



## Installation and Sizing Guidelines for IGEL UMS

The following installation and sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite (UMS) environment – UMS Server, UMS Console & UMS Web App, database, and, if required, load balancer and ICG instances. For information on the installation requirements, see Installation Requirements for the IGEL UMS.


The size and structure of the UMS setup depend mainly on the following criteria:

- Number of devices
- High Availability
- ICG connection for devices outside of your company network

## General Preconditions

The Installation and Sizing Guidelines apply for a standard UMS setup and describe the most common UMS environments. Any individual exceptions or requirements may not be covered by these scenarios.

- System requirements: UMS 6.05 and newer, ICG 2.02 and newer
- UMS Console may be located **inside the same (V)LAN as UMS Servers** (no NAT, no proxies) or **outside the VLAN** with firewalls/routing configured according to IGEL UMS Communication Ports.
- Devices **directly connected to the UMS Server** are in **the same (V)LAN as UMS Servers** (no NAT, no proxies). If there is a firewall, it must be configured according to IGEL UMS Communication Ports.
- Devices **outside of the internal LAN** are connected **via ICG**.
- Devices are **not booted/rebooted frequently** (once a day on average).
- **A maximum of 10 different firmware versions** is managed via UMS.
- UMS backups and exports are **not permanently stored on the UMS server** host.
- In the case of automatic device registration (see Registering Devices Automatically on the IGEL UMS): The **DNS** alias `igelrmsserver` or the **DHCP** tag can only point to ONE UMS installation. Therefore, the installation of several separate UMS Servers (without the High Availability Extension) in one network is not recommended.

 **High Availability with IGEL UMS Load Balancers:** All UMS Servers and UMS Load Balancers must reside on **the same VLAN**.  
For High Availability (UMS HA) with IGEL UMS Load Balancers, network traffic must be allowed over UDP broadcast port 6155, and TCP traffic and UDP broadcast traffic over port 61616. For further port configuration, see IGEL UMS Communication Ports.  
Note: IGEL UMS HA installation with IGEL UMS Load Balancers is not supported in cloud environments like Azure / AWS as they do not allow broadcast traffic within their networks. The HA installation without IGEL UMS Load Balancers (as well as the Distributed UMS) is, however, supported in cloud environments as of UMS version 6.10.

### Recommended Additional Information

IGEL UMS Communication Ports: Find a list with all ports that are relevant for the communication with the UMS.

Latest release notes: Find in the Supported Environment section the list of supported servers, clients, and backend databases.

High Availability (HA): Find useful how-tos and the reference guide around your HA installation.

IGEL Cloud Gateway: Find how-tos, the reference guide, and additional information concerning the management of endpoints outside the company network.

- 
- [IGEL UMS Sizing Guidelines & Architecture Diagrams](#) (see page 4)
  - [Performance Optimizations in IGEL UMS](#) (see page 17)
  - [IGEL Cloud Gateway vs. Reverse Proxy for the Communication between UMS 12 and IGEL OS Devices](#) (see page 23)

## IGEL UMS Sizing Guidelines & Architecture Diagrams

The following sizing guidelines are intended to support you with setting up the IGEL Universal Management Suite (UMS) environment – UMS Server, UMS Console & UMS Web App, database, and, if required, load balancer and ICG instances.

### ✔ **General Installation Recommendations**

For small installations, a single UMS Server instance (standard UMS) with an embedded database is usually sufficient. If required, a single-instance installation can be easily extended anytime to a Distributed UMS installation by installing additional servers (and in the case of an embedded database, by switching preliminarily to an external data source).

Large installations should use either the UMS High Availability or the Distributed UMS (preferable for new installations, e.g. because you do not have to configure additional firewall exclusions). For large installations, it is also recommended to use DNS-Round-Robin load balancing or IGEL Cloud Gateway.

For more information, see IGEL UMS Installation.



Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
<b>S</b>	< 5.000	<b>1 server</b>	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB free disk space			Embedded database	<b>1 ICG instance per 2,500 devices</b>
<b>M</b>	< 15.000	<b>1 server</b>	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB free disk space			<b>External database</b> 10 GB	<b>Server generally:</b> 8 GB RAM 2 CPUs 20 GB free disk space
<b>M / S (HA or Distributed UMS)</b>	< 15.000	<b>2 servers 2 load balancers</b>	9 GB RAM (Web App +1GB) 6 CPUs 25 GB free disk space	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB free disk space			<b>External database</b> 10 GB	<b>Only ICG service:</b> 4 GB RAM 2 CPUs 2 GB free disk space
<b>L (HA or Distributed UMS)</b>	< 50.000	<b>2 servers 2 load balancers</b>	6 GB RAM*** (Web App +1GB) 4 CPUs 25 GB free disk space	<b>Mandatory</b> 3 GB RAM 2 CPUs 1 GB free disk space			<b>External database</b> 10 GB	
<b>XL (HA or Distributed UMS)* ***</b>	< 300.000	<b>Up to 6 servers (1 server / 50,000 devices)</b>	9 GB RAM (Web App +1GB) 6 CPUs 25 GB free disk space	<b>Mandatory</b> 6 GB RAM 4 CPUs 1 GB free disk space	Up to 3 Load Balancer (1 LB / 3 Server)	4 GB RAM 4 CPUs 2 GB free disk space	<b>External database</b> 20 GB	



\* UMS Console can be installed on UMS Server host.

\*\* Follow the recommendation of the external database system on RAM and CPU.

\*\*\* RAM and CPU requirements are less than in the case of **M / S (HA)** installation since the UMS Console is installed on a separate host machine (**UMS Console Standalone = Mandatory**).

