IGEL SOFTWARE SUITE

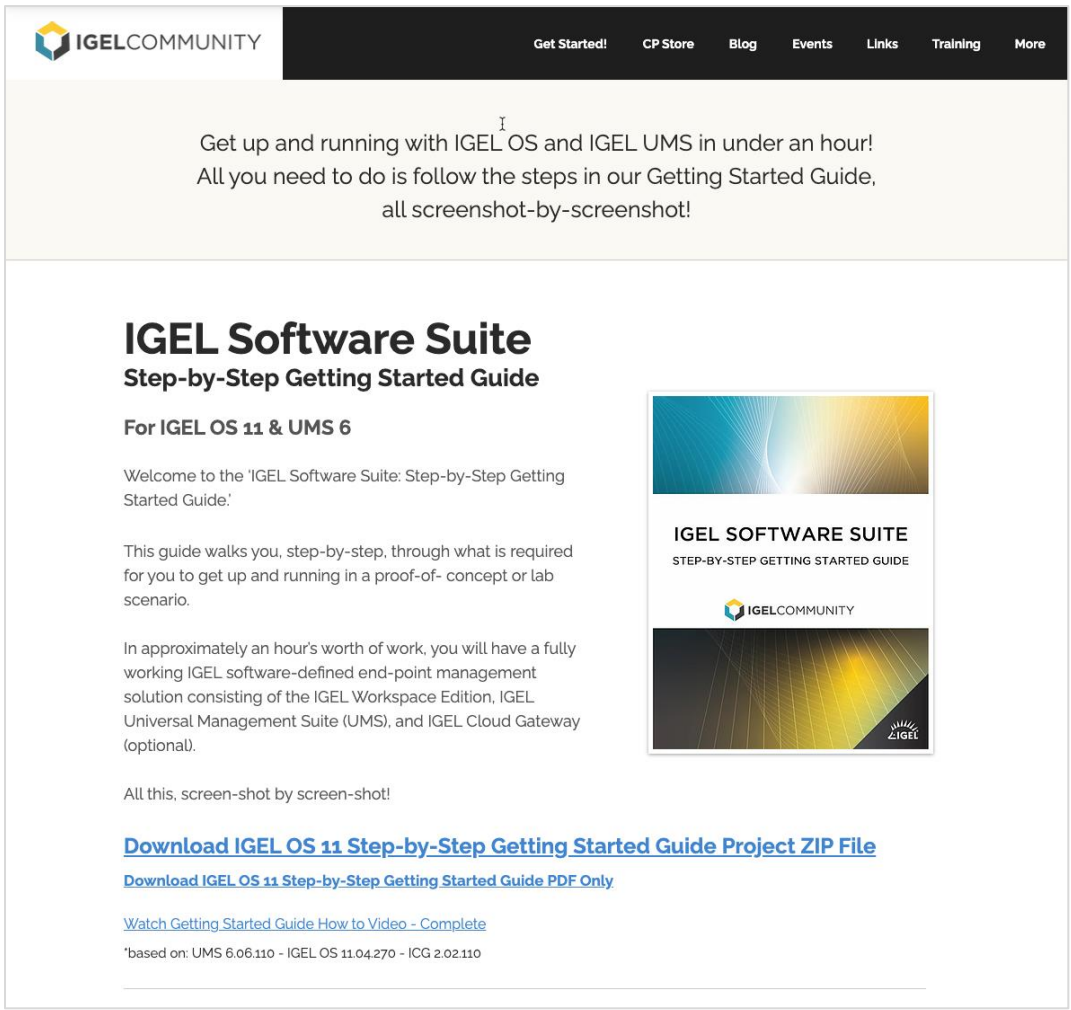
STEP-BY-STEP GETTING STARTED GUIDE

Version 2.3 - March 26, 2021

Current Released Software: UMS 6.06.110 - IGEL OS 11.05.120 - ICG 2.02.110

IMPORTANT

Please verify you have the latest version of this 'Getting Started Guide' as things do change. The newest version is available **here**.



NOTICE

Copyright

Trademarks

Disclaimer

IGEL Technologies and Solutions, designed in Germany, made from genius!

The above legalese aside, this is a product of the IGEL Community. Please feel free to do with it as you choose; share it, contribute to it, and use it! However, please do not Sauté.

Authors

This guide is a labor of love by the IGEL Community. The following fine folks put fingers to the keyboard to make this resource a reality.

Written and Maintained by Douglas A. Brown - brown@igel.com

The Experts:

Sébastien Pérusat - perusat@igel.com

Christian Drieling - drieling@igel.com

Udo Jetschmanegg - Jetschmanegg@igel.com

Fredrik Brattstig - Brattstig@igel.com

Timco Hazelaar - t.hazelaar@thipc.com

Special Thanks

This project is a community activity and a byproduct of many folks who gave of their time to contribute tech recommendations, proofing, testing and, much appreciated support. A huge thank you from me to them!

So, shines a good deed in a weary world!

Carl Webster

Benjamin Crill

Sébastien Pérusat

Dieter Boonen

Chris Calaf

Christian Drieling

Carl Behrent

Martijn van Tricht

Michael Greear

Thomas Poppelgaard

Mattias Jacobsson

Andrew Wood

Douglas DeCamp

Fredrik Brattstig

Timco Hazelaar

Falk Heiland

Abigail Arcilla

Kolja Knispel

Guido Jakobs

Henk-Jan Eiten

Rob Beekmans

Ian Anderson

René Bigler

Gamal Attia

Daniel Ugarte

Udo Jetschmanegg

Personal Thanks to the following Amazing Folks!

Christian Drieling & Fredrik Brattstig – Big thanks must be given to Fredrik and Christian as this guide would have never been possible without their help. They are the ones who taught me IGEL by walking me through the UMS step-by-step. They were more than happy to open a GTM session to help me during my first installs and even put up with my dumb questions. Without them, this project would not have been possible. They are real rock stars. Thank you both so very much!

Sébastien Pérusat – Sébastien is always more than happy to help and sent many great suggestions on improving the project along with a bunch of great tech tips. This is the type of feedback I love! Sébastien is one highly motivated guy, always willing to help! He is also my favorite Frenchmen!

Timco Hazelaar – One of the more challenging items to guide is SSL, but not for Timco. Without being told, he took it upon himself to contribute the '**How to Use a DigiCertificate SSL Certificate with ICG**' section of this guide. Many thanks for the great work Timco. However, this is par for his course. He is a goodie though I do not recommend you drive with him.

Udo Jetschmanegg – Even before becoming an IGEL employee, Udo was all over helping make this project better for all of us. He sent me a slew of screenshots and tips and tricks. You are always one step ahead of me!

Michael Greear and Kolja Knispel – These guys did the hard work! They scoured the guide and did their best to clean up my poor English and grammar. These are the changes I genuinely love, as this is the type of help I need most. It is not a fun job, but they did it, and now we have a more polished deliverable. Huge thanks to Michael and Kolja. I can't thank them enough!

Abigail Arcilla – A huge thank you goes out to Abie for all her help with the IGEL Community logo and book covers. I've worked with many designers, but I've never worked with one I've appreciated and respected as much as Abie! Truly one of the best!

René Recker – If you want terrific ideas? Talk with René! If you want to be more motivated and driven? Talk with René! This guy is remarkable and has helped make this project and the IGEL Community what it is today! Rene ROCKS!

Special thanks to **Jed Ayres** and **Simon Richards** for allowing us the time, resources, and support to build the IGEL Community. O Captains! My Captains! We have an army!

Changelog

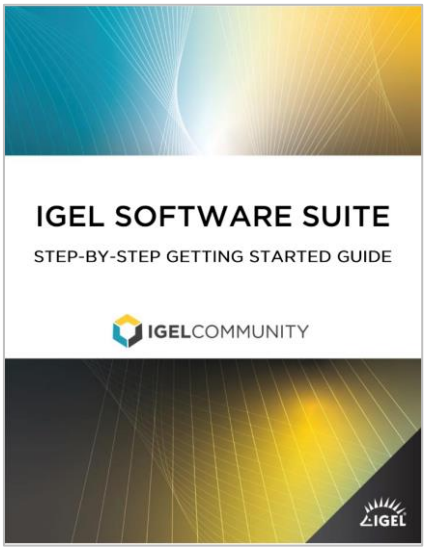
Date	Version	Description of Changes
12/7/2017	1.0 Public Draft 1	▪ First draft - public version
1/11/2018	1.0 Public Draft 2	▪ Added ICG section ▪ Fixed misc. grammar and spelling issues ▪ Added misc. feedback from IGEL community members
1/29/2018	1.0	▪ Added 'How to Use a DigiCertificate SSL Certificate with ICG' section. Contributed by Timco Hazelaar ▪ Fixed misc. grammar and spelling issues ▪ Added finial misc. feedback from community members ▪ Finalized look and feel of the guide
4/24/2018	1.5	▪ New cover artwork from the fantastic Abigail Arcilla. ▪ Miscellaneous grammar and other tweaks ▪ How to Customize the IGEL OS Look and Feel ▪ How to Update Firmware section updated with ICG section and more
9/18/2018	1.5.1	▪ Updated eDocs links to point to new kb.igel.com.
12/31/2018	1.9	▪ Updated all screenshots to reflect new UMS and ICG builds ▪ Added ICG Remote Installer ▪ Misc. fixes and more
3/6/2019	2.0	▪ Updated for IGEL OS 11 and UMS 6 ▪ NEW IGEL section for OS 11 and UMS 6 ▪ Added more links to 3rd party resources ▪ Removed 'How to Use a DigiCertificate SSL Certificate with ICG' section and made it a standalone white paper, link included in the additional resources section. ▪ Misc. fixes and more ▪ Removed the 'How to Customization' and' Firmware Update' sections and made them stand-alone white papers.
6/8/2020	2.1	▪ Update broken KB links ▪ Update IGEL OS 11 install licensing section ▪ Updated What's New in IGEL Software Suite section ▪ Updated all screenshots
2/25/2021	2.2	▪ Update broken KB links ▪ Update IGEL OS, UMS, and ICG software versions ▪ Update all screenshots
3/2/2021	2.3	▪ Updated to IGEL OS 11.05.100 ▪ Added how to create a Chromium session ▪ Added how to create a Chromium Kiosk session ▪ Added how to install a CA Root Certificate on IGEL OS ▪ Added how to configure Citrix Access via Chromium

Table of Contents

Introduction

1. Project Overview

Hello and welcome to the '**IGEL Software Suite: Step-by-Step Getting Started Guide**.' My goal for this guide is to provide you with the tools, knowledge, and understanding to download IGEL's software and perform basic installation and configuration without being forced to read many manuals and numerous web support articles.



This guide walks you, step-by-step, through what is required for you to get up and running in a proof-of-concept or lab scenario.

In approximately an hour's worth of work, you will have a fully working IGEL software-defined endpoint management solution consisting of the IGEL Workspace Edition, IGEL Universal Management Suite (UMS), and IGEL Cloud Gateway (optional).

All this, screen-shot by screen-shot!

Typically, the IGEL solution is installed when converting a PC or on preinstalled 'thin client' style hardware, but for testing, it could be recommended to install in a virtual environment. IGEL fully supports VirtualBox and VMware Workstation. At a minimum, you will need to create two virtual machines, a Windows VM to host the IGEL UMS and one for the IGEL OS. Installing the IGEL Cloud Gateway (ICG) is optional. By following the guide's steps, you can test ICG on an AWS free tier server at no additional cost.

Want to learn IGEL OS 11? Follow this guide as we have you covered, cover to cover!

I hope this guide starts you down the right path to success with IGEL solutions!

Douglas A. Brown
VP of Community | IGEL Technology
brown@igel.com

2. About the IGEL Community

IGEL understands the power of community! The IGEL Community is where you learn, share, and engage with like-minded customers, partners, and EUC industry experts.

You will have the ability to collaborate with others, interact with IGEL enthusiasts who are more than willing to help, get answers to your questions in minutes, brainstorm ideas, build relationships that will last you a lifetime, and so much more!

You will love it!

The IGEL Community is built using Slack, the world's leading tool for collaboration. Slack is where conversations happen, decisions are made, and the information is always at your fingertips. The IGEL Community on Slack is available via any browser, a local Windows or Mac app, and even on your mobile device (Android, iPhone, and your favorite tablet).

You will have the ability to:

- Collaborate with the best of the best
- Interact with other IGEL enthusiast customers, consulting and alliance partners who are more than willing to help
- Brainstorm ideas (feature requests) and see them end up in future releases
- Build relationships that will last you a lifetime
- Ask questions relating to IGEL installation and management
- and so much more!

Join the IGEL Community today and get help supporting IGEL OS, UMS, ICG, and all IGEL software and Thin Clients solutions. We welcome you with open arms!

Join here: **http://www.igelcommunity.com/join**.

3. The IGEL Software Suite Explained

In a nutshell, the IGEL Software Suite allows you to efficiently manage, deploy, and maintain secure endpoints in the office and while working from home at any time. This consists of many benefits, but its core is a secure enterprise-grade operating system and management suite that runs on any compatible 64-bit x86 device. It is designed to be a fast and centrally managed endpoint environment for the data center and cloud-delivered world.

The IGEL Software Suite allows you to address many use cases. For example:

- **The perfect endpoint for VDI, DaaS, and all Cloud-Delivered Workspaces** - The IGEL OS is widely used as a secure and centrally managed endpoint for Citrix, VMware, Microsoft, and all SBC, VDI, and DaaS environments. Why be forced to maintain a traditional desktop when using a remoting solution? The IGEL Software Suite delivers easy management, simple yet powerful control, all while providing you with the security and flexibility enterprises need in today's work from anyway world.
- **Save on capital expenditure** – IGEL enables IT to extend current assets' lives by turning them into fully managed and secure IGEL devices that last much longer than traditional PCs while being centrally maintained. Organizations can defer or bypass the dreaded "hardware refresh cycle entirely" while benefiting from potentially colossal hardware and software cost savings.
- **Lockdown end-user devices** – Security is a must in today's work from anywhere world. By deploying the IGEL OS combined with the IGEL Universal Management Suite, you can lock down a device to only the apps, configurations, and system components you need. In the end, you create an ultra-light 'just enough' OS that is more secure and manageable than traditional Windows environments.
- **Windows 10 migration** – When thinking about migrating to Windows 10, why not consider migrating to a more efficient, secure, and flexible endpoint OS? Windows was designed decades ago for a one-to-one relationship between the user and the computer. Today's user and corporate requirements are much different. The IGEL solution addresses these requirements by design.
- **Work from Home (WFH)** – In the 'new normal' and beyond, corporations will see more employees working from home than ever before, which opens many new challenges. How do you secure, update, and manage an endpoint that does not belong to you? Do you buy all new hardware for these remote use cases? IGEL has the perfect solution with the UD Pocket. Instantly and securely boot almost any

device into the IGEL OS and allow your employees to work as if they were sitting at their office desk. All centrally managed and secure.

3. 1. What's New?

In 2019 IGEL overhauled how it offers software allowing customers total control over when, where, and how to deploy devices while drastically simplifying the purchasing process and adding enterprise-class support. In 2020 IGEL continued to enhance these offerings based on feedback from customers and partners. The result is a pure software-defined offering that allows customers to easily license and manage any compatible 64-bit x86 devices from the cloud and port their licensed assets as needed to fit their environment.

IGEL consolidated its product portfolio down to two offerings, Workspace Edition and Enterprise Management Pack. Plus, IGEL released new software maintenance and support offerings that enable our customers to always stay current with the latest updates while providing enterprise support.

The base product is called **Workspace Edition**, which provides the core IGEL OS and the enterprise-class Universal Management Suite (UMS). Workspace Edition also incorporates the Multimedia Codec Pack (MMCP), UMS High Availability (HA), IGEL Management Interface (IMI) programming interface, the ability to install your applications via Custom Partitions.

If you require additional enterprise capabilities, IGEL released the **Enterprise Management Pack**, which includes remote device management, asset tracking, user-specific settings (Shared Workplace), and IGEL Cloud Gateway. The Enterprise Management Pack allows secure management no matter where the endpoint is located. For example, a home office.

3. 2. IGEL Workspace Edition

The IGEL Workspace Edition acts as the base product and comprises the core components required to deliver, manage, and maintain devices. Workspace Edition is offered as a transferable license, meaning you can deploy a Workspace Edition license to one device and then move it to another device in the future. Using the new approach, you can move licenses around every day if you want. In the past, you could transfer a license, but only if a licensed device were retired due to hardware failure, and then you could only transfer the ownership in the first year. Now your Workspace Edition license is your license forever.

Workspace Edition consists of the following components:

3. 2. 1 IGEL OS

The genius of the IGEL solution is the IGEL OS client operating system. From day one, IGEL designed the IGEL OS to be very simple, flexible, secure and centrally managed.

The IGEL OS is a modular operating system that will run on almost any x86 64-bit machine with minimal resources. The IGEL OS runs physically on a device, like any other operating system. You can choose to install the IGEL OS directly on traditional PC hardware, including laptops, and select tablets. You can also run IGEL OS on unique form factors like Intel NUCs or in a virtual machine. You can boot to the IGEL OS from an existing PC or Mac using the IGEL UD Pocket USB thumb drive without conflicting with currently installed operating systems. You can even install the IGEL OS on thin-client hardware from other companies like Dell and HP. Of course, you can still buy traditional thin client-style hardware from IGEL.

Not to mention, IGEL announced a new version of IGEL OS for the Arm platform and explicitly running on the NComputing Raspberry Pi hardware. For more information on this offering, please visit the **IGEL OS(RPI4) for Arm architecture** page on igel.com.

- **Product Page** & **KB Home Page**

Multi-media Codec Pack

Today's world is graphically intense and includes an abundance of multimedia content. To gives the best user experience in a virtual environment, it is best to render audio and video content locally on a device when multimedia content is encountered; however, doing so requires the appropriate codecs to decode media content rendered on the device.

In recent years, remoting protocol developers like Citrix (HDX), VMware (BLAST Extreme), Microsoft (RemoteFX), and NoMachine (NX) started using the H.264 multimedia codec to enhance their display primitives. This approach allowed for leveraging hardware-based media decoders on the endpoint; however, doing so requires the H.264 codec on the device for decoding the remoting protocols.

For years, IGEL has partnered with the leading codec vendor Fluendo to provide you with award-winning codecs for MP3, WMA, AAC, WMV (VC1), H264, MPEG-4, and MPEG-2; however, this was a charge feature. Now with the IGEL Workspace Edition, multimedia codecs are included with every license.

Learn more, view a list of **Supported Formats and Codecs.**

3. 2. 2 Universal Management Suite

The brain behind the genius of the IGEL OS is the IGEL Universal Management Suite (UMS), and its job is to allow IT to manage any IGEL OS easily.

The IGEL UMS provides you with the ability to fully automate the deployment, management, and maintenance of your devices. You can quickly enroll, index, manage and update all endpoints from the in-depth backend system. It is all done in an easy-to-use drag-and-drop interface with over 7,000 possible configurations. The sky is the limit, and flexibility is the outcome.

Out of the box, the IGEL UMS is scalable! For example, IGEL has a customer with over 30,000 devices in over 5,000 global locations. Only one person manages all this, and she does not even log in to the UMS, but once or twice a month, as once you configure your environment, you are not required to change it unless you desire. That is what I call scalable, manageable, powerful, and again flexible!

- **Product Page** & **KB Home Page**

Custom Partitions

The IGEL OS is a Linux operating system based on the Ubuntu Linux distribution but using a mainline kernel for maximum hardware compatibility and flexibility. Properly deployed, IGEL OS is locked down to the configurations and applications defined via UMS Profiles. The Custom Partitions feature allows you to deploy custom scripts, apps, or other files to one or a group of devices running the IGEL OS.

Typical use-cases might include deploying Google Chrome, Zoom, Microsoft Teams, Avaya Agent for Desktops call center application or a Linux version of a line-of-business application. For example, IGEL has a retail industry customer who installs their POS software directly to the IGEL OS to create a fully centralized solution for implementing and maintaining their devices anywhere, easily. Everything runs locally.

- **KB Custom Partition Tutorial**
- **IGEL Community Custom Partition Store**

High Availability (HA)

IGEL High Availability (HA) allows IT to build a network of several UMS management servers to ensure new settings are rolled out to several hundred devices at once or in environments where the fail-safe rollout of new configurations is mission-critical for an organization concerned. The HA feature is now included with every IGEL OS license, and it provides high availability, load balancing, and redundancy to the IGEL investment.

- **KB Home Page**

IGEL Management Interface (IMI)

The IGEL Management Interface (IMI) adds a REST API interface to the UMS. This gives IT the ability to connect to existing enterprise management systems (such as Microsoft SCCM, IBM Tivoli, and ServiceNow). Also, IMI provides the interface for REST-compatible programming languages, allowing you to create custom scripts or programs to enable further integration and automation.

- **KB Home Page**

3. 3. Enterprise Management Pack

The Enterprise Management Pack is a set of IGEL UMS extensions offered as a subscription-based license to enhance the enterprise capabilities of your IGEL environment. With the Enterprise Management Pack, you can manage devices residing in far-reaching locations like remote offices and work from home users through a secure connector.

- **Product Page**

The Enterprise Management Pack consists of the following components:

3. 3. 1 IGEL Cloud Gateway (ICG)

The IGEL Cloud Gateway (ICG) was designed as a secure connecting point for IGEL OS devices to communicate with the UMS from outside the corporate network without a VPN requirement. The ICG acts as a secure gateway between the IGEL OS and UMS. Although the ICG is not required to manage IGEL OS devices, it allows IT to securely and actively manage endpoints that are not part of the corporate network. The ICG is the perfect solution for remote offices, work from home users, and users utilizing IGEL's UD Pocket.

- **KB Home Page**

3. 3. 2 Asset Inventory Tracker (AIT)

Asset Tracking allows IT to perform the vital task of understanding what peripherals are attached to IGEL-managed devices at any given time. Besides providing a tool to help standardize peripherals, asset tracking helps ease hardware and software management, regulatory acquiescence, security, and license compliance.

The Asset Tracking feature collects and presents USB and Bluetooth assets connected to IGEL OS endpoints in the UMS, such as printers, scanners, smart card readers, etc. You can combine IGEL management with your existing asset management software via the IGEL IMI programming interface for complete control over your peripherals throughout the entire lifecycle. With over 80 integrated technology partners, this asset

tracking capability can provide great insight into all your connected peripherals!

- **KB Home Page**

3. 3. 3 Shared Workplace (SWP)

Shared Workplace (SWP) allows users to share endpoint devices and have their unique configuration applied to a device. The feature is made possible by tying user configurations to individual user accounts (or groups) in their Active Directory or other LDAP environments.

A typical use-case for the user-specific settings feature is when devices are used for shift work or call centers. Different users might use the same machine but need user-specific configuration settings, such as applications or mouse-button configuration for right/left-handed operation.

Another everyday use can be found in roaming environments, where users frequently switch workstations, such as in hospitals and at service/ticket counters, checkouts (POS), and customer reception areas. After a user logs on, the device automatically receives the user's corresponding configuration from the UMS and uses it to set up the user's environment as desired.

- **KB Home Page**

As you can tell, the Enterprise Management Pack is loaded with features to allow IT to manage remote devices securely, get a better understanding of your peripherals, and deliver a personalized experience no matter where users are working. All this extends the easy, secure, and flexible mantra that IGEL has promoted for years.

3. 4. Licensing 101

The most significant change in the IGEL Software Suite is licensing. In this section, I will share with you the workflow of licensing your devices.

The first thing you are required to do is procure a license. This can be done by either purchasing or by downloading three free licenses from igel.com. Depending on the type of license, a free or paid license will define how you move forward. The following workflow assumes you purchased the IGEL licenses.

The license is delivered via email in the form of a Delivery Token. This Delivery Token is what you will add to the IGEL License Portal. To do this, you will need an account. You can link to the account creation wizard from the IGEL Licensing Portal's sign-in page.

Once you log in to the IGEL License Portal, you will be challenged to add a new license. This is where you will enter the Delivery Token. Once you add your token to the IGEL License Portal, you have options. You can manually register your hardware, and the IGEL License Portal will create the license file for you to download and then upload it to the IGEL UMS. Alternatively, you can create an Automatic License Deployment ("ALD") token that you can add to your IGEL UMS. With the ALD, the IGEL UMS will "automagically" request a license from the IGEL License Portal of any unlicensed device running the IGEL OS. The ALD method is a fully automated solution for IGEL Licensing.

You will need to license your devices before using them. By default, all features on the IGEL OS are disabled until its licensed. You can still boot your machine and run the Setup Wizard set up to join the UMS and download a valid license and any configurations. At this time, the device is ready to be used by a user.

If your IGEL OS devices are out of software maintenance, the IGEL OS will freeze to the most recent OS version as of the expiration date. If your Enterprise Management Pack subscription is expired, the assigned devices will no longer be able to take advantage of the benefits of the pack. Very straightforward.

As always, easy like pie, and we think you will love the new IGEL Licensing Portal as it is packed with great statistics for understanding how and where your licenses are used.

3. 4. 1 Evaluation Licenses

The IGEL evaluation license enables you to test all the features of the IGEL Software Suite, including the Enterprise Management Pack. It is a full license, with no functionality omitted or crippled in any way.

The evaluation license enables the following features:

- IGEL OS
- Multimedia Codec Pack
- High Availability
- IGEL Cloud Gateway
- Shared Workplace
- Asset Tracking
- Custom Partitions

The evaluation license is valid for 90 days from the date you procure the license until the license expiration. If an IGEL OS evaluation license is expired and there is no other license in the system to be assigned to the device in question, then the device behaves as if no license has been installed. The base functionality stops working, and users are no longer able to connect to their applications.

> **Important!** The IGEL OS ships with a "starter license". This license allows you to get up and running in case you do not have the ability to 1) properly license the device right way 2) not able to connect an evaluation license (the 90-day license). It is very important to understand, the starter license does NOT ship with the Multimedia Codec Pack and hence the user-experience will be degraded when doing multimedia, basically most tasks a user does in the modern age. Hence, this license is meant to get your started and NOT for testing and never for production use. If you wish to test the IGEL OS, please register for the 90-day evaluation license, as documented later in this guide.

3. 5. Software Maintenance & Support

Starting with IGEL OS 11, IGEL is offering software maintenance. Software maintenance allows customers to stay current with the latest firmware updates and product upgrades. It also maintains the 'license portability' feature.

Without software maintenance, IGEL OS licenses are entitled to one year of firmware updates and upgrades. After that date, the IGEL software version freezes to the most recent version as of the expiration date. When a device is out of maintenance, you cannot update its firmware, nor will you be able to transfer the license to another device, known as "license portability."

When you are on software maintenance, you also receive the **Select Support** tier of IGEL enterprise support at no additional cost.

Software Maintenance is offered in 1, 3, and 5-year options.

If you require an advanced IGEL support program, IGEL offers two more levels of enterprise support.

- **Priority Support** – Enterprise-class Web, email, phone, and remote access support. Monday – Friday, standard business hours coverage, next business day response, four business hours critical response.
- **Priority Plus Support** - Enterprise-class web, email, phone, and remote access support. 24x7, four business hours response, two hours critical response.

▸ **Learn More**

3. 6. IGEL Advanced Services & Training

IGEL created an Advanced Services division that offers the following solutions for customers and partners:

3. 6. 1 IGEL Consulting Services

IGEL offers professional consulting services based on structured processes built up from IGEL's extensive knowledge and experience. IGEL Consulting Services provides many different offerings, from custom engagements to the following predefined services:

Milestone Based Offerings

- Quick Start Standard
- Quick Start Enterprise
- Quick Start Enterprise+

Deliverable Based Offerings

- IGEL Environment Health Check
- IGEL Implementation Design Session
- Business Continuity Accelerator
- Production Pilot

▸ **Learn more**

3. 6. 2 IGEL Technical Relationship Manager (TRM)

IGEL TRMs are long-term dedicated IGEL trusted advisors and industry subject matter experts who can assist with the technical needs of customers to ensure a successful IGEL implementation and management. IGEL offers multiple levels of TRM services:

- Premier TRM
- Enterprise TRM
- Enterprise Plus TRM

▸ **Learn more**

3. 6. 3 IGEL Education

It is here! IGEL offers formal training courses on IGEL products geared towards beginners and experienced users alike. IGEL training consists of both online and in-person classroom courses, whatever fits your needs and requirements.

IGEL Academy - LMS (Learning Management System)

Welcome to the IGEL Academy, IGEL's Learning Management System (LMS), the home for IGEL Education, online course, certification, and more. IGEL has both a free and premium (paid) model for the Academy. Learn more and join today. You will love it.

IGEL Instructor-Led Training Services

In addition to the training available through the IGEL Academy LMS learning portal, customized on-site training can be made available for larger numbers of students within one organization. You will receive:

- An on-site trainer prepared to instruct up to 15 students – Where possible and permitted due to Covid travel restrictions
- Hands-on experience via labs for each student
- Vouchers for up to 15 students to take the IGEL Certification exam
- PDF of training materials, including the slides presented during the course

IGEL Certification Program

IGEL has enhanced its certification program by offering multiple tracks, depending on your level and if you are technical or sales.

Today, IGEL offers the following certification levels:

- IGEL Certified Professional (ICP)
- IGEL Certified Engineer (ICE)
- IGEL Certified Sales Professional (ICSP)

Once you complete the certification, you will have instant access to your certificate and award logo, all through the IGEL Academy LMS learning portal.

- **Learn more about the IGEL Academy**
- **Join the IGEL Academy**

3. 7. Customer Onboarding

IGEL cares, and we want to make sure our customers are as happy and productive as possible. One of the services we have implemented to help accomplish this vision is a formal onboarding process.

If you are new to IGEL or even an existing customer, you may not be aware of our latest services and updated content available ONLY to IGEL customers. Hence, we would like to onboard or reboard you!

You will chat with one of our specialists and can ask questions, give feedback, and will be brought up to speed on the following:

- **IGEL Account(s) Creation** – IGEL License Portal, Support, IGEL Community
- **IGEL Community Resources** – a community platform for "all things IGEL" created for IGEL customers, partners, and employees. A place where you can learn, collaborate, meet like-minded IT Pros, grow technically, and get help supporting IGEL software and thin client solutions.
- **Technical Support** – a review of the three different IGEL support offerings
- **IGEL Academy** – an online learning platform that includes certifications for advanced skillset achievements.
- **Advanced Services Offerings** – a review of IGEL service offerings and packages. The best in IGEL expertise, straight from the source.
- **Who is Your IGEL Team** – who should you call when you need IGEL assistance (or have a question)? Your IGEL team stands ready to assist.

We feel this will bring you up to speed with what is new at IGEL and all the benefits and offerings you have at your disposal.

If you are interested, please learn more and apply for an appointment **here**.

Installation

1. Installation and Infrastructure Considerations

The goal of this guide is to allow you the tools and knowledge to set up the IGEL Software Suite as a simple proof-of-concept in your lab. For this purpose, you are not required to worry about high availability, 3rd party databases, etc. We will discuss the basics and include links to more advanced resources to learn more about a subject.

The necessary infrastructure requirements you need to complete the steps in this guide are as follows:

- One physical, cloud instance, or virtual server to host the IGEL UMS software
- An AWS account with the ability to create a free tier Linux server instance to host the IGEL Cloud Gateway (ICG) software (optional)
- x86 64-bit device to install the IGEL Workspace Edition. For a lab environment, you can install it in a virtual machine. No physical device required.

IGEL provides detailed documentation and support articles at **https://kb.igel.com**. This guide is not meant to be a replacement for reading the official administrator guides.

For testing, you can deploy the IGEL Software stack in an Oracle VirtualBox or VMware Workstation virtual environment. For my lab, I have installed the UMS and IGEL OS in VirtualBox virtual machines, and the ICG is running on AWS.

To ICG or not to ICG? This is the Question!

For a basic lab deployment, you are not required to install the IGEL Cloud Gateway. The ICG comes in handy when you are deploying and testing any IGEL-managed device located outside your physical network. It acts as the secure broker to allow the UMS to connect with the IGEL OS without using a VPN. Thus, by installing the ICG, you can thoroughly test the IGEL solution and roam throughout the world with a UD Pocket and any IGEL OS-based device.

If you do not already have a UD Pocket to play with, please **join the IGEL Community** and message me. One might find its way to your door.

To successfully install the IGEL Software Suite, you are required to perform the following tasks:

- **Install the IGEL Workspace Edition's required components**
  - Download IGEL Software
  - Install IGEL Universal Management Suite (UMS)
  - Install IGEL OS
  - Register IGEL OS with the UMS
  - Create a basic folder structure
  - Create basic UMS Profiles
  - Customize the look and feel to your pleasing (optional)

- **Install IGEL Enterprise Management Pack (optional)**
  - Create an AWS Instance for ICG
  - Open Firewall Ports Required by ICG
  - Create Required DNS Records
  - Create and install an SSL Certificate to ICG
  - Perform a remote install of the IGEL ICG Software via the UMS
  - Configure the ICG device authentication method
  - Configure IGEL OS to use ICG

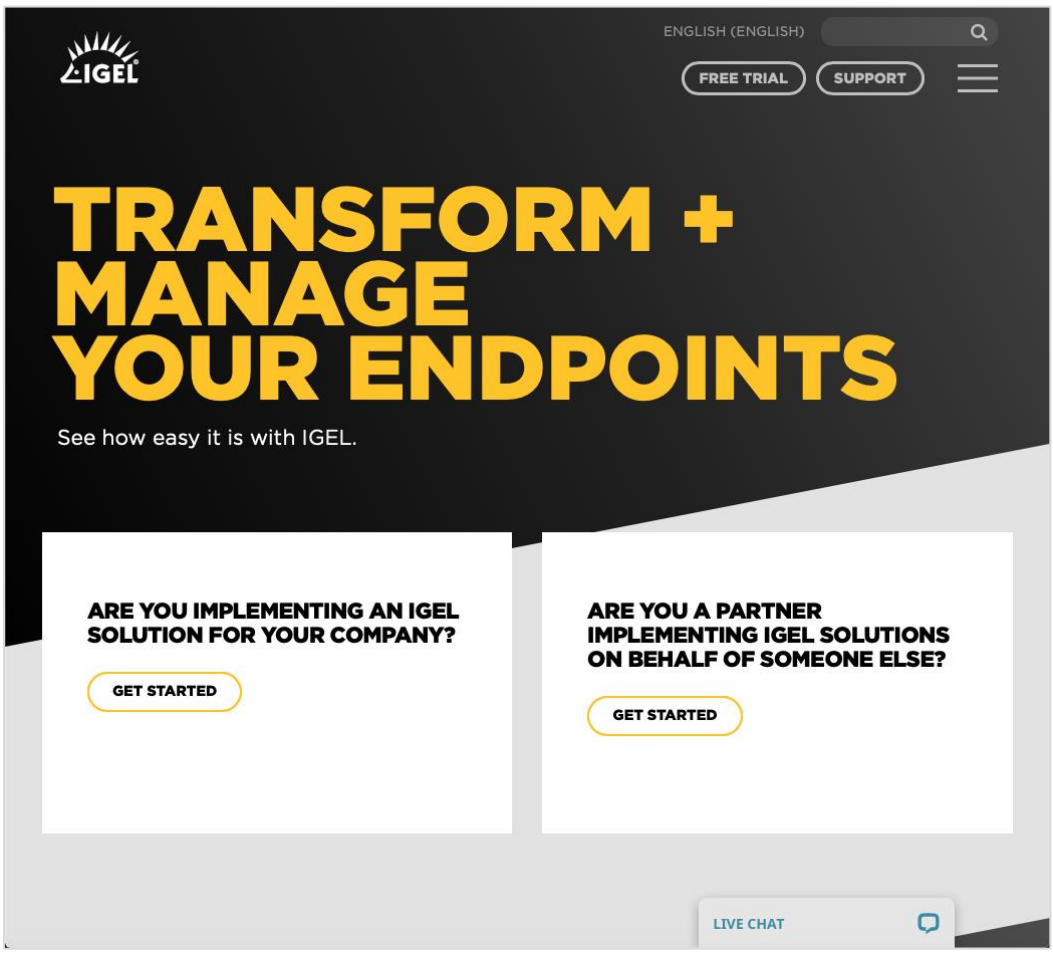
2. Download IGEL Software

The first step is to get your hands on the latest IGEL software. No worries, IGEL makes this easy. For your testing enjoyment, IGEL provides you free 30-day trial licenses that include both the Workspace Edition and all Enterprise Management Pack features fully activated.

> If you are deploying the IGEL Cloud Gateway software, you are required to download it separately. You will install it in a bit. Hold your horses!

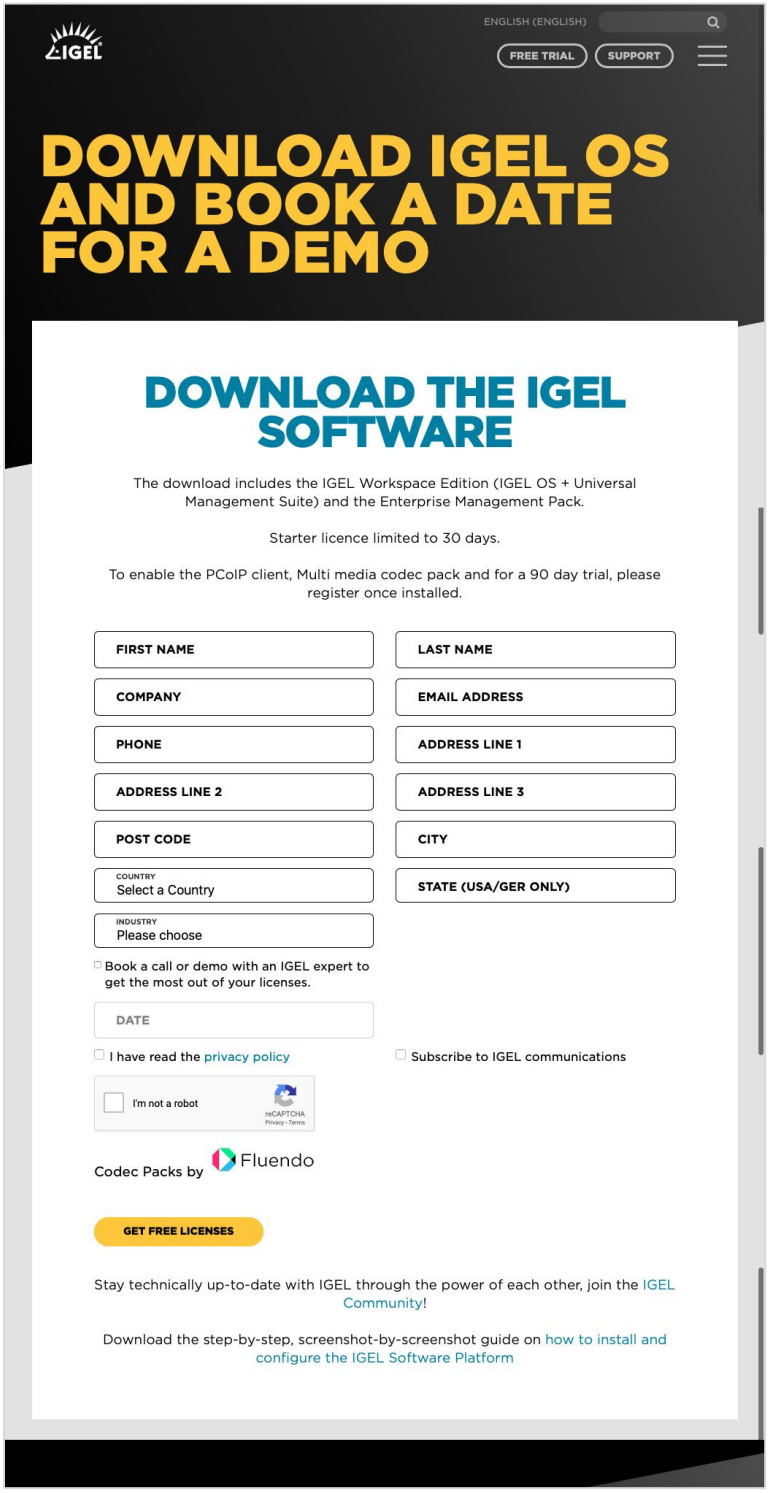
The following steps walk you through downloading the IGEL Workspace Edition and Enterprise Management Pack:

1. Open your favorite browser and browse to **https://www.igel.com/download/**. Depending on if you are a customer or partner, click the appropriate button to continue.



2. You are brought to the **Download the IGEL Software** page. Please fill out the required text boxes, click to check the **I have read the privacy policy** checkbox, click the **I'm not a robot** checkbox and comply with the captcha question(s).

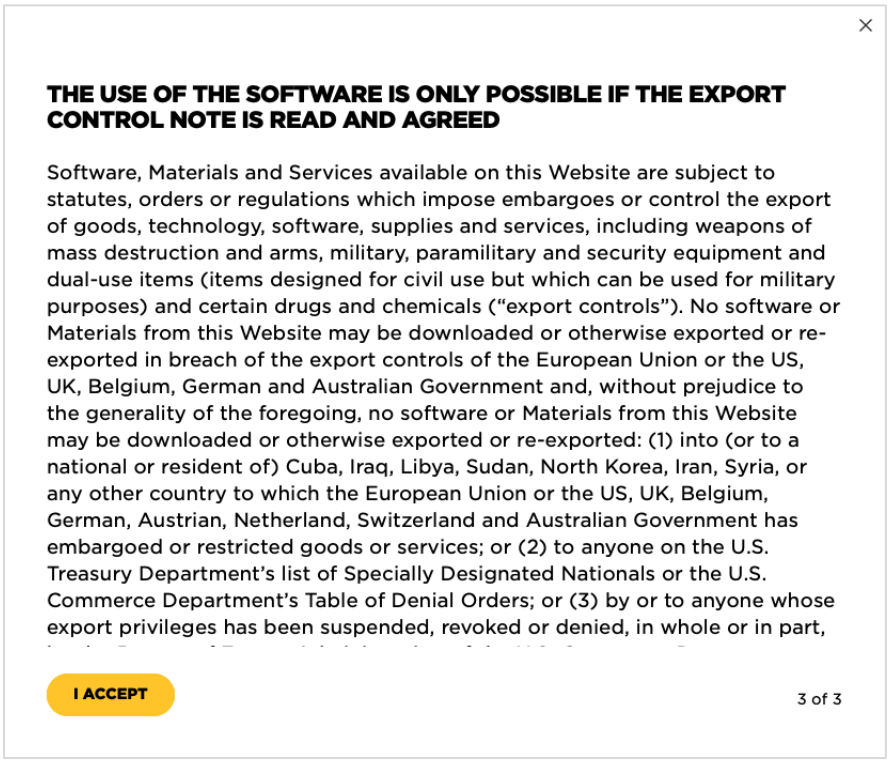
   Once finished, click the **GET FREE LICENSES** button.



3. Read the IGEL EULA and click the **I ACCEPT** button to continue.

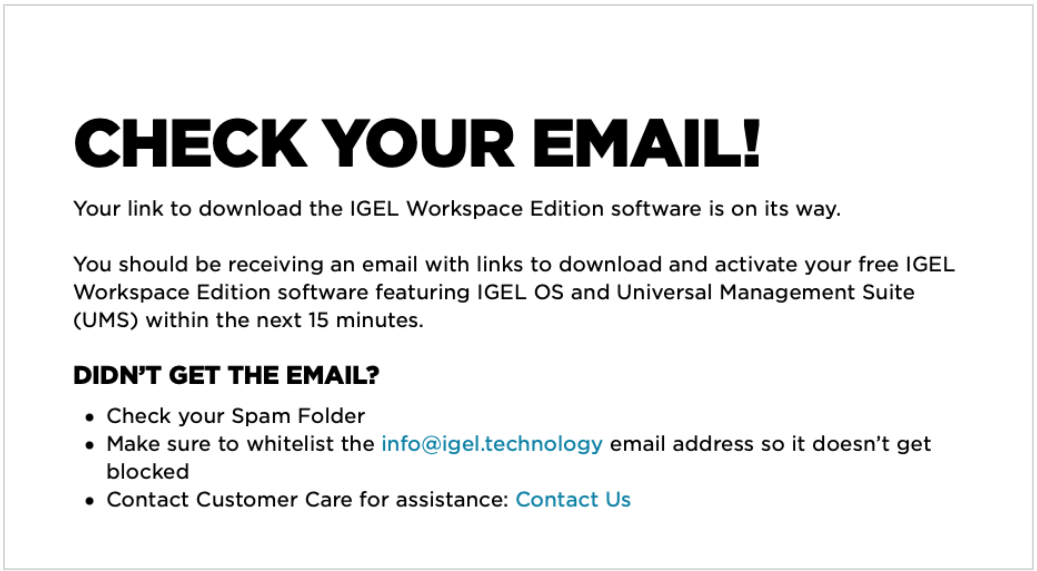
4. Click the **I ACCEPT** button to accept the embedded solutions EULAS found in the IGEL OS.

5. Click the **I ACCEPT** button to accept the export control agreement

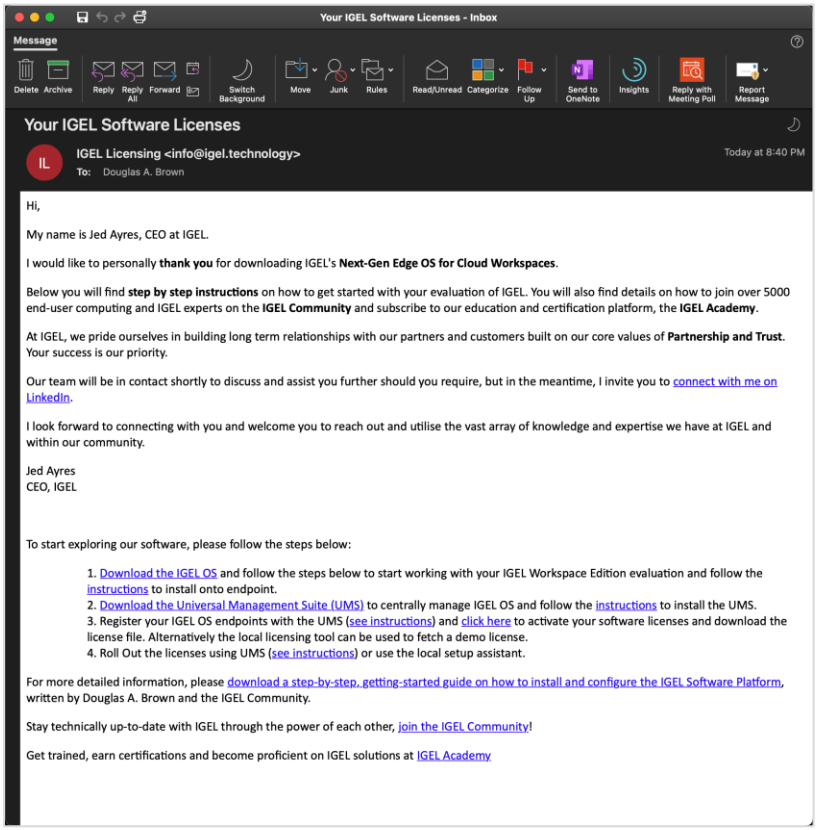


6. You are done. IGEL will send you an email with the desired download links and other information.

   If you do not receive the email in your inbox within a couple of minutes, please check your **Spam** folder. If you find the email in your spam folder, please move it to your inbox and click to open it.



7. Find the email from IGEL Licensing and open it. Once opened, the email should look something like the following. Don't worry about all the links. We walk you through every step and make this process as pleasant and straightforward as eating pie! After all, who does not love a piece of cake? Let's move on!



8. In the above email, there are only two links you should concern yourself with, and they are the links to download the software.
    - **IGEL UMS** - Click the **Download the Universal Management Suite (UMS)** link in the email above to download the IGEL UMS Windows installer package.
    - **IGEL OS 11** - Click the **Download the IGEL OS** link in the email above. The IGEL OS download zip file will contain everything required to install the IGEL OS directly on x86 hardware or in a virtual machine. Once downloaded and extracted, you will find the IGEL OS ISO image used to install the IGEL OS into a virtual machine or onto a USB thumb drive/CD.

After downloading the above two files, you are ready to get started! Let's get to installing the IGEL Software Suite. The first step is to install the IGEL Universal Management Suite (UMS).

Let's get going! The fun is afoot!

3. Install IGEL Universal Management Suite (UMS)

The first thing we will do is install the IGEL Universal Management Suite (UMS). The IGEL UMS is a Java-based server application that is installed on either Linux or Windows.

UMS on Linux

In the following guide, you will learn how to install the UMS on Windows, although you can install the UMS on Linux too.

Currently, if you are installing from the IGEL download zip file you downloaded above, you will only find the Windows version. You are required to download the Linux version separately.

The following IGEL KB article details how to download and install the UMS on a Linux server - **Installation under Linux.**

Learn more:

- **IGEL Universal Management Suite (UMS) Manual**
- **IGEL Universal Management Suite KB support home**

The process of installing the UMS is divided into the following four steps:

- Comply with the UMS System requirements
- Install the IGEL UMS software
- Install the UMS Console on a remote PC (Optional)

3. 1. UMS System Requirements

The following are the system requirements to install, configure, and run the IGEL Universal Management Suite (UMS).

- IGEL UMS supports physical, virtual, and cloud instances running Microsoft Windows or Linux (x86 and x86_64).
- Minimum 9 GB RAM free memory
- Minimum 6 GB of free storage space - By default, your database is installed on the server running the UMS. Storage requirements vary depending on the IGEL UMS database's size, which relies on the number of devices and policies you have configured.
- The UMS was NOT designed to be an Internet-facing server. To manage devices that are not on the same corporate network as the UMS, you must use the IGEL Cloud Gateway (ICG) or a VPN.

For additional information regarding IGEL UMS System requirements, please visit **https://kb.igel.com/endpointmgmt-6.06/en/installation-requirements-37281947.html**

View a list of supported environments here: **https://kb.igel.com/endpointmgmt-6.06/en/supported-environment-6-04-120-37282894.html**

> No matter the deployment's size, even when deploying in a lab environment, you are required to plan for and implement a backup strategy. Plus, during the installation of the UMS Server, a self-signed certificate is created. This certificate is of high importance, as it is added to all devices when they join the UMS. The UMS denies communications from devices that do not present themselves with the same certificate. Put in practice, if you have thousands of devices in your organization and the original UMS is lost, you are required to reset all devices to factory defaults, which might be an exhausting operation. Thus, it is highly recommended to back up the UMS server.
>
> To learn more about backing up the UMS, please refer to the following IGEL KB article **https://kb.igel.com/endpointmgmt-6.06/en/backups-37282869.html**.

3. 2. How to Install the IGEL UMS

You are ready to install the IGEL UMS software on a Windows Server. The following steps detail how to install the UMS in a Microsoft Windows environment:

1. First, you will want to configure the network to allow the client devices to find the IGEL UMS automatically without user interaction. When an IGEL OS boots, it attempts to establish a connection with a UMS server. The client looks for the UMS server by the name of **igelrmserver**.

   You can configure automatic client detection in two ways:

   1) Create a DNS entry - Create a DNS A record named '**igelrmserver**' with the IP address of the UMS server.

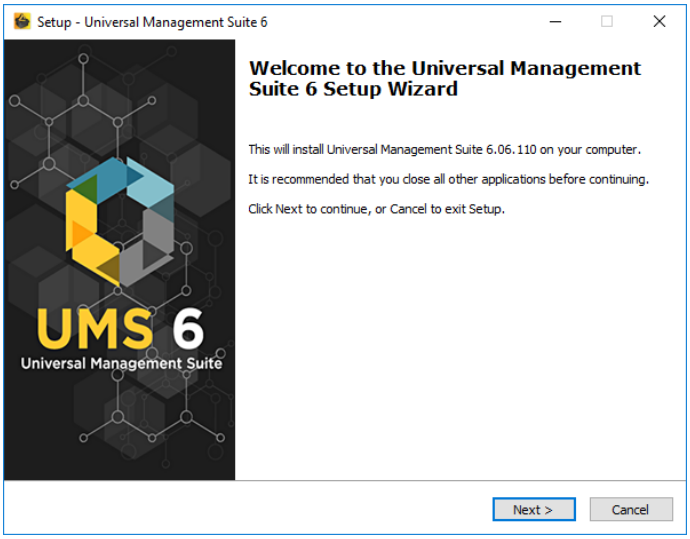
   2) Create a DHCP option (224) - Set the DHCP option 224 as a string, not a DWORD, to the IP address of the server by adding the following to the dhcpd.conf file in the appropriate section. For example, in the global area:

      option igelrmserver code 224 = text

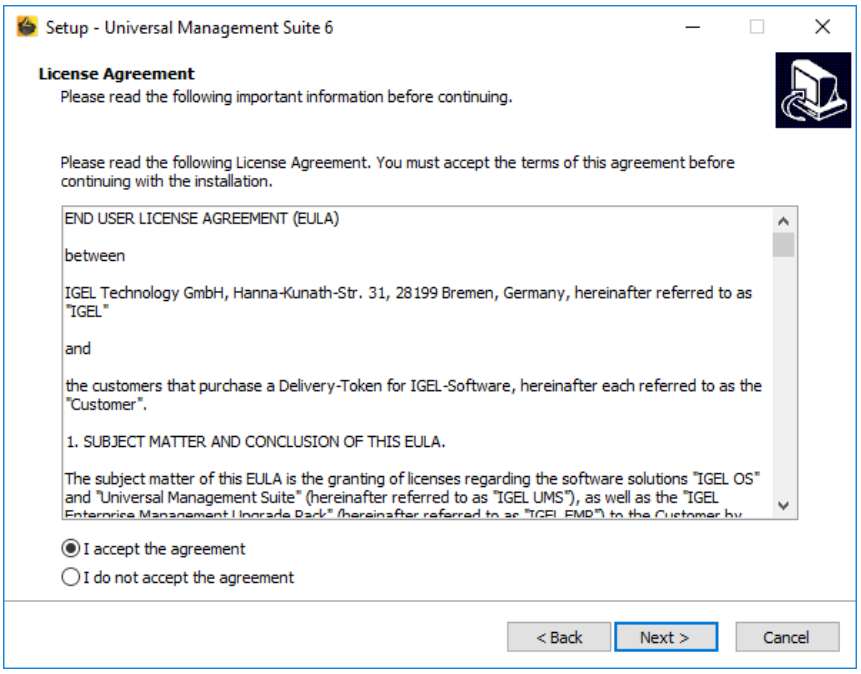
      option igelrmserver "<IP of the UMS server>"

> The above step is not required, although highly recommended. Learn more at **https://kb.igel.com/endpointmgmt-6.06/en/registering-devices-automatically-37282020.html**.

