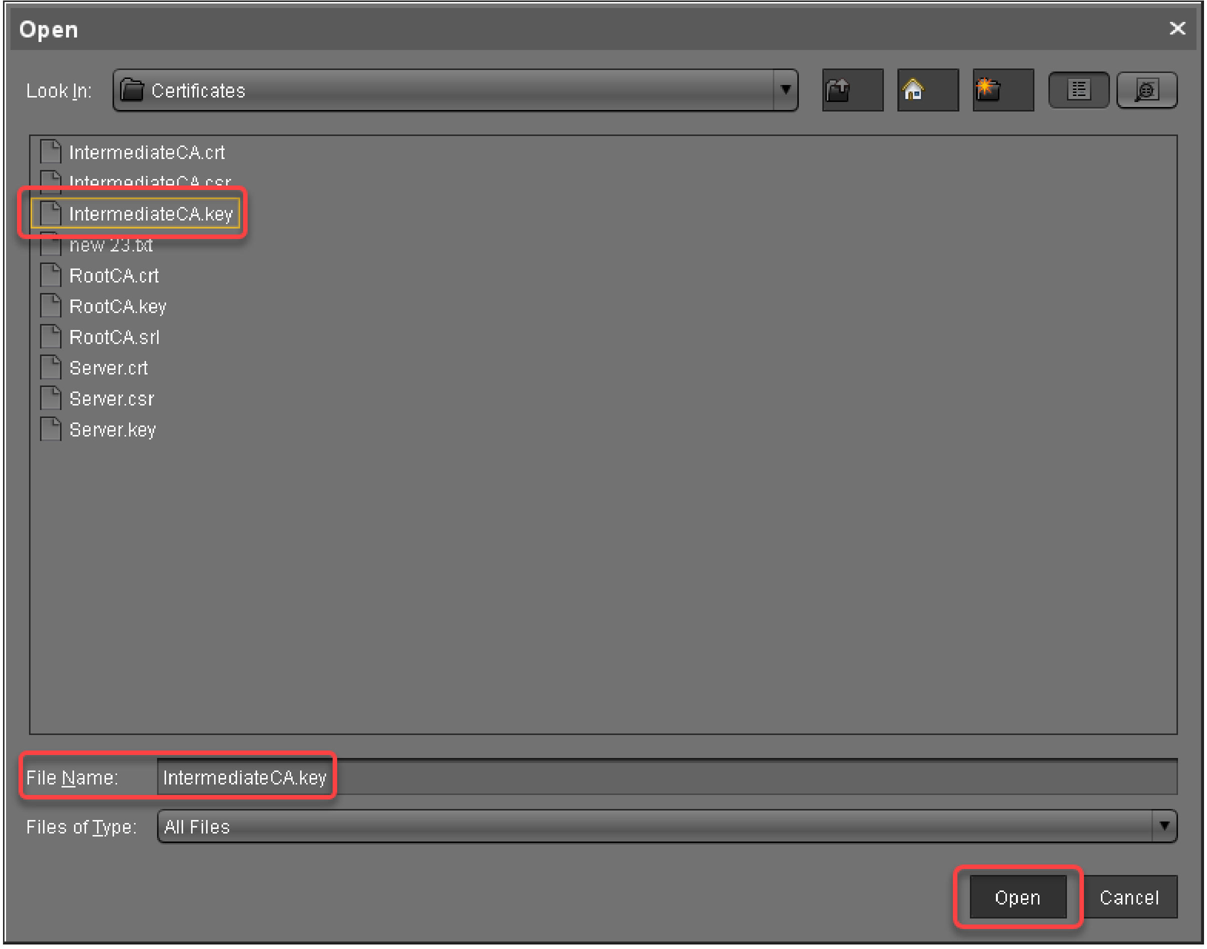


The intermediate certificate is imported.

3. Select the intermediate certificate, open the context menu, and select **Import decrypted private key**.


RootCA.crt
IntermediateCA.crt
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone Certificate
Remove Certificate

4. Select the private key file of the intermediate certificate and click **Open**.



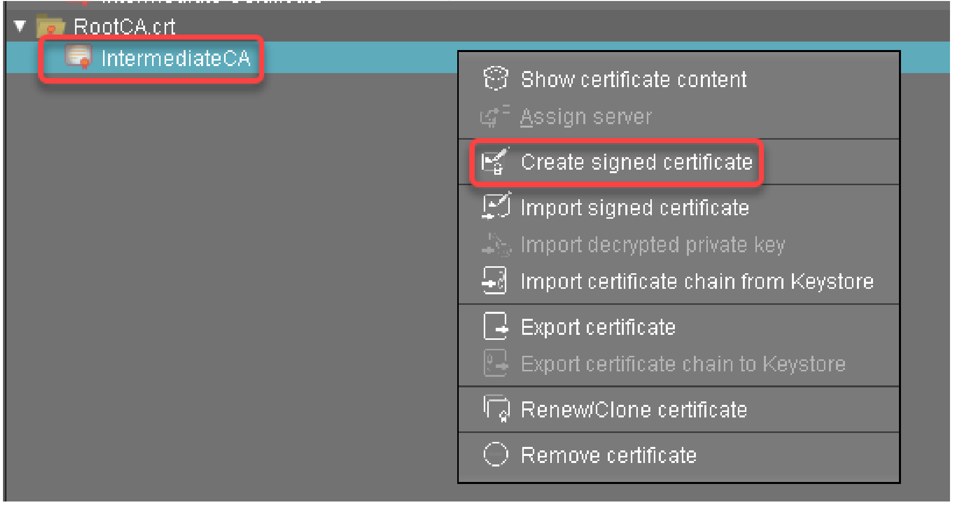
The private key of the intermediate certificate is imported.

> ⚠ The private key is encrypted again when saved into the UMS Database.

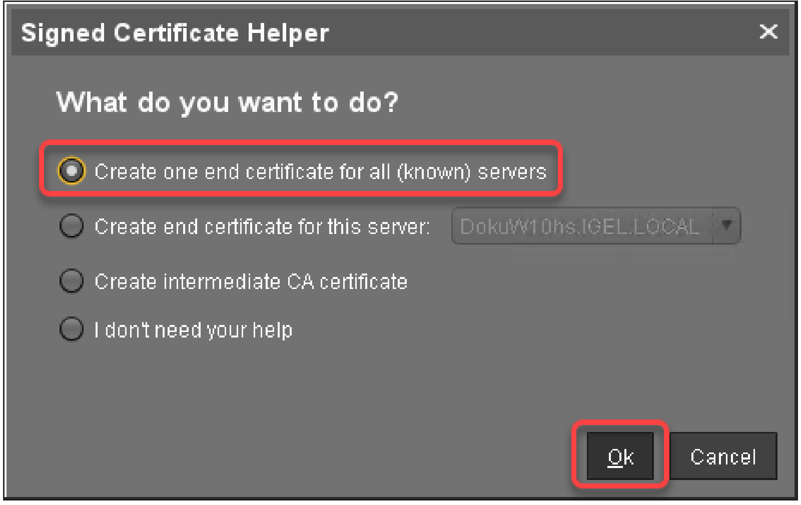
Creating End Certificates

Repeat the following steps for each server in your UMS environment:

1. Select the intermediate certificate, open the context menu, and select **Create signed certificate**.


RootCA.crt
IntermediateCA
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone certificate
Remove certificate

2. In the **Signed Certificate Helper**, select **Create one end certificate for all (known) servers**.


Signed Certificate Helper

What do you want to do?

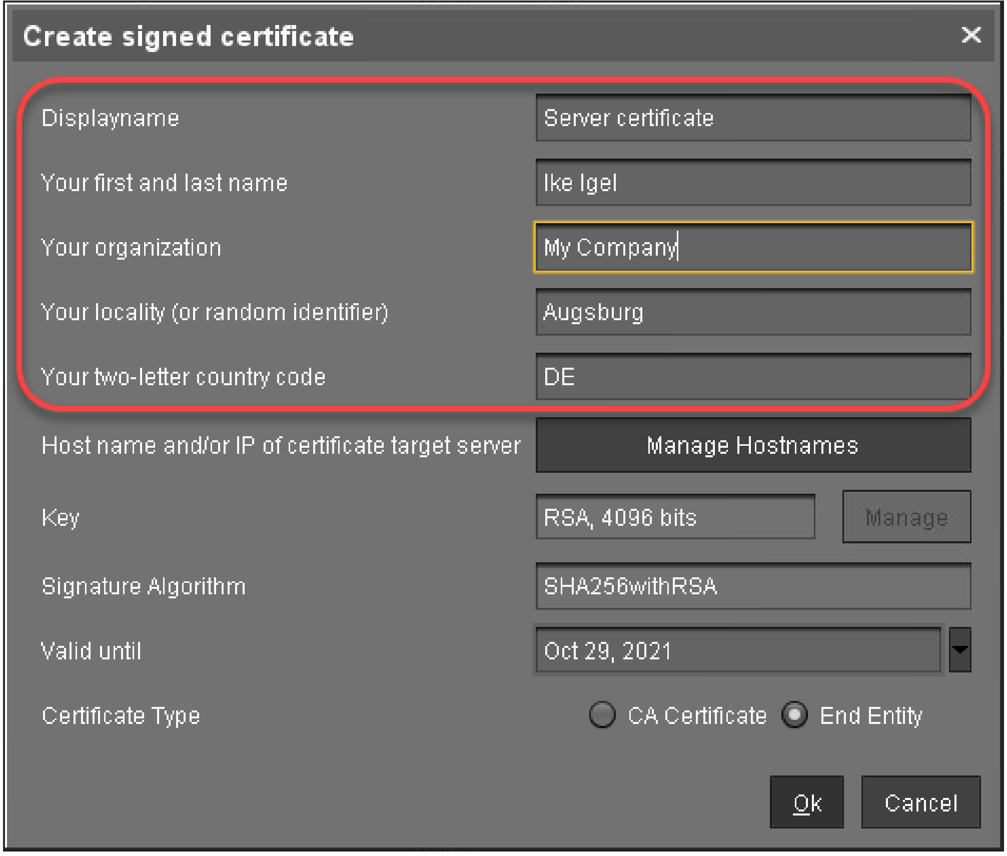
● Create one end certificate for all (known) servers

○ Create end certificate for this server: DokuW10hs.IGEL.LOCAL

○ Create intermediate CA certificate

○ I don't need your help

3. In the dialog **Create Signed Certificate**, fill in the data as required.



Create signed certificate

Displayname: Server certificate

Your first and last name: Ike Igel

Your organization: My Company

Your locality (or random identifier): Augsburg

Your two-letter country code: DE

Host name and/or IP of certificate target server: Manage Hostnames

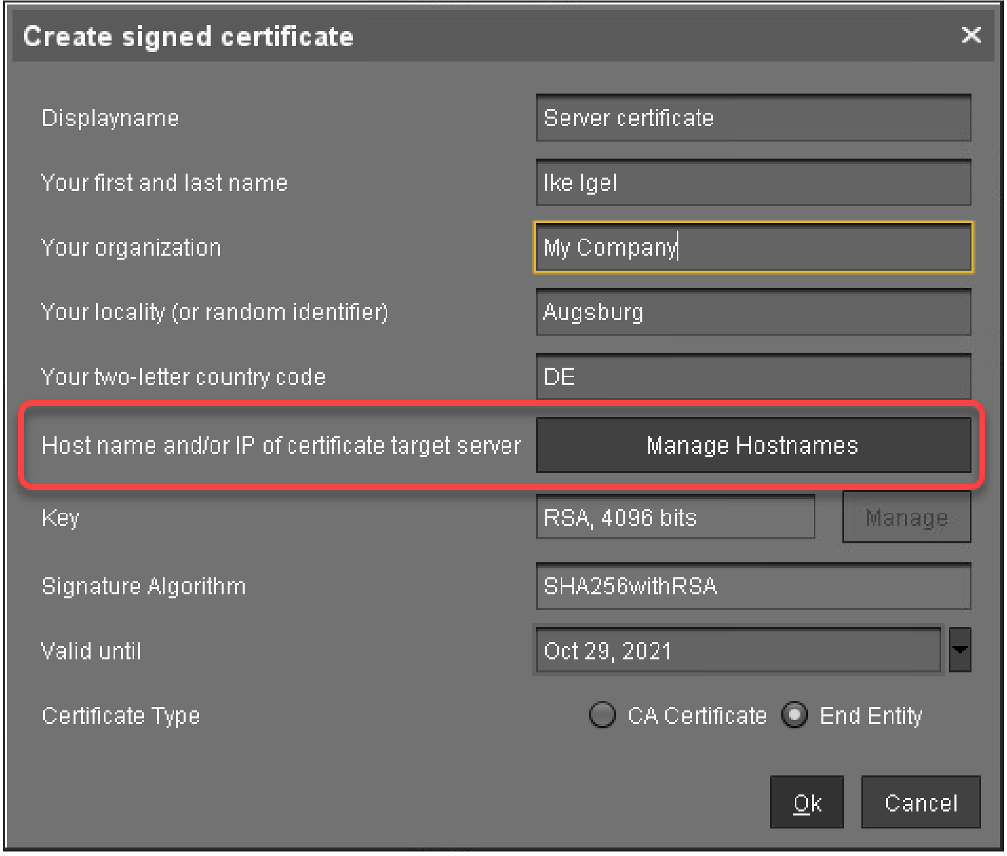
Key: RSA, 4096 bits

Signature Algorithm: SHA256withRSA

Valid until: Oct 29, 2021

Certificate Type: ○ CA Certificate ● End Entity

4. Click **Manage hostnames**.



Create signed certificate

Displayname: Server certificate

Your first and last name: Ike Igel

Your organization: My Company

Your locality (or random identifier): Augsburg

Your two-letter country code: DE

Host name and/or IP of certificate target server: Manage Hostnames

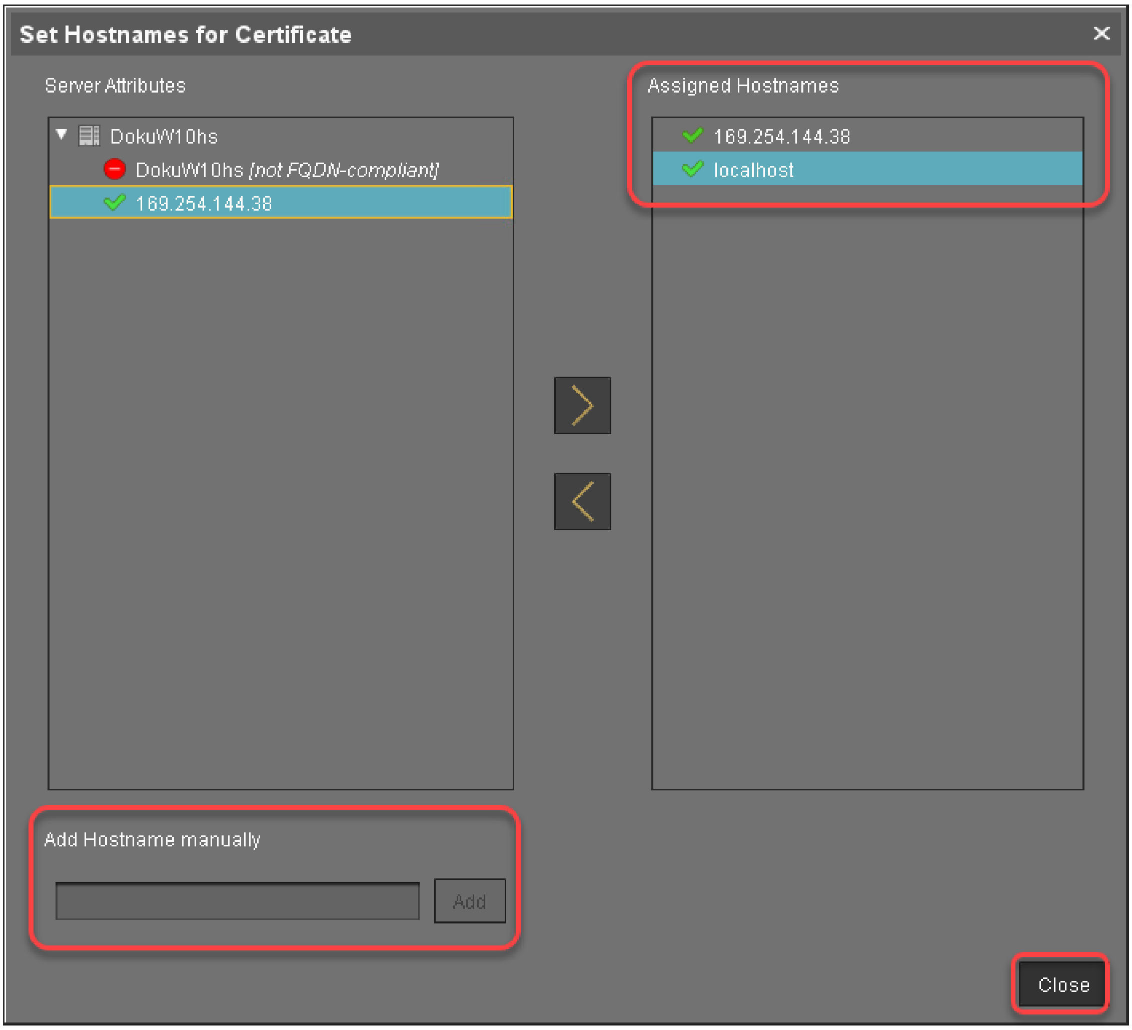
Key: RSA, 4096 bits — Manage

Signature Algorithm: SHA256withRSA

Valid until: Oct 29, 2021

Certificate Type: ○ CA Certificate ● End Entity

5. In the dialog **Set Hostnames for Certificate**, adjust the settings as follows:
   - Check if "localhost" and all IP addresses and FQDNs (Fully Qualified Domain Names) under which your server is reachable are displayed under **Assigned hostnames**. If not, add the missing IP addresses and FQDNs under **Add hostname manually**.
   - Remove all IP addresses and FQDNs you do not want to be part of the certificate.



Set Hostnames for Certificate

Server Attributes

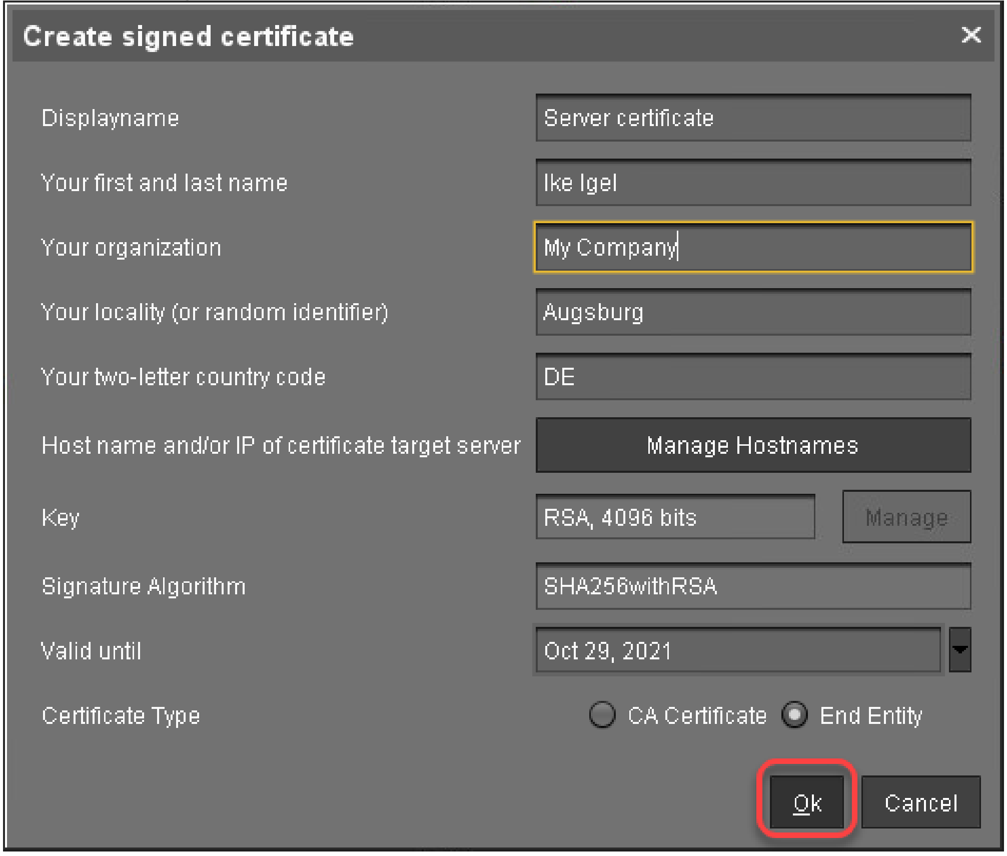
- DokuW10hs
  - DokuW10hs *[not FQDN-compliant]*
  - ✓ 169.254.144.38

Assigned Hostnames

- ✓ 169.254.144.38
- ✓ localhost

Add Hostname manually

6. Close the dialog **Create Signed Certificate** with **Ok**.



Create signed certificate

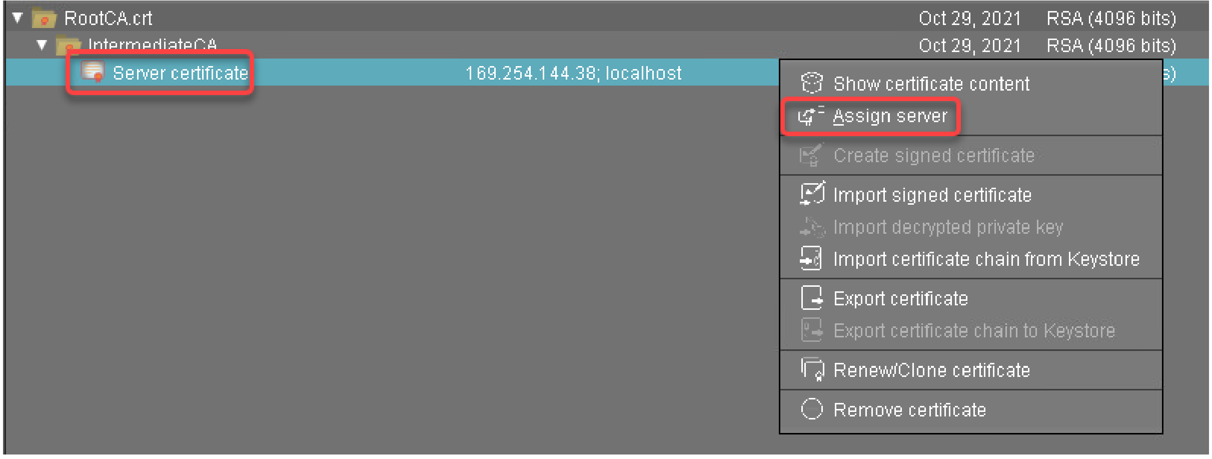
Displayname	Server certificate
Your first and last name	Ike Igel
Your organization	My Company
Your locality (or random identifier)	Augsburg
Your two-letter country code	DE
Host name and/or IP of certificate target server	Manage Hostnames
Key	RSA, 4096 bits
Signature Algorithm	SHA256withRSA
Valid until	Oct 29, 2021
Certificate Type	○ CA Certificate ● End Entity

The signed server certificate is created.

7. Continue with Assigning all Servers to the Certificate (see page 212).

Assigning All Servers to the Certificate

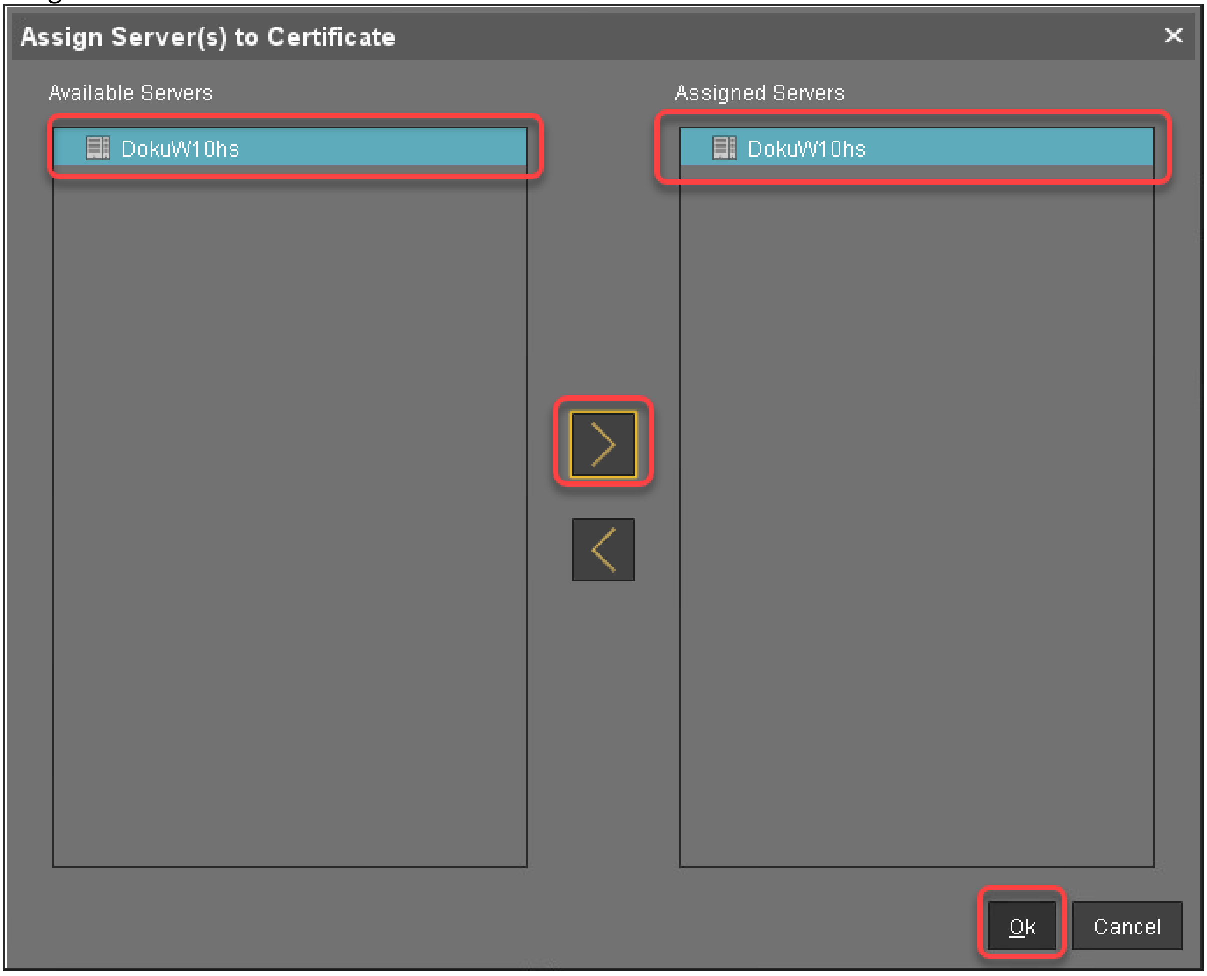
1. Select the server certificate, open the context menu, and select **Assign server**.



RootCA.crt		Oct 29, 2021	RSA (4096 bits)
IntermediateCA		Oct 29, 2021	RSA (4096 bits)
Server certificate	169.254.144.38; localhost		

Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to Keystore
Renew/Clone certificate
Remove certificate

2. Assign all servers to the certificate.



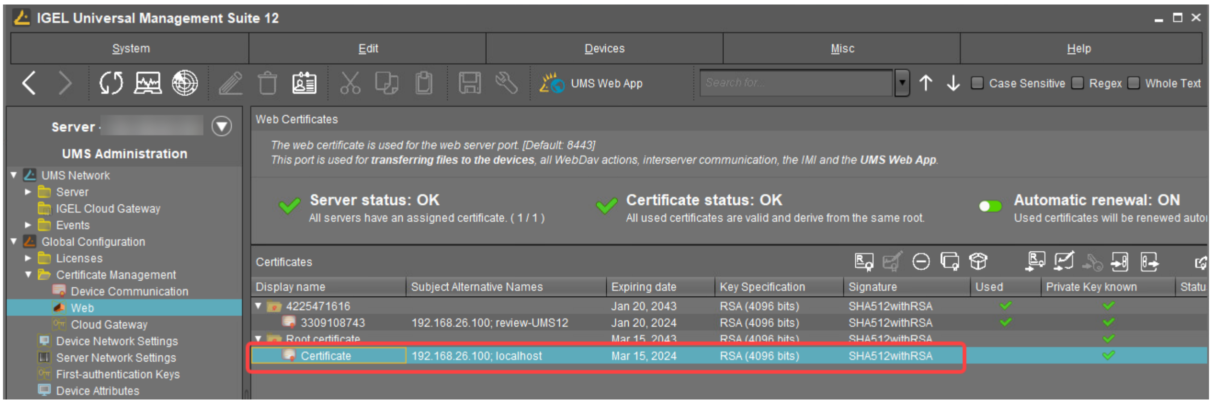
3. If you are managing IGEL OS 12 devices, see If You Exchange a Root Web Certificate for IGEL OS 12 Devices (see page 213).

If You Exchange a Root Web Certificate for IGEL OS 12 Devices

ⓘ New root web certificates are deployed to IGEL OS 12 devices on reboot.

For IGEL OS 12 devices, you can view which devices will no longer trust the UMS and will be unmanageable when you assign a new root certificate:

1. Select the certificate you want to be used under **UMS Console > UMS Administration > Global Configuration > Certificate Management > Web**.



Web Certificates

The web certificate is used for the web server port. [Default: 8443]
*This port is used for **transferring files to the devices**, all WebDav actions, interserver communication, the IMI and the **UMS Web App**.*

✓ **Server status: OK**
All servers have an assigned certificate. (1 / 1)

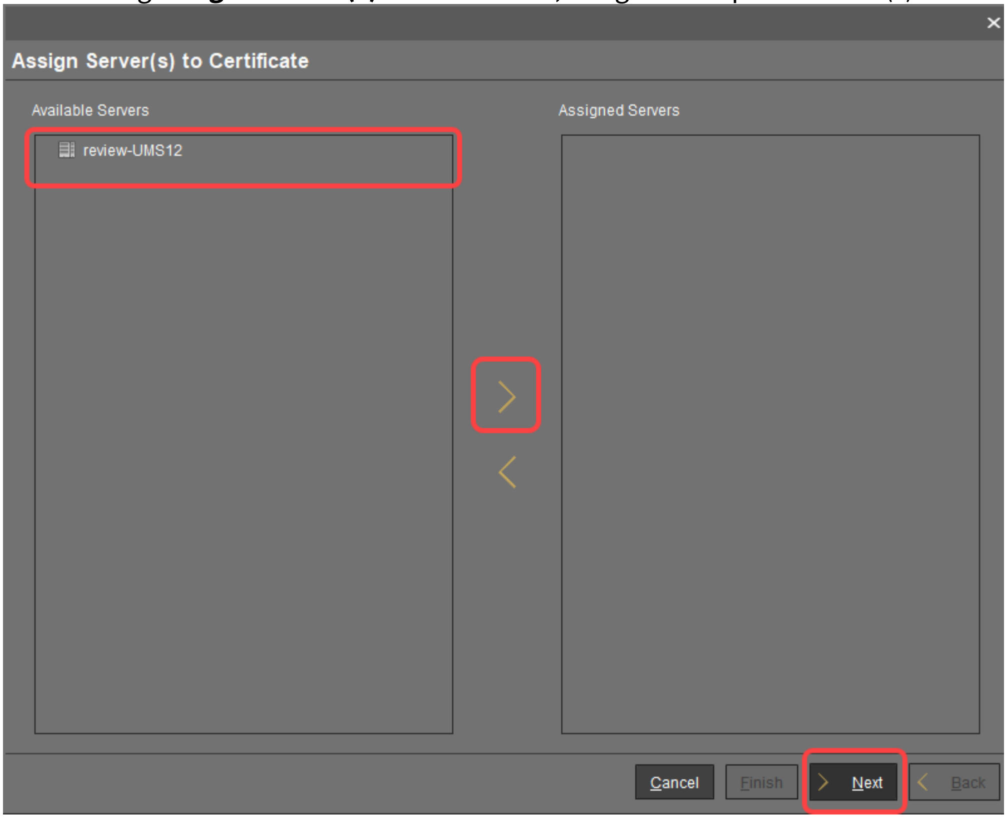
✓ **Certificate status: OK**
All used certificates are valid and derive from the same root.

Automatic renewal: ON
Used certificates will be renewed auto

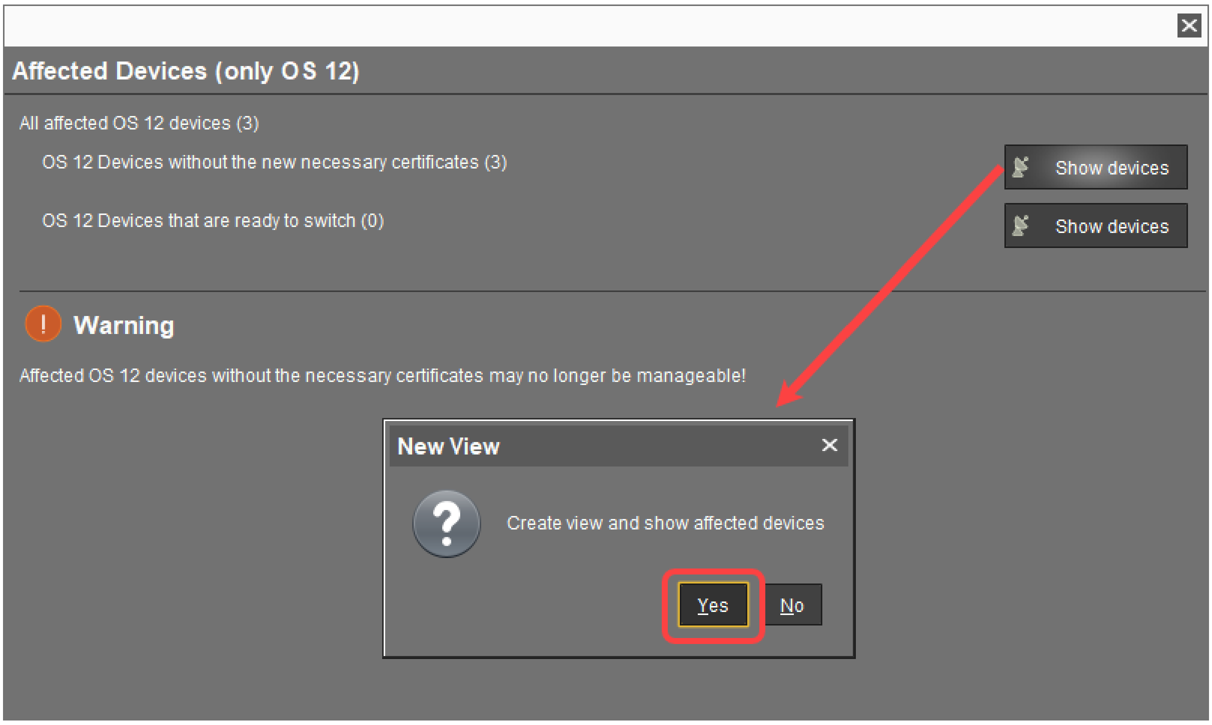
Display name	Subject Alternative Names	Expiring date	Key Specification	Signature	Used	Private Key known	Statu
▼ 4225471616		Jan 20, 2043	RSA (4096 bits)	SHA512withRSA	✓	✓	
3309108743	192.168.26.100; review-UMS12	Jan 20, 2024	RSA (4096 bits)	SHA512withRSA	✓	✓	
▼ Root certificate		Mar 15, 2043	RSA (4096 bits)	SHA512withRSA		✓	
Certificate	192.168.26.100; localhost	Mar 15, 2024	RSA (4096 bits)	SHA512withRSA		✓	

2. Click or select **Assign server** in the context menu.

3. In the dialog **Assign Servers(s) to Certificate**, assign the required server(s) and click **Next**.



4. For IGEL OS 12 devices, you will see the **Affected Devices** dialog. Review it:
If the **OS 12 devices without the new necessary certificates** number = 0 and there is no warning dialog, you can complete the assignment. The devices will safely switch to the new certificate.
If the **OS 12 devices without the new necessary certificates** number > 0, click **Show devices** to create a view that collects the affected devices:



Affected Devices (only OS 12)

All affected OS 12 devices (3)

OS 12 Devices without the new necessary certificates (3)

OS 12 Devices that are ready to switch (0)

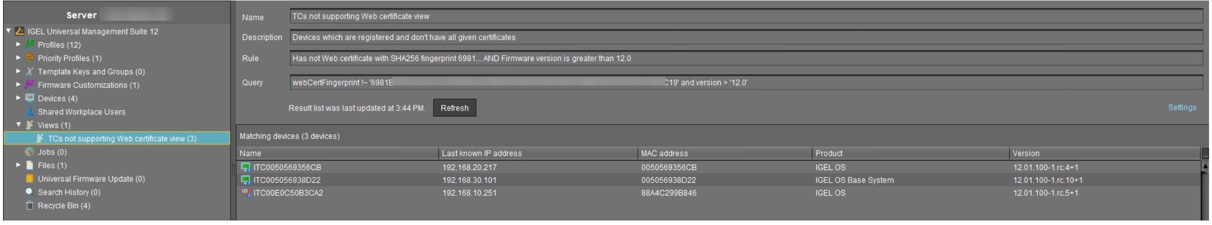
Warning

Affected OS 12 devices without the necessary certificates may no longer be manageable!

New View

Create view and show affected devices

The view is created, and the UMS Console switches to the newly created view.



Server [redacted]
IGEL Universal Management Suite 12
Profiles (12)
Priority Profiles (1)
Template Keys and Groups (0)
Firmware Customizations (1)
Devices (4)
Shared Workplace Users
Views (1)
TCs not supporting Web certificate view (3)
Jobs (0)
Files (1)
Universal Firmware Update (0)
Search History (0)
Recycle Bin (4)
Refresh
Settings

Name: TCs not supporting Web certificate view

Description: Devices which are registered and don't have all given certificates

Rule: Has not Web certificate with SHA256 fingerprint 6981... AND Firmware version is greater than 12.0

Query: webCertFingerprint !~ '6981E[redacted]C19' and version > '12.0'

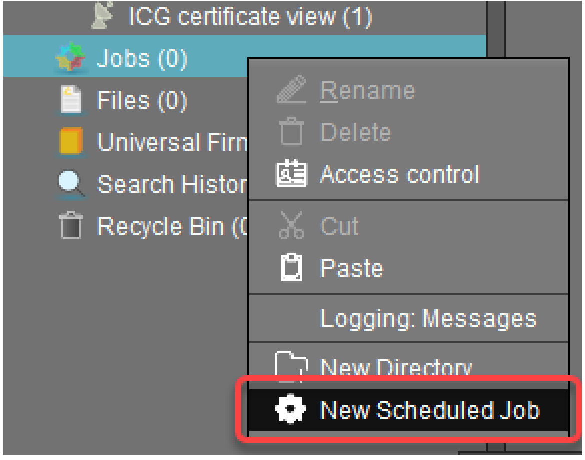
Result list was last updated at 3:44 PM.

Matching devices (3 devices)

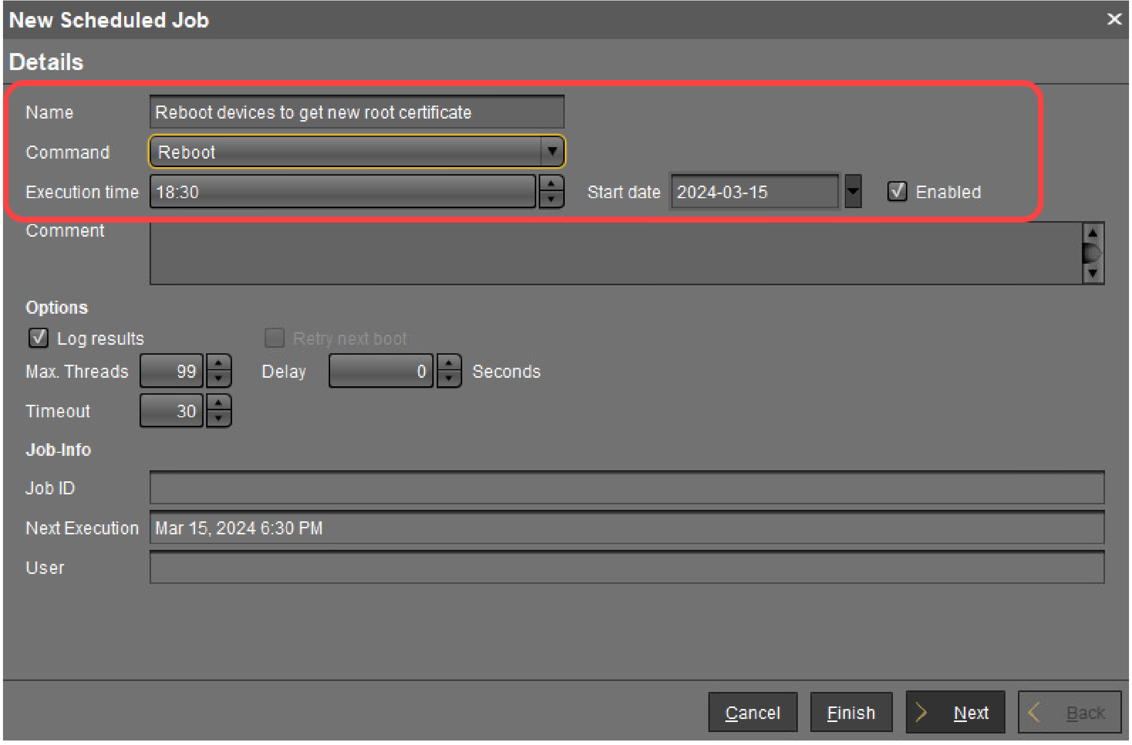
Name	Last known IP address	MAC address	Product	Version
ITC0050569356CB	192.168.20.217	0050569356CB	IGEL OS	12.01.100-1.rc.4+1
ITC005056938D22	192.168.30.101	005056938D22	IGEL OS Base System	12.01.100-1.rc.10+1
ITC00E0C50B3CA2	192.168.10.251	88A4C299B846	IGEL OS	12.01.100-1.rc.5+1

Now, it is necessary to restart the affected devices. On reboot, the devices will receive all certificates from the UMS; afterward, they are ready to switch to the new certificate.
To restart all affected devices at a defined time, it makes sense to create a scheduled job.

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



6. In the **New Scheduled Job** window, change the settings as follows and click **Next**:
   - **Name**: A name for the job
   - **Command**: Select "Reboot"
   - **Execution time**: Select the time at which the restart should take place.