\*\*\*\* General recommendation: 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

For the architecture diagrams of the installations, see:

- [Small Environment: UMS S](#) (see page 7)
- [Medium Environment: UMS M](#) (see page 9)
- [Small and Medium Environments: UMS M/S \(HA\)](#) (see page 11)
- [Large Environment: UMS L \(HA\)](#) (see page 13)
- [Extra Large Environment: UMS XL \(HA\)](#) (see page 15)



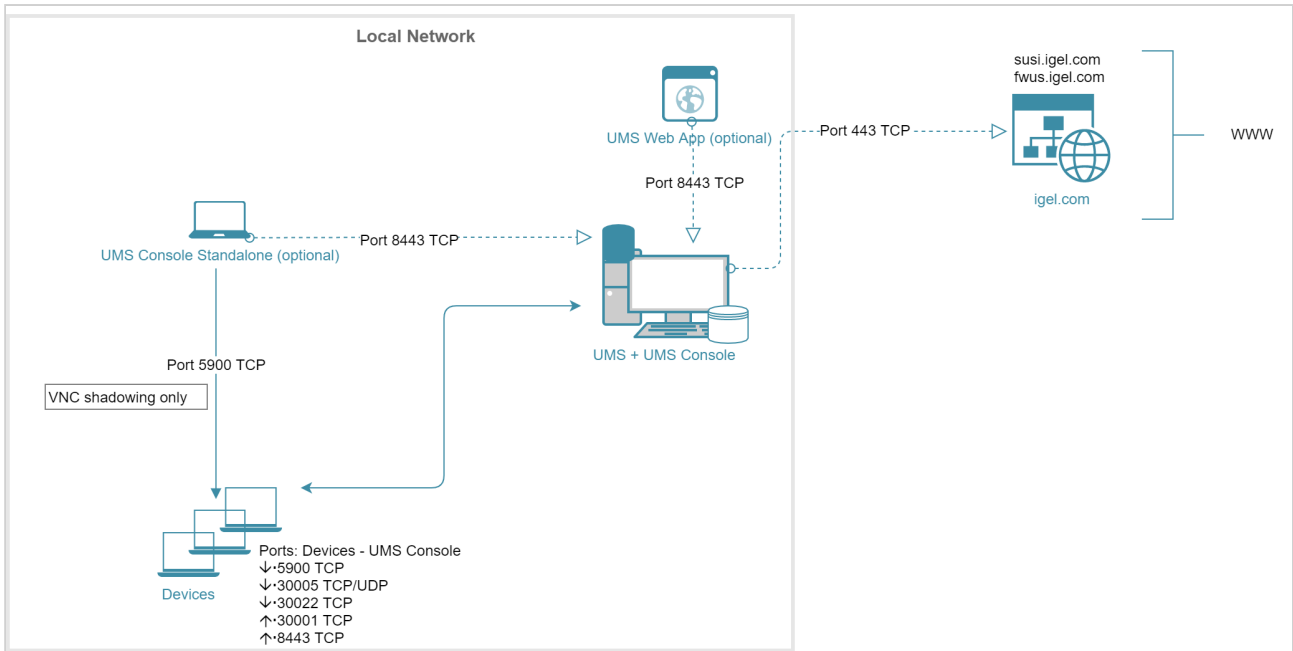
## Small Environment: UMS S

Small Size UMS Installation (<5k Devices) or Demo/POV Environment with an Embedded Database

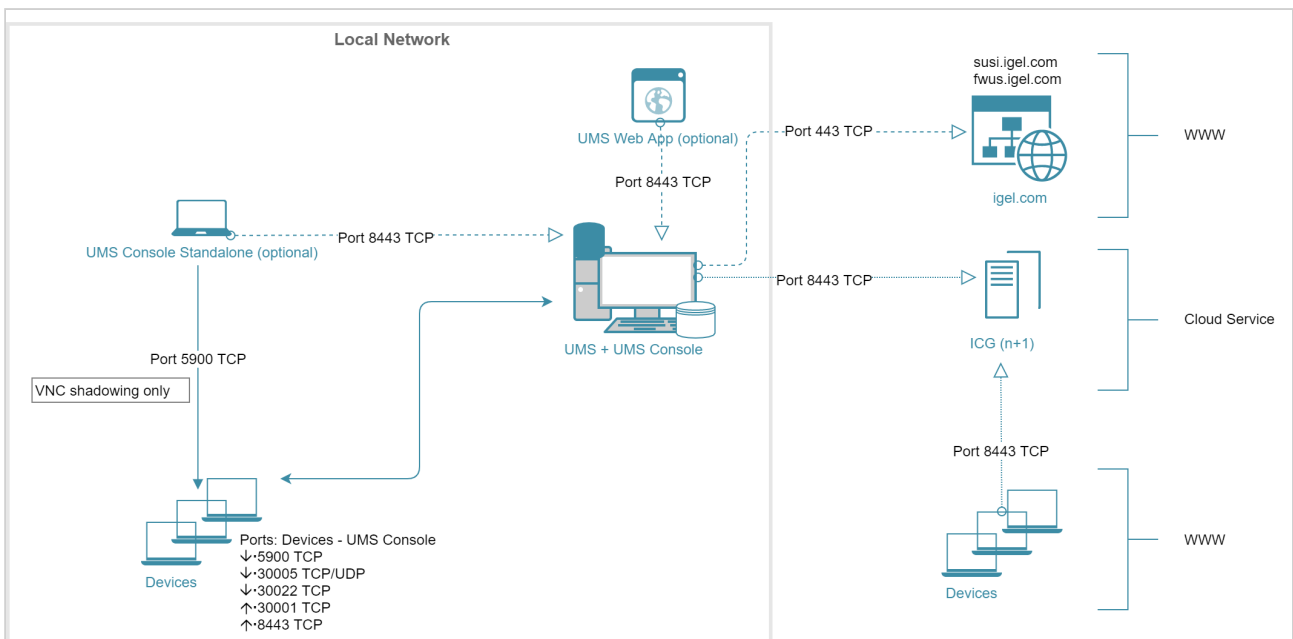
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database	ICG
<b>S</b>	< <b>5.000</b>	<b>1 server</b>	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB HDD			Embedded database	<b>1 ICG instance per 2,500 devices</b>  <b>Server generally:</b> 8 GB RAM 2 CPUs 20 GB HDD  <b>Only ICG service:</b> 4 GB RAM 2 CPUs 2 GB HDD

\* UMS Console can be installed on UMS Server host.