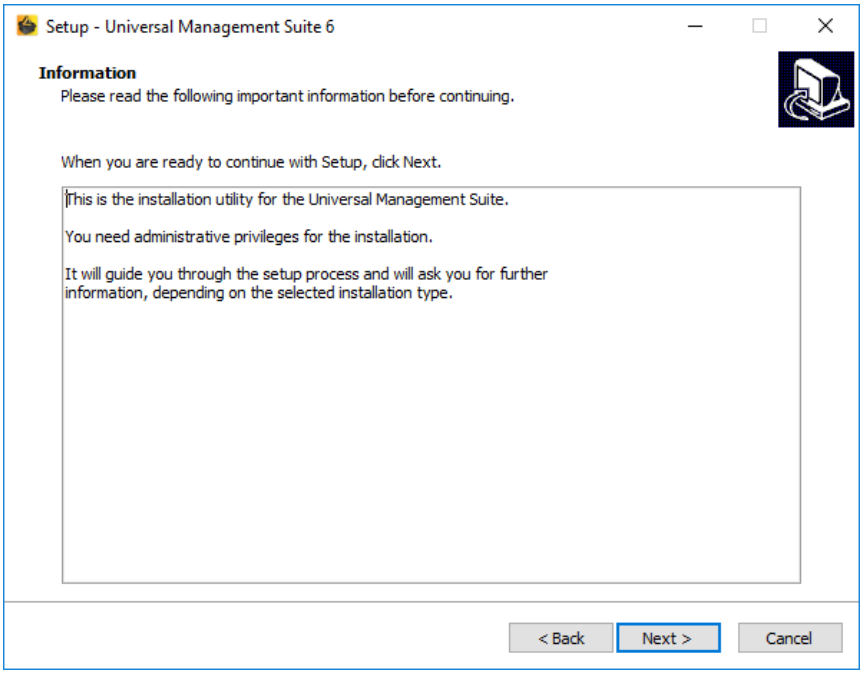
2. Copy the IGEL UMS installation program you downloaded above to the Window Server you wish to install the UMS on and double-click to execute the installation program. Click **Next** to continue.



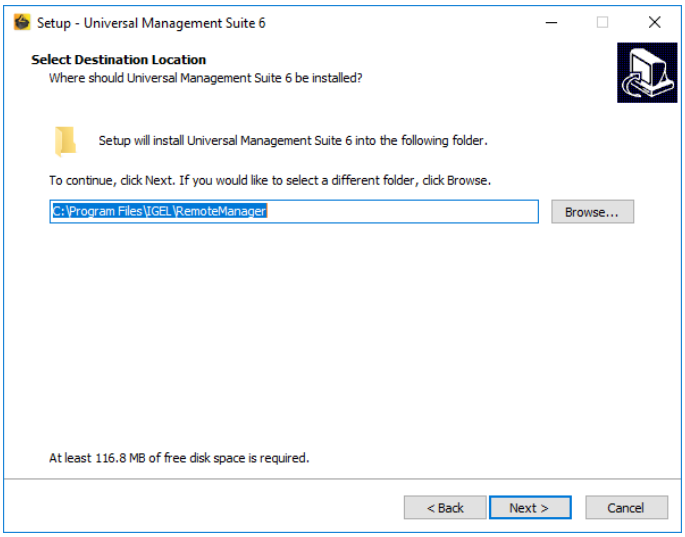
3. Read and agree to the IGEL UMS License Agreement. Click to select the **I accept the agreement** checkbox, then click the **Next** button to continue.



4. Click **Next** to continue.

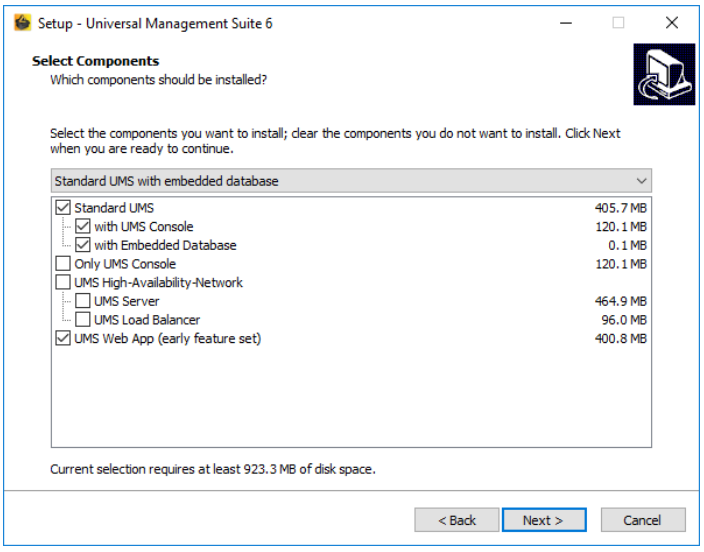


5. Enter the desired location to install the UMS system files and click **Next** to continue.



6. You are prompted to select the components you wish to install. For this example, please accept the defaults. Click **Next** to continue.

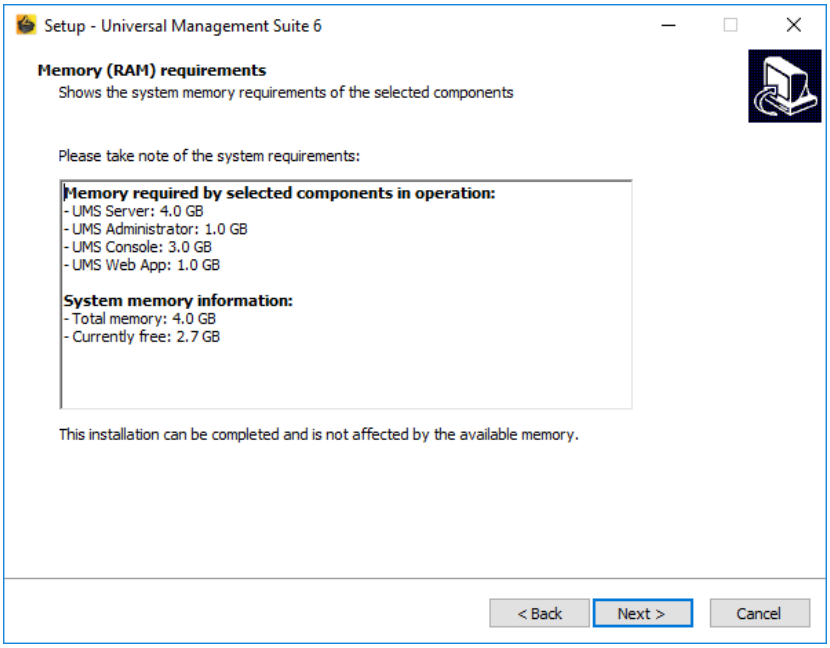
> Learn more about the different UMS components at **https://kb.igel.com/endpointmgmt-6.06/en/installation-on-windows-37281195.html**.



> Above you will notice the new UMS Web App feature. This feature is not covered in this guide, yet. For more information, please refer to the following KB article **https://kb.igel.com/endpointmgmt-6.06/en/ums-web-app-37283248.html**.

7. You are presented with the UMS memory requirement screen. Verify you meet the minimum requirements and click the **Next** button to continue.

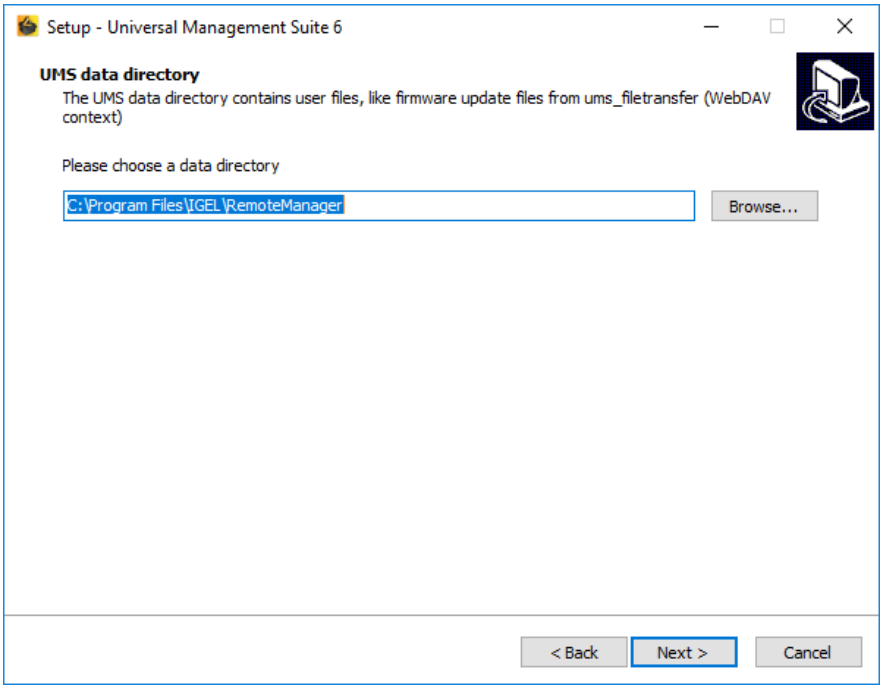
> For a default installation, the UMS requires approximately 500M in the beginning. It grows over the UMS deployment's lifespan. 2 GB would be sufficient for even the largest installations. Of course, this is excluding any IGEL firmware updates or windows snapshots. Firmware updates take up to 2 GB each, and Windows Images can be as large as 6 GB. Not to mention, if you are using the **Asset Inventory Tracking** feature, you might want to add additional space, depending on the size of your deployment, the number of devices you are tracking, and the number of images you plan to store. Please mind-your-step as you might find yourself running out of disk space.



8. Enter the location you wish to store the UMS data directory. The data directory is where large files, such as firmware, are stored.

> Be mindful of the location of the UMS data directory as it grows over time. It is highly recommended that you select an expandable volume.

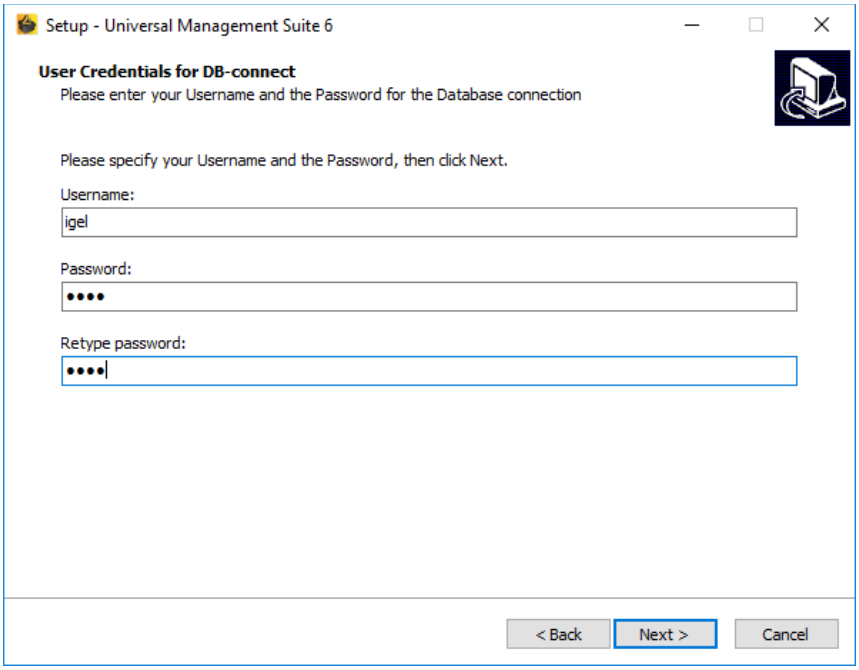
Click **Next** to continue.



9. Next, you are required to create the database's superuser account. The superuser account is used to login to the UMS and has full access to the UMS database. It is not a Windows user account but a user created specifically for the IGEL UMS.

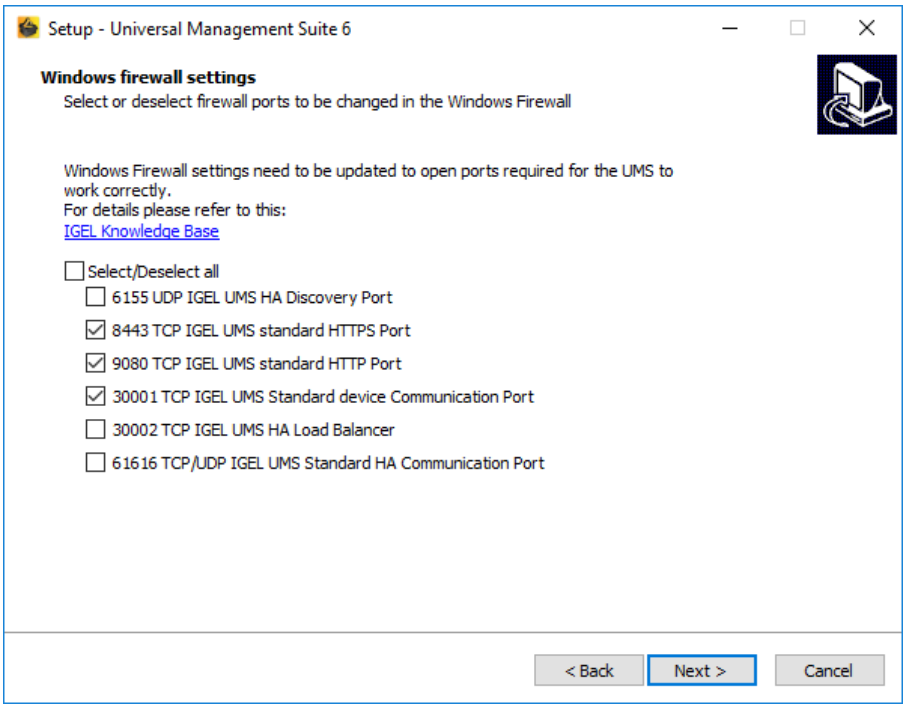
> Usernames and passwords are essential. Never use a username such as 'Admin' or 'Administrator' as if in the future you would like to move the database from the UMS to a dedicated MySQL server. The DBA might not want that. Plus, as always, follow stringent guidelines for passwords as if someone gains access, they learn the keys to your IGEL kingdom.
>
> Be aware, both the UseRnaMe and PaSswOrd are case-sensitive.

Enter the desired username and password and click **Next** to continue.

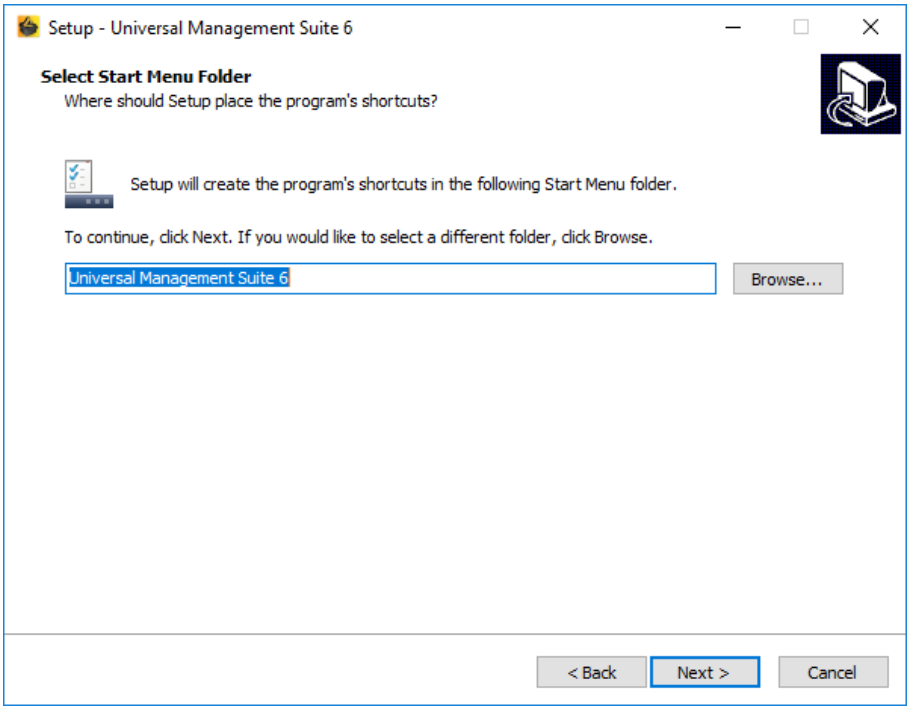


> On the UMS server, there is an application called **rmadmin.exe** (UMS Administrator). Within this application, you see the root UMS account name and can change the root UMS accounts password without knowing the original password.

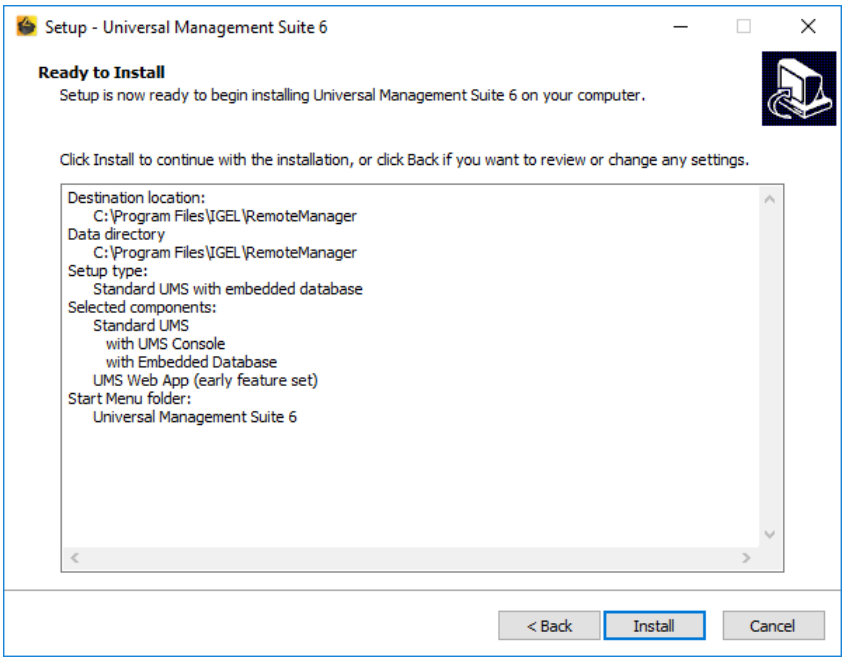
10. Next, you are prompted to select or deselect the firewall ports you will require opened or closed. Check the desired boxes and click the **Next** button to continue.



11. You are prompted to enter the location where the setup places the shortcut to the IGEL UMS server's console. Enter the desired location and click **Next** to continue.

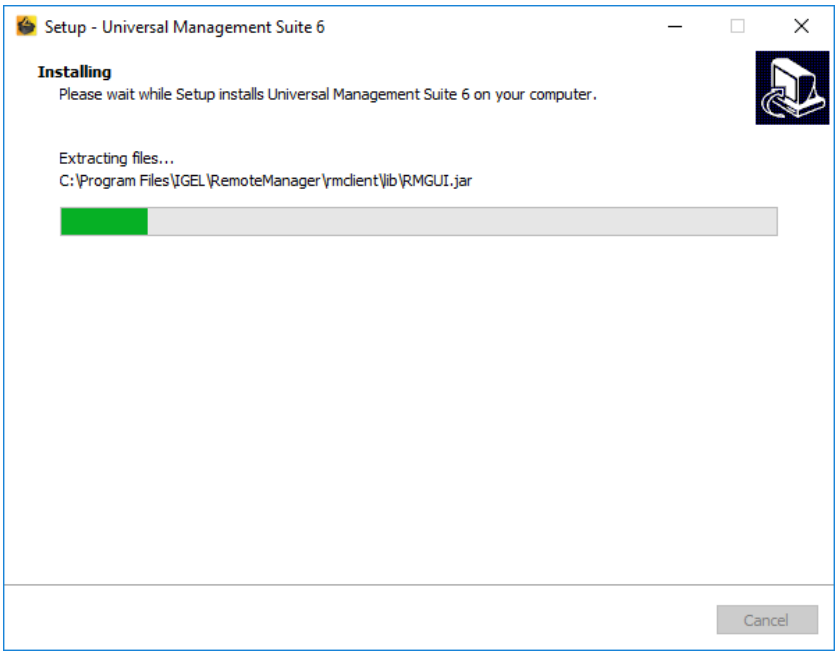


12. Please verify the settings are correct and click the **Install** button for setup to install the IGEL UMS.



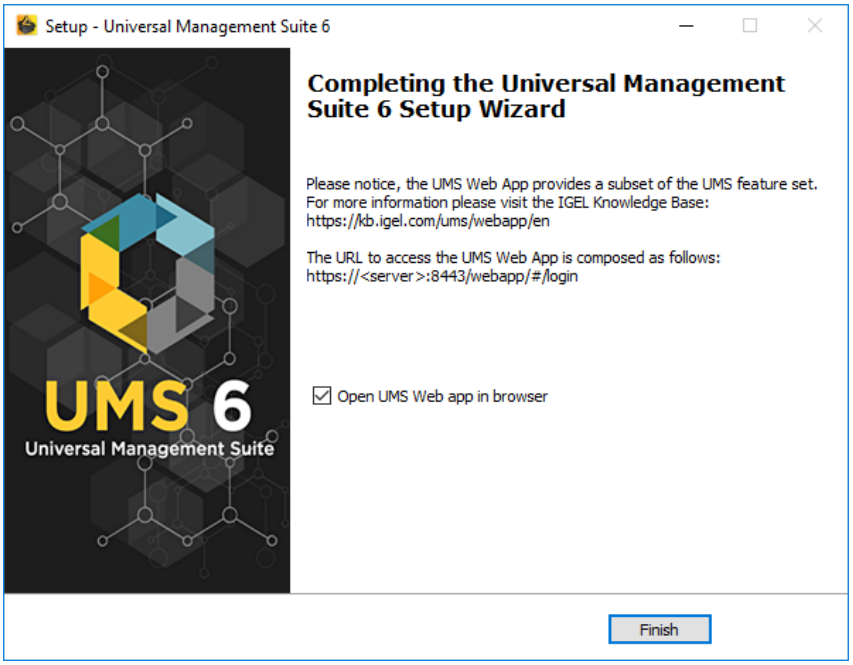
13. Depending on the speed of the server, this could take a few moments.

> It is possible that Virus software could prevent the installation program from properly installing the UMS due to the size of the UMS' .jar file. If you experience this issue, please disable any Anti-Virus and restart the installation.



14. If all goes as planned, you are prompted to click the **Finish** button to close the UMS installation program.

    Click the **Finish** button to continue.

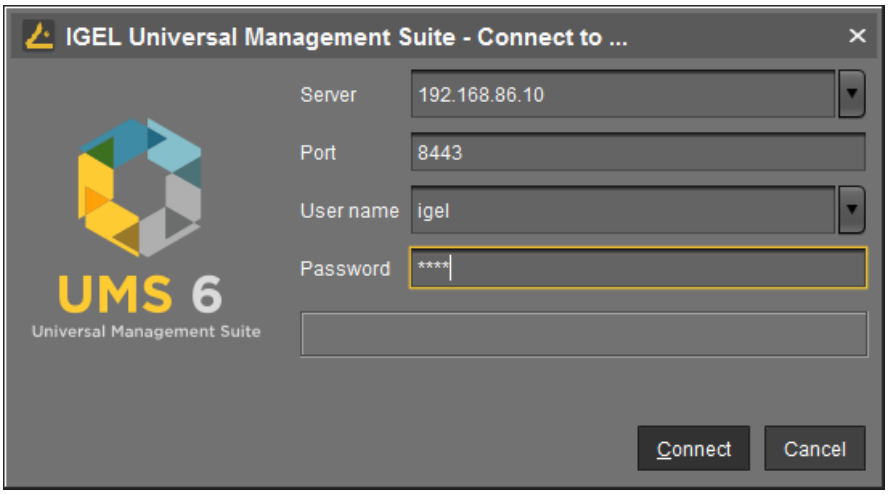


15. You notice the IGEL UMS Console's shortcut on the server's desktop or the location you specified during installation. Go ahead and double-click it to launch the UMS Console and login for the first time!

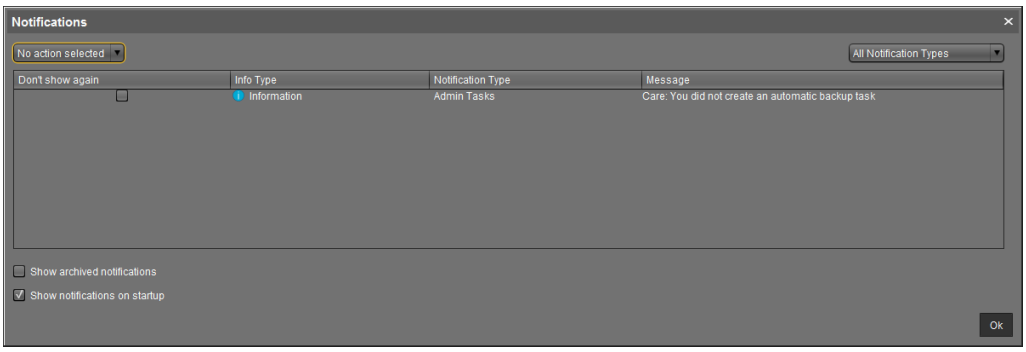
16. You are presented with the **IGEL Universal Management Suite - Connect to** screen. Since you are running the UMS Console from the server, there is no requirement to enter the server IP/DNS as it defaults to the local machine. If you previously created the '**igelrmserver**' DNS record, you could use it or '**localhost'.**

    Enter the default port number (8443), username, and password, as configured in step 8 above.

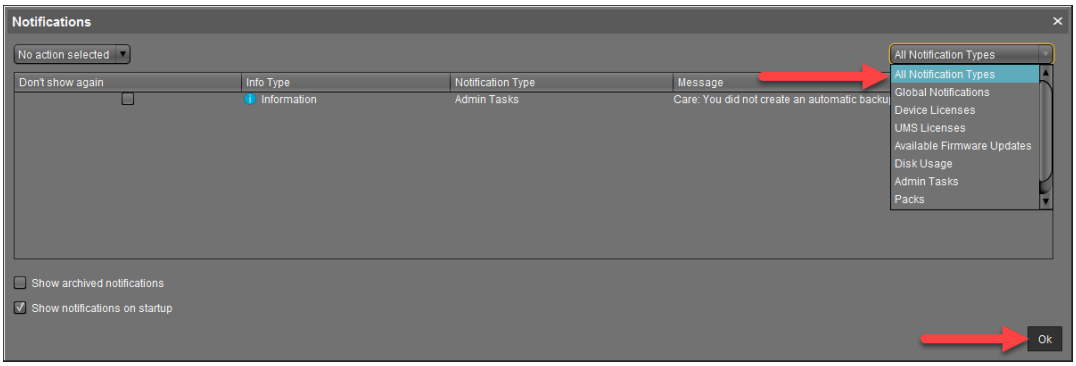
    Click the **Connect** button to connect to the UMS.



17. If the stars aligned or you correctly followed the above steps, you should see the UMS Console!

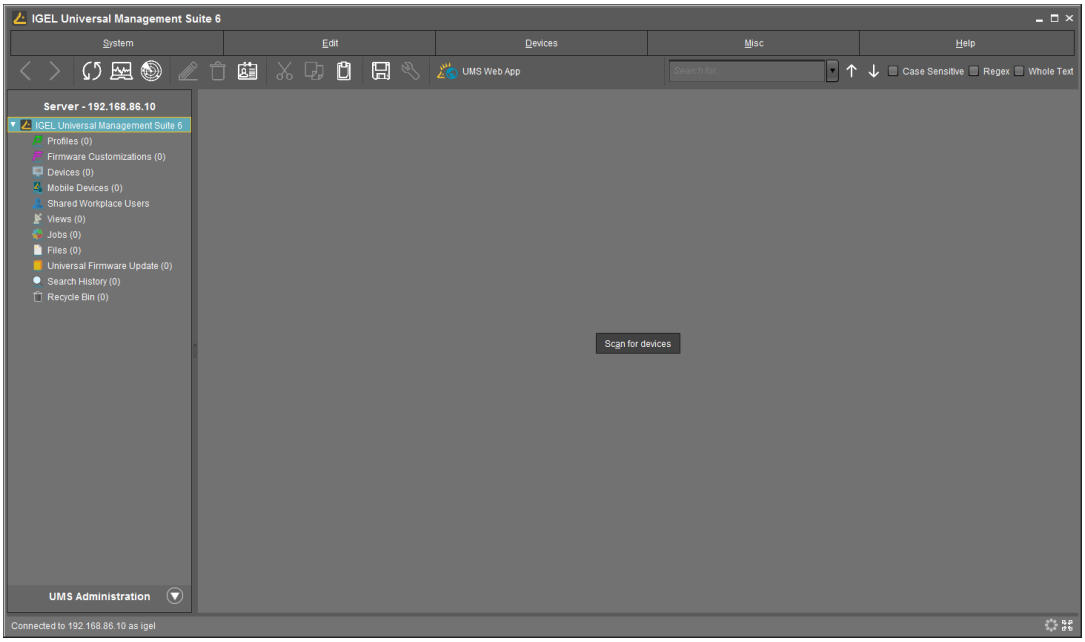


18. A new feature introduced in UMS 5.09.100 allows you to be notified of newly available IGEL OS updates, IGEL OS licenses, or UMS licenses. By default, the notification feature is enabled for all notification types. Select the desired setting and click the **OK** button to continue.



> Learn more about UMS notifications at **https://kb.igel.com/endpointmgmt-6.06/en/notifications-always-be-informed-37281473.html**.

19. You are brought to the UMS home page and are ready to start creating policies and adding IGEL clients. However, in due time my friend, you still have a bit of work left to do.



3. 3. How to Install the UMS Console on Remote PC

During the installation of the IGEL UMS, the administrator console was installed on the server, as shown above. If you wish to install it remotely, you can. This comes in handy if you want to log into the UMS from your local machine. For example, if the UMS server runs on Linux or a public cloud instance (AWS, Azure).

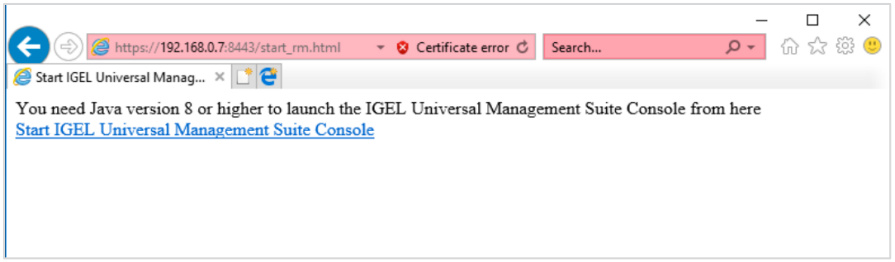
The UMS Management Console remote install has the following system requirements:

- Minimum 1.5 GB RAM (2 GB recommended)
- Minimum 250 MB free storage space
- Java Runtime Environment 1.8.0_40 or newer – Downloaded **here**.

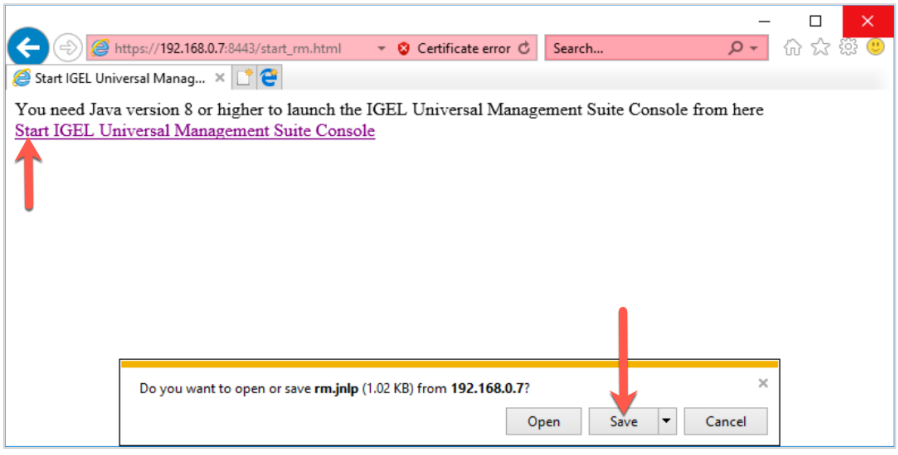
The following steps detail how to install the UMS Console on a remote PC.

1. Open the local browser and browse to **https://igelrmserver:8443/start_rm.html**.

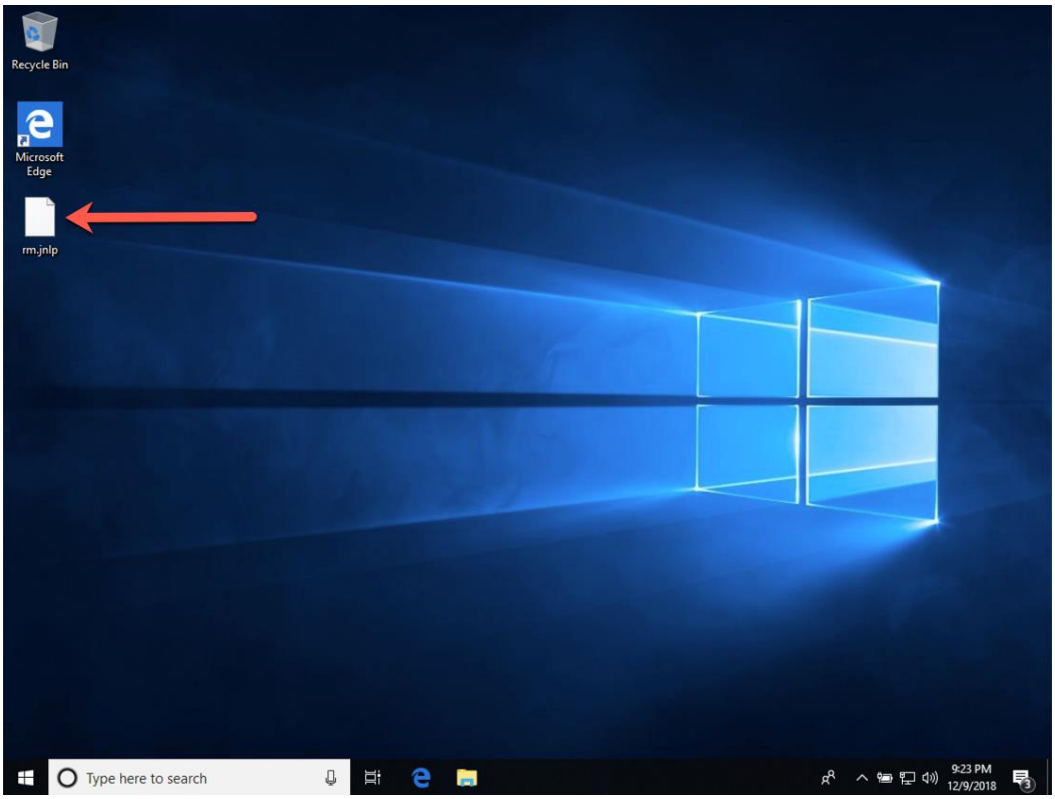
> If you did not create the '**igelrmserver**' DNS or DHCP setting as documented above, you are required to replace '**igelrmserver**' with the server name or IP address of the IGEL UMS server.



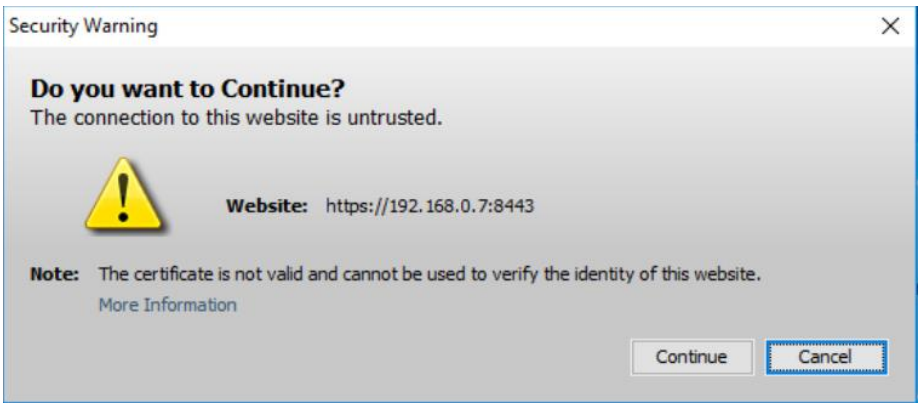
2. Click the **Start IGEL Universal Management Suite Console** link and click the **Save As** button to save the Java applet to the desired location.



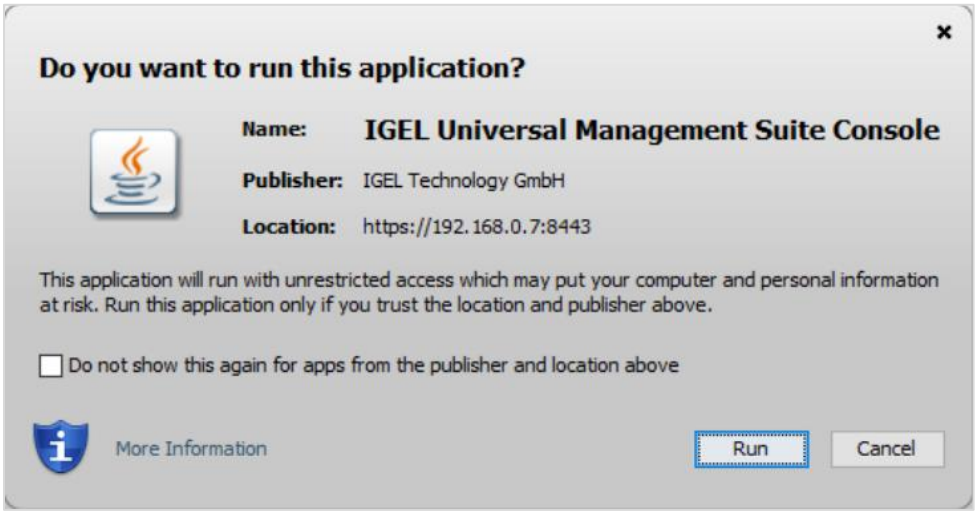
3. The Java app is copied to the place you defined above. Double-Click the **rm** shortcut to launch the IGEL UMS Console.



4. Click the **Continue** button to accept the security warning.



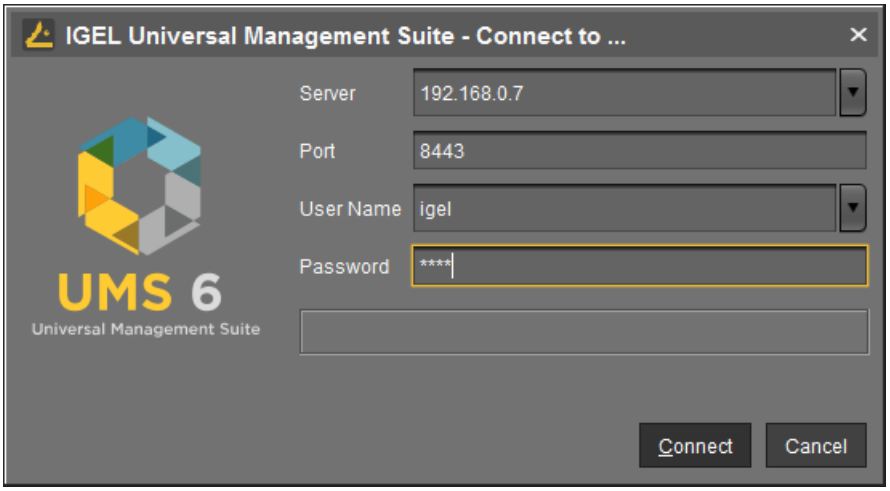
5. Click the **Run** button to accept the Java security message. Hopefully, you trust the fine folks at IGEL!



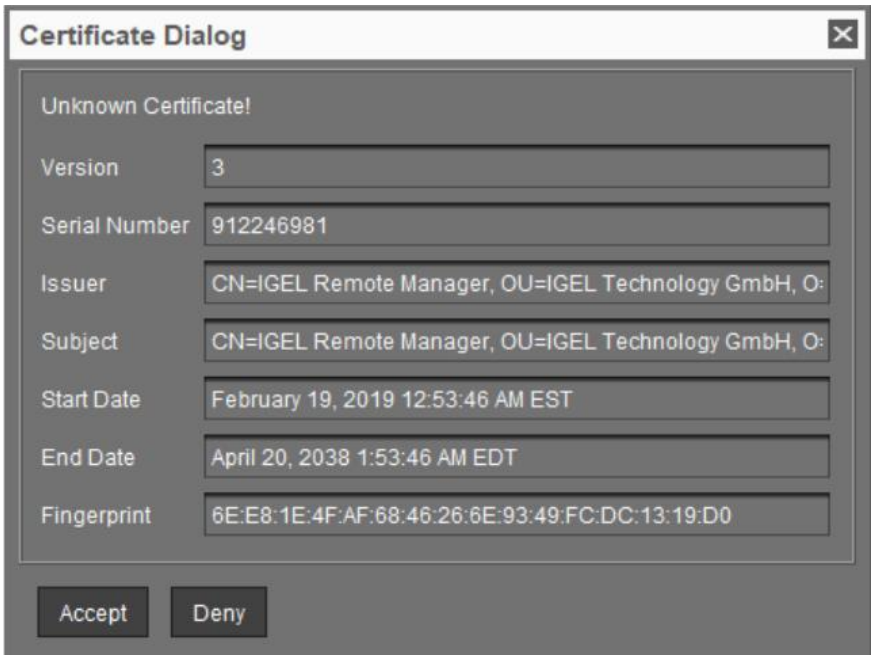
6. Enter the UMS server address in the **Server** text box, use '**igelrmserver'** if you created the DNS or DHCP setting, as recommended above. If you are connecting to the UMS from the UMS server, you can leave the Server textbox empty, as it defaults to itself.

   Enter the default port number (8443), username, and password.

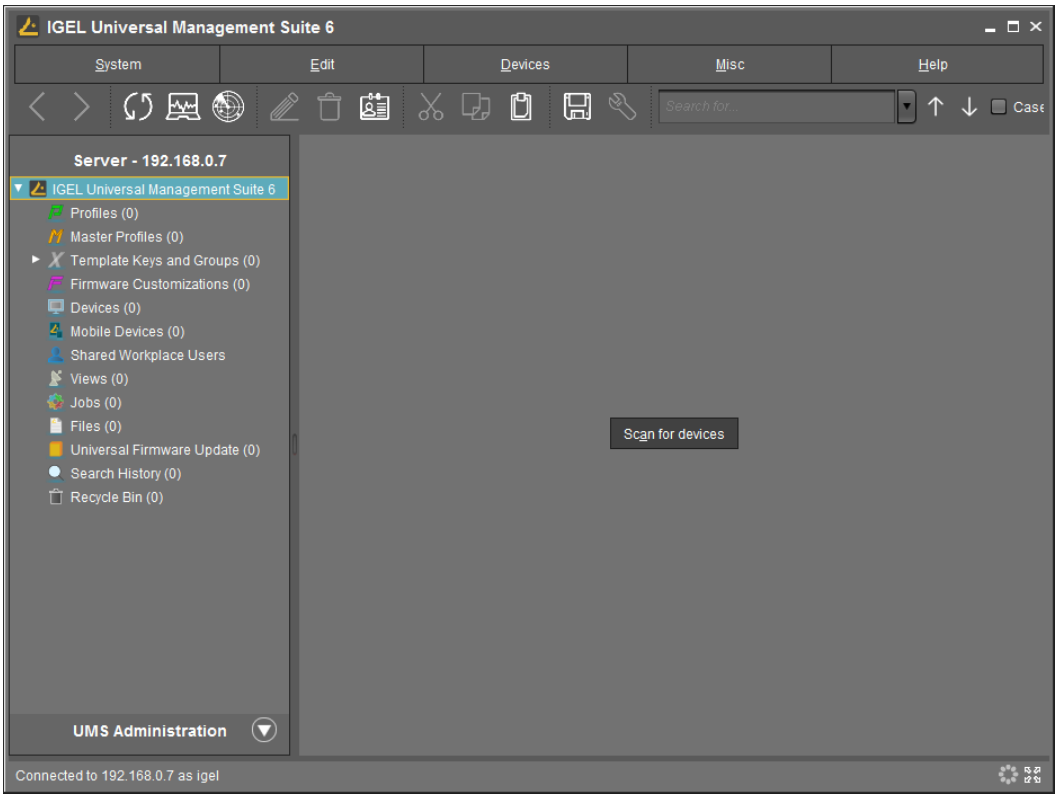
   Click the **Connect** button to connect to the remote UMS.



7. You are prompted to accept an unknown certificate. Again, I feel you can trust IGEL, so click the **Accept** button to continue.



8. If all goes as planned, the UMS opens, and away you go! Happy days are here to stay!



4. Install IGEL OS 11

The base product in the IGEL Software Suite is known as Workspace Editon. It consists of the IGEL OS, UMS, Multi-Media Codec Pack, IMI HA, and Custom Partitions. For this guide, you will be installing IGEL OS and UMS. The Multi-Media Codec Pack is included in every IGEL OS installation by default. No additional configuration is required.

IGEL Workspace Edition was designed to support being installed in multiple scenarios.

IGEL OS

Many businesses wish to replace old hardware with new end-user devices that are much smaller, energy-efficient, centrally managed, and affordable. This is what we call the traditional 'thin client.' IGEL has a long history of creating world-class thin clients. This history continues when you purchase an IGEL RPI4, UD 2, 3, 6, or 7 preinstalled with the IGEL OS!

But, please remember, the magic in IGEL is all about the software. Even when you purchase IGEL hardware, you can take advantage of license portability and the ability to move IGEL OS to any x86 64bit compatible machine or IGEL PRI4 device.

Learn more, review the **IGEL OS Creator Manual** and **IGEL OS KB home** resources.

IGEL OS Creator (OSC)

The IGEL OS Creator allows you to install IGEL OS 11 on any x86 64-bit supported devices. This comes in handy when a business wishes to save money by extending the life of perfectly good but older hardware. The IGEL OS Creator replaces any existing operating system and data on the device and replaces it with the IGEL OS. The devices can then be assigned a license and be centrally administered via the IGEL Universal Management Suite (UMS). Simple, smart, and secure, what is not to love?

The IGEL OS Creator also comes in handy when you need to recover from a crashed IGEL OS installation. Just reinstall the IGEL OS and re-register with the UMS. It's just so simple with IGEL!

Learn more, review the **IGEL OS Creator (OSC)** page.

> By following this guide's steps, you are installing the IGEL OS via the IGEL OS Creator.

UD Pocket

The UD Pocket delivers the IGEL OS via a simple USB thumb drive. When using a UD Pocket, all the user needs to do is plug the UD Pocket into a USB port on a compatible device and boot. The device will then boot the IGEL OS and pull the configuration from the UMS, anywhere, anyplace, at any time.

To learn more, visit the **UD Pocket** page.

> IGEL OS fully supports being run in an Oracle VirtualBox or VMware Workstation virtual machine. Running the IGEL OS in a virtual machine works great for testing, demos, and lab fun. Please refer to the following IGEL video on installing the IGEL OS in a VirtualBox environment **https://www.youtube.com/watch?v=odsHIfrfAJM**.

Learn more:

- **IGEL OS Creator Manual**
- **IGEL OS - KB Support Home**

The process of deploying the IGEL OS is broken down into the following four steps:

- Comply with the IGEL OS System Requirements
- Create a Bootable USB Drive
- Install IGEL OS
- Register the IGEL OS with a UMS server

4. 1. IGEL OS 11 System Requirements

To successfully install the IGEL OS 11 the target device must meet the following requirements:

- x86 64-bit compatible hardware
- 2 GB RAM or greater
- At least 2 GB storage (hard disk, flash memory, SSD, eMMC, or NVME)

  > A local hard drive is not required if you use the IGEL UD Pocket as the UD Pocket itself is the hard drive.

- Devices that have 2 GB RAM and shared video memory, a maximum of 512 MB, may be used as video memory.
- Intel, ATI/AMD, or NVIDIA graphics chip

  For a complete list of supported graphics chipsets, please refer to **https://www.igel.com/linux-3rd-party-hardware-database/** or the IGEL Community curated Community HCL – **http://www.igelcommunity.com/hcl**
- USB 3.0 or 2.0 port from which the device can boot (alternatively a DVD drive) or, as stated above, you can install the IGEL OS inside a virtual machine.
- Ethernet or wireless adapter.

> Installing the IGEL OS operating system via IGEL OS Creator destroys all data on the target device's hard drive. Please be careful and do not accidentally delete the client machine's hard drive.
>
> In case you require the device's hard drive to remain intact, the IGEL UD Pocket is your best solution as you boot from the IGEL UD Pocket's USB drive vs. the local machine's hard drive. This allows you to maintain the local machine's OS. For this reason, the UD Pocket works excellent in an anywhere computing scenario.

4. 2. How to Create a Bootable USB Drive

If you wish to install IGEL OS 11 directly on an existing or new device, you will need to create installation media. This is where the IGEL OS Creator comes into play.

Once you have downloaded and extracted the ZIP file's contents, you will notice an executable inside called ‘preparestick.’ This applet is used to prepare a CD or USB thumb drive used to deploy the IGEL OS.

After you create the installation media, you will need to configure the target device to boot. Upon boot, the IGEL OS Creator installation wizard will appear to walk you through installing the IGEL OS.

Once installed, the target device runs the same version of IGEL OS as found on any IGEL device, and all fully manageable via the UMS.

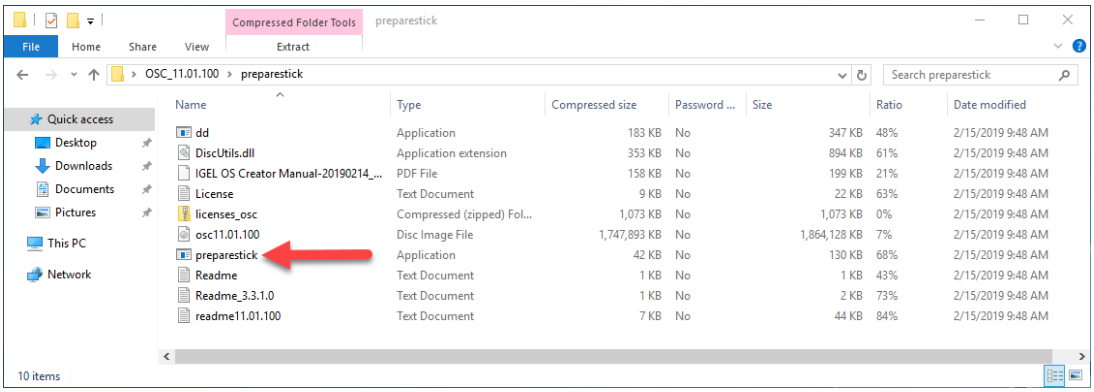
The following steps detail how to create a bootable USB drive containing the IGEL OS Creator.

1. Connect a USB thumb drive to a Windows-based PC.
2. Extract the IGEL OS zip file you downloaded earlier in this guide. Open the newly extracted folder to reveal the installation files.

   Double-click the **preparestick** executable.