New Scheduled Job

Details

Name: Reboot devices to get new root certificate

Command: Reboot

Execution time: 18:30 Start date: 2024-03-15 ☑ Enabled

Comment:

Options

☑ Log results ☐ Retry next boot

Max. Threads: 99 Delay: 0 Seconds

Timeout: 30

Job-Info

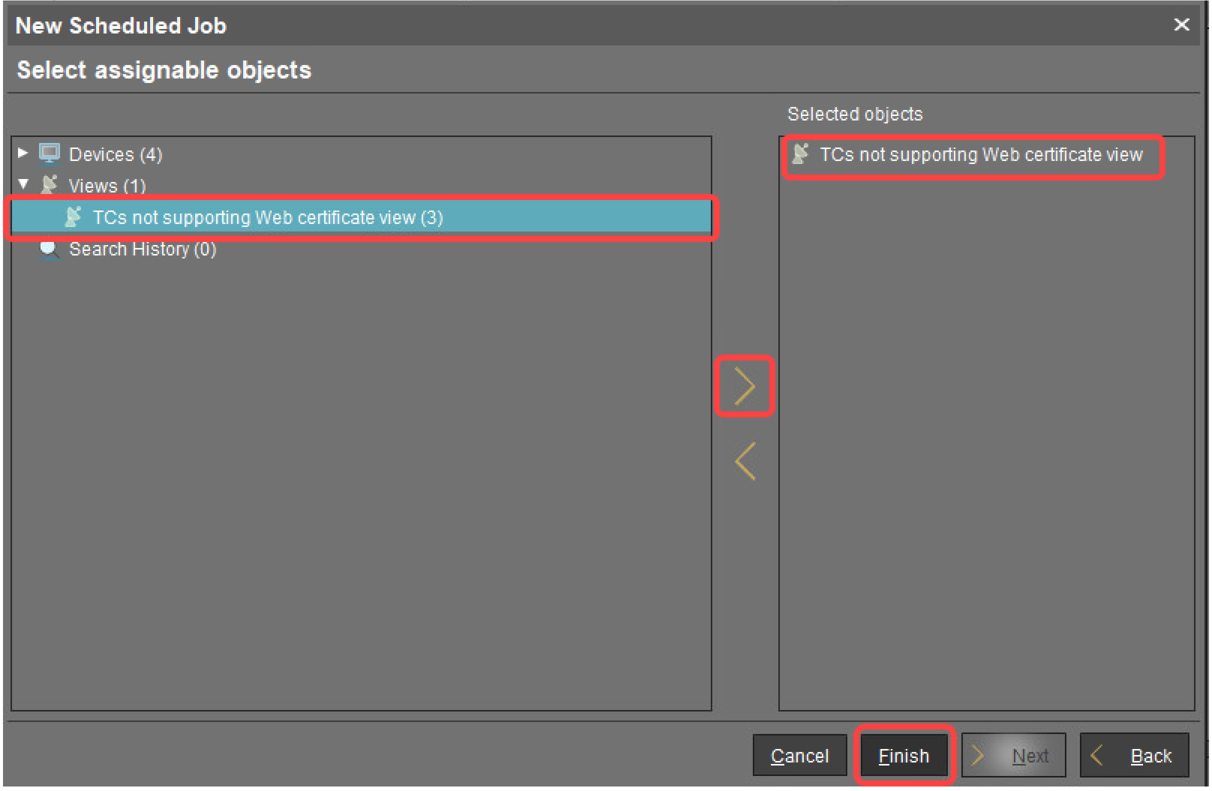
Job ID:

Next Execution: Mar 15, 2024 6:30 PM

User:

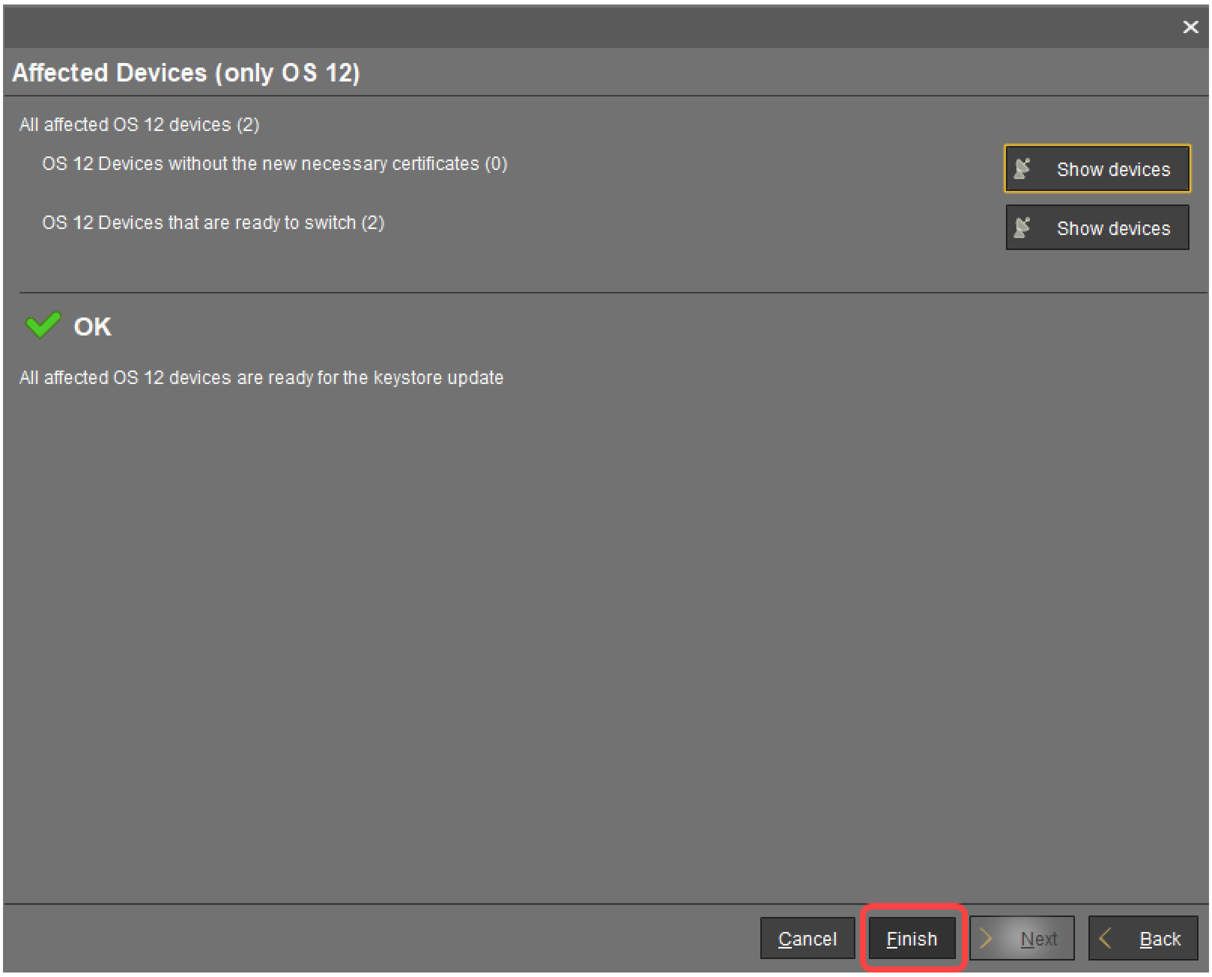
7. In the next step, leave the settings as they are and click **Next**.

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


New Scheduled Job
Select assignable objects
Selected objects
Devices (4)
Views (1)
TCs not supporting Web certificate view (3)
Search History (0)
TCs not supporting Web certificate view
Cancel
Finish
Next
Back

9. After the reboot, complete the assignment: Under **UMS Administration > Global Configuration > Certificate Management > Web**, select the required certificate and click ⧉ or **Assign server** in the context menu.
If the output in the **Affected Devices** dialog is like this, click **Finish**. The devices will safely switch

to the new certificate.



Affected Devices (only OS 12)

All affected OS 12 devices (2)

OS 12 Devices without the new necessary certificates (0)

OS 12 Devices that are ready to switch (2)

✓ OK

All affected OS 12 devices are ready for the keystore update

Wake on LAN

Deploying a Wake on LAN Proxy for Distributed Environments

Problem

The UMS is residing outside the network which contains your devices, so it cannot wake up your devices by Wake on LAN.

Goal

You want the UMS to wake up your devices from outside their network.

Solution

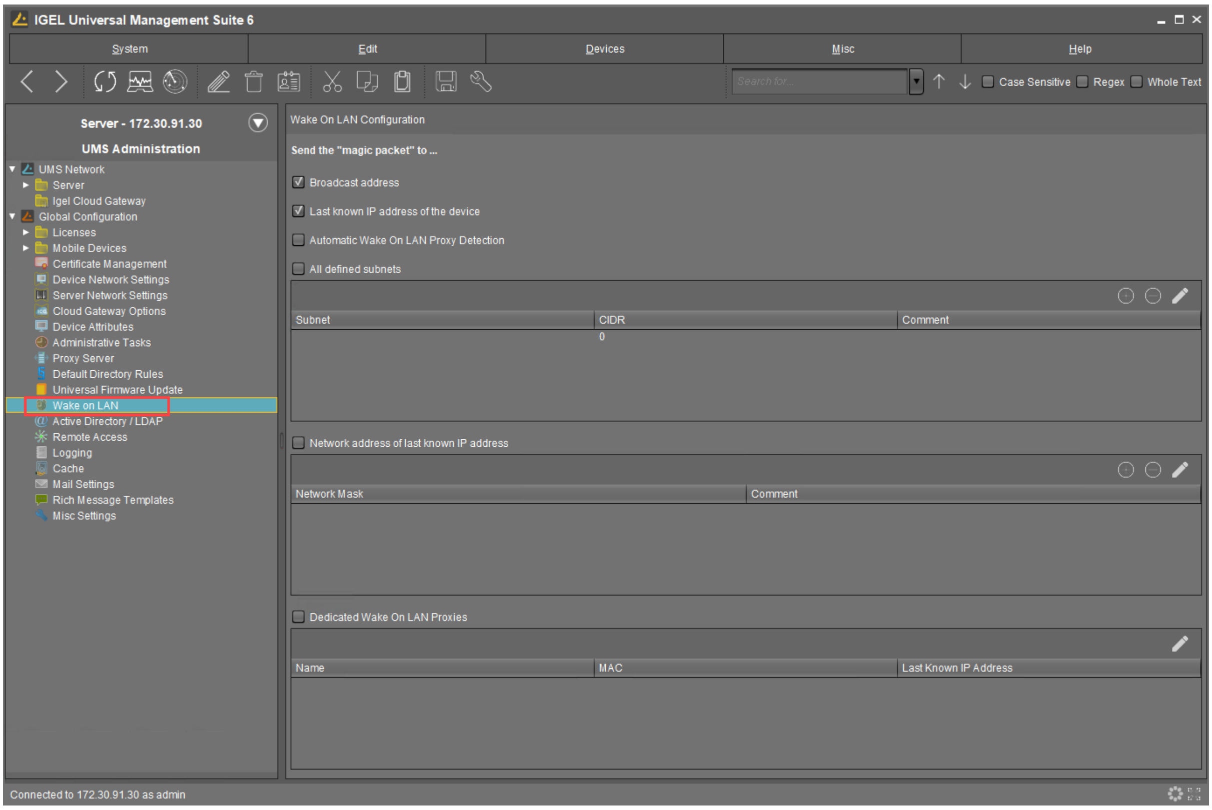
If you are using UMS version 5.02.100 or higher and devices running Linux version 5.09.100 or higher, you can make a device act as a proxy which sends the Wake on LAN packets on behalf of the UMS.

Defining Devices as Wake on LAN Proxy

You can define one or more devices as a Wake on LAN proxy.

To define a device as a Wake on LAN proxy:

1. Logon to the UMS console.
2. Go to **UMS Administration**.
3. Select **Wake on LAN**.



Wake On LAN Configuration

Send the "magic packet" to ...

☑ Broadcast address

☑ Last known IP address of the device

☐ Automatic Wake On LAN Proxy Detection

☐ All defined subnets

Subnet	CIDR	Comment
	0	

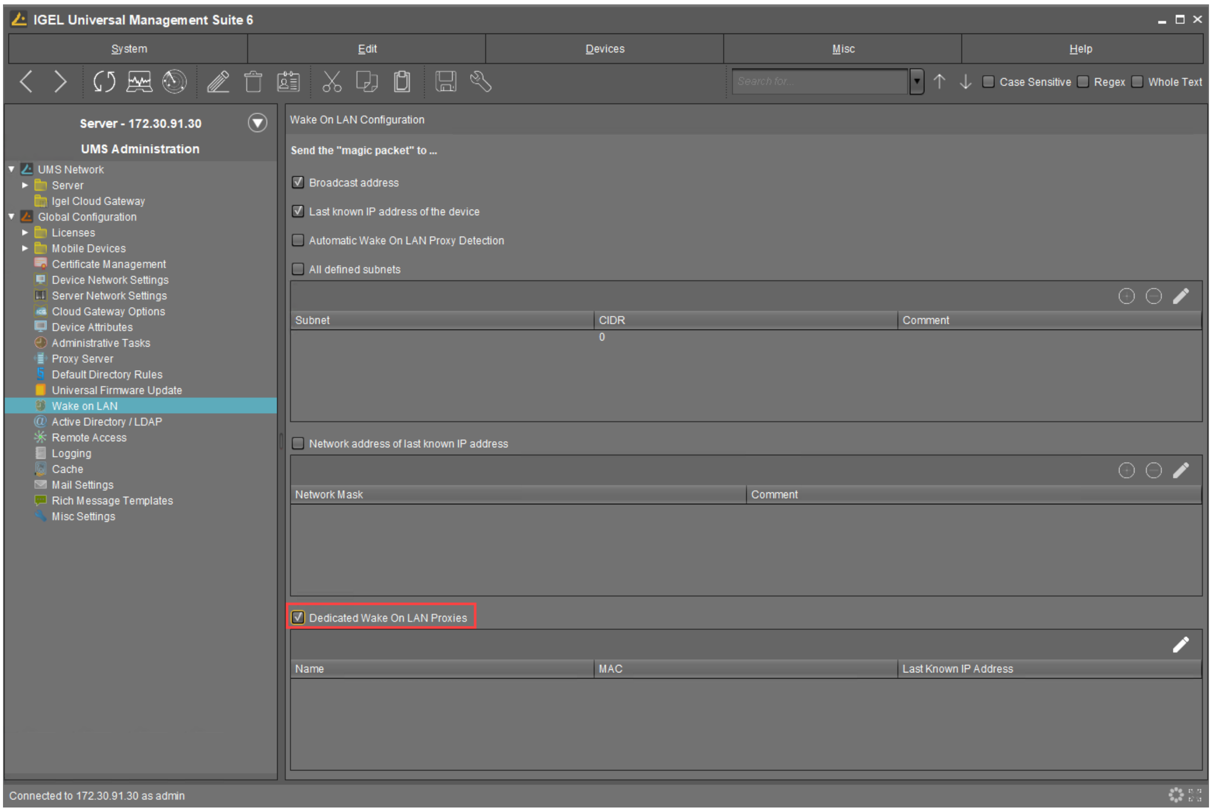
☐ Network address of last known IP address

Network Mask	Comment

☐ Dedicated Wake On LAN Proxies

Name	MAC	Last Known IP Address

4. Activate **Dedicated Wake on LAN Proxies**.



Wake On LAN Configuration

Send the "magic packet" to ...

☑ Broadcast address

☑ Last known IP address of the device

☐ Automatic Wake On LAN Proxy Detection

☐ All defined subnets

Subnet	CIDR	Comment
	0	

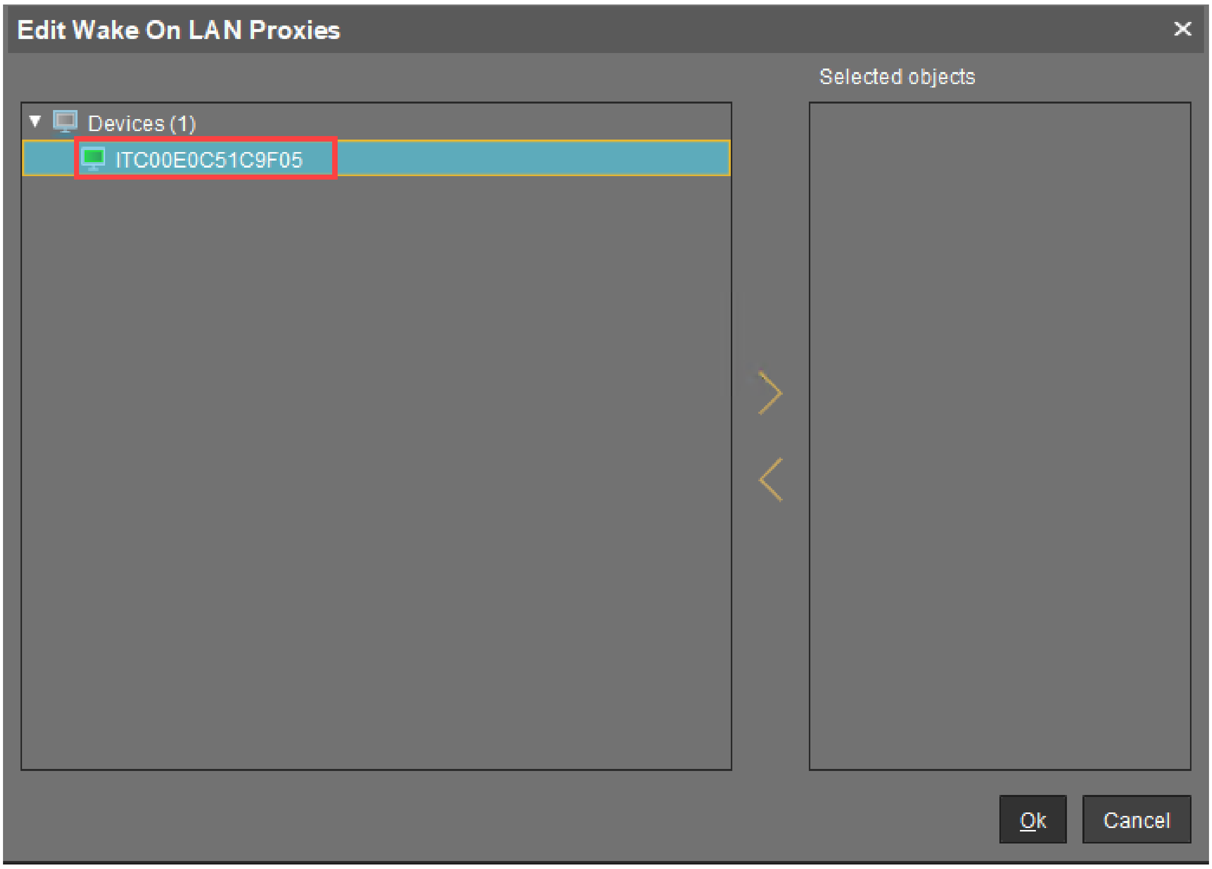
☐ Network address of last known IP address

Network Mask	Comment

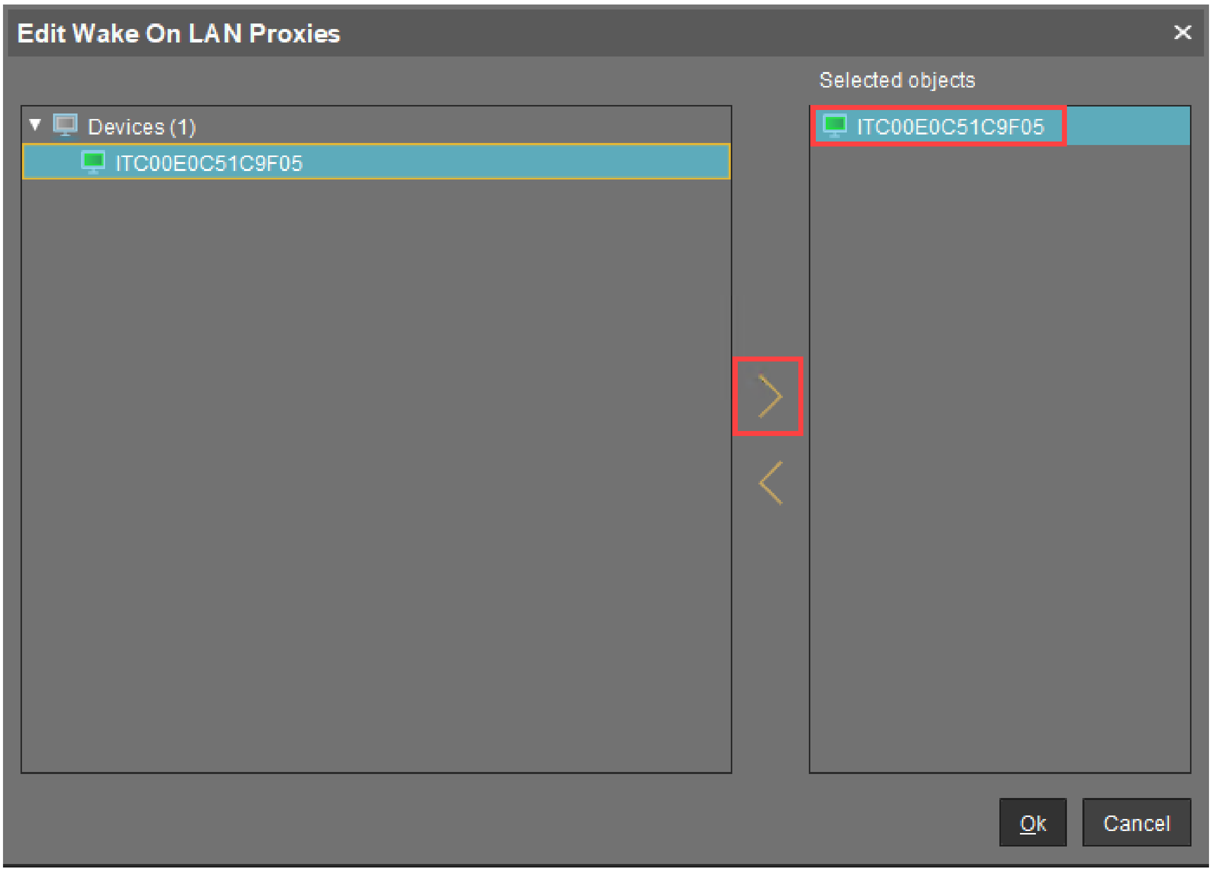
☑ Dedicated Wake On LAN Proxies

Name	MAC	Last Known IP Address

5. Click ✎.
   The dialog **Edit Wake ON LAN Proxies** opens.
6. Select the device you want to use as a Wake on LAN proxy.



7. Click ❯.
   The selected device is listed under **Selected objects**.



8. Click **Ok**.
   The selected device is configured as a Wake on LAN proxy. In the device's registry, the **parameter** `system.remotemanager.wol_proxy.enabled` is set to true.

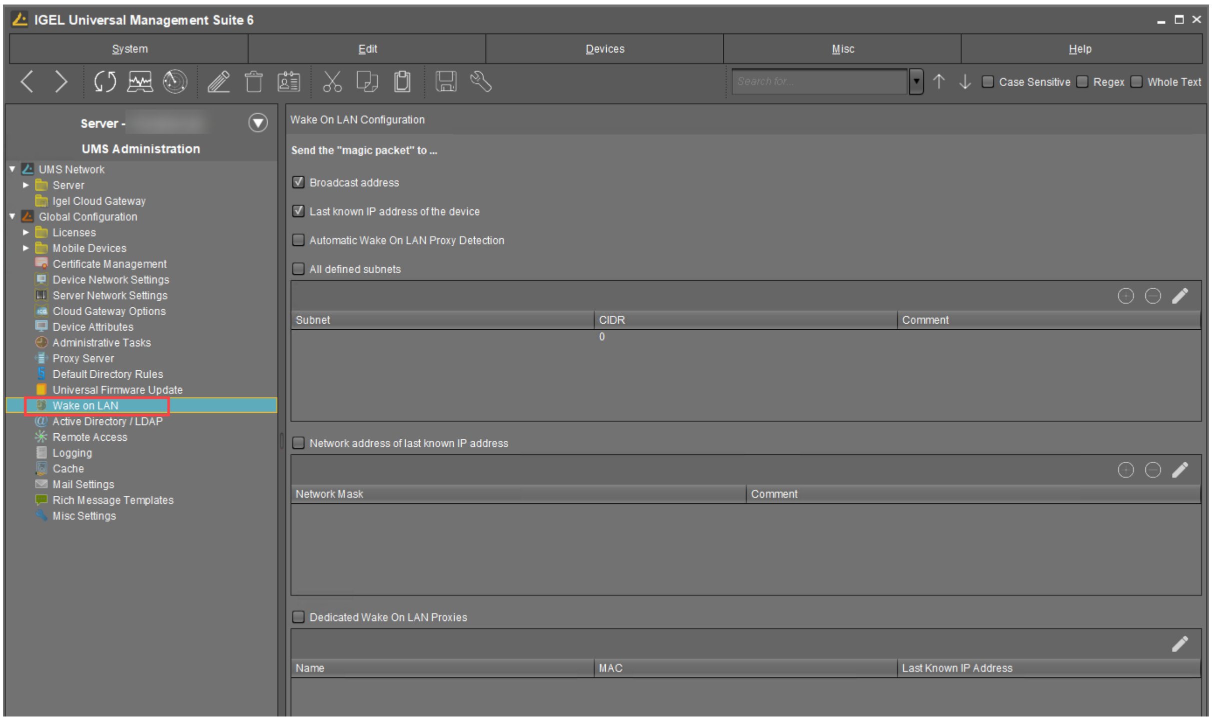
> ⓘ A device that is configured as a Wake on LAN proxy cannot be set to standby or shut down. This lock is in effect as soon as the device has received its settings from the UMS.

Removing a Wake on LAN proxy

You can remove the Wake on LAN proxy function from a device.

To define one or more devices as Wake on LAN Proxy:

1. Log in to the UMS Console.
2. Go to **UMS Administration**.
3. Select **Wake on LAN**.



Wake On LAN Configuration

Send the "magic packet" to ...

☑ Broadcast address

☑ Last known IP address of the device

☐ Automatic Wake On LAN Proxy Detection

☐ All defined subnets

Subnet	CIDR	Comment
	0	

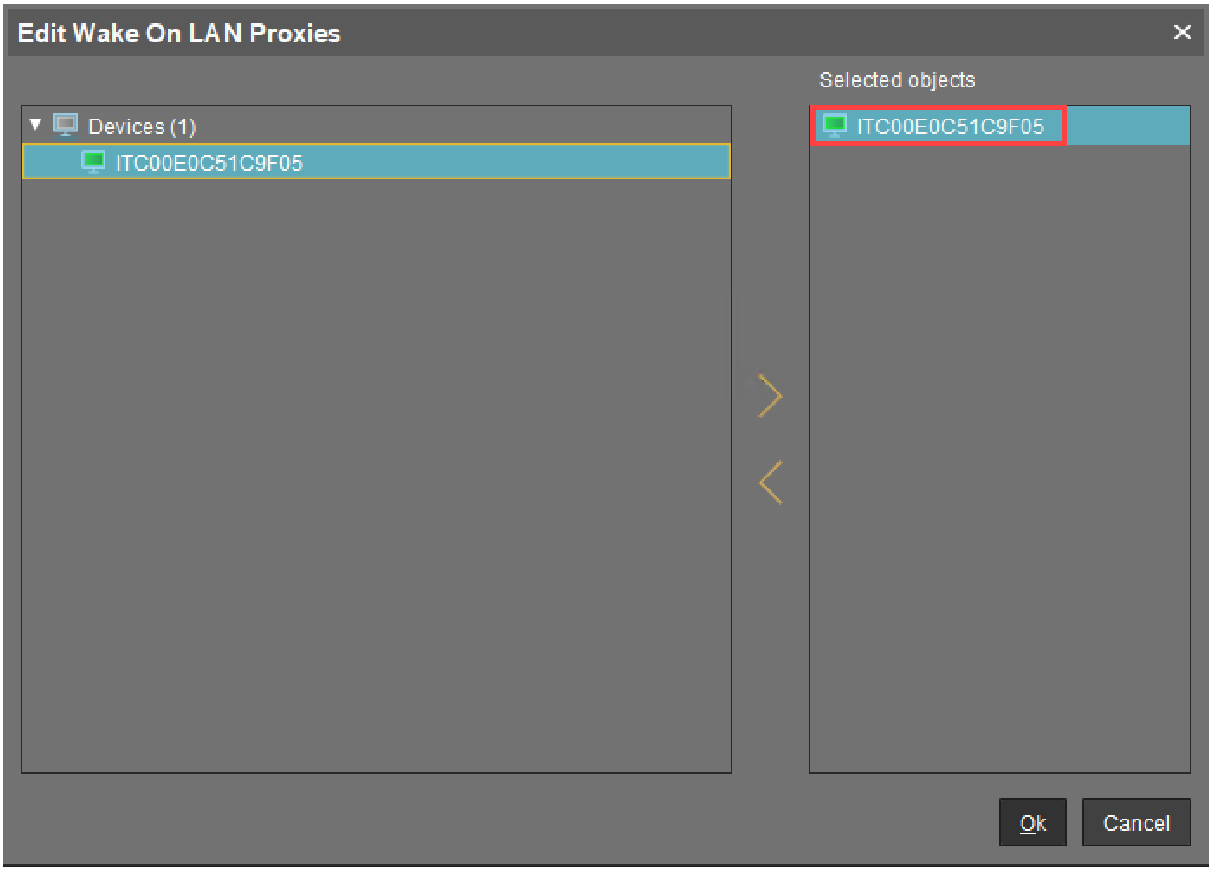
☐ Network address of last known IP address

Network Mask	Comment

☐ Dedicated Wake On LAN Proxies

Name	MAC	Last Known IP Address

4. Click ✎.
   The dialog **Edit Wake ON LAN Proxies** opens.
5. Select the device you do not want to use as Wake on LAN proxy.



6. Click ‹ .
7. Click **Ok**.
   The selected device is no longer configured as a Wake on LAN proxy. As soon as the device has received its settings from the UMS, it can be set to standby and shut down as normal. In the device's registry, the parameter **system > remotemanager > wol_proxy > enabled** is set to "false".

Distributing Wake on LAN Packets

IGEL UMS sends the magic packets as UDP datagrams to port 9. In order to work for different subnets, this has to be supported by the routers involved.

Wake on LAN settings can be configured in **UMS Console** under **UMS Administration > Global Configuration > Wake on LAN**.

UMS supports sending Wake on LAN magic packets to

- the broadcast address
- the last known IP address of the device
- all defined subnets
- the network address of the last known device IP address (define one or more network masks to be applied)
- a dedicated Wake on LAN proxy to wake up thin clients in another network; see Use a WoL Proxy for Waking up Devices (see page 228)

Use a WoL Proxy for Waking up Devices

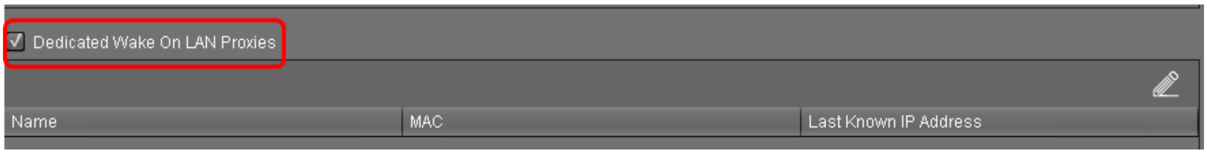
You have the possibility to wake up devices even if they live in a different network that does not allow broadcast packets from the WAN. The trick is to set up one or more devices as Wake-on-LAN proxy. A device acting as a Wake-on-LAN proxy will never fall asleep itself, as its job is to listen to a special wake-up call from the UMS. This wake-up call tells the Wake-on-LAN proxy to send magic packets to all devices or a selection of devices in its network. To support this functionality, the Wake-on-LAN proxy device must have IGEL Linux version 5.09.100 or higher.

You can define a dedicated Wake-on-LAN proxy, or, alternatively, set the UMS to determine a Wake-on-LAN proxy automatically. However, the latter option cannot guarantee that a Wake-on-LAN proxy can be defined, as this depends on an appropriate device being online in the relevant subnet.

For detailed information, see the Wake on LAN chapter in the manual.

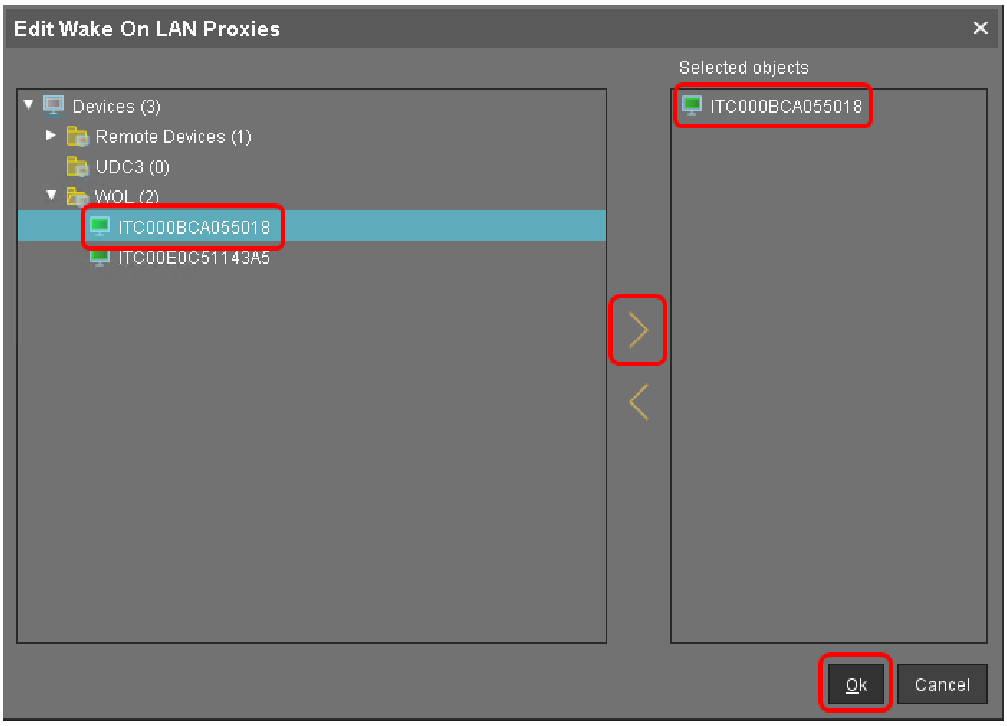
To define a dedicated Wake-on-LAN proxy:

1. Go to **UMS Administration > Global Configuration > Wake On LAN**.
2. Under **Send the "magic packet to ..."**, choose the adress(es) to which the Wake-on-LAN proxies should send their wake-up calls.
3. Activate **Dedicated Wake On LAN Proxies**.



☑ Dedicated Wake On LAN Proxies

4. In the area below **Dedicated Wake On LAN Proxies**, click on ✎.
5. Highlight the desired device in the left-hand column.
6. Click on › to select the device.
7. Click on **OK**.



The device will now function as a Wake-on-LAN proxy.

> ⓘ A device that is configured as a Wake-on-LAN proxy can no longer be put on standby or shut down. This restriction applies as soon as the device receives the settings from the UMS.

> ⓘ As an alternative or parallel one can also use the **Automatic WoL Proxy Detection**. However, you cannot be sure that this proxy is always running, while the **Dedicated WoL Proxy** is always running.

Using an HTTP Proxy for Firmware Updates in UMS

Symptom

You want UMS to download firmware updates from the Internet.

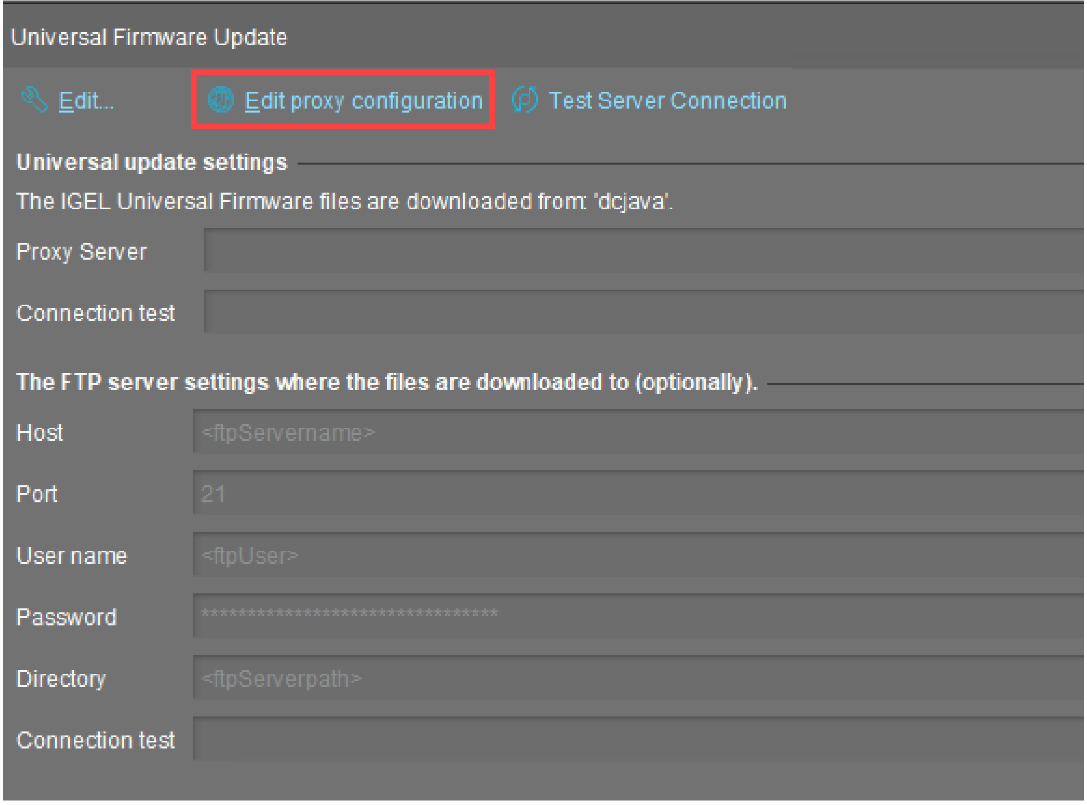
Problem

Internet access is only available via an HTTP proxy in your environment.

Solution

Configure an HTTP proxy for firmware downloads in UMS:

1. In UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**
2. Click **Edit Proxy Configuration**



Universal Firmware Update

Universal update settings

The IGEL Universal Firmware files are downloaded from: 'dcjava'.

Proxy Server

Connection test

The FTP server settings where the files are downloaded to (optionally).

Host: <ftpServername>

Port: 21

User name: <ftpUser>

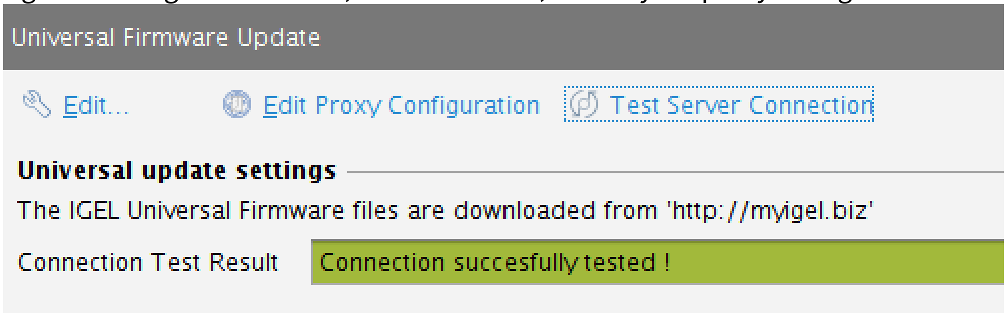
Password: ********************************

Directory: <ftpServerpath>

Connection test

The **Edit Proxy Configuration** dialog opens.
3. Check **Use proxy for HTTP connection to firmware update server**.
4. Enter the **Proxy-Host** name or IP address.
5. Enter the proxy host **Port**.

6. Enter the proxy **User**.
7. Enter the proxy **Password**.
8. Click **Save**.
   The dialog closes.
9. To test the connection via the proxy, click **Test Server Connection**.
   A green bar signifies success, if the bar is red, review your proxy configuration and test again.



Universal Firmware Update

Universal update settings

The IGEL Universal Firmware files are downloaded from 'http://myigel.biz'

Connection Test Result: Connection succesfully tested !

UMS Cannot Contact Download Server Any More

Symptom

After the UMS has been updated to version 6.03.130 or higher, it can not reach the download server anymore.

Environment

- UMS 6.03.130 or higher

Problem

From UMS 6.03.130 onwards, the UMS contacts https://fwus.igel.com (port 443) instead of http://fwu.igel.com (port 80). This may be blocked by a firewall.

Solution

▶ Allow https://fwus.igel.com (port 443) in your firewall.

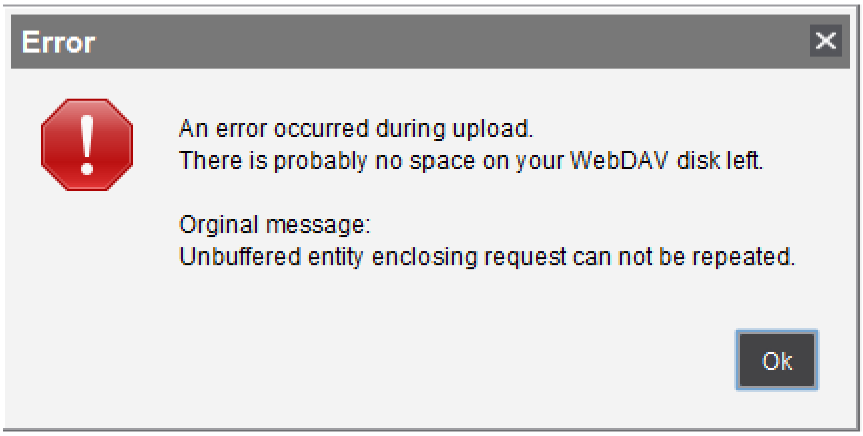
Error During Firmware Upload in UMS: No Space on WebDAV

Solution Based on Experience from the Field

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

Issue

When importing a firmware into the UMS, the following error message appears:



An error occurred during upload.
There is probably no space on your WebDAV disk left.

Orginal message:
Unbuffered entity enclosing request can not be repeated.

```
An error occurred during upload.
There is probably no space on your WebDAV disk left.

Original message:
Unbuffered entity enclosing request can not be repeated.
```

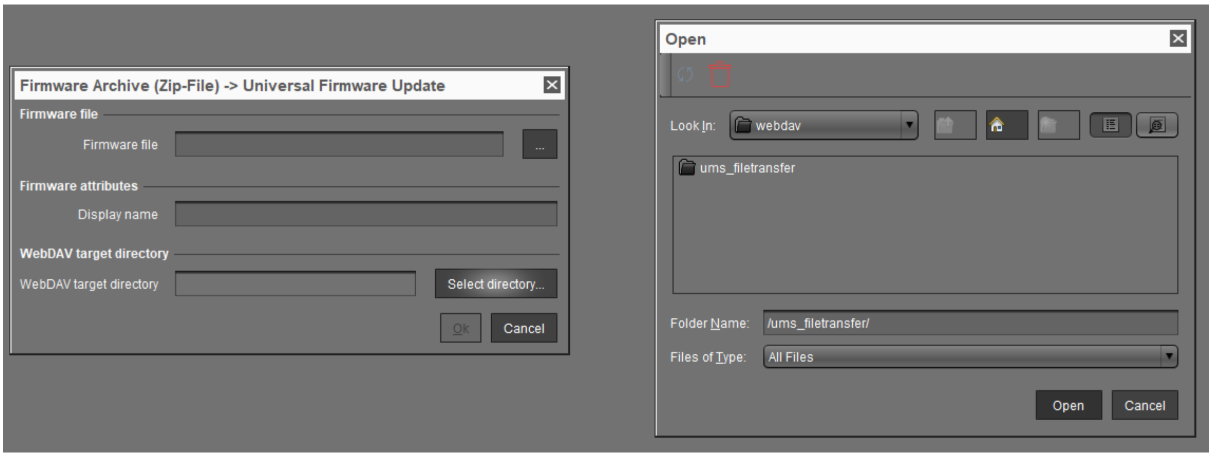
Cause

This error is caused when a file is being imported into a WebDAV folder which has no available space remaining.

Solution

1. Check that the host system of the UMS Server has available storage.

2. Ensure that the **ums_filetransfer** folder is selected during the firmware import process:



Look In: webdav

Folder Name: /ums_filetransfer/

Files of Type: All Files

How to Configure Java Heap Size for the UMS Server

You experience performance issues with IGEL Universal Management Suite (UMS). Manifold reasons can underlie performance degradation, and there are various solutions like optimizing the UMS according to recommendations under Performance Optimizations in IGEL UMS, expanding the server's physical RAM, switching from the embedded database to the external database, updating the UMS components, etc. The following article covers only the increase of UMS Server memory (Java heap size).

Symptom

You face performance problems and encounter memory issues in the UMS Server log files (`catalina.log` ; see Where Can I Find the IGEL UMS Log Files? (see page 332)), e.g. `java.lang.OutOfMemoryError` .

Problem

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

- numerous jobs
- numerous administrative tasks
- a lot of concurrent device requests (e.g. hundreds of devices booting up in a narrow time frame)
- a large number of devices in the database (>10.000)
- the UMS Web App installed
- the combination of the above factors

The more jobs, administrative tasks, etc. are created, the more heap is "eaten up", so there may be no memory left for additional tasks. In such situations, it can make sense to increase the Java heap size for the UMS Server.