## Architecture: Small Environment



### Architecture: Small Environment + ICG in Cloud







## Medium Environment: UMS M

Medium Size UMS Installations (up to ~15k Devices); No High Availability

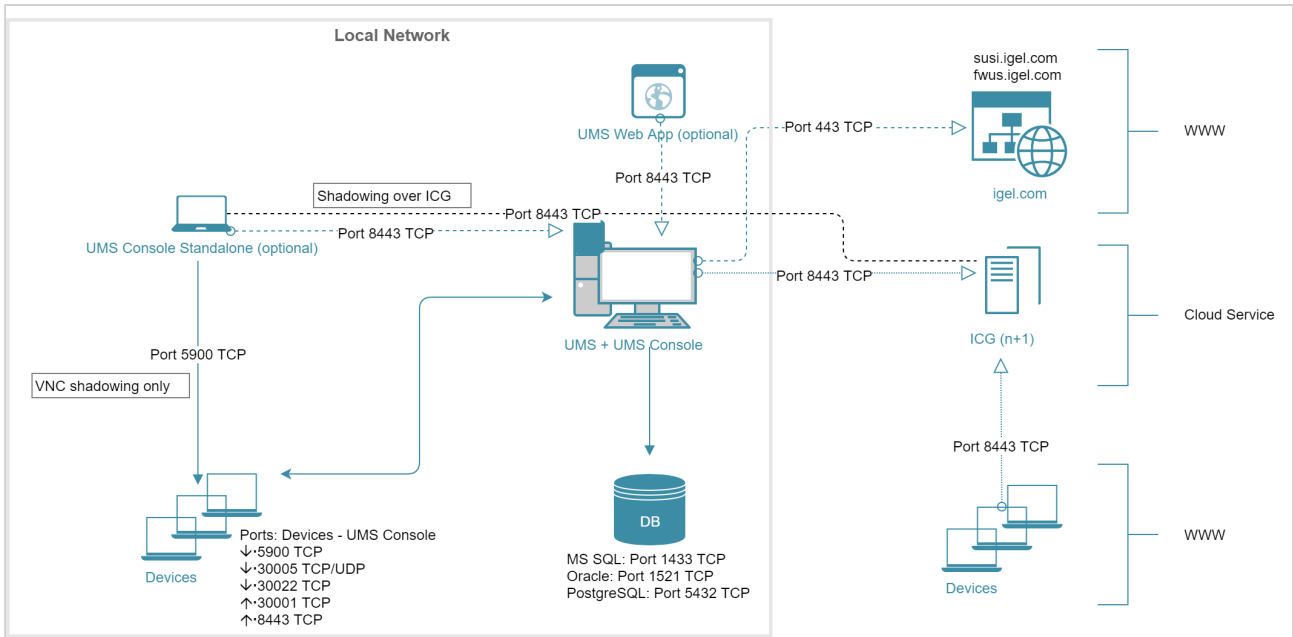
Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
<b>M</b>	< <b>15,000</b>	<b>1 server</b>	8 GB RAM (UMS Web App + 1 GB) 4 CPUs 25 GB free disk space	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB HDD			<b>External database</b> 10 GB	<b>1 ICG instance per 2,500 devices</b>  <b>Server generally:</b> 8 GB RAM 2 CPUs 20 GB HDD  <b>Only ICG service:</b> 4 GB RAM 2 CPUs 2 GB HDD

\* UMS Console can be installed on UMS Server host.

\*\* Follow the recommendation of the external database system on RAM and CPU.

 For High Availability, see [Small and Medium Environments: UMS M/S \(HA\)](#) (see page 11).

## Architecture: Medium Environment + ICG





## Small and Medium Environments: UMS M/S (HA)

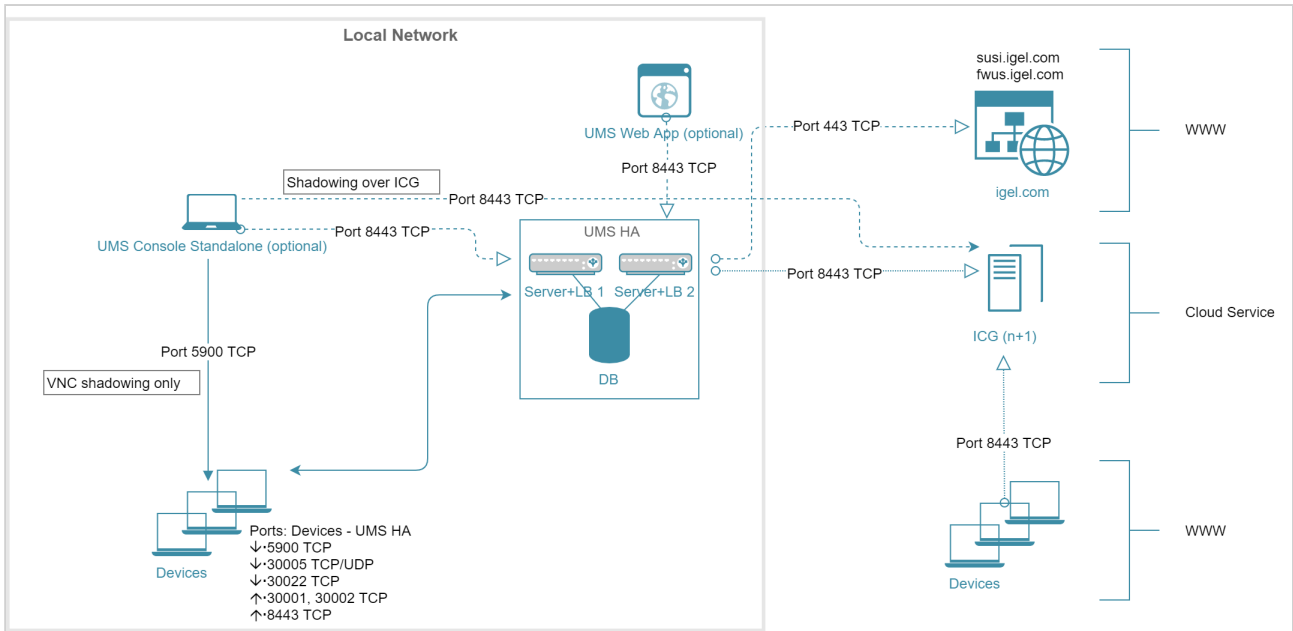
Small and Medium Size UMS Installations (up to ~15k devices); High Availability