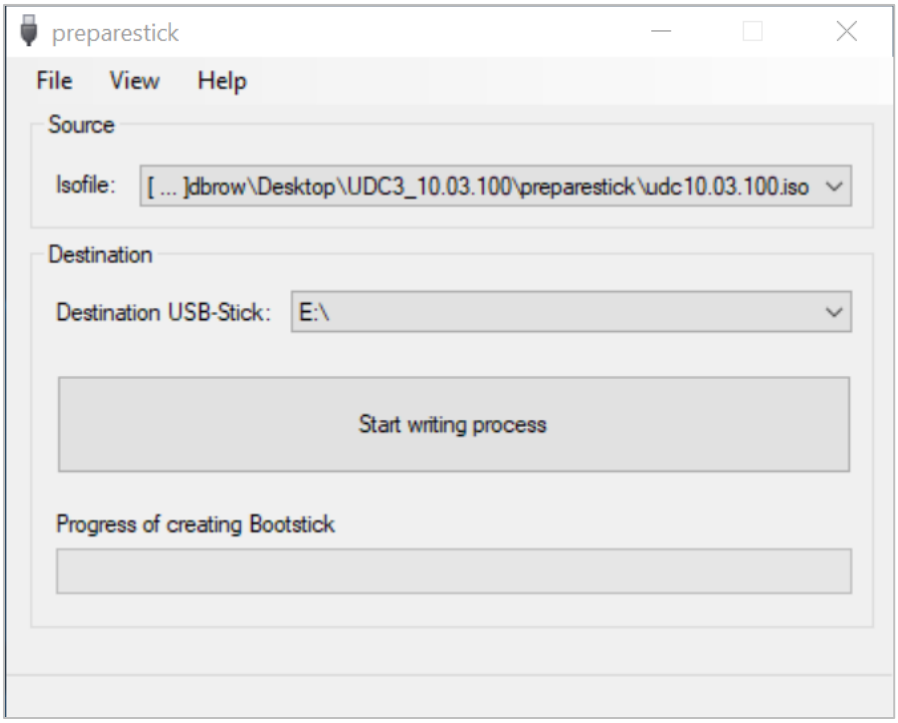
> It is required to run the **preparestick** application with administrative context, or the app may fail. If this step fails, please check your local Antivirus, or/and use another imaging too, such as Rufus.

> In the folder, you notice the ISO file. This is a full-blown IGEL OS image. In the following steps, you learn how to install the IGEL OS on a USB drive, but it is important to understand you can also utilize this ISO image and install the IGEL OS in a virtual machine.



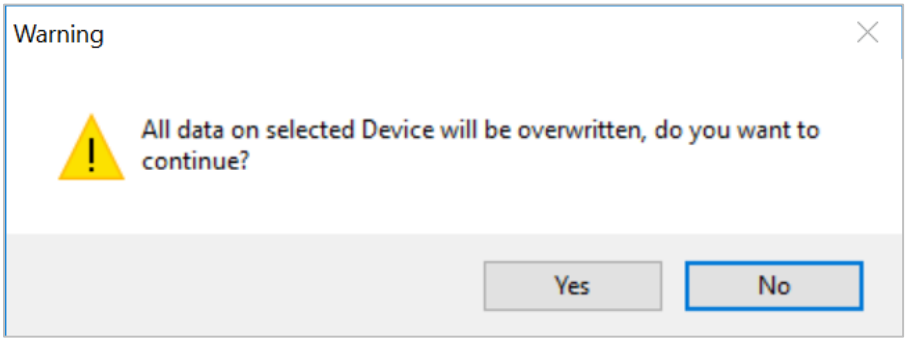
3. The **preparestick** application opens and presents you with the IGEL OS Creator source location (the ISO image discussed above) and destination you wish to install the IGEL OS Creator software, too, in this case, a USB thumb drive.

   Enter the required configurations and click the **Start writing process** button to create the bootable USB stick.

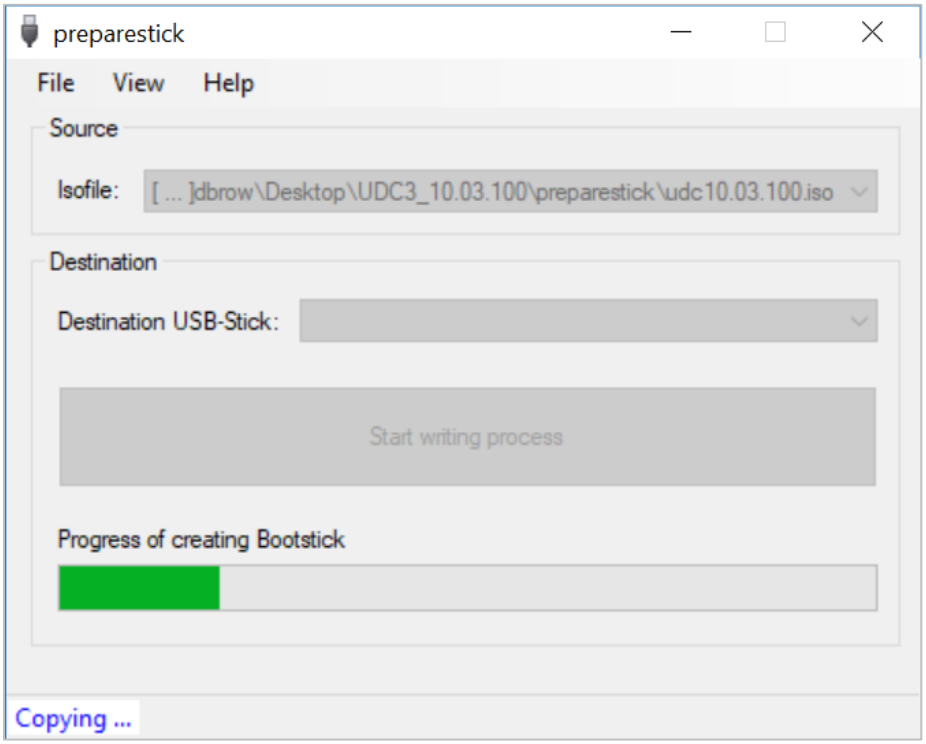


4. Beware, this tool formats the USB stick. Thus any data on the drive is lost. Please be careful and double-check to make sure you do not delete the wrong hard-drive by accident.

   Click **Yes** to continue.

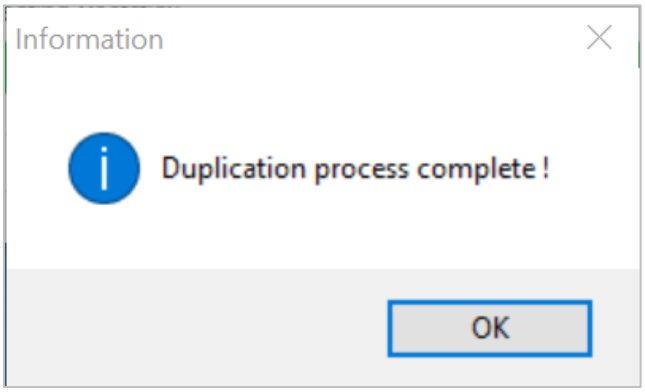


5. The preparestick program copies the IGEL OS installation program to the USB drive and makes it bootable.



6. Once the installation of the IGEL OS setup program is complete, the **Duplication process complete!** dialog box appears.

   Click **OK** to continue.



You have a bootable USB stick with the IGEL OS Creator setup program installed and are ready to insert the USB stick in the desired device and boot from it to install the IGEL OS!

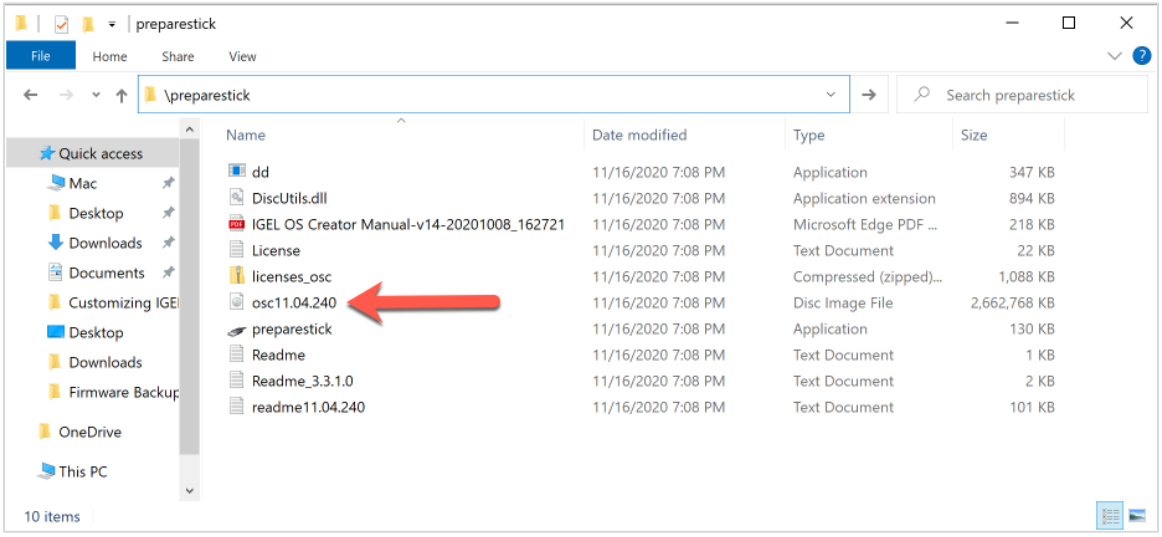
4. 3. How to Install IGEL OS

Now that you have created your installation media, you are ready to use it to install the IGEL OS on the desired device.

The following details how to install and configure using the IGEL OS Creator:

1. From the device you wish to install the IGEL OS, insert the USB drive you created above, turn on the device, and configure the computer to boot from the USB drive.

> If you are installing the IGEL OS in a virtual machine, you are required to configure the virtual machine software to boot to the **osc11.05.100.iso** image (file name varies depending on IGEL OS version) located in the **preparestick** folder of the extracted download.

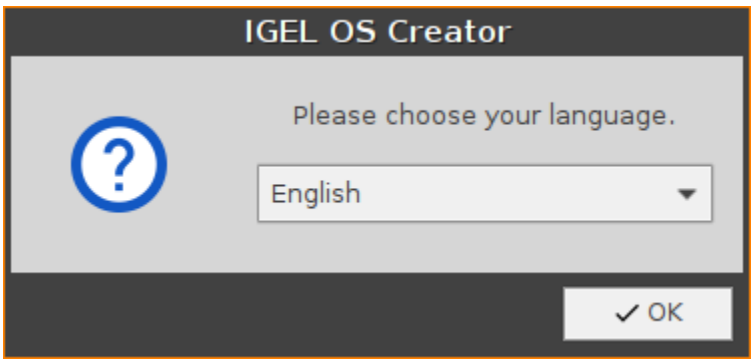


> Before starting the installation, ensure that all RAID configurations are turned off in the computer's BIOS. If you are not using standalone disks, the installation might go well, but you will not boot the operating system.

2. Once you successfully boot to the IGEL OS Creator, you are presented with the following options list. Select the **Standard Installation + Recovery** entry.

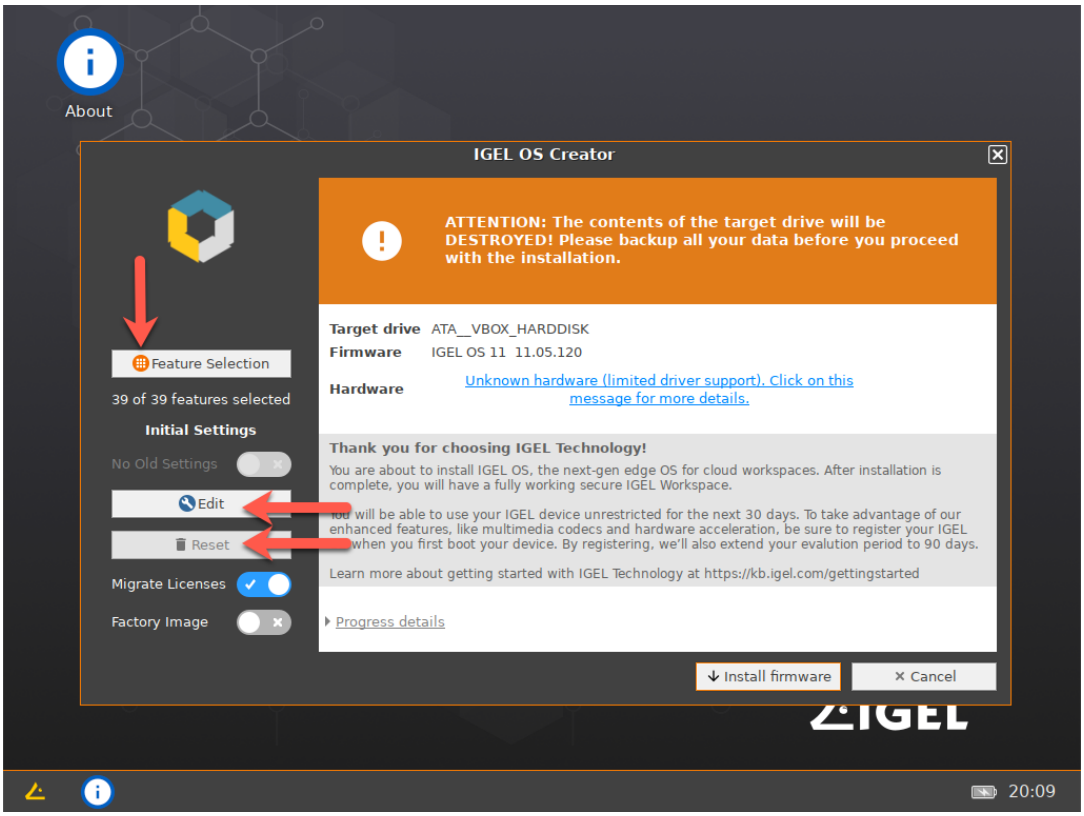
3. The wizard walks you through installing the IGEL OS Creator.

   Select your desired language and click the **OK** button to continue.



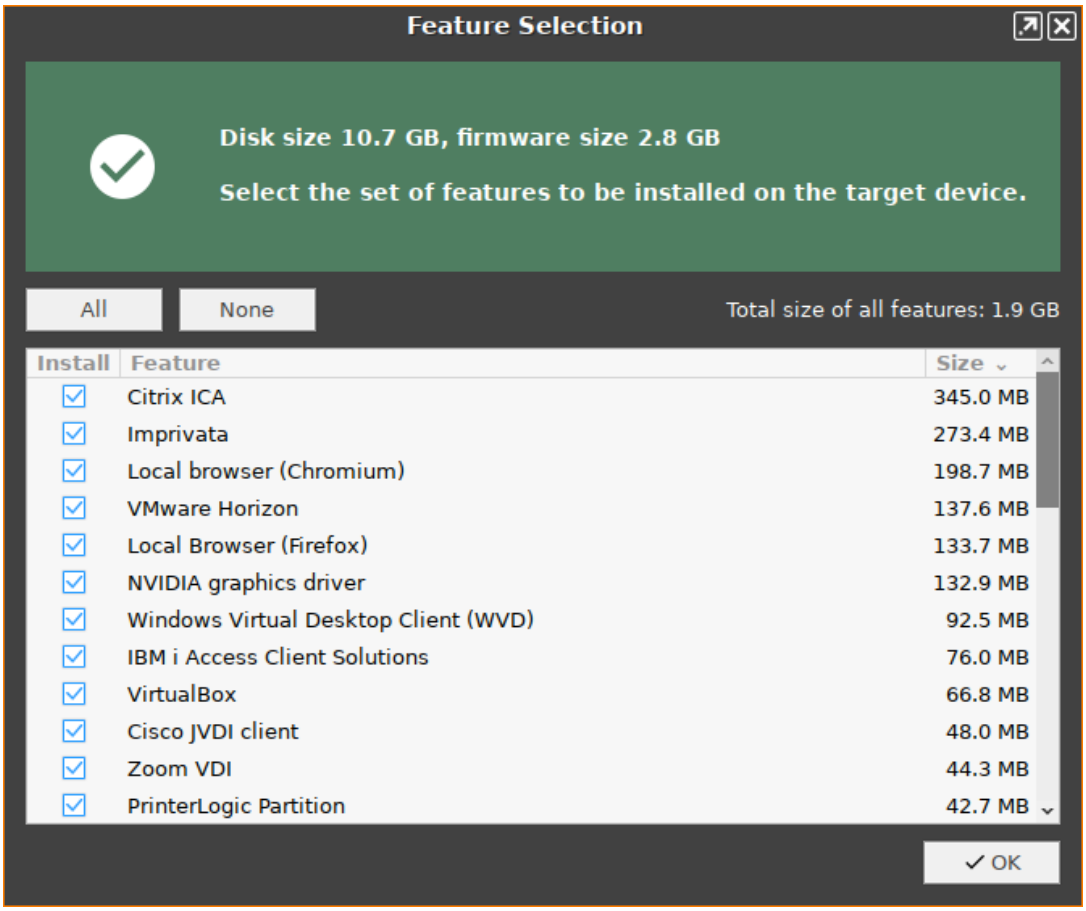
4. Next, you can select the features you would like added to the IGEL OS. This allows you to install only the components you require. This results in a smaller OS footprint and the ability for added security due to fewer potential risks.

   Click the **Feature Selection** button to continue.



5. Browse the list of features and uncheck the items you know you will not require. For example, if you are not installing on VirtualBox, you can remove it. Be careful as if you remove an item and then find you need it later, you will be out of luck and required to reinstall IGEL OS.

   Unselect the desire items and click **OK** to continue.

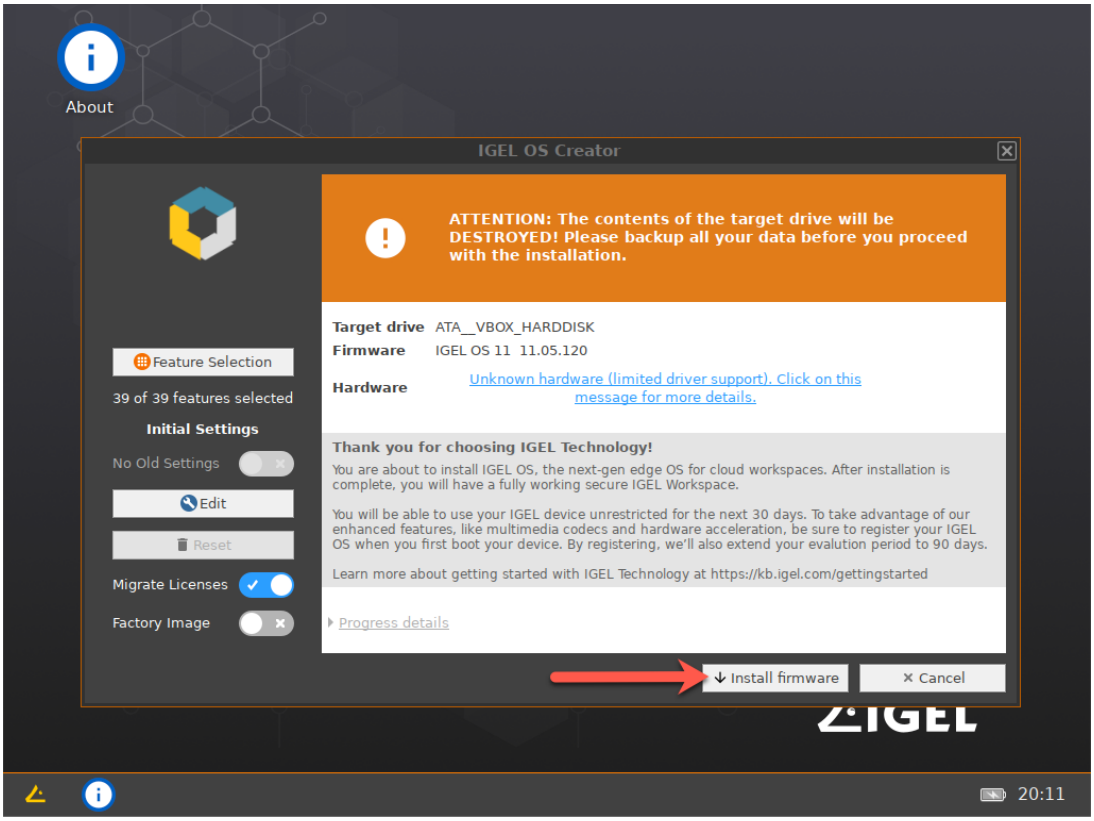


6. You are brought back to the previous screen and are ready to install the IGEL OS on the local hard drive.

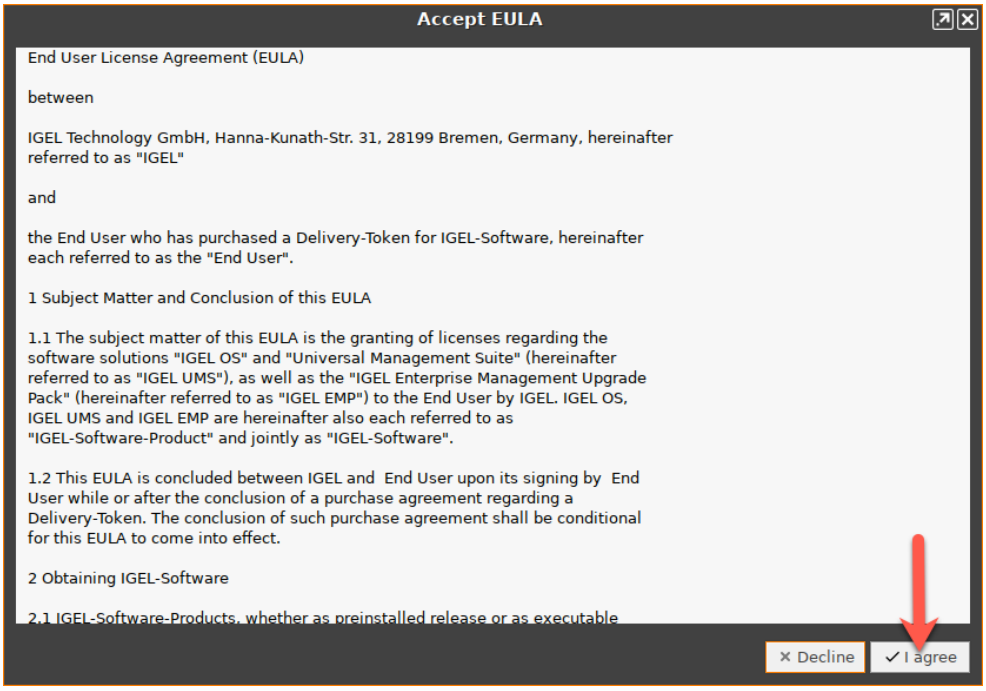
   IMPORTANT! Please verify you are installing to the correct hard drive as once you click the **Install firmware** button. The selected disk is erased without any way to restore it.

   Click the **Install firmware** button to install the IGEL OS.

   > Pay close attention to "unknown hardware" details. Although, if there is unknown hardware noted, generally, it works fine.

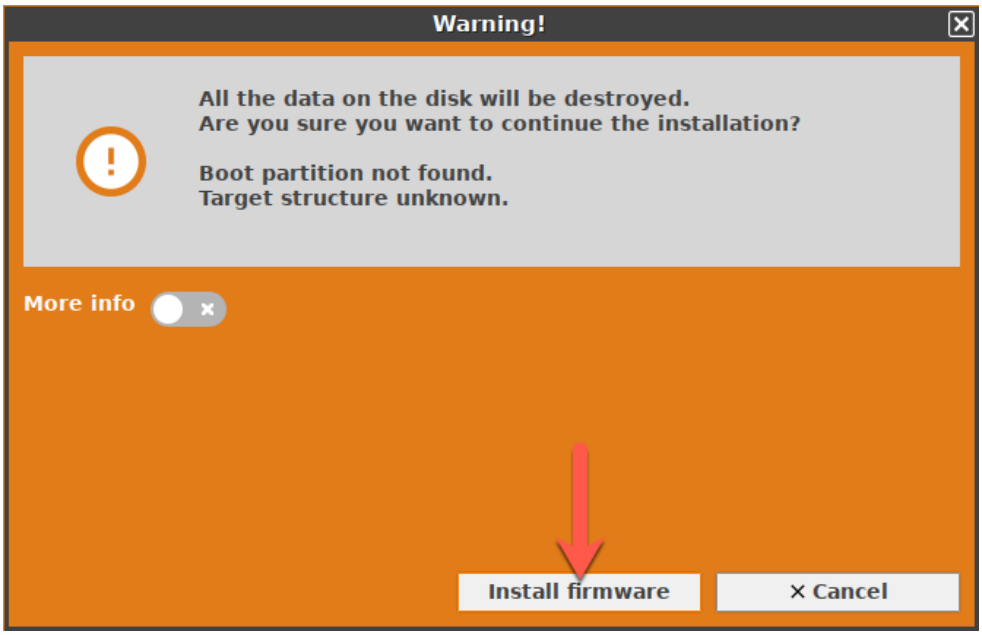


7. Click the **I agree** button to accept the IGEL license agreement.

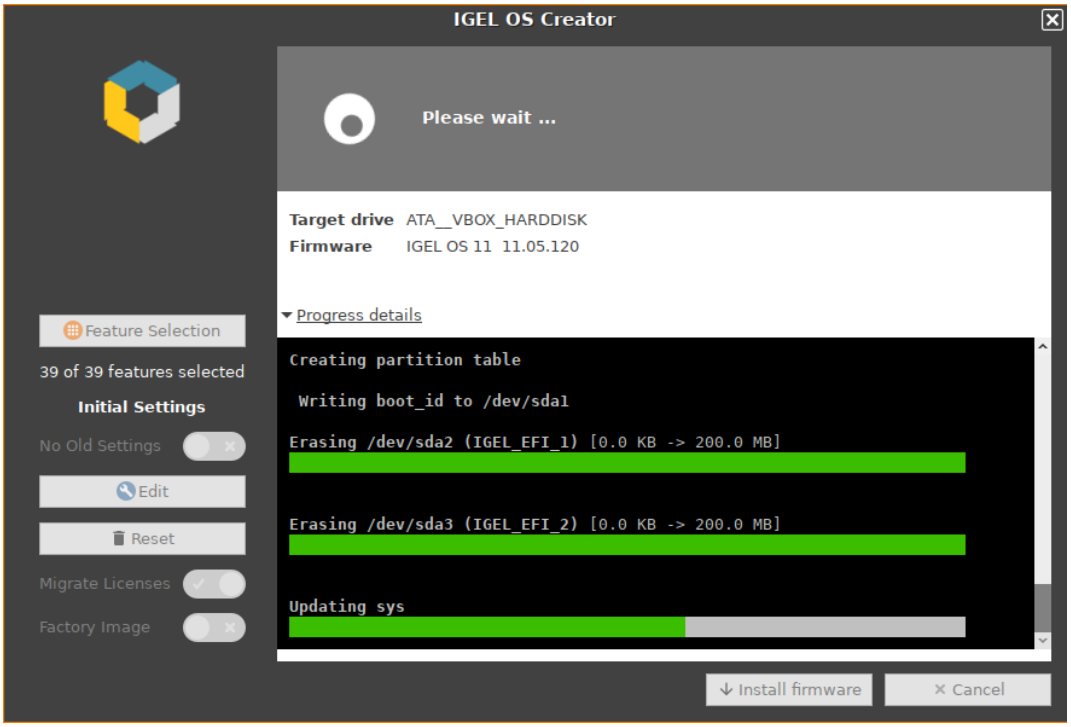


8. Again, be careful. You are about to delete the hard drive. If you install IGEL OS on an existing machine thinking you are setting up a dual boot, you are wrong. By clicking the Install firmware button, you erase the drive and install IGEL OS!

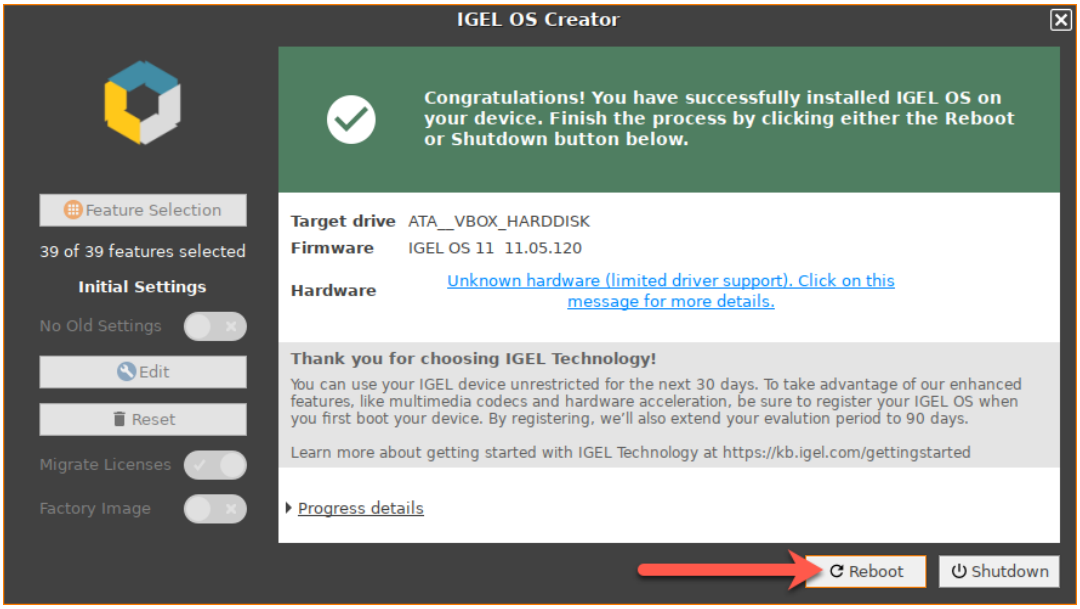
   Once you are 100% sure, click the **Install firmware** button to install IGEL OS!



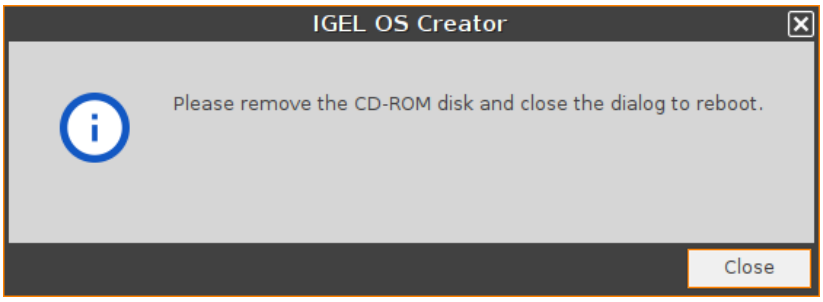
9. IGEL OS 11 installs on the selected hard drive!



10. Once finished installing, you are prompted to click the **Reboot** button. Click it to reboot the device and complete the installation of the IGEL OS.



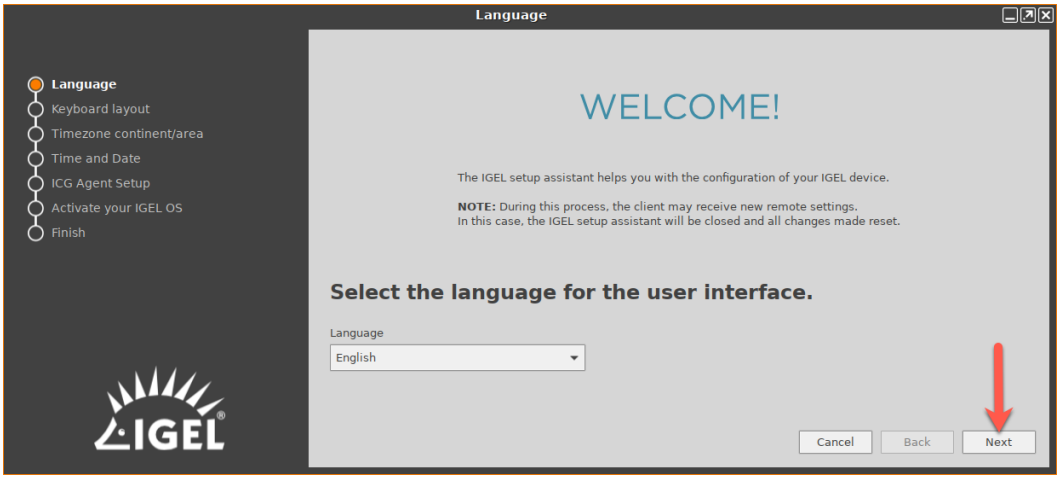
11. Click the **Close** button to reboot the device.



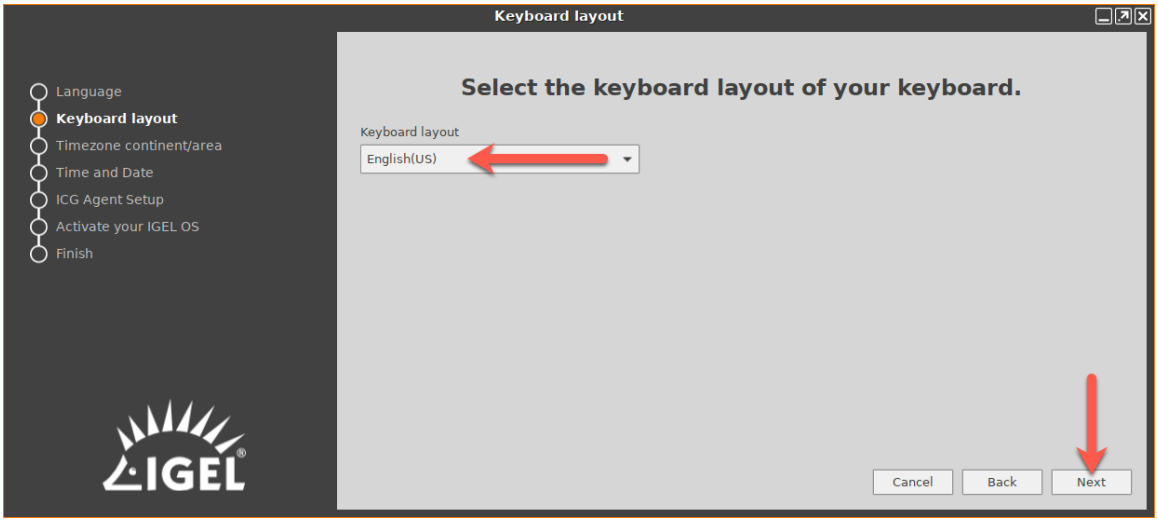
12. After the machine has restarted, you are logged in to the IGEL OS desktop. If you successfully configured the '**igelrmserver**' DNS or DHCP entry, the **Welcome Wizard** will not run. You are ready to skip to the next section of this guide. If not, you are presented with the following **Welcome Wizard**.

> I have seen issues where the Welcome Wizard does not launch the first time. If you experience this, all you need to do is reboot the IGEL OS, and you should be good to go. Do Not continue until the **Welcome Wizard** appears. It is required if you are not using the '**igelrmserver**' configuration for registration.

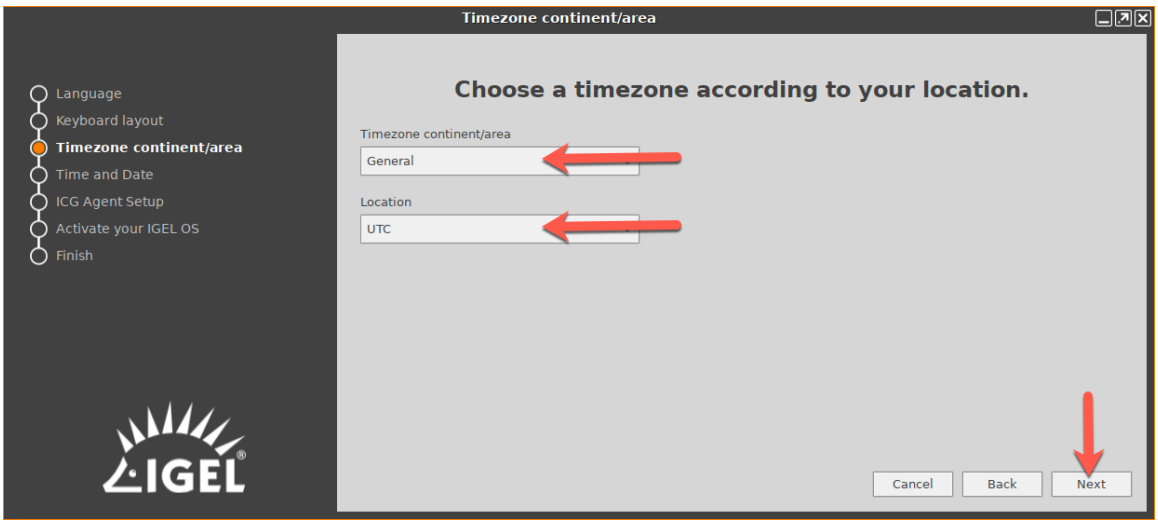
Select your desired language and click **Next** to continue.



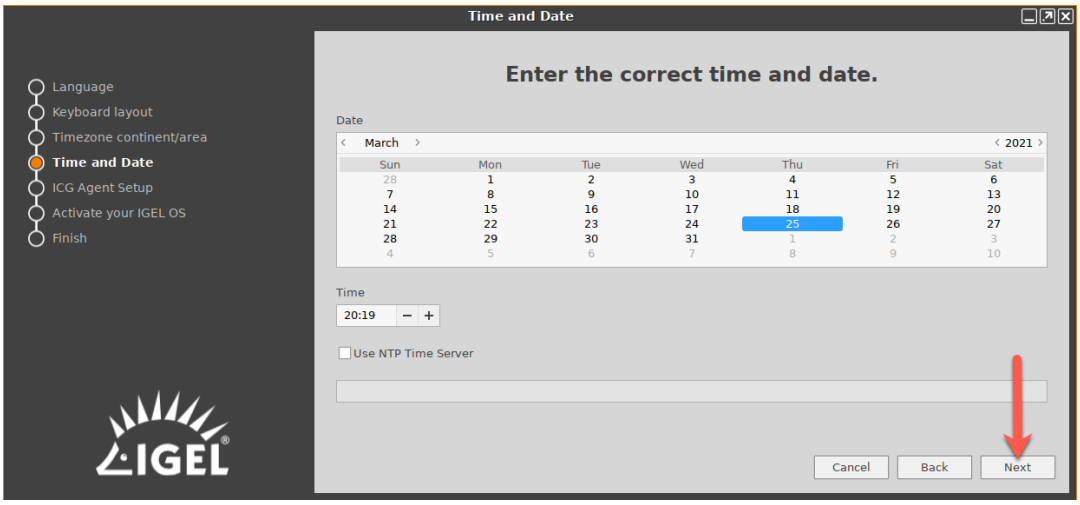
13. Select the desired keyboard layout and click **Next** to continue.



14. Select the desired time zone and location. Click **Next** to continue.



15. Enter the desired time and date and click the **Apply** button and then the **Next** button to continue.

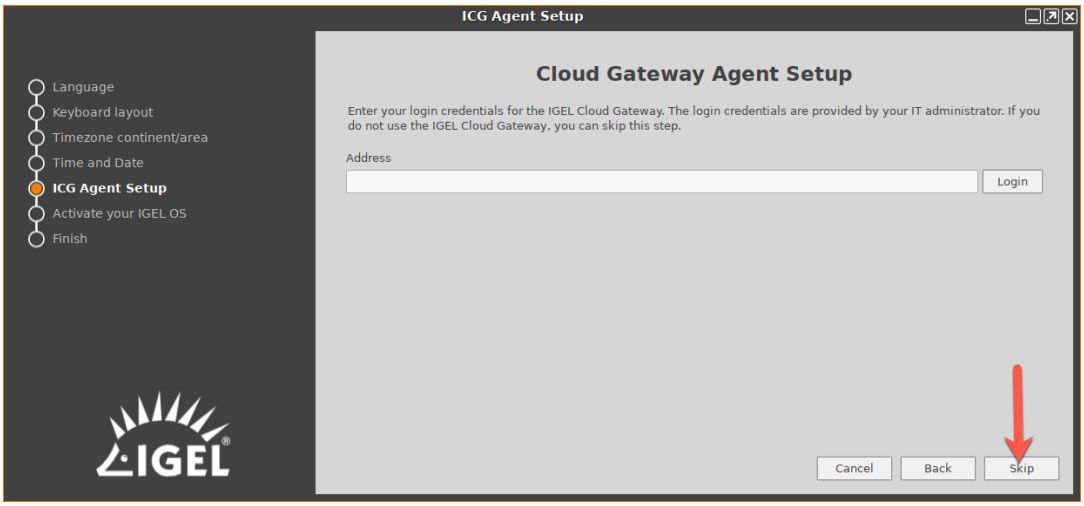


> For this guide, we have chosen to document the eval license option for acquiring a device license. To learn more about all three licensing opportunities, please refer to the **IGEL Software License Overview** KB page.

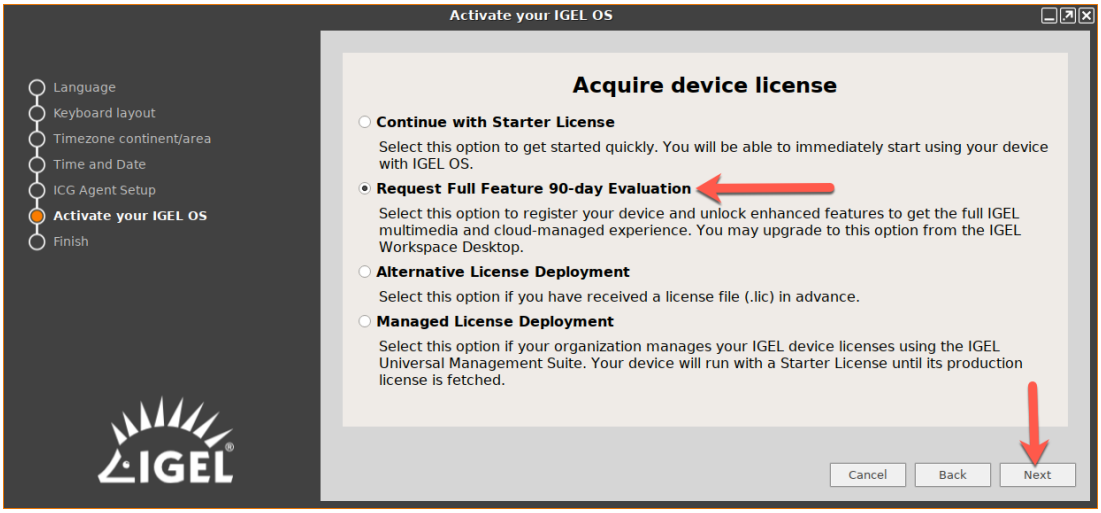
> **Important!** The IGEL OS ships with a "starter license". This license allows you to get up and running in case you do not have the ability to 1) properly license the device right way 2) not able to connect an evaluation license (the 90-day license). It is very important to understand, the starter license does NOT ship with the Multimedia Codec Pack and hence the user-experience will be degraded when doing multimedia, basically most tasks a user does in the modern age. Hence, this license is meant to get your started and NOT for testing and never for production use. If you wish to test the IGEL OS, please register for the 90-day evaluation license, as documented later in this guide.

16. You are presented with the option to connect the IGEL OS to an ICG server. Since you are just getting started, you won't have an ICG server yet. Hence, let's skip this step for now.

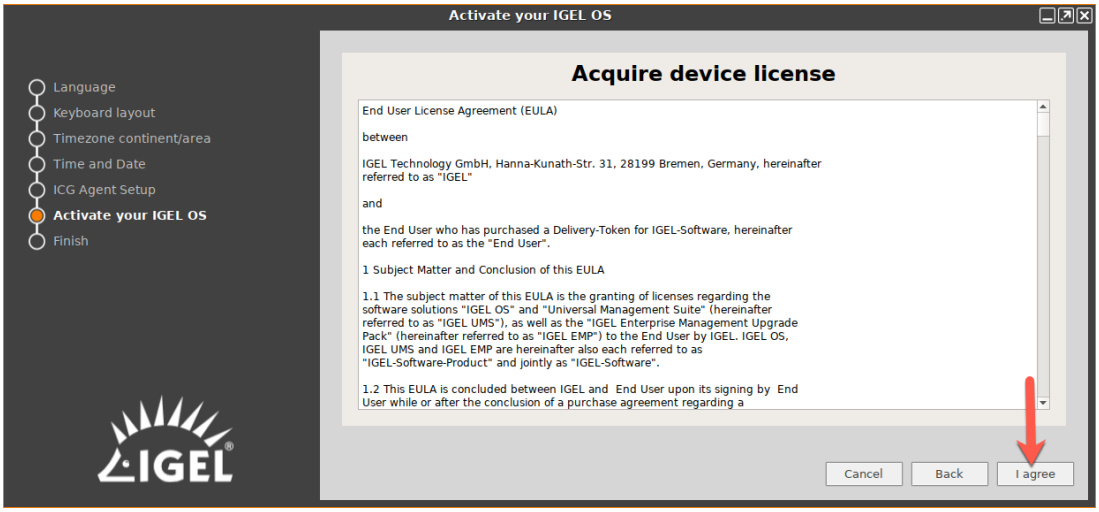
    Click the **Skip** button to continue.



17. Next, you are required to define the type of license you will be using. Click to select the **Request Full Feature 90-day Evaluation** radio button and click the **Next** button to continue.

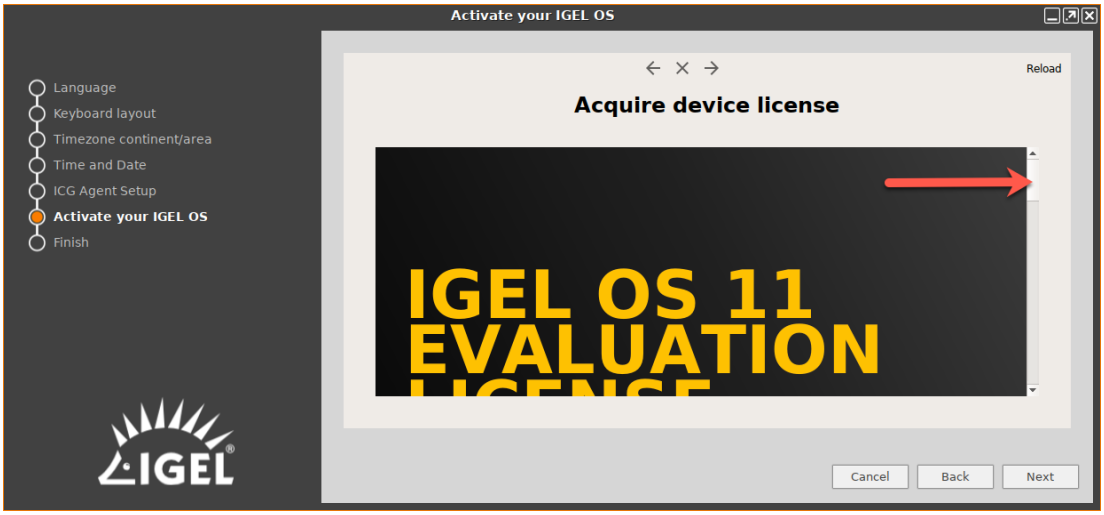


18. Click the **I agree** button to accept the IGEL EULA and continue.

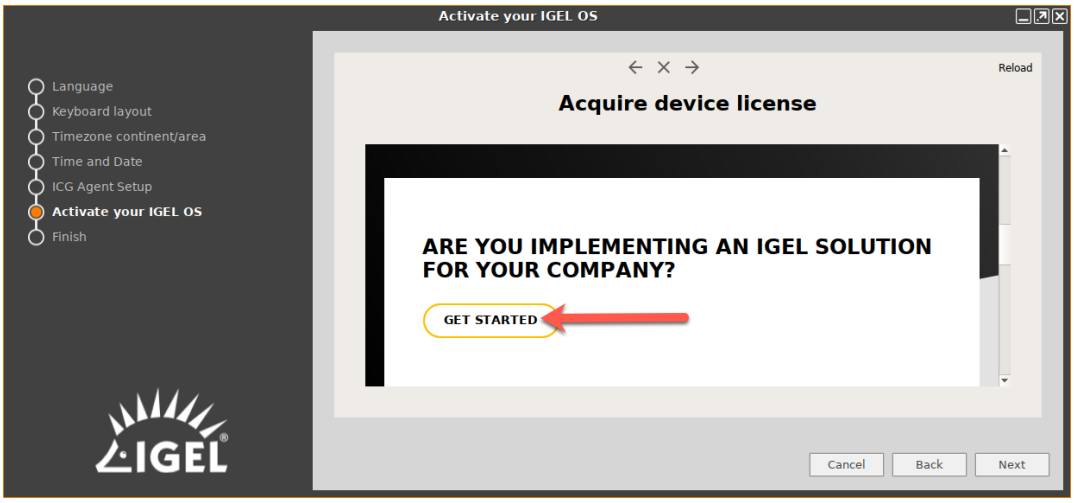


19. You are brought to the **Acquire device license** screen. This is an embedded web page, so be mindful. The arrows and x buttons on the top middle of the screen allow you to browse through the wizard. You should not need these.

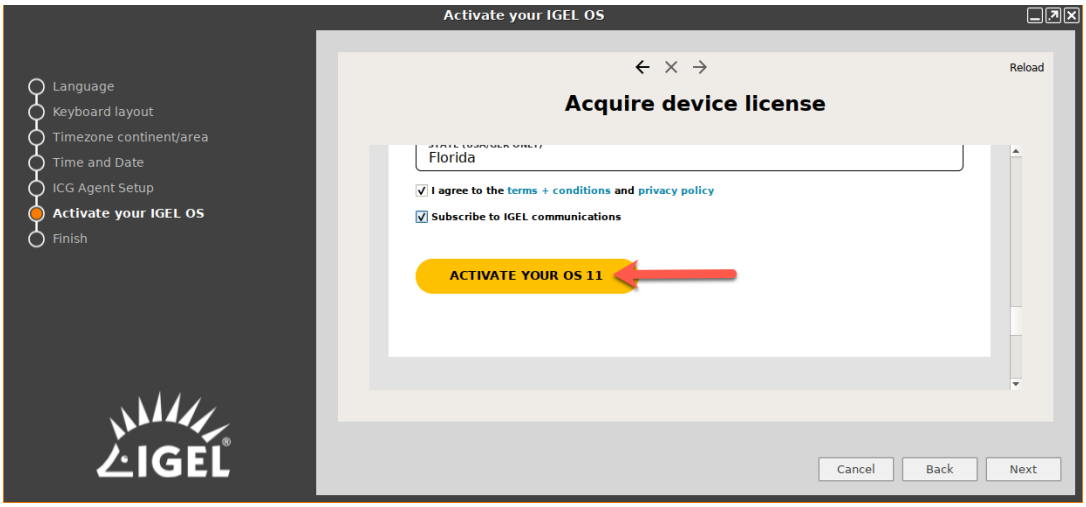
    Scroll down to view the rest of the page.



20. Select the type of deployment you will be doing and click the **Get Started** button for your company type.



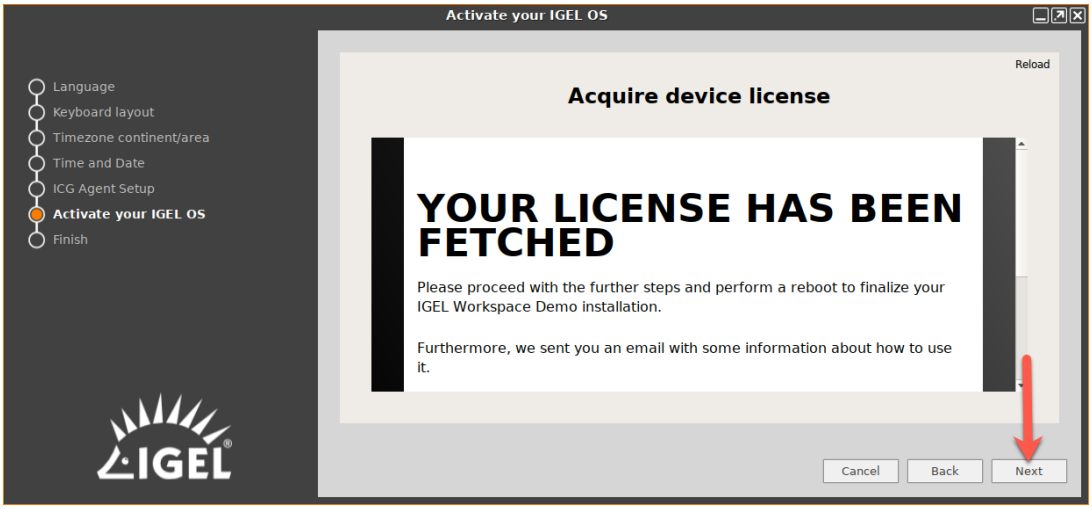
21. Next, you are prompted to enter your data to request a free license. Fill out all entries. You will need to scroll down the embedded web page to expose the entire form. Once finished, click the **ACTIVATE YOUR OS 11** button.