Solution: Change Java Heap Size for the UMS Server

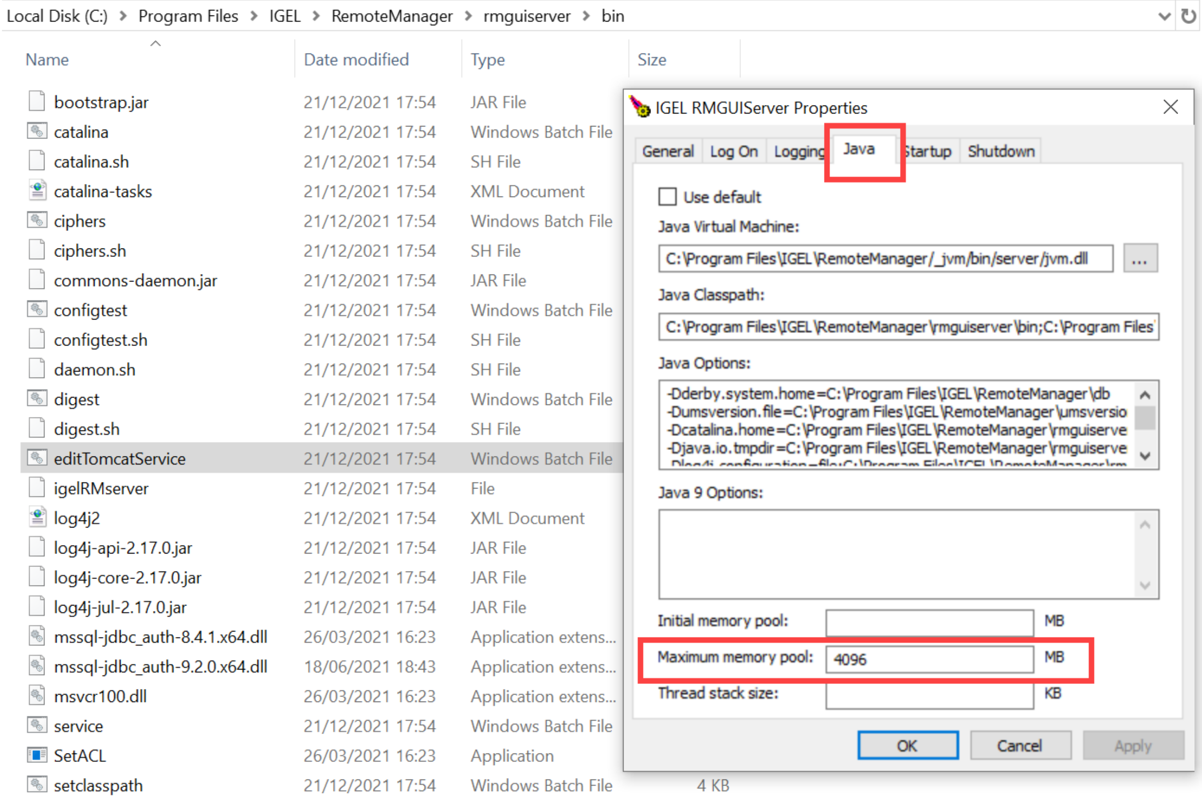
Windows

For the UMS Server installed on Windows, you can modify the Java heap size during the UMS update/installation. For details, see IGEL UMS Installation under Windows. You can also modify the heap size as follows:

1. Stop the `IGEL RMGUIServer` service. For details on how you can stop it, see IGEL UMS HA Services and Processes.
2. Navigate to `C:\Program Files\IGEL\RemoteManager\rmguiserver\bin`.

3. Launch `editTomcatService.bat`.

4. Select the **Java** tab and adapt the **Maximum memory pool** value according to your needs. (Default: 4096 MB)



Local Disk (C:) > Program Files > IGEL > RemoteManager > rmguiserver > bin

Name	Date modified	Type	Size
bootstrap.jar	21/12/2021 17:54	JAR File	
catalina	21/12/2021 17:54	Windows Batch File	
catalina.sh	21/12/2021 17:54	SH File	
catalina-tasks	21/12/2021 17:54	XML Document	
ciphers	21/12/2021 17:54	Windows Batch File	
ciphers.sh	21/12/2021 17:54	SH File	
commons-daemon.jar	21/12/2021 17:54	JAR File	
configtest	21/12/2021 17:54	Windows Batch File	
configtest.sh	21/12/2021 17:54	SH File	
daemon.sh	21/12/2021 17:54	SH File	
digest	21/12/2021 17:54	Windows Batch File	
digest.sh	21/12/2021 17:54	SH File	
editTomcatService	21/12/2021 17:54	Windows Batch File	
igelRMserver	21/12/2021 17:54	File	
log4j2	21/12/2021 17:54	XML Document	
log4j-api-2.17.0.jar	21/12/2021 17:54	JAR File	
log4j-core-2.17.0.jar	21/12/2021 17:54	JAR File	
log4j-jul-2.17.0.jar	21/12/2021 17:54	JAR File	
mssql-jdbc_auth-8.4.1.x64.dll	26/03/2021 16:23	Application extens...	
mssql-jdbc_auth-9.2.0.x64.dll	18/06/2021 18:43	Application extens...	
msvcr100.dll	26/03/2021 16:23	Application extens...	
service	21/12/2021 17:54	Windows Batch File	
SetACL	26/03/2021 16:23	Application	
setclasspath	21/12/2021 17:54	Windows Batch File	4 KB

IGEL RMGUIServer Properties

☐ Use default

Java Virtual Machine: C:\Program Files\IGEL\RemoteManager/_jvm/bin/server/jvm.dll

Java Classpath: C:\Program Files\IGEL\RemoteManager\rmguiserver\bin;C:\Program Files

Java Options:

```
-Dderby.system.home=C:\Program Files\IGEL\RemoteManager\db
-Dumsversion.file=C:\Program Files\IGEL\RemoteManager\umsversio
-Dcatalina.home=C:\Program Files\IGEL\RemoteManager\rmguiserve
-Djava.io.tmpdir=C:\Program Files\IGEL\RemoteManager\rmguiserve
```

Java 9 Options:

Initial memory pool: MB

Maximum memory pool: 4096 MB

Thread stack size: KB

> The Java heap size must always be defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but it must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[7]; see also the `-Xmx` option there.
>
> Note also the following:
>
> - All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Server will be unable to run.
> - Reducing the memory may affect the function of the UMS and is NOT recommended.

5. Click **Ok**.

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

6. Restart the `IGEL RMGUIServer` service.

Linux

For the UMS Server installed on Linux, you can modify the Java heap size as follows:

1. Stop the UMS Server process. For details on how you can stop it, see IGEL UMS HA Services and Processes.
2. Edit `/opt/IGEL/RemoteManager/rmguiserver/conf/ums-server.env`
3. Find the option `CATALINA_OPTS=-Xmx4096m` and change the `-Xmx` value according to your needs. (Default: 4096 MB)

   > ⚠ The Java heap size must always be defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but it must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[8]; see also the `-Xmx` option there.
   > Note also the following:
   > - All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Server will be unable to run.
   > - Reducing the memory may affect the function of the UMS and is NOT recommended.
   > - During the UMS update, the heap size value is set to the default. Therefore, you have to adapt it again.

4. Restart the UMS Server process.

Related Topics

How to Configure Java Heap Size for the UMS Console (see page 238)

How to Configure Java Heap Size for the ICG

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

How to Configure Java Heap Size for the UMS Console

You use IGEL Universal Management Suite (UMS) and experience performance issues with the UMS Console. Manifold reasons can underlie performance degradation, and there are various solutions like optimizing the UMS according to recommendations under Performance Optimizations in IGEL UMS, updating the UMS components, etc. The following article covers only the increase of UMS Console memory (Java heap size).

Symptom

You face performance problems and encounter memory issues in the UMS Console log files (`igel-ums-console.log` ; see Where Can I Find the IGEL UMS Log Files? (see page 332)), e.g. `java.lang.OutOfMemoryError` .

Problem

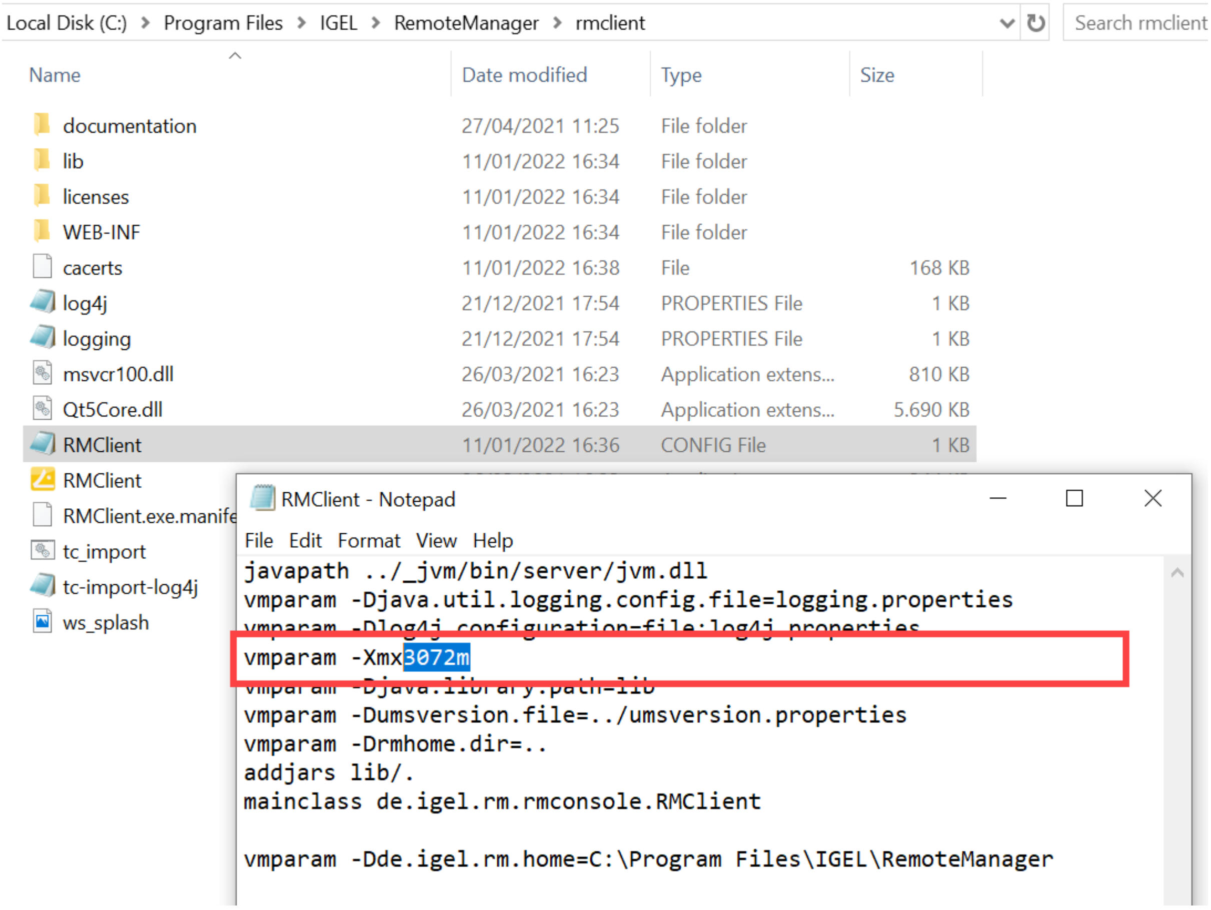
The default Java heap size may be insufficient for the UMS Console. This usually happens if you have

- a large number of devices registered (>10.000)
- a lot of devices in one folder (a flat directory structure under **Devices** in the UMS Console; >1.000 per folder)

Solution: Change Java Heap Size for the UMS Console

For the UMS Console, you can modify the Java heap size during the UMS update/installation. For details, see IGEL UMS Installation under Windows. You can also modify the heap size as follows:

1. Close the UMS Console.
2. Open the following file:
   Default path on Windows: `C:\Program Files\IGEL\RemoteManager\rmclient\RMClient.config`
   Default path on Linux: `/opt/IGEL/RemoteManager/rmclient/RemoteManager.config`
3. Find the line `vmparam -Xmx3072m` and change the `-Xmx` value according to your needs. (Default: 3072 MB)



Local Disk (C:) > Program Files > IGEL > RemoteManager > rmclient
Search rmclient

Name	Date modified	Type	Size
documentation	27/04/2021 11:25	File folder	
lib	11/01/2022 16:34	File folder	
licenses	11/01/2022 16:34	File folder	
WEB-INF	11/01/2022 16:34	File folder	
cacerts	11/01/2022 16:38	File	168 KB
log4j	21/12/2021 17:54	PROPERTIES File	1 KB
logging	21/12/2021 17:54	PROPERTIES File	1 KB
msvcr100.dll	26/03/2021 16:23	Application extens...	810 KB
Qt5Core.dll	26/03/2021 16:23	Application extens...	5.690 KB
RMClient	11/01/2022 16:36	CONFIG File	1 KB
RMClient			
RMClient.exe.manife			
tc_import			
tc-import-log4j			
ws_splash			

```
javapath ../_jvm/bin/server/jvm.dll
vmparam -Djava.util.logging.config.file=logging.properties
vmparam -Dlog4j.configuration=file:log4j.properties
vmparam -Xmx3072m
vmparam -Djava.library.path=lib
vmparam -Dumsversion.file=../umsversion.properties
vmparam -Drmhome.dir=..
addjars lib/.
mainclass de.igel.rm.rmconsole.RMClient

vmparam -Dde.igel.rm.home=C:\Program Files\IGEL\RemoteManager
```

The Java heap size is defined INDIVIDUALLY depending on the configuration of the server and your UMS environment, but must be less than the amount of available physical RAM. General recommendations can be found in the Oracle article Tuning Java Virtual Machines (JVMs)[9]; see also the `-Xmx` option there.

Note also the following:

- All heap size changes are at your own risk! Change the heap size only if you know exactly what you are doing. In the case of improper configuration, the UMS Console will be unable to run.
- Reducing the memory may affect the function of the UMS and is NOT recommended.

4. Save the changes.

5. Restart the UMS Console.

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

Related Topics

How to Configure Java Heap Size for the UMS Server (see page 235)

How to Configure Java Heap Size for the ICG

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

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

IGEL Environment

- IGEL UMS 6.09.100 or higher

How to Request the Current Status of the UMS Server

▶ Use the following requests to check the status of the UMS Server. If you use a browser for this purpose and the UMS deploys a self-signed certificate, the browser may display a security/certificate warning. Accept the risk and continue, or make the certificate known to the browser.

```
https://[server]:[web_server_port]/ums/check-status
```

OR

```
http://[server]:[jws_server_port]/ums/check-status
```

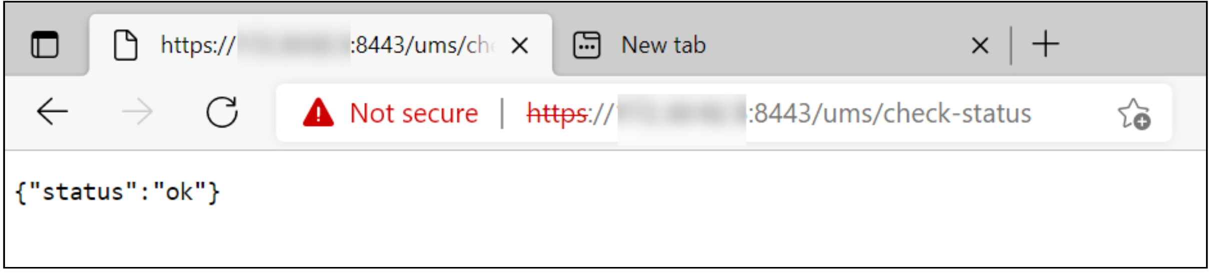
The following responses are possible:

1. If the (check status) service is up and running, HTTP status code 200 is returned. The response body contains a `JSON` document with information on the UMS Server status:

   ```
   {“status”: ”init|ok|warn|err”}
   ```

   For the details, see Monitoring the UMS Server: Possible Statuses (see page 242) below.

   Example:

   
   https://[redacted]:8443/ums/ch
   New tab
   Not secure
   https://[redacted]:8443/ums/check-status

   ```
   {"status":"ok"}
   ```

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

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

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

Monitoring the UMS Server: Possible Statuses

The response statuses returned during the monitoring of the UMS Server indicate the following situations:

ok	The server is up and running.
warn	• The server is in HA update mode; see Updating the Installation of an HA Network. • The server is not connected to one or more configured IGEL Cloud Gateways; see Connecting the UMS to the ICG. • Certificates used for communication with endpoint devices, i.e., certificates of the `tc.keystore` file, are not in sync with the database. This might happen, for example, if you make changes to certificates and the automatic synchronization stops functioning due to some network issues or if the IGEL network token differs between the components, e.g., when a wrong network token was chosen during the server installation.
err	• There is no database connection – no database is configured, or the database connection has failed. For where to configure the database, see How to Set Up a Data Source in the IGEL UMS Administrator. • The device communication port is not ready. For where to configure the device communication port, see Settings - Change Server Settings in the IGEL UMS Administrator; for details on UMS ports, see IGEL UMS Communication Ports (see page 4).
init	Server initialization has not been completed yet. Note: If the initialization process is not finished within 120 seconds, the status automatically changes to **err**.

Related Topics

How to Monitor the IGEL Cloud Gateway

Monitoring Device Health and Searching for Lost Devices (see page 269)

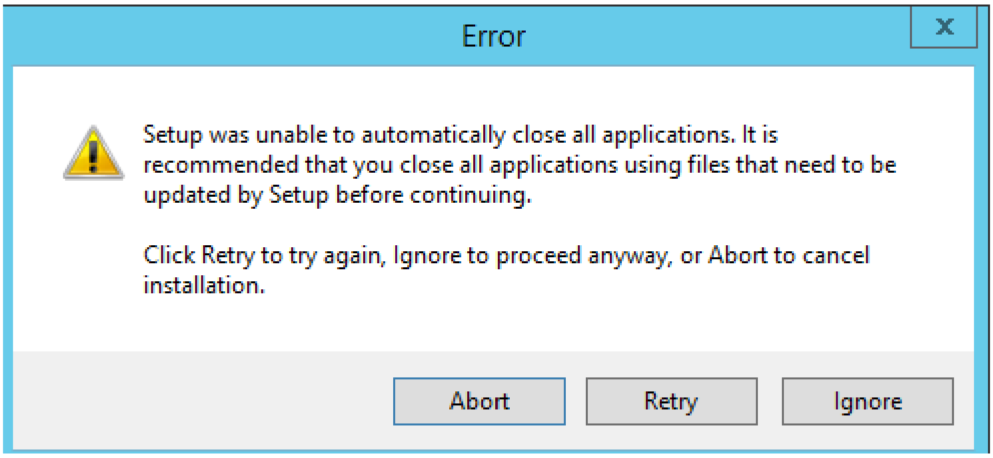
UMS HA Health Check - Analyse Your IGEL UMS High Availability and Distributed UMS Systems

High Availability

Load Balancer Is Not Stopping during the Update of the HA Installation

Symptom

When updating the High Availability (HA) installation, an error message appears saying that not all applications could be closed before the update. A retry does not solve the problem.



Error

Setup was unable to automatically close all applications. It is recommended that you close all applications using files that need to be updated by Setup before continuing.

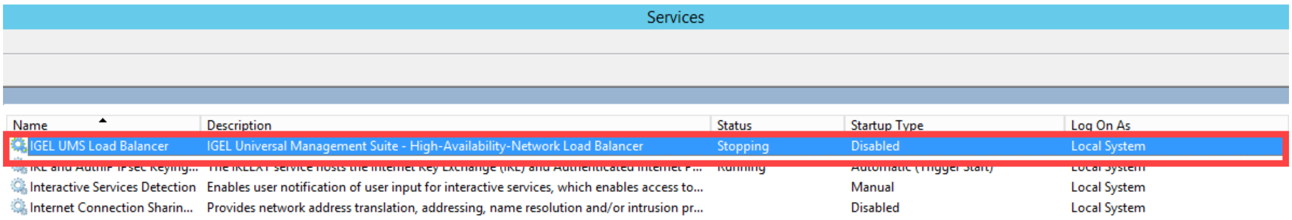
Click Retry to try again, Ignore to proceed anyway, or Abort to cancel installation.

Environment

- UMS HA installation

Problem

The load balancer does not stop and stays in the "Stopping" mode:



Services

Name	Description	Status	Startup Type	Log On As
IGEL UMS Load Balancer	IGEL Universal Management Suite - High-Availability-Network Load Balancer	Stopping	Disabled	Local System
IKE and AuthIP IPsec Keying...	The IKEEXT service hosts the Internet Key Exchange (IKE) and Authenticated Internet P...	Running	Automatic (Trigger Start)	Local System
Interactive Services Detection	Enables user notification of user input for interactive services, which enables access to...		Manual	Local System
Internet Connection Sharin...	Provides network address translation, addressing, name resolution and/or intrusion pr...		Disabled	Local System

Solution

▶ Stop the load balancer manually and proceed with the update. For information regarding stopping the HA services, see IGEL UMS HA Services and Processes.

Which Files Are Automatically Synchronized between the IGEL UMS Servers?

You have a multi-instance IGEL Universal Management Suite (UMS) installation and want to know which files are automatically synchronized between the servers.

Prerequisites

- A High Availability (HA) environment with UMS version 6.06.100 or higher
- A Distributed UMS installation with UMS version 6.10.100 or higher

General Overview

The following files are synchronized between the UMS Servers automatically:

- Files registered in the UMS Console

  > Files that are not created as file objects in UMS, but only stored in the file system in `ums_filetransfer`, are NOT synchronized. For details on how/where you can create a file object, see Files - Registering Files on the IGEL UMS Server and Transferring Them to Devices and Create Firmware Customization.

- The files of Universal Firmware Updates if the synchronization is enabled under **UMS Administration > Global Configuration > Universal Firmware Update** and a WebDAV directory is set as the target path for the download. For details, see the section "Synchronization of Universal Firmware Updates (see page 245)" below.

The objects are synchronized immediately – unless a UMS Server is temporarily unreachable. In that case, the synchronization takes place every 5 minutes or at server startup.

The synchronization applies to the file system and does not refresh the view in any UMS Console other than the one in which the object has been created. Thus, you may need to press [F5] or the refresh button 🔄 to view the object in the UMS Console on the other server.

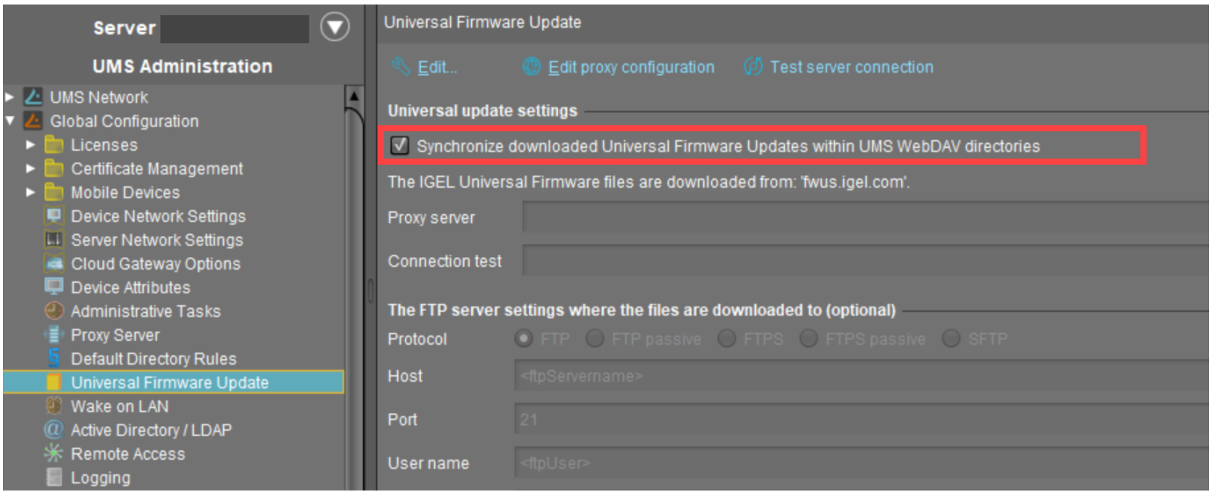
> ⚠ To avoid problems with your HA installation, make sure that the time on the servers of the HA network does not differ by more than one minute. After each manual time reset, the HA services on the relevant server must be restarted.

Synchronization of Universal Firmware Updates

To enable the automatic synchronization of the firmware updates between the UMS Servers, proceed as follows:

1. In the UMS Console, go to **UMS Administration > Global Configuration > Universal Firmware Update**.

2. Activate **Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories**.



Universal Firmware Update

Universal update settings

☑ Synchronize downloaded Universal Firmware Updates within UMS WebDAV directories

The IGEL Universal Firmware files are downloaded from: 'fwus.igel.com'.

Proxy server

Connection test

The FTP server settings where the files are downloaded to (optional)

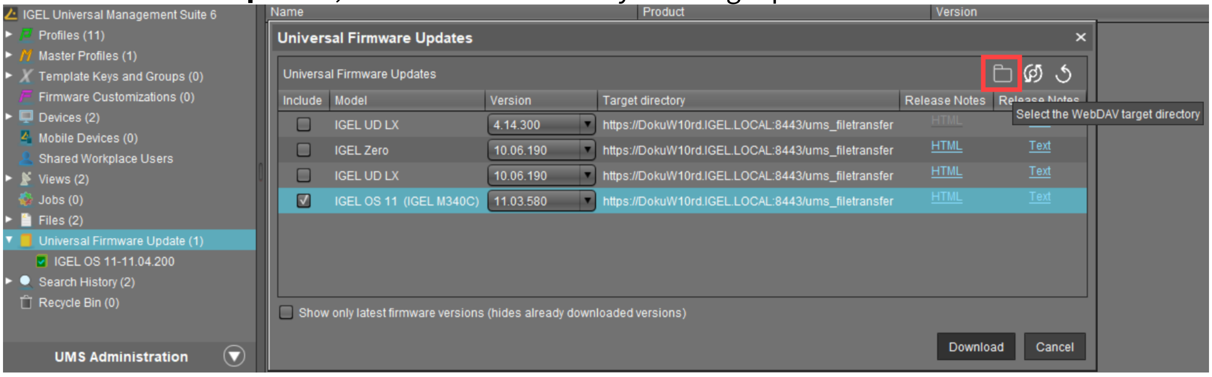
Protocol ● FTP ○ FTP passive ○ FTPS ○ FTPS passive ○ SFTP

Host <ftpServername>

Port 21

User name <ftpUser>

3. When adding a firmware update under **Universal Firmware Update > [context menu] > Check for new firmware updates**, set a WebDAV directory as a target path for the download.



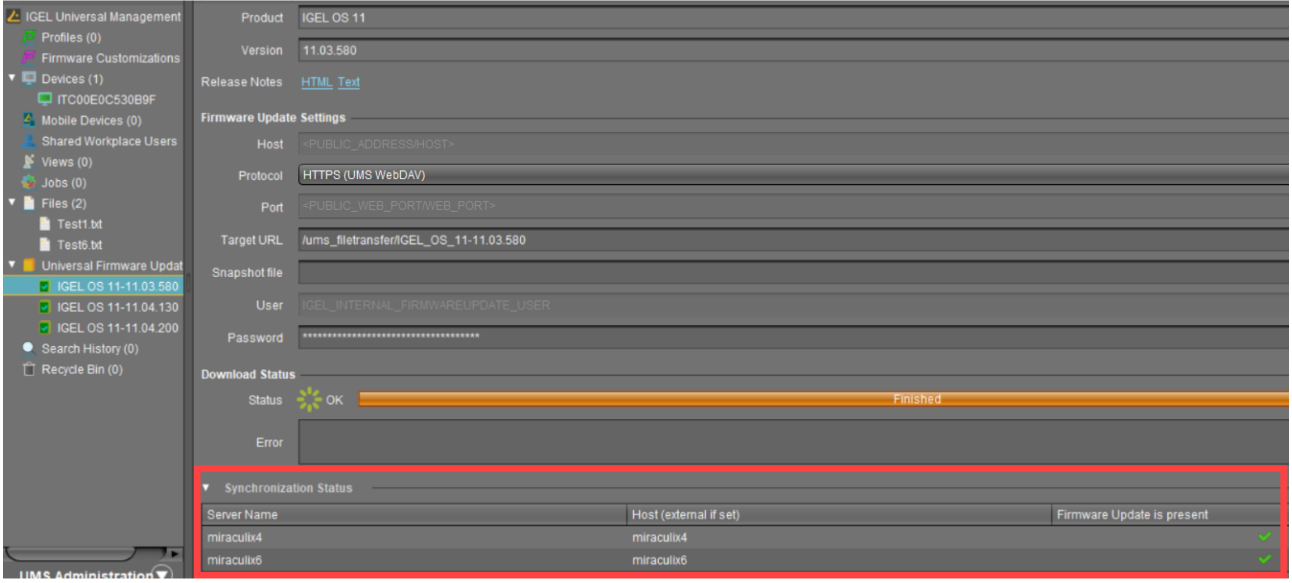
Universal Firmware Updates

Universal Firmware Updates

Include	Model	Version	Target directory	Release Notes	Release Notes
□	IGEL UD LX	4.14.300	https://DokuW10rd.IGEL.LOCAL:8443/ums_filetransfer	HTML	
□	IGEL Zero	10.06.190	https://DokuW10rd.IGEL.LOCAL:8443/ums_filetransfer	HTML	Text
□	IGEL UD LX	10.06.190	https://DokuW10rd.IGEL.LOCAL:8443/ums_filetransfer	HTML	Text
☑	IGEL OS 11 (IGEL M340C)	11.03.580	https://DokuW10rd.IGEL.LOCAL:8443/ums_filetransfer	HTML	Text

□ Show only latest firmware versions (hides already downloaded versions)

When the download is complete, you can see under **Synchronization Status** the servers for which the firmware update has already been synchronized.



Product IGEL OS 11

Version 11.03.580

Release Notes HTML Text

Firmware Update Settings

Host <PUBLIC_ADDRESS/HOST>

Protocol HTTPS (UMS WebDAV)

Port <PUBLIC_WEB_PORT/WEB_PORT>

Target URL /ums_filetransfer/IGEL_OS_11-11.03.580

Snapshot file

User IGEL_INTERNAL_FIRMWAREUPDATE_USER

Password ***********************************

Download Status

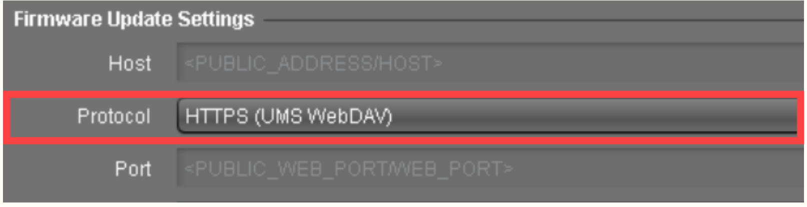
Status OK Finished

Error

Synchronization Status

Server Name	Host (external if set)	Firmware Update is present
miraculix4	miraculix4	✓
miraculix6	miraculix6	✓

Universal Firmware Updates are synchronized between the UMS Servers only if **HTTPS (UMS WebDAV)** or **HTTP (UMS WebDAV)** is selected under **Protocol**. These protocols are used for transferring the firmware update files from the UMS WebDAV directory to the devices.



Firmware Update Settings

Host <PUBLIC_ADDRESS/HOST>

Protocol HTTPS (UMS WebDAV)

Port <PUBLIC_WEB_PORT/WEB_PORT>

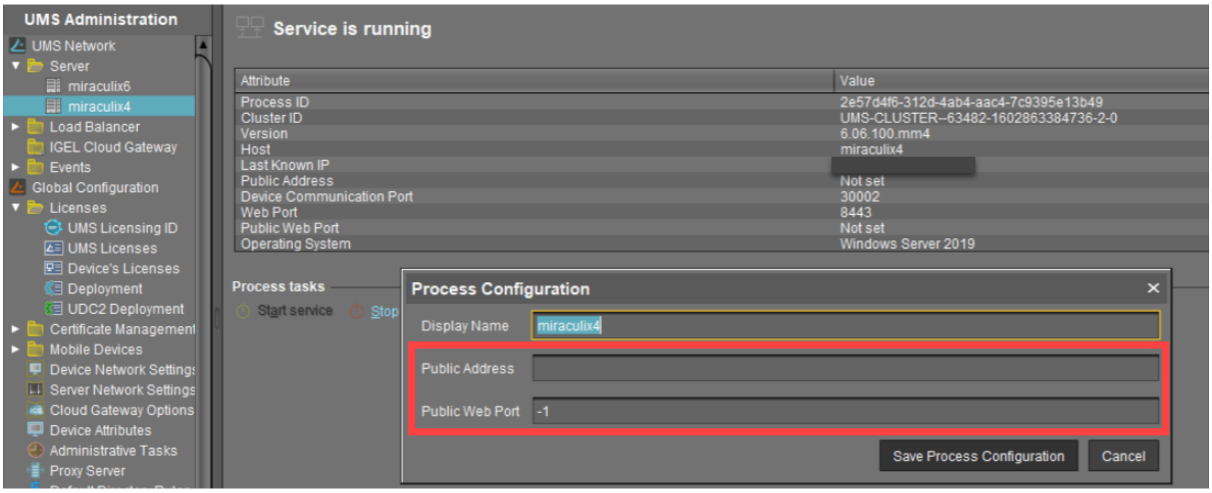
With any other protocol, firmware updates are not synchronized between the servers.

Connection Data Used during the Update

When a firmware update is assigned to a device, the connection information of the current server is sent to the device if the firmware update is present in the UMS WebDAV directory of the server. If the firmware update is absent for some reason, the connection information of a server with the firmware update available is sent.

The connection information contains

- a **Public Address** if it is configured for the server under **UMS Administration > UMS Network > Server > [server's context menu] > Edit**. Otherwise, the stored hostname is used.
- a **Public Web Port** if it is configured for the server under **UMS Administration > UMS Network > Server > [server's context menu] > Edit**. Otherwise, the stored web port is used.



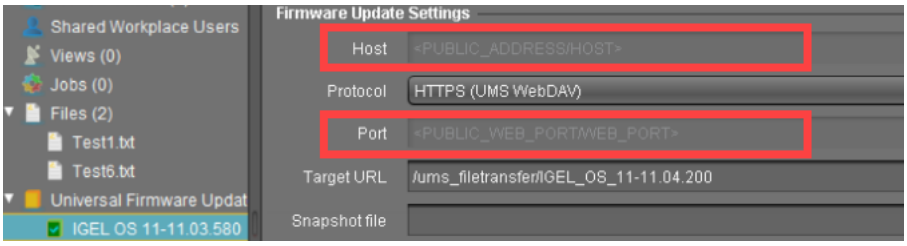
Service is running

Attribute	Value
Process ID	2e57d4f6-312d-4ab4-aac4-7c9395e13b49
Cluster ID	UMS-CLUSTER--63482-1602863384736-2-0
Version	6.06.100.mm4
Host	miraculix4
Last Known IP	[redacted]
Public Address	Not set
Device Communication Port	30002
Web Port	8443
Public Web Port	Not set
Operating System	Windows Server 2019

Process Configuration

Display Name	miraculix4
Public Address	
Public Web Port	-1

Since the connection information is dynamically adjusted, **Host** and **Port** data are not editable for the downloaded firmware update (with the HTTP(S) (UMS WebDAV) protocol set):



Firmware Update Settings

Host	<PUBLIC_ADDRESS/HOST>
Protocol	HTTPS (UMS WebDAV)
Port	<PUBLIC_WEB_PORT/WEB_PORT>
Target URL	/ums_filetransfer/IGEL_OS_11-11.04.200
Snapshot file	

Load Distribution with a Number of Load Balancers

If a UMS Server and Load Balancer are installed on a shared computer, the UMS Server communicates with the IGEL OS 11 devices via port 30002, otherwise via port 30001 as is customary with a single server installation. The Load Balancer always communicates with the IGEL OS 11 devices via port 30001.

Load distribution to the load balancers can be performed as follows. When booting, the OS 11 devices attempt to establish contact with the UMS Server in this order:

- DHCP tag 224
- Name `igelrmserver` in the DNS (*Record Type A*)
- Local list of **Remote Management Servers** (in the specified order)

In a UMS High Availability network, the load balancers are automatically specified in the list of remote management servers in the local device configuration.

If the DNS entry `igelrmserver` or DHCP tag 224 is used in an HA network, the IP of a load balancer must be entered.

If neither this DNS entry nor the DHCP tag 224 is used, endpoint devices always connect to the first load balancer in the setup list, i.e. all devices are communicating with a single load balancer. The other load balancers are merely stand-bys and will be used only if the first load balancer in the list is not available.

To achieve load distribution between the load balancers, you can however use the DNS entry `igelrmserver` with a *Round Robin DNS*. To do this, the IP addresses of all load balancers are recorded in the DNS as a *Resource Record Set* for the `igelrmserver` entry (cf. https://en.wikipedia.org/wiki/Round-robin_DNS). The devices then connect randomly to one of the available load balancers, thus distributing the query load of all devices.

Manual Synchronization of the UMS ID

When the main UMS ID is not synchronized between the IGEL UMS Servers, **UMS ID status** under **UMS Administration > Global Configuration > UMS ID** reads "Not in sync, please restart server", see UMS ID. However, even when you restart the UMS Server, the UMS ID sometimes remains unsynchronized. In this case, the manual synchronization is required.

Environment

- UMS 12.01.100 or higher
- High Availability (HA) or Distributed UMS environment

Instructions

The manual synchronization of the UMS ID includes the following steps:

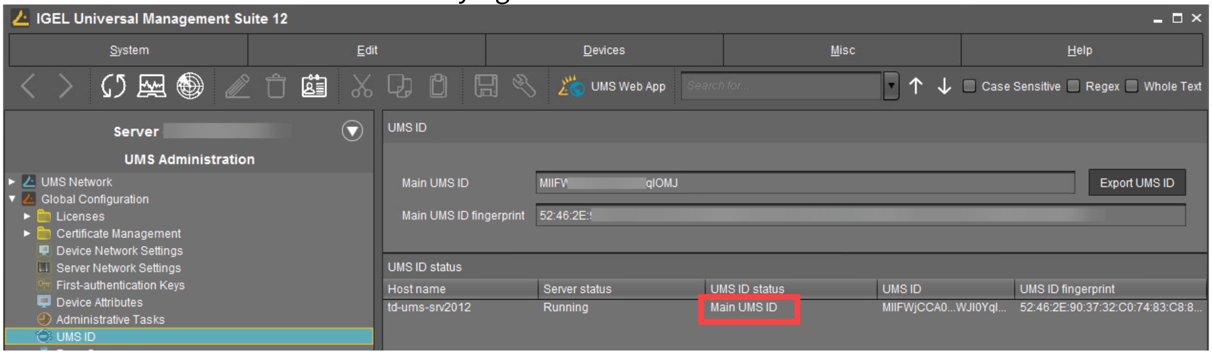
1. Locating the server holding the main UMS ID (see page 250)
2. Creating a backup of the UMS ID (see page 250) on that server
3. Restoring the created backup on all servers with the UMS ID unsynchronized (see page 251) and restarting all servers

Locating the Server Holding the Main UMS ID

To find out which server of the HA or Distributed UMS installation holds the **Main UMS ID**:

1. Open **UMS Console** and navigate to **UMS Administration > Global Configuration > UMS ID**.

2. Find the server with **UMS ID status** saying "Main UMS ID".



UMS ID

Main UMS ID: MIIFW[redacted]qIOMJ

Main UMS ID fingerprint: 52:46:2E:[redacted]

UMS ID status

Host name	Server status	UMS ID status	UMS ID	UMS ID fingerprint
td-ums-srv2012	Running	Main UMS ID	MIIFWjCCA0...WJI0Yql...	52:46:2E:90:37:32:C0:74:83:C8:8...

Creating a Backup of the UMS ID

1. Open the UMS Administrator on the server with the main UMS ID you located in the previous step.

2. Go to **UMS ID Backup** and create a backup as described under UMS ID Backup in the IGEL Administrator.

3. Transfer the created backup to every server where the UMS ID is not in sync.

Restoring the Backup on All Servers with the UMS ID Unsynchronized

1. Open the UMS Administrator on every server where the UMS ID is not in sync.

2. Go to **UMS ID Backup** and restore the backup as described under UMS ID Backup in the IGEL Administrator.

3. Repeat the procedure for all servers with the UMS ID unsynchronized.

4. When the backup restoring procedure is complete, restart all servers if you have not yet done so. In the UMS Console, the **UMS ID status** under **UMS Administration > Global Configuration > UMS ID** should show that the UMS ID is now synchronized on all servers.

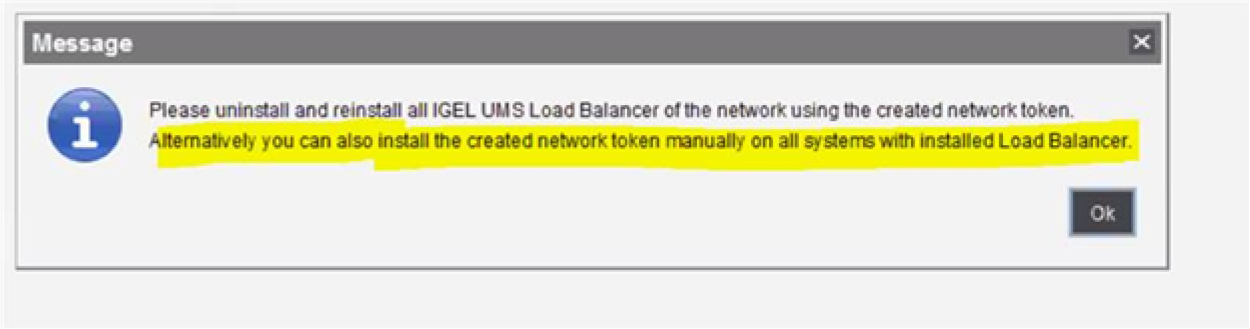
Error Message When Switching Back from an Externally Signed CA to the Internal CA

Solution Based on Experience from the Field

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

Symptom

After testing externally signed CA, if switch back to the internal one, an error message will come up:



Please uninstall and reinstall all IGEL UMS Load Balancer of the network using the created network token.
Alternatively you can also install the created network token manually on all systems with installed Load Balancer.

Environment

- UMS HA; UMS version: any

Solution

1. Run the installer again.
2. Choose **Repair**.
3. Point to the HA 'token' / certificate and install it that way.

How to Migrate an UMS High Availability Installation to a Distributed UMS

This article describes a step-by-step procedure to manually switch from a High Availability IGEL Universal Management Suite (UMS) to a Distributed UMS installation. You can find the procedure for Windows and for Linux.

ⓘ Before the migration, learn about the differences between High Availability UMS and Distributed UMS under IGEL UMS Installation.

The migration procedure consists of the following tasks:

1. Removal of some objects from the current installation which indicate High Availability to the installer, like UMS Watchdog, Load Balancer, and config file for ActiveMQ.
2. Normal installation or upgrade workflow with downtime. For details, see Updating HA Installation: With Downtime of the Servers (igel.com).
3. Validation of the installation.

Switch the Installation on Windows

⚠ Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All the steps must be executed with Administrator privileges:

1. Stop the UMS Server service on all servers.

2. Choose one server and perform the following:

   a. Go to the installation folder of the UMS.

   b. Stop the Windows Services for the Load Balancer and the Watchdog.

   c. Execute the following commands in the Windows command shell:
      - `umswatchdog\etc\bin\jsl.exe -remove`
      - `umsbroker\etc\bin\jsl.exe -remove`

      Both Windows Services should now be removed from the Windows Services.

   d. Delete the folders *umswatchdog* and *umsbroker* from the installation home directory.

   e. Delete the file *rmguiserver\conf\IAMQ_info_storage.xml.*

   f. Reinstall the current UMS version or upgrade the UMS.

   g. You should get the possibility to choose Distributed UMS in the selection dialog of the installation. Choose Distributed UMS and finish the installation.

   h. Verify in the UMS Administrator that the Device Communication Port is set to 30001.

   i. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is selected.