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
<b>M / S (HA or Distributed UMS)</b>	< 15,000	<b>2 servers 2 load balancers</b>	9 GB RAM (Web App +1 GB) 6 CPUs 25 GB HDD	<b>Optional*</b> 3 GB RAM 2 CPUs 1 GB HDD			<b>External database</b> 10 GB	<b>1 ICG instance per 2,500 devices</b>  <b>Server generally:</b> 8 GB RAM 2 CPUs 20 GB HDD  <b>Only ICG service:</b> 4 GB RAM 2 CPUs 2 GB HDD

\* UMS Console can be installed on UMS Server host.

\*\* Follow the recommendation of the external database system on RAM and CPU.

## Architecture: Small and Medium Environment (HA) + ICG





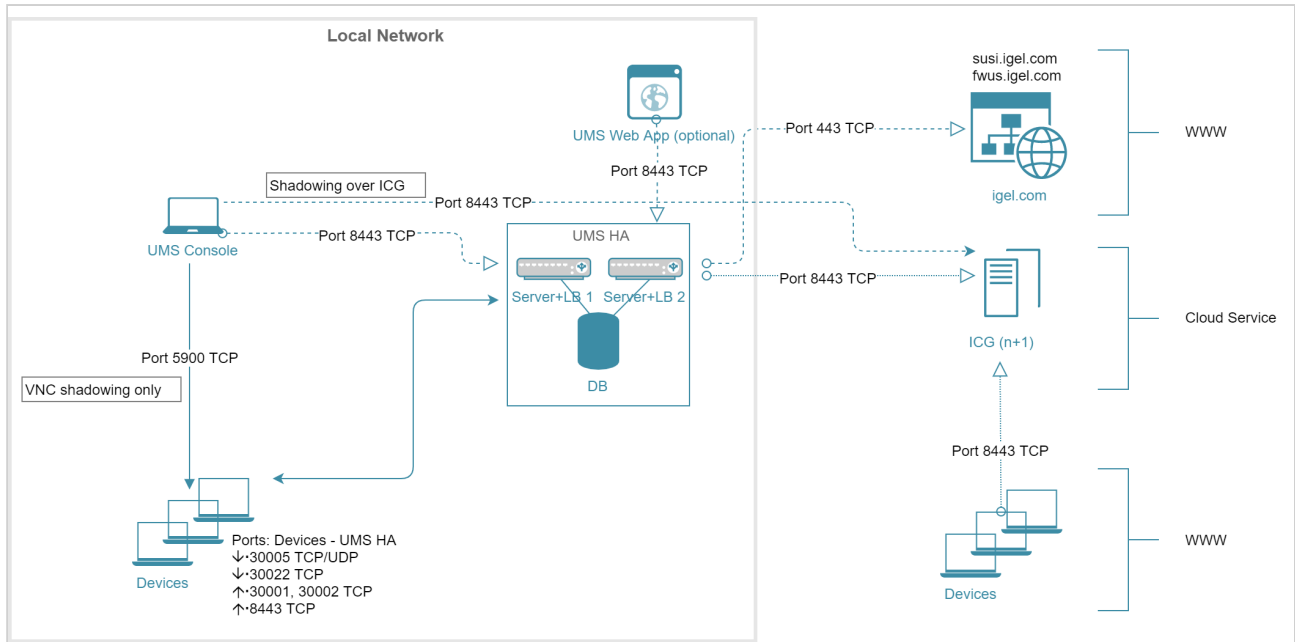
## Large Environment: UMS L (HA)

### Large UMS Installations with up to 50k Devices; High Availability + ICG

Installation Size	#Devices	#UMS Server Host (+ Load Balancer)	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
L (HA or Distributed UMS)	< 50,000	2 servers 2 load balancers	6 GB RAM (Web App +1GB) 4 CPUs 25 GB HDD	Mandatory 3 GB RAM 2 CPUs 1 GB HDD			External database 10 GB	1 ICG instance per 2,500 devices  Server generally: 8 GB RAM 2 CPUs 20 GB HDD  Only ICG service: 4 GB RAM 2 CPUs 2 GB HDD

\* Follow the recommendation of the external database system on RAM and CPU.