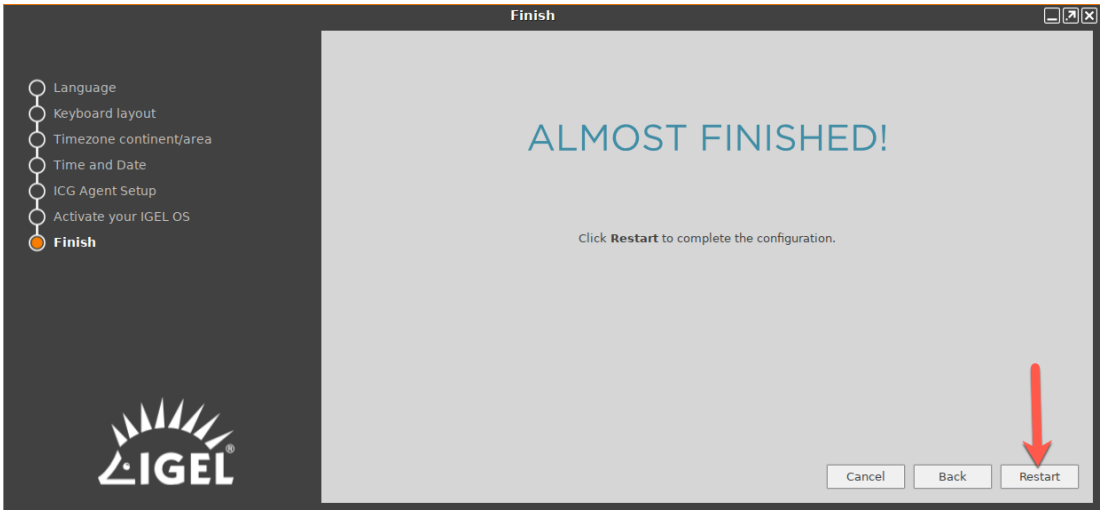
> An important point to understand is that while fetching a license, an actual license has been downloaded and added to the device. The device is now fully licensed, whereas, in the past, you had more steps to activate, download, and deploy the license.
>
> You will have the option to keep or remove the devices' license if you wish to reset the machine to factory defaults.
>
> Again, you now have a fully licensed IGEL OS 11 device.

22. If the licensing gods are happy, you are informed your license has been successfully fetched. You are also informed an email was sent to you ‘about how to use it.’ No need to worry about this for now. We will walk you through everything you need to know below.

    Please click the **Next** button to continue.

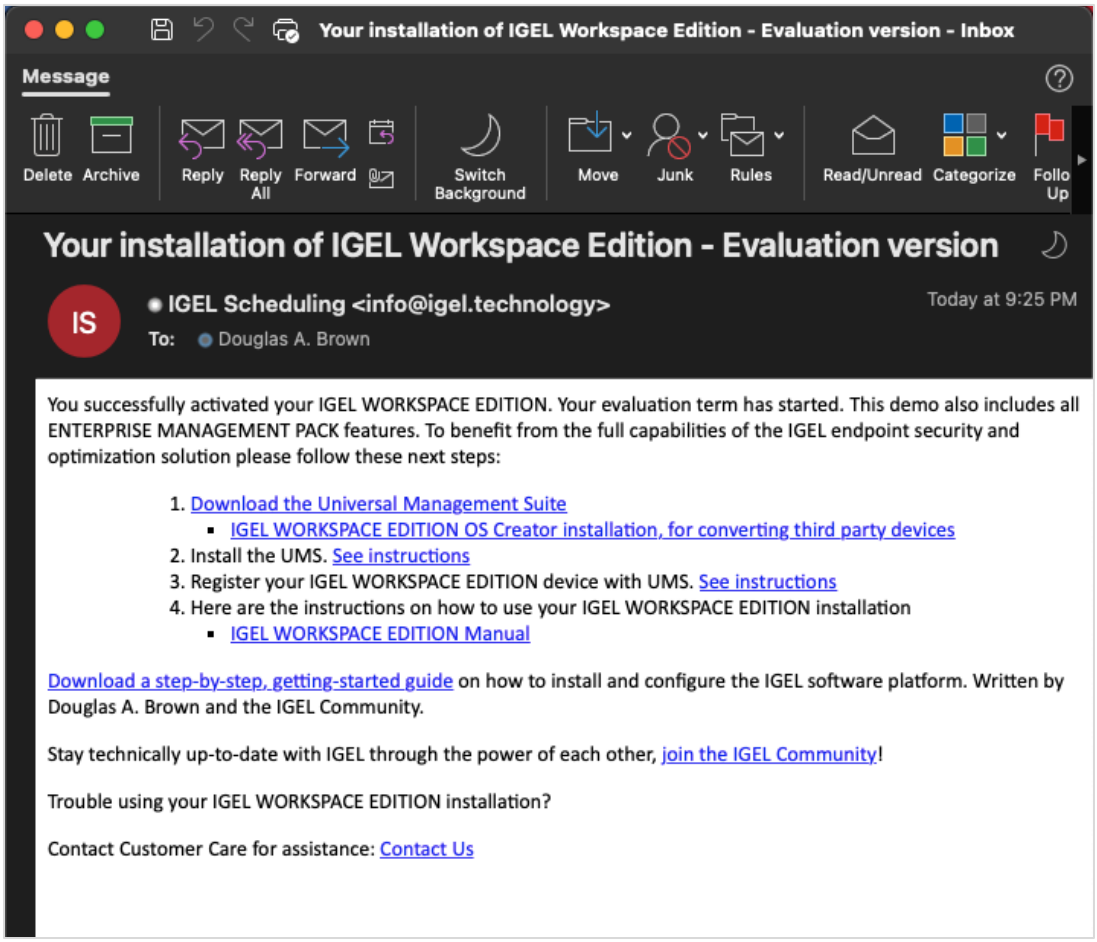


23. Almost Finished! Click the **Restart** button to reboot the device and finish the installation.



24. You can flip over to your email client, and you should find a new email from IGEL. Don't worry about this information. This guide will walk you through everything you need. You can safely delete it.

    Though, we do recommend you to join the IGEL Community. If you are not already a member - **join.igelcommunity.com**.



4. 4. How to Register the IGEL OS with a UMS Server

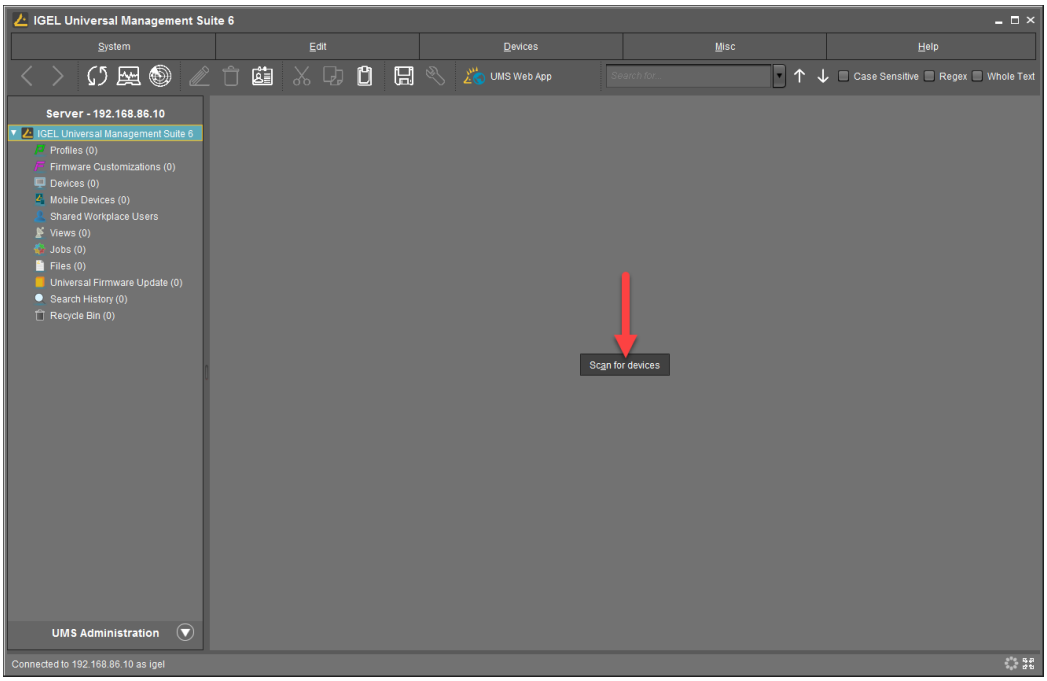
You now have a working IGEL UMS and your first IGEL OS endpoint installed. The next step is to trigger the UMS server to find and register any available IGEL OS devices.

> If you connect to a UMS server via an ICG connection, you are not required to register the device as that process is performed when setting up the ICG session on the client device.

The following details how to configure the UMS to find new IGEL OS instances and import them into the UMS:

1. Click to select the **IGEL Universal Management Suite 6** node to expose a big button prompting you to scan for devices, thus find all new devices.

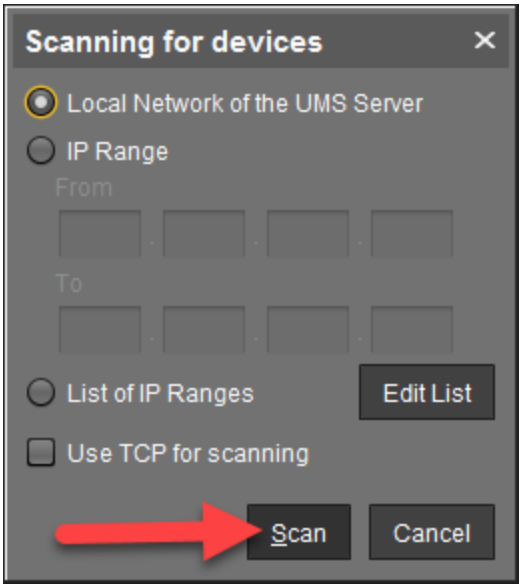
   Click the **Scan for devices** button to continue.



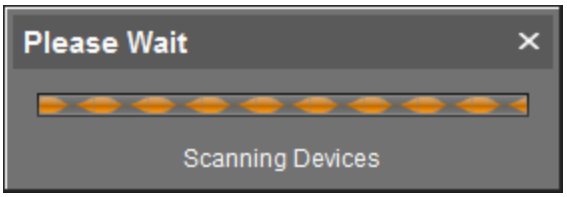
2. The **Scanning for devices** windows opens, prompting you to define the network you wish to scan.

> For more information on importing and managing IGEL devices, please refer to **Managing Thin Clients in IGEL UMS 5 (Universal Management Suite)** video along with the **Searching for Devices** KB article.

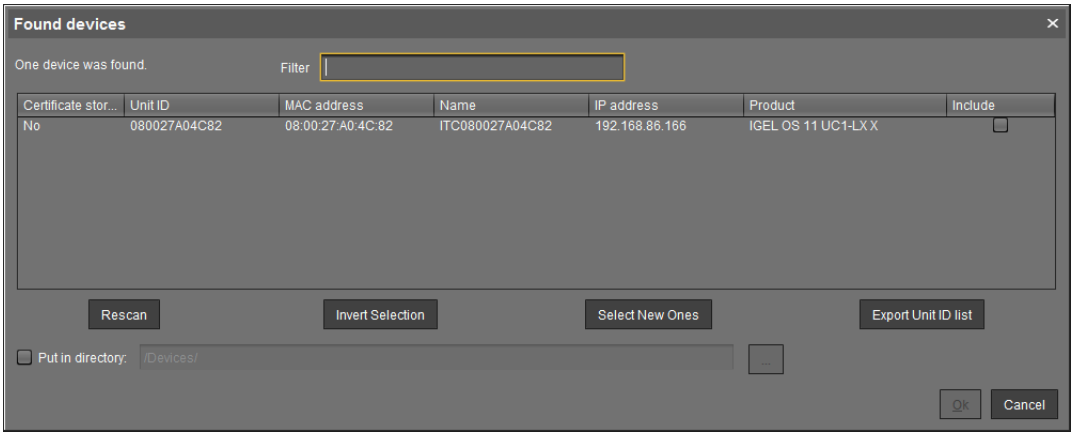
> If the UMS experiences problems finding your clients, please verify you have connectivity between hosts. UDP should be open between the IGEL OS and UMS. Try the checkbox **Use TCP for scanning** to help with figuring out if this is the problem. You can try scanning a specific IP Range when **Use TCP for scanning** is checked.
>
> For more information, refer to **Registration of a Device fails** and **Device Scan or Online Check fails** KB articles.



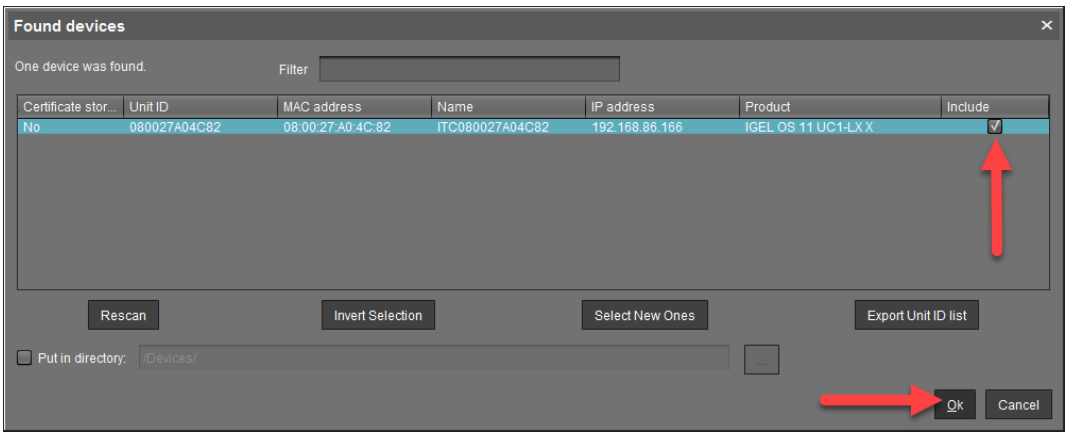
3. The UMS scans the desired network(s) for any available IGEL OS devices.



4. The **Found devices** window opens, listing all IGEL OS devices that were found.



5. Click to check the **Include** checkbox of the IGEL OS device you wish to import and click the **OK** button to continue.



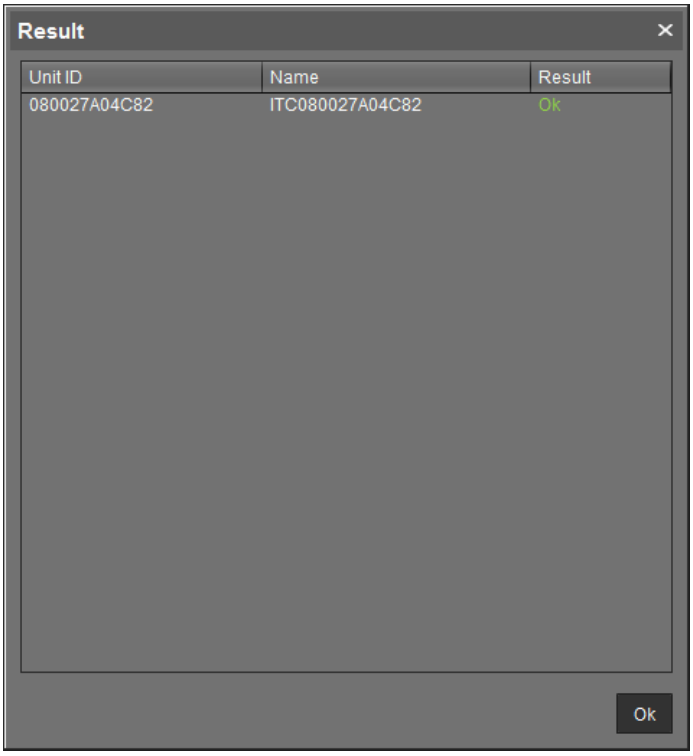
6. The UMS registers the selected IGEL OS devices and adds them to the UMS as registered clients.

   If all goes as planned, you should see a happy green **OK** text.

   In general, if the result is NOT OK, the reason is that the device cannot connect to the UMS Server on TCP 30001. In my case, the Windows Firewall was preventing access.

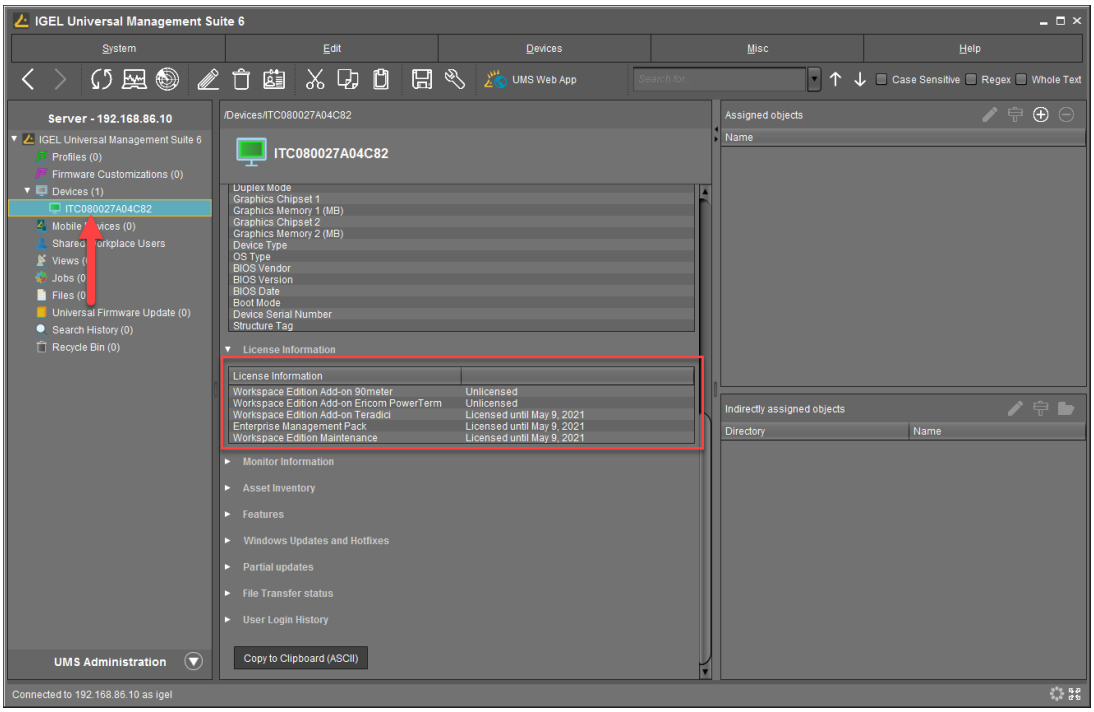
   For more information on troubleshooting this issue, please refer to **https://kb.igel.com/endpointmgmt-6.06/en/registration-of-a-device-fails-37281897.html**

   Click the **OK** button to continue.



7. You should see your newly registered device under the **Devices** node, as seen below.

> Please check out the **License Information** section. You will see your license is an evaluation license, and you are also licensed for the Enterprise Management Pack. You will notice the trial's expiration date.



5. Install IGEL Cloud Gateway

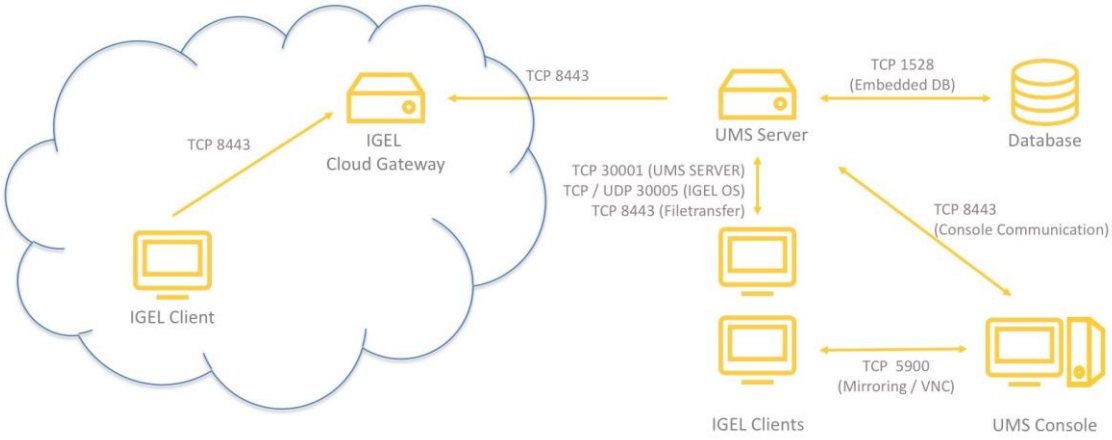
You are ready to install the IGEL Enterprise Management Pack's Cloud Gateway (ICG) technology. The ICG enables the Universal Management Suite (UMS) to manage endpoint devices outside the company network securely by acting as a secure gateway between the UMS and IGEL managed device.

It is not required to install an ICG server to test the IGEL OS and UMS. It does come with much goodness and is something you should think about if deploying to remote users using a UD Pocket or any IGEL OS devices without the requirement of a VPN.

Basic Architecture

The primary design goal for the ICG is security. In a nutshell, the ICG is an SSL secure gateway between the IGEL OS and the UMS. Thus, it is recommended to install the ICG host on a different network than the UMS. For example, in your DMZ or on a cloud instance.

The architecture of IGEL Cloud Gateway



Feature Parity?

It is essential to understand, not every UMS/IGEL OS feature is available when connecting through an ICG server. Please refer to the following KB article for a complete list of supported features - **https://kb.igel.com/igelicg-2.02/en/limitations-31600940.html**.

Licensing

IGEL Cloud Gateway (ICG) is a feature of the Enterprise Management Pack. Since you are installing using the demo license, you are fully licensed. The demo license is a full license, only restricted by time.

ICG on Microsoft Azure

IGEL now offers you the ability to utilize a preconfigured IGEL Cloud Gateway (ICG) appliance on the Microsoft Azure Marketplace.

Learn more:

- **IGEL Cloud Gateway on Azure Marketplace**.
- **Using IGEL Cloud Gateway on Microsoft Azure Marketplace**

Learn more:

- **ICG Manual**
- **ICG KB support home**

The process of installing and configuring the IGEL Cloud Gateway server on an AWS EC2 instance is broken down into the following ten steps:

- Comply with the ICG system requirements
- Create an AWS Instance for the ICG
- Open Firewall Ports Required by the ICG
- Create Required DNS Records
- Generate CSR File
- Create an SSL Certificate for the ICG
- Add SSL Certificates to the UMS
- Install the IGEL ICG using the UMS Remote Installer
- Configure the ICG device authentication method
- Configure IGEL OS to use ICG

5. 1. ICG System Requirements

The IGEL Cloud Gateway is a Linux application delivered as a traditional Linux binary or a virtual appliance.

Software Installation

The ICG software can be manually installed or pushed from the UMS to the ICG target server via the IGG Remote Installer feature. ICG can be installed on any virtual or physical hardware meeting the following requirements:

- View a list of **Prerequisites**
- Requires x86 64-bit architecture running a support operating system. Refer to the **Supported Environment** KB support page for a complete list of supported operating systems.
- Recommended 2 GB RAM for production environments.

> For a test/lab environment, you should be able to get away using 1GB RAM. By following this guide, you install the ICG on a free AWS EC2 instance with 1GB RAM. However, if you are going to put a load on the system, you should upgrade to 2GB of RAM.

- The following packages are required: *dialog, uuid-runtime, super, unzip, realpath*.
- Python 2.6 or higher, Python 3.x is not supported. Create a symlink python2 pointing to the python 2.6+ installation.
- UMS (Universal Management Suite) in version 5.07.100 or newer.
- IGEL OS in version 10.02.100 or newer. If shadowing or Secure Shadowing is needed, version 11.02.100 or higher is required.

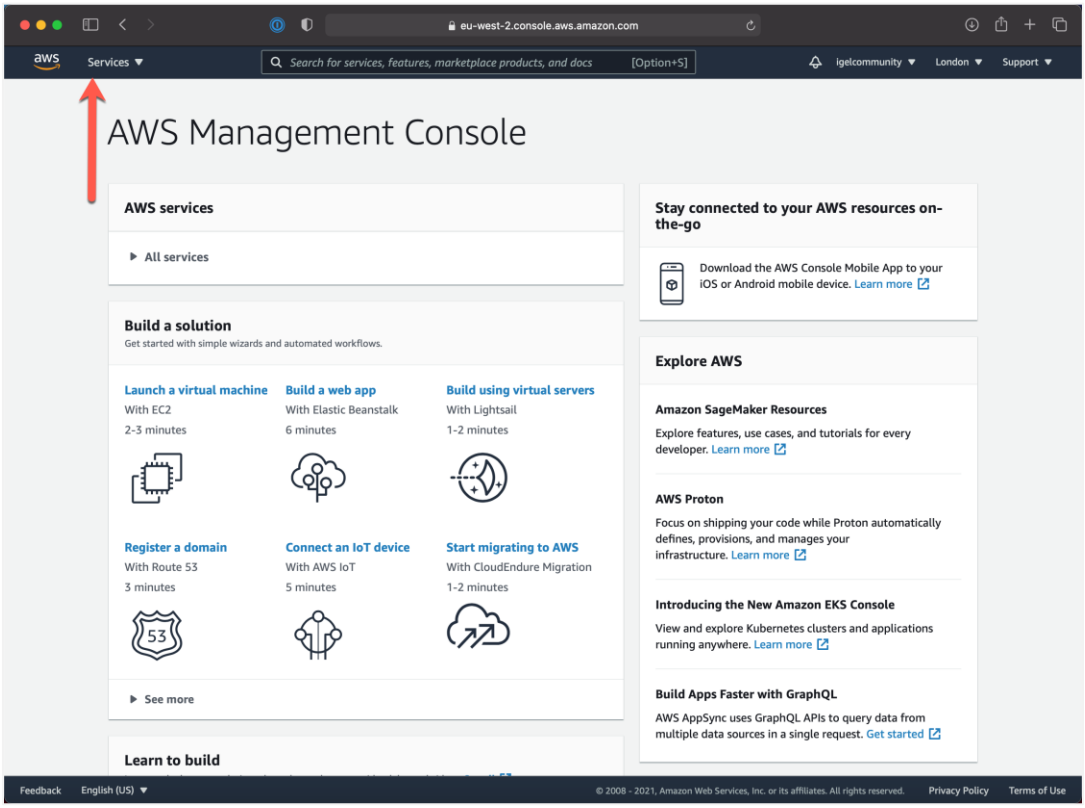
5. 2. How to Create an AWS Instance for ICG

As we will be using a free tier AWS EC2 instance for this project, you must set up an AWS account. Browse to **https://aws.amazon.com/** and create your free account.

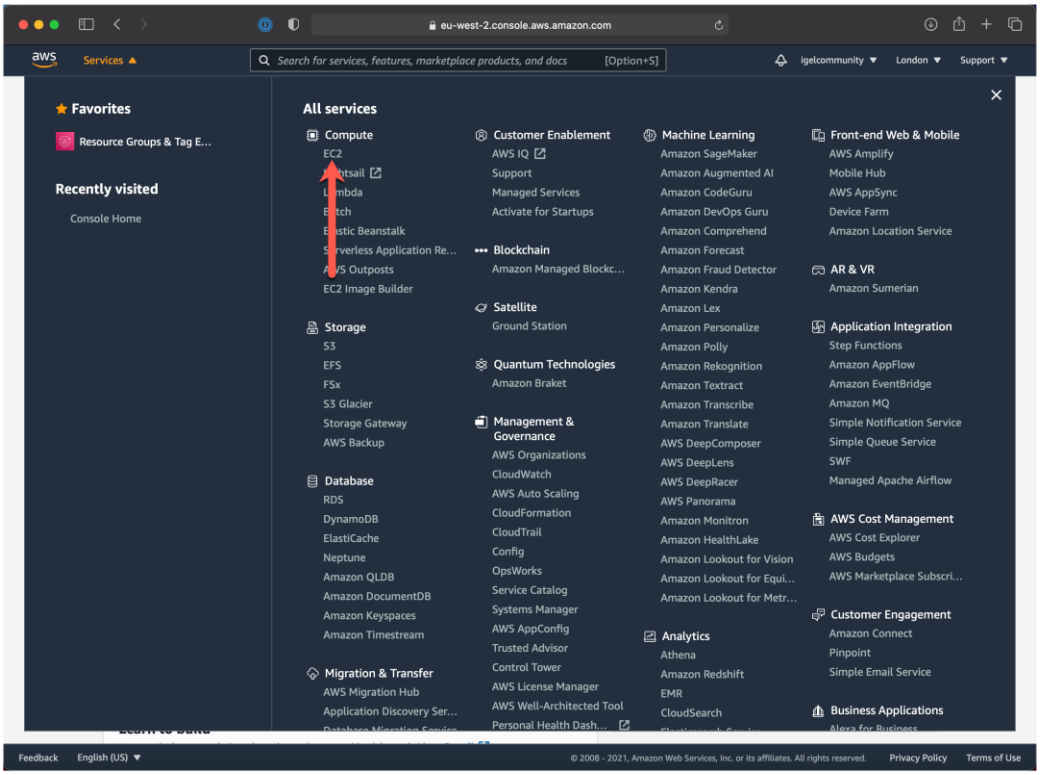
> In this guide, we document how to install the ICG on an AWS EC2 instance, but this is not required. The ICG software can be installed on any Linux server, meeting the basic system requirements utilizing the same steps you find below, minus the AWS-specific instructions.

The following details how to install the ICG on an AWS EC2 cloud instance:

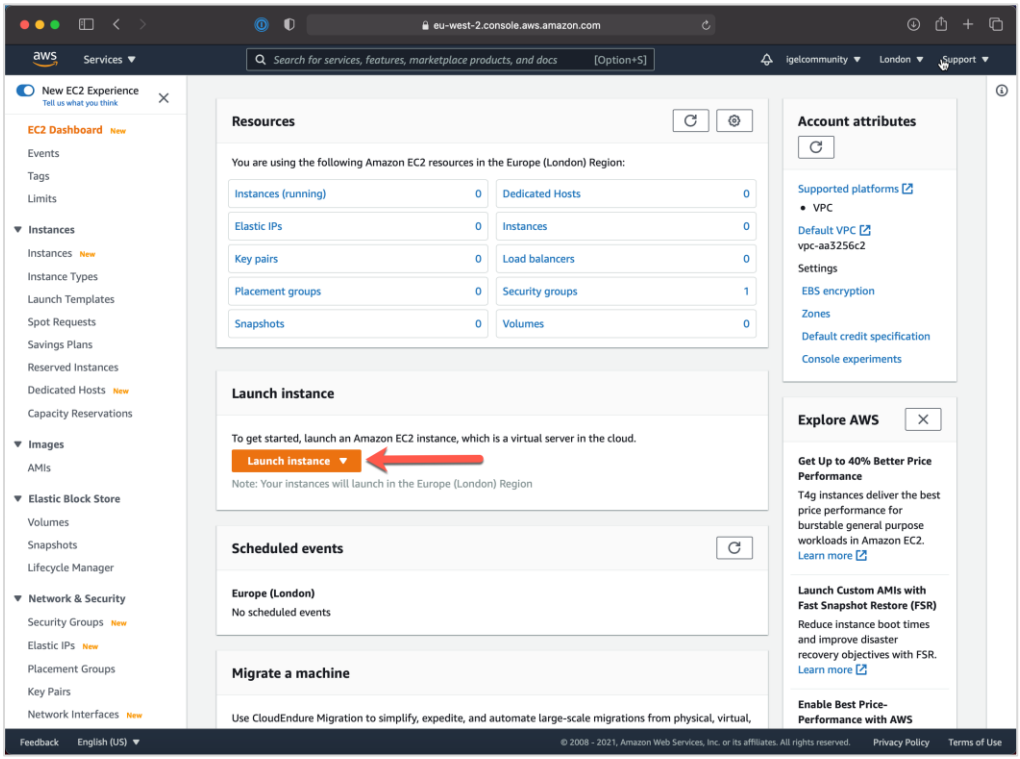
1. Login to your AWS account and click on the **Services** link located in the top menu bar.



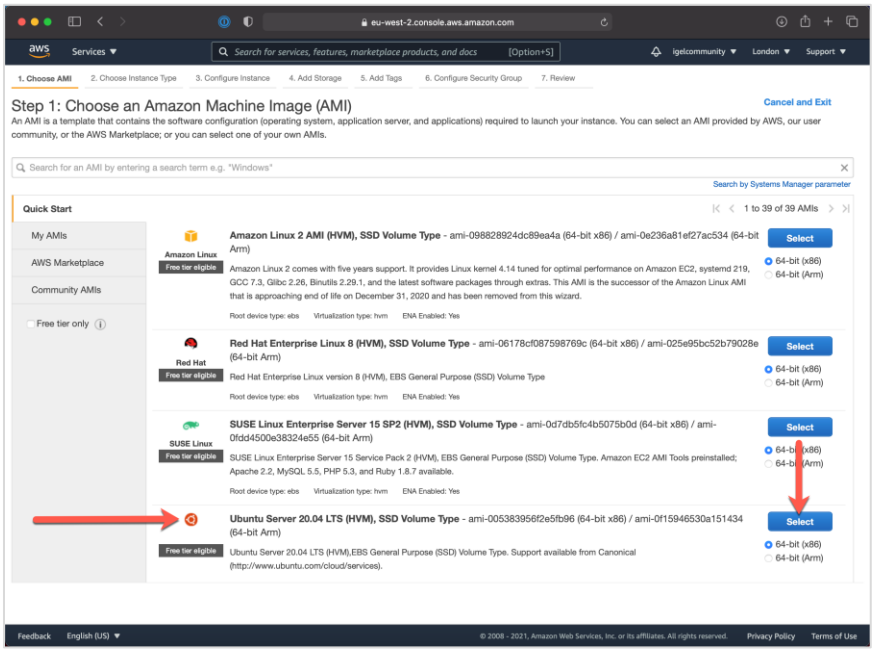
2. Click the **EC2** link.



3. You are ready to create an AWS instance for ICG. Click the blue **Launch Instance** button.

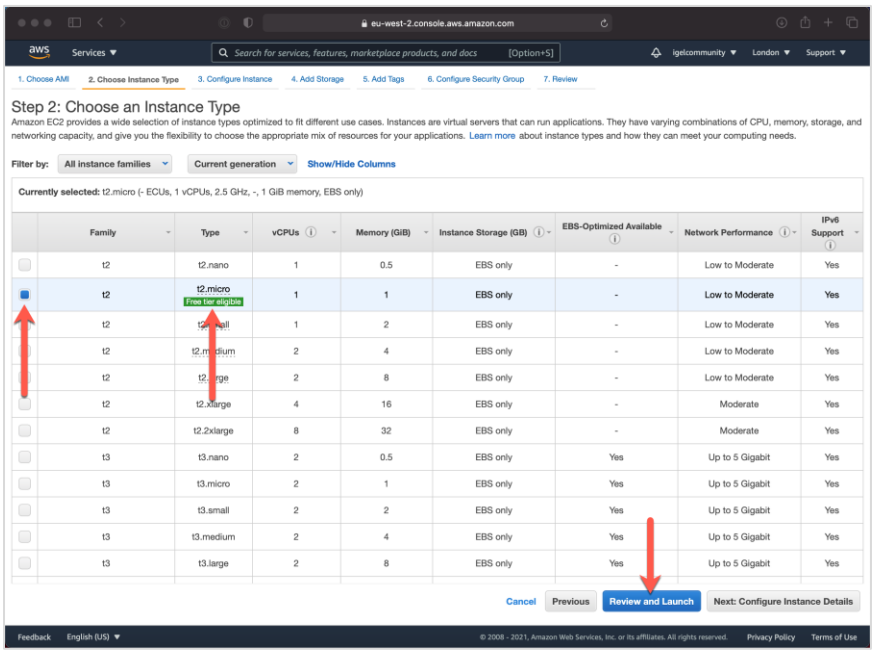


4. Click the **Select** button for **Ubuntu Server 18.04 LTS (HVM), SSD Volume Type** (or newer).

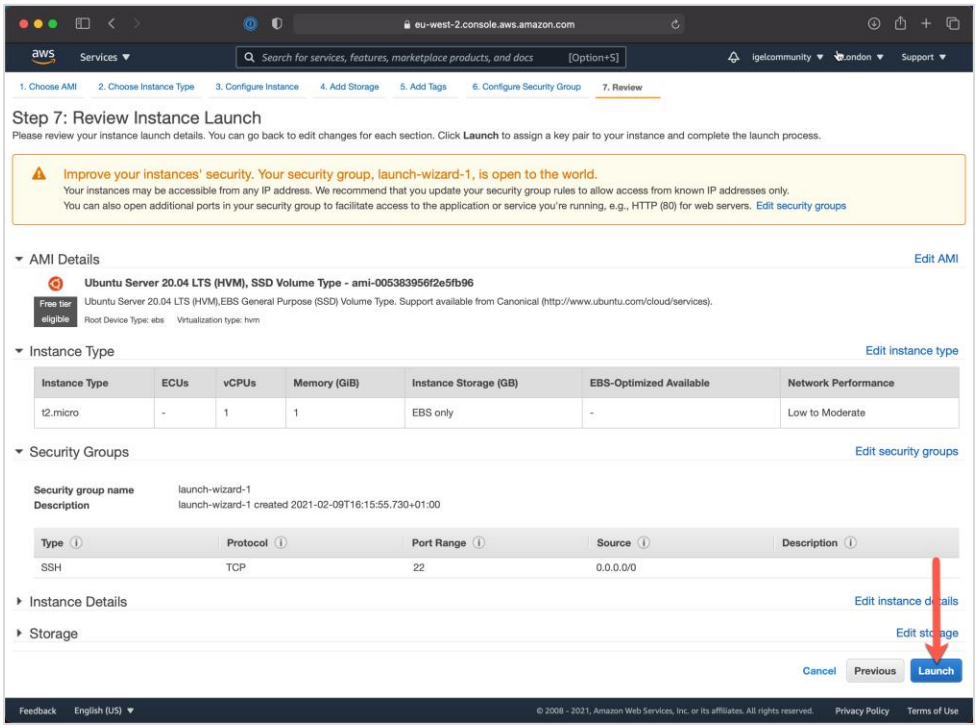


5. You are prompted to pick the type of instance to deploy. The amount of CPUs and RAM depends heavily on how many users you are required to support. For this example, you are creating a personal demo environment. The AWS Free Tier works fine for this use case. Click the **Review and Launch** button to continue.

> If you experience issues with slowness, please upgrade your instance to 2GB RAM

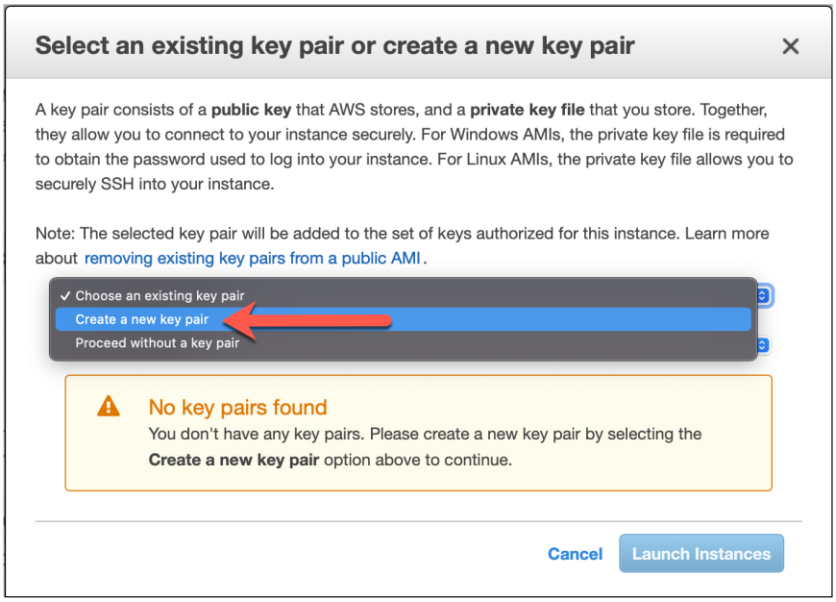


6. Confirm you selected the correct instance and click the blue **Launch** button to start the virtual machine.



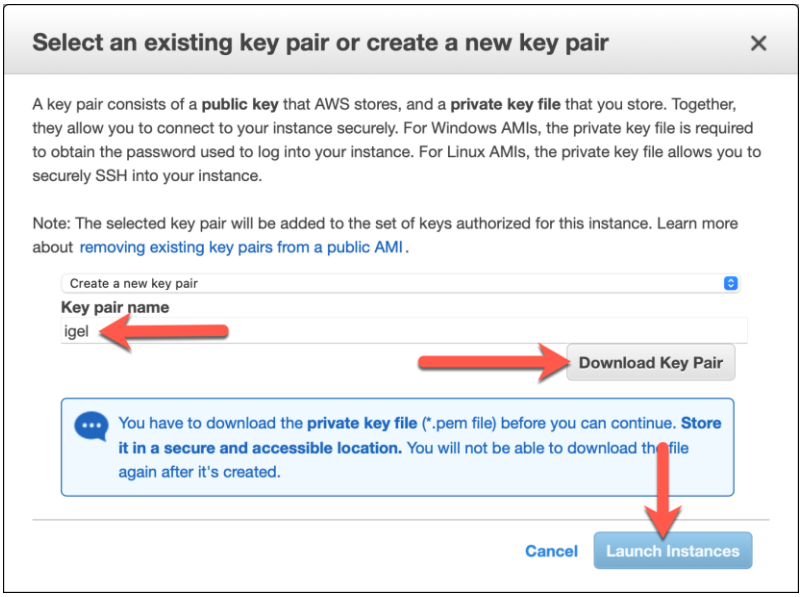
7. You are prompted to create a new key pair. This key is used to login to the ICG's Linux server via SSH and FTP. It acts as your login credentials.

   Select the **Create a new key pair** item from the dropdown list.



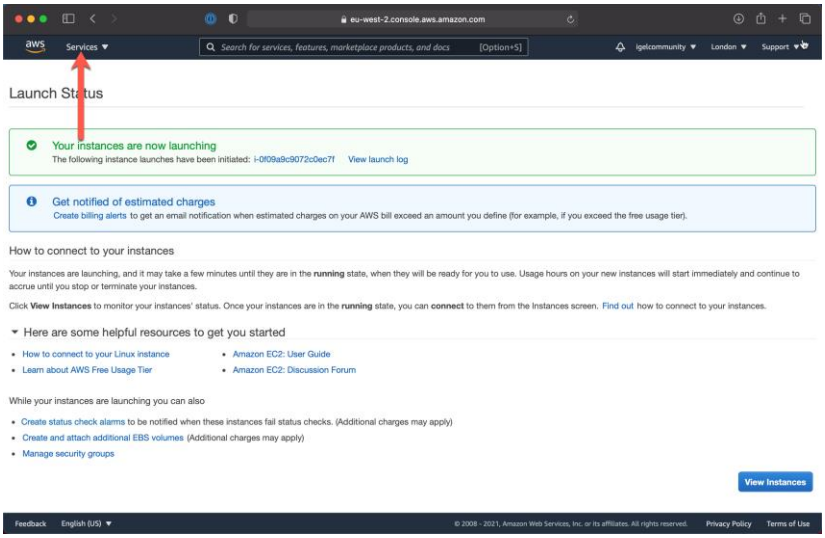
8. Enter a name for your key pair in the **Key pair name** text box and click the **Download Key Pair** button. The private key is downloaded to your local computer. You should keep this file in a safe place as if you lose it; you cannot redownload it.

   Once you have successfully downloaded the key, please click the blue **Launch Instances** button.

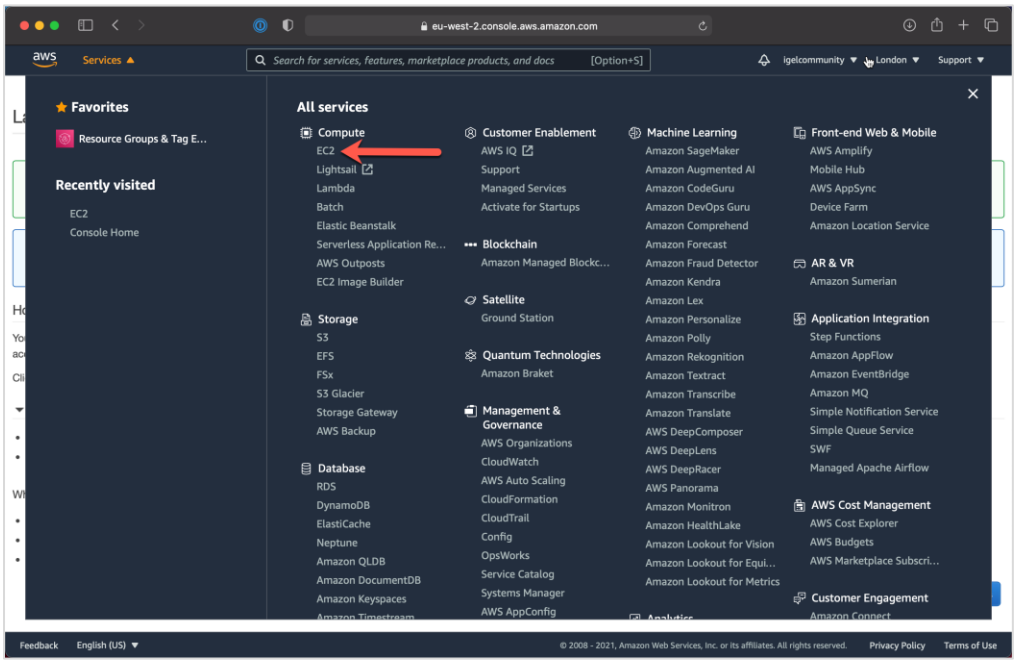


9. The file download looks something like the following, depending on your OS type. Please store it in an easily accessible and safe place.

10. Click the **Services** link located in the top menu.

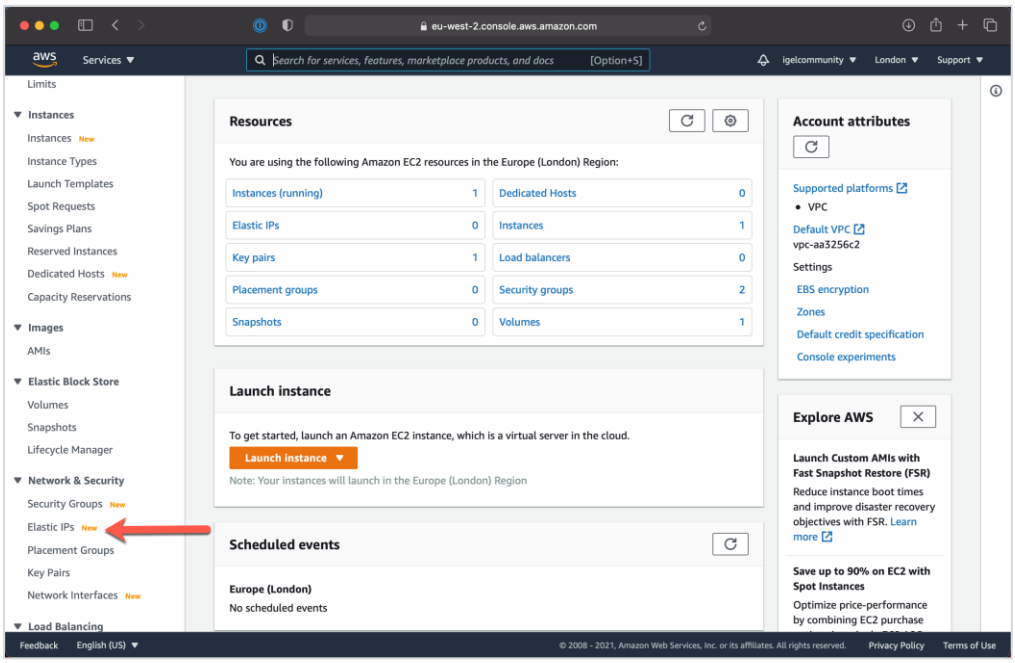


11. Click the **EC2** link.

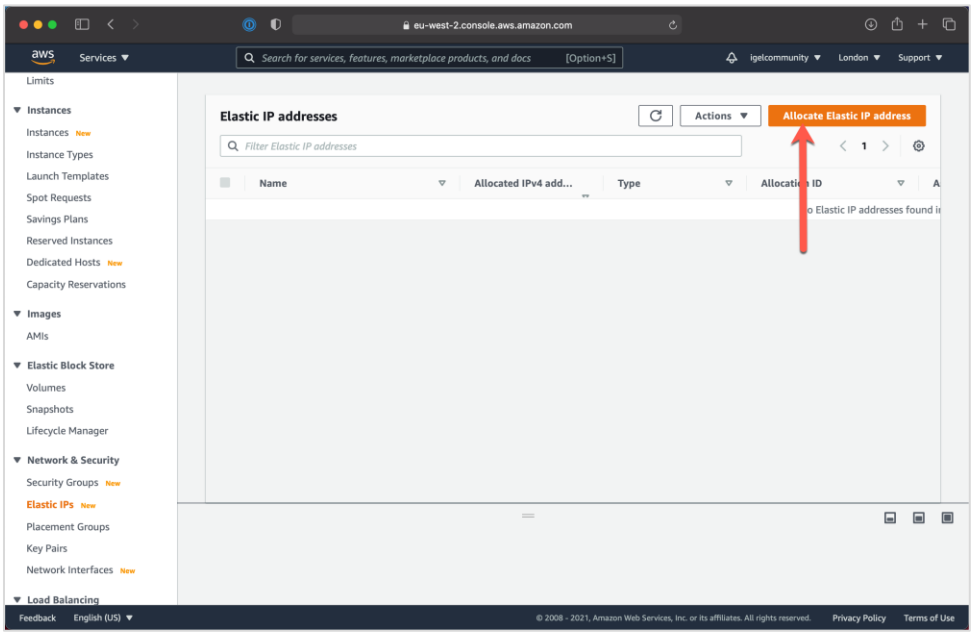


12. You are ready to add a static IP address to your newly created Linux instance.

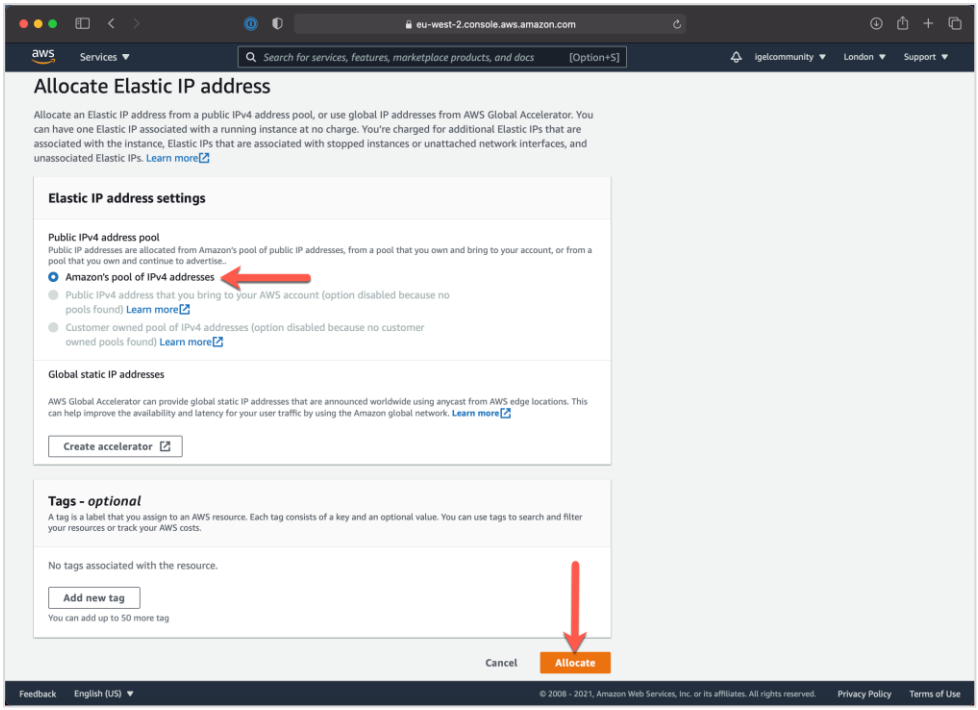
    Click to select the **Elastic IPs** link located in the left menu.