3. Execute step 2 for the remaining servers. This can be done in parallel.

4. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.

5. Update load balancing configurations if they are using UMS Load Balancer addresses.

Switch the Installation on Linux

> ⚠ Before the switch, create a backup of the database and create backups of all the servers.

To switch the installation, you need to perform the following steps. All steps must be executed with Administrator privileges. We omit *sudo* in the following description:

1. Stop the UMS Server service on all servers.

2. Choose one server and perform the following:

   a. Go to the installation folder of the UMS.

   b. Stop the Windows Services for the Load Balancer and the Watchdog:
      - `systemctl stop igel-ums-broker.service`
      - `systemctl disable igel-ums-broker.service`
      - `rm /etc/systemd/system/igel-ums-broker.service`
      - `systemctl stop igel-ums-watchdog.service`
      - `systemctl disable igel-ums- watchdog.service`
      - `rm /etc/systemd/system/igel-ums- watchdog.service`

   c. Delete the folders *umswatchdog* and *umsbroker* from the installation home directory.

d. Delete the file *rmguiserver/conf/IAMQ_info_storage.xml.*

e. Reinstall the current UMS version or upgrade UMS.

f. You should get the possibility to choose Distributed UMS in the selection dialog of the installation. Choose Distributed UMS and finish the installation.

g. Verify in the UMS Administrator that the Device Communication Port is set to 30001.

h. Open the UMS Console, navigate to **Server Network Settings** and verify that Distributed UMS is selected.

3. Execute step 2 for the remaining servers. This can be done in parallel.

4. Delete existing UMS Load Balancers which are installed on other servers where no UMS Server is installed.

5. Update load balancing configurations if they are using UMS Load Balancer addresses.

Final Steps - Validation

To validate the Distributed UMS installation you can do the following:

- Test the communication to some devices.
- Check if IGEL Cloud Gateway (ICG) is still connected to all UMS Servers.
- Create a ‘Save Support Information’ archive. The archive should contain log files from all UMS Servers.
- Perform other checks that you do after an upgrade of UMS.

Device

Device Scan or Online Check fails

Symptom

Although a device responds to a ping command, it does not appear in the UMS Console's list of scanned devices, can not be registered or shows up as offline (red) in the UMS Console's navigation tree.

Problem

The packets for scanning the devices or checking their online status are getting blocked within the network, e.g. by a firewall or VPN.

Solution

Make sure UDP packets on port 30005 are not blocked within your network. Those packets are used for both, scanning for devices as well as checking the status of the clients.

See also IGEL UMS Communication Ports (see page 4).

Troubleshooting: Registration of a Device via Scanning for Devices Fails

The following article explains the possible reasons and solutions for device registration failure in the IGEL Universal Management Suite (UMS) when using the scan and register method. For details on the method, see Scanning the Network for Devices and Registering Devices on the IGEL UMS.

Symptom

Although a device can be scanned from the UMS Console, it cannot be registered on the UMS Server. One of the following error messages will appear in the UMS Console:

- `Cannot connect to remote management server`
- `Protocol state invalid`
- `Certificate invalid`

Problem

This may be caused by

- the server's firewall blocking the process
- an already existing UMS certificate on the device
- some database service hanging
- network transfer delays or losses affecting the registration process
- not correct time / date on the device or the UMS Server

Solution

Solving the Firewall Problem

1. On your system running the UMS Console and UMS Server, add the following port to the Windows firewall as an exception:
   - **Name** = `IGEL RMGUIServer`
   - **TCP Port** = `30001`

   > ⓘ If you have changed the standard port 30001 in the UMS Administrator, open the firewall accordingly for this port. For more details on ports, see IGEL UMS Communication Ports (see page 4).

2. Make sure no other firewall within the network is blocking ports 30001 and 30005.
3. Try to import the device again.

> ⓘ It can also be useful to check the network firewall for SSL inspection.

Solving the Certificate Problem

With OS 11 devices:

▶ Delete the `server.crt` certificate from `/wfs/` folder on the device. Try to register the device again.

OR

▶ If you know from which UMS Server exactly the device has received the certificate and have access to this UMS Server, you can remove the certificate as described under How to Remove a UMS Certificate from an OS 11 Device (see page 346).

With OS 11 or OS 12 devices:

▶ Reset the device to factory defaults and try to register the device again. For how to reset the IGEL OS device to factory defaults, see Reset to Factory Defaults.

Solving the Database Problem

▶ In the **UMS Administrator** > **Datasource**, disable the currently active data source and re-activate it again. Try to register the device again.

For details on the UMS Administrator, see The IGEL UMS Administrator.

Checking the Network

▶ Check if the network is fine by sending pings from the device console to your UMS Server:

```
ping -s  -c 10 -M do
```

Start with SIZE =1500 and decrease the size of packages until all packages got transferred without fragmentation or package loss. 1440 / 1400 / 1350 / 1300 are good values to test with.

> ⓘ For "pinging" the UMS Server on a device with IGEL OS, you can use the built-in network tools (by default, **Start menu > System > Network Tools**; see Network Tools).

Checking Time and Date

▶ Check if the time and date are set correctly on the device (see Time and Date) and on the UMS Server.

✓ **Tip**
If you have problems with device registration in the UMS, it is generally recommended to check

- if the registration directly from the endpoint device functions, see UMS Registration. If not, it is usually a sign of some network problems.
- if there is another UMS on the network, and the DHCP and/or DNS server configuration points to the "wrong" UMS.

Related Topics

Device Registration fails with Error Message: Unexpected end of input stream (see page 261)

Device Registration Behind SonicWall Firewall Fails (see page 262)

Device Scan or Online Check fails (see page 257)

Device Registration fails with Error Message: Unexpected end of input stream

Symptom

UMS console shows an error message like "Unexpected end of input stream found at ..." during registration of devices.

Problem

Devices cannot register with UMS over a remote link via VPN gateway, router, firewall or other networking device due to issues with large packets.

The error may occur even if there is no NAT used and the networking device seems to be configured correctly so e.g. pinging is successful in both directions.

Solution

Please consult the documentation for your network device and look up the options for handling large packets. In the case of SonicWall devices the solution is setting the `Ignore Don't Fragment Bit` option.

Device Registration Behind SonicWall Firewall Fails

Symptom

The devices are detected by the UMS during a scan, but registration fails. UMS console shows an error message like "Unexpected end of input stream found at ...".

Possible Causes

The following causes have been reported with firewalls by SonicWall;

- Large packets: See Thin Client Registration fails with Error Message "Unexpected end of input stream" (see page 261).
- SonicWall DPI-SSL replaces the UMS certificate: If SonicWall DPI-SSL is enabled, it functions as intermediate CA and sends its own certificate to the devices instead of the original UMS certificate. As a consequence, the devices refuse to register because they would only accept the original UMS certificate.

Solution

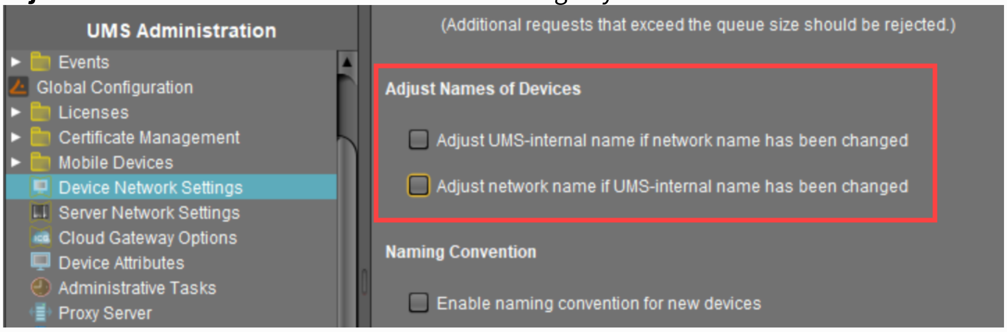
1. In SonicWall, under **DPI-SSL Status**, add the IP address of the UMS server to the list of DPI-SSL exclusions.
2. Restart the VPN tunnel.

Renaming IGEL OS Devices

By default, if no naming convention is activated and the original hostname of the IGEL OS device has not been changed, the name a device gets upon registration in the UMS is composed of the prefix “ITC” ("TC-", in the case of import with the serial number) and the MAC address of the device.

Example: ITC00E0C520XXXX; TC-00E0C520XXXX

Before renaming/registering the devices, it is recommended, first of all, to pay attention to the following settings in **UMS Console > UMS Administration > Global Configuration > Device Network Settings > Adjust Names of Devices**. Activate them according to your needs:



(Additional requests that exceed the queue size should be rejected.)

Adjust Names of Devices

□ Adjust UMS-internal name if network name has been changed

□ Adjust network name if UMS-internal name has been changed

Naming Convention

□ Enable naming convention for new devices

Renaming upon Registration

Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Before registering the devices, activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see Device Network Settings.
2. If the network name, i.e. terminal name, of the device, should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.
3. Save the changes.

Tip

If the network name remained unchanged after the device registration is complete, click **Other commands > Settings UMS->Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can import the devices with the names that fulfill your requirements. For the general instruction, see Importing Devices.

1. When preparing the import file, specify the required device names. See Import with Short Format or Import with Long Format.

2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed**.

Option 3: Via IGEL Setup > Accessories > UMS Registration (only for IGEL OS 11 or Earlier)

If the **Naming Convention** is not activated and you need to register only a small number of devices, you can specify the required name when registering the device as follows:

▶ On the device, open **IGEL Setup > Accessories > UMS Registration** and specify the device name you need under **New host name**. For more information, see Using UMS Registration Function.

Option 4: Via IGEL Setup > Network

If the **Naming Convention** is not activated:

▶ Before registering the device in the UMS, adjust its name locally

- IGEL OS 12: under **IGEL Setup > Network > Computer name**
- IGEL OS 11 and earlier: under **IGEL Setup > Network > LAN Interfaces > Terminal name**

When the device is registered, this name will also be used in the UMS.

Renaming Already Registered Devices

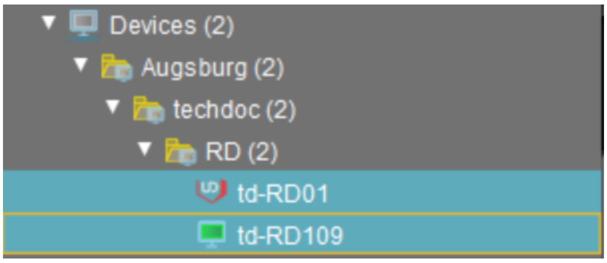
Option 1: Via UMS Console > Device Network Settings > Naming Convention

1. Activate and define **Naming Convention** in the UMS under **UMS Administration > Global Configuration > Device Network Settings**, see Device Network Settings.

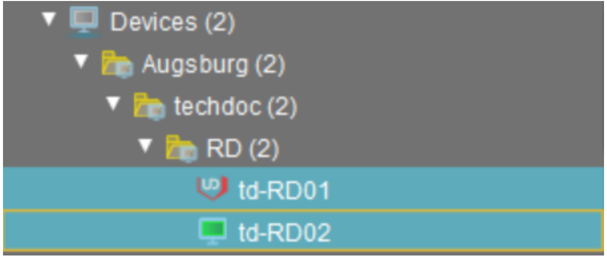
2. If the network name, i.e. terminal name, of the device should be adjusted, enable **Device Network Settings > Adjust network name if UMS-internal name has been changed**.

3. Save the changes.

4. To rename the devices, select one of the following options:
    - **Rename all devices**: All devices registered in the UMS will be renamed in accordance with the naming convention.
      Example:



- **Rename and renumber all devices**: All devices will be renamed in accordance with the naming convention. If the parameter Identifier under **UMS Administration > Global Configuration > Device Network Settings** has been set to **Sequential Number** (UMS 12.02.120 or higher) or you are using UMS 12.02.100 or lower, this will result in continuous, end-to-end numbering. All names will be reallocated. If numbers have become free because devices were taken out of service, these numbers will be used for other devices. For details on the naming options, see Device Network Settings.
  Example:



> **Tip**
>
> If the network name remains unchanged, click **Other commands > Settings UMS->Device** from the device's context menu.

Option 2: Via UMS Console > System > Import > Import Devices (Short or Long Format Only) If the Required Names Are Preliminarily Defined in the Import File

If the **Naming Convention** option does not suit your needs, you can reimport the devices with the names that fulfill your requirements. For the general instruction, see Importing Devices.

1. When preparing the import file, specify the required device names. See Import with Short Format or Import with Long Format.

2. If the network name, i.e. terminal name, of the devices, should be adjusted, enable **UMS Administration > Global Configuration > Device Network Settings > Adjust network name if UMS-internal name has been changed**.

Option 3: Via UMS Console > [device's context menu] > Rename or via Setup > Network

▶ If you have to rename individual devices, see Changing the Hostname of an IGEL Device via UMS (see page 267).

Option 4: Via IGEL Management Interface (IMI)

▶ If you are using IMI, you can rename your devices as described under PUT /v3/thinclients/{tcId}.

⚠ **General Notes**

- After renaming via UMS, it may be necessary to reboot the endpoint up to three times before the changed network name is displayed correctly.
- Scripts under **System > Firmware Customization > Custom Commands** as well as some DNS or DHCP infrastructure settings may interfere and obstruct the renaming of devices.

Changing the Hostname of an Endpoint Device via IGEL UMS

There are two different ways to change the hostname of an endpoint device via the IGEL Universal Management Suite (UMS):

Option 1:

If **Adjust UMS-internal name if network name has been changed** is checked under **UMS Console > UMS Administration > Global Configuration > Device Network Settings**:

For IGEL OS 12:

1. In the **UMS Web App > Devices**, select the device.
2. Click **Edit Configuration**.
3. Go to **Network > Computer name** and specify the required hostname.
4. Save the settings.
5. Select that you want the settings to be applied **Now**.
6. Refresh the browser window in order to see the changed hostname.
7. Reboot the device.

For IGEL OS 11 and earlier:

1. In the **UMS Console > Devices**, right-click the device.
2. Choose **Edit Configuration**.
3. Go to **Network > LAN Interfaces**.
4. Change **Terminal name**.
5. Click **Save**.
6. Select that you want the settings to be applied **Now**.
7. Click the **Refresh** button in the UMS in order to see the changed hostname.
8. Reboot the device.

Option 2:

If **Adjust network name if UMS-internal name has been changed** is checked under **UMS Console > UMS Administration > Global Configuration > Device Network Settings**:

1. In the **UMS Console > Devices**, right-click the device.
2. Choose **Rename**.
3. Change the name.
4. Click **OK**.
5. Right-click the device.
6. Choose **Other commands > Settings UMS -> Device**.
7. Reboot the device.

Monitoring Device Health and Searching for Lost Devices

Overview

You have two possibilities of monitoring the devices' health:

- Online check: The UMS initiates a regular poll to all devices.
- Last contact between the UMS and the devices: The UMS is aware of the time and date when it had its last interaction with devices; with IGEL OS 11.05.100 or higher, devices can send periodical heartbeat signals to the UMS.

Both methods can be combined; it is recommended to review the advantages and disadvantages. Generally speaking, a combination makes sense if network load is not an issue.

Environment

- Reportable heartbeat: Endpoint devices with IGEL OS 11.05.100 or higher or with IGEL OS 12.01.100 or higher
- Checking the last contact between the device and the UMS: UMS 12.01.100 or higher
- UMS and endpoint devices are connected directly or via ICG

Online Check (UMS Polls the Devices)

The UMS Server polls the devices in a configurable time interval. When a device responds to the poll, its icon is green ; when a device does not respond, its icon turns red . (When the online check is disabled, the icon is grey). For more information on icons, see:

- for the UMS Console: Devices
- for the UMS Web App: Devices - View and Manage Your Endpoint Devices in the IGEL UMS Web App

The online check can be enabled or disabled under **Misc > Settings > Online Check**; also, the time interval can be configured there.

Advantages:

- Works with any firmware version (and any UMS version).
- Provides an instant insight into device health by means of colored icons.
- Status updates can be very frequent (max. every 0.1 seconds).

Disadvantages:

- Causes relatively high network load, as all devices are polled at the same time (the overall network load is dependent on the time interval).
- Offline devices cannot be traced systematically, must be looked up manually in the structure tree.

Last Contact between Device and UMS (Devices Send Data to the UMS)

You can search explicitly for devices that did not have any interaction with the UMS for a given time. By creating an appropriate view, you can determine which device last had contact with the UMS at which time. This may be useful for detecting devices that are not operational anymore.

In addition to the previously existing contacts, devices with IGEL OS 11.05.100 or higher can send periodical heartbeat signals to the UMS to indicate that they are still operational.

Advantages:

- Systematic searches for lost devices are possible.
- The search results can be saved and sent by e-mail.
- Low network load, or no additional load at all:
    - When the heartbeat feature is used: The heartbeat signals are sent with random delay times. (Of course, the overall network load is dependent on the time interval).
    - When the heartbeat feature is not used: No additional network load is generated.

Disadvantage:

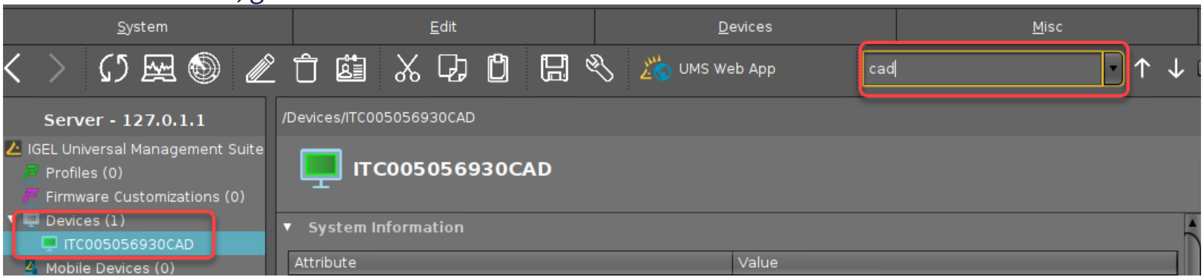
- Status updates cannot be as frequent as with the online check.

Tracing Devices by Their Last Contact with the UMS

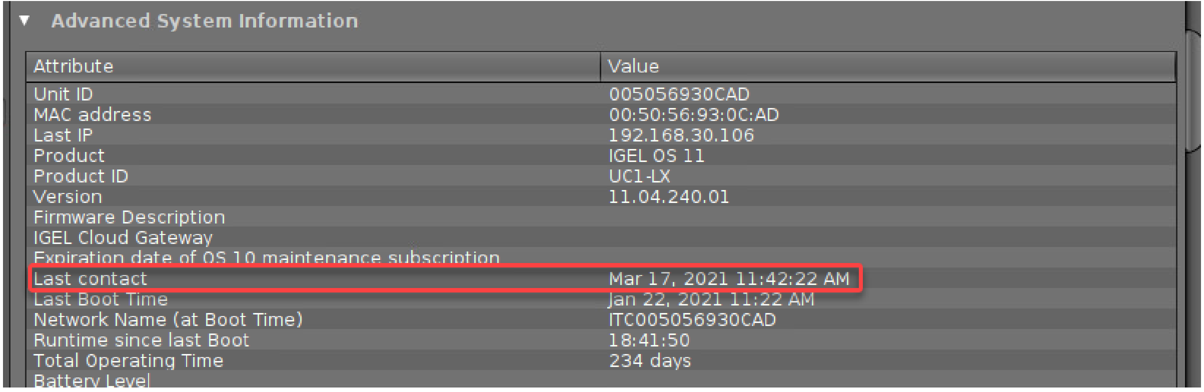
Tracing a Specific Device

UMS Console:

1. In the UMS Console, go to **Devices** or use the search slot to find the desired device.



2. In the **Advanced System Information** area, check out the value of the **Last contact**.



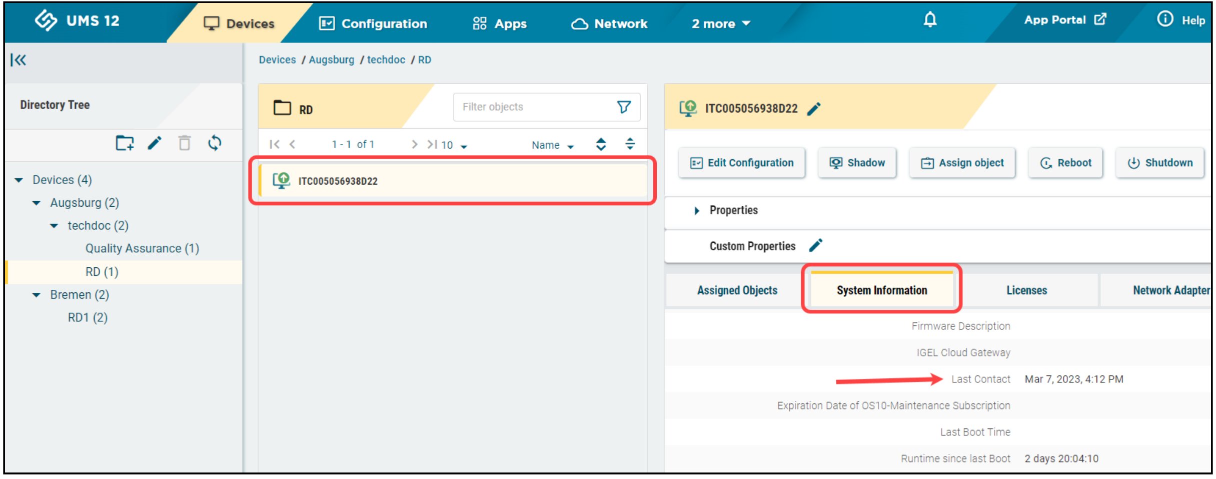
▼ Advanced System Information

Attribute	Value
Unit ID	005056930CAD
MAC address	00:50:56:93:0C:AD
Last IP	192.168.30.106
Product	IGEL OS 11
Product ID	UC1-LX
Version	11.04.240.01
Firmware Description	
IGEL Cloud Gateway	
Expiration date of OS 10 maintenance subscription	
Last contact	Mar 17, 2021 11:42:22 AM
Last Boot Time	Jan 22, 2021 11:22 AM
Network Name (at Boot Time)	ITC005056930CAD
Runtime since last Boot	18:41:50
Total Operating Time	234 days
Battery Level	

UMS Web App:

1. In the UMS Web App, go to **Devices** and select the required device.

2. Under **System Information**, check out the value of the **Last contact**.

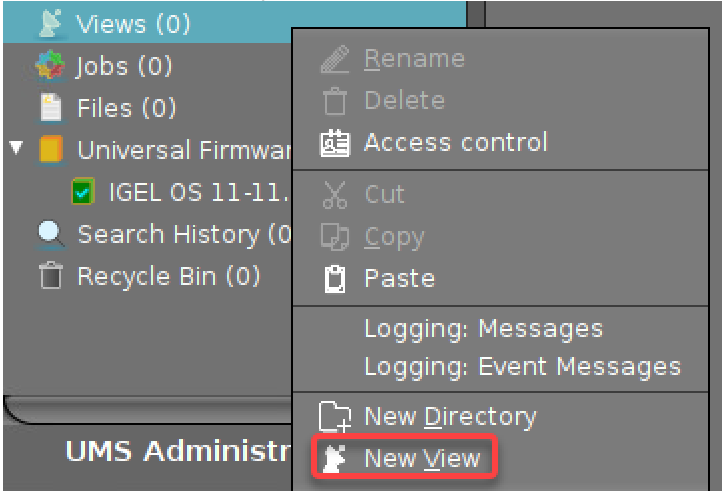


Firmware Description	
IGEL Cloud Gateway	
Last Contact	Mar 7, 2023, 4:12 PM
Expiration Date of OS10-Maintenance Subscription	
Last Boot Time	
Runtime since last Boot	2 days 20:04:10

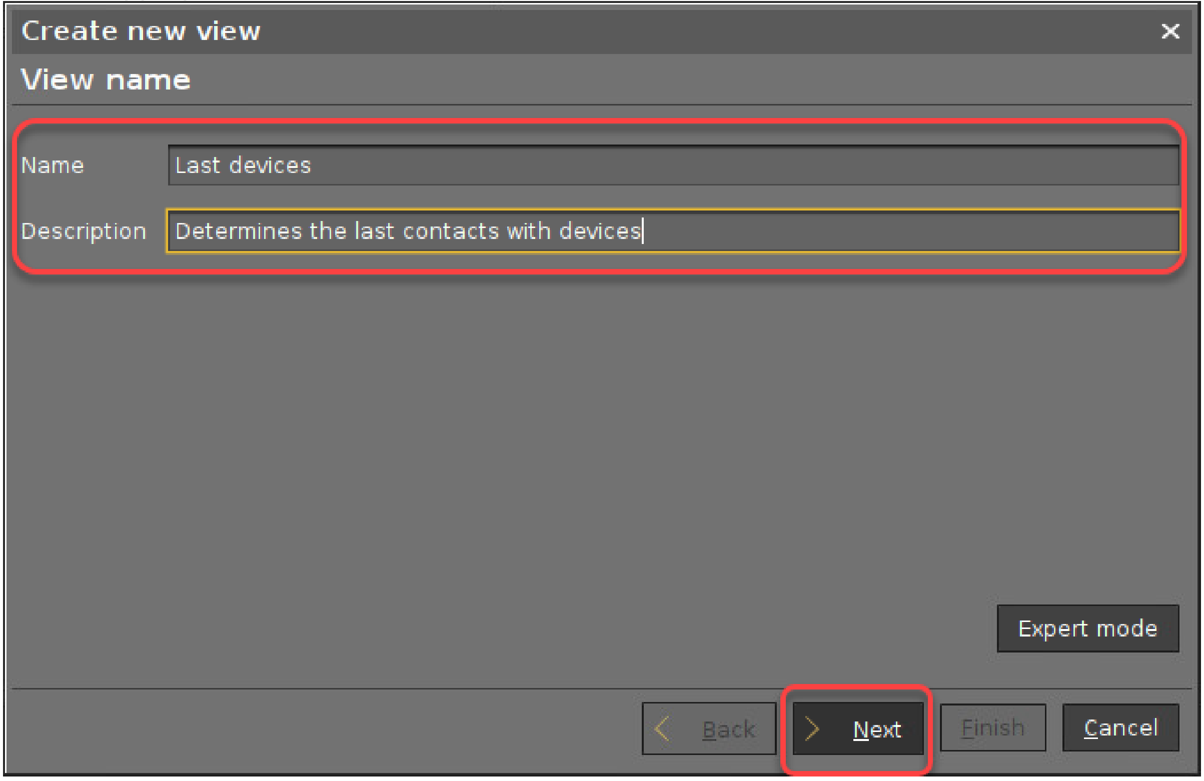
ⓘ For IGEL OS 11 devices, the **Last contact** timestamp is updated on each command sent from a device to the UMS. Or, if you configure a reportable heartbeat interval, a heartbeat command will be sent in a certain time period if no other command has been sent, and the timestamp will be updated correspondingly.
For IGEL OS 12 devices, the **Last contact** timestamp is updated not on each command, but only in the configured heartbeat interval (for online devices only).
For how to configure a reportable heartbeat interval, see Configuring Devices to Send a Reportable Heartbeat (see page 278) below.

Finding Devices That Have Not Shown Up since a Given Time

1. In the structure tree, go to **Views**, open the context menu, and select **New View**.



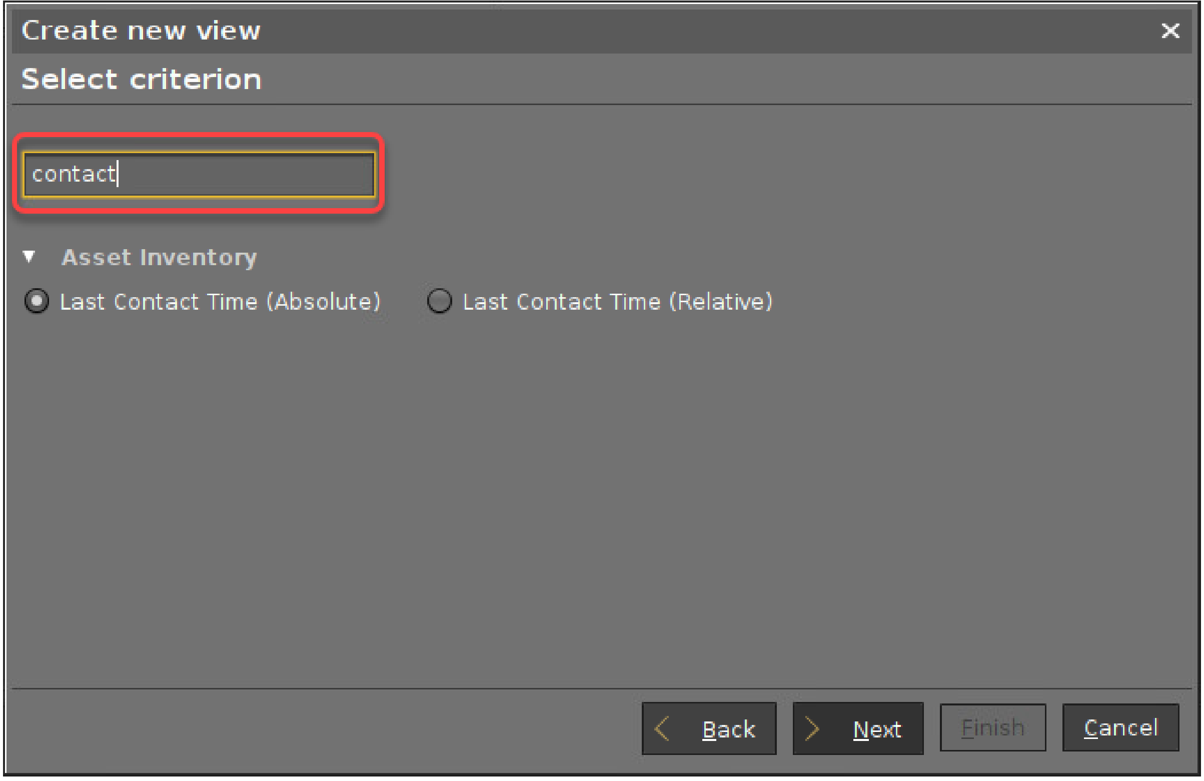
2. Enter an appropriate **Name**, and, **optionally**, a **Description**, and click **Next**.



Name: Last devices

Description: Determines the last contacts with devices

3. In the search field, type "contact" to reduce the number of criteria.



Create new view

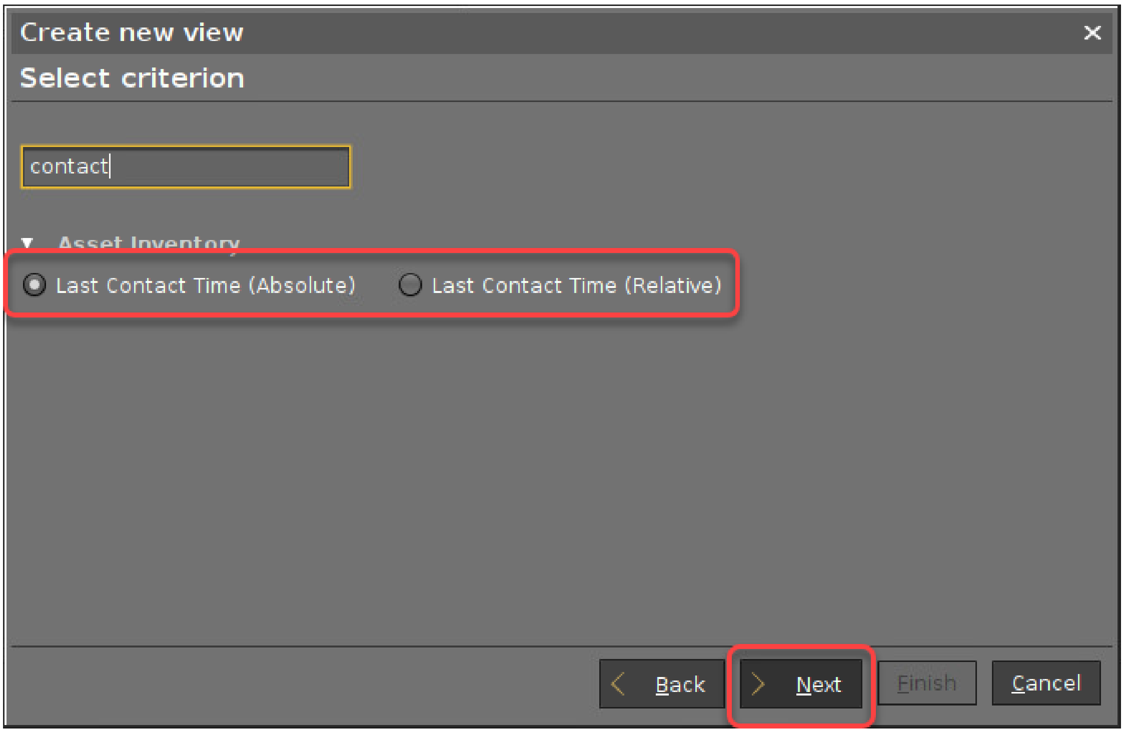
Select criterion

contact

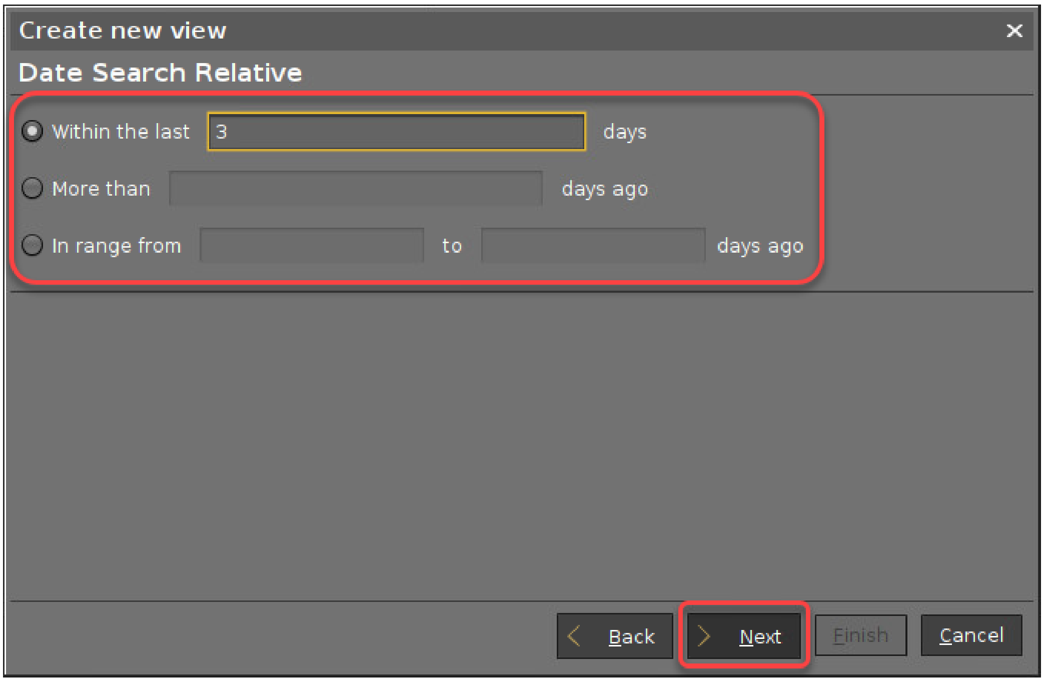
▼ Asset Inventory

● Last Contact Time (Absolute) ○ Last Contact Time (Relative)

4. Choose one of the following criteria and click **Next**:
   - **Last contact time (relative)**: The time interval between the last contact between the UMS and the device and now. This can be the last received heartbeat or any other kind of communication.
   - **Last contact time (absolute)**: The date of the last contact between the UMS and the device. This can be the last received heartbeat or any other kind of communication.



5. Provide the data, depending on whether you chose **Last contact time (relative)** or **Last contact time (absolute)**, and then click **Next**.
   - If you have selected **Last contact time (relative)**:
     - **Within the last [number of] days**: Find devices whose last contact with the UMS was between yesterday and the given number of days ago.
     - **More than [number of] days ago**: Find devices whose last contact with the UMS is more than the given number of days ago.
     - **In range from [number] to [number of] days ago**: Find devices whose last contact with the UMS was within the given time interval.



Create new view

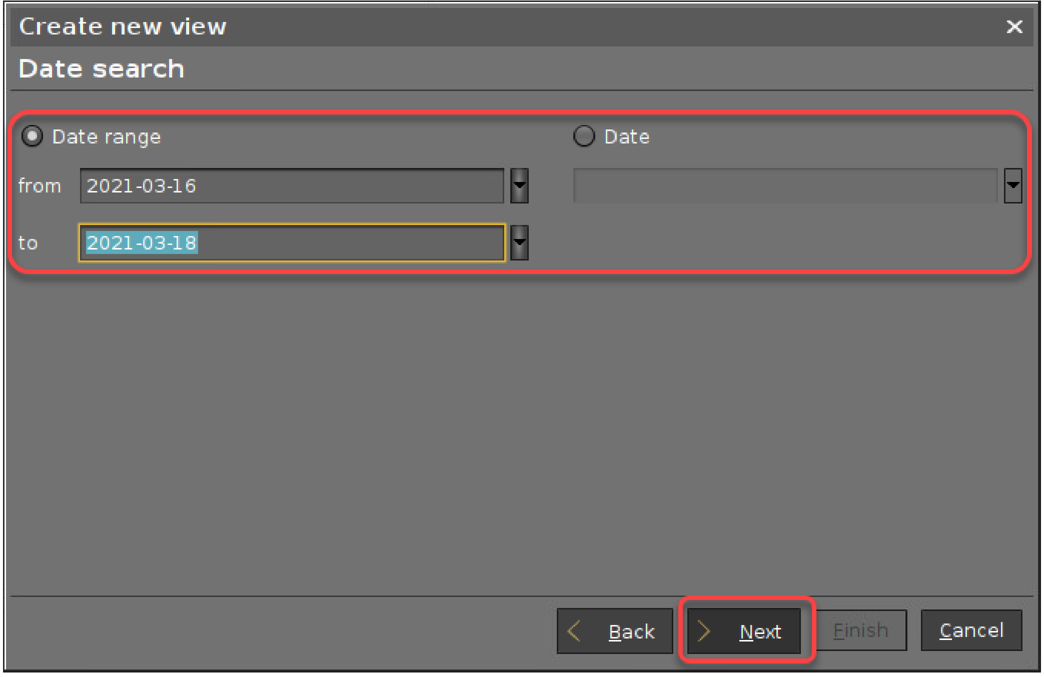
Date Search Relative

● Within the last 3 days

○ More than days ago

○ In range from to days ago

- If you have selected **Last contact time (absolute)**:
  - **Date range**: Find devices whose last contact with the UMS was within the given date range.
  - **Date**: Find devices whose last contact with the UMS was on the given date.



Create new view

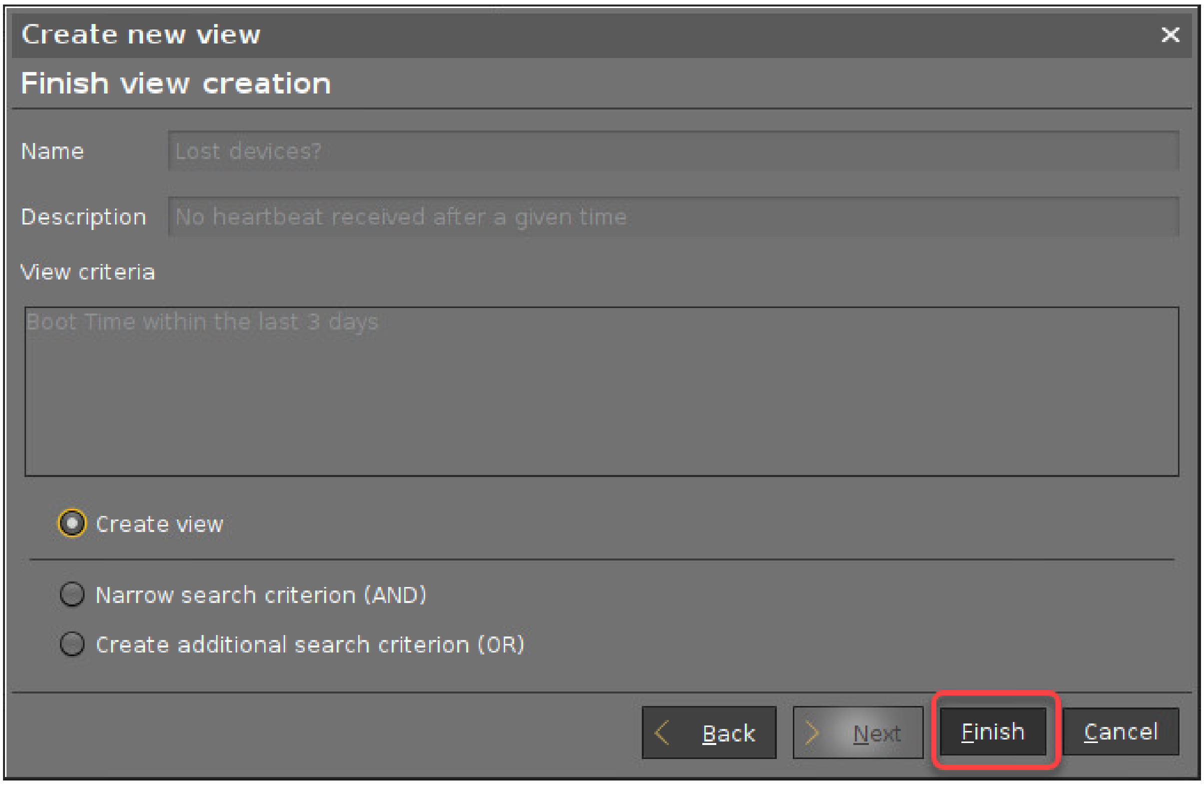
Date search

● Date range ○ Date

from 2021-03-16

to 2021-03-18

6. Review your settings and click **Finish**.



Create new view

Finish view creation

Name: Lost devices?

Description: No heartbeat received after a given time

View criteria

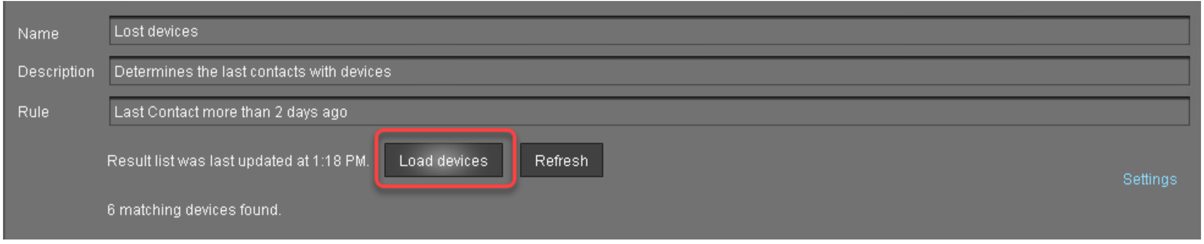
Boot Time within the last 3 days

● Create view

○ Narrow search criterion (AND)

○ Create additional search criterion (OR)

7. If the devices are not shown immediately, click **Load devices**.



Name: Lost devices

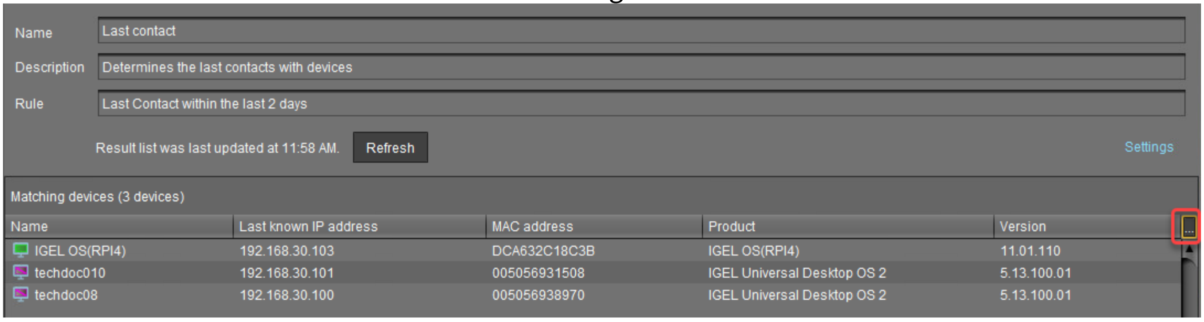
Description: Determines the last contacts with devices

Rule: Last Contact more than 2 days ago

Result list was last updated at 1:18 PM.