### Architecture: Large Environment (HA) + ICG





## Extra Large Environment: UMS XL (HA)

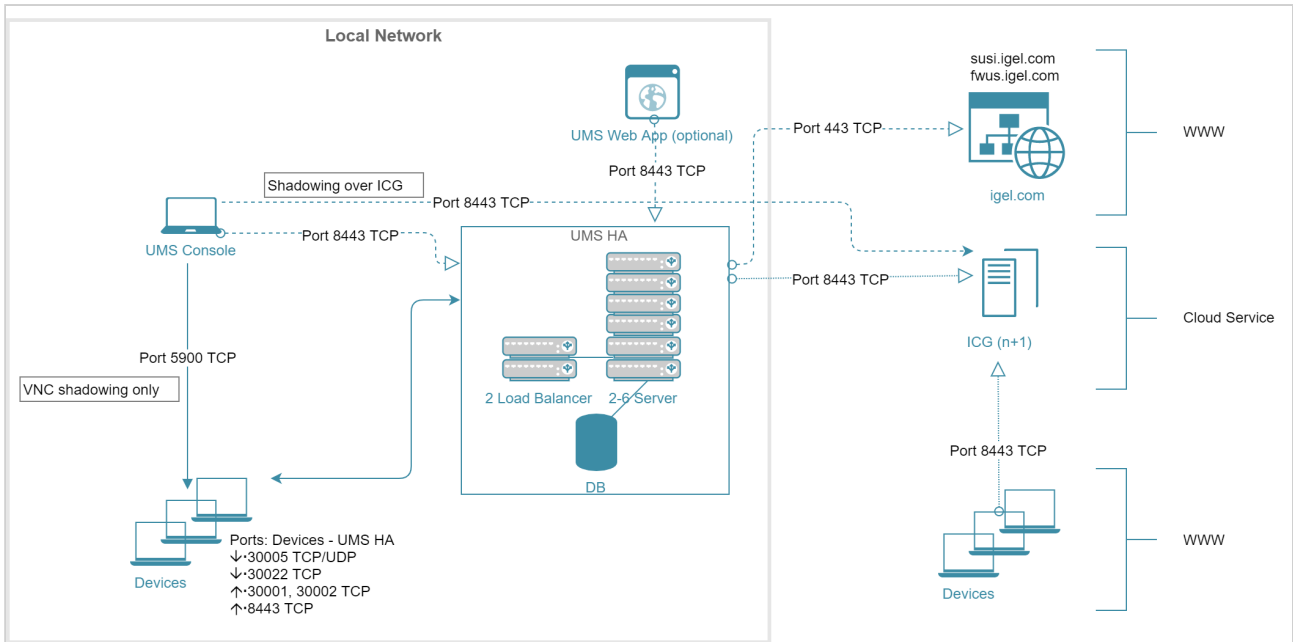
### Extra Large UMS Installations with up to 300k Devices; High Availability + ICG

Installation Size	#Devices	#UMS Server Host	UMS Server	UMS Console Standalone	#Load Balancer Standalone	Load Balancer Standalone	Database*	ICG
<b>XL (HA or Distributed UMS)*</b>	<b>&lt; 300,000</b>	<b>Up to 6 servers</b> (1 server / 50,000 devices)	9 GB RAM (Web App +1GB) 6 CPUs 25 GB HDD	<b>Mandatory</b> 6 GB RAM 4 CPUs 1 GB HDD	Up to 3 load balancers (1 load balancer / 3 servers)	4 GB RAM 4 CPUs 2 GB HDD	<b>External database</b> 20 GB	<b>1 ICG instance per 2,500 devices</b>  <b>Server generally:</b> 8 GB RAM 2 CPUs 20 GB HDD  <b>Only ICG service:</b> 4 GB RAM 2 CPUs 2 GB HDD

\* Follow the recommendation of the external database system on RAM and CPU.

\*\* General recommendation: 1 UMS Server per 50,000 devices, 1 load balancer for 3 UMS Servers.

## Architecture: Extra Large Environment (HA) + ICG





## Performance Optimizations in IGEL UMS

### Data Sizing

- The number of registered firmware versions has the **largest impact** on the size of the database. (Listed in UMS Console under **Misc > Firmware Statistics**)
- The number of devices or profiles has a **minor impact**.
- Average size per...
  - Firmware configuration: ~15 MB
  - Profile (depends on the number of active parameters): ~100 kB
  - Device: ~100 kB
- Reserve 500 MB up to 1 GB for database transaction logs of excessive database calls like **Remove unused Firmware**. Please note that the usage depends on the database system used.

### Latencies

If you are struggling with long-distance connections and high latency, please consider the following recommendations:

- Minimize latency between...
  - Database <-> UMS Server: <= 20 ms
  - Several UMS Servers: <= 50 ms
  - Load balancer <-> UMS Server: <= 50 ms
- High latency between the database and the UMS Server has a **huge impact** on the performance. The communication between the device and the UMS Console will slow down, the UMS Console itself will become lazy.
- High latency between the device and the UMS Server has **little impact** on overall performance.

### Performance Optimizations

- **UMS logs:**  
Use administrative tasks to automatically clean up logs (logging data, job execution data, execution data of administrative tasks, process events, asset information history) or remove old UMS log files ( `/rmguiserver/logs` ) when storage space runs out.
- **Firmware:**  
Remove unused firmware regularly.
- **Embedded database only:**
  - Optimize database regularly (UMS Administrator application, e.g. once a month)
  - Check for free storage space and expand the storage size if necessary (keep at least 1 GB free at all times)
- **Number of devices:**
  - If the device count is high (>10k) and overall performance is low, increase UMS Server and UMS Console memory. See How to Configure Java Heap Size for the UMS Server and How to Configure Java Heap Size for the UMS Console.



- Avoid too many devices (>5k) in one folder.
- **Assignments:**  
Keep the number of assignments per device (direct and indirect) at a low level (<25).
- **Administrative tasks and jobs:**  
The more administrative tasks and jobs are created, the more heap is "eaten up", so it may be necessary to increase UMS Server memory. See How to Configure Java Heap Size for the UMS Server.
- **Default directory rules:**  
Do not use default directory rules with the **Apply rule when device boots** option unless they are required.
- **Concurrent device requests:**  
If you are experiencing problems with many concurrent device requests (delays in configuration deployment or logging on to the device), open the UMS Console and use the options under **UMS Administration > Global Configuration > Device Network Settings > Device Requests** (thread and queue size) to control the throughput of the device requests. Contact support for recommendations.

## Limitations: UMS HA

- Device actions that are manually triggered in the UMS Console are performed by **one UMS Server** (the one the UMS Console is currently connected to); there is no load balancing for these actions.