13. Click the orange **Allocate Elastic IP address** button.

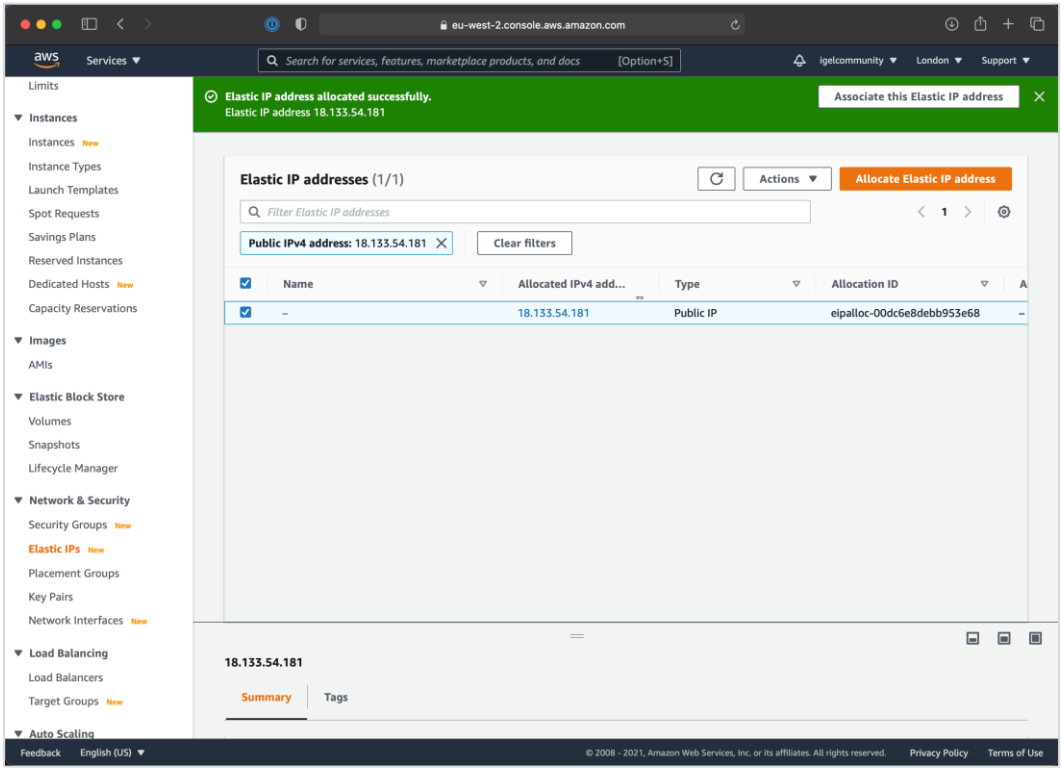


14. Click the blue **Allocate** button to continue.

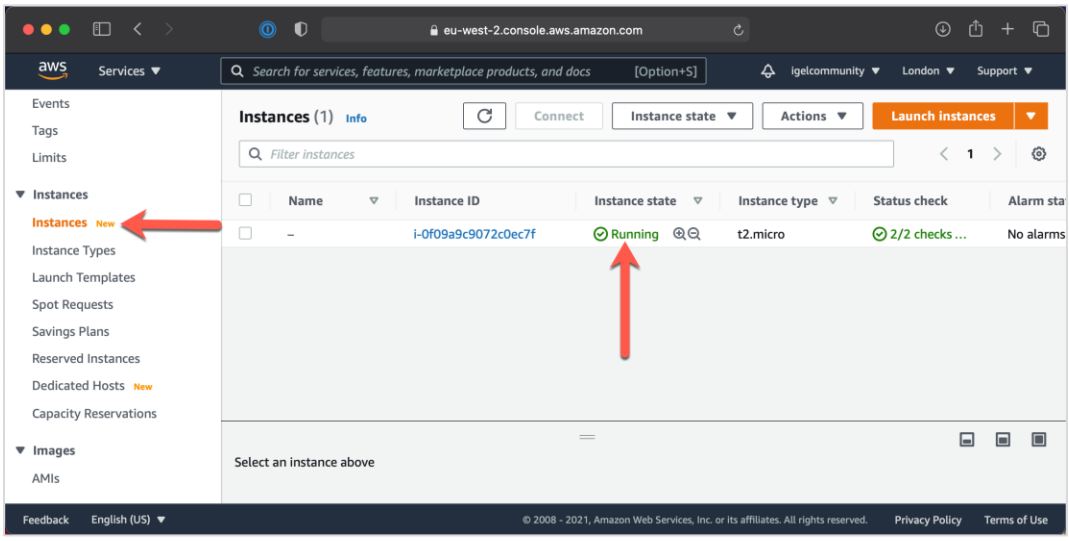


15. The IP address is now allocated, and the newly created address is displayed. Please make a note of this address for your records as you will use it soon and are required to create a DNS entry pointing to it.

    You are brought to the list of elastic IP addresses you have issued.

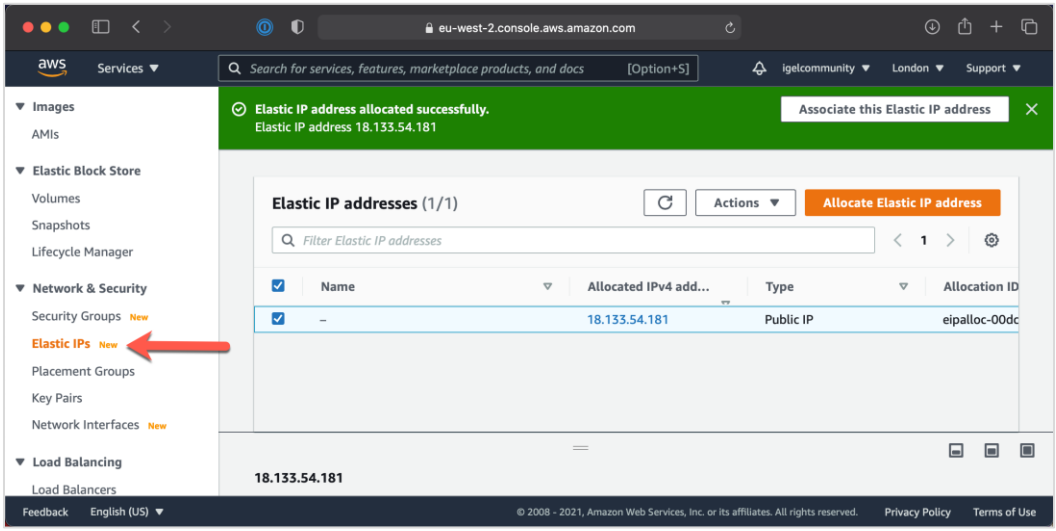


16. Click the **Instances** item on the left menu to view the new server and verify it is up and running. If all goes well, your view should be pretty much the same as the image below.

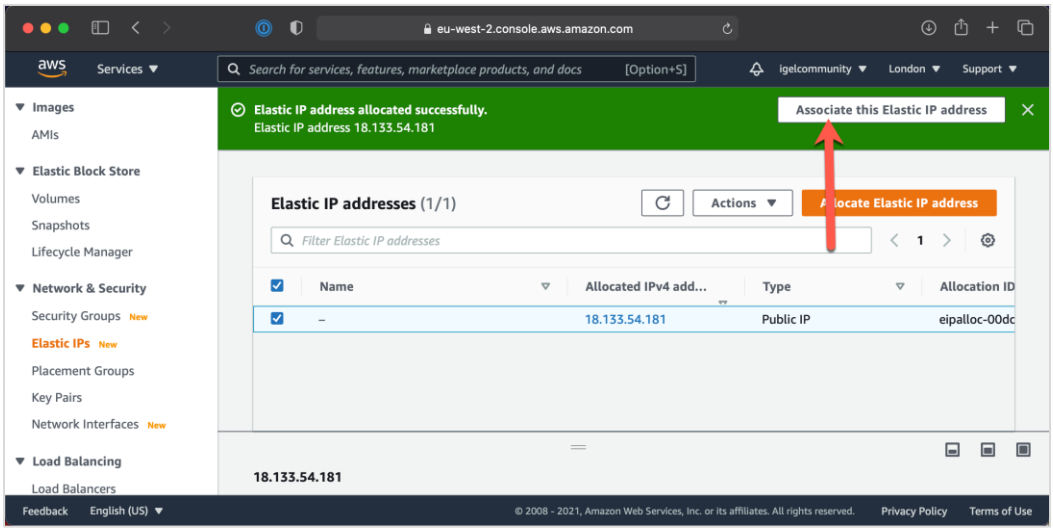


17. Now you need to assign the new IP address to your new Linux instance.

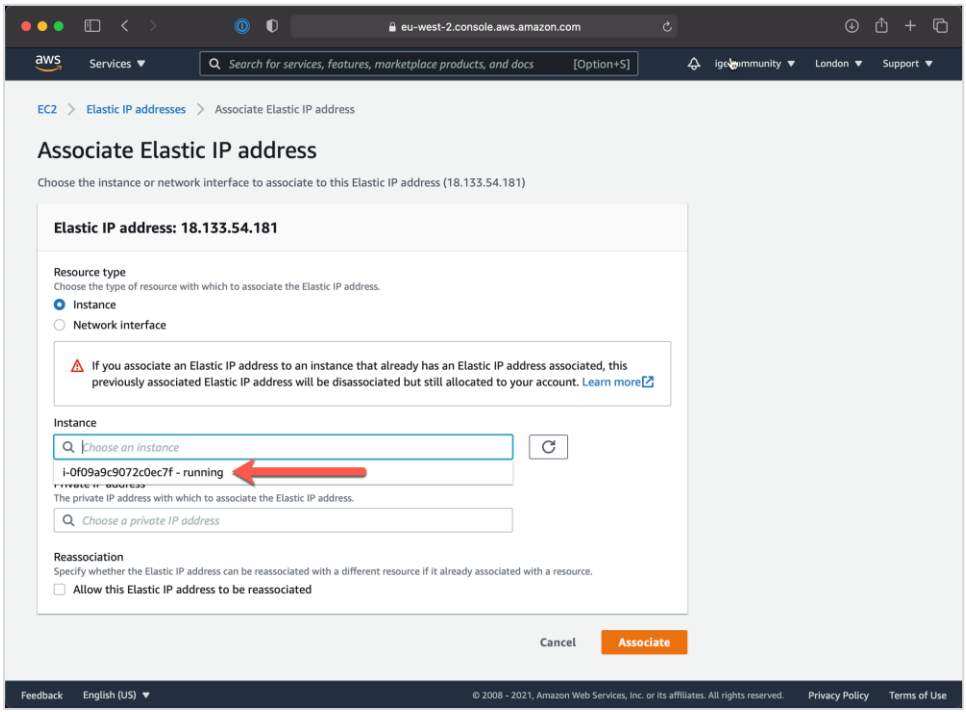
    Click on the **Elastic IPs** link located in the left menu.



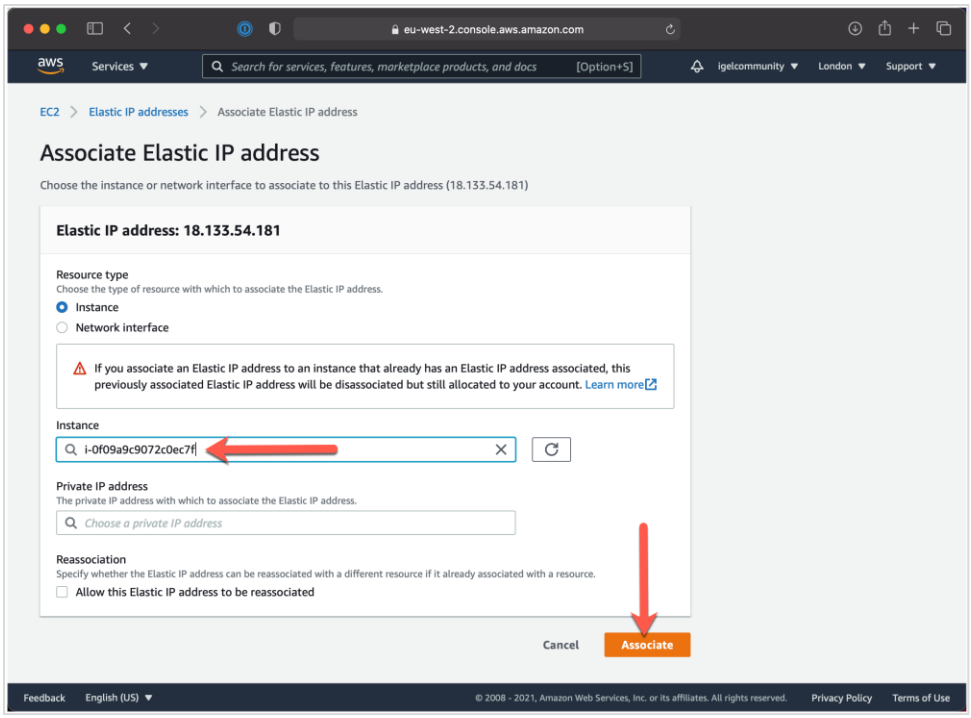
18. You are brought to the list of IP addresses issued, as seen above. Click to check the checkbox to the left of the IP address you wish to assign to the ICG instance and click the **Associate this Elastic IP address** button.



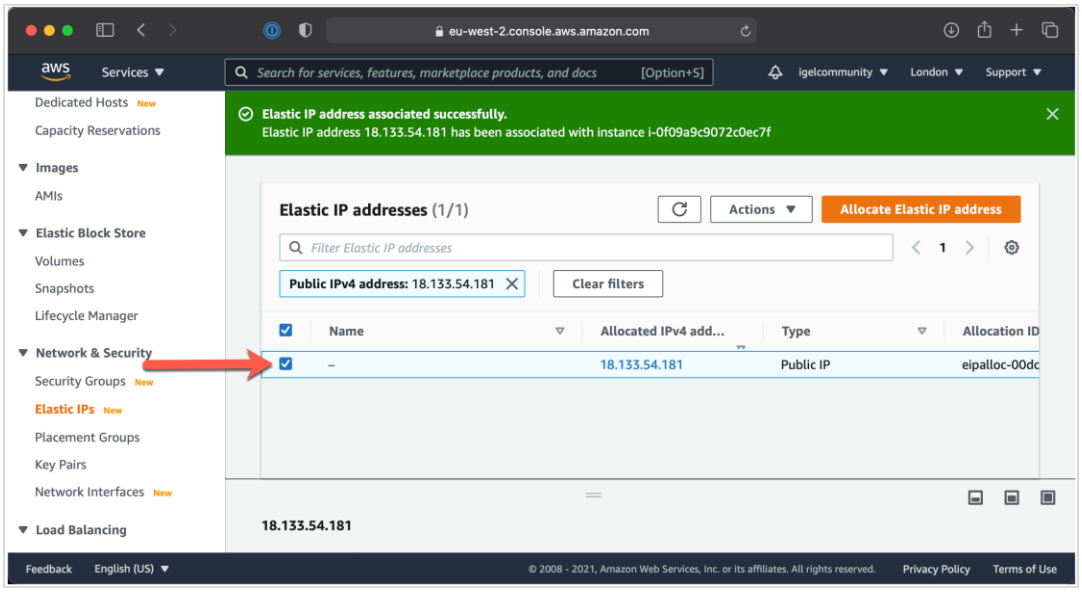
19. From the **Instance** combo box's dropdown list, select the freshly created ICG instance.



20. Verify you have selected the correct instance and click the blue **Associate** button to assign the IP to the selected AWS instance.

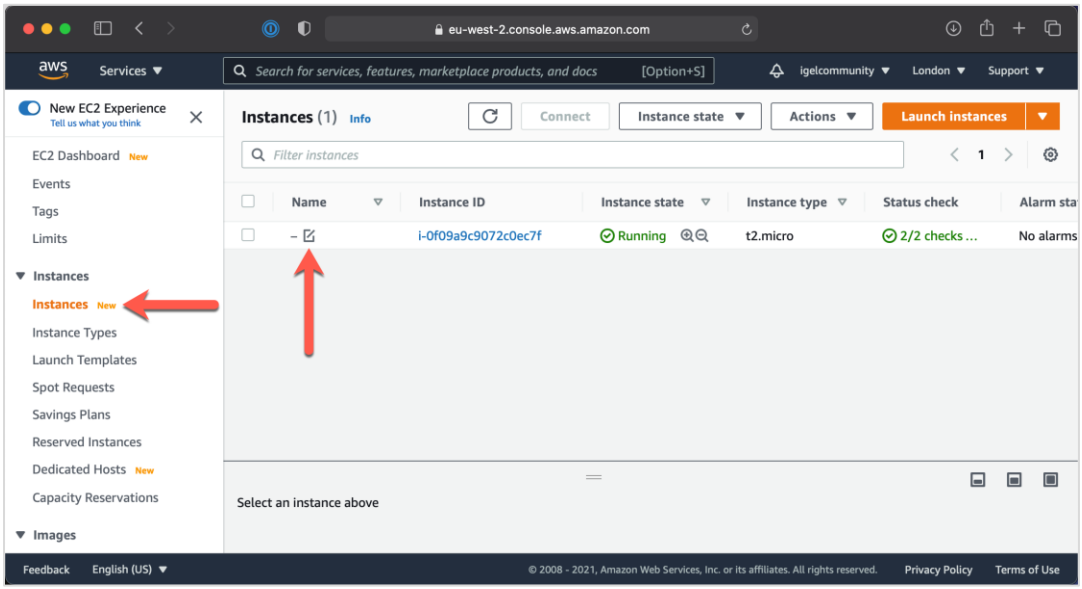


21. You are presented with the list of IP addresses and will notice it has been assigned to your new instance.

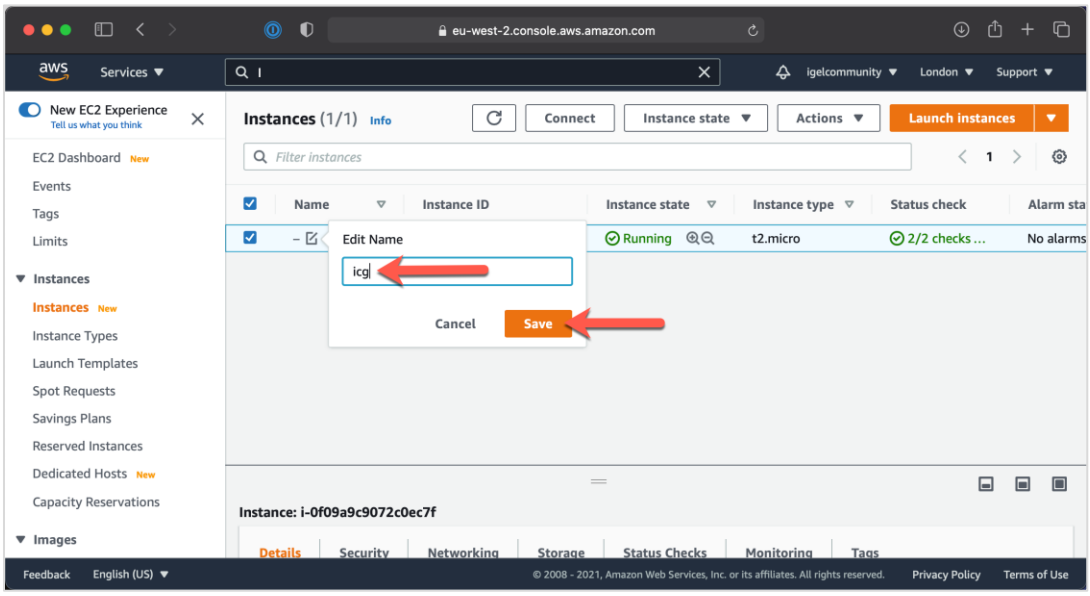


22. Before you move too far, it is always good housekeeping to give your new instance a name anyone can understand.

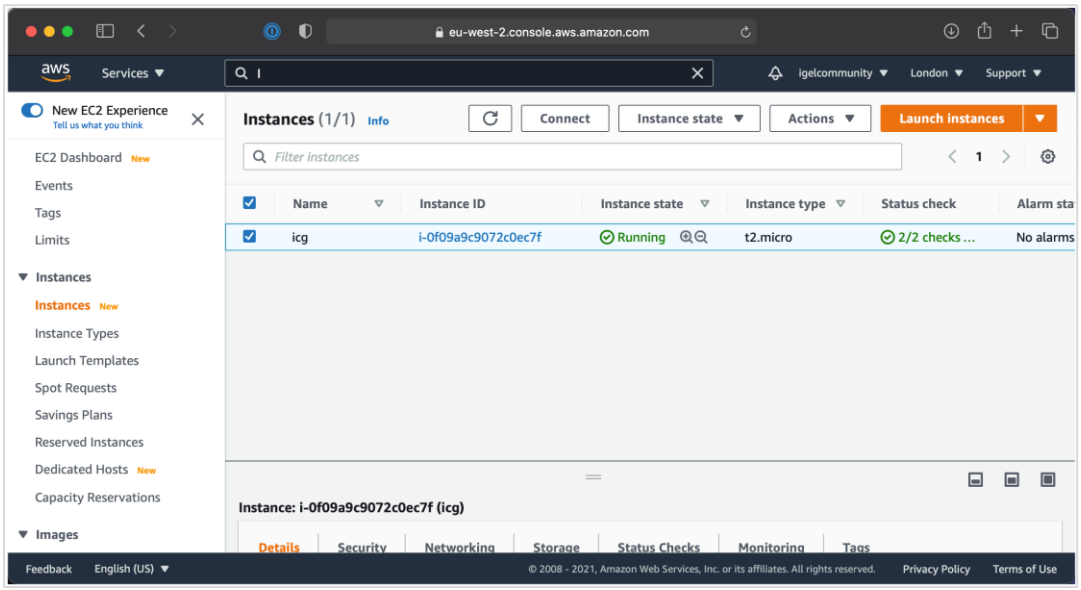
    Click on the **Instance** link in the left menu and hover over the IP address you wish to change the name of to reveal the edit icon. Click it to edit the name.



23. Type the new name for the EC2 instance and click the **Save** button to continue.



24. Your new IGEL Cloud Gateway instance is up and running with a working IP address and a friendly name.



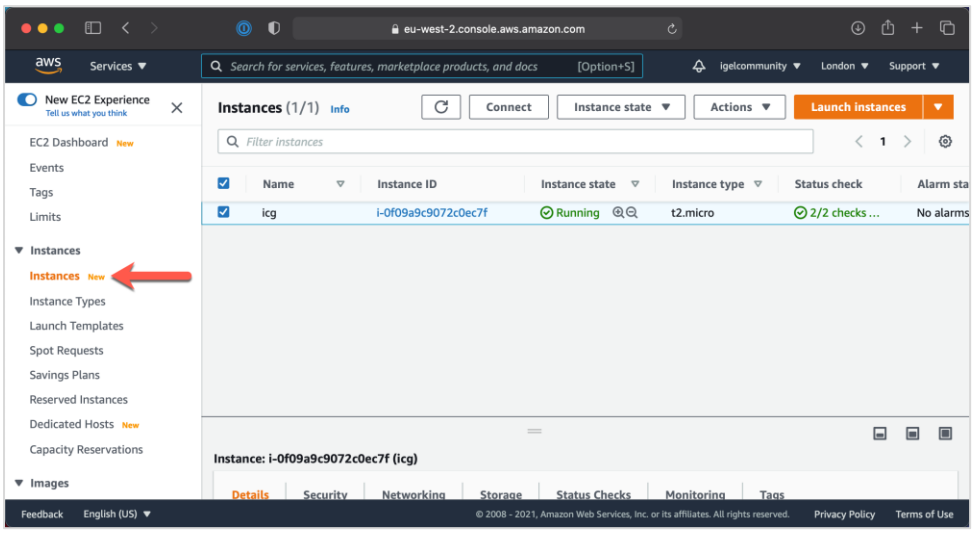
You are ready to configure the AWS firewall, create a certificate, and install the ICG software itself.

5. 3. How to Open Firewall Ports Required by ICG

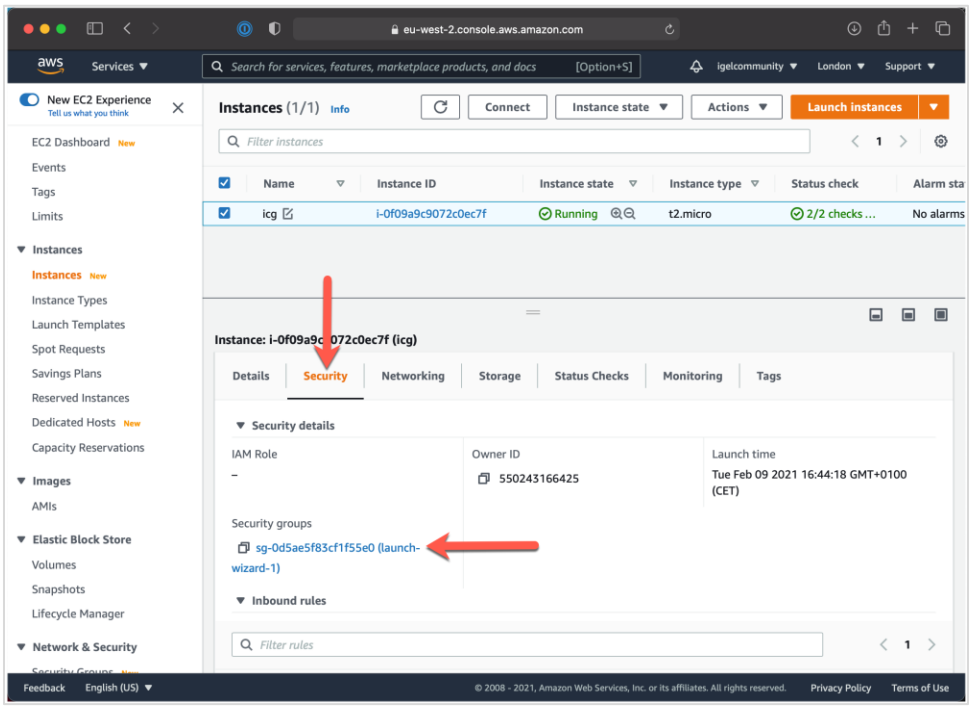
The ICG server communicates with the UMS over port 8443. Thus you are required to configure the AWS firewall with the proper rules to allow access.

The following details how to open the required ports:

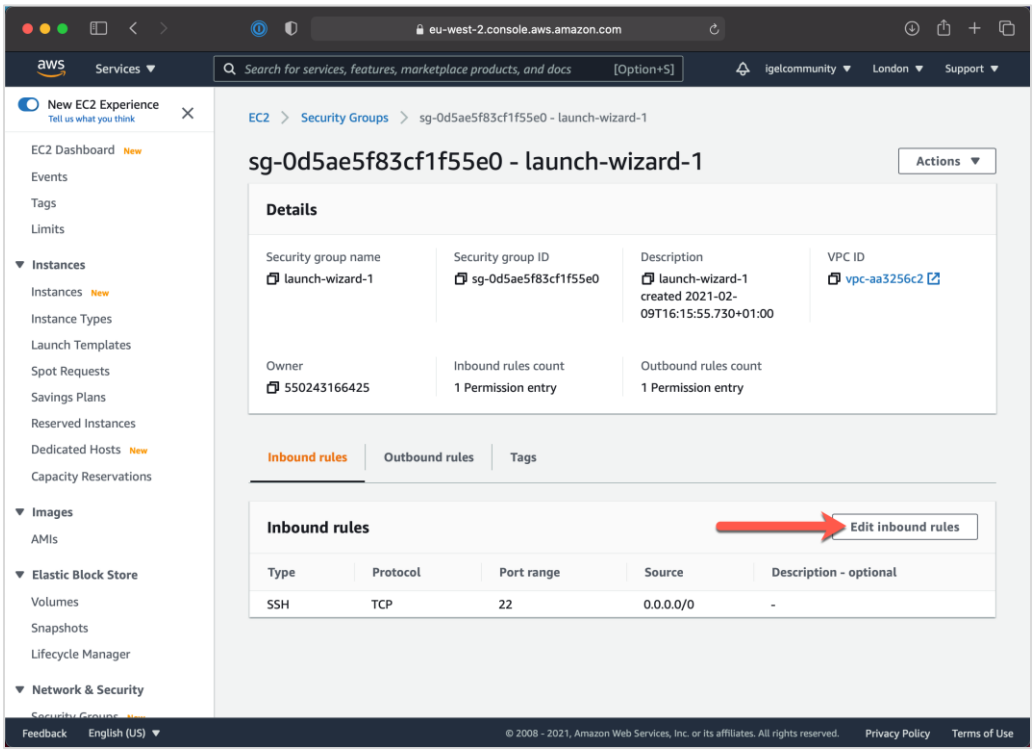
1. Click the **Instances** link located on the left menu.



2. Click to select the newly created ICG instance and scroll down to the **Security** tab. Click the **launch-wizard-1** link (your security group's name might have a different number associated).

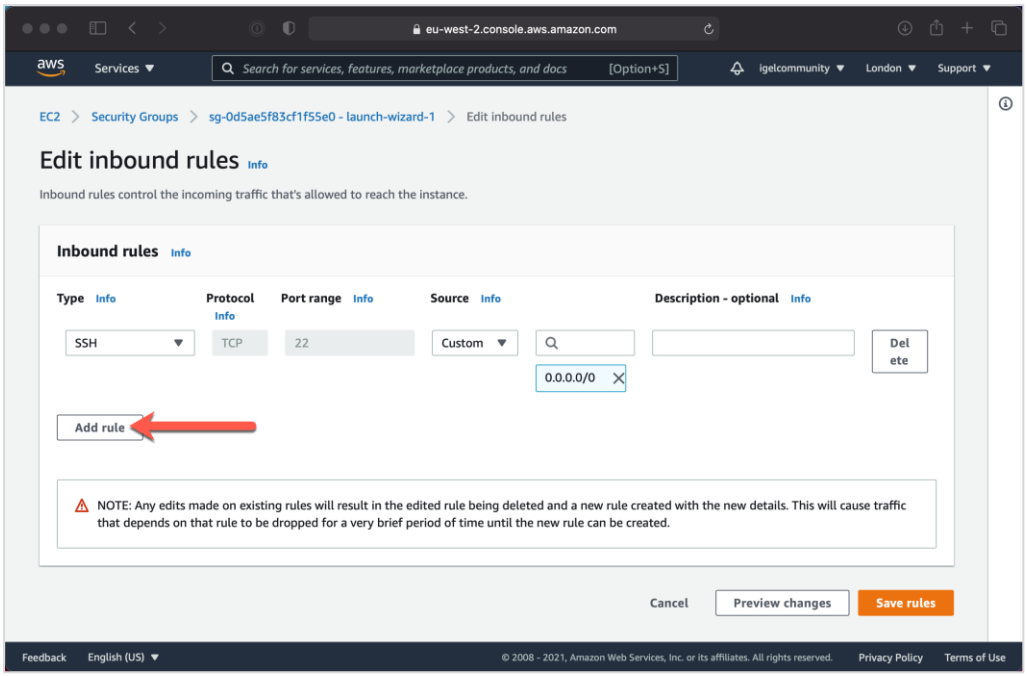


3. You are brought to the **Inbound rules** tab. Click the **Edit inbound rules** button.



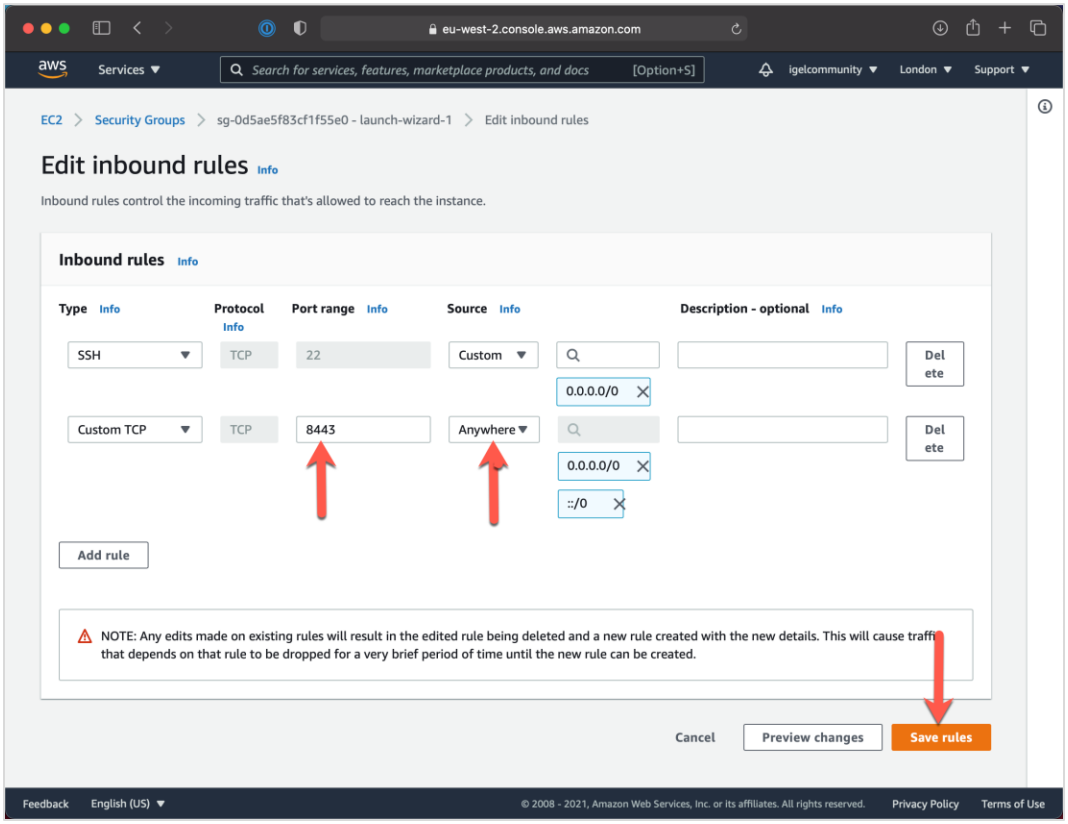
4. The **Edit inbound rules** window opens, allowing you to add, delete, or edit inbound rules. In this case, you need to create a new rule for UMS/ICG traffic.

   Click the **Add Rule** button.



5. Configure the new rule as follows:
    - Type: **Custom TCP**
    - Protocol: **TCP**
    - Port Range: **8443**
    - Source: **Anywhere**

Click the blue **Save rules** button to save your new rule and continue.



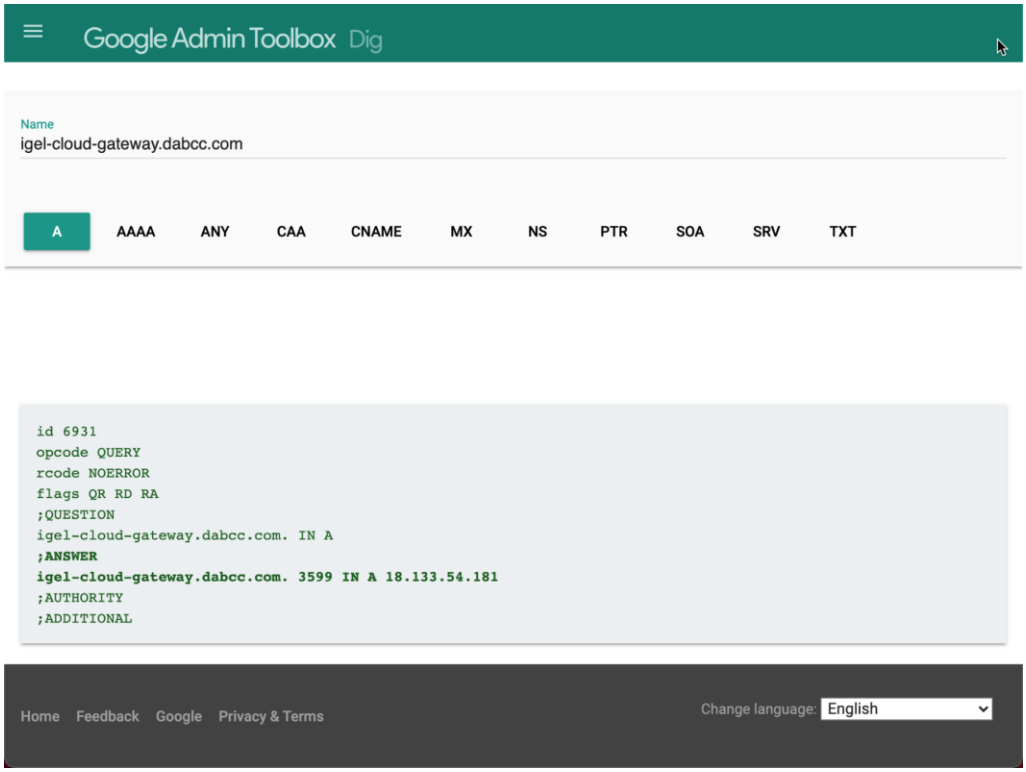
5. 4. Create Required DNS Records

It is time to create the required DNS entries for your new IGEL Cloud Gateway. These records are needed to be made on a public-facing DNS server. For example, DYN.com

- Create a new **A record** with the name **igel-cloud-gateway. <yourdomain.com>** pointing to a public IP address of your ICG Cloud Gateway server.
- Add a **TXT record** for the host **igel-cloud-gateway** with the data: **https://<public ICG server IP address>:8443/usg/endpoint**

It is recommended to use a tool like **Google's G Suite Toolbox Dig** to verify your TXT entry is set up and working correctly

Enter the DNS name of your ICG server and click to select the **TXT** link. If all goes well, you should see a happy green text displaying the query was answered correctly.



Now when users enter their email address user@example.com as the server address in the ICG Agent Setup, the setup looks up the record on the domain name server to find the corresponding ICG address.

> Depending on your DNS host, it could take up to 24 hours for your DNS changes to take effect across the globe. To verify the required DNS entries are active, you can use the **DNS Propagation Checker**.

5. 5. How to Create an SSL Certificate for ICG

To use the ICG, you are required to create an SSL certificate. This can be done in many ways, including both public and private certificate authorities. For the best experience and usability from the ICG, it is recommended to have a publicly signed certificate.

In the following steps, we walk you through how to obtain and install a public certificate that costs only $15 (per year) from PSW Group (**http://www.psw.net/**). This is a small price to pay for the benefits it brings. However, if you do wish to try it without spending any money, you can select the free 1-month SSL certificate from the list, as shown below. You can also generate a certificate from the authority of your choosing or even create a self-signed certificate.

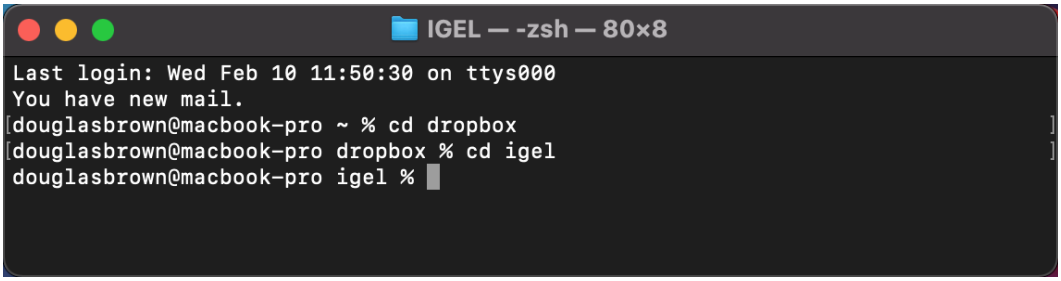
> The following steps use an SSL certificate from pws.net, which is excellent for our use case and more affordable. However, this SSL certificate has only one root CA and no intermediate certificates. To use a more expensive yet flexible certificate that comes with a root CA certificate and an intermediate certificate, please refer to the **How to Use a DigiCertificate SSL Certificate with ICG** white paper to learn how to deploy a certificate from **http://www.digicert.com**.
>
> One of the main benefits of a public certificate is that you are not required to enter the part of the certificate fingerprint while connecting the IGEL OS to the ICG. Not to mention, it is always more secure when using a trusted certificate authority as there is a piece of mind that comes with knowing the certificate was vetted prior.

To procure the required SSL certificate for your Cloud Gateway server, you need to create a certificate request file (CSR). Since you already created your ICG server, you will do this from its command line.

The following details how to create and request an SSL certificate from PSW.net:

1. First, you need to log in to the ICG server via SSH. This can be done using your favorite SSH client or even the Terminal app on a Mac.

   Open the SSH client and browse to the location of the pem file you created when setting up your ICG instance on Amazon. In your case, it was saved as **igel.pem**.



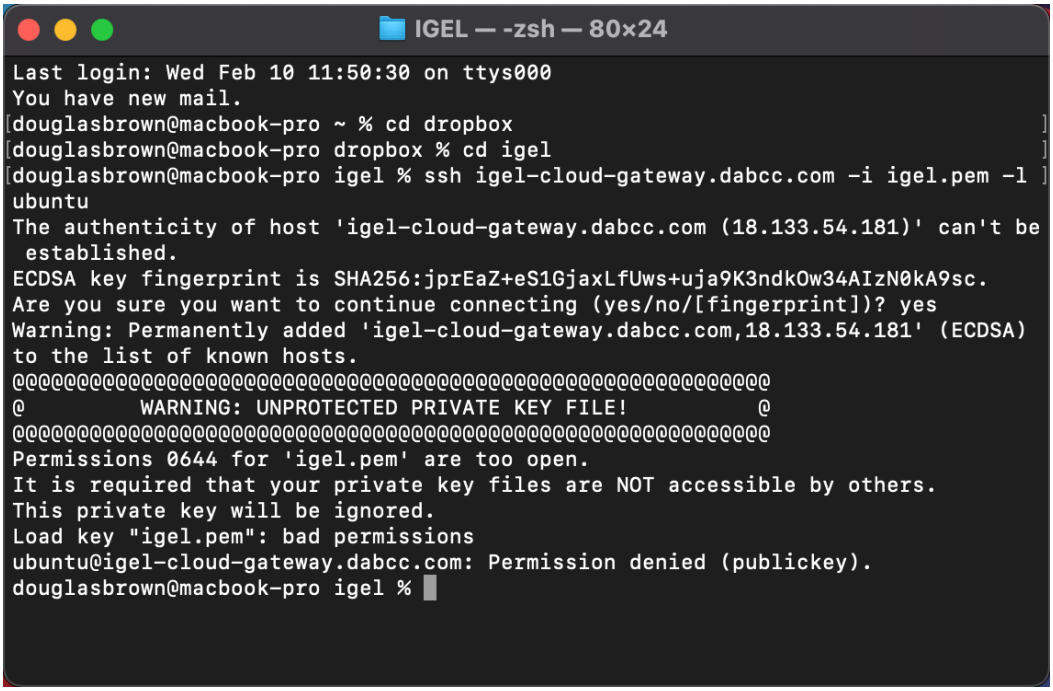
2. Log in to the remote ICG instance by typing the following:

   ssh <FQDN of ICG server> -i <name of pem file> -l <username>

   > To log in from a Windows desktop, please refer to the following AWS article - How to log in to your ICG instance using Windows and Putty: **https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html**.

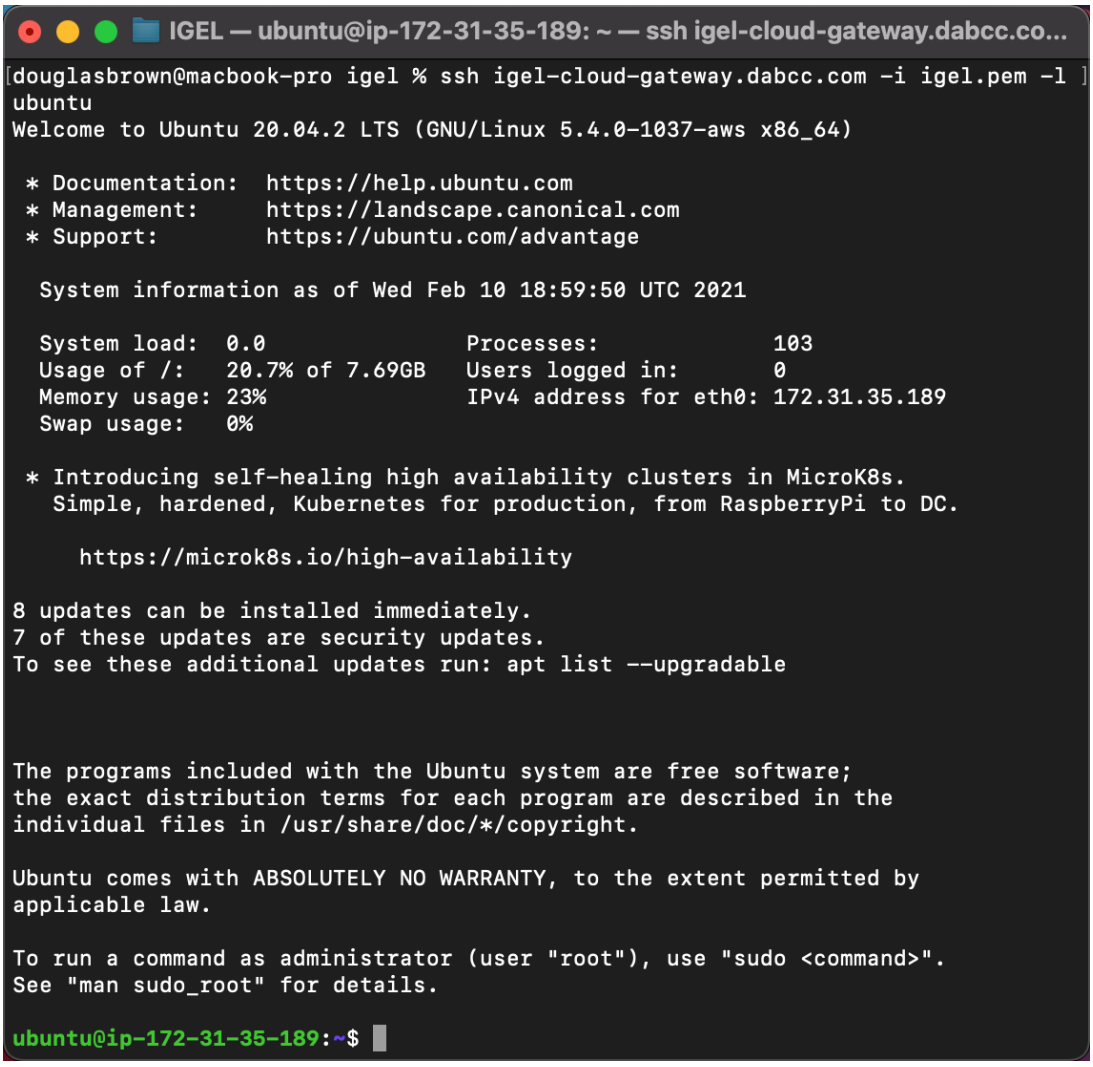
   In the first login, you are prompted to verify the authenticity of the ICG host. Type **yes** to continue.

3. You might be presented with the following screen. In this case, you will need to give the correct permissions to secure your pem file.



4. Type the following: **`chmod 400 <name of pem file>`**

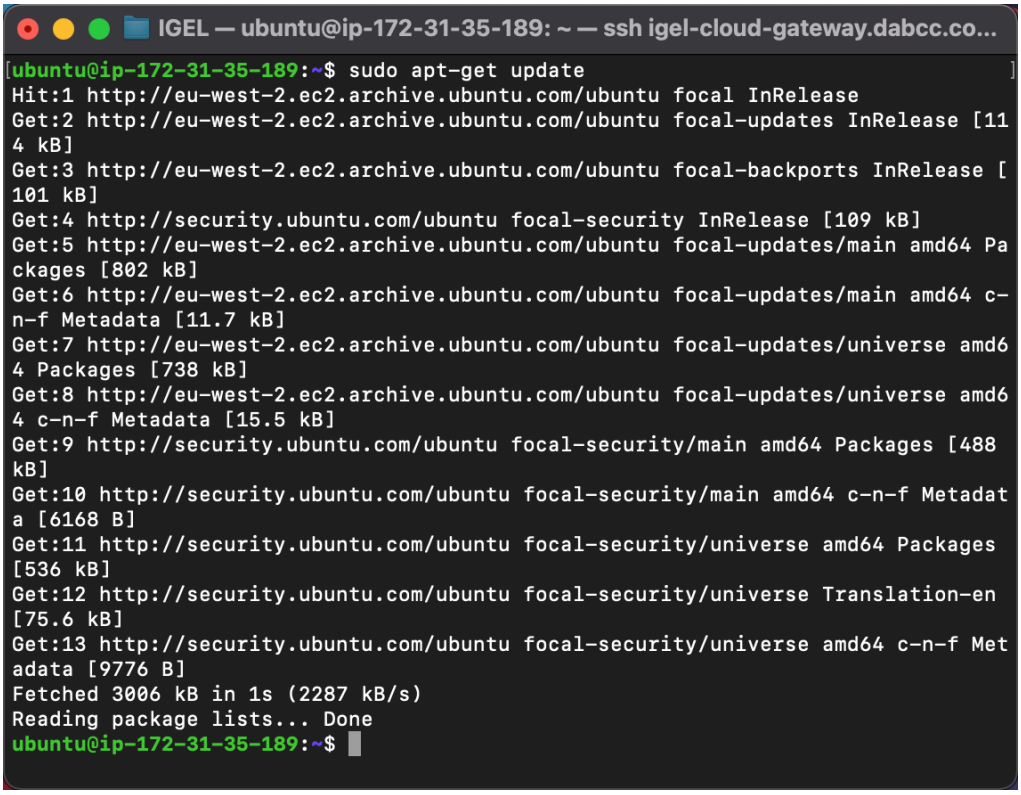
5. Try the login again. Type **`ssh <FQDN of ICG server> -i <name of pem file> -l <username>`** and hit enter.



6. It is always important to update your new server with the latest updates, fixes, and security patches.

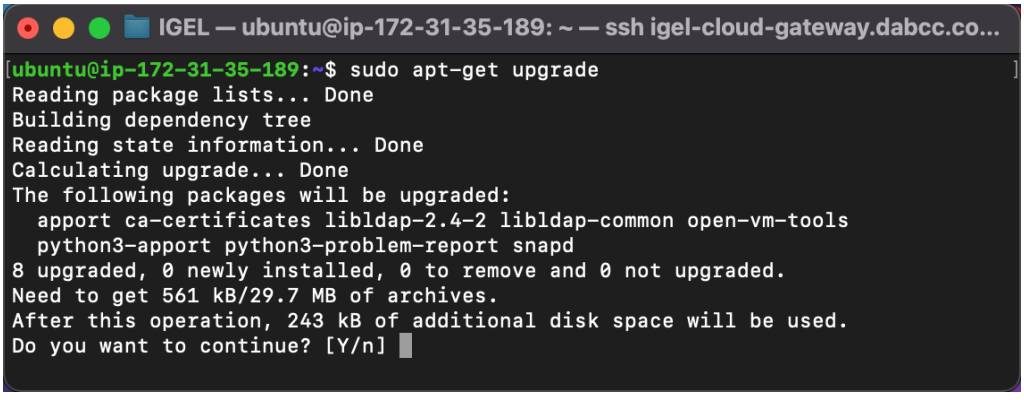
   Type the following:

   sudo apt-get update



7. To update, type the following:

   sudo apt-get upgrade

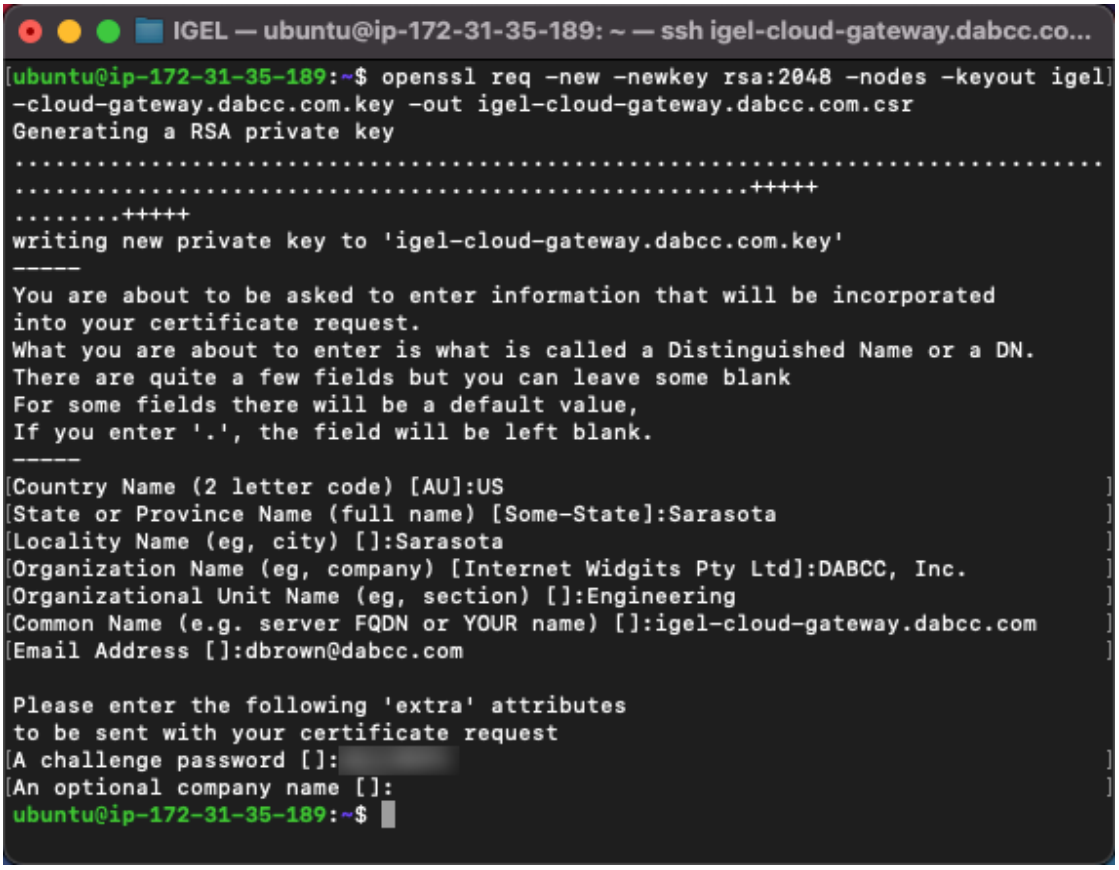


8. You are ready to generate a CSR. To do this, type the following:

   `openssl req -new -newkey rsa:2048 -nodes -keyout igel-cloud-gateway.<your domain>.key -out igel-cloud-gateway.<your domain>.csr`

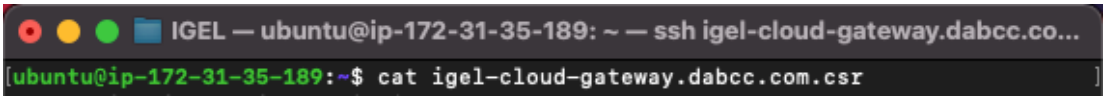
9. You are asked to enter a bit of information that is used within your certificate request. This information needs to be valid as the Certificate Authority will verify it before issuing you a certificate.

   Enter your information until the CSR is successfully created.