6 matching devices found.

8. To make the **Last contact** column visible, click the icon that is shown underneath and then select **Last contact** in the **Choose visible columns** dialog.



Name: Last contact

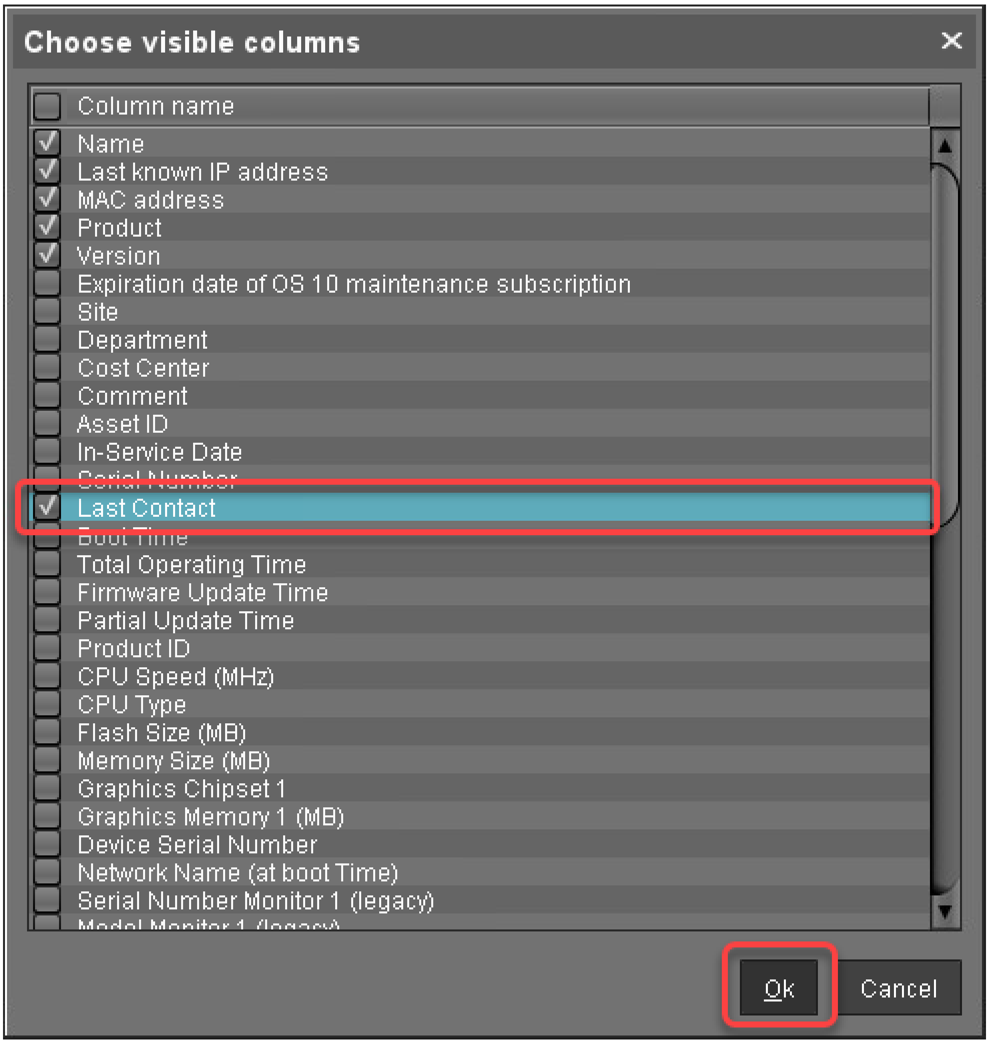
Description: Determines the last contacts with devices

Rule: Last Contact within the last 2 days

Result list was last updated at 11:58 AM.

Matching devices (3 devices)

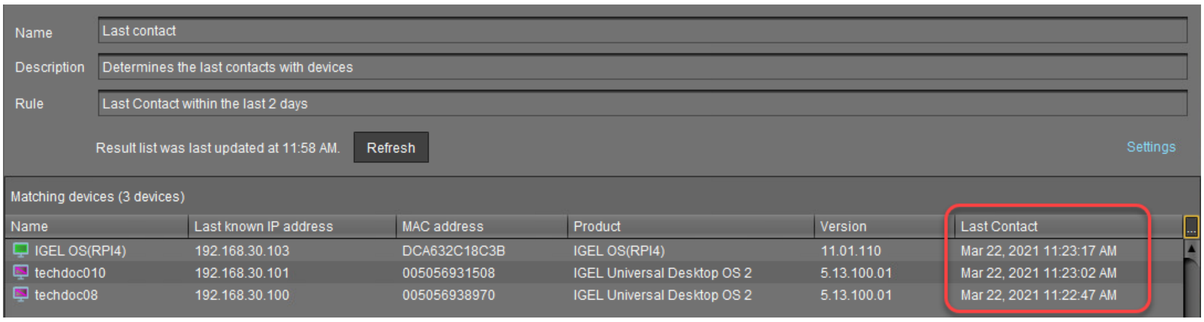
Name	Last known IP address	MAC address	Product	Version
IGEL OS(RPI4)	192.168.30.103	DCA632C18C3B	IGEL OS(RPI4)	11.01.110
techdoc010	192.168.30.101	005056931508	IGEL Universal Desktop OS 2	5.13.100.01
techdoc08	192.168.30.100	005056938970	IGEL Universal Desktop OS 2	5.13.100.01



Choose visible columns ✕

□ Column name
☑ Name
☑ Last known IP address
☑ MAC address
☑ Product
☑ Version
□ Expiration date of OS 10 maintenance subscription
□ Site
□ Department
□ Cost Center
□ Comment
□ Asset ID
□ In-Service Date
□ Serial Number
☑ Last Contact
□ Boot Time
□ Total Operating Time
□ Firmware Update Time
□ Partial Update Time
□ Product ID
□ CPU Speed (MHz)
□ CPU Type
□ Flash Size (MB)
□ Memory Size (MB)
□ Graphics Chipset 1
□ Graphics Memory 1 (MB)
□ Device Serial Number
□ Network Name (at boot Time)
□ Serial Number Monitor 1 (legacy)
□ Model Monitor 1 (legacy)

The results are shown.



Name: Last contact
Description: Determines the last contacts with devices
Rule: Last Contact within the last 2 days

Result list was last updated at 11:58 AM.

Matching devices (3 devices)

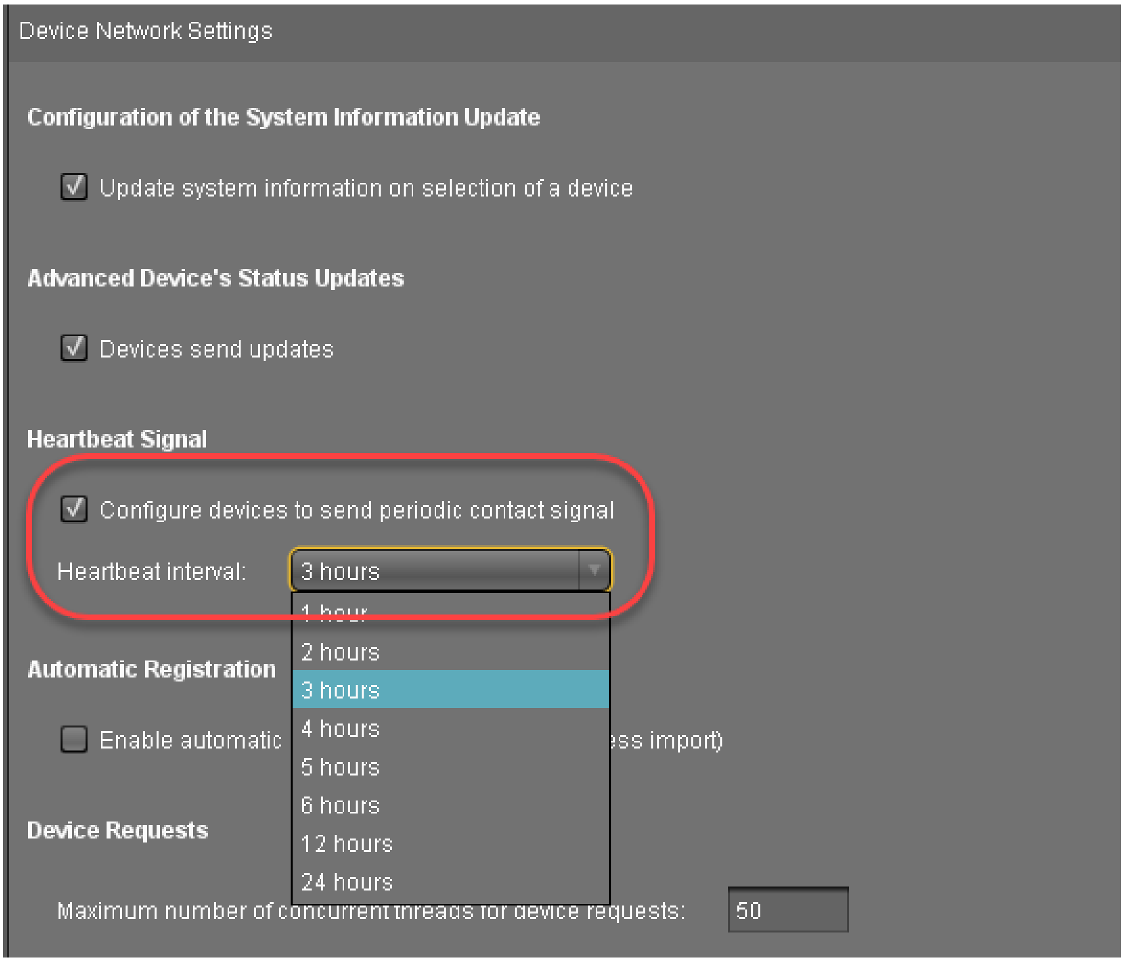
Name	Last known IP address	MAC address	Product	Version	Last Contact
IGEL OS(RPI4)	192.168.30.103	DCA632C18C3B	IGEL OS(RPI4)	11.01.110	Mar 22, 2021 11:23:17 AM
techdoc010	192.168.30.101	005056931508	IGEL Universal Desktop OS 2	5.13.100.01	Mar 22, 2021 11:23:02 AM
techdoc08	192.168.30.100	005056938970	IGEL Universal Desktop OS 2	5.13.100.01	Mar 22, 2021 11:22:47 AM

You can save the results in various formats (see Saving the View Results List) or send them via e-mail (see Sending a View as Mail).

Configuring Devices to Send a Reportable Heartbeat

1. In the UMS Console, go to **UMS Administration > Device Network Settings** and edit the settings as follows:
   - Activate **Configure devices to send periodic contact signal**
   - Set **Heartbeat interval** to the desired value.

   > ⓘ The heartbeat signal will have a random delay of 0 to 10 minutes. This is to avoid overloads which might occur when large amounts of devices send their heartbeat signals simultaneously.

   Device Network Settings

   Configuration of the System Information Update

   ☑ Update system information on selection of a device

   Advanced Device's Status Updates

   ☑ Devices send updates

   Heartbeat Signal

   ☑ Configure devices to send periodic contact signal

   Heartbeat interval: 3 hours

   Automatic Registration

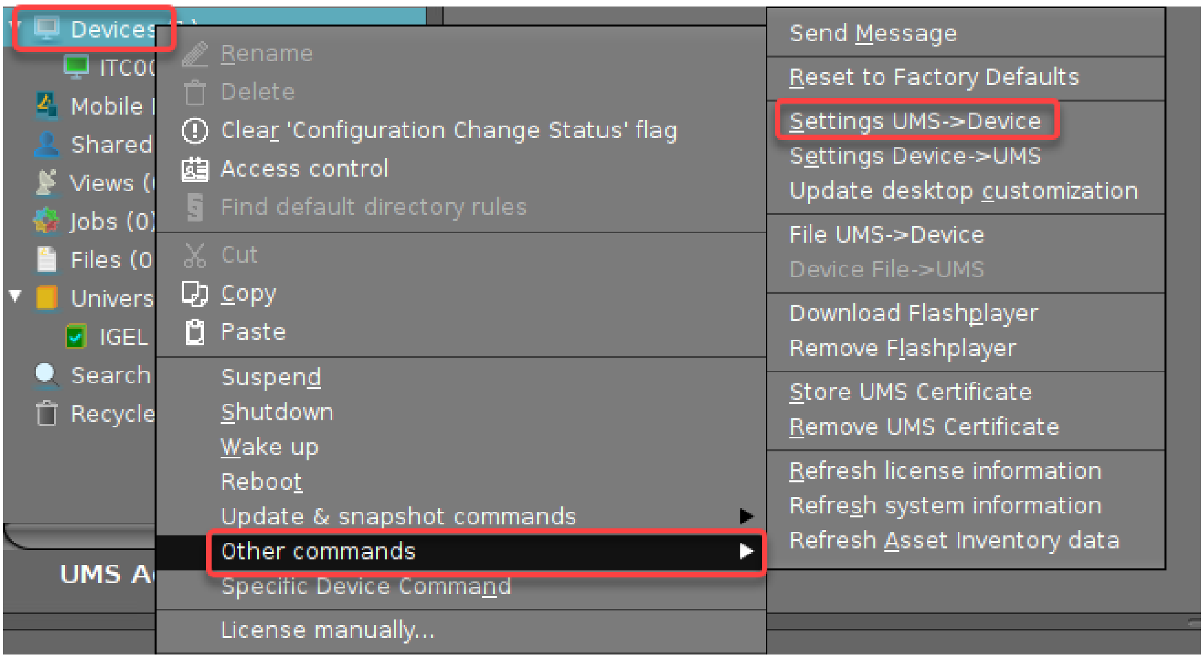
   ☐ Enable automatic ess import)

   Device Requests

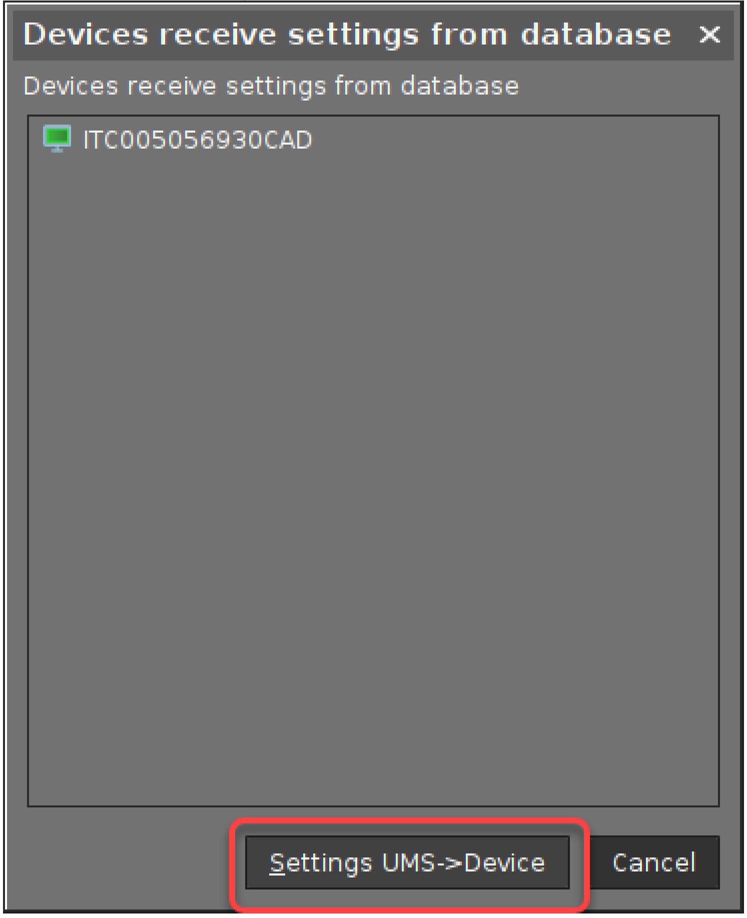
   Maximum number of concurrent threads for device requests: 50

2. Click 💾 to save your settings.
   The settings will become effective the next time the devices receive their settings from the UMS.

3. To make the new settings effective immediately, go to **Devices**, open the context menu, and select **Other commands > Settings UMS->Device**.


Devices
ITC0(
Mobile
Shared
Views (
Jobs (0)
Files (0
Univers
IGEL
Search
Recycle
UMS A
Rename
Delete
Clear 'Configuration Change Status' flag
Access control
Find default directory rules
Cut
Copy
Paste
Suspend
Shutdown
Wake up
Reboot
Update & snapshot commands
Other commands
Specific Device Command
License manually...
Send Message
Reset to Factory Defaults
Settings UMS->Device
Settings Device->UMS
Update desktop customization
File UMS->Device
Device File->UMS
Download Flashplayer
Remove Flashplayer
Store UMS Certificate
Remove UMS Certificate
Refresh license information
Refresh system information
Refresh Asset Inventory data

4. Confirm with Settings **UMS->Device**.



Devices receive settings from database

Devices receive settings from database

ITC005056930CAD

Managing IGEL OS Devices by Device Specific Data - What Device Attributes Can Do for You

Self-defined device attributes can be used to configure devices with the IGEL Universal Management Suite (UMS) according to device-specific data like location, department, or attached hardware.

To use this functionality, you create a custom script on the device that retrieves the desired data and sets the value of the relevant device attribute accordingly.

Note that you must use the UMS internal name of an attribute, not the display name. The UMS internal identifier is displayed in the UMS Console under **UMS Administration > Global Configuration > Device Attributes**; see also Managing Device Attributes for IGEL OS Devices.

Also, note that permission to change attribute values must be granted by the UMS. This is the case if the **Overwrite Rule** is set to **Devices** or **All** in the UMS Console under **UMS Administration > Global Configuration > Device Attributes**; see also Managing Device Attributes for IGEL OS Devices.

> ⓘ The character limit for device attributes is 100 characters. Longer entries will not be synchronized with the UMS.

Environment

For OS 11 Devices

- IGEL UMS 6.10 or higher
- Devices with IGEL OS 11.07.100 or higher

For OS 12 Devices

- IGEL UMS 12.03.100 or higher
- Devices with IGEL OS 12.3.0 or higher

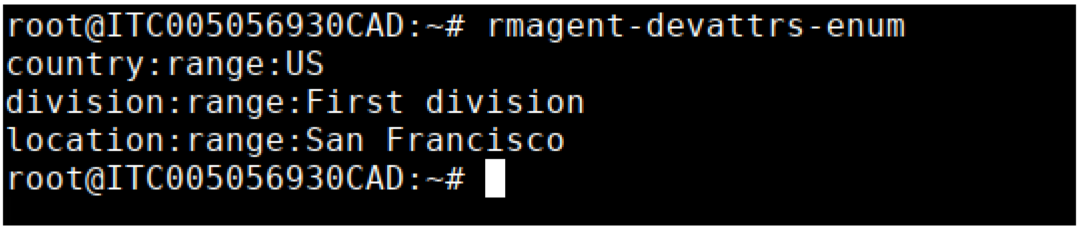
Command Reference

List All Device Attributes

```
/sbin/rmagent-devattrs-enum
```

Lists all device attributes including the current value for this device. The enumeration is ordered according to the attribute's order id.

Example:



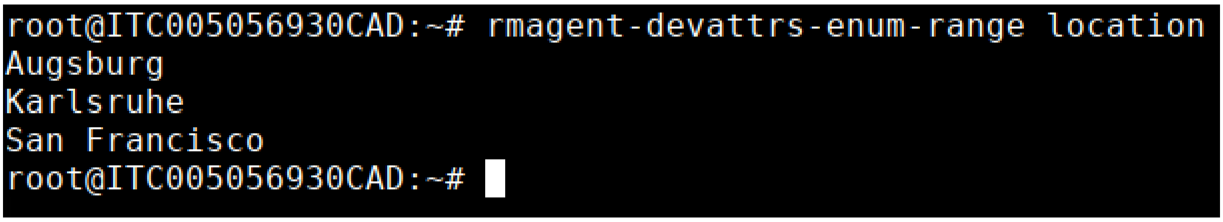
```
root@ITC005056930CAD:~# rmagent-devattrs-enum
country:range:US
division:range:First division
location:range:San Francisco
root@ITC005056930CAD:~#
```

Device Attribute of the Type "List": List All Possible Values

```
/sbin/rmagent-devattrs-enum-range <ATTRIBUTE_NAME>
```

Enumerates entries of the given range. The enumeration is ordered according to the range item's order id.

Example:



```
root@ITC005056930CAD:~# rmagent-devattrs-enum-range location
Augsburg
Karlsruhe
San Francisco
root@ITC005056930CAD:~#
```

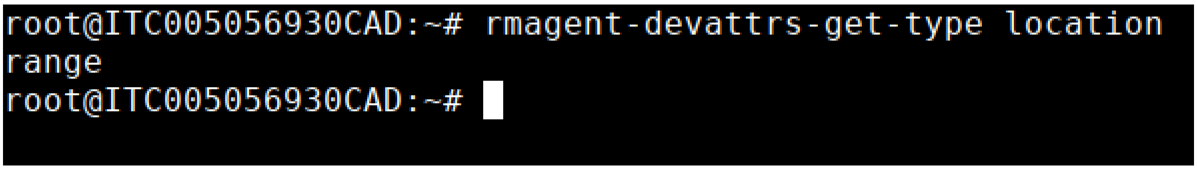
Print Attribute Type

```
/sbin/rmagent-devattrs-get-type <ATTRIBUTE_NAME>
```

Prints the type of the given attribute. Possible types are:

- string
- number
- date (format: yyyy-mm-dd)
- range

Example:



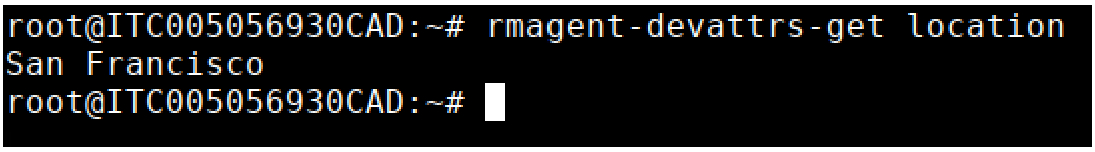
```
root@ITC005056930CAD:~# rmagent-devattrs-get-type location
range
root@ITC005056930CAD:~#
```

Print Attribute Value

```
/sbin/rmagent-devattrs-get <ATTRIBUTE_NAME>
```

Prints the current value of the given attribute.

Example:



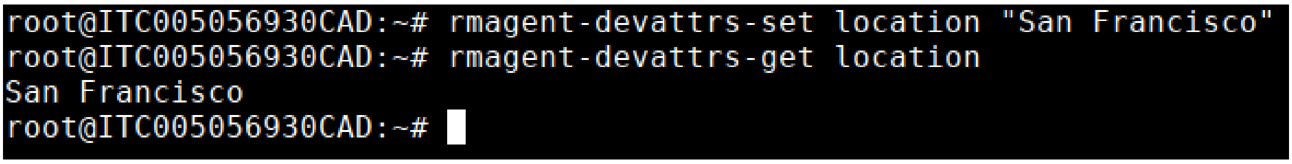
```
root@ITC005056930CAD:~# rmagent-devattrs-get location
San Francisco
root@ITC005056930CAD:~#
```

Set Attribute Value

```
/sbin/rmagent-devattrs-set <ATTRIBUTE_NAME> <ATTRIBUTE_VALUE>
```

Sets the given attribute to the specified value. If the overwrite rule for this attribute does not permit the device to change the value, an error is returned. Note that this command does not check the value type.

Example:



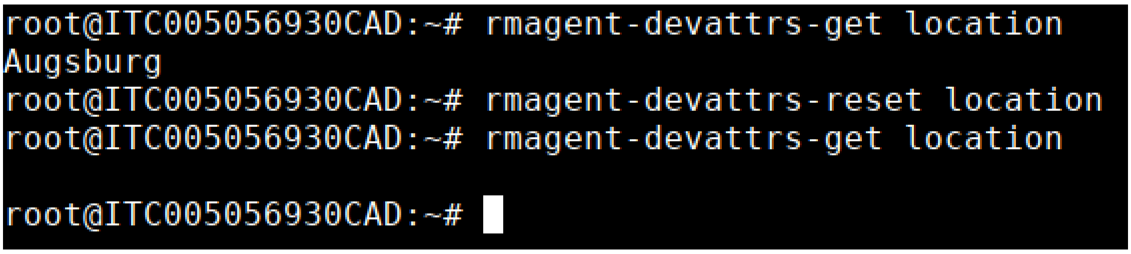
```
root@ITC005056930CAD:~# rmagent-devattrs-set location "San Francisco"
root@ITC005056930CAD:~# rmagent-devattrs-get location
San Francisco
root@ITC005056930CAD:~#
```

Reset Attribute Value

```
/sbin/rmagent-devattrs-reset <ATTRIBUTE_NAME>
```

Resets the given attribute to an empty value.

Example:



```
root@ITC005056930CAD:~# rmagent-devattrs-get location
Augsburg
root@ITC005056930CAD:~# rmagent-devattrs-reset location
root@ITC005056930CAD:~# rmagent-devattrs-get location

root@ITC005056930CAD:~#
```

Send Attributes to UMS If a Value Has Been Changed by Device

```
/sbin/rmagent-devattrs-sync
```

If any of the attribute values have been changed by the device, the complete set of attributes is sent to the UMS.

Send Attributes to UMS

```
/sbin/rmagent-write-device-attributes
```

The complete set of attributes is sent to the UMS.

Start of the UMS Console / Web App

UMS Web App: The Browser Displays a Security Warning (Certificate Error)

Symptom

When opening the UMS Web App, the browser displays a security warning and/or reports a certificate error.

Environment

- UMS Web App (UMS 6.06 or higher)

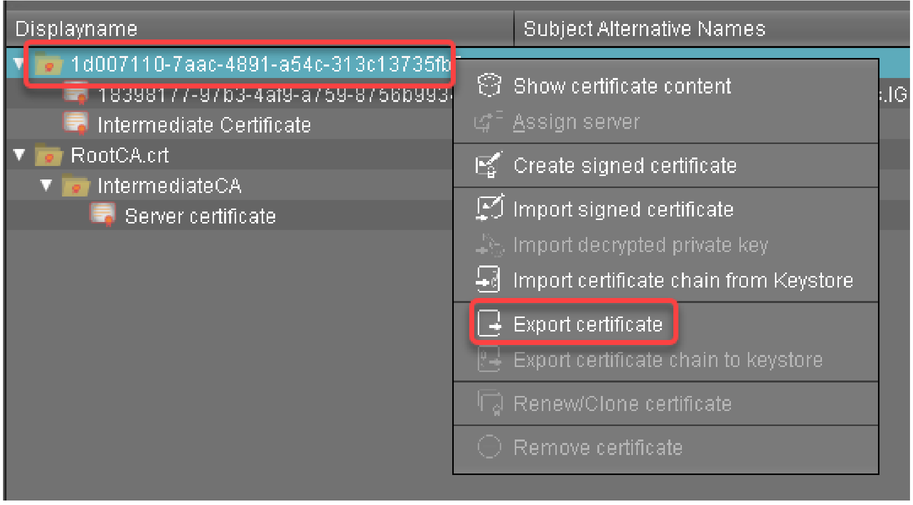
Problem

The customer uses an end certificate from a root CA that is not known to the browser. This is the case for self-signed certs, e.g. the default implementation.

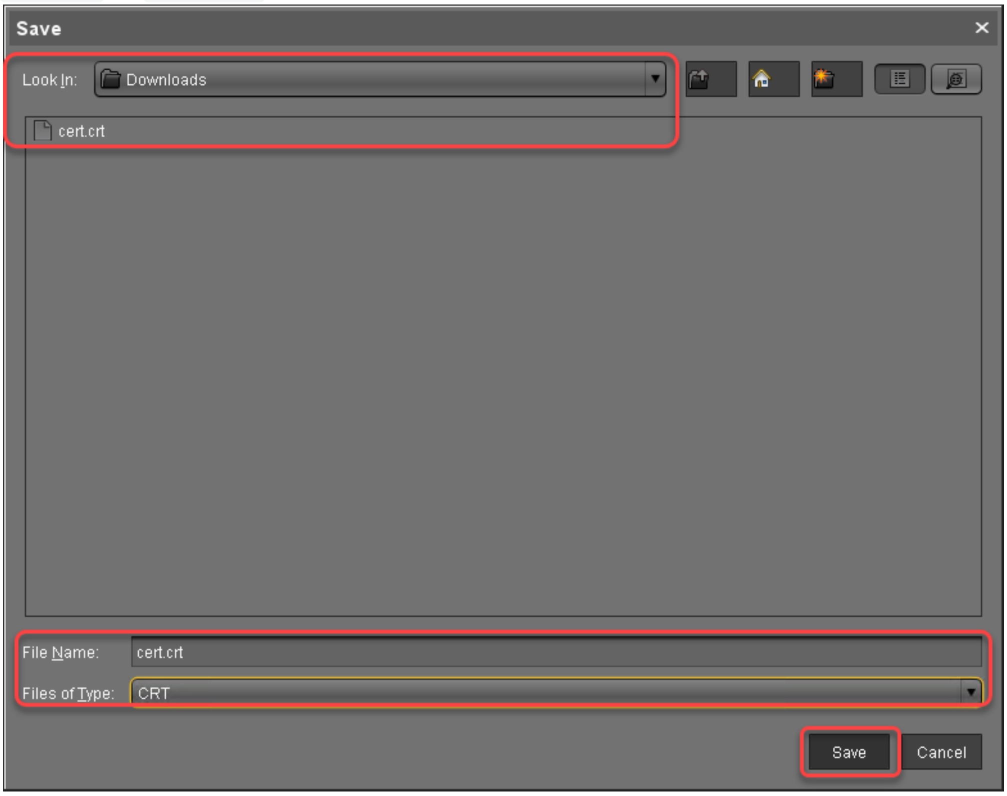
Solution

Exporting the Certificate from the UMS

1. In the UMS Console, go to **UMS Administration > Global Configuration > Certificate Management > Web**.
2. Make sure all end certificates in use are derived from the same root CA certificate.
3. Select the root CA certificate in use, open the context menu, and select **Export certificate**.


Displayname
Subject Alternative Names
1d007110-7aac-4891-a54c-313c13735fb
18398177-97b3-4af9-a759-8756b993
.IG
Intermediate Certificate
RootCA.crt
IntermediateCA
Server certificate
Show certificate content
Assign server
Create signed certificate
Import signed certificate
Import decrypted private key
Import certificate chain from Keystore
Export certificate
Export certificate chain to keystore
Renew/Clone certificate
Remove certificate

4. Select an appropriate location, select the correct file extension for your browser (most common: `*.crt` or `*.cert`), and click **Save**.



File Name: cert.crt

Files of Type: CRT

5. Add the certificate to the trusted certificates of your browser. For instructions, see Importing the Certificate into the Browser (see page 287).

Importing the Certificate into the Browser

⚠ The procedures described here may differ if you have a different browser version.

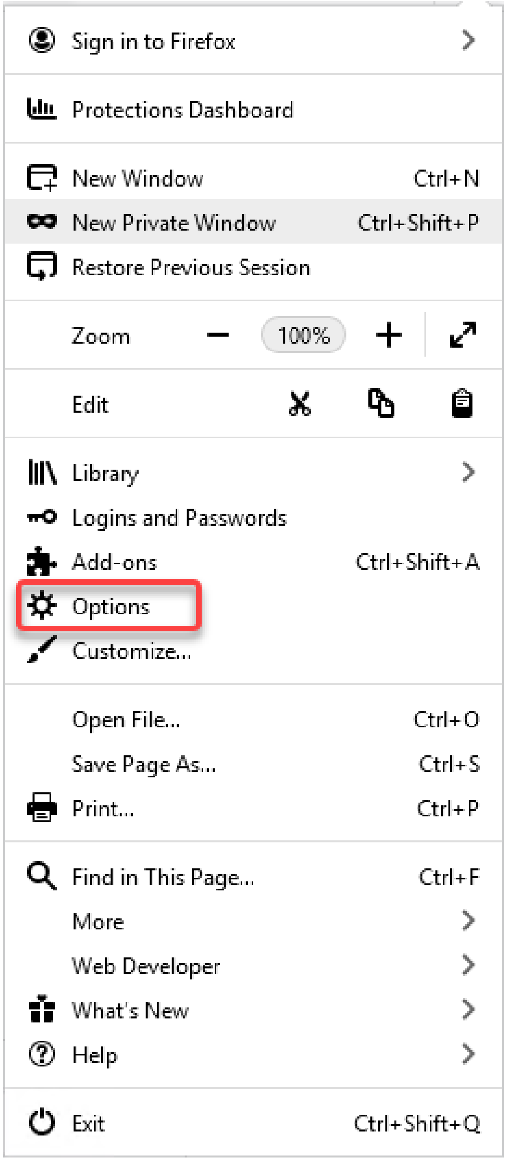
The following browsers are described here:

- Firefox (see page 287)
- Chrome (see page 291)
- Microsoft Edge (see page 298)

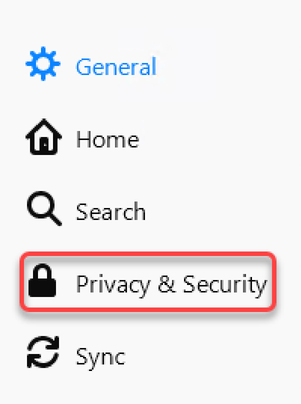
Firefox

1. Click ☰ to open the menu.

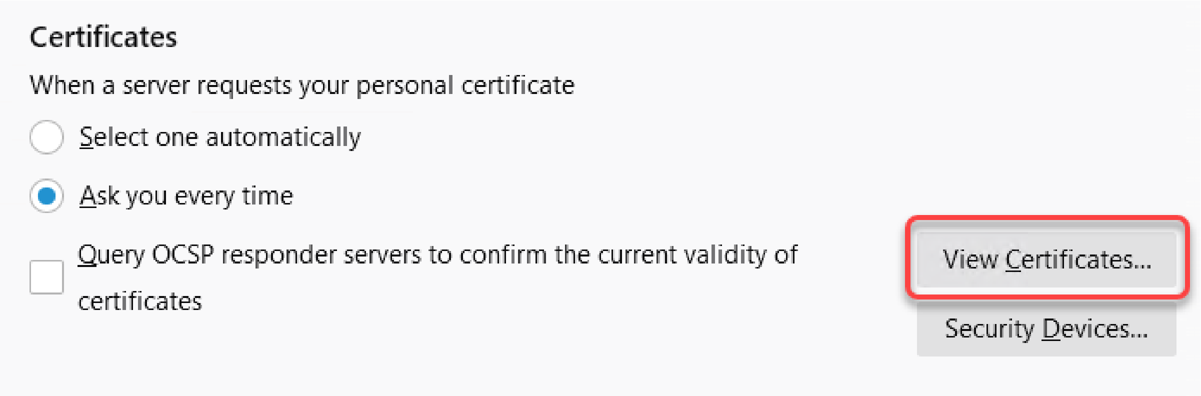
2. Select **Options**.



3. Select **Privacy & Security**.



4. Scroll down to Certificates and click **View Certificates**.



Certificates

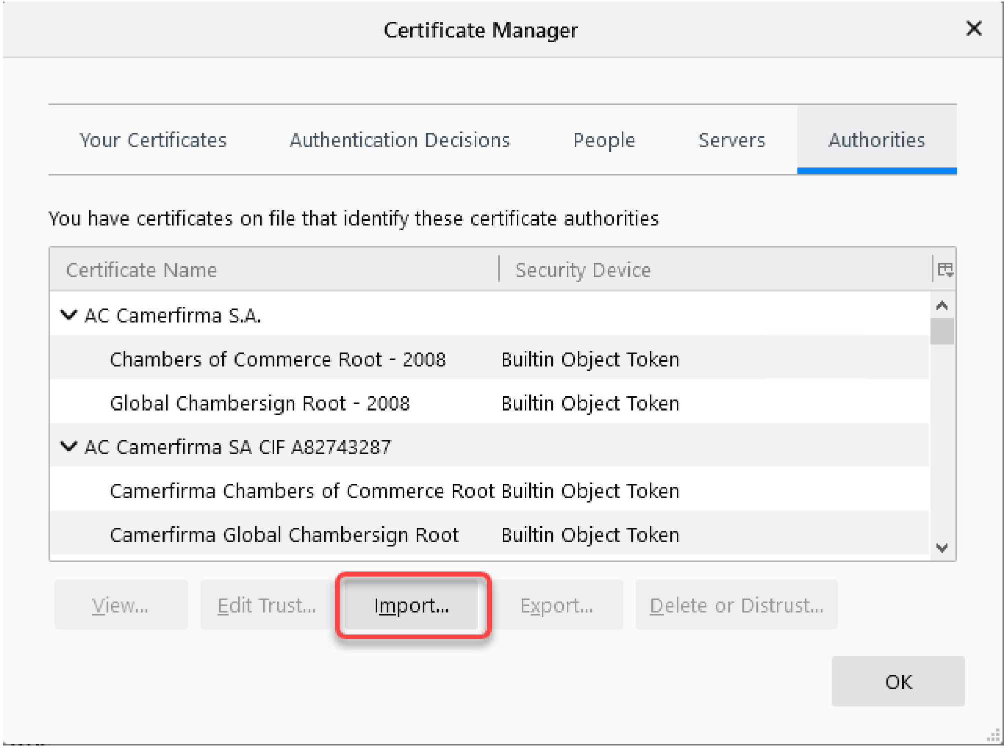
When a server requests your personal certificate

○ Select one automatically

● Ask you every time

□ Query OCSP responder servers to confirm the current validity of certificates

5. Click **Import**.



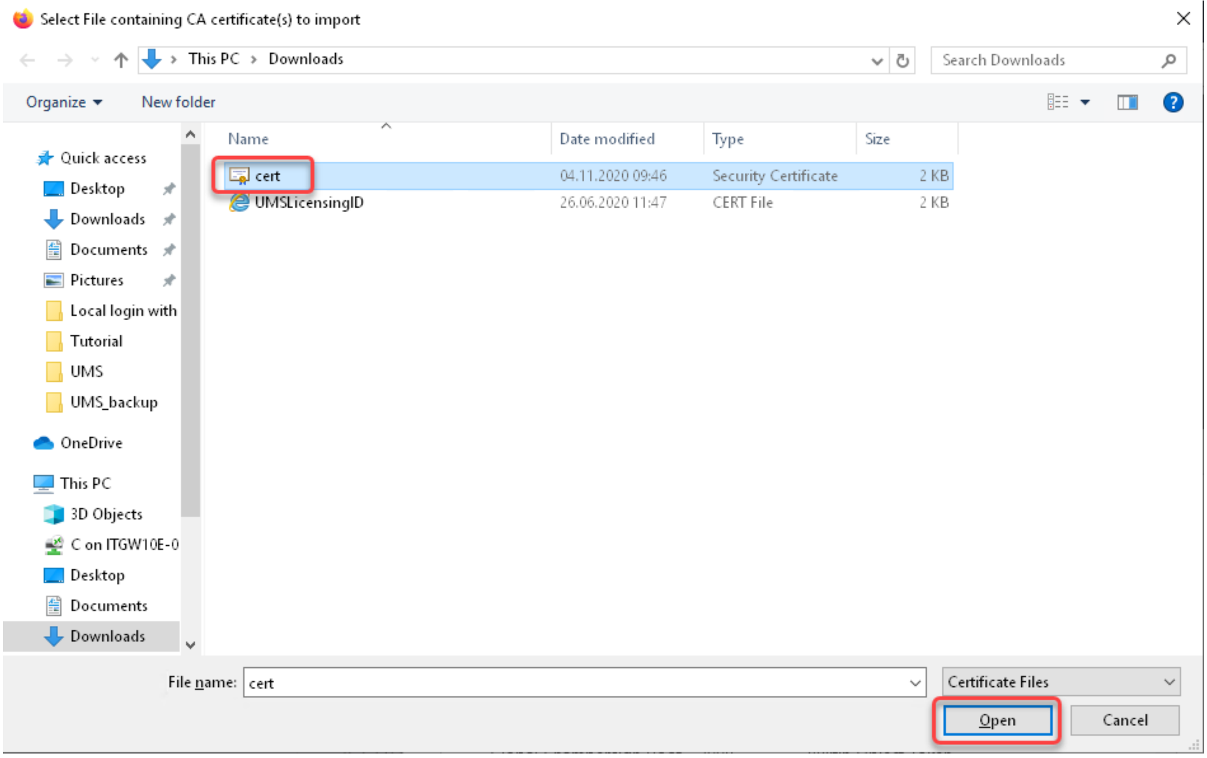
Certificate Manager

Your Certificates | Authentication Decisions | People | Servers | Authorities

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

6. Select your certificate file and click **Open**.



Select File containing CA certificate(s) to import

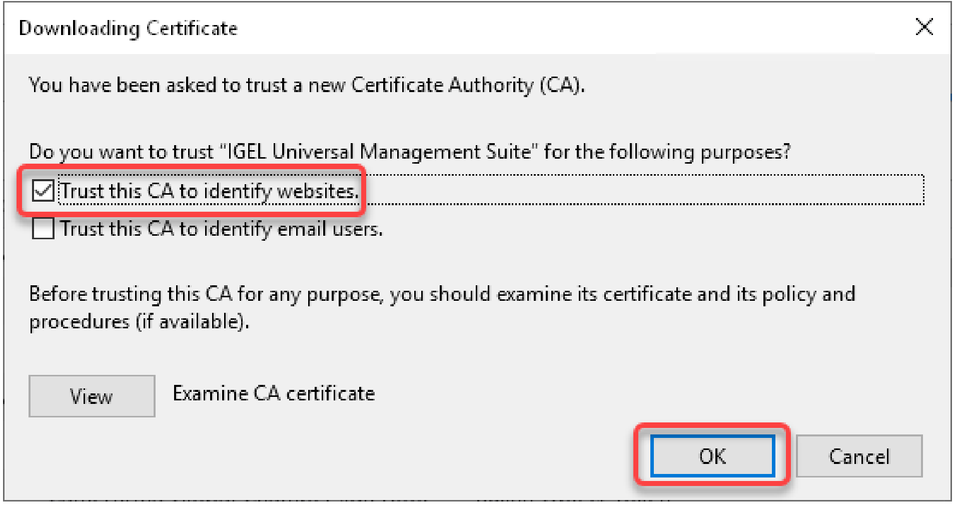
This PC › Downloads

Name	Date modified	Type	Size
cert	04.11.2020 09:46	Security Certificate	2 KB
UMSLicensingID	26.06.2020 11:47	CERT File	2 KB

File name: cert

Certificate Files

7. Activate **Trust this CA to identify websites** and click **OK**.



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

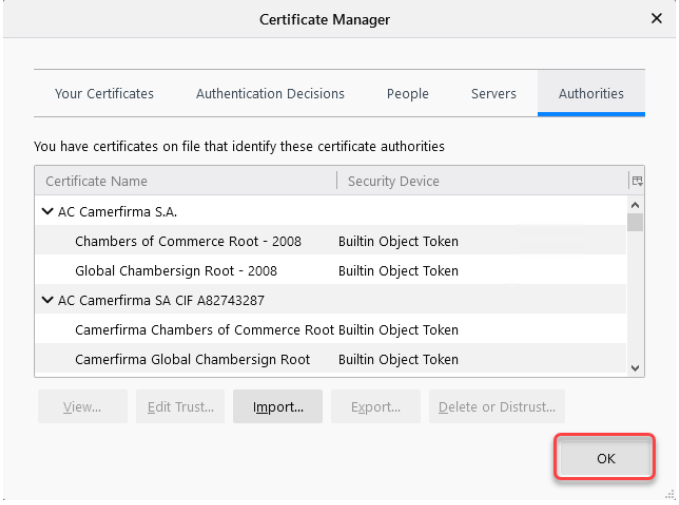
Do you want to trust "IGEL Universal Management Suite" for the following purposes?