## IGEL UMS Maintenance Tasks

There are a few items that are recommended to configure after your IGEL Universal Management Suite (UMS) server(s) are set up to make sure they are properly maintained and running as efficiently as possible. This article outlines some recommended configurations that should be made to make sure your UMS database and file structure are maintained properly.

### Recommended Administrative Tasks (Scheduled Jobs)

There are multiple tasks that should be scheduled to properly maintain a UMS server/cluster and database.

 As part of the tasks, you will be asked to provide a location to back up the data before deleting them. This can be done on a mapped (lettered) drive in Windows, or a mounted remote location on Linux if required.

### Scheduling

It is recommended to schedule each task on a different day, two hours after any backups are made. This will give each task enough time to complete and allow for a rollback via the backup if data is removed that is required.

### Recommended Tasks

	Task Name	Task Details	Task Notes
1	<b>Delete job execution data</b>	<b>UMS Administration &gt; Administrative Tasks &gt; Dialog Create Administrative Task &gt; Action Delete job execution data</b>	With this administrative task, you can delete the job execution results listed under <b>Jobs &gt; [job name]</b> .  For details, see Delete Job Execution Data.
2	<b>Delete process events</b>	<b>UMS Administration &gt; Administrative Tasks &gt; Dialog Create Administrative Task &gt; Action Delete process events</b>	With this administrative task, you can delete the process events displayed under <b>UMS Administration &gt; UMS Network &gt; Events &gt; [timespan]</b> .  For details, see Delete Process Events.



Task Name	Task Details	Task Notes
3 <b>Delete administrative task execution data</b>	<b>UMS Administration &gt; Administrative Tasks &gt; Dialog Create Administrative Task &gt; Action Delete administrative task execution data</b>	With this administrative task, you can delete the results of the execution of administrative tasks listed under <b>UMS Administration &gt; Global Configuration &gt; Administrative Tasks &gt; [task name]</b> .  For details, see Delete Administrative Task Execution Data.
4 <b>Delete asset info history</b>	<b>UMS Administration &gt; Administrative Tasks &gt; Dialog Create Administrative Task &gt; Action &gt;Delete asset info history</b>	With this administrative task, you can delete the stored asset information that is displayed under <b>Devices &gt; [device name]</b> .  For details, see Delete Asset Information History.
5 <b>Delete logging data</b>	<b>UMS Administration &gt; Administrative Tasks &gt; Dialog Create Administrative Task &gt; Action &gt;Delete logging data</b>	With this administrative task, you can delete the log messages that can be configured under <b>UMS Administration &gt; Global Configuration &gt; Logging</b> . For details, see Delete Logging Data.

Example:

Administrative Tasks							
Name	Job	Last Execution	Next Execution	Execution Status	Active	Send result	
Nightly - Backup	Create backup	Jul 15, 2023, 10:00 PM	Jul 17, 2023, 10:00 PM	completed	✓		
Monday - Delete Job Execution Data	Delete job execution data	Jul 10, 2023, 10:59 PM	Jul 17, 2023, 11:59 PM	completed	✓		
Tuesday - Delete Process Events	Delete process events	Jul 11, 2023, 10:59 PM	Jul 18, 2023, 11:59 PM	completed	✓		
Wednesday - Delete Administrative	Delete administrative task execution data	Jul 12, 2023, 11:00 PM	Jul 19, 2023, 11:59 PM	completed	✓		
Thursday - Delete Asset Inventory H	Delete asset info history	Jul 13, 2023, 10:58 PM	Jul 20, 2023, 11:59 PM	completed	✓		
Friday - Delete Logging Information	Delete logging data	Jul 14, 2023, 10:59 PM	Jul 21, 2023, 11:59 PM	completed	✓		

## UMS Server Backups

### Backup Schedule

It is recommended to schedule a backup at least once a week of the UMS database and local file repositories.

- This could be scheduled as frequently as once a day during device deployment or mass configuration changes.

This backup should be scheduled to occur at a minimum of two hours after any other Administrative Tasks are scheduled to run.



### External Database

For external / third-party databases, such as Postgres and Microsoft SQL, you will need to utilize their respective backup options, or a third-party software to manage database backups.

For the internal IGEL database, see [IGEL Embedded Database](#) (see page 21).

### Local Files

For UMS, the IGEL database is the most critical component that needs to be backed up, and this should be handled via a third-party application connected to your external database. However, some local directories should be backed up outside of UMS. These locations are noted below.

Directory	Usage
<code>%INSTALL_DIR%/RemoteManager/rmguiserver/webapps/ums_filetransfer</code>	Contains all transfer files deployed via UMS including Universal Firmware Packages, wallpaper files, icon files, and SSL certificates, etc.
<b>UMS12 and later:</b> <code>%INSTALL_DIR%/RemoteManager/rmguiserver/persistent/ums-appproxy</code>	Contains OS 12 application packages for the local UMS Web Proxy

**⚠** By default the IGEL install directory (`%INSTALL_DIR%`) will be located in one of the locations below. If UMS was installed to a different directory, please update the path accordingly.

Operating System	Location(s)
<b>Windows</b>	<code>C:\Program Files\IGEL\</code> or <code>C:\Program Files(x86)\IGEL\</code>
<b>Linux</b>	<code>/opt/IGEL/</code>

### IGEL Embedded Database

For the embedded database, there are a couple more items that are recommended to perform.



**⚠** IGEL recommends moving to an external database for production environments, so this should only be required in POC / Lab environments. However, some smaller environments may still utilize the embedded database in production.

### Local Database Optimization

If you are using the IGEL embedded database, it is recommended to run a database optimization at least every 3 months, and maybe more depending on the size of your environment. You can find more details on this process under [Optimizing the Active Embedded DB](#), but keep in mind that this will halt services on UMS and the console will be unavailable until it completes.