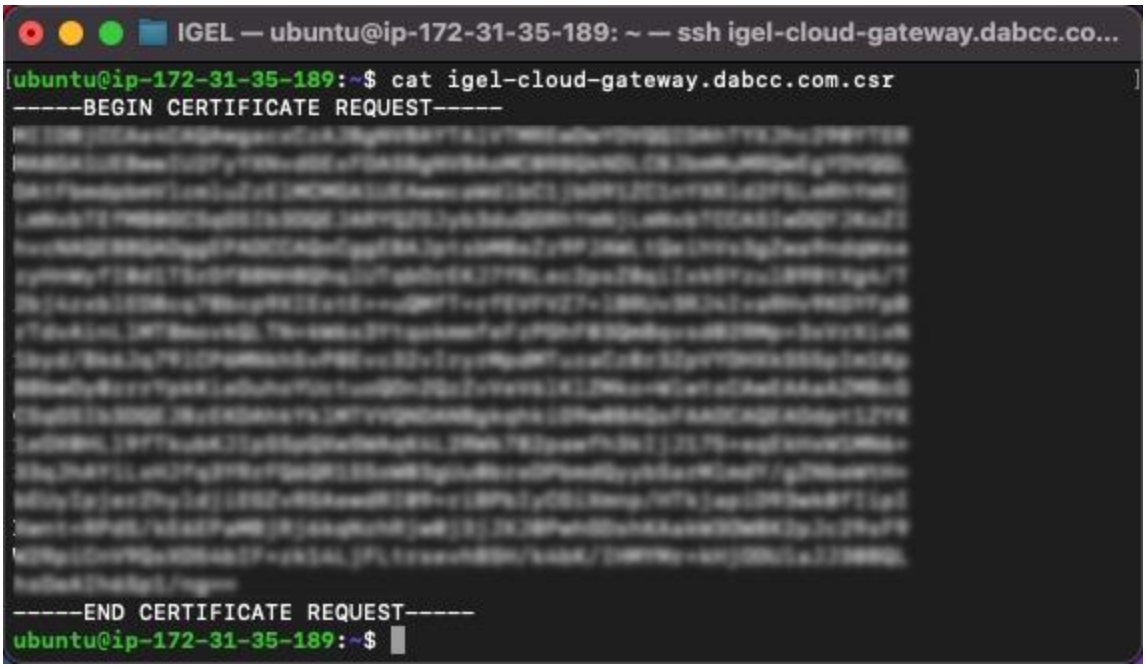


10. To view your newly created CSR file, type the following:

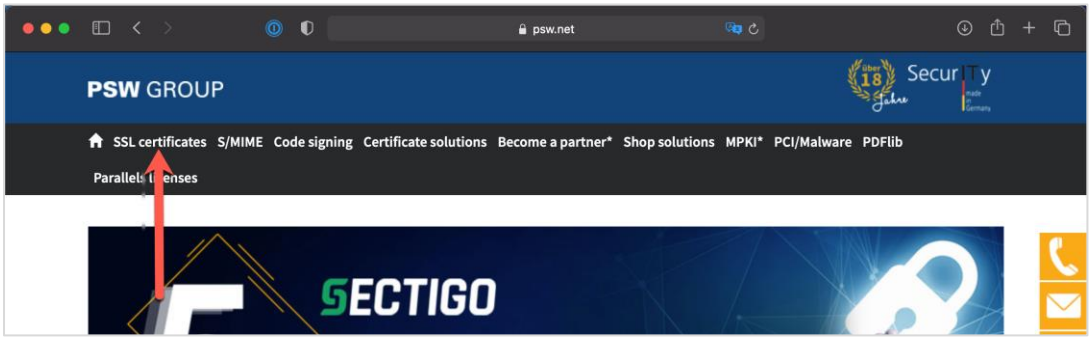
    `cat igel-cloud-gateway.<your domain>.csr`



11. Copy all text starting with ------ **BEGIN CERTIFICATE REQUEST** ------- through --------**END CERTIFICATE REQUEST**------. Please save it to a text file, as you will submit it to the certificate authority in a few steps.

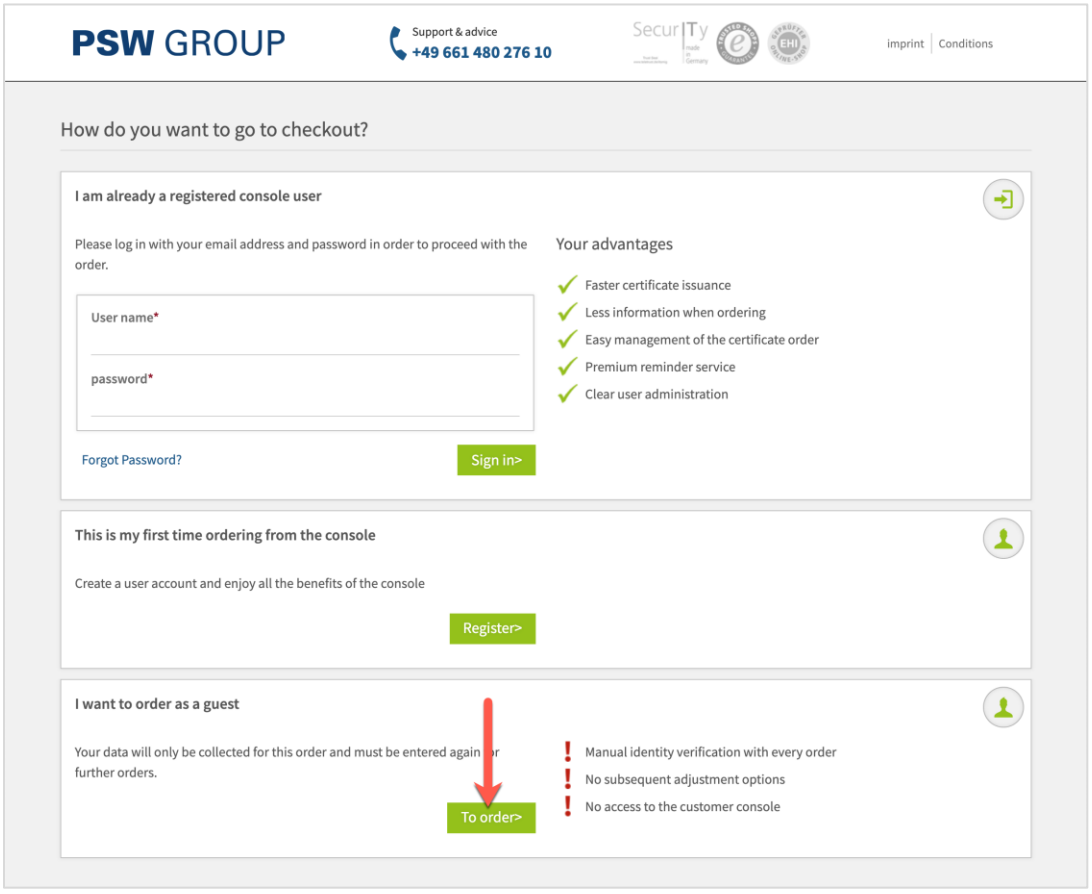


12. Browse to **http://www.psw.net/** and click the **SSL Certificates** link on the top left of the page.



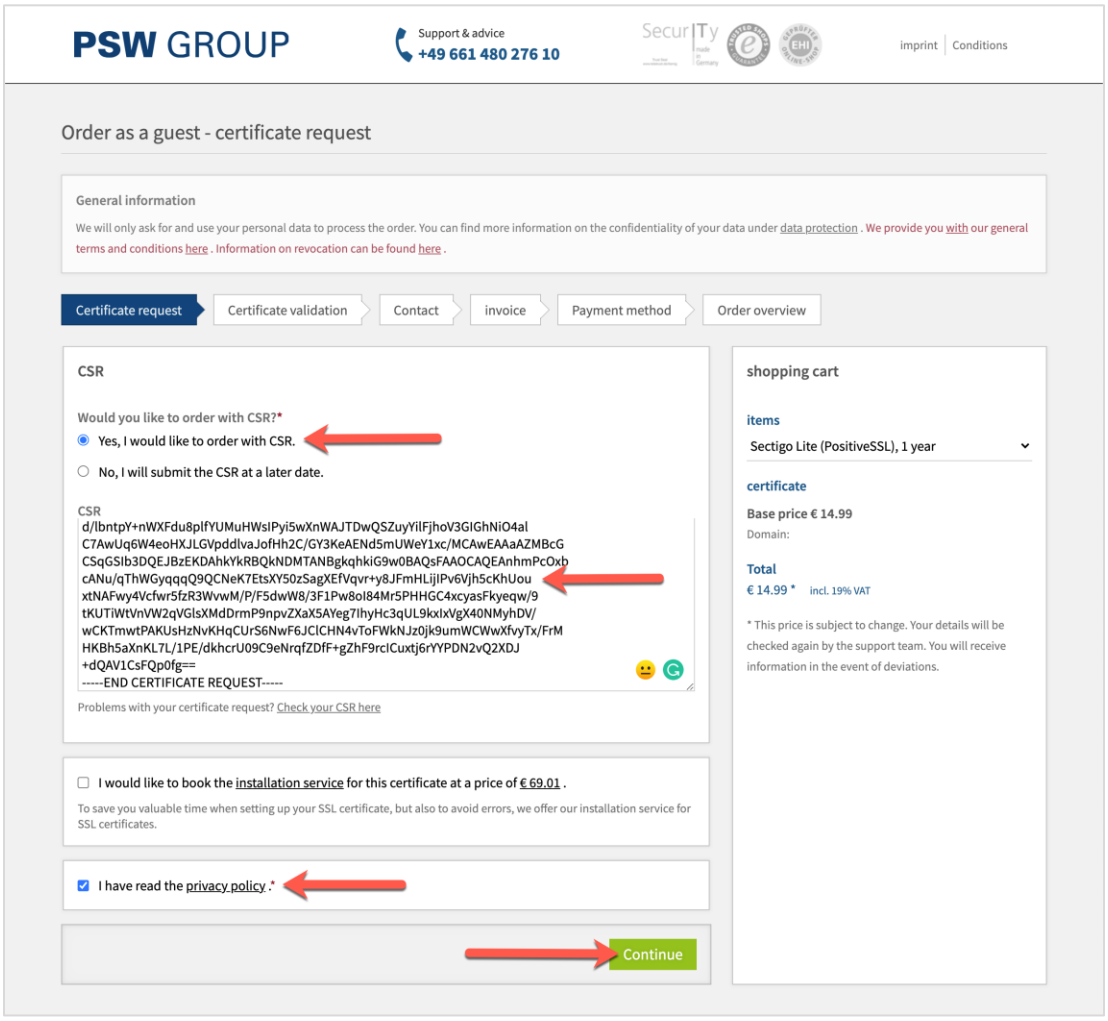
13. Scroll down until you find the **ORDER CERTIFICATES DIRECTLY: INDIVIDUAL CERTIFICATES** section and click either the 30 day or 1-year link. This is up to you.

14. You are prompted to log in, create an account, or order as a guest. For this example, we will order as a guest. Please click the **To order** button to continue.

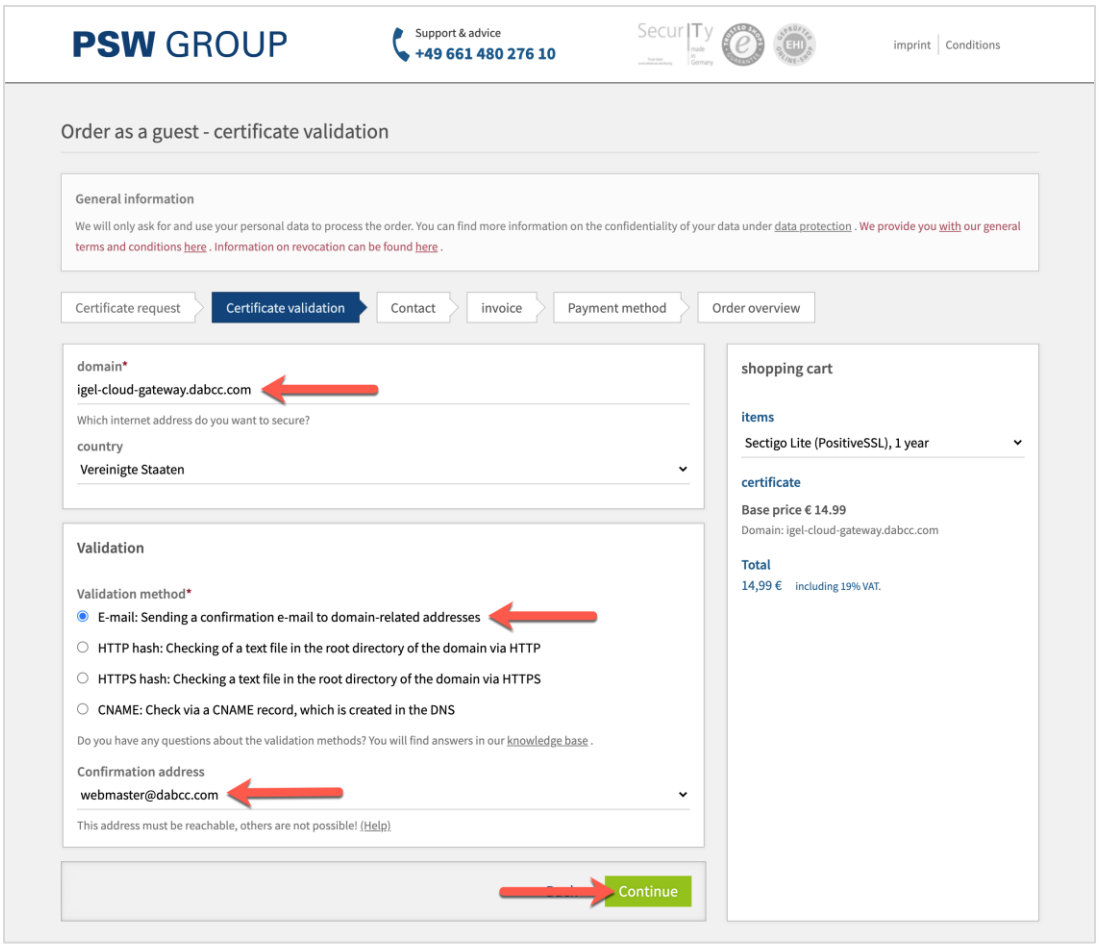


15. Next, you are prompted to create the Certificate request. Click the **Yes, I would like to order with CSR** radio button and then enter the CSR file created above into the CSR text box.

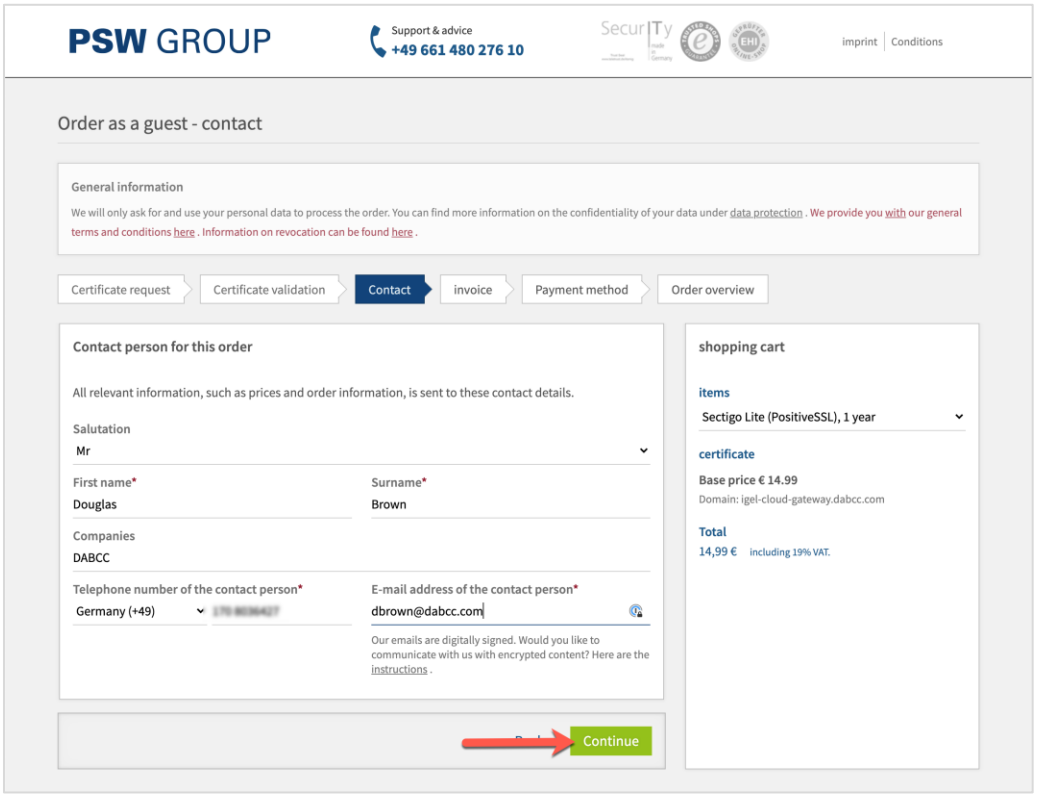
    Scroll the page down to click the **I have read the privacy policy** checkbox and then click the **Continue** button.



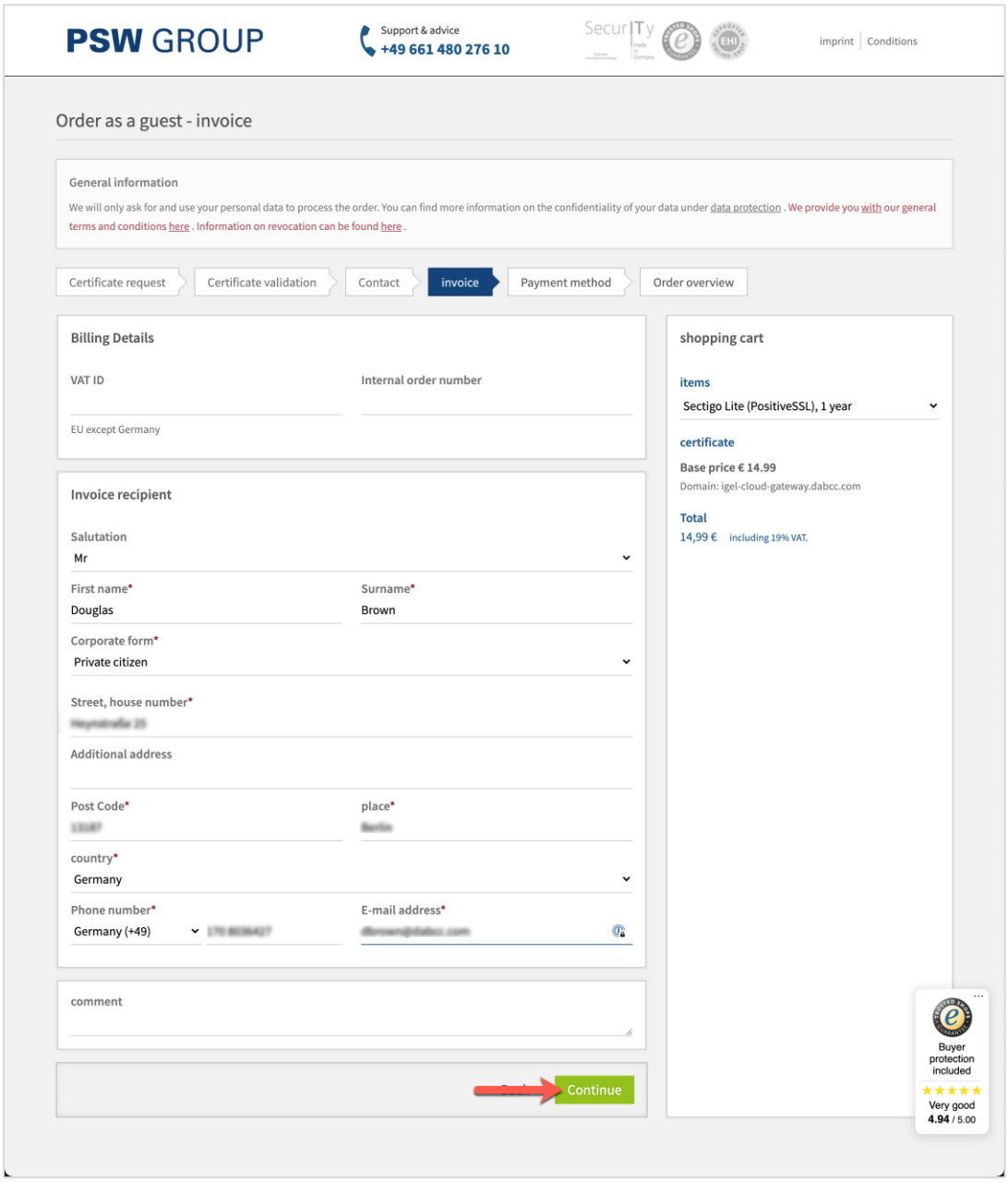
16. Next, you are required to enter your details for certificate validation. Enter the domain name you used when creating the CSR into the **domain** textbox. Select the validation method you wish to use. For this example, select the email method. Then, enter an email address that will be used to validate the certificate from the **Confirmation address** combo box. Once finished, click the **Continue** button.



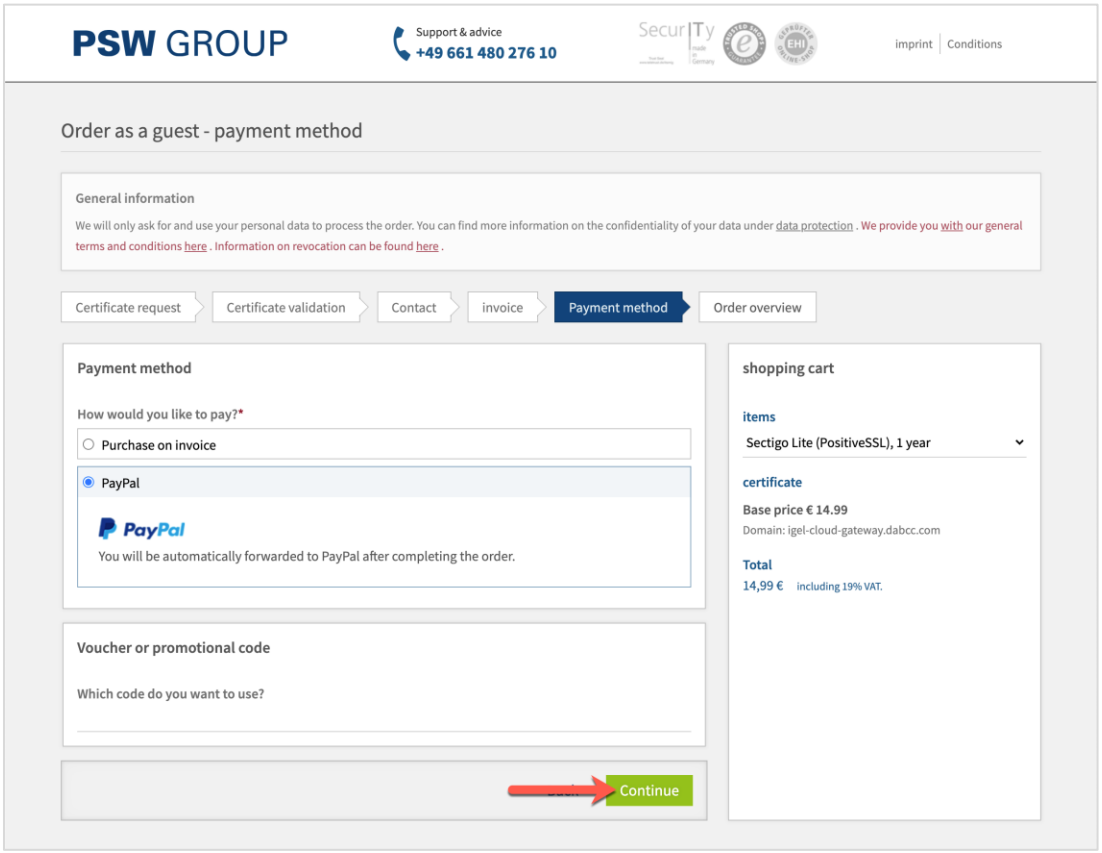
17. You are prompted to enter your contact information, name, address, company, telephone, and email address. Once finished, click the **NEXT** button to continue.



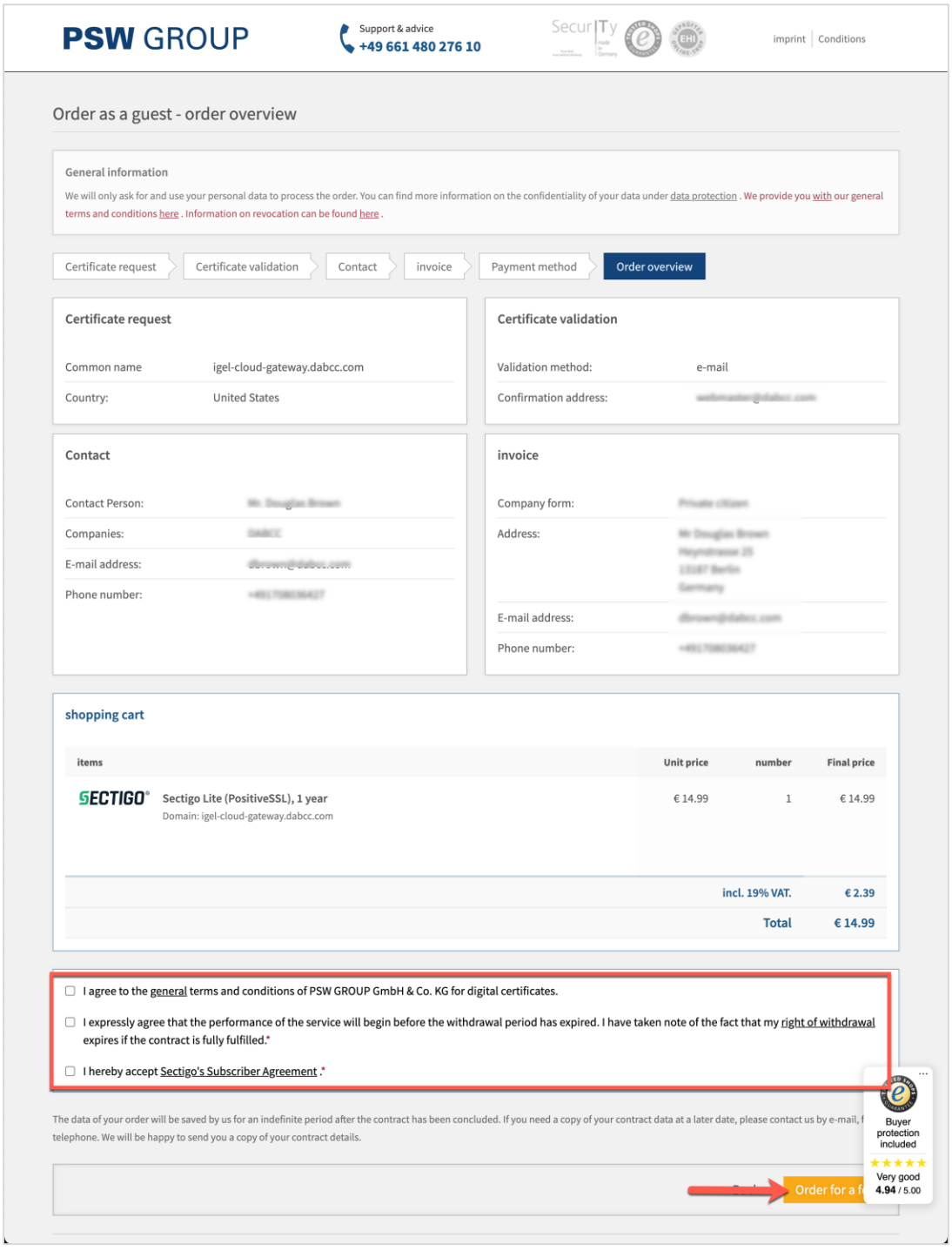
18. Enter your payment info and click the **Continue** button.



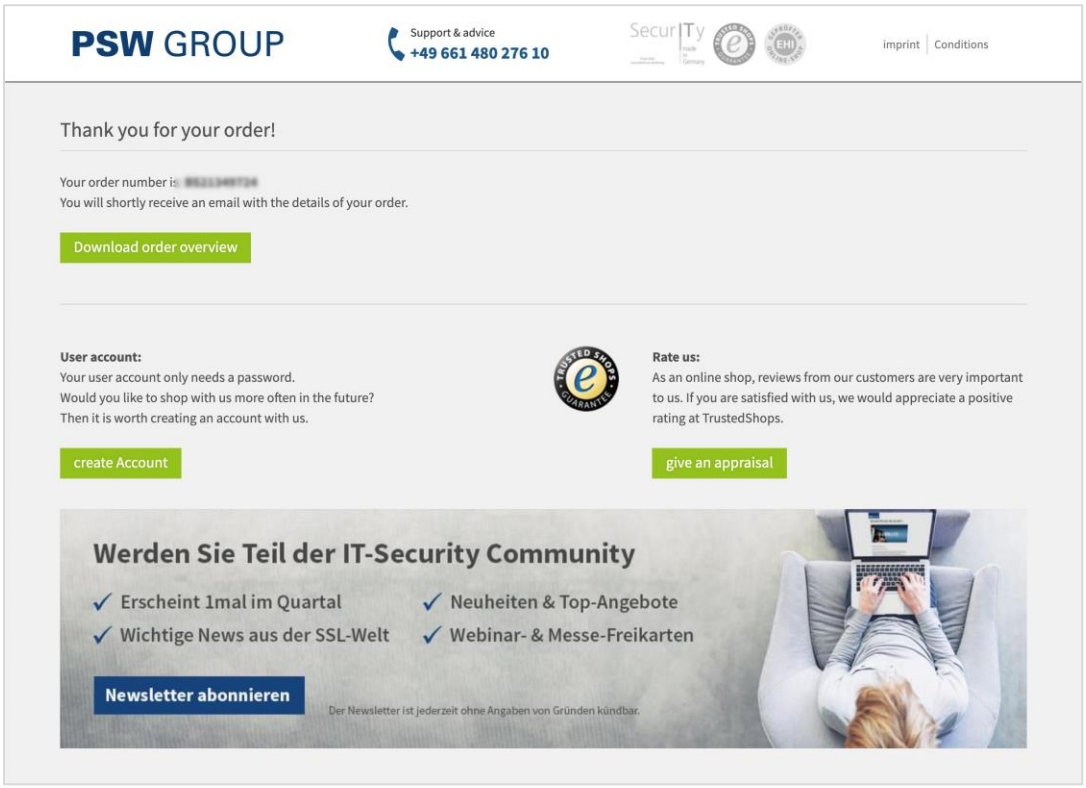
19. Enter your desired payment method, and click the **Continue** button.



20. You are done. Verify all information is correct, check the required legal checkboxes, and then click the **Order for a fee** button.



21. Your certificate is delivered to you via email. Please stay tuned as you need it for the next section.

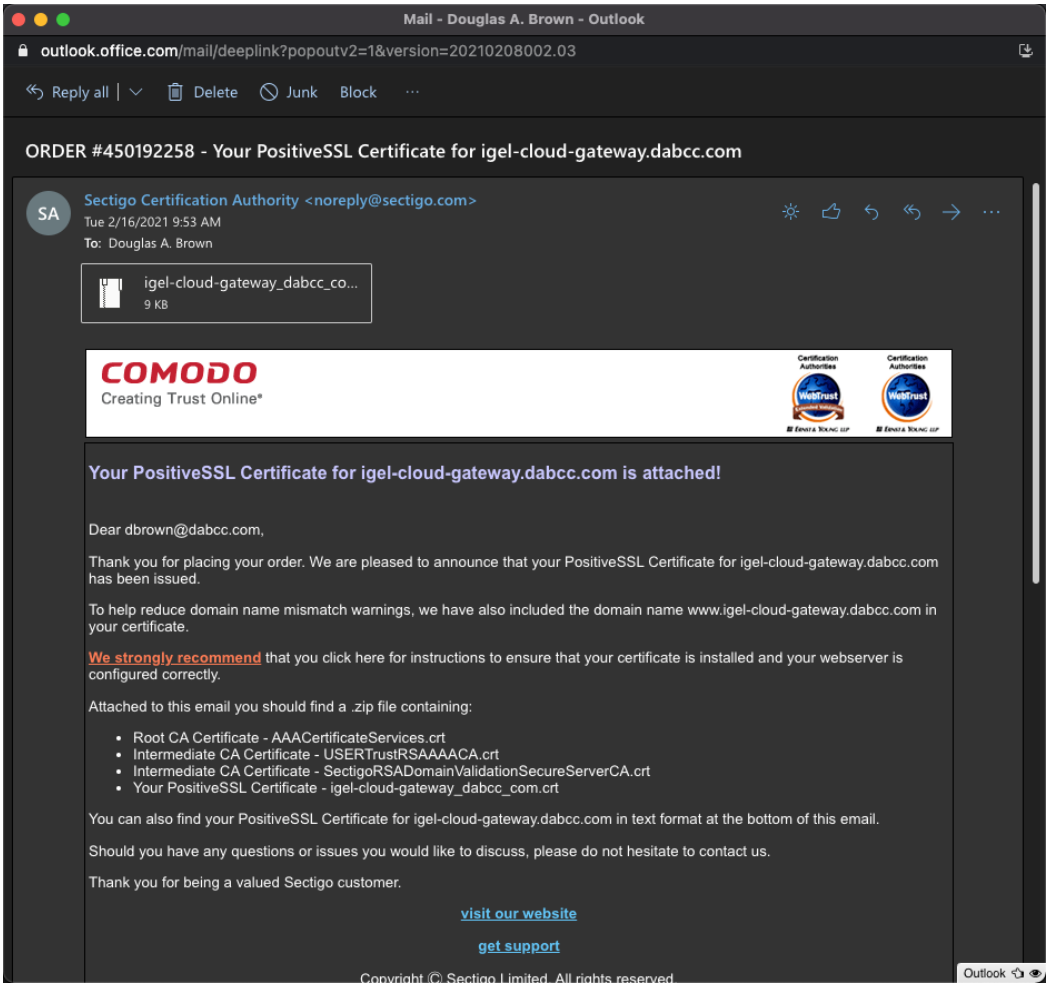


5. 6. How to Add an SSL Certificate to the UMS

Once you receive your SSL certificate from the Certificate Authority, you are ready to add it to the UMS.

The following details how to add an SSL certificate to the UMS:

1. Copy the zip file you received from the certificate authority to the UMS server. If you received your certificate from pw.net, the email would look something like the following.



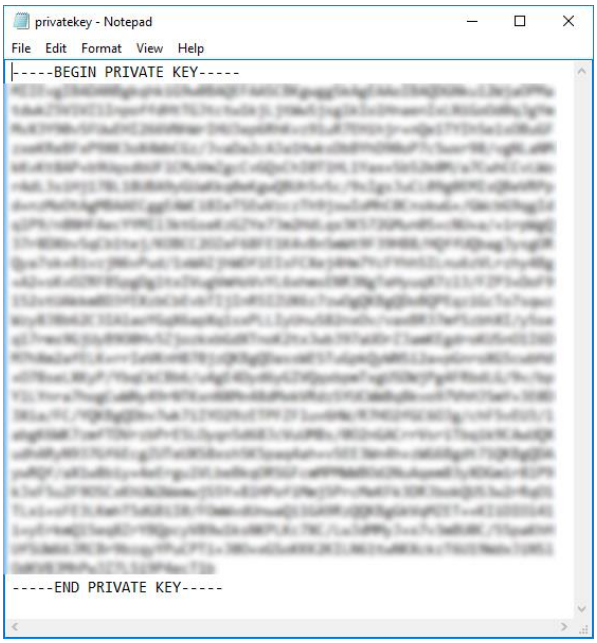
2. You are required to generate the private key. To do this, open your favorite SSH client, as you did above. Log in to your ICG server if you are not still logged in.

   Type the following:

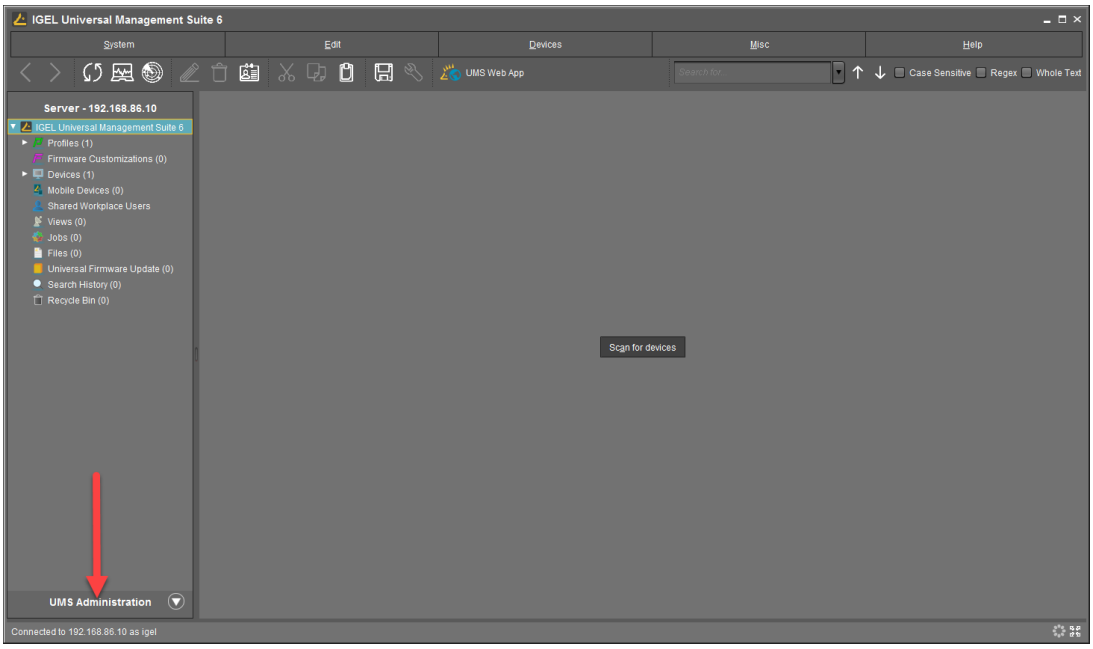
   `cat igel-cloud-gateway.<your domain>.key`

   For example, `cat igel-cloud-gateway.igelcommunity.com.key`

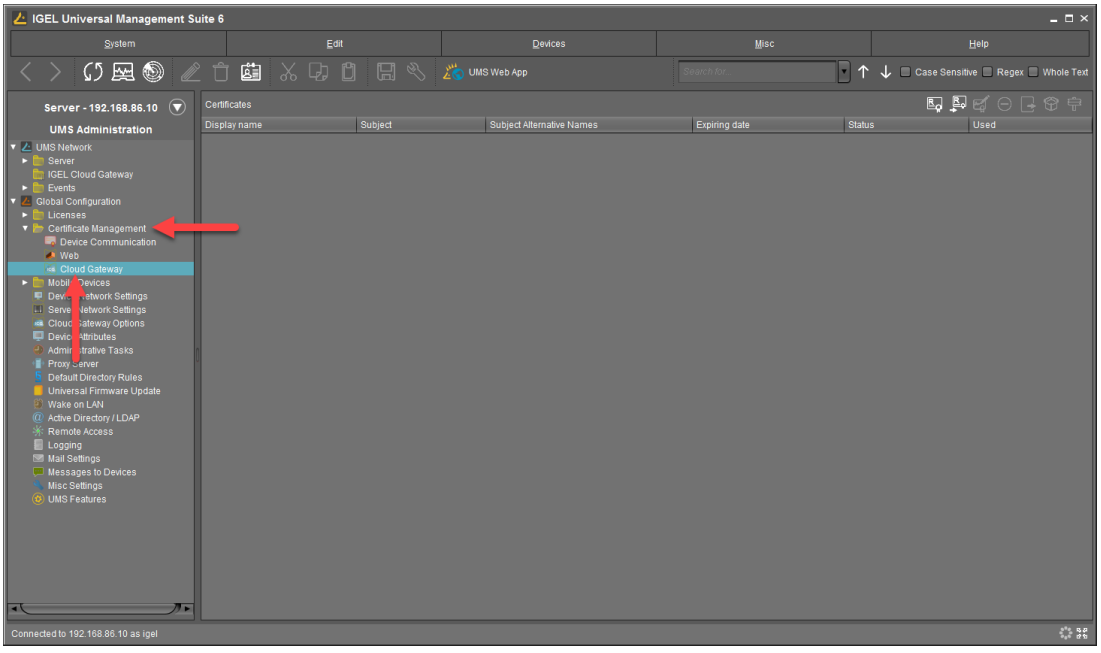
3. Create a new file, copy, and paste the private key (the text above) to a txt file. Please make sure it is a text file. This is important. Save it to something like privatekey.txt. You import it into the UMS soon.



4. From the UMS, click to select the **UMS Administration** link at the bottom of the left menu.

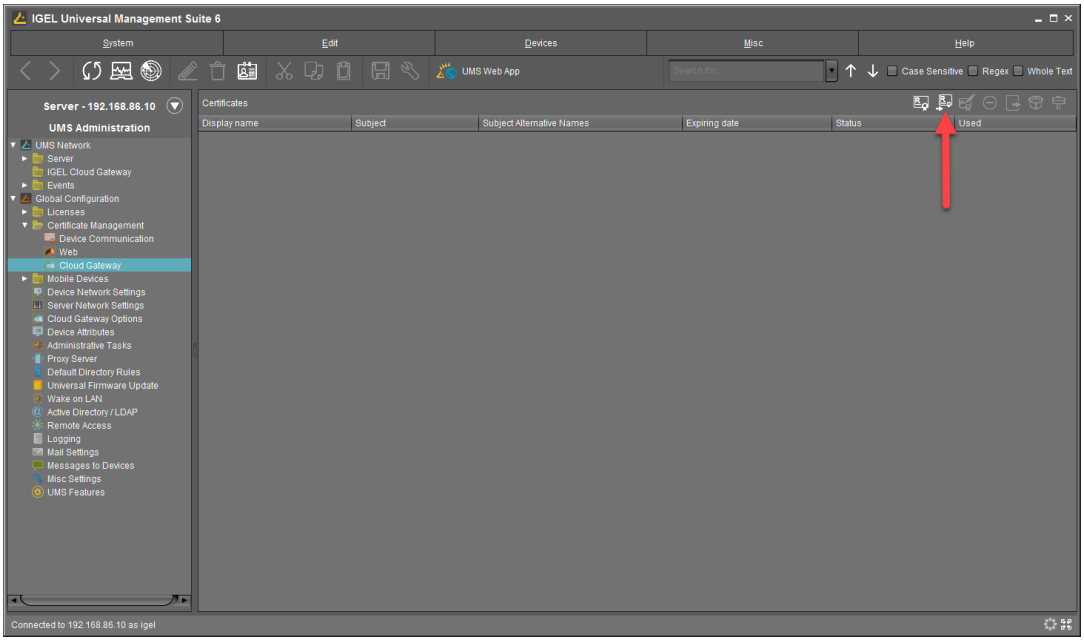


5. Click to expand the **Global Configuration** > **Certificate Management** nodes and click the **Cloud Gateway** link in the left menu.

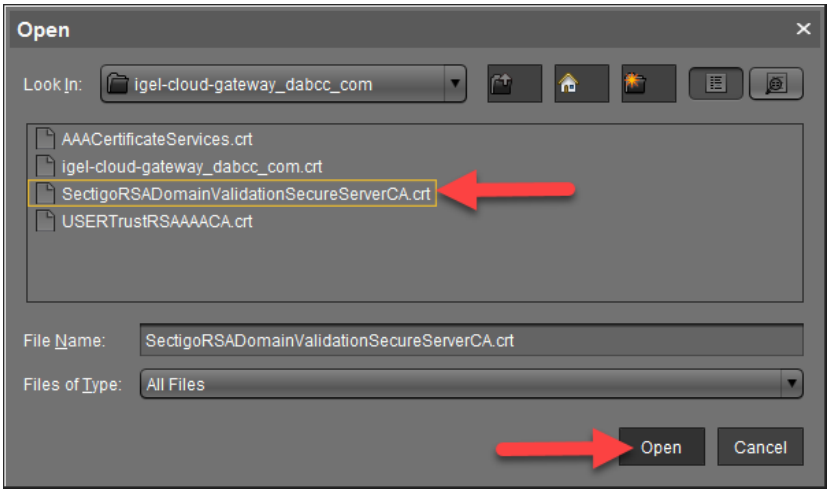


6. You are ready to import the public certificate and private key for the cert.

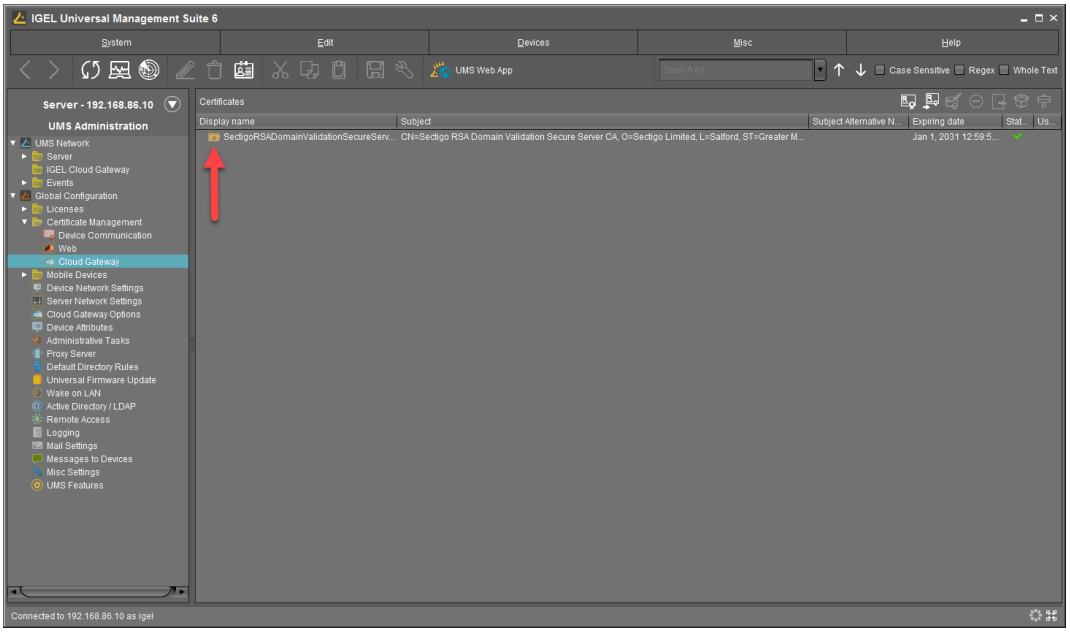
   Click the **Import root certificate** button on the top right of the UMS menu bar.



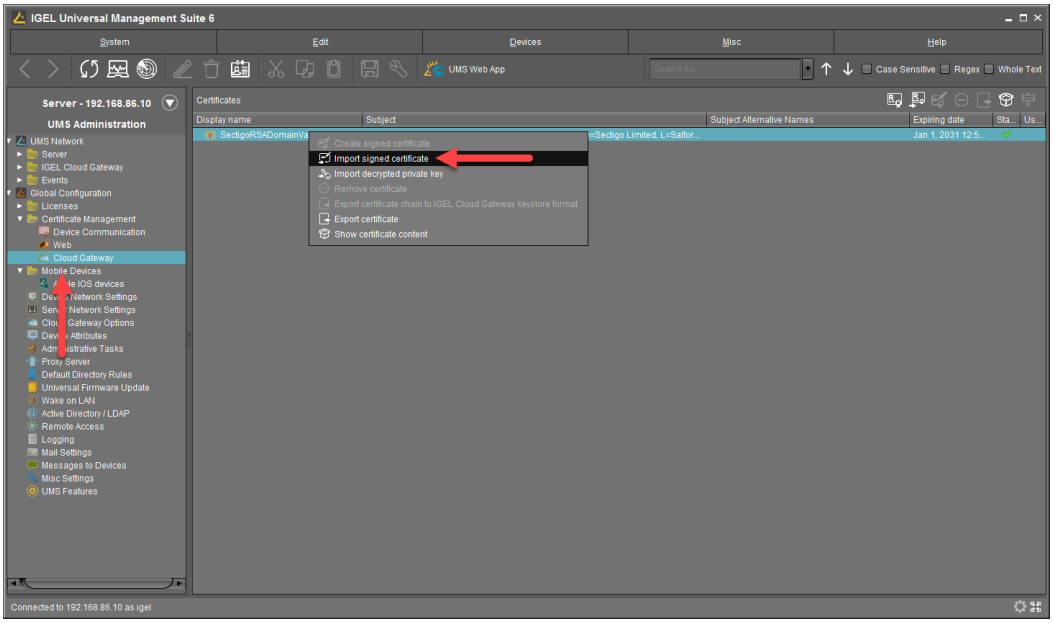
7. You are prompted to select the certificate file you received via email. Browse to the location of the .crt file, select the CA certificate, and click the **Open** button to continue.



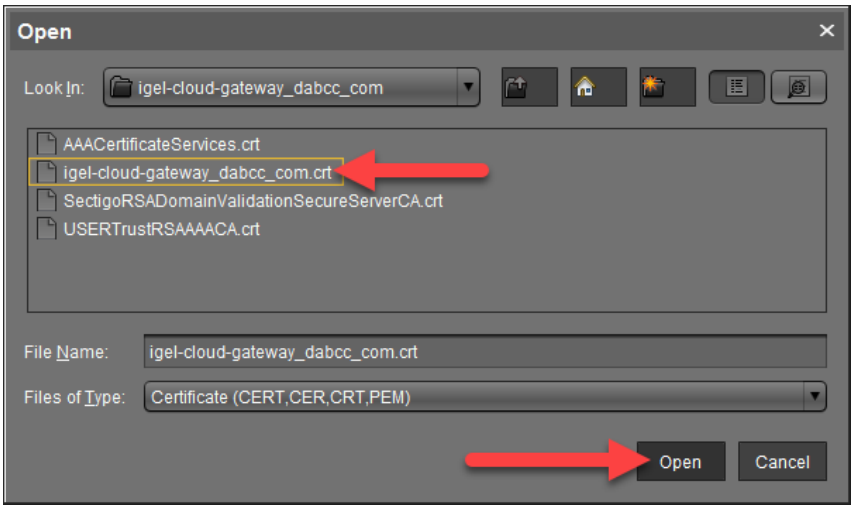
8. The certificate is imported and added to the list of UMS certificates.



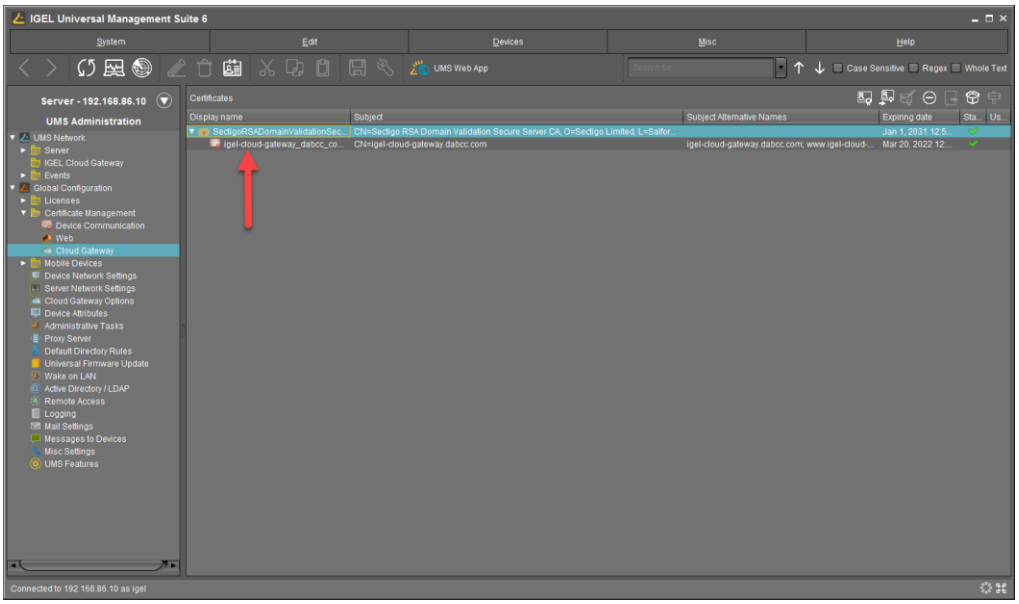
9. Right-click on the newly added certificate and click the **Import signed certificate** item.