☑ Trust this CA to identify websites.

□ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

8. Close the Certificate Manager window with **OK**.



You have certificates on file that identify these certificate authorities

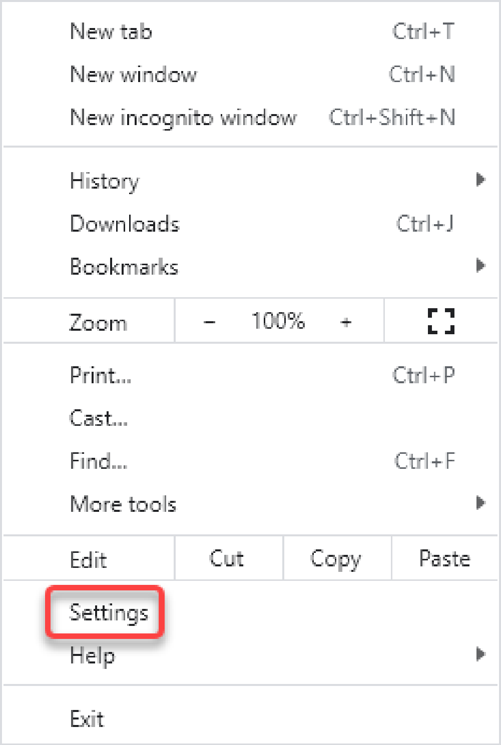
Certificate Name	Security Device
AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token

9. Restart the browser.
   The browser can access the UMS Web App without problems.

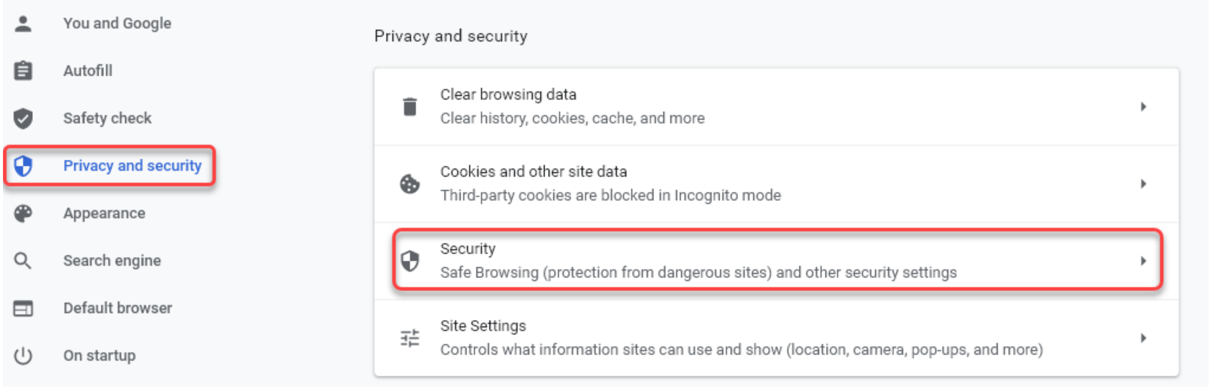
Chrome

1. Click ⋮ to open the menu.

2. Select **Settings**.



3. Go to **Privacy and security** and select **Security**.



Privacy and security

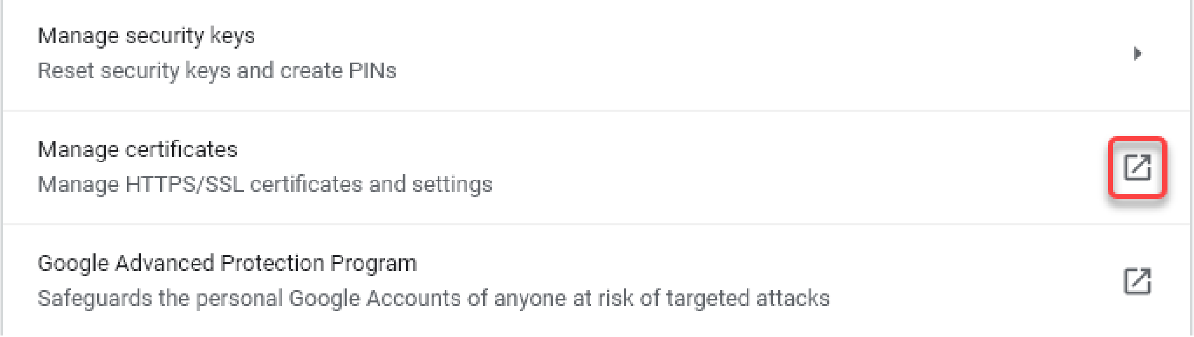
Clear browsing data
Clear history, cookies, cache, and more

Cookies and other site data
Third-party cookies are blocked in Incognito mode

Security
Safe Browsing (protection from dangerous sites) and other security settings

Site Settings
Controls what information sites can use and show (location, camera, pop-ups, and more)

4. Scroll down and click the symbol next to **Manage certificates**.

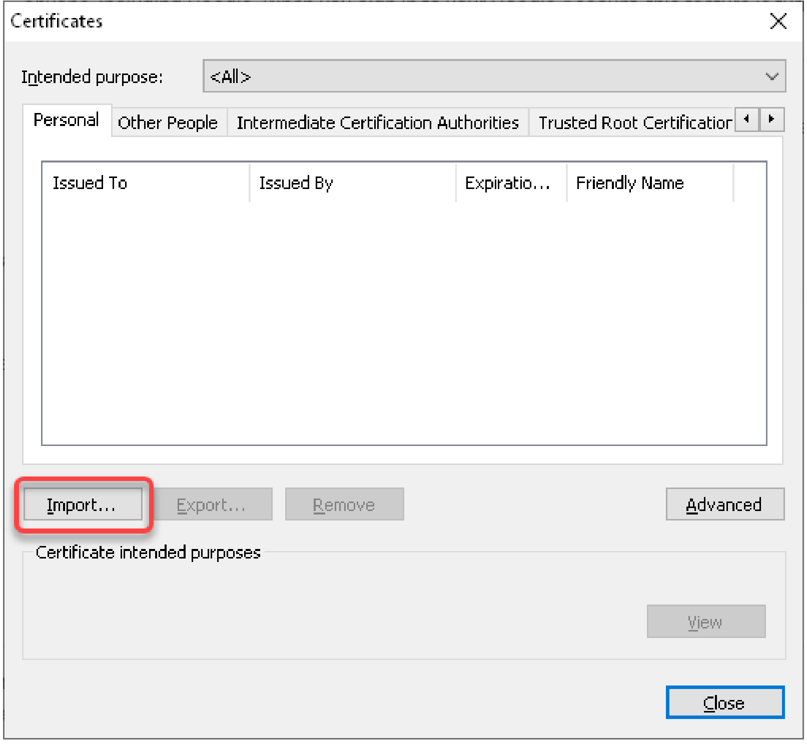


Manage security keys
Reset security keys and create PINs

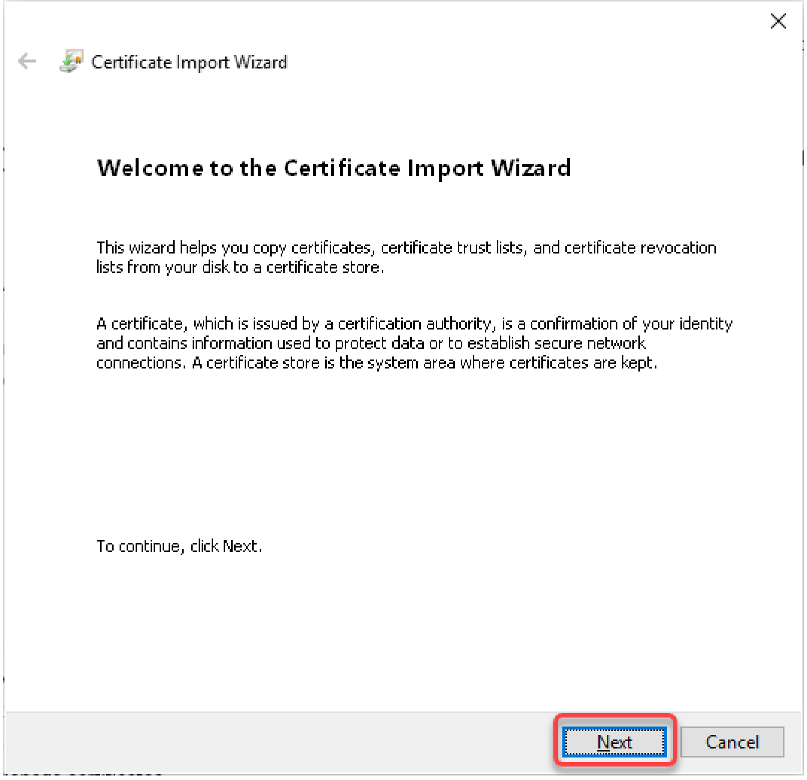
Manage certificates
Manage HTTPS/SSL certificates and settings

Google Advanced Protection Program
Safeguards the personal Google Accounts of anyone at risk of targeted attacks

5. In the **Certificates** dialog, click **Import**.



6. In the **Certificate Import Wizard**, click **Next**.



Certificate Import Wizard

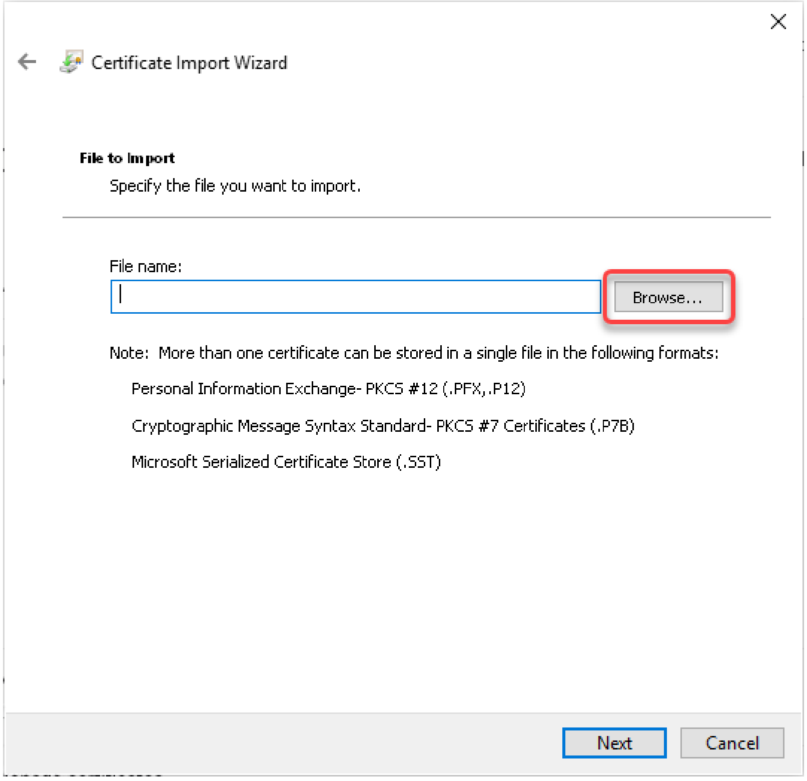
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Click **Browse** to open the file chooser.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

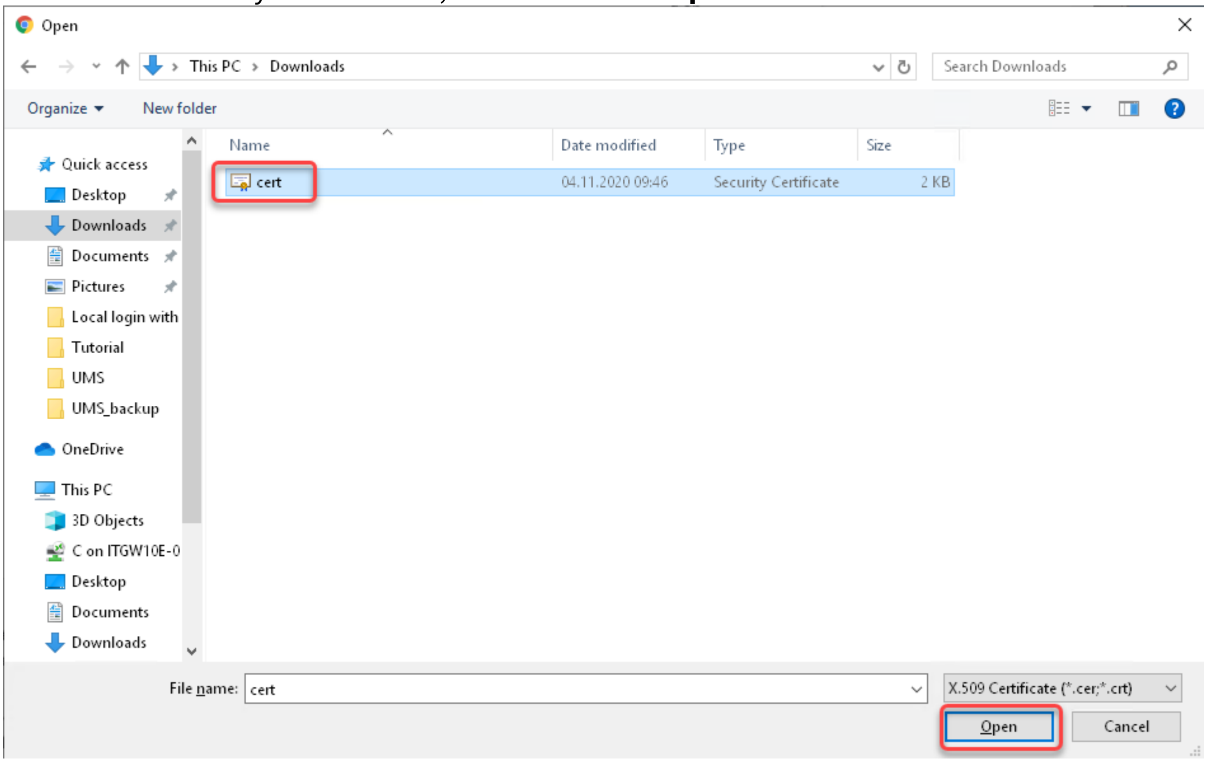
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

8. Go to the location of your certificate, select it and click **Open**.

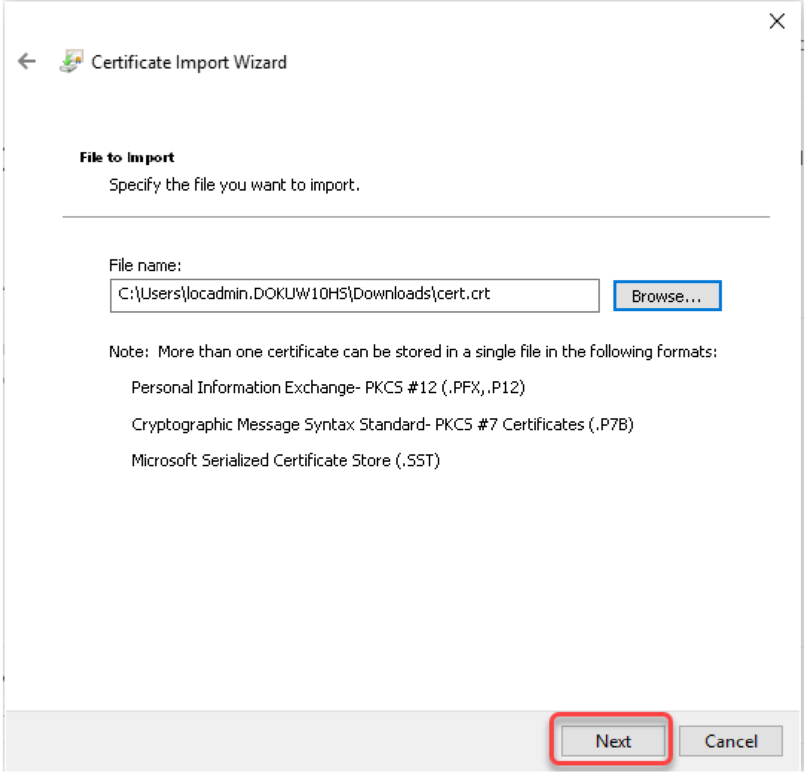


Name	Date modified	Type	Size
cert	04.11.2020 09:46	Security Certificate	2 KB

File name: cert

X.509 Certificate (*.cer;*.crt)

9. Back in the Certificate Import Wizard, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\locadmin.DOKUW10HS\Downloads\cert.crt

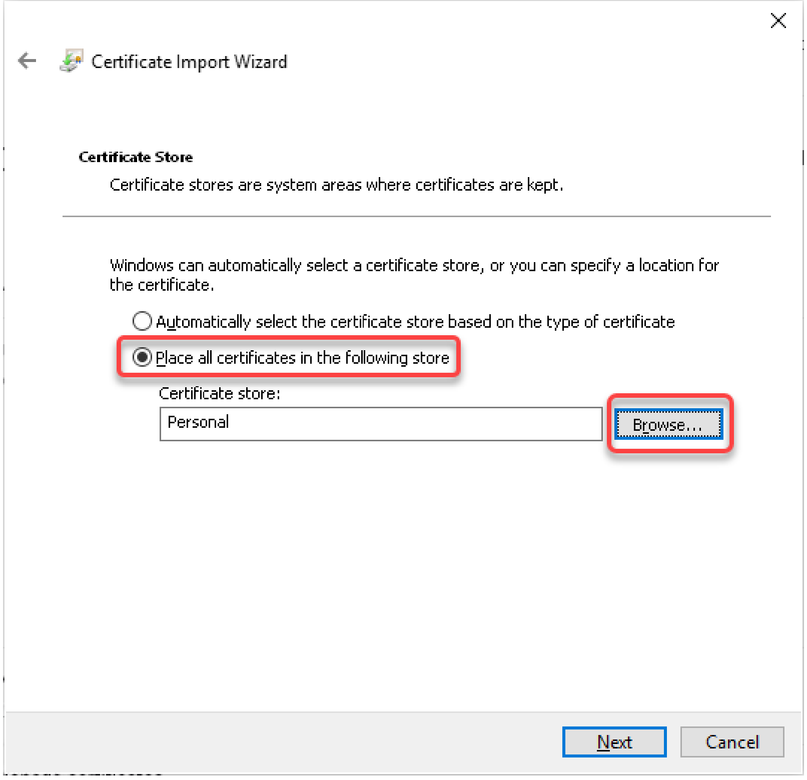
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

10. Select **Place all certificates in the following store** and click **Browse** to determine the certificate store.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

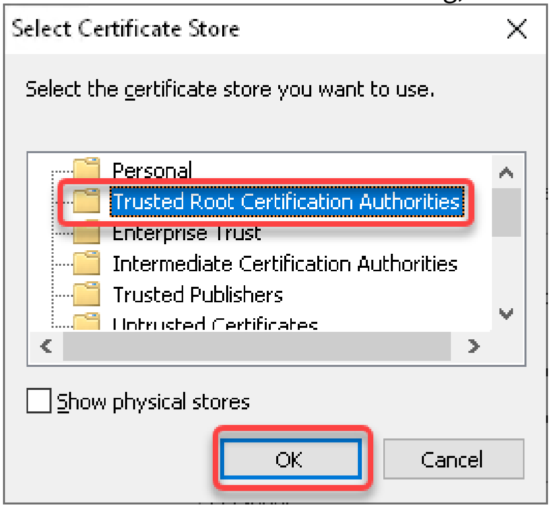
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Personal

11. In the **Select Certificate Store** dialog, select **Trusted Root Certification Authorities** and click **OK**.



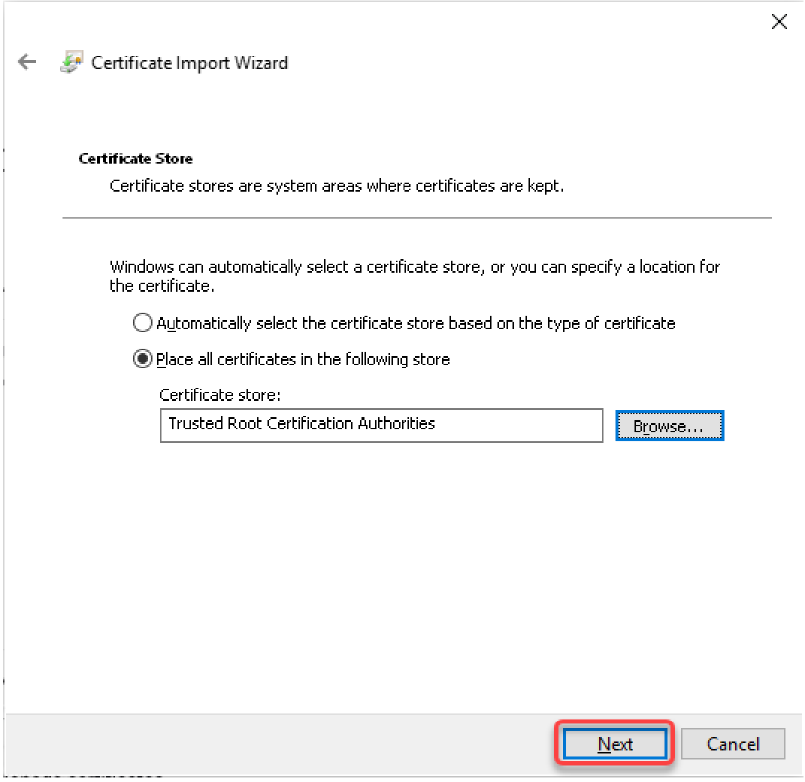
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

12. Back in the **Certificate Import Wizard**, click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

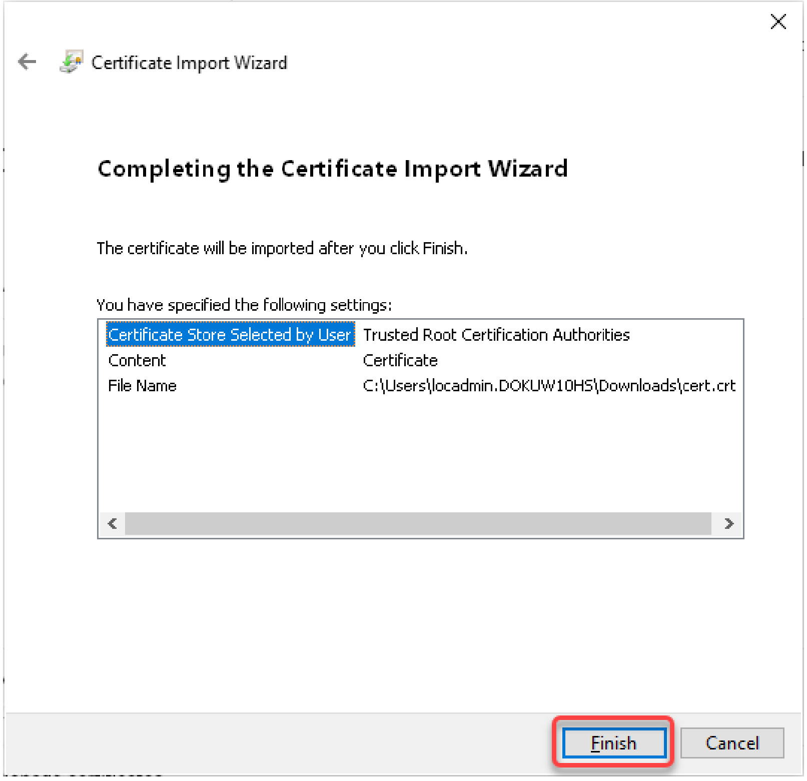
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

13. Review your settings and click **Finish**.



Certificate Import Wizard

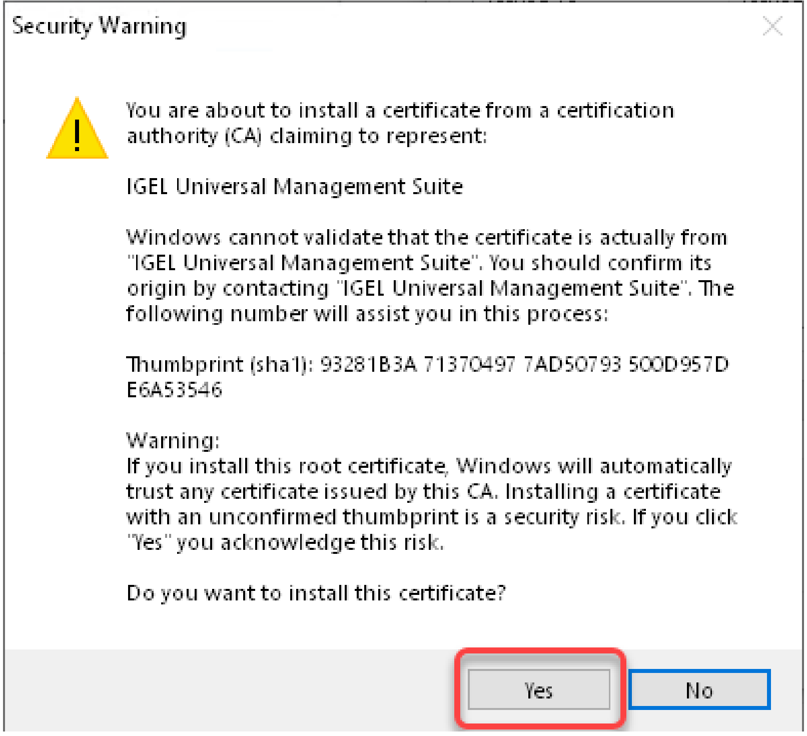
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	C:\Users\locadmin.DOKUW10HS\Downloads\cert.crt

14. Confirm the **Security Warning** with **Yes**.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

IGEL Universal Management Suite

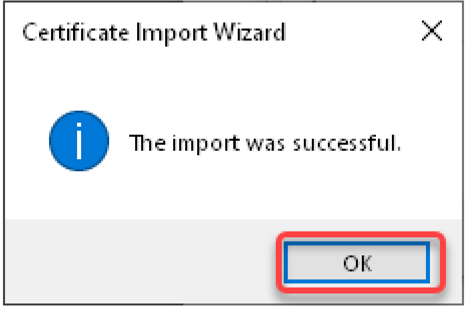
Windows cannot validate that the certificate is actually from "IGEL Universal Management Suite". You should confirm its origin by contacting "IGEL Universal Management Suite". The following number will assist you in this process:

Thumbprint (sha1): 93281B3A 71370497 7AD50793 500D957D E6A53546

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

15. If the import was successful, a success message is displayed.



Certificate Import Wizard

The import was successful.

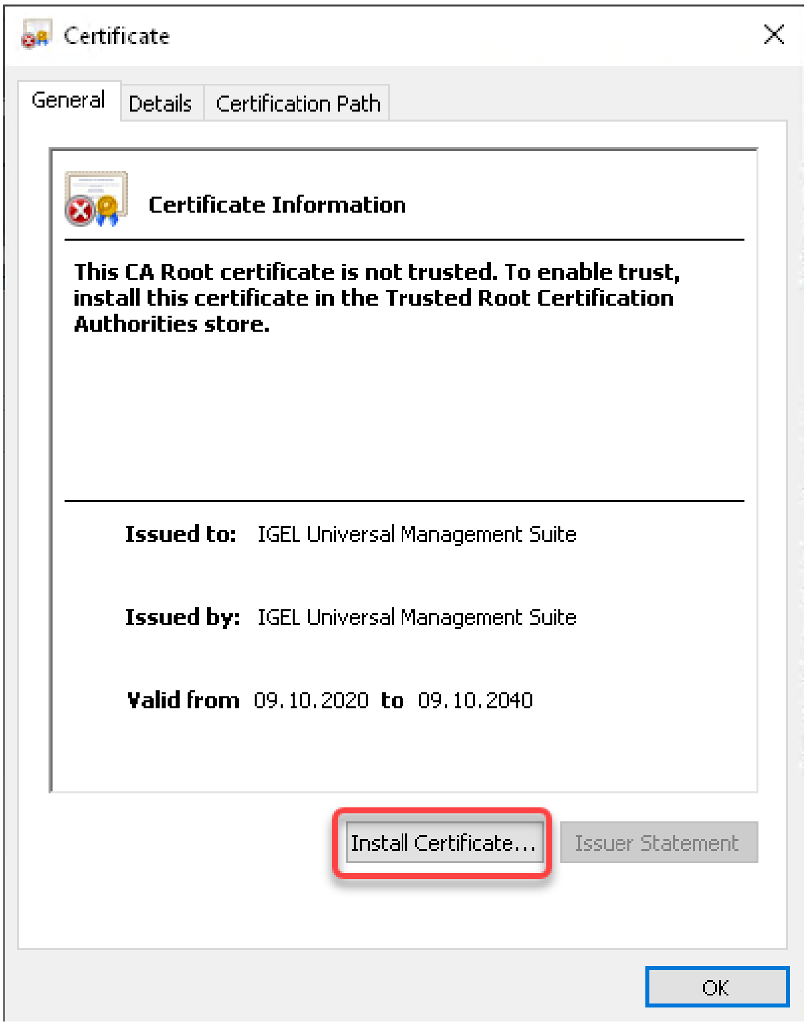
The certificate is installed on your system.

16. Restart the browser.
The browser can access the UMS Web App without problems.

Microsoft Edge

1. Make sure you have administrator permissions.
2. Go to the location where you have stored the certificate and double-click the certificate file.
The **Certificate** dialog of your Windows system opens.

3. Click **Install Certificate...**.



Certificate Information

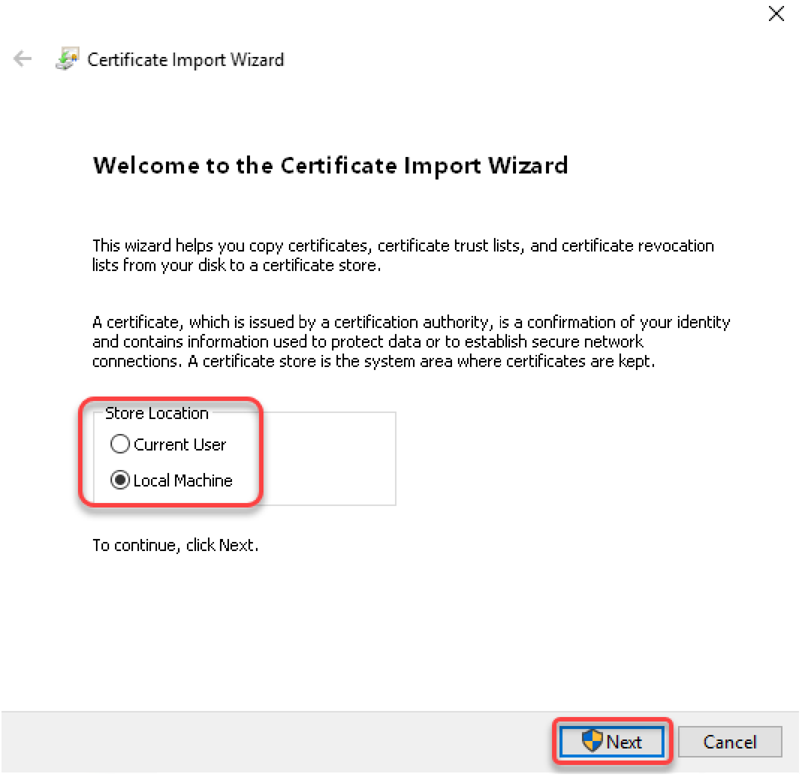
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: IGEL Universal Management Suite

Issued by: IGEL Universal Management Suite

Valid from 09.10.2020 to 09.10.2040

4. Define whether the certificate should be installed for the current user only or for all users (**Local Machine**) and click **Next**.



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

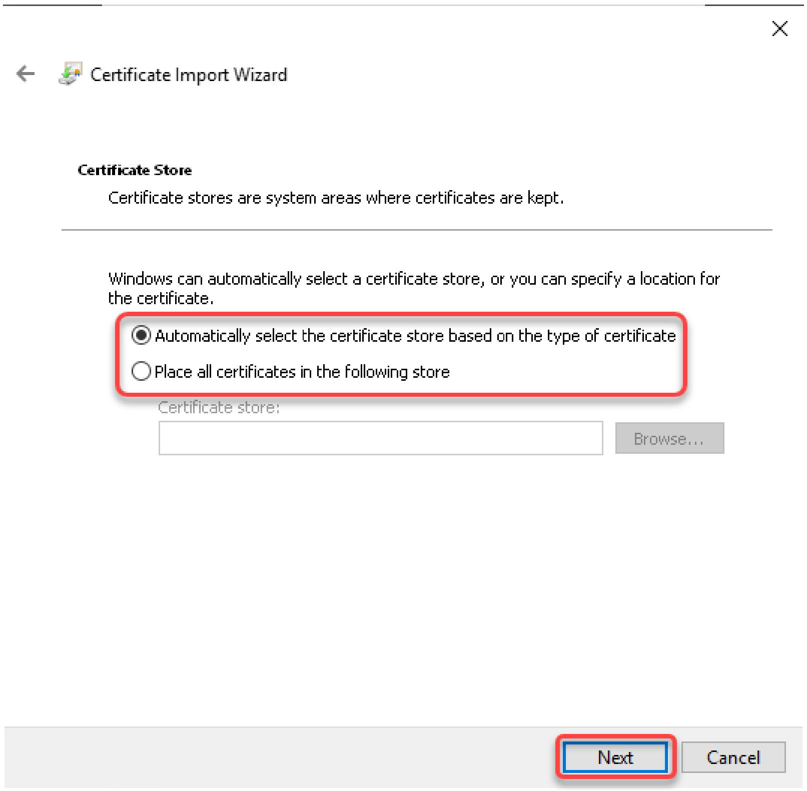
○ Current User

● Local Machine

To continue, click Next.

5. Confirm the **User Account Control** dialog.

6. Define whether the certificate store should be determined automatically or manually and click **Next**.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

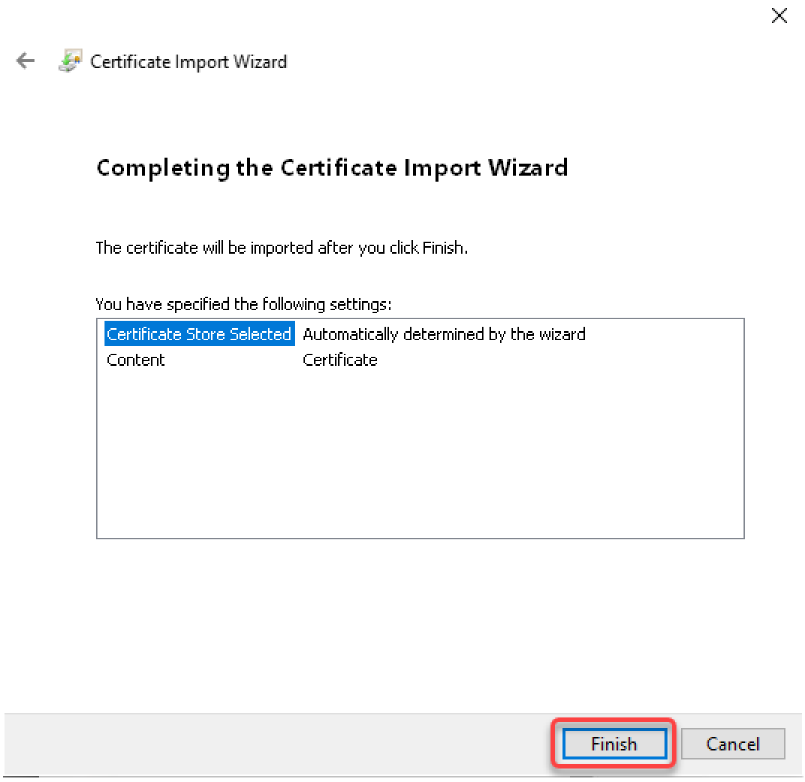
Windows can automatically select a certificate store, or you can specify a location for the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

7. Review your settings and click **Finish**.



Certificate Import Wizard

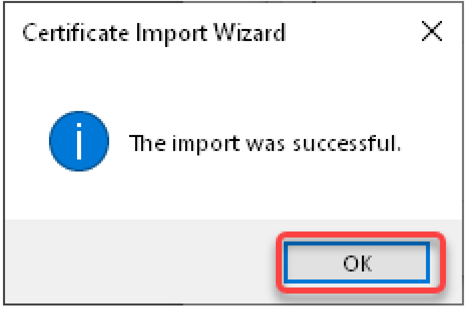
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by the wizard
Content	Certificate

If the import was successful, a success message is displayed.



Certificate Import Wizard

The import was successful.

The certificate is installed on your system.

8. Restart the browser.
   The browser can access the UMS Web App without problems.

Starting UMS Console Crashes NX Session

Symptom

When you are connected to an Ubuntu host via NX, starting the UMS Console on the Ubuntu host crashes the NX session.

Solution

1. Become **Root** on the Ubuntu host.
2. Open the configuration file `/opt/IGEL/RemoteManager/rmclient/RemoteManager.bin.config` in a text editor.
3. Add the line `vmparam -Dsun.java2d.xrender=false` to the file.
4. Save the file.
5. Become a regular user.
6. Start the UMS Console.

UMS Console doesn't start on Linux System without X11

Symptom

IGEL UMS doesn't start on Linux system without X11.

Problem

The UMS console application needs X11 to run.

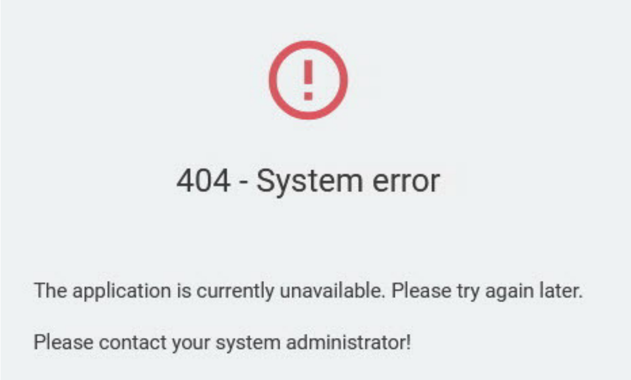
Solution

▶ Install X Window System (X11) to run IGEL UMS.

UMS Web App: "404 - System Error" Message

Symptom

After the installation of the Universal Management Suite, the UMS Web App starts with a 404 system error.



404 - System error

The application is currently unavailable. Please try again later.

Please contact your system administrator!

Environment

- UMS 6.08.100 or higher with the embedded database
- Microsoft Windows Server 2019

Problem

This might happen at startup when the UMS Web App is starting faster than the UMS Server service.

Solution

▶ Restart the Windows service `IGEL RMGUIServer`. Details on how to do this can be found under IGEL UMS HA Services and Processes.

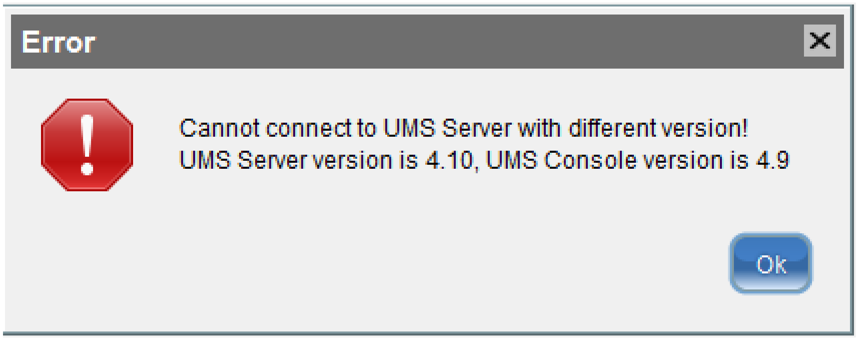
Logon failures

UMS Console Logon fails

Symptom

When you try to log on to the console you get the error message **Unable to load tree**.

More recent UMS versions show the following error message:



Cannot connect to UMS Server with different version!
UMS Server version is 4.10, UMS Console version is 4.9

Problem

Problems with the connection between the UMS console and the UMS server may be caused by a difference in software versions, e.g. if the UMS server was updated but the console still uses an old version.

Solution

Check the version status:

1. Check the version of the console by selecting **Help > Info** from the UMS console menu.
2. Check the version of the server by selecting **Help > Info** from the UMS administrator menu.
3. If necessary, update the UMS console to the same version as the server or newer.

UMS Console Login with AD User Account fails

Symptom

UMS console login fails for Active Directory user.

Problem

1. Open catalina log file `C:\Program Files\IGEL\RemoteManager\rmguiserver\logs\catalina.log`
2. Check the log for message `KDC has no support for encryption type (14)`

Solution

If this happens, the following things needs to be done/checked:

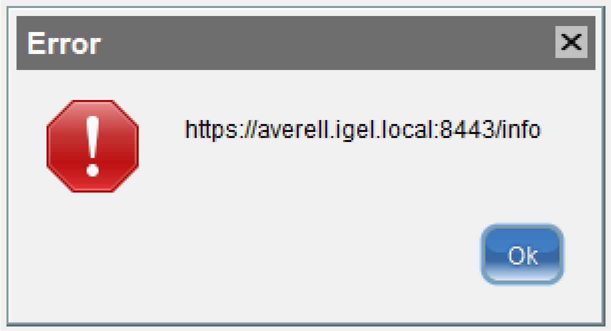
1. Have a look at http://technet.microsoft.com/en-us/library/cc733991.aspx.
2. Disable **DES encryption** for the AD user account, this can be done in the account setup of the Windows user administration > Account options.
3. Follow http://docs.oracle.com/javase/6/docs/technotes/guides/security/jgss/tutorials/Troubleshooting.html.

Login to the UMS Fails after the Update

Symptom

You cannot log in to the UMS after an update or the installation of the UMS Server.

An error message with the URL `https://[ums_server_host]:8443/info` appears:



https://averell.igel.local:8443/info

Problem

The IGEL RMGUI Server Service has not fully started yet.

Solution

Wait for a few minutes more. After that, try to log in again.

Active Directory / LDAP

Integrating Active Directory

Problem

Instead of creating and organizing UMS administrators manually you are looking for an easy way of importing them from your existing Active Directory.

Reason

You would like to import users and user groups from the Active Directory to the UMS, using the same AD group assignments and credentials as already defined in the AD.

Solution

In this paper we explain the best way of importing users from the Active Directory as UMS administrator accounts.

We will import users from the Active Directory to the UMS console in three steps by:

- Configuring the connection to the Active Directory
- Selecting the users to be imported and starting the import
- Assigning permissions

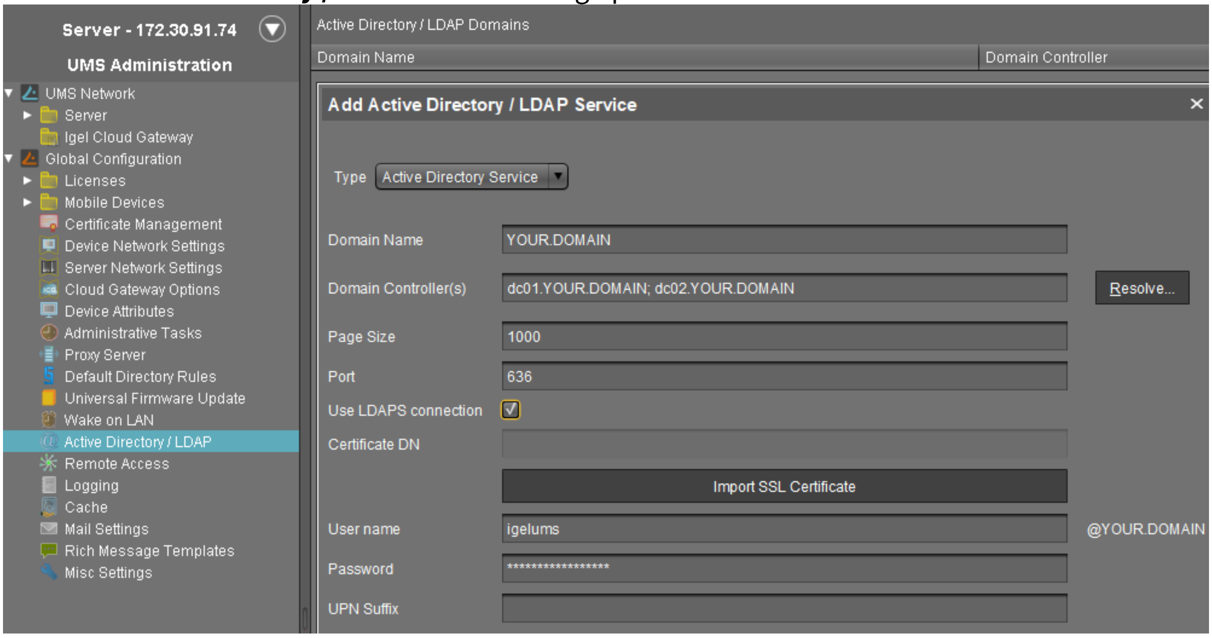
Configuring an AD Connection

Perform the following steps to set up the connection between the UMS and the Active Directory of your company:

1. If you have user and group dependencies between different configured domains/subdomains, then you might want to activate **Include all configured AD domains for search and import of AD users / groups**. This option activates the group search for a user within all configured domains. On activation, a confirmation dialog is shown.