### Local Database Backup

If you are using the IGEL embedded database, then you will want to schedule an additional administrative task in UMS to perform this action.

Task Name	Task Details	Notes
Database Backup	Creates a backup of the database, and other optional components.	<ul style="list-style-type: none"> <li>Recommended to backup only the database, but you can also select the transfer files as well. Doing so may take a long time, and will create a larger backup file.</li> <li>Backing up the server configuration is not required or recommended</li> </ul>

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

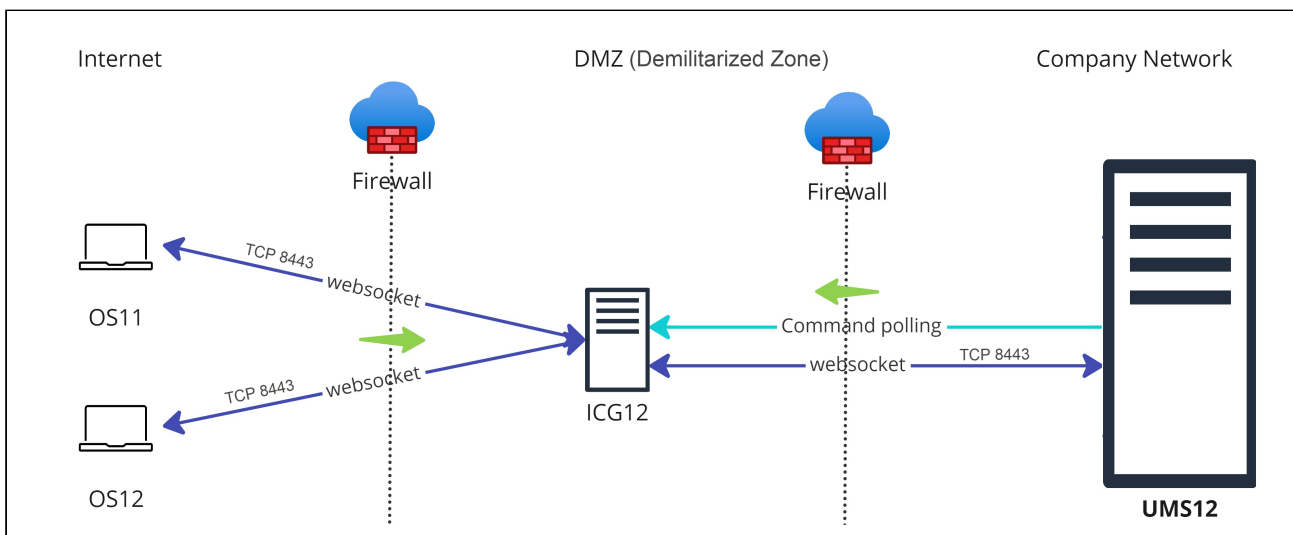
With the launch of IGEL Universal Management Suite (UMS) 12, the Unified Protocol used for all communication between the UMS and IGEL OS 12 devices was introduced, see Overview of the IGEL UMS. The Unified Protocol is a secure protocol that uses TCP 8443, see IGEL UMS Communication Ports. However, depending on the structure of your UMS environment, company's security policies, etc., it may be insufficient, and the use of the IGEL Cloud Gateway (ICG) or reverse proxy may be required. In the following article, you will find pros and cons of each solution.

**i** In general UMS/ICG only needs routing for the configured web port between the device and the UMS/ICG. If any of the network components terminates SSL, the client cert needs to be forwarded in a HTTP header.

**⚠** The example configurations in the pictures are for general illustrative purposes. Each network configuration will vary depending on the network setup, i.e. whether the UMS is in a DMZ or not.

### Option 1: ICG 12

In the case of the ICG, endpoint devices connect to the ICG as well as the UMS connects to the ICG, see Devices and UMS Server Contacting Each Other via ICG. The WebSocket communication between the ICG and the UMS as well as between the ICG and the device is only established after mutual authentication, and the communication is encrypted with TLS. All data is routed through this WebSocket.



Advantages:

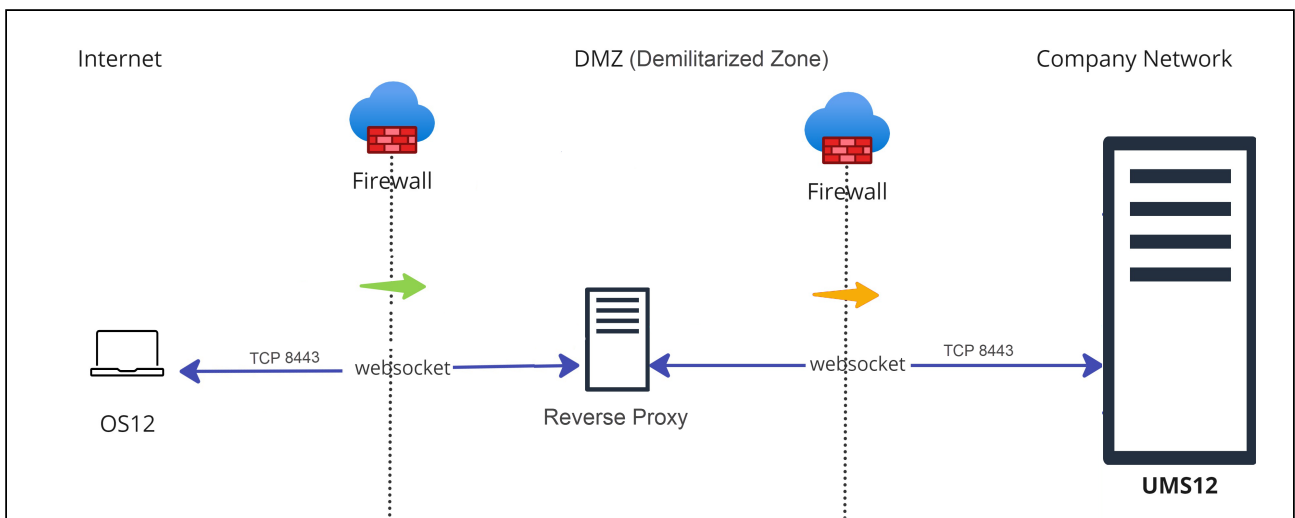
- Suitable for mixed environments when you manage both IGEL OS 12 and IGEL OS 11 devices
- No inbound connection from the device to the UMS
- Only the ICG is exposed to the Internet. Thus, if compromised, the UMS is NOT compromised at the same time.
- Simple and lightweight, which minimizes the attack surface