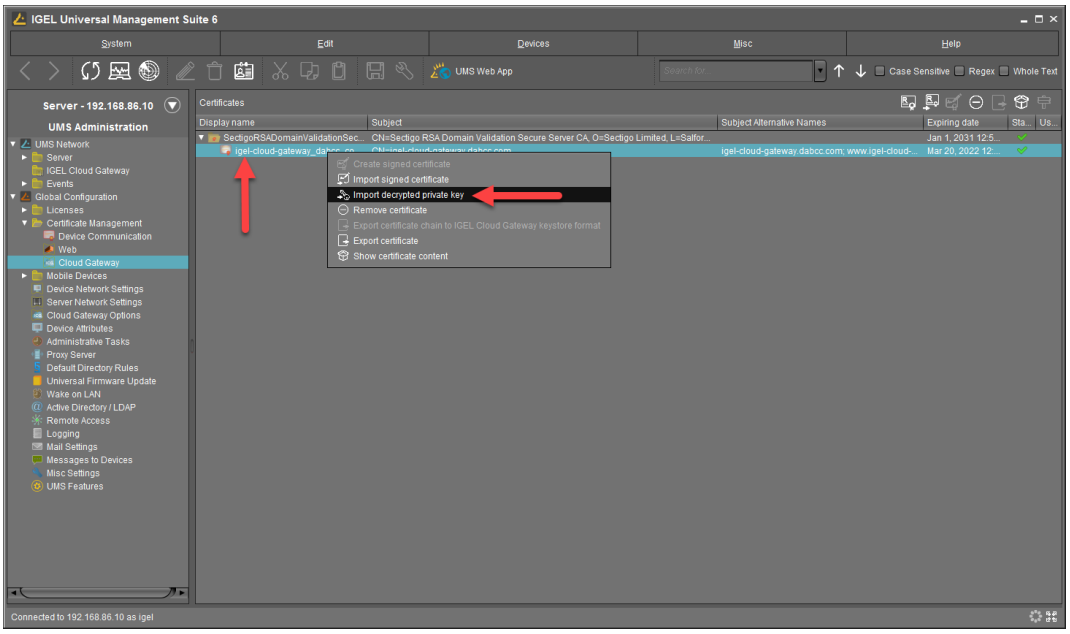
10. Browse to the location of the **.crt** file, select the certificate, and click the **Open** button to continue.



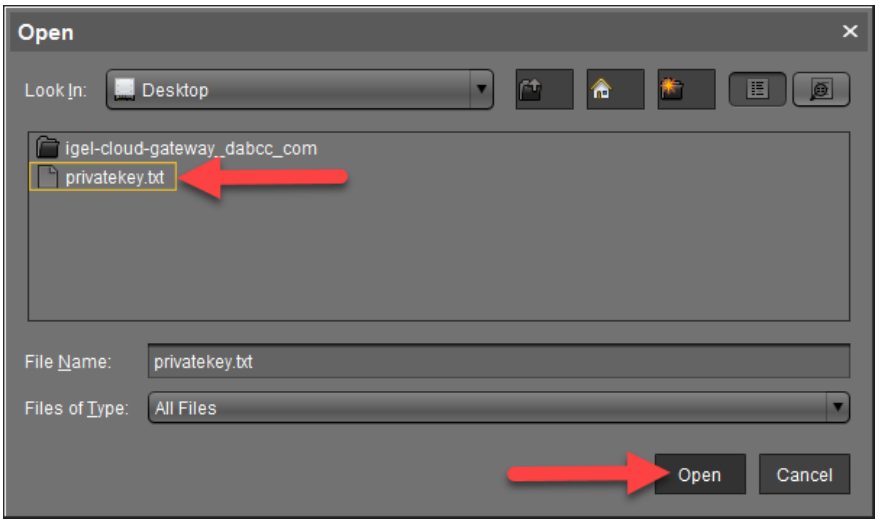
11. You should see your new SSL certificate listed.



12. Right-click on the newly added certificate. This time click the **Import decrypted private key** entry**.**

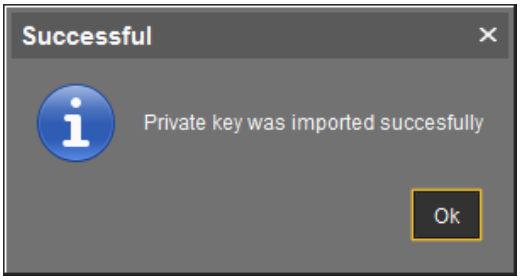


13. Browse to the location of the private key certificate you created above and click to select it. Click the **Open** button to continue.



14. If all goes as expected, you are prompted that your **Private key was imported successfully**!

    Click the **OK** button to continue.



The SSL Certificate has been successfully added, and you are ready.

5. 7. How to Install ICG using the UMS Remote Installer

The environment is set up, signed, and ready for you to finally install the IGEL Cloud Gateway software onto your new ICG AWS instance. To do this, you have two types of installations you can choose from. 1) Manually installing the ICG software on the ICG server, 2) Use the new ICG Remote Installer wizard that will assist you in installing and configuring the ICG installation on a remote server via the UMS in only a few steps. Works great and is easy as 1,2,3.

> Learn more! As stated above, there are two different methods for deploying ICG. Below are a few resources to help you learn more.
>
> - How to ICG Remote Installer video - **https://www.youtube.com/watch?v=kCwfV7aVjCs**
> - Installing the ICG without Remote Installer - **https://kb.igel.com/igelicg-2.02/en/installing-the-icg-without-remote-installer-31601162.html**

The following details how to install the ICG software using the Remote Installer feature:

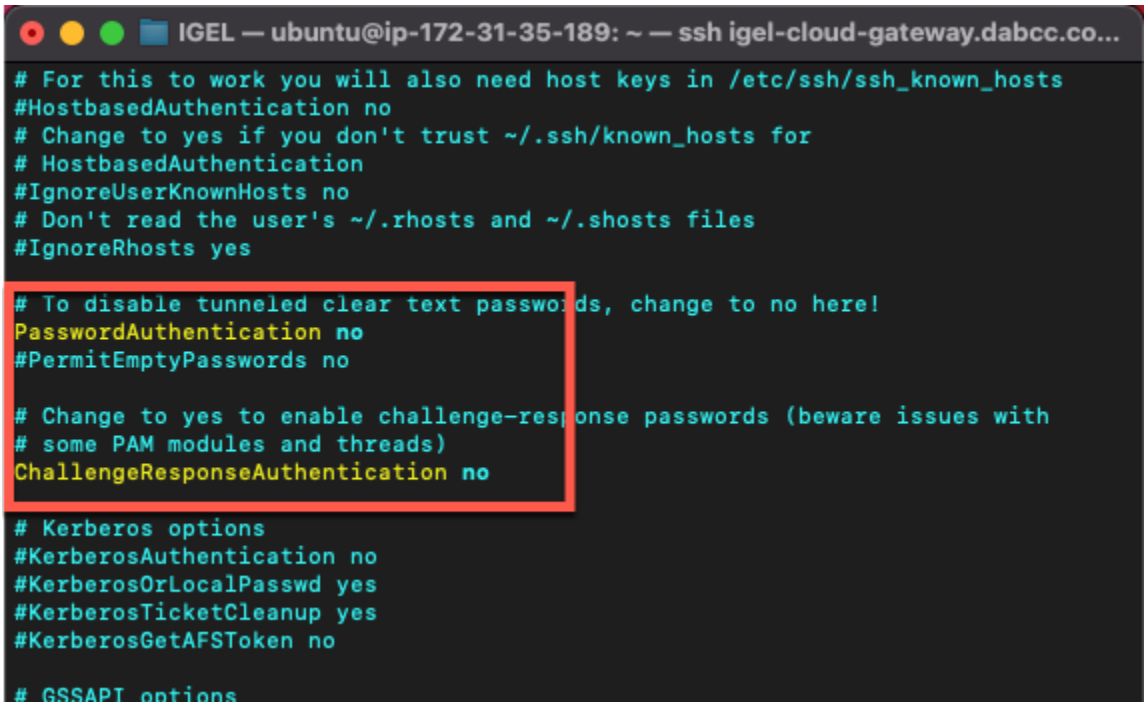
1. Log back into your ICG server, as documented above. The first thing you will need to do is prepare the ICG AWS instance to allow the UMS to install the ICG software remotely. Type the following:

   ```
   sudo vi /etc/ssh/sshd_config
   ```

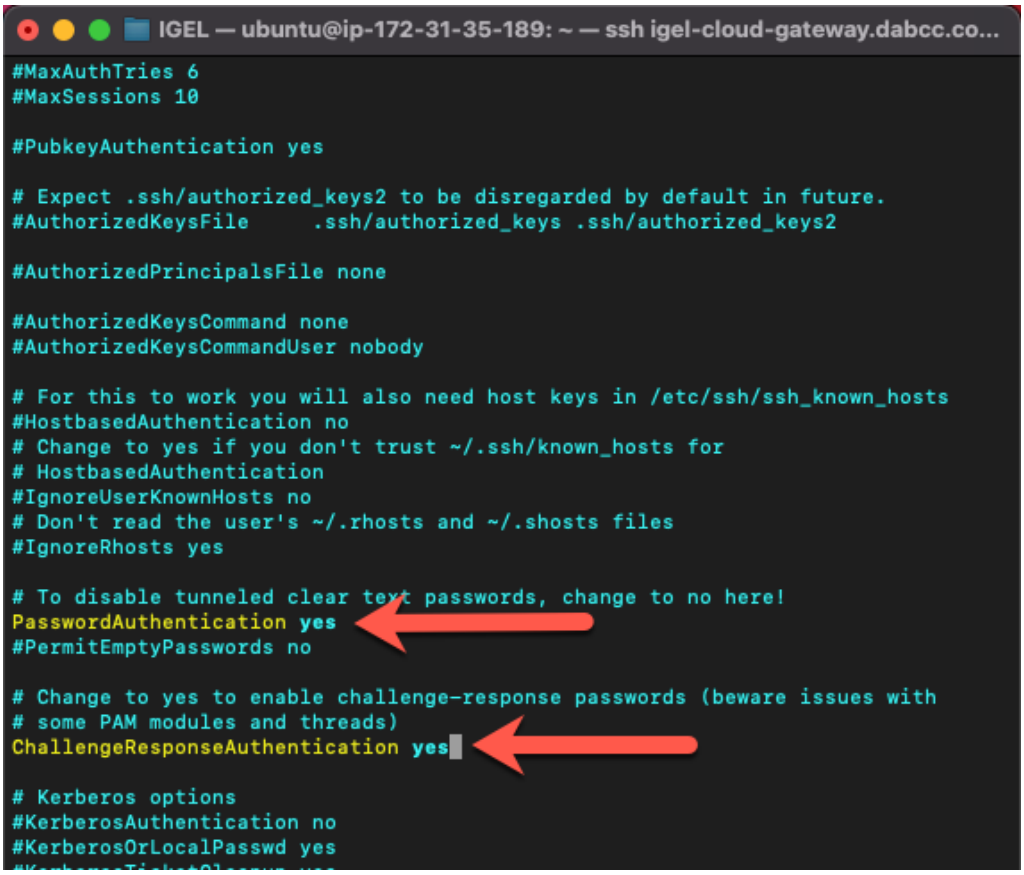
   

2. As we learned above, by default AWS uses a PEM file for authentication. The ICG Remote Installer software currently does not support PEM files, so you will need to configure the AWS server to allow password authentication.

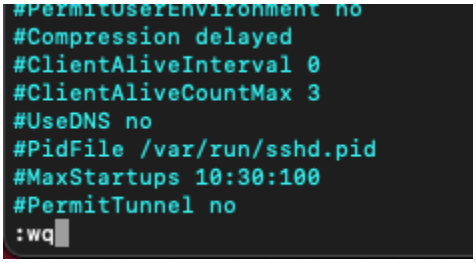
   Scroll down the ssh_config file until you find the **PasswordAuthentication** and **ChallengeResponseAuthentication** entries.



3. Change the value from no to **yes** for both entries. Press the **i** key to put the editor in insert (edit) mode.

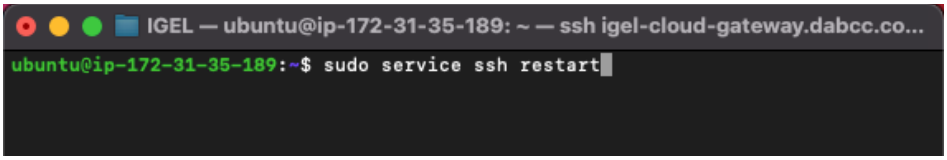


4. You need to save the file. To do this, hit the **ESC** key and type **:wq**. This will save your changes and close the ssh config file.



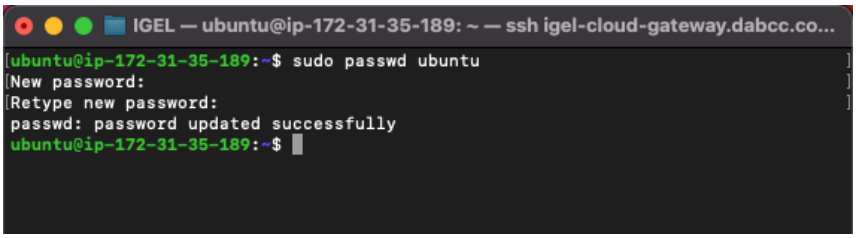
5. For the above changes to take effect, you will need to restart the ssh service. Type the following command:

```
sudo service ssh restart
```



6. By default, AWS uses the ubuntu account for these actions, but it is not preconfigured with a password. You will need to assign one. Type the following and enter your desired password:

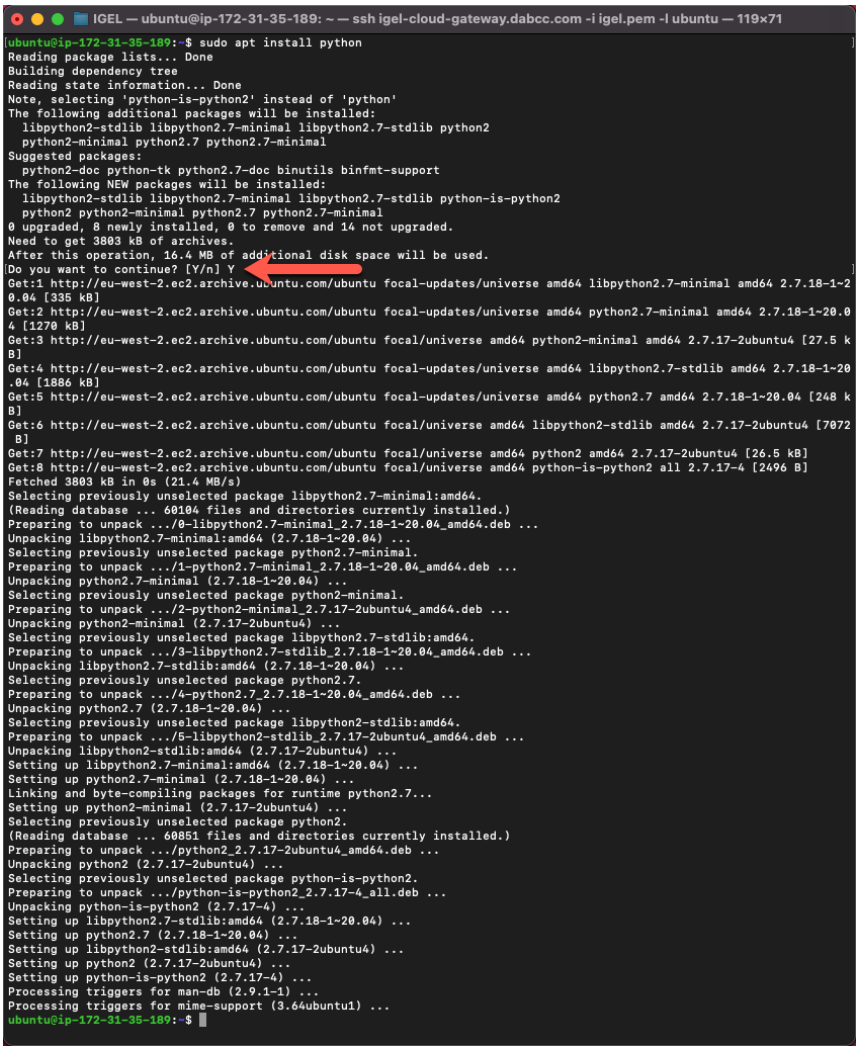
   `sudo passwd ubuntu`



7. ICG 1.4 requires Python, and by default, it is not preinstalled in the AWS ubuntu instance. To install Python, type the following:

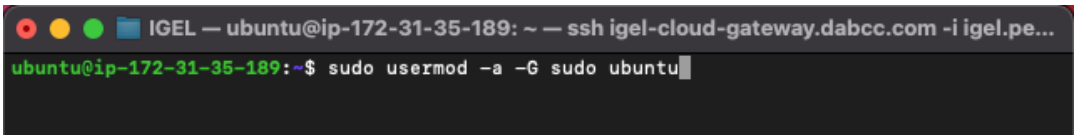
   `sudo apt install python`

   Type **Y** to confirm you wish to install Python.

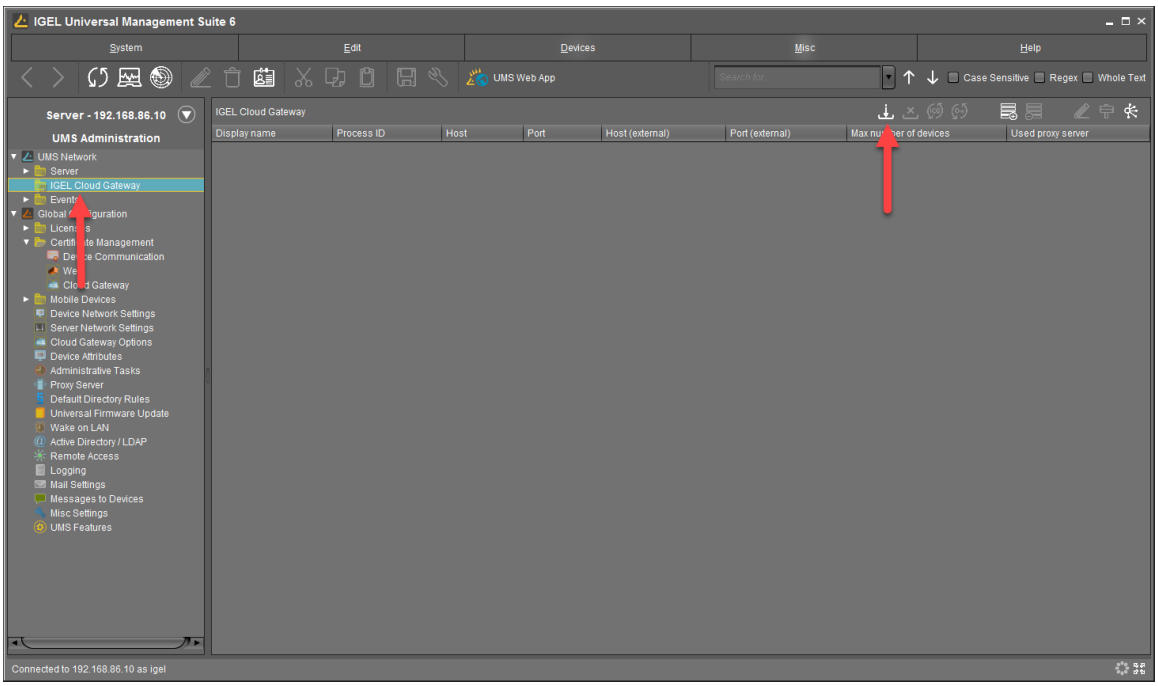


8. The last step you must do before you are ready to use the Remote Installer feature is to give the ubuntu account admin permissions. Type the following:

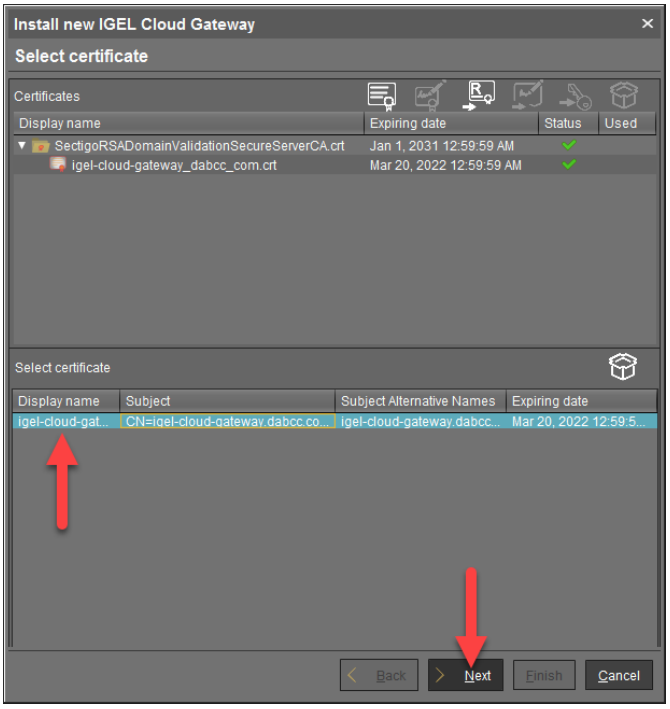
```
sudo usermod -a -G sudo ubuntu
```



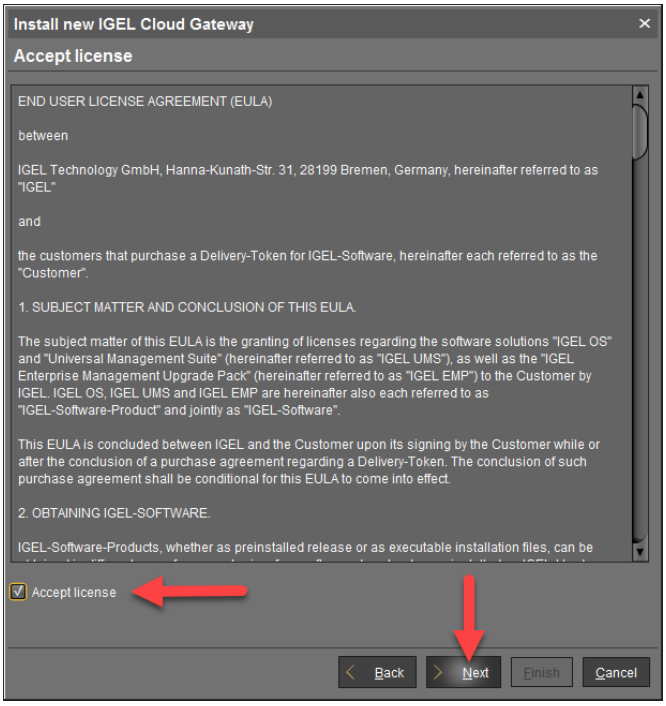
9. Open the UMS again and browse to the **UMS Administration** section and expand the **Server** folder under the **UMS Network** entry. Click the **IGEL Cloud Gateway** node and then click the down arrow icon located on the top right of the UMS.



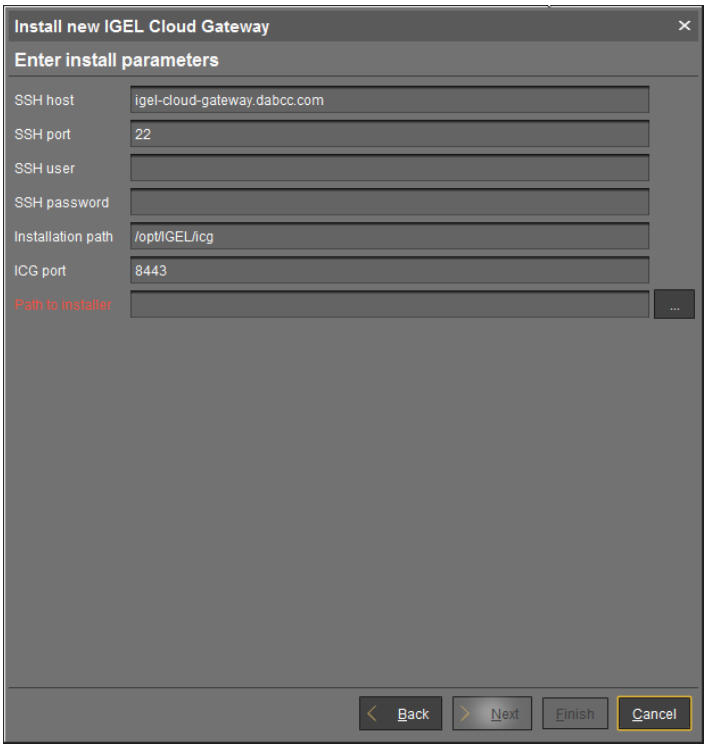
10. The ICG Cloud Gateway Remote Installer window opens and presents you with a list of certificates installed on the UMS server. You should be presented with the certificate you installed in the previous section. Click to select it and then click the **Next** button to continue.



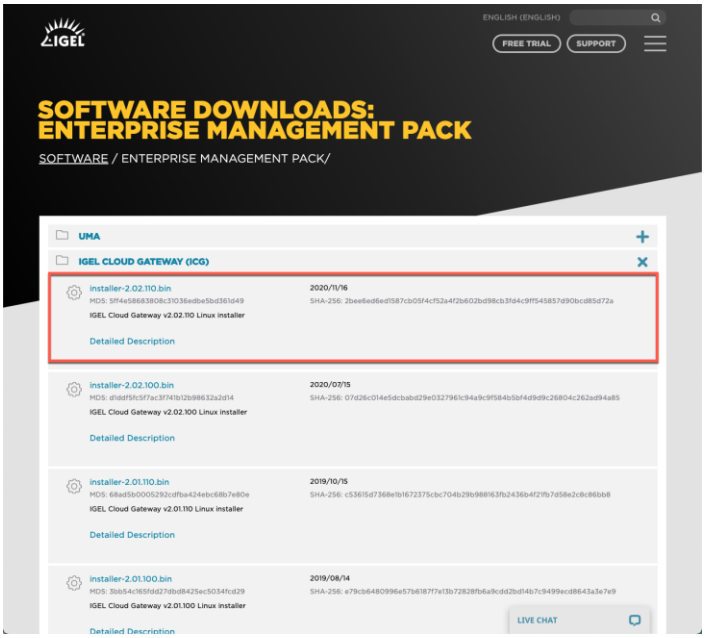
11. Read the IGEL Cloud Gateway End-User License Agreement (EULA) and click to check the **Accept license** checkbox. Click the **Next** button to continue.



12. You are ready to enter your new ICG server's connection information. For example, a username, password, the path to the ICG software the Remote Installer will push to the desired server, and a few more.



13. Before you do this, you will need to download the ICG software and copy it to the UMS server. Open your favorite Internet browser and browse to **https://www.igel.com/software-downloads/enterprise-management-pack/** and download the latest ICG software bin file.



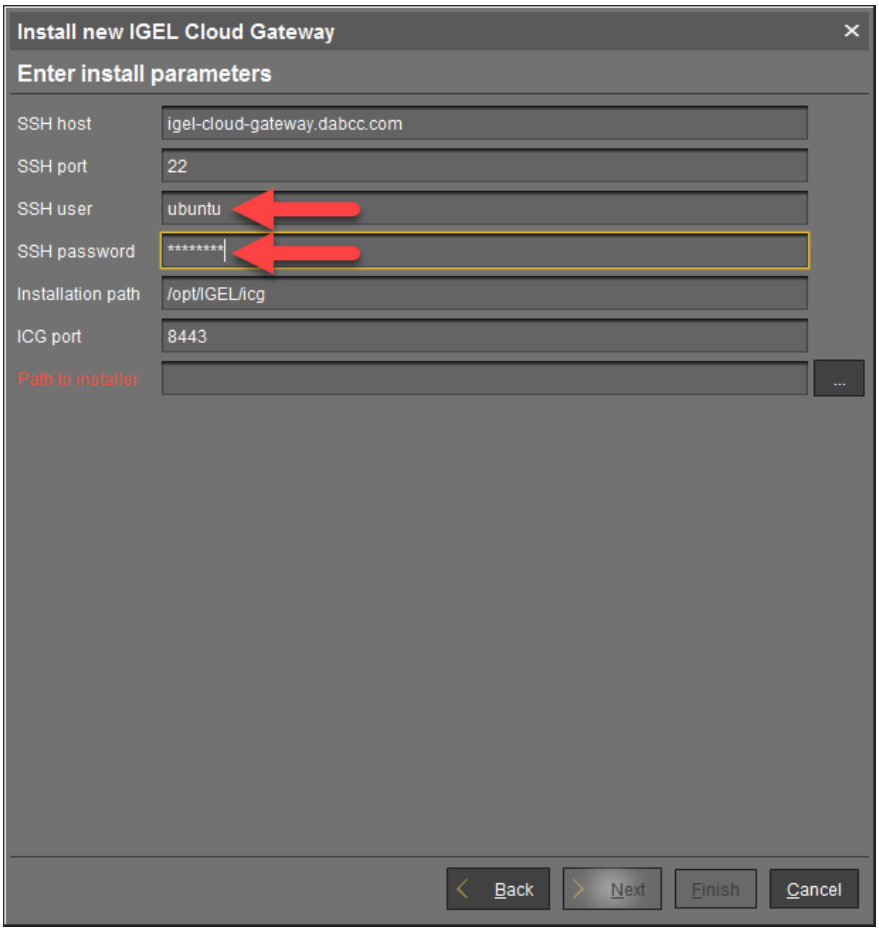
14. Once the software is downloaded and you are ready to enter the relevant details.

    If you followed the above steps as defined, enter the domain name of your ICG server in the **SSH host** text box, for example, igel-cloud-gateway.<your-domain-name>.

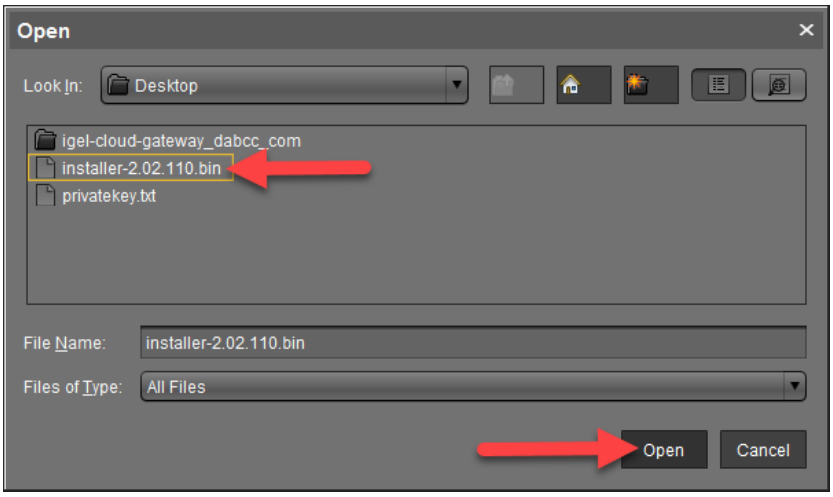
    SSH user = **ubuntu**

    SSH password = **password you set in step 6**

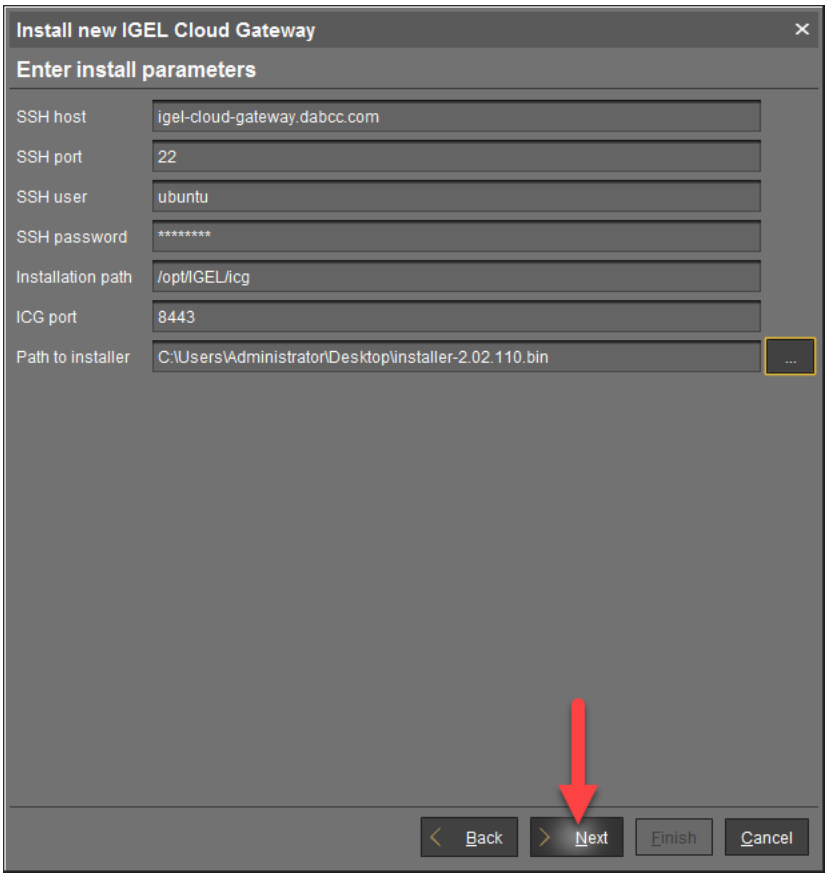
    Click the **…** button to the right of the Path to Installer text box.



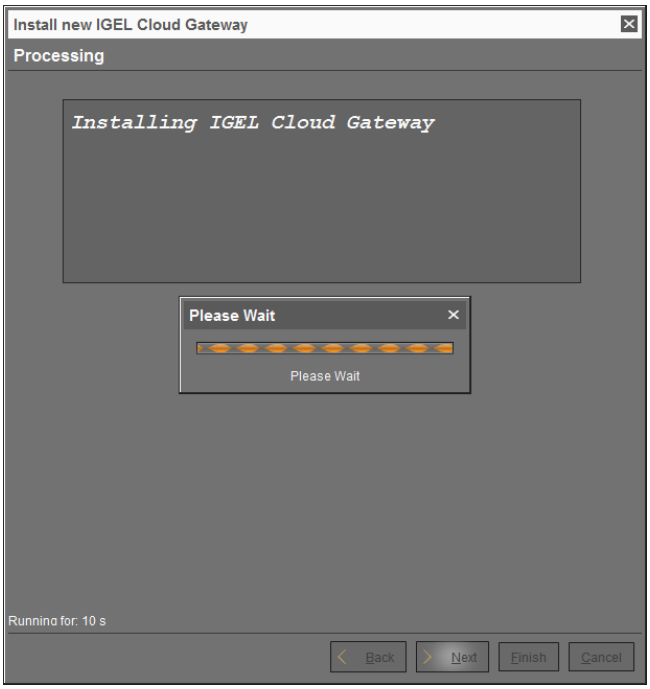
15. Browse to the ICG binary location you downloaded above, select it, and click the **Open** button to continue.



16. Verify all settings are correct and click the **Next** button to continue.

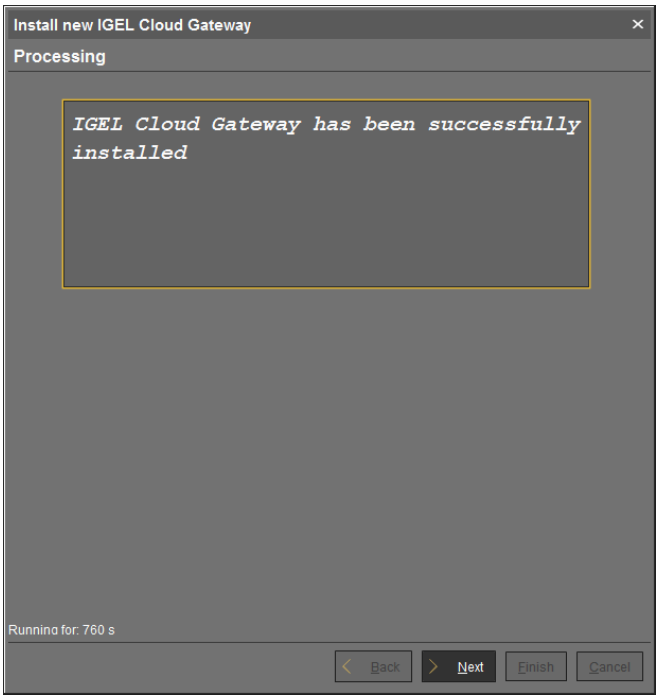


17. The Remote Installer is now installing the ICG software. Depending on the speed of your Internet connection, this could take a couple of minutes, so sit back and enjoy the relaxing break. You have been working hard!

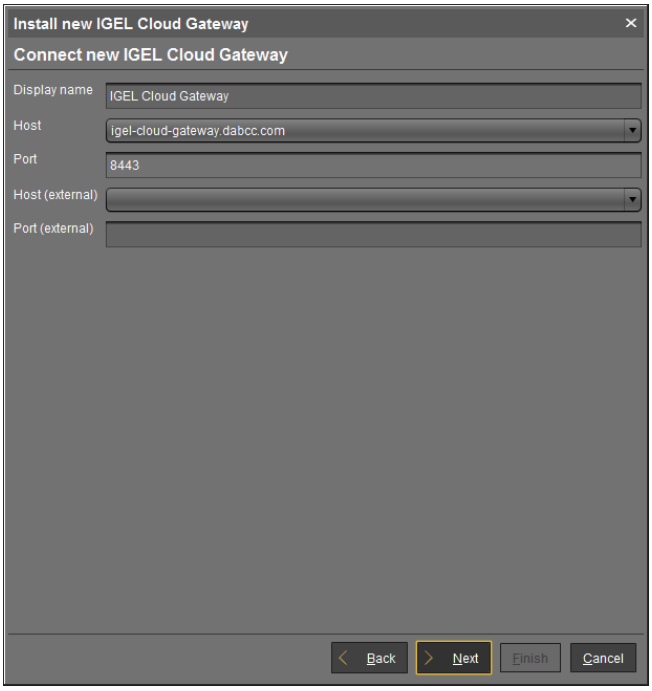


18. If you have a good connection and you followed the above steps just perfectly, you will see that the text **IGEL Cloud Gateway has been successfully installed**!

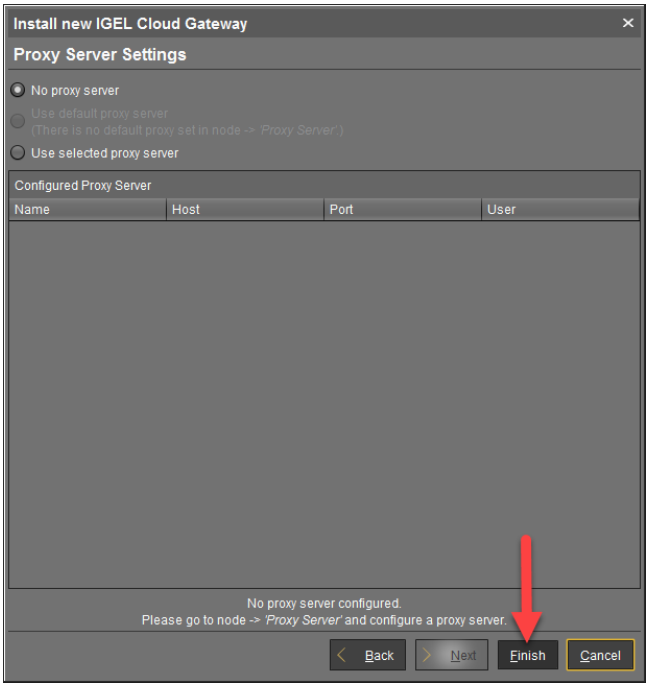
    Click the **Next** button to continue.



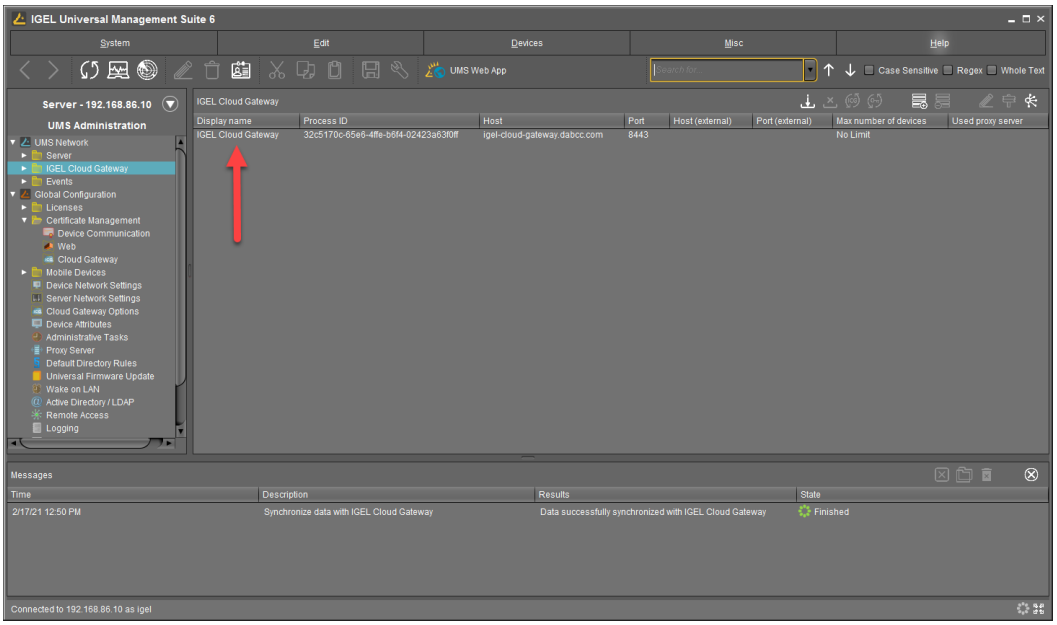
19. Now you will connect the new ICG server to the UMS. By default, the **Displayname** and **Host** text boxes will be filled out for you based on the information you entered previously. You can also configure the external host and port used by endpoint devices to connect to the ICG if it differs from what you entered earlier. Once finished, click the **Next** button to continue.



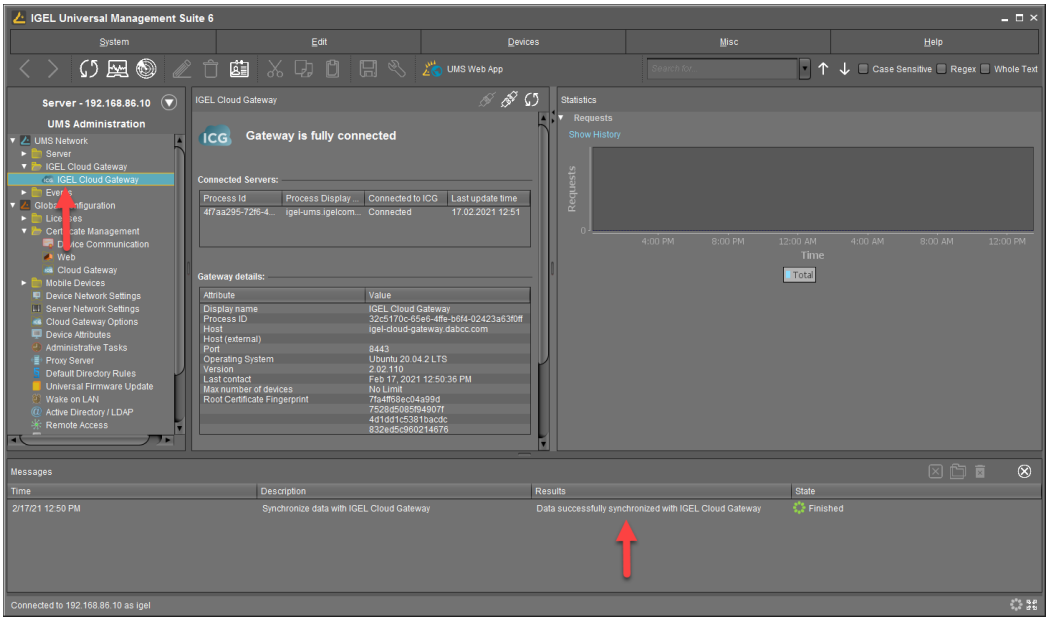
20. If you are using a proxy server, you will enter it now. If not, then accept the default of No Proxy Server. You are done. Click the **Finish** button!



21. The UMS will try to connect to the ICG server, and if everything was configured correctly, you should see your new ICG server listed, as shown below.



22. You will also notice a new entry has been added under the IGEL Cloud Gateway folder containing the new ICG server. Click it to view the details, as shown below.



The IGEL Cloud Gateway server is installed, configured, and almost ready to use. One more step is required.

More ICG Resources:

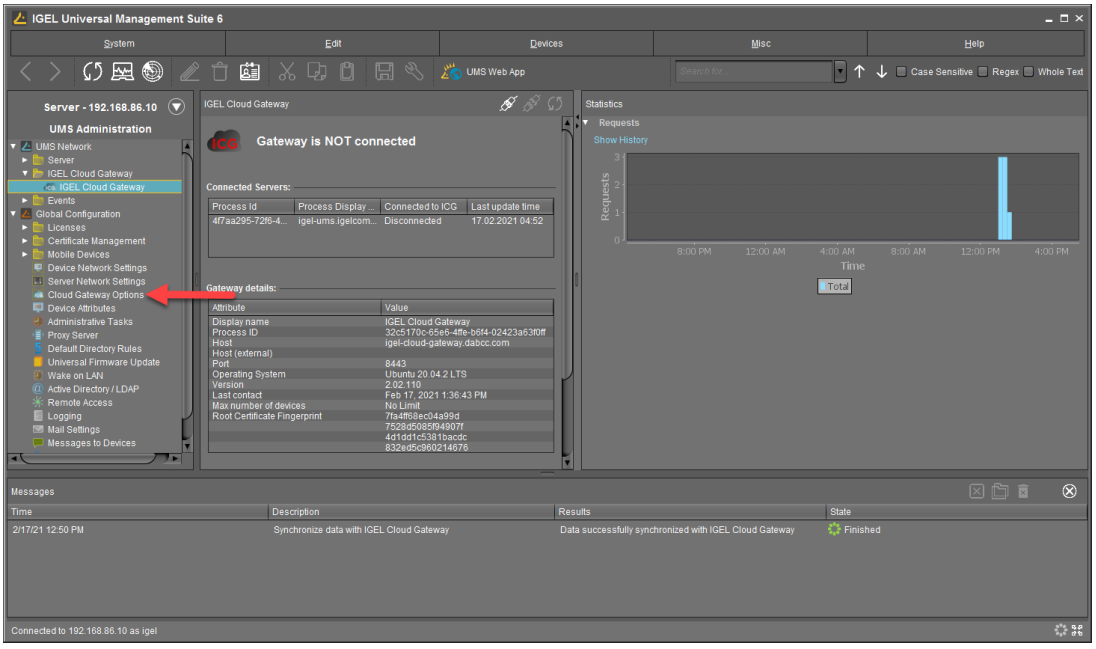
- How to toggle between ICG and direct connection - **https://kb.igel.com/igelicg-2.02/en/toggling-between-icg-and-direct-connection-31601128.html**
- Using Citrix NetScaler ADC as an SSL Bridge for ICG - **https://kb.igel.com/igelicg-2.02/en/using-citrix-netscaler-adc-as-an-ssl-bridge-for-icg-31601172.html**
- How to configure Apache Tomcat for TLS 1.2 only - **https://kb.igel.com/igelicg-2.02/en/how-to-configure-apache-tomcat-for-tls-1-2-only-31601153.html**
- How to stop and disable the SSH server - **https://kb.igel.com/igelicg-2.02/en/how-to-stop-and-disable-the-ssh-server-31600923.html**

5. 8. Configure the ICG Device Authentication Method

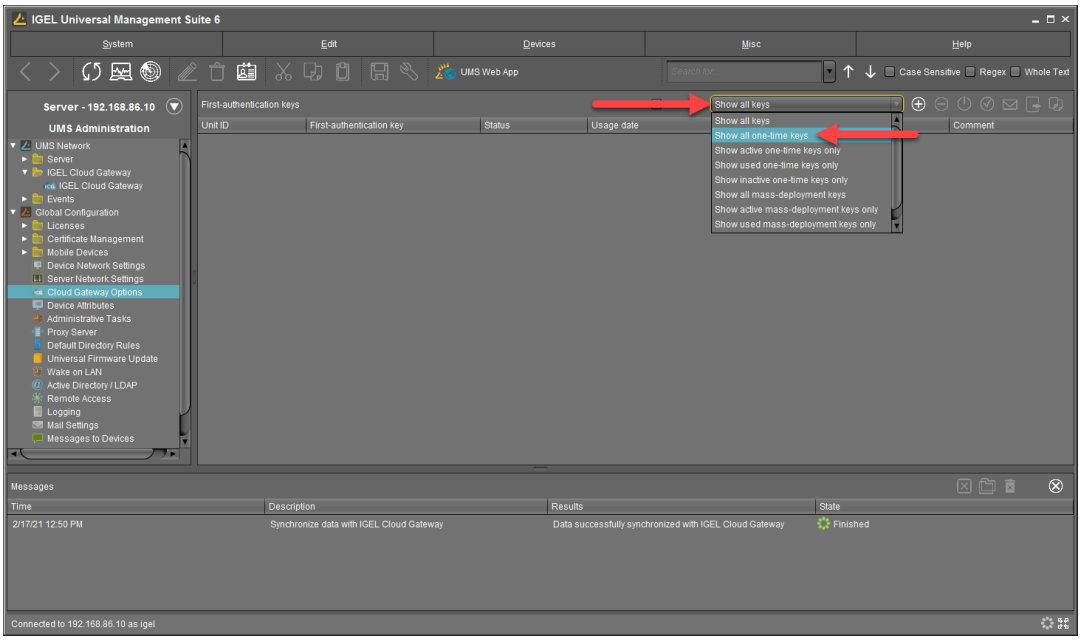
Now you have an ICG server installed and connected to the UMS. You are ready to configure the client authentication method. For a device to connect to the UMS via the ICG server, it must first authenticate with the ICG. To verify it is an authorized device. You have the following three authentication options:

- **One-time passwords** – can be used by any device, but once it is used, it cannot be used by another device.
- **Device-specific One-time passwords** - can only be used by the device you assign to the one-time password.
- **Multiple-time passwords** - this is the most flexible as any device can use a single password at any time.

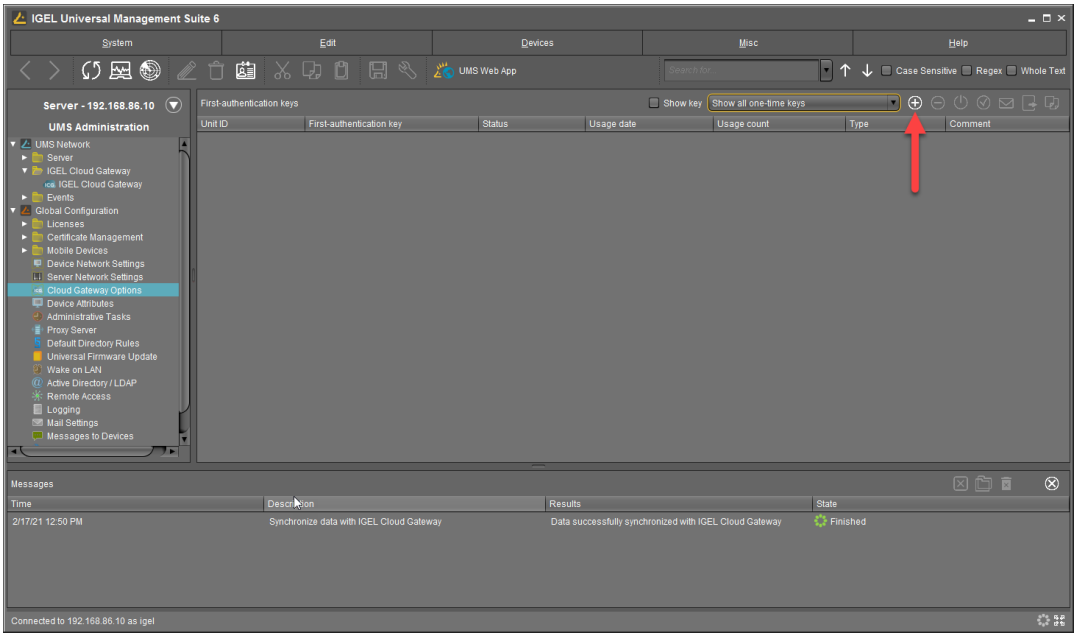
1. To configure the ICG device password, click to select the **Cloud Gateway Options** node in the left menu.



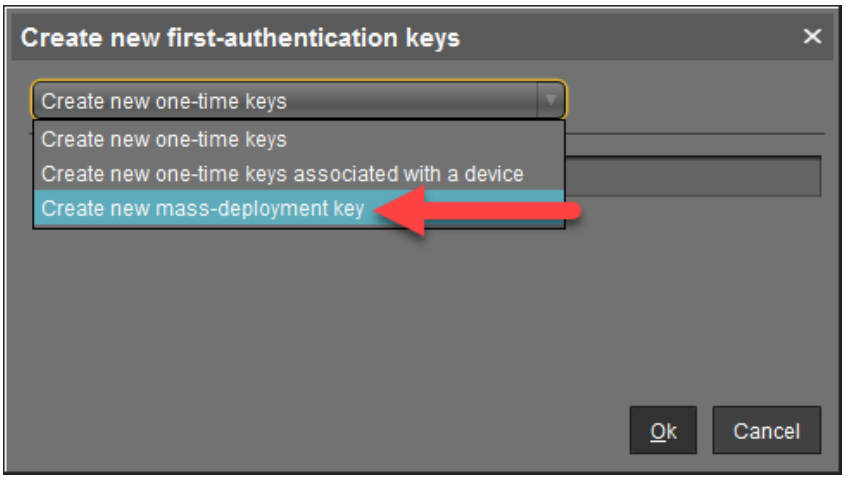
2. Click the **Show all keys** drop-down box located in the First-authentication keys section to reveal the different types of keys you can create. For this example, click the **Show all one-time keys** entry.