> ⓘ If this option is activated, a user may gain additional permissions. This will be the case if
> - the user is in a group that has been discovered due to this option,
> - this group has been imported under **System > Administrator accounts**,
> - and permissions have been assigned to this group i.e. permissions the user would not have otherwise.
>
> Please note that, due to the additional lookups, this option might have an impact on the performance in the following areas:
> - UMS login
> - Permission dialogs
> - Shared Workplace (SWP)

2. Click **Add (+)** under UMS console > **UMS Administration > Global Configuration > Active Directory / LDAP**.
The **Add Active Directory / LDAP Service** dialog opens.



Type: Active Directory Service

Domain Name: YOUR.DOMAIN

Domain Controller(s): dc01.YOUR.DOMAIN; dc02.YOUR.DOMAIN

Page Size: 1000

Port: 636

Use LDAPS connection: ☑

Certificate DN:

User name: igelums @YOUR.DOMAIN

Password: ****************

UPN Suffix:

3. Select **Active Directory Service** as **Type.**

4. Enter the **Domain Name**.

> Several Active Directories can be linked. You should therefore ensure that you provide the correct domain when logging in (e.g. to the UMS console).

5. Enter the **Domain Controller(s)** manually or click **Resolve...** for the automatic search.
   To separate domain controllers, use a semicolon.

   > If the option **Use LDAPS connection** (see below) is enabled, make sure that a fully qualified name of the **Domain Controller** has been entered. See Problems When Configuring an Active Directory with LDAP over SSL (see page 323).

6. Enter **Page Size**.
   The **Page Size** property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but not the number of overall results. The standard value is "1000". Change this value in line with your server configuration.

7. Activate **Use LDAPS connection** to secure the connection with the provided certificate.
   The **Port** changes automatically to default "636".

8. Click **Import SSL Certificate** to configure the certificate and to verify the **Certificate DN**.

   > Since the name of the **Domain Controller** is checked against the certificate, they must correspond. If more than one domain controller is used, the root certificate of the domain must be configured. See Problems When Configuring an Active Directory with LDAP over SSL (see page 323).

   > The supported certificate formats are `.cer`, `.pem` and `.der`

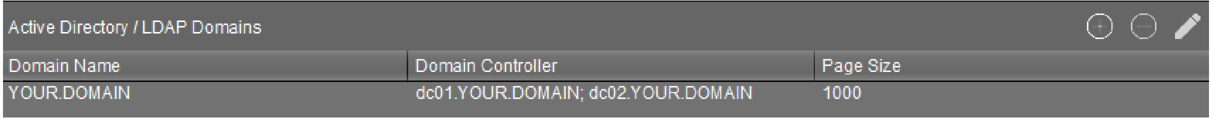
9. Under **User name** and **Password**, enter your user credentials. This user must have read access in Active Directory.

10. Enter **UPN Suffixes** (aliases) if you have defined any (semicolon separated list). Example:
    `domain.local;test.local`

    > The settings must correspond to the configuration of the Active Directory. If there are registered UPN suffixes in the AD, they should be known also by the UMS.

11. Click on **Test Connection** to check that you have entered a valid configuration.

12. Click **Ok** to confirm your settings.
    The Active Directory domain is listed under **Active Directory / LDAP Domains**.



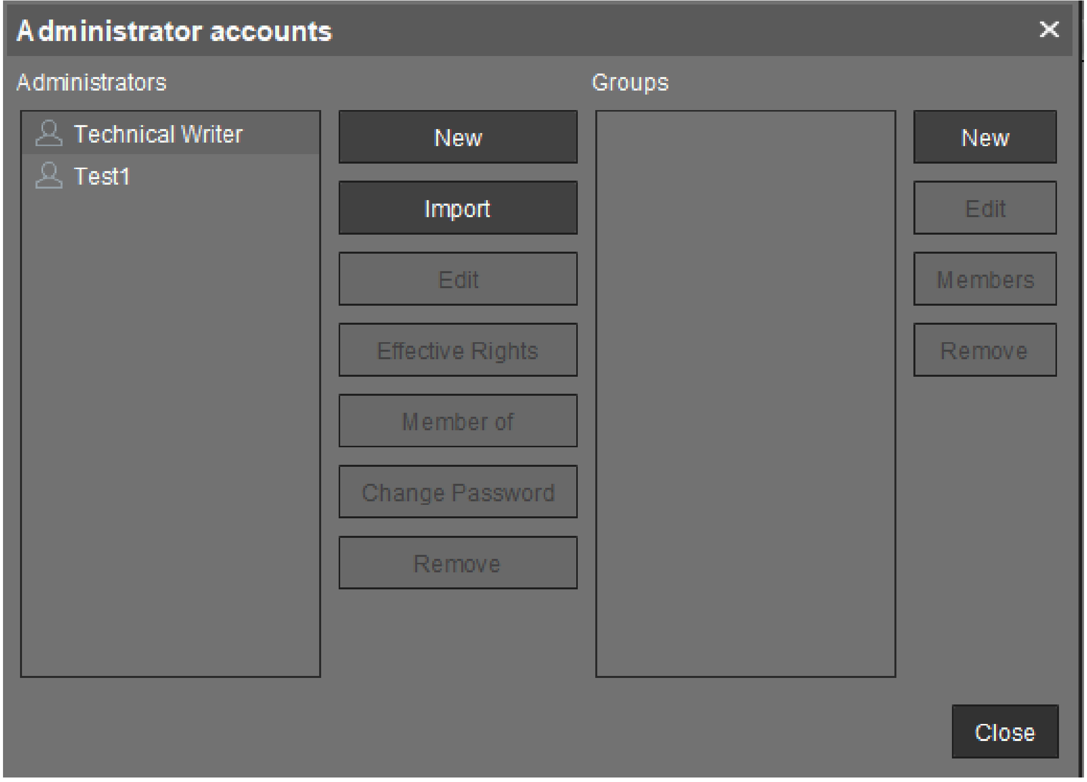
Active Directory / LDAP Domains

Domain Name	Domain Controller	Page Size
YOUR.DOMAIN	dc01.YOUR.DOMAIN; dc02.YOUR.DOMAIN	1000

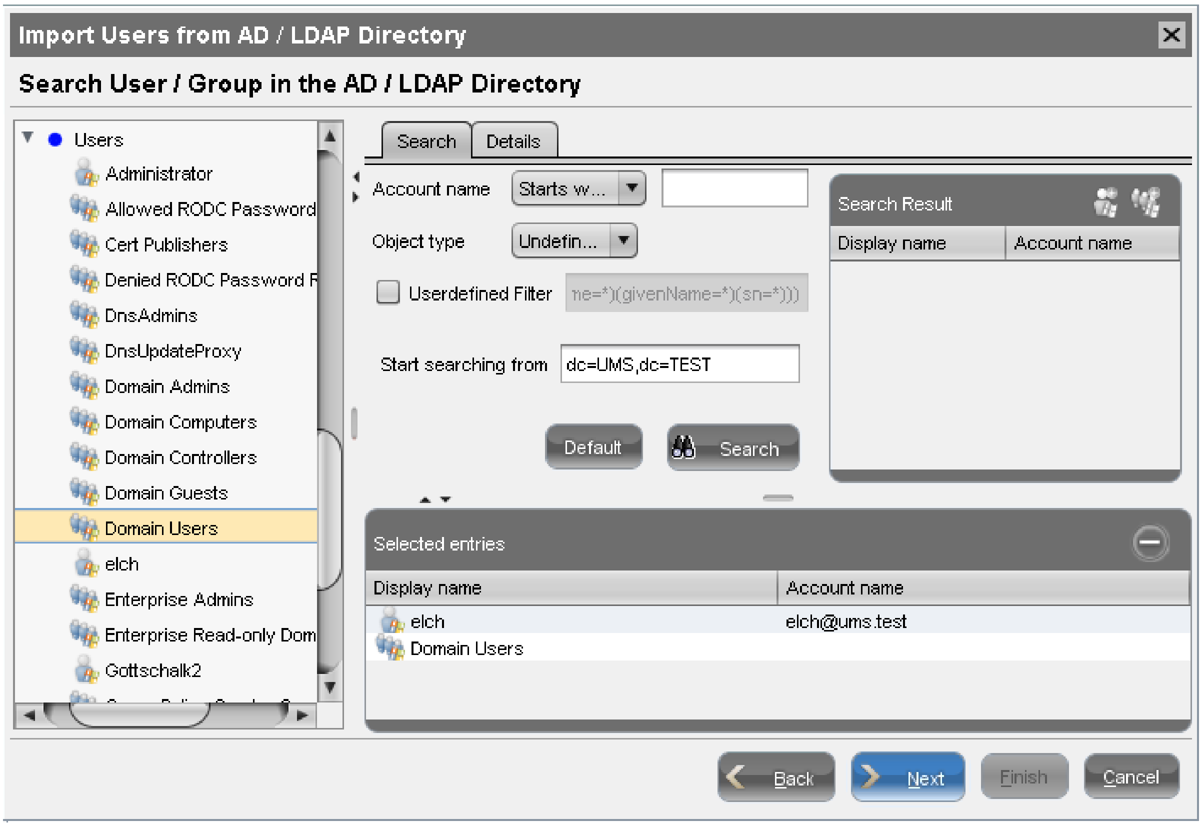
Importing Users from AD to UMS

After connecting the Active Directory you can import users or user groups to the UMS:

1. Click **System > Administrator Accounts**.
   The **Administrator Accounts** window opens:



2. Click **Import** to log in to the AD/LDAP service.
3. Select the domain and enter your credentials, if not already defined.
4. Click **Next** to open the Active Directory browser.
5. Select individual users or groups from the structure tree of your AD.
6. Use drag and drop to add your selection to the **Selected Entries** list.



Account name: Starts w...

Object type: Undefin...

□ Userdefined Filter: ne=*)(givenName=*)(sn=*)))

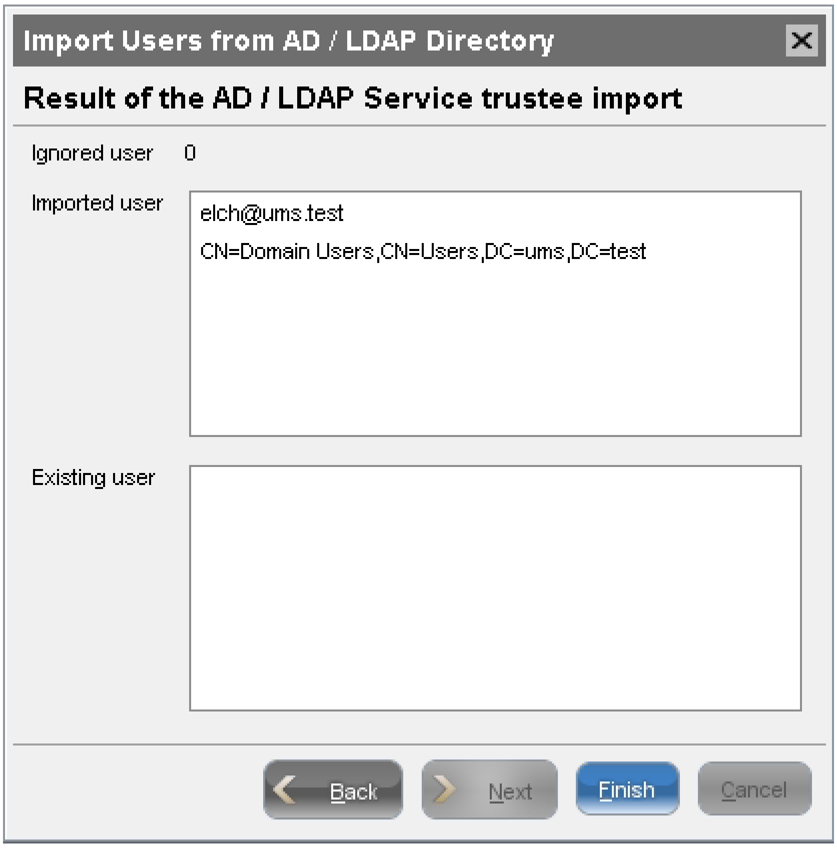
Start searching from: dc=UMS,dc=TEST

Selected entries

Display name	Account name
elch	elch@ums.test
Domain Users	

ⓘ As an alternative to navigating in the structure tree, you can also add users or groups to your selection using the Search function.

7. Click **Next** and confirm to start the import.
   A result list of imported accounts opens.



Result of the AD / LDAP Service trustee import

Ignored user 0

Imported user
elch@ums.test
CN=Domain Users,CN=Users,DC=ums,DC=test

Existing user

8. Click **Finish** to complete the import.

If the result list is either empty or some accounts are missing from the list, see Import of Administrator Accounts from Active Directory Fails (see page 324).

> A UMS administrator set up by mistake must be deleted manually using the dialog 'Administrator accounts'. The IGEL UMS uses the 'User logon name' from the AD as the name of the imported user.

Assigning Permissions

After the AD users have been imported, they can access the UMS with their Active Directory credentials.

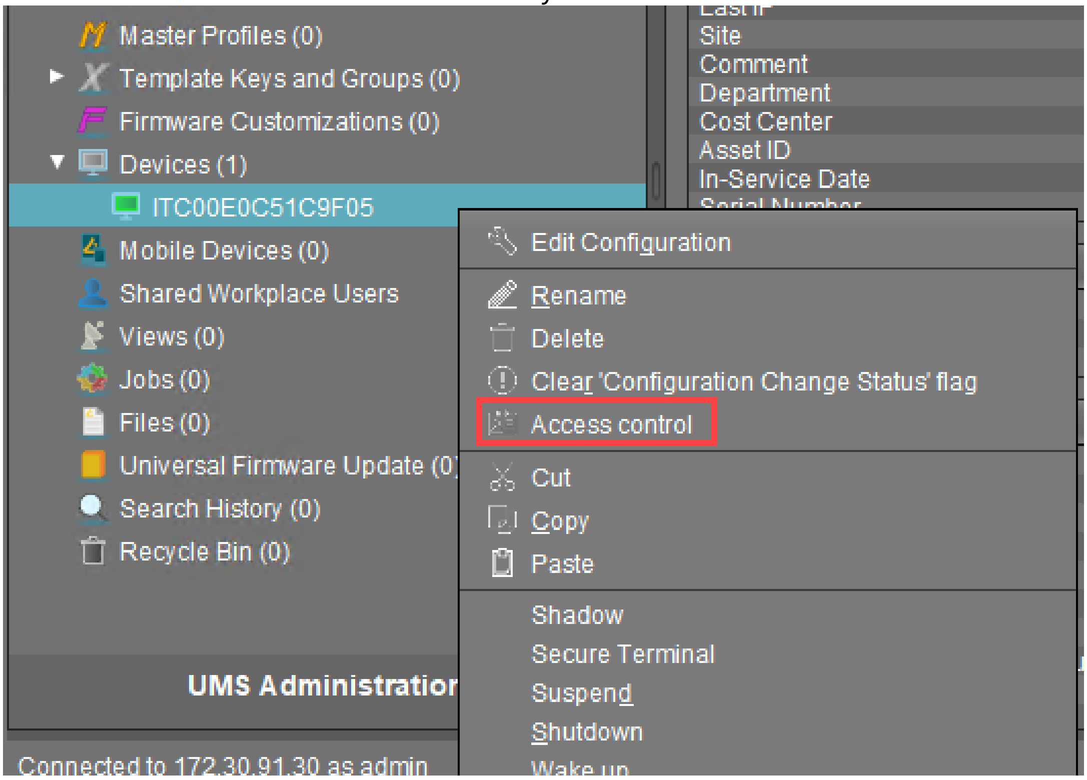
As UMS administrators, the users still need individual access rights.

ⓘ The logon to the UMS is not possible via the 'pre Windows 2000 logon name' ('DOMAIN\logon name'), but only via the format 'logon name@DOMAIN'.

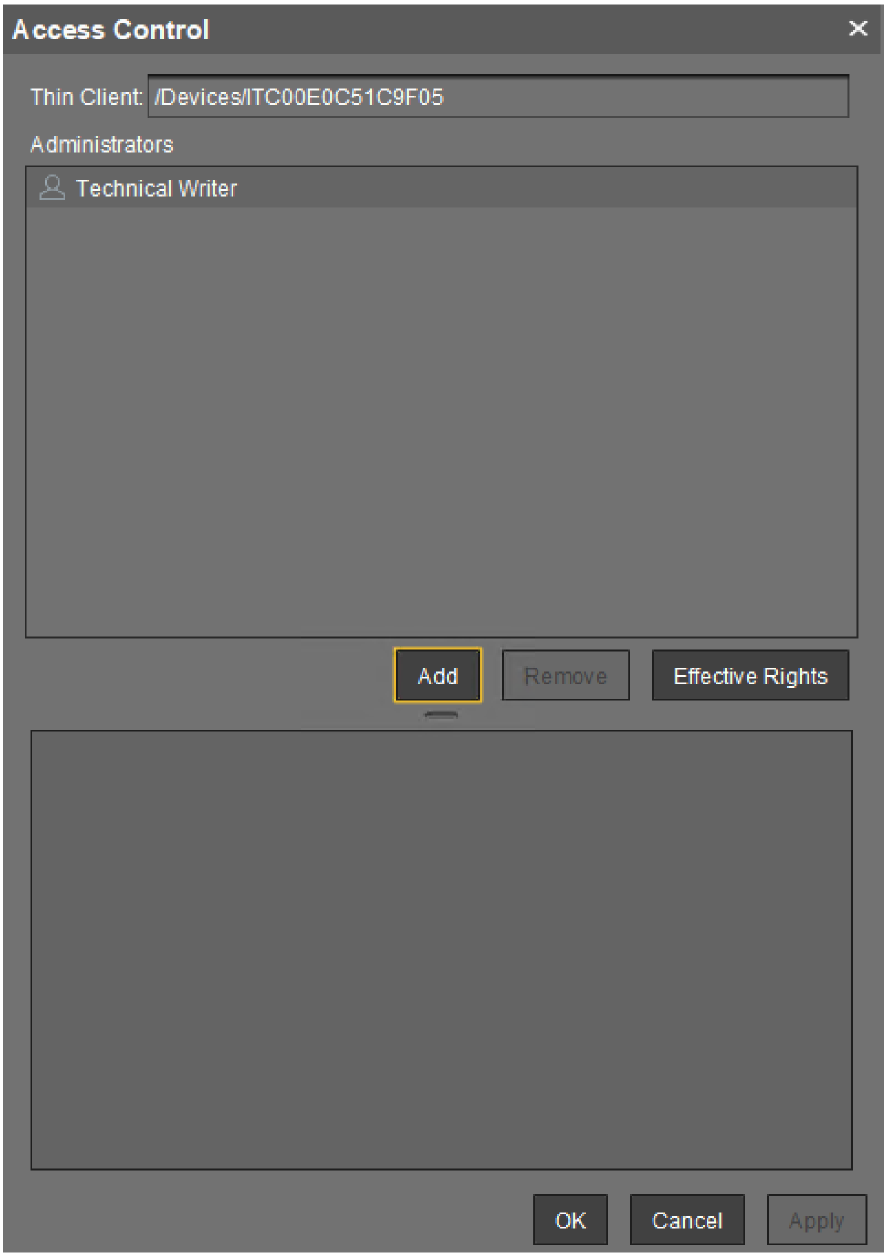
ⓘ For example, in order to be able to change the configuration of a thin client, a user requires authorization to browse the thin client's directory path and configure the thin client itself.

To assign these rights, proceed as follows:

1. In the structure tree of the UMS console choose the **Devices** node or a subgroup of devices or a single client.
2. Click **Access Control** in the context menu of your selection.



3. The **Access Control** window opens.

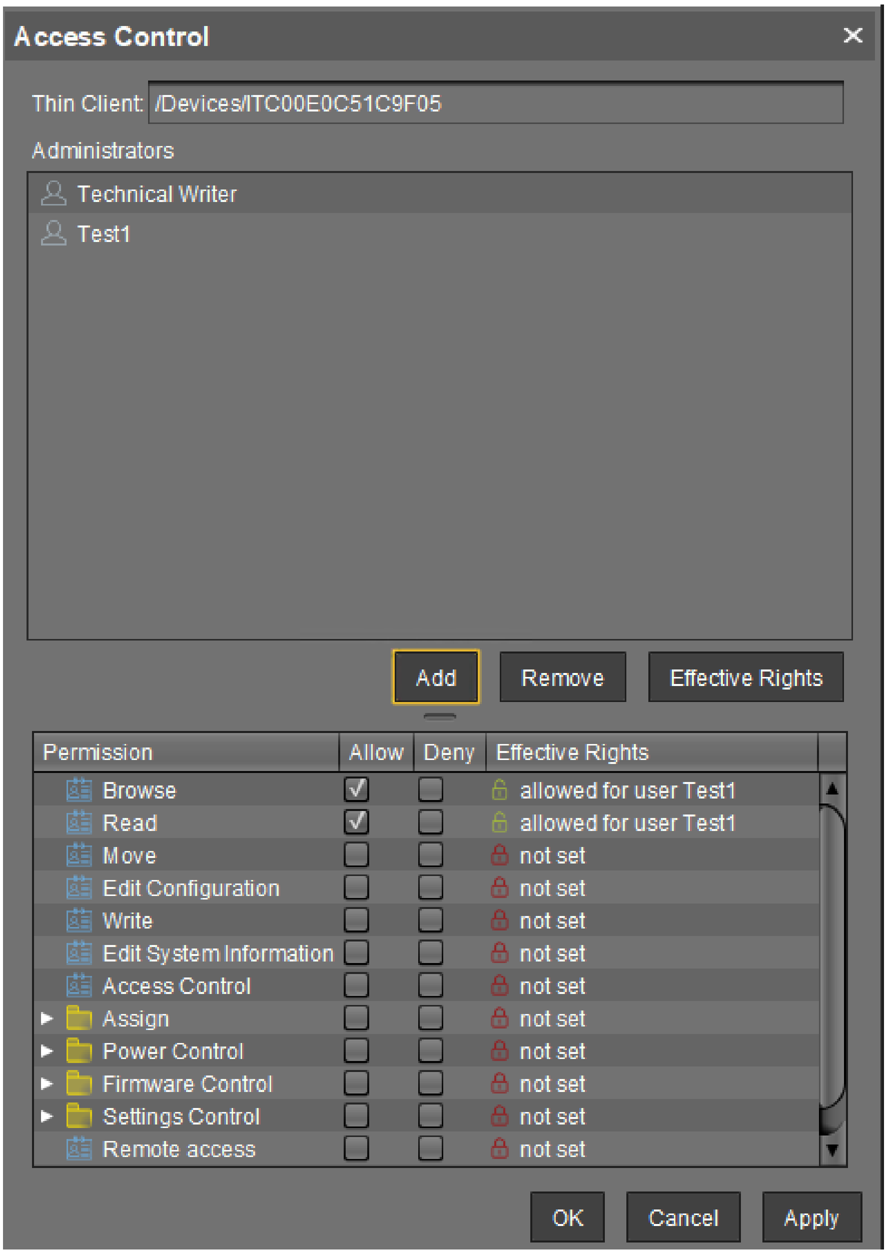


Thin Client: /Devices/ITC00E0C51C9F05

Administrators

Technical Writer

4. Click **Add** to select your new user/group.
5. The corresponding **Effective Rights** will be listed in the lower part of the mask.



Access Control

Thin Client: /Devices/ITC00E0C51C9F05

Administrators

- Technical Writer
- Test1

Permission	Allow	Deny	Effective Rights
Browse	☑	□	allowed for user Test1
Read	☑	□	allowed for user Test1
Move	□	□	not set
Edit Configuration	□	□	not set
Write	□	□	not set
Edit System Information	□	□	not set
Access Control	□	□	not set
▶ Assign	□	□	not set
▶ Power Control	□	□	not set
▶ Firmware Control	□	□	not set
▶ Settings Control	□	□	not set
Remote access	□	□	not set

6. **Allow** or **Deny** the rights of the selected group or user for access to the selected devices
7. Confirm the settings with **OK**.

8. Click the **Refresh** button of the console to apply the changes in the UMS.

> ⓘ If you have changed the rights of registered users they only take effect after a refresh.

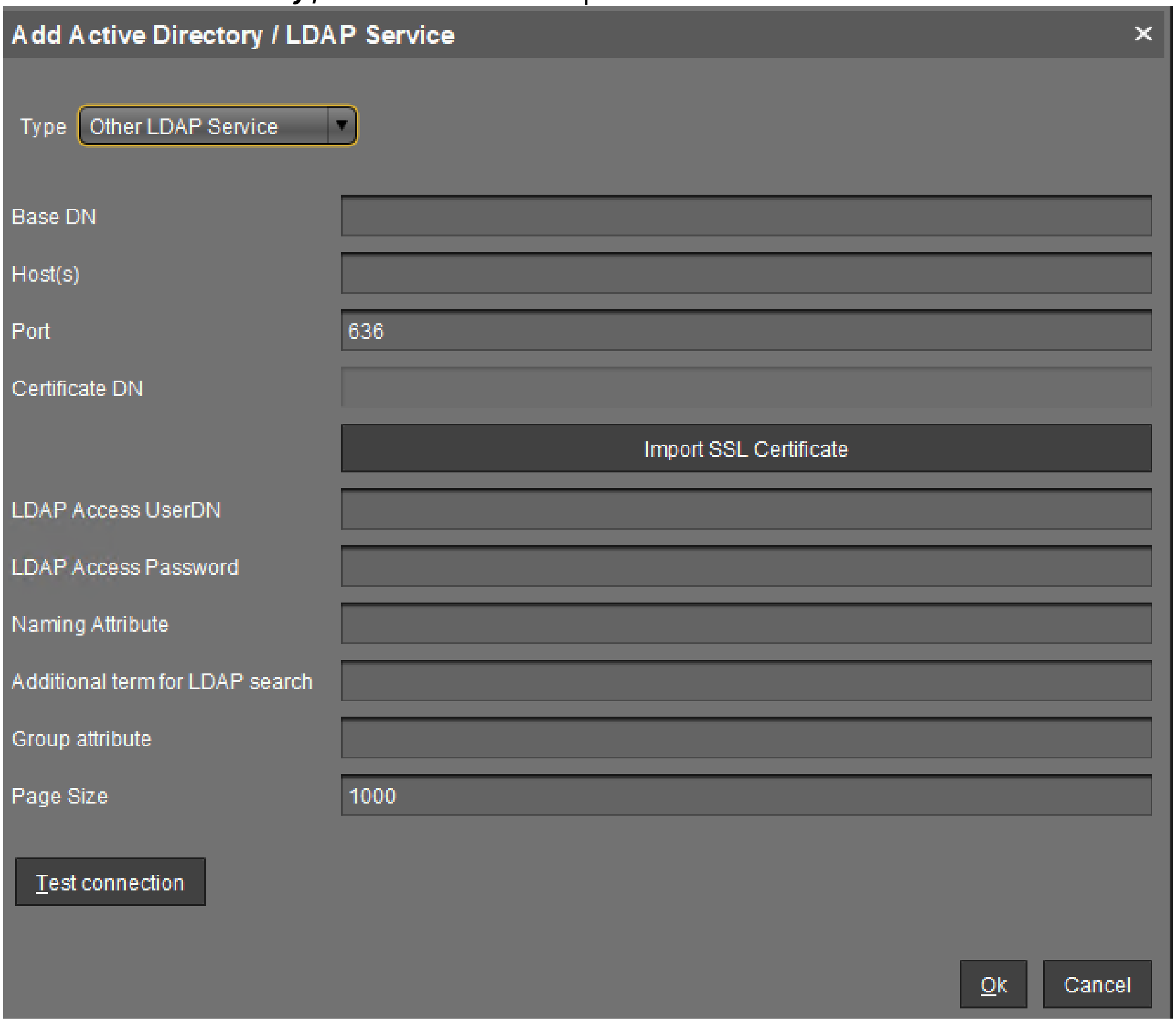
For further details about authorization rules see our How-To IGEL UMS: User Authorization Rules (see page 147).

ⓘ Access rights to objects or actions within the IGEL UMS are attached to the administrator accounts and groups. The rights of the database user account cannot be restricted. They are created during installation or when setting up the data source. The account always has full access rights in the UMS.

Configuring an LDAP Connection

As a variant you may connect other LDAP directory services, i.e. Novell eDirectory and OpenLDAP, to the UMS:

1. Click **Active Directory / LDAP** in the **UMS Administration** area of the UMS console.
2. Click **Add (+)** in the **Active Directory / LDAP Domains** mask.
3. The **Add Active Directory / LDAP Service** mask opens.



Add Active Directory / LDAP Service

Type: Other LDAP Service

Base DN:

Host(s):

Port: 636

Certificate DN:

LDAP Access UserDN:

LDAP Access Password:

Naming Attribute:

Additional term for LDAP search:

Group attribute:

Page Size: 1000

4. Select **Other LDAP Service** as **Type**.
5. Enter the **Base DN** and the **LDAP Access UserDN** in accordance with the LDAP Data Interchange Format.
6. Enter the IP of your device in the **Host(s)** field; for more devices, use a comma separated list.
7. The default **Port** for LDAP over SSL is 636.

> ⓘ For security reason UMS supports secure LDAP connections only.

8. Under **LDAP Acess UserDN/Password** enter the credentials of the LDAP Service access. The user needs to have read rights on the whole directory service, because it will be used for the determination of the structure in the directory service.
9. Under **Naming Attribute** enter the name of the LDAP attributes, which contains the distinct user account name.
10. Optionally, you can add an **Additional term for LDAP search**, which will be attached to the search for users. This way, performance can be optimized.
11. As **Group attribute** enter the name of the LDAP attribute, which contains the group membership of a user.
12. Define the **Page Size**. This property sets the maximum number of items in each page of results that will be returned by a search. It affects query performance, but NOT the number of overall results. The standard value is 1000. Change this value in line with your server configuration.
13. Click **Import SSL Certificate** to verify the **Certificate DN**.

Problems When Configuring an Active Directory with LDAP over SSL

Symptom

You cannot configure an AD Connection under **Active Directory / LDAP** with the option **Use LDAPS connection** activated. When testing the connection, one of the following types of error messages appears:

- "`The connection to the LDAP service failed! Check the certificate and server name`";
- "`simple bind failed`".
  The log file looks like:
- "`2019-05-23 14:13:38,512 ERROR [https-jsse-nio-8443-exec-151] dec: simple bind failed: QA-DC01:636 javax.naming.CommunicationException: simple bind failed: QA-DC01:636 [Root exception is javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: No subject alternative DNS name matching QA-DC01 found.]`"
  or
- "`javax.naming.CommunicationException: simple bind failed: dc01.your.domain:636 [Root exception is javax.net.ssl.SSLHandshakeException: PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to requested target]`"

Problem

The **Domain Controller(s)** name and the certificate configured under **Import SSL Certificate** do not match.

Solution

1. Check that a *fully qualified name of the domain controller* has been entered, e.g. "dc01.your.domain". An IP address or a short name such as "dc01" will not be accepted when the domain controller name is checked against the certificate.
2. If several domain controllers are used, make sure that the *root certificate* has been configured.

Import of Administrator Accounts from Active Directory Fails

Symptom

The import of UMS administrators from an Active Directory fails, the result list of imported accounts is either empty or some accounts are missing on the list.

Problem

Active Directory user accounts may have an empty User Principal Name (UPN). This occurs when updating an older Active Directory (e.g. on Windows NT 4.0) to a new one migrating the AD user accounts to the new AD.

Solution

1. Set the UPN of each AD account to be imported.
2. Retry the import of AD users in IGEL UMS.

Profiles

Find Out a Profile's Priority in the IGEL UMS

Using profiles is a very powerful method to manage and configure one, ten, or thousands of endpoint devices with the IGEL Universal Management Suite (UMS). However, when you are deploying a great number of profiles, things can get confusing. Some profiles may have overlapping scopes and thus try to set different values for one specific parameter on a device. One profile will always win, but which one is it? Luckily, the UMS can show the order of priorities at a glance.

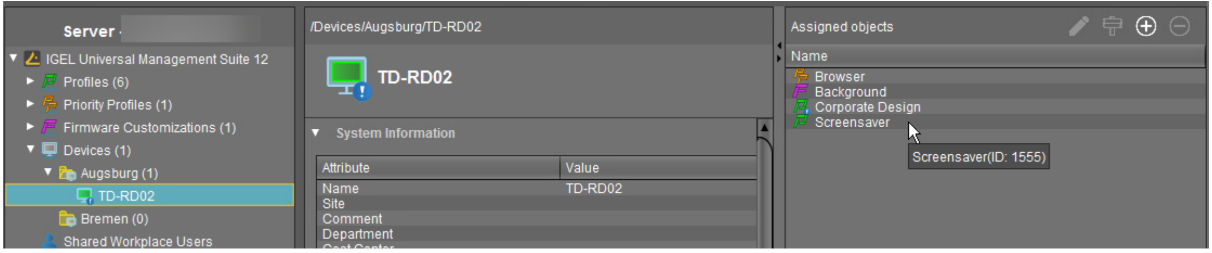
For a comprehensive reference of profiles, see Profiles in the IGEL UMS; the prioritization is covered in Prioritization of Profiles in the IGEL UMS.

The following example shows how to find out a profile's priority:

1. In the **UMS Console > Devices**, select the device for which you want to see the order of profile priorities.

2. Take a look at the **Assigned objects** area. All profiles that are assigned to the device are listed by priority, in descending order. The profile with the highest priority is listed first, and so on.

   In the following screenshot, the profile with the highest priority is a so-called priority profile. It is followed by a firmware customization, which has in turn higher priority than a standard profile, see Firmware Customizations in the IGEL UMS. And at the bottom, the object with the lowest priority is displayed – a standard profile with the lower profile ID.



/Devices/Augsburg/TD-RD02

TD-RD02

System Information

Attribute	Value
Name	TD-RD02
Site	
Comment	
Department	

Assigned objects

Name
Browser
Background
Corporate Design
Screensaver

Screensaver(ID: 1555)

Precedence of IGEL UMS Profiles and Universal Firmware Updates

This article explains which firmware update settings will be effective when several concurring settings are assigned to your IGEL OS devices. Firmware update settings can be defined locally on the device, by one or more profiles, or by one or more Universal Firmware Update.

General Order of Priority

Generally, the order of priority is as follows, from highest to lowest priority:

- Universal Firmware Update
- Profile
- Local settings

For details, see the following sections.

Universal Firmware Update vs. Profile

If both a Universal Firmware Update and a profile that contains update settings are assigned to your device, the Universal Firmware Update has priority over the profile. This is also valid if the profile is a so-called priority profile; for further information, see Prioritization of Profiles in the IGEL UMS.

The following settings under **System > Update > Firmware Update** are overwritten by the Universal Firmware Update:

- **Protocol**
- **Server name**
- **Port**
- **Server path**
- **User**
- **Password**

Profile vs. Local Settings

The settings of a profile always overwrite the local settings.

Universal Firmware Update vs. Universal Firmware Update

If several Universal Firmware Updates are assigned to one device, the rules described below apply.

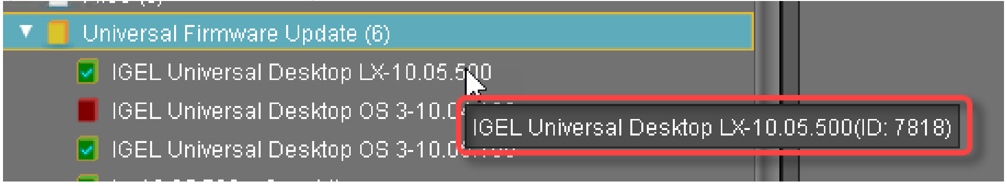
Assignment to Different Levels in a Hierarchical Order of Folders

If several Universal Firmware Updates are assigned to a device via different folders and subfolders, the one that is closest to the device has priority over all others.
Example: A Universal Firmware Update for IGEL OS 10.05.100 is assigned to a folder named "devices", which contains our device. Another Universal Firmware Update which contains IGEL 10.06.100 is assigned to a folder named "teamA". The folder "teamA", on this part, contains the folder "devices". As a result, the devices will be

updated to IGEL OS 10.05.100 (or keep IGEL OS 10.05.100) because the Universal Firmware Update for IGEL OS 10.05.100 is closer to the device in the folder hierarchy.

Assignment on the Same Level

If several Universal Firmware Updates are assigned to a device on the same hierarchical level, the one with the highest ID has priority over the others.
To find the ID of a Universal Firmware Update, move the mouse pointer over the Universal Firmware Update in question and read the tooltip:


Universal Firmware Update (6)
IGEL Universal Desktop LX-10.05.500
IGEL Universal Desktop OS 3-10.0
IGEL Universal Desktop OS 3-10.0
IGEL Universal Desktop LX-10.05.500(ID: 7818)

In this example, the ID is 7818.

Compatibility

Only those Universal Firmware Updates are effective which are compatible with the device.

Assigning Profiles to Devices filtered by Views or Search

Valid for UMS version 5.02.100 and higher.

If you need to assign a profile to a group of devices which meet a certain criterion, you can proceed in the following way:

1. Define a view which filters the clients with a certain criterion (e. g. all devices which contain a USB storage hotplug).
2. Right-click the view to open the context menu.
3. Click **Assign profiles to the thin clients of the view**.
   The **Assign profiles** window opens.
4. Select the relevant profile (e. g. the profile which allows USB storage hotplug).
5. Click > to move it from the left to the right column.
6. Confirm the setting with **OK**.

In the same way you can assign profiles to devices of a search result:

1. Right-click the search result to open the context menu.
2. Click **Assign profiles to the thin clients of the search**.
   The **Assign profiles** window opens.
3. Select the relevant profiles and click > to move them from the left to the right column.
4. Confirm the setting with **OK**.

▶ To cancel the profile assignment, click **Detach profiles from the device of the view** or **search**.

ⓘ You can also assign profiles to views or search results automatically and regularly as an administrative task.

Troubleshooting: Profile Settings Not Applied

Problem

When an IGEL Universal Management Suite (UMS) profile is applied to a OS 11 or OS 12 device, some settings from the profile are not applied correctly to the device.

Solution

Adding an automatic reboot to the UMS profile ensures the correct application of the settings from the profile to the device.

To trigger the automatic reboot when the profile is applied to the device:

1. In the UMS profile go to **System > Firmware Customization > Custom Commands > Desktop**. For more on custom commands, see Eigene Befehle and Custom Commands.
2. Add the following as a **Final desktop command**:

```
if [ ! -f /wfs/.one_more_reboot_done ] ; then touch /wfs/.one_more_reboot_done ; systemctl reboot ; fi
```

3. Save the profile.

Misc

Where Can I Find the IGEL UMS Log Files?

The following article details where you can find and configure IGEL Universal Management Suite (UMS) log files.

For enabling the logging of UMS user actions and actions initiated by a device, see Logging.

If you manage IGEL OS 12 devices, see Debugging / How to Collect and Send Device Log Files to IGEL Support.

If you require UMS log files for IGEL Support, see Save Support Information / Send Log Files to Support.

UMS 12.01 or Higher

To change the logging settings for UMS 12.01 or higher, see the file `README.md` under `[IGEL installation directory]/RemoteManager/rmguiserver/logs`.

If you change the logging configuration, the restart of the UMS Server is not required.

UMS Server

`rmguiserver/logs` (Read `rmguiserver/logs/README.md` for configuring the logs)	
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`ums-api.log`	Logging of the API service
`ums-server.log` (= `catalina.log` before UMS 12) `ums-server-err.log`	Central log file for all logging events
`device-connector.log` `device-connector-err.log`	Logging of the device connector
`ums-device-service.log` `ums-device-service-err.log`	Logging of OS 12 device functionality

`ums-appproxy.log` `ums-appproxy-err.log`	Logging of the UMS as an Update Proxy
`rmguiserver/logs/ ums-server` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging (High Availability and Distributed UMS)
`ums-server-communication.log`	Logging of communication with UMS Console or devices Edit at `<!-- Logging of UMS communication -->`
`ums-server-threaddump.log`	Periodic logging of the threads
`ums-server-icg-communication.log`	Logging of communication with ICG Edit at `<!-- Logging of UMS communication -->`
`ums-server-health.log`	Logging of the UMS HA Health Check
`ums-server-monitoring.log`	Performance logging Edit at `<!-- Logging of monitoring data -->` ; change INFO to DEBUG to get detailed information on each method call

Example of where to edit the logging configuration for the UMS Server

This is an example of `rmguiserver/conf/logback.xml` where you can configure the logs for the UMS Server, i.e. switch the logging on/off, change the scan period or the number of days for the logging history, etc.:

```
<?xml version="1.0" encoding="UTF-8"?>

-<configuration scanPeriod="60 seconds" scan="true" debug="false">


<!-- The length of logging history in days -->

<property value="30" name="logs.history"/>


<!-- The maximum size of one log file -->
```

```
<property value="100MB" name="logs.maxsize"/>

<!-- The maximum size of the history -->
<property value="1GB" name="logs.historysizecap"/>

<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property value="INFO" name="monitoring.level"/>

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property value="OFF" name="server2console.level"/>
<property value="OFF" name="server2tc.level"/>
<property value="OFF" name="server2usg.level"/>
<property value="OFF" name="usg2server.level"/>
<property value="OFF" name="server2server.level"/>

<!-- Logging level of domain service -->
<!-- OFF, INFO, DEBUG, ERROR -->
<property value="WARN" name="domainservicelog.level"/>
<!-- The appenders -->
```

```
rmguiserver/logs/unifiedprotocol
```

`communication.log`	Logging of communication between the device and UMS (both ingoing and outgoing commands) Edit `rmguiserver/webapps/device-connector/WEB-INF/classes/config/logback.xml` for configuring the logs. Edit at `<!-- Logging of device communication -->`; change `OFF` to `INFO` for logging command headers or to `ALL` for logging command headers and payload
`domain-service.log`	Central log file for all events in the command handling Edit `rmguiserver/conf/logback.xml` for configuring the logs. Edit at `<!-- Logging level of domain service -->`
`device-auth.log`	Logging of device onboarding and device authentication issues

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - for configuring the logs)	
`ums-broker.log`	Central log file for all logging events
`ums-broker-msg.log`	Logging of the messages exchanged
`ums-broker-health.log`	Logging of the UMS HA Health Check
`ums-broker-monitoring.log`	Performance logging Edit at `<!-- Logging of monitoring data -->`; change `INFO` to `DEBUG` to get detailed information on each method call

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - for configuring the logs)	
`ums-watchdog.log`	Central log file for all logging events
`ums-watchdog-msg.log`	Logging of the messages exchanged
`ums-watchdog-health.log`	Logging of the UMS HA Health Check

UMS Console

`$HOME/.igel`	
`RMClient.exe.log`	Startup logging
`$HOME/.igel/logs` (`rmclient/logback.xml` - for configuring the logs)	
`ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging
`rmguiserver/logs` (`rmadmin/logback.xml` - for configuring the logs)	
`ums-admin.log`	Central log file for all logging events

UMS 6.10.110 or Higher

In UMS version 6.10.110, the outdated logging framework Log4j 1.x was replaced with Logback[10]; see also ISN 2022-19: Log4j 1.x Remainder in UMS.

To change the logging settings for UMS 6.10.110 or higher, use `logback.xml` .