Disadvantages:

- UMS as an Update Proxy feature cannot currently be used, i.e. IGEL OS devices can download the apps from the App Portal only, not from the UMS Server. See Configuring Global Settings for the Update of IGEL OS Apps.
- Higher latency and longer command execution in comparison to the reverse proxy. For large enterprise environments, the use of a reverse proxy may be considered.

## Option 2: Reverse Proxy

Another possibility to route the traffic via port 8443 is to use a reverse proxy. The reverse proxy will forward the requests from devices to the UMS.



Technical details:

- Reverse proxy with SSL offloading is possible as of UMS 12.02. See NGINX: Example Configuration for as Reverse Proxy in IGEL OS with SSL Offloading.
- The FQDN and port of the reverse proxy must be specified as a Cluster Address, see Server Network Settings in the IGEL UMS.

**i** A reverse proxy / load balancer can also be used to distribute traffic from devices within the company network. For more information on network component integration, see IGEL Universal Management Suite Network Configuration.



- It is advisable to use TLS 1.3 for the reverse proxy configuration.

Advantages:

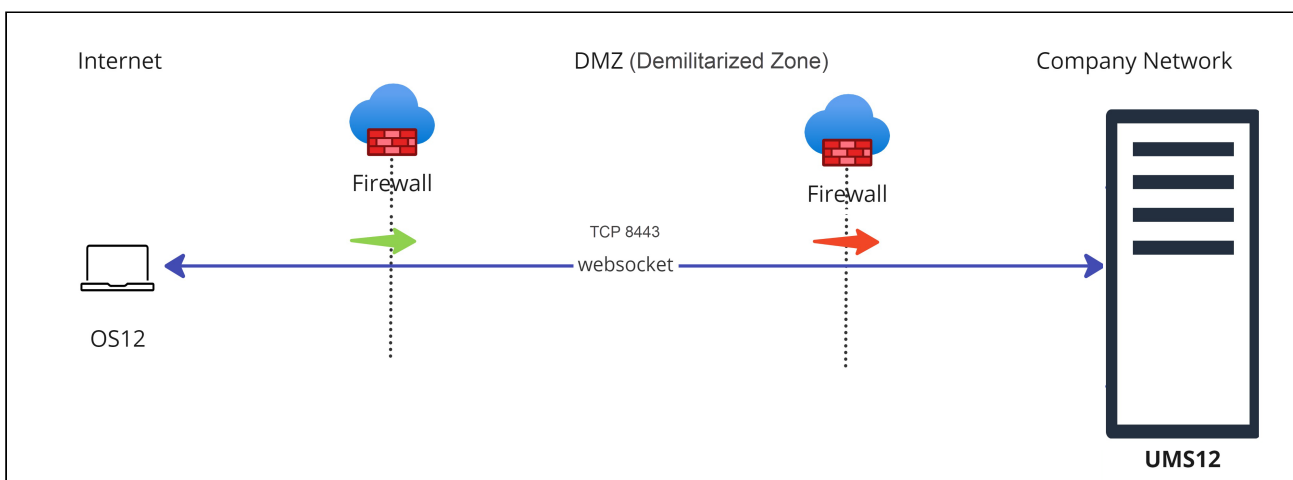
- Load balancing
- UMS as an Update Proxy feature can be used, i.e. IGEL OS devices can download the apps from the UMS Server. See Configuring Global Settings for the Update of IGEL OS Apps.

Disadvantages:

- Can be used if you manage IGEL OS 12 devices only.
- Proper configuration and maintenance of the reverse proxy is required. For security reasons, you may want to restrict access to any components you do not require, but note that the following paths must be enabled:
  - For IGEL OS 12 device onboarding and communication: TCP 8443 /device-connector/\*
  - For IGEL OS 12 and UMS as an Update Proxy feature: TCP 8443 /ums-appproxy/\*
  - For the UMS Web App: TCP 8443 /wums-app/\* and /webapp/\*
- If used to connect devices from outside the company network, the devices have an inbound connection to the UMS. In comparison, with the ICG, there is no inbound connection from the devices to the UMS.
- Adds an extra layer of security (depending on the configuration), but, if compromised, the reverse proxy can provide access to the UMS. In comparison, the ICG does not expose the UMS to the Internet.

### Option 3: Direct Connection of the Devices to the UMS via Unified Protocol (No ICG, No Reverse Proxy)

In this case, IGEL OS 12 devices communicate directly with the UMS, see Devices Contacting UMS.




Advantages:

- port 8443 (can be changed under **UMS Administrator > Settings > Web server port**) must be opened in a firewall, but no other configuration is required
- suitable for communication with devices within the company network

Disadvantages:


- Inbound connection from the device to the UMS
- For communication with devices outside the company network, it is advised to consider the use of a reverse proxy or the ICG

 IGEL Onboarding Service (OBS) is NOT a substitute for an ICG or a reverse proxy and is only meant to authenticate and register the endpoint device with the correct UMS during the onboarding. For more information on the OBS, see Initial Configuration of the IGEL Onboarding Service (OBS) and Onboarding IGEL OS 12 Devices.

---

Legend to the images:

 : Shows that the traffic in the WebSocket runs in both directions.

 (multicolored): Shows from which side firewalls etc. must be opened.