[10] https://logback.qos.ch/

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`catalina.log`	Central log file for all logging events
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging
`ums-server-communication.log`	Logging of communication with UMS Console or devices Edit at `<!-- Logging of UMS communication -->`
`localhost.log`	Technical logging of the Apache Tomcat server
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`ums-server-threaddump.log`	Periodic logging of the threads
`ums-server-icg-communication.log`	Logging of communication with ICG Edit at `<!-- Logging of UMS communication -->`
`ums-server-health.log`	Logging of the UMS HA Health Check
`ums-server-monitoring.log`	Performance logging Edit at `<!-- Logging of monitoring data -->` ; change INFO to DEBUG to get detailed information on each method call (the server restart is then required)

Example of where to edit the logging configuration for the UMS Server

This is an example of `rmguiserver/conf/logback.xml` where you can configure the logs for the UMS Server, i.e. switch the logging on/off, change the scan period or the number of days for the logging history, etc.:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration debug="false" scan="true" scanPeriod="60 seconds">
```

```
<!-- General settings -->

<!-- Logging of monitoring data -->
<!-- Elevate to 'DEBUG' to see the individual calls -->
<property name="monitoring.level" value="INFO" />

<!-- Logging of UMS communication -->
<!-- Set to 'ALL' to enable and 'OFF' to disable -->
<property name="server2console.level" value="OFF" />
<property name="server2tc.level" value="OFF" />
<property name="server2usg.level" value="OFF" />
<property name="usg2server.level" value="OFF" />

<!-- The base folder for log files -->
<property name="base.dir" value="${catalina.home}/logs" />

<!-- The default logging pattern -->
<property name="pattern.format" value="%-5(%d{[yyyy-MM-dd HH:mm:ss.SSS]})
%-5level [%thread] %logger{10}.%M - %msg%n" />

<!-- The length of logging history in days -->
<property name="logs.history" value="30" />

<!-- The appenders -->
```

`rmguiserver/logs` (`rmguiserver/conf/logback.xml` - for configuring the logs)	
`ums-api.log`	Logging of the API service

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/logback.xml` - for configuring the logs)	
`ums-broker.log`	Central log file for all logging events

`ums-broker-msg.log`	Logging of the messages exchanged
`ums-broker-health.log`	Logging of the UMS HA Health Check
`ums-broker-monitoring.log`	Performance logging Edit at `<!-- Logging of monitoring data -->` ; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/logback.xml` - for configuring the logs)	
`ums-watchdog.log`	Central log file for all logging events
`ums-watchdog-msg.log`	Logging of the messages exchanged
`ums-watchdog-health.log`	Logging of the UMS HA Health Check

UMS Console

`$HOME/.igel`	
`RMClient.exe.log`	Startup logging

`$HOME/.igel/logs` (`rmclient/logback.xml` - for configuring the logs)	
`ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging

`rmguiserver/logs` (`rmadmin/logback.xml` - for configuring the logs)	
`ums-admin.log`	Central log file for all logging events

Before UMS 6.10.110

UMS Server

`rmguiserver/logs` (`rmguiserver/conf/log4j.properties` - for configuring the logs)	
`catalina.log`	Central log file for all logging events
`ums-server-msg.log`	Logging of the Apache ActiveMQ messaging
`communication.log`	Logging of communication with UMS Console or devices Edit at `# communication logging - define the log levels` ; refer to Log4j documentation[11]
`license_deployment.log`	Logging of licenses Edit at `# license deployment logging` ; refer to Log4j documentation[12]
`localhost.log`	Technical logging of the Apache Tomcat server
`stderr.log`	Error output of the Apache Tomcat server
`stdout.log`	Standard output of the Apache Tomcat server
`umsthreaddump.log`	Periodic logging of the threads Edit with `# threaddump logging` ; refer to Log4j documentation[13]

[11] https://logging.apache.org/log4j/2.x/manual/index.html
[12] https://logging.apache.org/log4j/2.x/manual/index.html
[13] https://logging.apache.org/log4j/2.x/manual/index.html

`usgcommunication.log`	Logging of communication with ICG Edit at `# communication logging - define the log levels`; refer to Log4j documentation[14]
`health.log`	Logging of the UMS HA Health Check
`monitoring.log`	Performance logging Edit at `# execution monitoring`; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)
`rmguiserver/logs` (`rmguiserver/conf/log4japi.properties` - for configuring the logs)	
`api.log`	Logging of the API service

UMS Load Balancer

`umsbroker/etc/work/logs` (`umsbroker/etc/conf/log4j.properties` - for configuring the logs)	
`igel-ums-broker.log`	Central log file for all logging events
`broker-msg.log`	Logging of the messages exchanged
`broker-health.log`	Logging of the UMS HA Health Check
`broker-monitoring.log`	Performance logging Edit at `# monitoring logging`; change `INFO` to `DEBUG` to get detailed information on each method call (the server restart is then required)

UMS Watchdog

`umswatchdog/etc/work/logs` (`umswatchdog/etc/conf/log4j.properties` - for configuring the logs)

[14] https://logging.apache.org/log4j/2.x/manual/index.html

`igel-ums-watchdog.log`	Central log file for all logging events
`watchdog-msg.log`	Logging of the messages exchanged
`watchdog-health.log`	Logging of the UMS HA Health Check

UMS Console

`$HOME/.igel`	
`RMClient.exe.log`	Startup logging
`$HOME/.igel/logs` (`rmclient/log4j.properties` - for configuring the logs)	
`igel-ums-console.log`	Central log file for all logging events

UMS Administrator

`$HOME/.igel`	
`RMAdmin.exe.log`	Startup logging
`rmguiserver/logs` (`rmadmin/log4j.properties` - for configuring the logs)	
`igel-ums-admin.log`	Central log file for all logging events

Clearing stdout.log and stderr.log in IGEL UMS

Here, you can find options to limit the size of the files `stdout.log` and `stderr.log` created in connection with your IGEL Universal Management Suite (UMS) Server.

Problem

Besides the log files created by the IGEL UMS Server application, two log files are created by the Windows/Linux service which starts the UMS Server process. These log files (`stdout.log` and `stderr.log`) are not controlled by the logging configuration in `logback.xml` and so do not obey the sizing limits. Upon UMS Server restart these log files are cleared but if the UMS Server runs a long time the size can grow.

Solution 1 - Restart

Restart the UMS Server once in a while. The restart clears the log files, and thus keeps the size under control.

Solution 2 - Scheduled Task

Create a scheduled operating system task to clear the log files:

- On Windows, you can use the Powershell command `Clear-Content stdout.log`
- On Linux, the corresponding command is `truncate -s 0 stdout.log`
- Scripts to run as an administrator are available in the folder `rmadmin` (`truncateStdLogs.ps1` , `truncateStdLogs.sh`).

Clearing up the UMS

Problem

You have several firmware versions in the UMS. Your collection of clients and profiles has become large and confusing. You are losing track of assignments and connections between these elements.

Goal

You want to minimize the variety of firmware and profiles to simplify processes. You just want to see what you need.

The firmware, clients, and profiles are interdependent. So, what is the best way to proceed?

Solution

> ⓘ We advise making a back-up of the UMS before deleting any components. You can also use the UMS recycle bin for the deleted objects.

The following are the main steps for reorganizing the UMS:

1. Download the new firmware.
2. Move clients to the new firmware.
3. Move profiles to the new firmware.
4. Delete old firmware, clients, and profiles that are no longer required.

Downloading the new Firmware

1. Check our download server[15] to see whether there are new updates that are relevant for your applications.
2. Download the relevant update files. Install an update directory for the files on the UMS server or on your FTP server.

Moving Clients to the New Firmware

Find out how many different firmware versions you really need.

Upgrading all clients to the same firmware:

1. Create a new **View** to search for all clients using a firmware version older than the current version. Example:
   View Name: Show all UD LX devices with old firmware
   Rule: Product name is like (!reg!)(?i).*Universal Desktop LX.* AND Firmware version is less than 5.04.100

[15] https://www.igel.com/software-downloads/

2. Assign the update directory to these devices.
3. Start the update process.

Moving Profiles to New Firmware

Examine your profiles and decide which of them are relevant for the new firmware. You have three possibilities you can do now:

- Adjust the firmware version the profiles are based on, to be sure that they will work with the new firmware.
- Leave the profile settings as they are.
  If the parameters of the new firmware match the parameters of the old version, a profile will work anyway. If they do not match, these parameters will be ignored.
- Create new profiles.

For more information see UMS Manual: Creating Profiles.

Deleting old Firmware, Clients and Profiles that are no longer required

To finally clear up the UMS you now should delete obsolete objects.

- Use again Views to select the clients, which are no longer required.
  For more Information see UMS Manual: How to Create a New View in the IGEL UMS.
- Select the obsolete profiles. You can do this manually or by using the search option: **Misc > Search > Profiles > Product&Firmware**.
- Delete old firmware which is not assigned any longer to a client or profile: **Misc > Remove Unused Fimwares**.

Do you have also obsolete **Views**, **Jobs**, **Template Keys**? Delete them as well.

For **Template Keys** the **Profile Relation** is shown in the setting mask.

How to Remove a UMS Certificate from an OS 11 Device

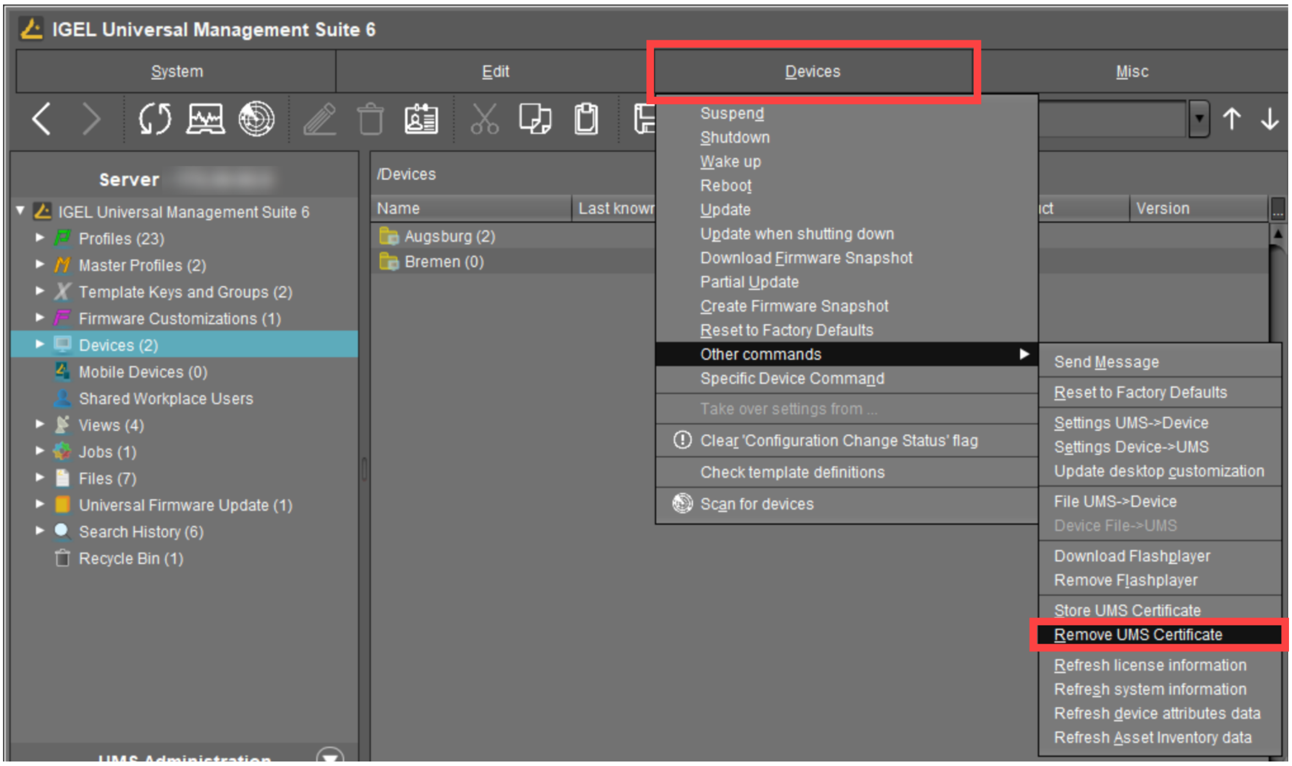
The IGEL Universal Management Suite (UMS) allows you to remove the UMS Server certificate from OS 11 devices.

The removal of the certificate from devices may be necessary

- in order to prepare for moving a device from the test environment to the productive environment
- in order to prepare for replacing the server certificate

To remove the certificate, proceed as follows:

▶ Under **Devices > Other commands**, select **Remove UMS Certificate**.
Each IGEL UMS Server can now access the device configuration until one of the servers registers the device.



Related Topics

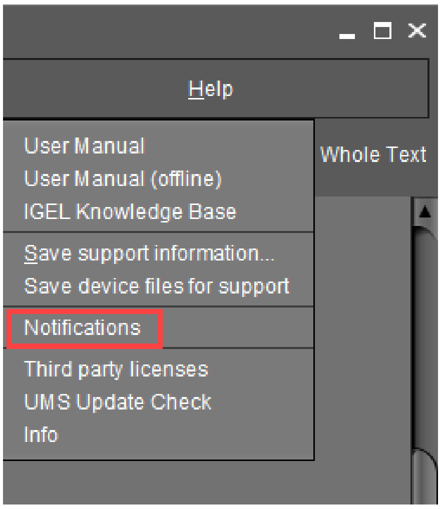
If you face problems during the device registration because of certificate issues: Troubleshooting: Registration of a Device via Scanning for Devices Fails (see page 258)

How to Configure Notifications in the IGEL UMS

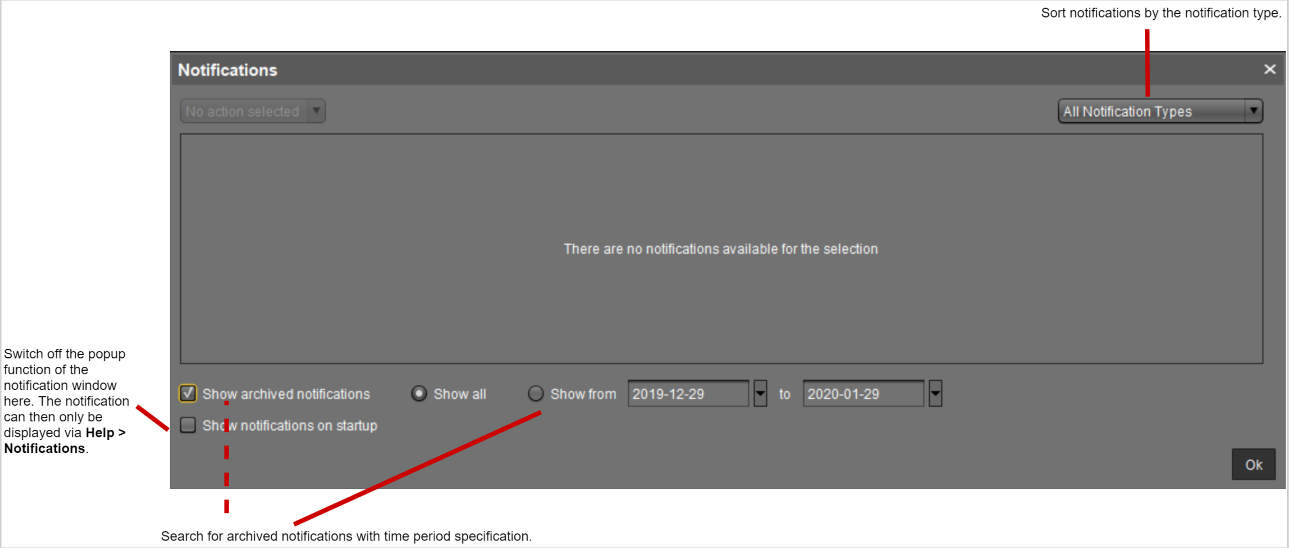
In the IGEL Universal Management Suite (UMS), you can get notifications about newly available firmware updates, device licenses, etc. By default, notifications are enabled and pop up when you start the UMS Console. In this article, you will learn how to adapt this feature to your needs.

About Notifications

Basically, all users with read permission can see the notifications. The notifications are displayed after starting the UMS Console. When the dialog is closed, the notifications can still be viewed anytime under **Help > Notifications**.



The Notification Window



There are no notifications available for the selection

Sort notifications by the notification type.

Switch off the popup function of the notification window here. The notification can then only be displayed via **Help > Notifications**.

Search for archived notifications with time period specification.

Enabling the Notification Function

1. In the UMS Console, go to **UMS Administration > Global Configuration > Misc Settings**.
2. Activate **Enable notifications**.

The notification feature is active. The notifications can be viewed under **Help > Notifications**.

Exporting Notifications and Sending Them by Email

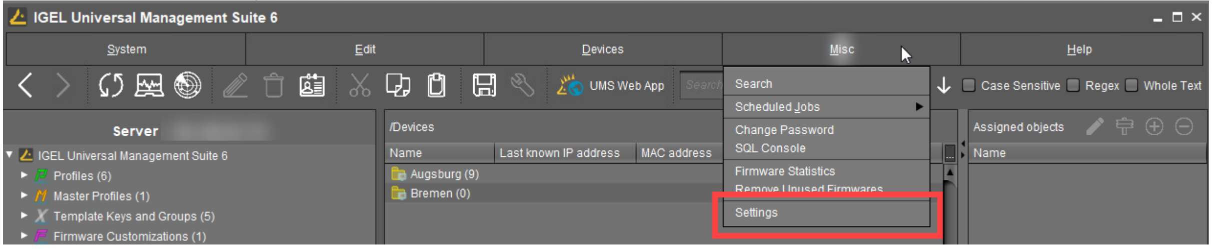
Notifications can be exported and sent via email: **UMS Administration > Global Configuration > Administrative Tasks > add > Action: "Send notification information via email"**.

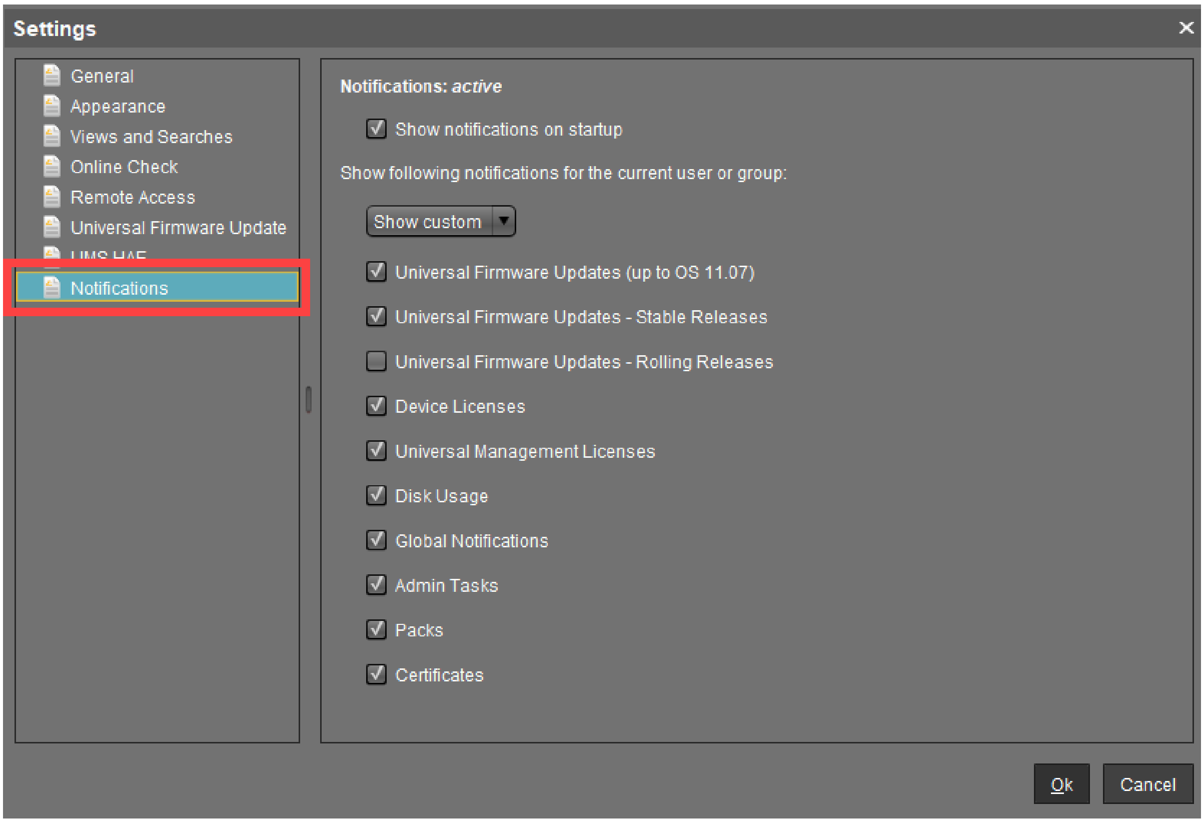
For more information, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS.

Configuring the Notification Pop-Up and Notification Types

To configure and customize the notification pop-up:

1. In the UMS Console, go to **Misc > Settings > Notifications**.





Settings

- General
- Appearance
- Views and Searches
- Online Check
- Remote Access
- Universal Firmware Update
- UMS HAE
- Notifications

Notifications: *active*

☑ Show notifications on startup

Show following notifications for the current user or group:

Show custom ▾

☑ Universal Firmware Updates (up to OS 11.07)

☑ Universal Firmware Updates - Stable Releases

□ Universal Firmware Updates - Rolling Releases

☑ Device Licenses

☑ Universal Management Licenses

☑ Disk Usage

☑ Global Notifications

☑ Admin Tasks

☑ Packs

☑ Certificates

2. Enable **Show notifications on startup** to display the notification window as a pop-up every time the UMS Console is started.

3. Under **Show following notification for the current user or group**, select **Show custom**.

4. Specify which content should be displayed in the notification.
   Possible options (as of UMS 6.10.110):
   - **Universal Firmware Updates (up to 11.07)**: Informs about the latest firmware updates for devices with IGEL OS versions before 11.07.

     > To view notifications generated by UMS version below 6.10.110, leave the feature **Universal Firmware Updates (up to 11.07)** activated.

   - **Universal Firmware Updates - Stable Releases**: Informs about the latest Stable Releases. The feature is officially supported for devices with IGEL OS version 11.07 or higher.
   - **Universal Firmware Updates - Rolling Releases**: Informs about the latest Rolling Releases. The feature is officially supported for devices with IGEL OS version 11.07 or higher.

     > Activate this feature to get the latest client versions and bug fixes.

   - **Device Licenses**: Informs about the expiration of device licenses.

- **Universal Management Licenses**: Informs about the expiration of UMS licenses and if the available license amount is exceeded.
- **Disk Usage**: Informs about a critical value of free disc space. For more details, see "Disk Usage" below.
- **Global Notifications**: Informs about important news like maintenance times and bug fixes. For more details, see "Global Notifications" below.
- **Admin Tasks**: Automatically informs in a set of cases if no administrative task has been defined. For more details, see "Admin Tasks" below.
- **Packs**: Informs if license packs will expire.
- **Certificates**: Informs if certificates will expire.

5. Confirm the settings with **Ok**.

Disk Usage

This notification informs the user when there is not enough free drive space anymore. The individual critical drive space value can be set under **UMS Administration > Global Configuration > Misc Settings > Notifications**.

> Each server executes an administrative task every 6 hours to check the available space on the drive and deliver the disk usage information to the notification system. In order to display the notification, the server must have been running continuously for up to 6 hours.
> Disk usage admin tasks executions older than 24 hours are considered out-of-date: An additional warning message is shown.

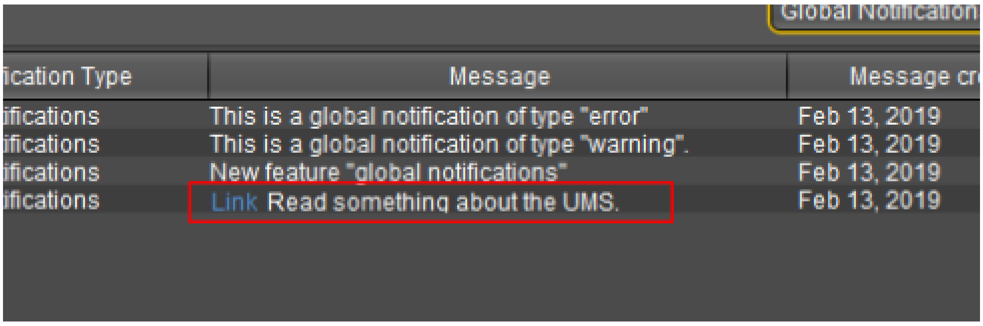
Types of disk usage notifications:

- Specific notification for each connected server: The server hostname and the available drive space will be shown in the notification message.
- Installation path and database path are on different file systems: Two notifications for each file system will be shown.

Global Notifications

This notification type informs the user about important news like maintenance times and bug fixes.

Global Notifications can include an additional web link that can provide more information. The web link is displayed as a blue link button next to the global notification.



ication Type	Message	Message cr
ifications	This is a global notification of type "error"	Feb 13, 2019
ifications	This is a global notification of type "warning".	Feb 13, 2019
ifications	New feature "global notifications"	Feb 13, 2019
ifications	Link Read something about the UMS.	Feb 13, 2019

▶ Click the link to open the web page in the standard browser.

▶ Move the mouse over the link to display the URL.

Admin Tasks

Notifications of this type are displayed in the following cases:

- When an embedded database is active, but NO administrative task for **creating a database backup** has been set.
- When logging is enabled, but NO administrative task for **deleting logging data** has been set.
- When at least one job is available, but NO administrative task for **deleting job execution data** has been set.

For detailed information on administrative tasks, see Administrative Tasks - Configure Scheduled Actions for the IGEL UMS.

Updating Timezone Information (Daylight Saving Time, DST)

Symptom

The device is showing an incorrect time of day for your location, although you have set the correct time zone.

Problem

The time zone or the regulation for Daylight Saving Time (DST) for your location has changed.

Solution

Update the time zone information files via IGEL Universal Management Suite (UMS). This is known to work for

- IGEL Linux version 10.01.100 or newer
- IGEL Linux version 5.04.100 or newer
- IGEL Linux version 4.14.100 or newer
- IGEL Linux ARM version 1.09.100 or newer.

Retrieving current time zone information files:

On Windows

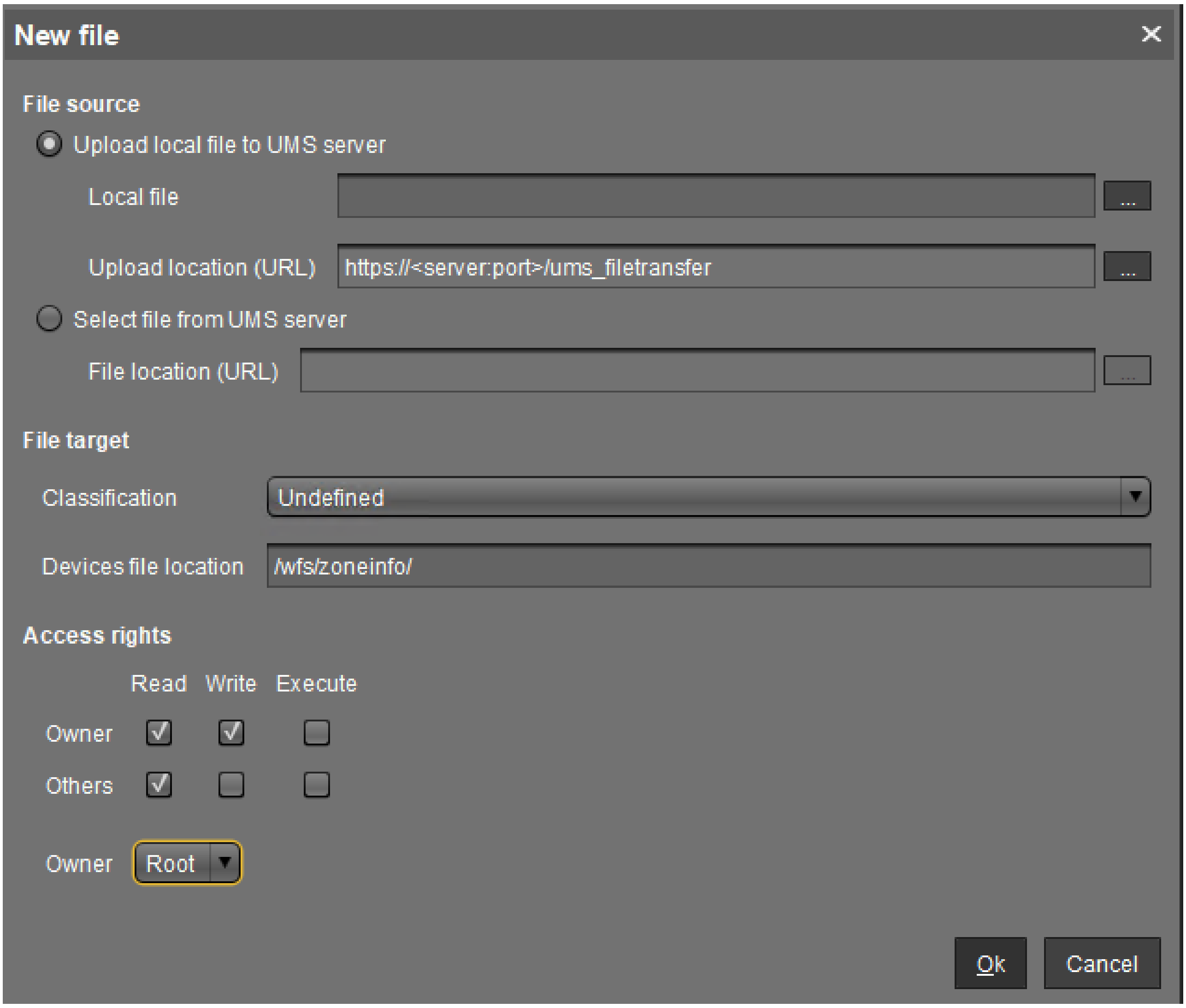
- Use your web browser to download the following package files:
  - http://packages.ubuntu.com/xenial-updates/all/tzdata/download for *IGEL Linux* version 10.x
  - http://packages.ubuntu.com/trusty-updates/all/tzdata/download (for *IGEL Linux* version 5.x)
  - http://packages.ubuntu.com/precise-updates/all/tzdata/download (for *IGEL Linux* version 4.x)
- Extract the package contents using the program 7-Zip (freely available from http://www.7-zip.org).
- Find the file for your location in the extracted directory in `usr/share/zoneinfo/`, e.g. `usr/share/zoneinfo/Africa/Casablanca` for Morocco.

On Linux

- Update your system time zone information with these commands: `sudo apt-get update` `sudo apt-get install tzdata`
- Find the file for your location in the system directory `/usr/share/zoneinfo/`, e.g. `/usr/share/zoneinfo/Africa/Casablanca` for Morocco.

Distributing the files from IGEL Universal Management Suite

- Select **System > New > New File** from the UMS Console menu bar or go to **Files** in the tree structure and select **New File** from the context menu.
- Select the time zone file for your location under **Local File**.
- Select **Undefined** under **Classification**.
- Specify `/wfs/zoneinfo/` as the **Devices file location**.
- Set the **Access rights** to Read and Write for the Owner, and to Read for Others.
- Select Root as the **Owner**.
- Click **OK** to confirm the settings.



New file

File source

● Upload local file to UMS server

Local file:

Upload location (URL): https://<server:port>/ums_filetransfer

○ Select file from UMS server

File location (URL):

File target

Classification: Undefined

Devices file location: /wfs/zoneinfo/

Access rights

	Read	Write	Execute
Owner	☑	☑	□
Others	☑	□	□

Owner: Root

On a device, you can verify the transfer and activation of the new time zone information files:

- In the **Local Terminal**, enter `grep 'timezone_config' /var/log/messages`

  > ⓘ On *IGEL Linux version 10.x*, use: `journalctl | grep 'timezone_config'`

- The output should look like the following:

```
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/Africa/Casablanca
Feb 27 11:28:13 (none) timezone_config: loading /wfs/zoneinfo/Casablanca to /usr/share/zoneinfo/posix/Africa/Casablanca
Feb 27 11:28:13 (none) timezone_config: configure timezone Africa/Casablanca
```

E-Mail Settings for Gmail Accounts

Purpose

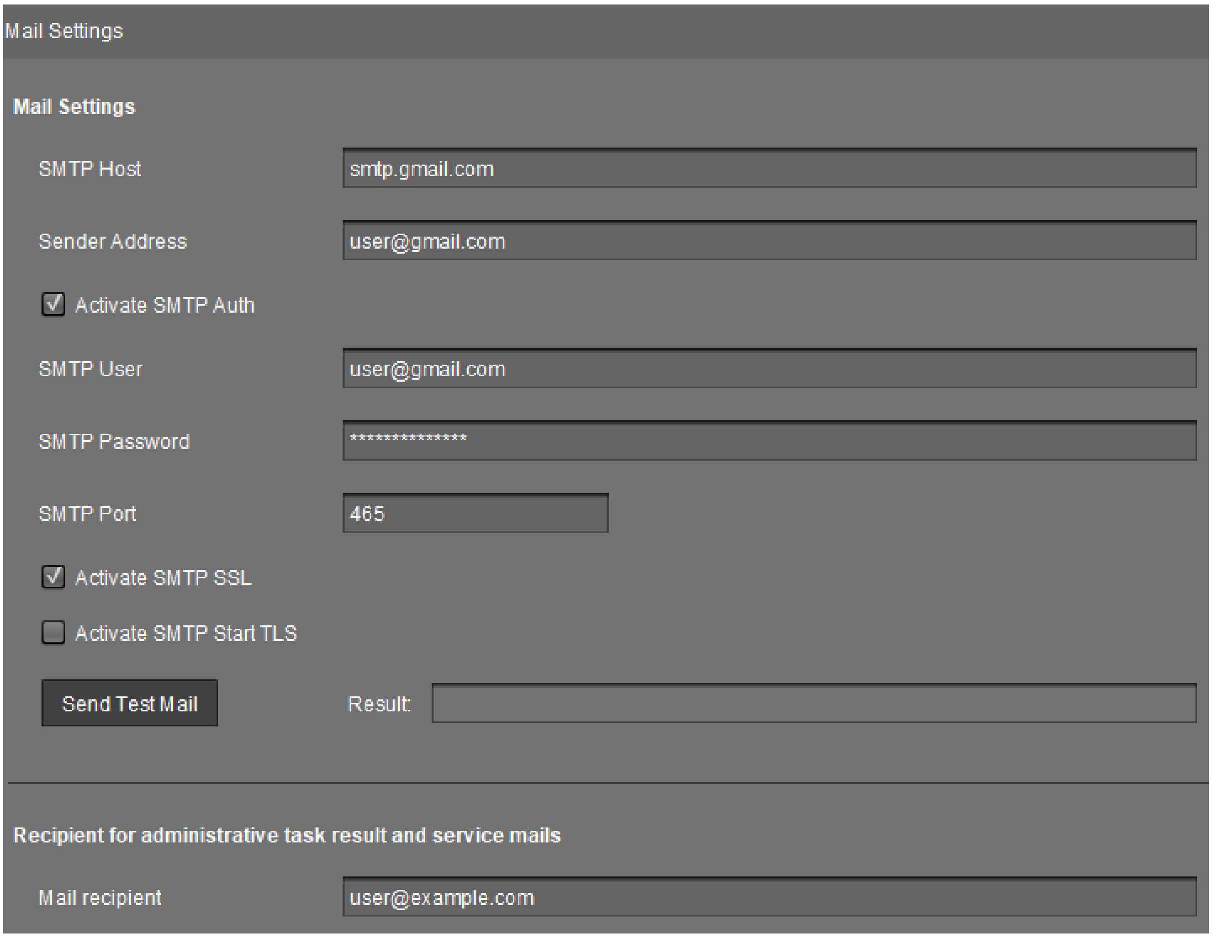
You want to send views from the IGEL Universal Management Suite by email using a Gmail account.

Solution

ⓘ In order to allow the UMS to send emails via Gmail, you have to make the following setting in your Google account:

- Log in to Google.
- Go to **My Account > Sign-in & security > Connected apps & sites**.
- Set **Allow less secure apps** to `ON` .

1. Go to **UMS Administration > Global Configuration > Mail Settings**.
2. Enter `smtp.gmail.com` as the **SMTP Host**.
3. Enter your Gmail address under **Sender Address**.
4. Enable **Activate SMTP Auth.**
5. Enter your Gmail address under **SMTP User**.
6. Enter your Gmail password under **SMTP Password**.
7. Enter `465` under **SMTP Port**.
8. Enable **Activate SMTP SSL**.
9. Under **Mail recipient**, enter the email address you want administrative emails from the UMS to be sent to.



Mail Settings

Mail Settings

SMTP Host: smtp.gmail.com

Sender Address: user@gmail.com

☑ Activate SMTP Auth

SMTP User: user@gmail.com

SMTP Password: ***************

SMTP Port: 465

☑ Activate SMTP SSL

□ Activate SMTP Start TLS

Recipient for administrative task result and service mails

Mail recipient: user@example.com

10. Click **Send Test Mail** to test your settings.

Additional Information

https://support.google.com/a/answer/176600?hl=en

Searching with Regular Expressions in the UMS

The IGEL Universal Management Suite (UMS) can help you to manage large device installations. Often you will want to search or filter for objects with certain properties, and the UMS offers a wide selection. For advanced searches, however, you might need regular expressions, a powerful feature built into the UMS.

You can use them in:

- Quick Search
- **Misc > Search**
- **Views > New View**
- **Edit > Edit Configuration > System > Registry > Search parameter ...**
- **UMS Administration > Global Configuration >Default Directory Rules**

The UMS uses Java regular expressions. These are different from the globbing patterns that you may know from the DOS/Windows Command Prompt or the Linux commandline. For example, instead of using `*` to match any number of characters, you use in the UMS:

```
.*
```

Here the `.` matches any character. The `*` acts as a quantifier, stating how often the preceding pattern may occur, in this case zero or more times.

So, if you want to find something that begins with IGEL, use:

```
IGEL.*
```

Something beginning with IGEL and ending with 12:

```
IGEL.*12
```

If you want to find something ending with IGEL:

```
*.IGEL
```

Find out more about Java regular expressions in Oracle's documentation[16].

[16] https://docs.oracle.com/javase/7/docs/api/java/util/regex/Pattern.html

Copy Sessions in Setup or UMS

Sometimes you want to create a session that differs from another only in a few details. *IGEL* Linux *version 5.10.100* or newer and UMS *version 5.02.100* or newer let you copy complete sessions. Once the session is copied, you can easily adapt the required settings.

Copying is available in the **Sessions** section of *IGEL* Setup (and occasionally in some other sections) as well as in the **Edit Configuration** function in UMS.

To copy a session, proceed as follows:

1. In the setup, open the menu path **Sessions > [Session Type] > [Session Type] Sessions**.
   Example: **Sessions > RDP > RDP Sessions**
   The existing sessions are shown.
2. Highlight the session that you want to copy.
3. Click ⧉.
   A copy of the session will be created within the same folder.

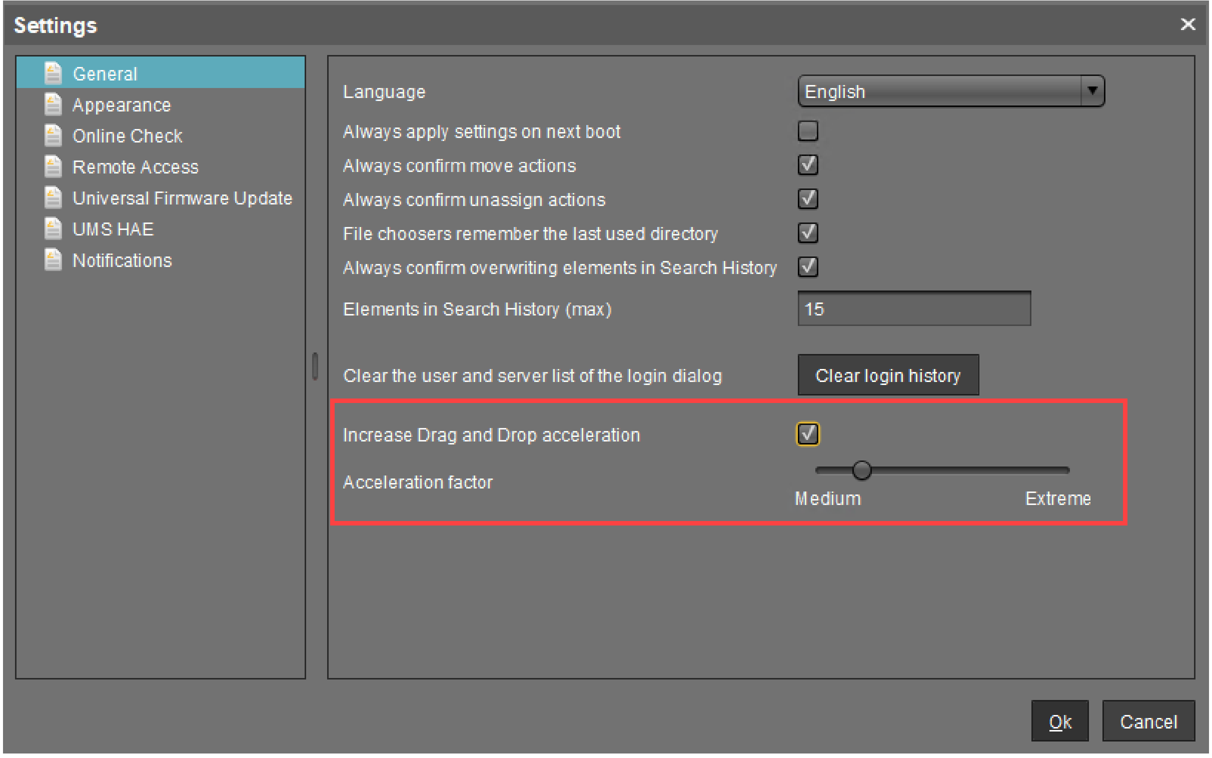
Drag & Drop Acceleration for Large Structure Trees

If you have a really large number of objects in your IGEL UMS (Universal Management Suite), it can be tedious to drag and drop an object to a new position if the new position is quite far away from the current position.

But with UMS version 5.03.100 or newer, you can increase your scrolling speed. As soon as the object you are moving touches the bottom edge of the structure tree window, the acceleration starts.

To enable drag and drop acceleration:

1. Open the UMS and go to **Misc > Settings > General**.
2. Activate **Increase Drag and Drop acceleration.**
3. Adjust the **Acceleration factor** according to your needs and click **Ok**.



Settings

- General
- Appearance
- Online Check
- Remote Access
- Universal Firmware Update
- UMS HAE
- Notifications

Language: English
Always apply settings on next boot □
Always confirm move actions ☑
Always confirm unassign actions ☑
File choosers remember the last used directory ☑
Always confirm overwriting elements in Search History ☑
Elements in Search History (max): 15
Clear the user and server list of the login dialog: Clear login history
Increase Drag and Drop acceleration ☑
Acceleration factor: Medium — Extreme

Drag & drop acceleration is ready.

Which UMS Directories Should Be Scanned for Viruses, Which Can Be Excluded?

Question

Which UMS directories can be excluded from antivirus scanning, which directories should be scanned?

Environment

This article is valid for the following environment:

- UMS 5.08 or higher
- UMS is installed on Microsoft Windows server

Answer

Everything in `C:\<Program Files>\IGEL\RemoteManager\` can be excluded.

If your UMS also manages Windows devices, the downloadable files in `C:\<Program Files>\IGEL\RemoteManager\rmguiserver\webapps\ums_filetransfer\` should be scanned.

Licensing with Smartcard fails

Symptom

You can not create licenses from smartcard in IGEL UMS (**License Management**) although valid licenses are stored on the SIM / smartcard and the smartcard reader's driver is installed to your system.

▶ The smardcard reader shows a problem in the Windows Hardware Manager [**!**].

Problem

Another smartcard reader (eg. built-in cardreader) overrides the access.

Solution

Deactivate or deinstall all other smartcard readers in the Windows Hardware Manager.