3. Click the + icon located in the **First-authentication keys** box.

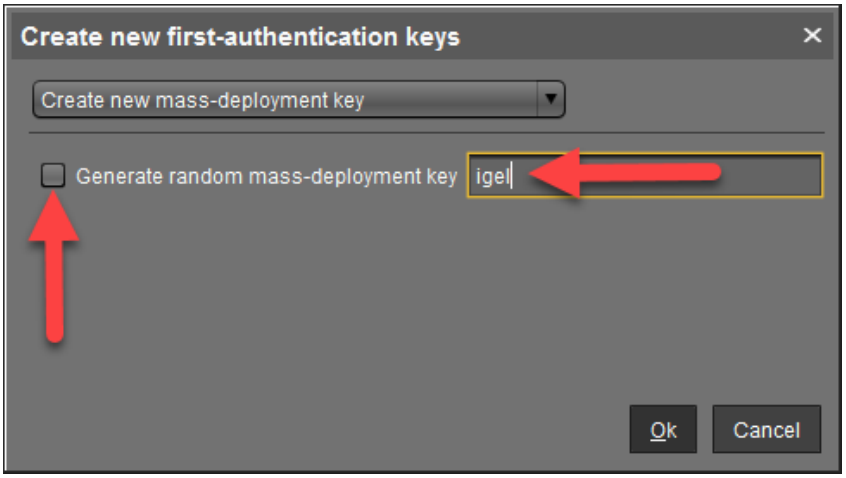


4. The **Create new first-authentication keys** window opens. Select **Create new mass-deployment key** from the dropdown list.

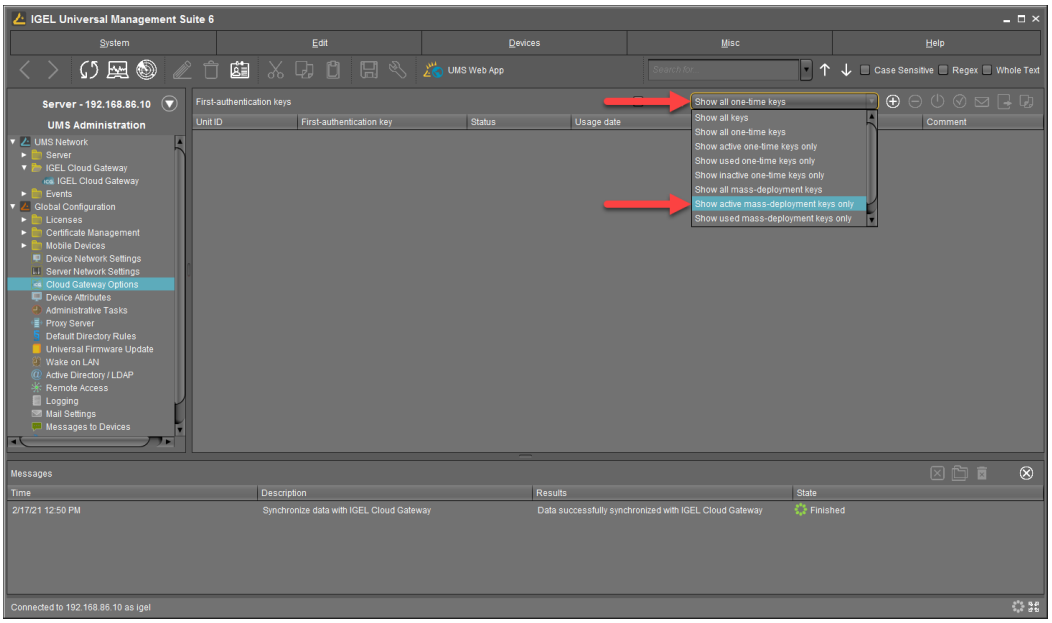


5. Uncheck the **Generate random mass-deployment key** checkbox and enter the desired password used to connect to the ICG. Click **OK** to continue.

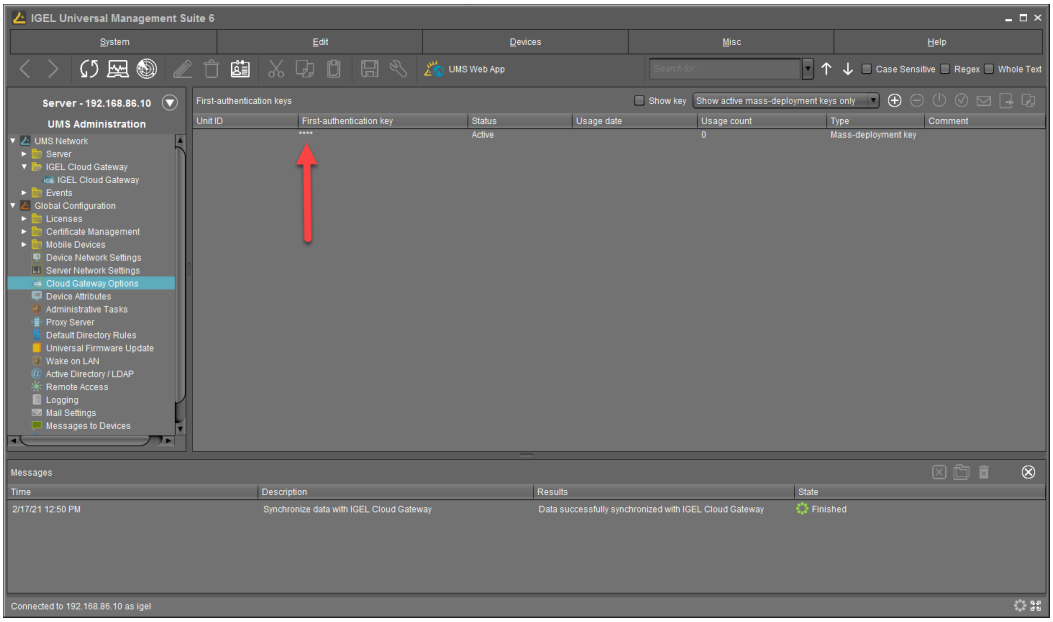
> Typical end-users will use this key. Please make sure to make it strong enough to pass your password criteria guidelines but not so hard that an average user is challenged trying to enter it.



6. From the drop-down box on the top of the **First-authentication keys** section, select **Show all mass-deployment keys**.



7. Your newly created ICG key is set. Save it in a safe place as you are required to use it when managing IGEL OS devices via the IGG.

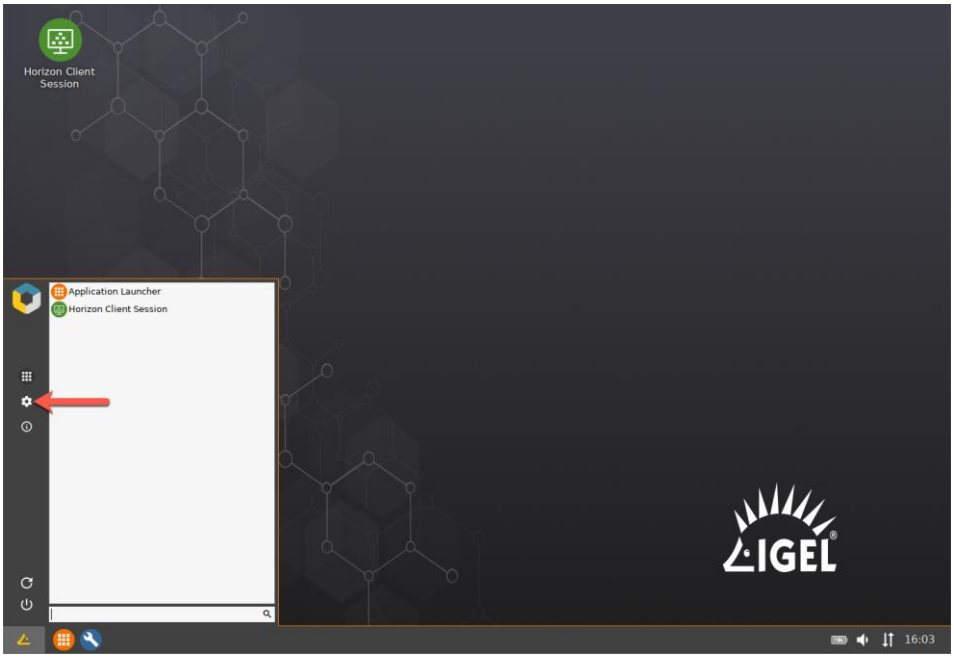


Your IGEL Cloud Gateway server is up and running. It is time to configure your IGEL OS device to use the ICG.

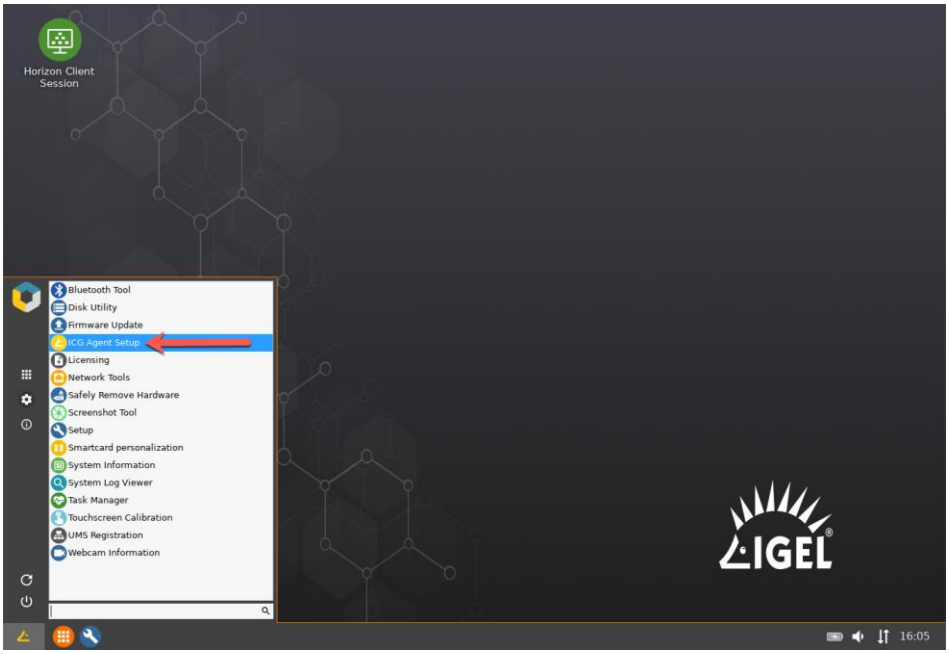
5. 9. Configure IGEL OS to use ICG

Now that you have an ICG server installed and connected to the UMS, you are ready to configure the IGEL OS to use it.

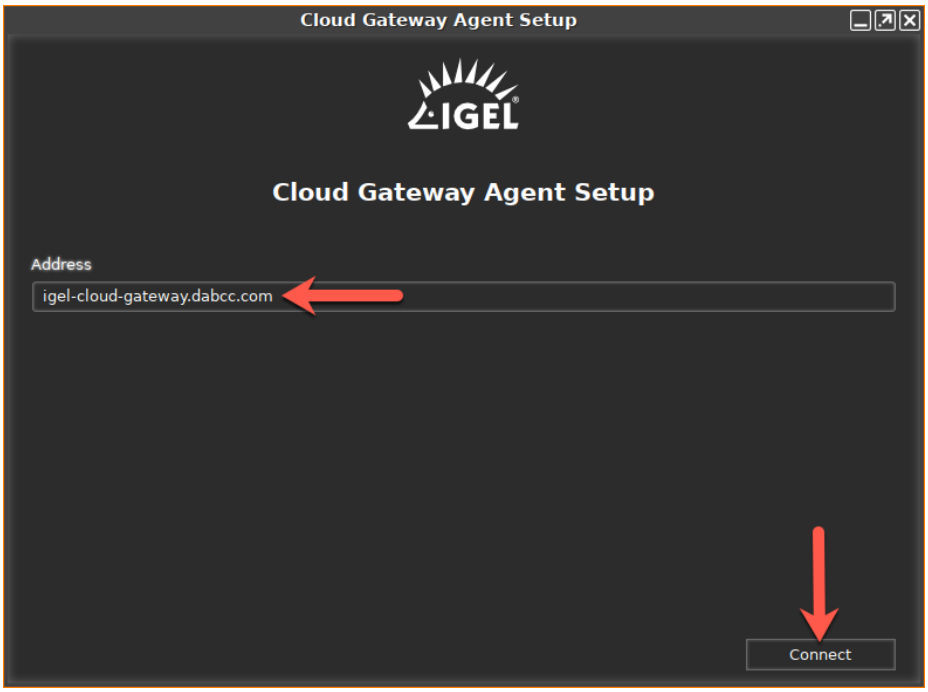
1. From the desktop of the IGEL OS, click the **start button** to open the start menu. Click the **gear icon**.



2. Click the **ICG Agent Setup** application.

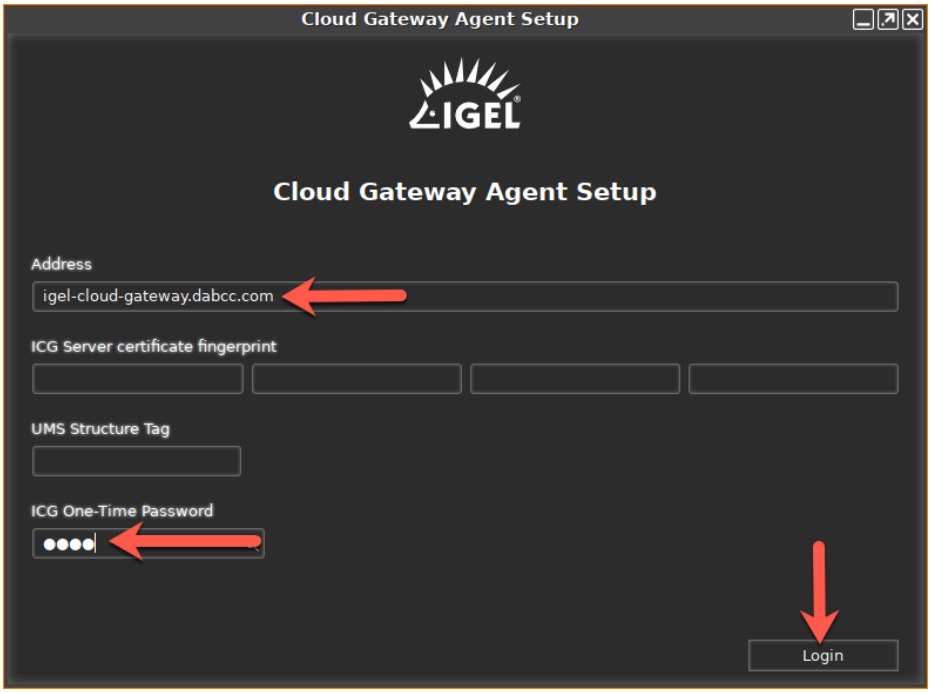


3. The **Cloud Gateway Agent Setup** wizard starts and prompts you for the address of the ICG server. Enter the correct address and click the **Connect** button.

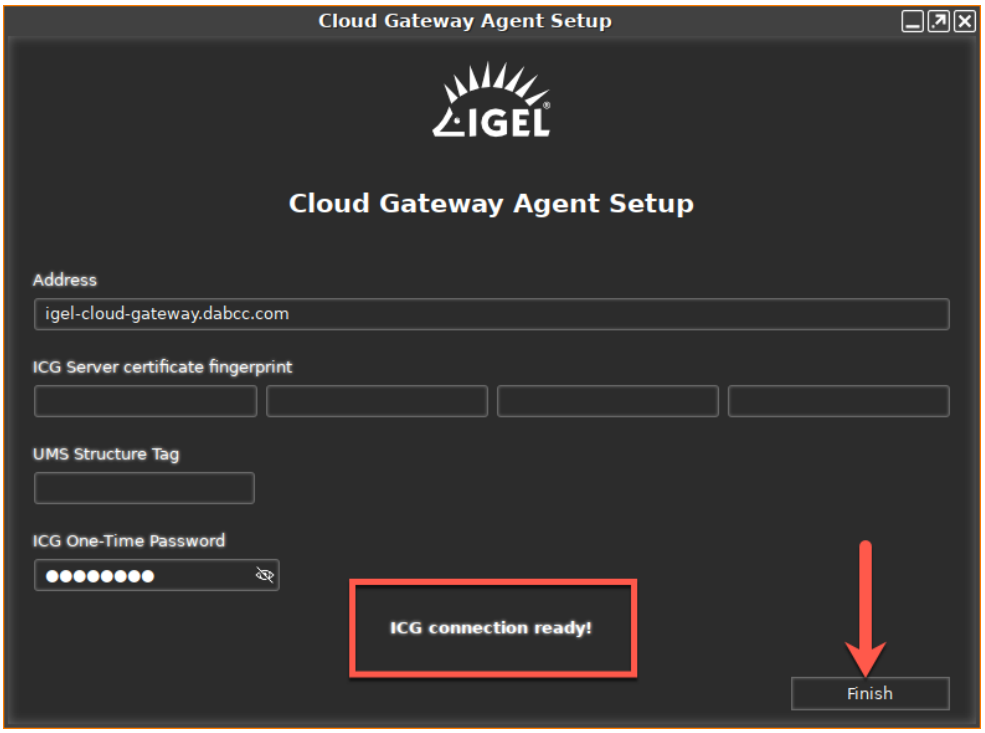


4. The wizard contacts the ICG server, and if successful, it prompts you to enter the ICG one-time password you created above.

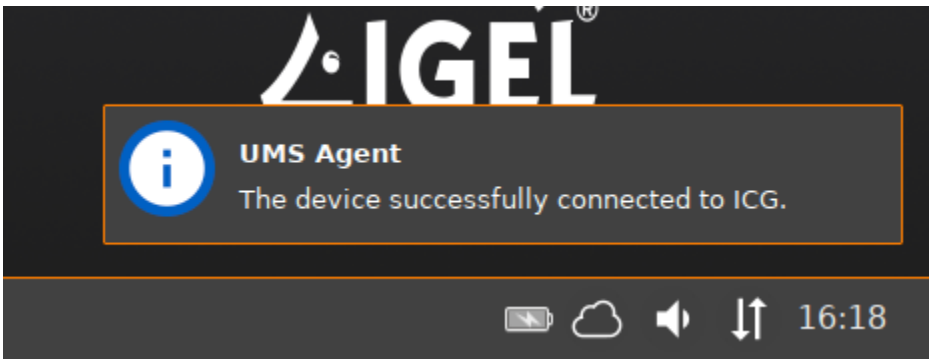
   Enter the password in the **ICG One-Tine Password** text box and click the **Login** button.



5. If successful, you are informed with the text **ICG connection ready!** Click **Finish** to save the settings and return to the IGEL OS desktop.

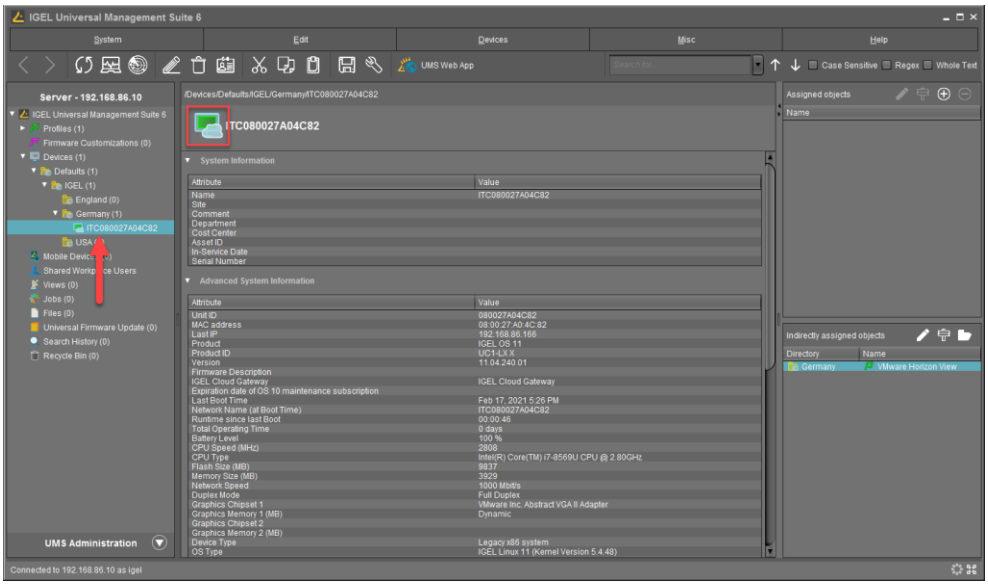


6. You are presented with a notification popup informing you the IGEL OS is in the process of registering with the UMS.



7. Once the registration process is finished, you are brought back to the IGEL OS desktop. You will notice a cloud-shaped icon has been added to the right side of the taskbar. This icon notifies your ICG server's connection status.

8. Flip back to the UMS, and you should see the newly added IGEL OS device under the **Devices** node. Click it to display device information, for example, name, IP, license type, etc.



You should be a proud person as you now have successfully installed the IGEL Software Suite, IGEL OS, UMS, and ICG! Great work! Let's have some fun and create a few profiles and custom configurations!

Configuration & Maintenance

1. UMS Profiles Overview

Profiles are where you configure the IGEL OS settings, everything from the look and feel to the applications and sessions the user will have access to. Profiles are extremely powerful. Profiles allow you to do almost anything you can imagine to the IGEL OS.

The first thing to note about profiles is the profile features or settings are specific to the versions of IGEL OS. For example, as IGEL releases updates, they might add new profile settings. Hence profiles are tied to OS versions. If you did not follow this guide step-by-step and thought, you could install the UMS and skip straight to creating profiles before installing and registering your first IGEL OS. You would have found this is not possible. Profiles are added to the UMS server when a new version of IGEL OS is added to the UMS.

In the following section, you will learn how to install and configure the subsequent sessions and recommended configurations:

- Chromium Web browser
- Chromium Web browser in kiosk mode
- Citrix access via the Chromium Web browser
- Citrix access via Citrix StoreFront
- Citrix access via Self-Service
- How to Turn Citrix Native USB Redirection Off
- How to enable Citrix HDX Realtime Webcam Redirection

> It is recommended to create one profile per configuration/setting and not have a single profile for EVERY feature/setting. This will allow you to mix and match settings as you so desire.

1. 1. How to Create a Basic Folder Structure

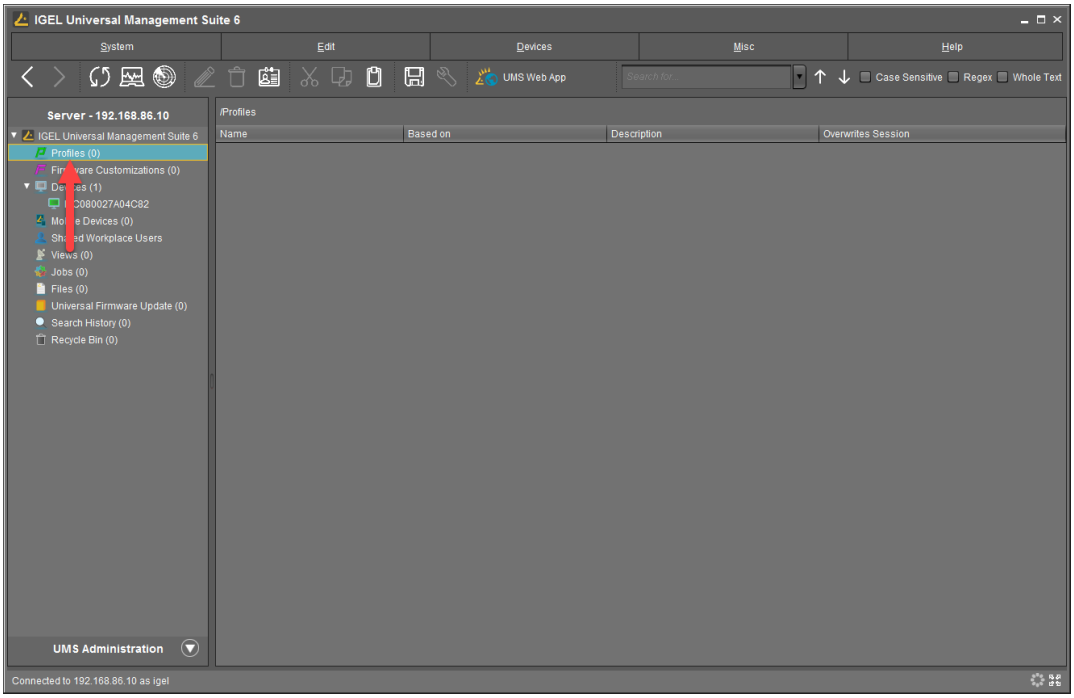
The first thing you will want to do when setting up the IGEL UMS is to create an organized folder configuration. Of course, there is indeed no “right way” to do this, but there are best practices that are designed to make your life a bit better in the long run.

In this section, we will recommend a folder structure based on best practices, although you are not required to keep this structure. The sky is the limit. It is entirely up to you on how to design your folder structure.

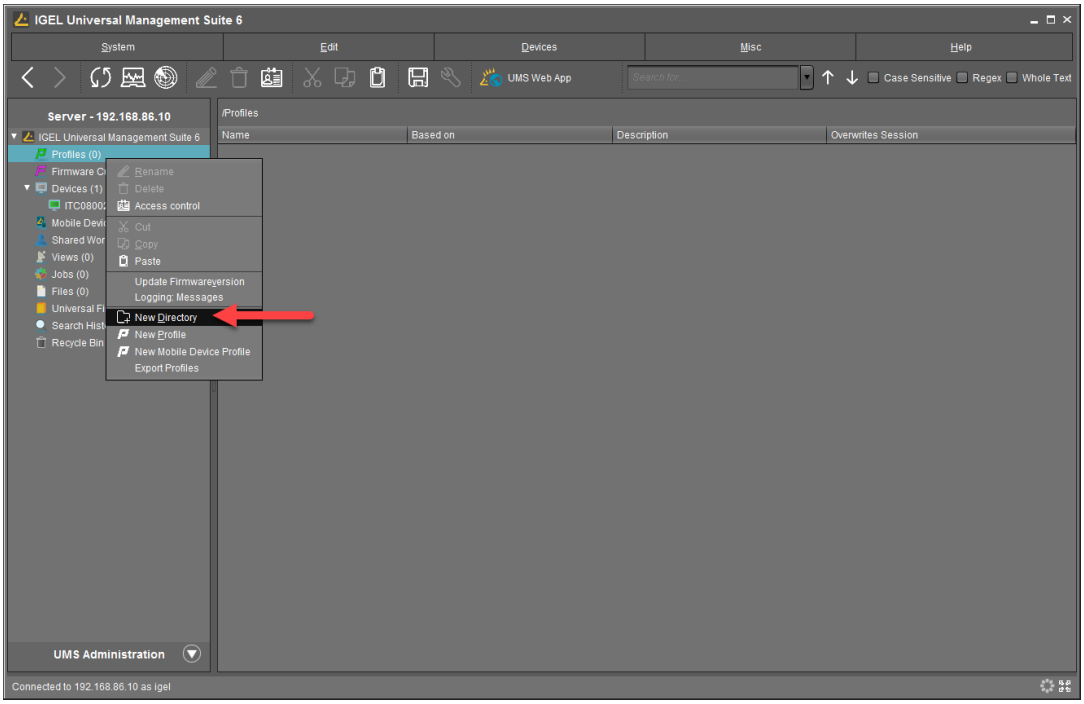
> Learn more about Profile folder structure at **https://kb.igel.com/endpointmgmt-6.06/en/creating-profiles-37281247.html**
>
> Learn more about Device structure at **https://kb.igel.com/endpointmgmt-6.06/en/creating-device-structures-37281229.html**

The following details how to create a basic folder structure for your profiles:

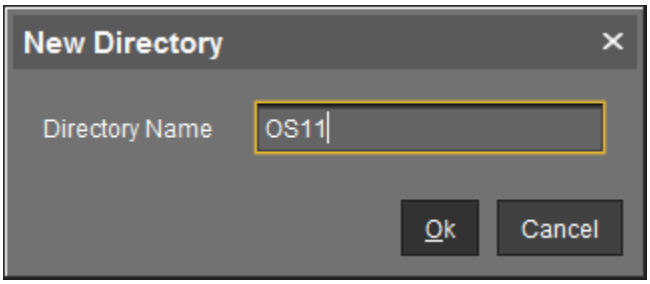
1. From the UMS, right-click on the **Profiles** item in the left menu.



2. Click **New Directory**.

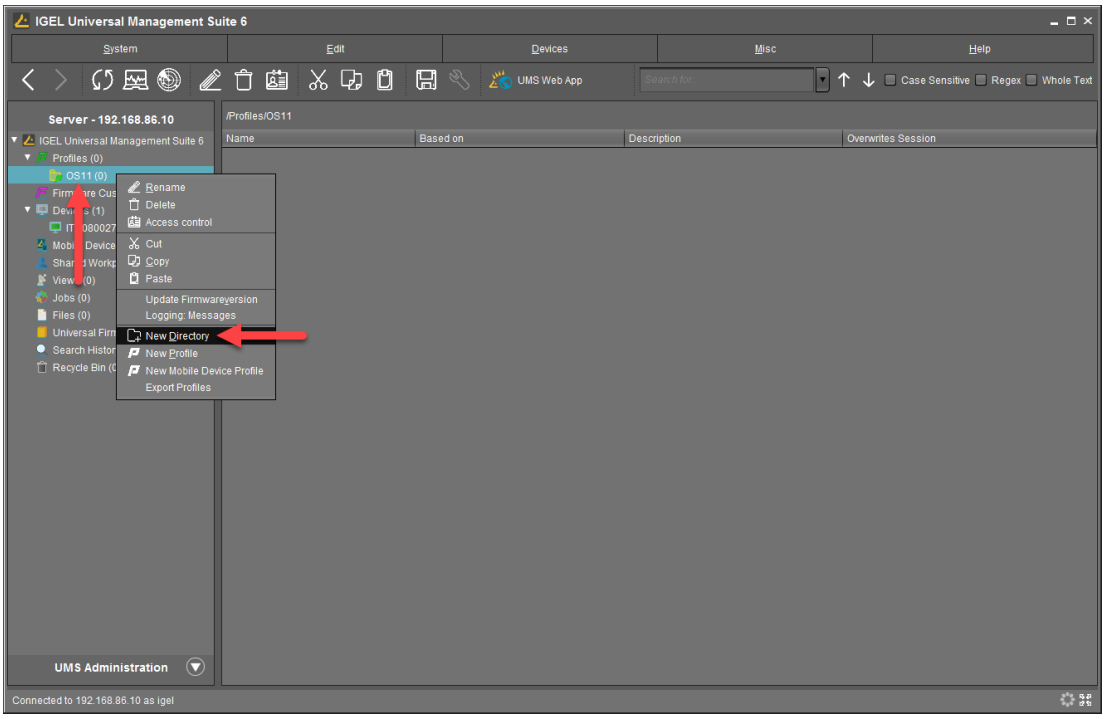


3. As stated above, IGEL UMS profiles are based on IGEL OS versions. In this example, you are installing the IGEL OS Creator using the IGEL OS 11 firmware. Enter **OS11** in the **Directory Name** text box and click **Ok** to create the new folder.

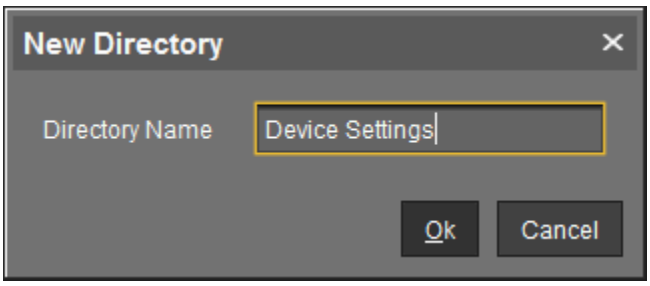


4. Under the OS11 folder, you will create a folder for the different profiles you will be making. These folders will store profiles that control how the local operating system should look and behave.

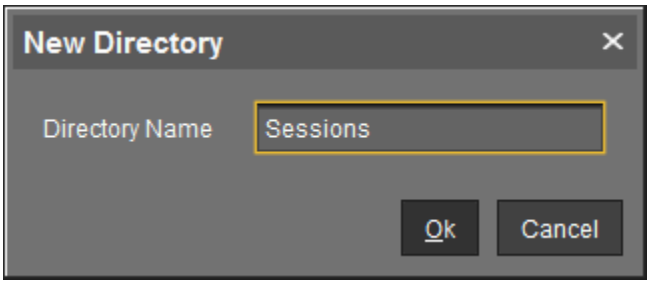
   Right-click on the newly created **OS11** folder and click **New Directory** entry.



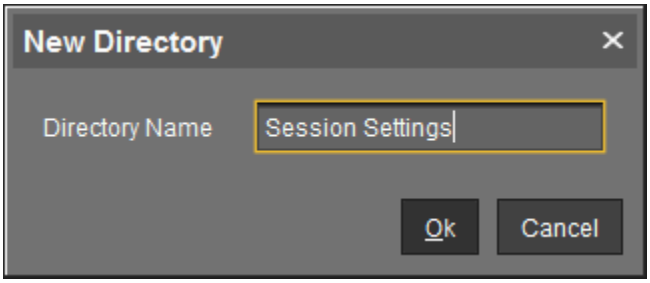
5. Create a folder to save the device-specific configurations. Enter **Device Settings** in the **Directory Name** text box and click **OK** to continue.



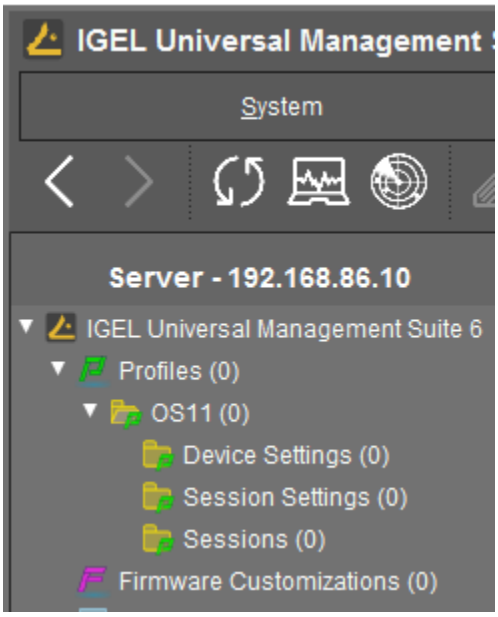
6. Repeat the above two steps, but this time create a new folder named **Sessions**. This folder will store the different types of sessions you will be deploying to the IGEL OS.



7. The last folder you want to create is **Session Settings** and is used to store profiles for specific settings, located in the **Sessions** folder.

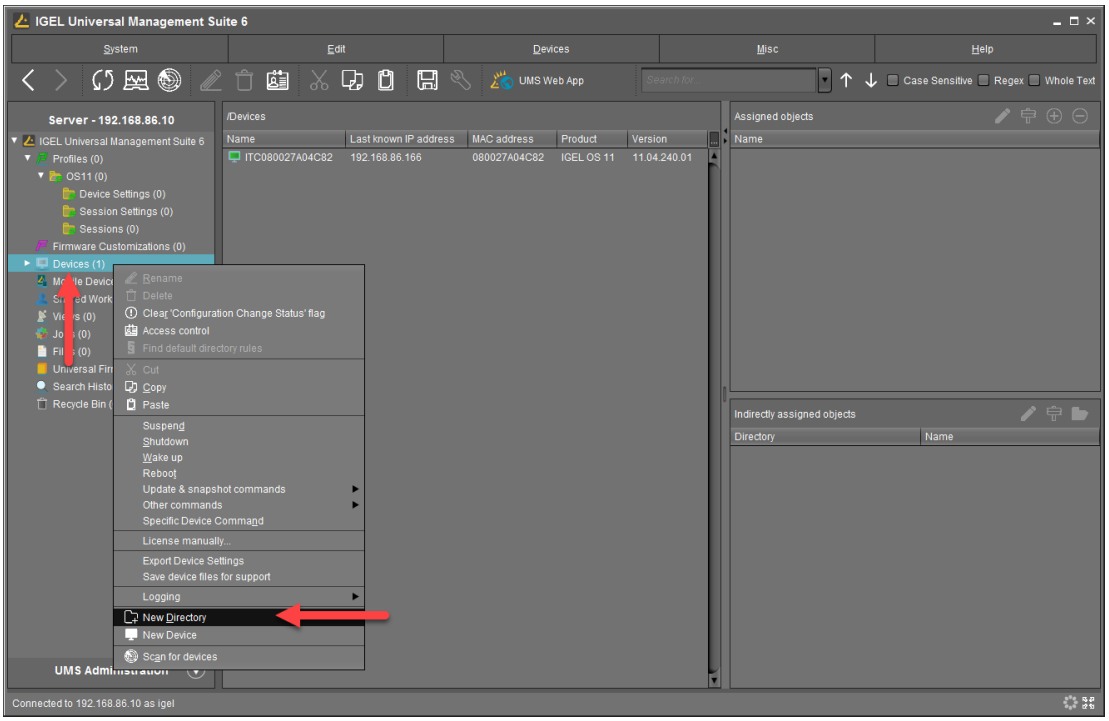


8. Once finished, you will see a Profile folder structure that looks like the following image.



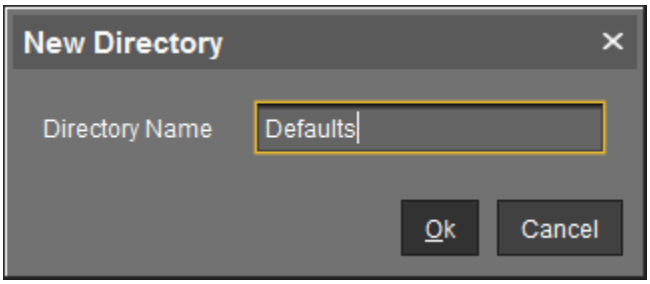
9. Now you are ready to configure a folder structure for your devices. This can be done in many different ways. For example, by location, business department, etc. It is indeed up to you! For our case, we will configure a folder structure based on geolocation!

   Right-click on the **Devices** node and select **New Directory**.

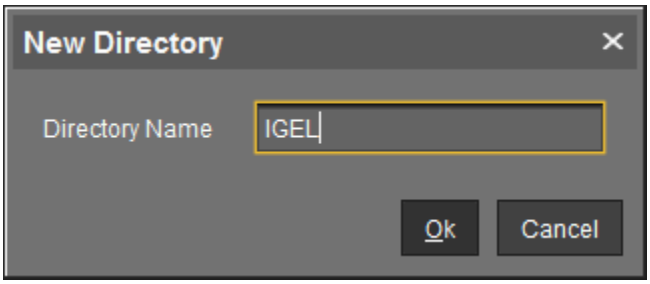


10. From time-to-time, it is nice to take a device back to an OS without any assigned configurations by removing predefined settings. To do this, I would recommend having a simple ‘defaults’ folder where you can drag-and-drop devices to eliminate any settings instantly. The device can always be moved back to the desired folders at will.

    In the **Directory Name** text box, enter **Defaults** and click the **OK** button to create the new folder.

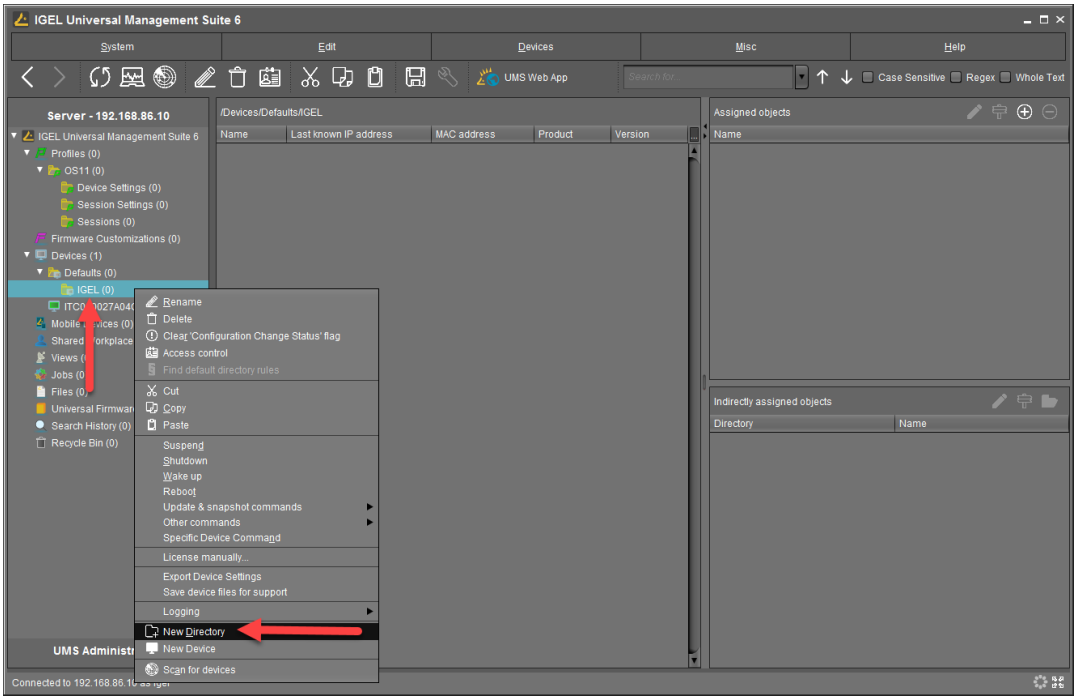


11. Next, I like to create a high-level folder based on the company or organizational group. As above, create a new folder with the name of your predefined organizational group.

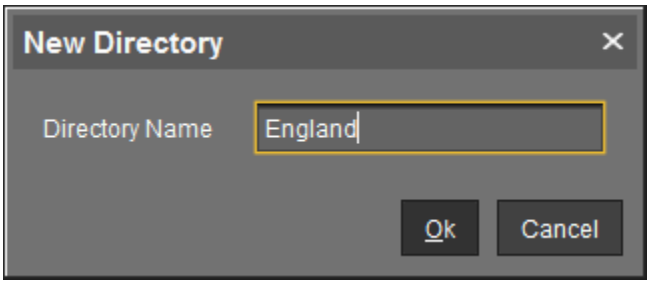


12. Now you will create a geolocation folder, but remember, how you make your structure is up to you. You can define it any way you see best.

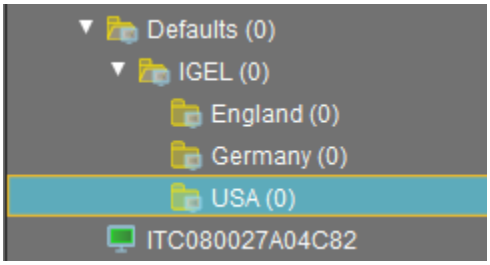
    The point of this example is to teach you what is possible and that anything is possible. Right-click on the folder you created above and click the **New Directory** link.



13. Give the new directory a name and click the **Ok** button to save the new grouping. Repeat this step for every directory you wish to create.

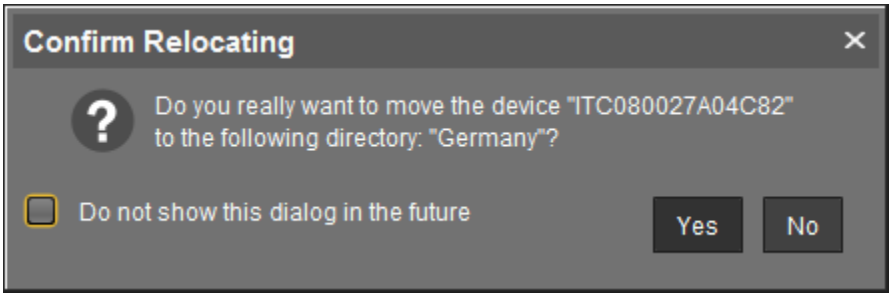


14. Once finished, your directories will be created to your liking based on your organization and what is best for organizing your devices.



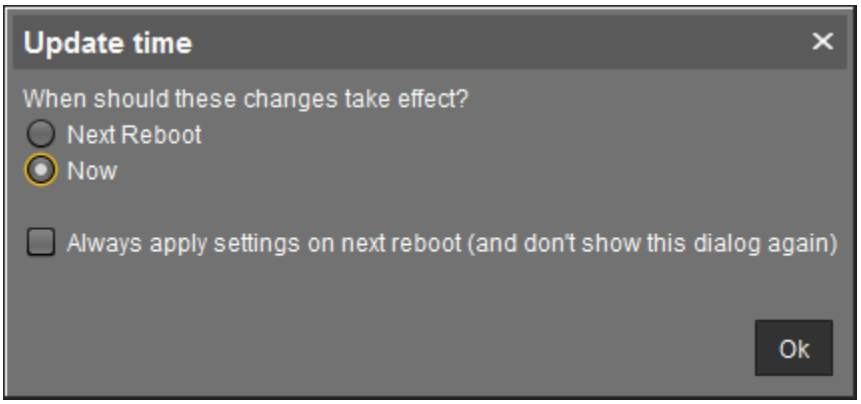
15. Now it is time to move the device(s) we created above to the desired folders. To do this, you can right-click on a device and click copy and then paste it. You can also easily drag-and-drop the device to the folder of your choosing using the mouse. Now that is what I call cool and powerful.

    Click **Yes** to continue.

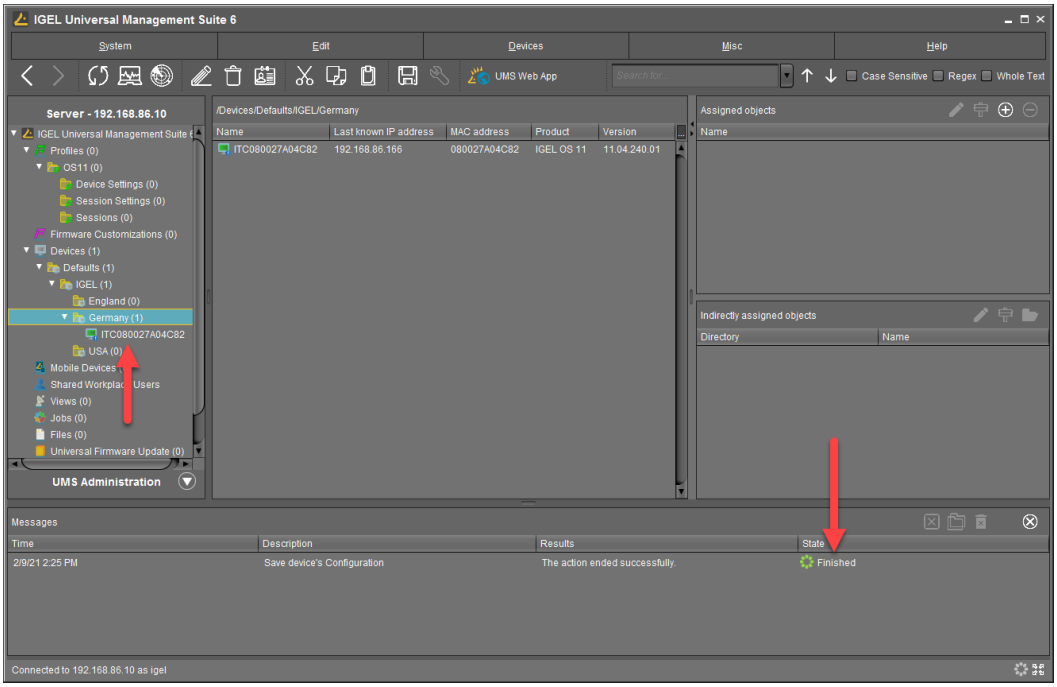


16. When you move a device from folder to folder, you change the configuration associated with the device. It will now inherit the settings assigned to the new folder and its hierarchy.

    Of course, we have not configured anything yet, but soon you will. Go ahead and click the **Ok** button to continue.



17. Once finished, you will see a devices folder structured just how defined!



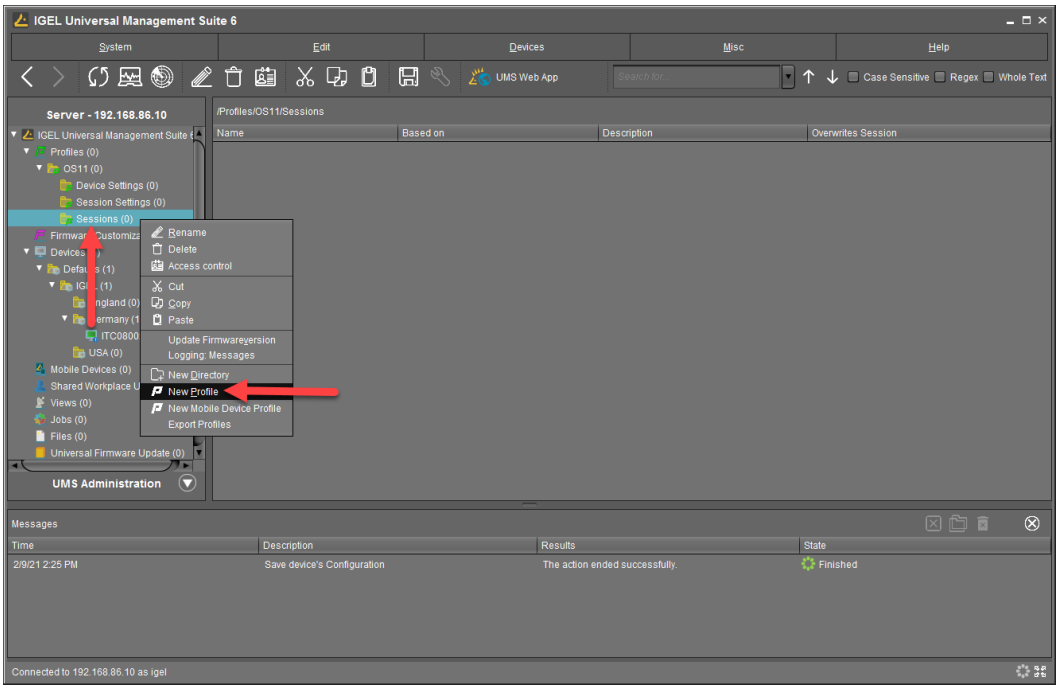
You are ready to create your first profile so let's get to it.

1. 2. How to Create Basic UMS Profiles

Now that you have set up a basic folder structure, you can configure the IGEL OS. Let's bring this thing to life and create your first profile.

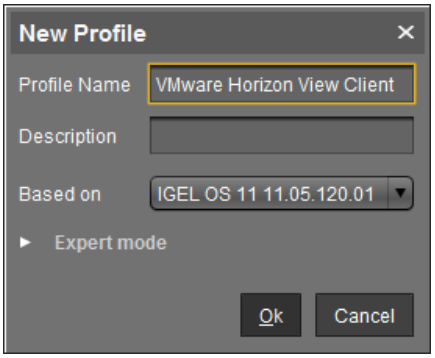
The following steps detail how to create a basic profile and assign it to client devices running the IGEL OS. In this example, you will configure the **VMware Horizon View client**.

1. From the left window of the UMS, expand the **Profiles** node and right-click on the **Sessions** folder you created above, and click **New Profile**.



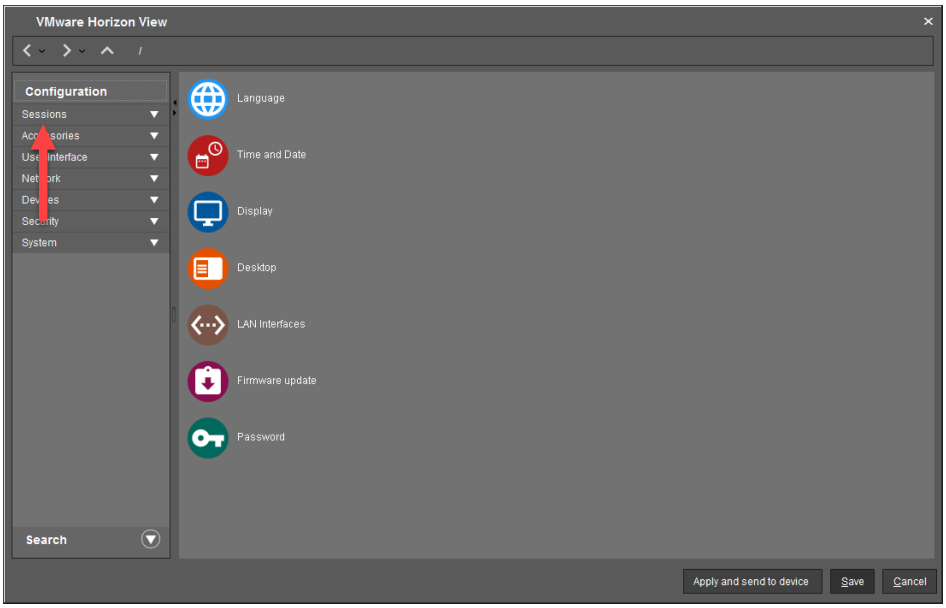
2. The **New Profile** window opens. Enter the name of the profile in the **Profile Name** text box. Make this title descriptive so you and others understand its purpose — for example, **VMware Horizon View Client**.

   Click the **Ok** button to continue.



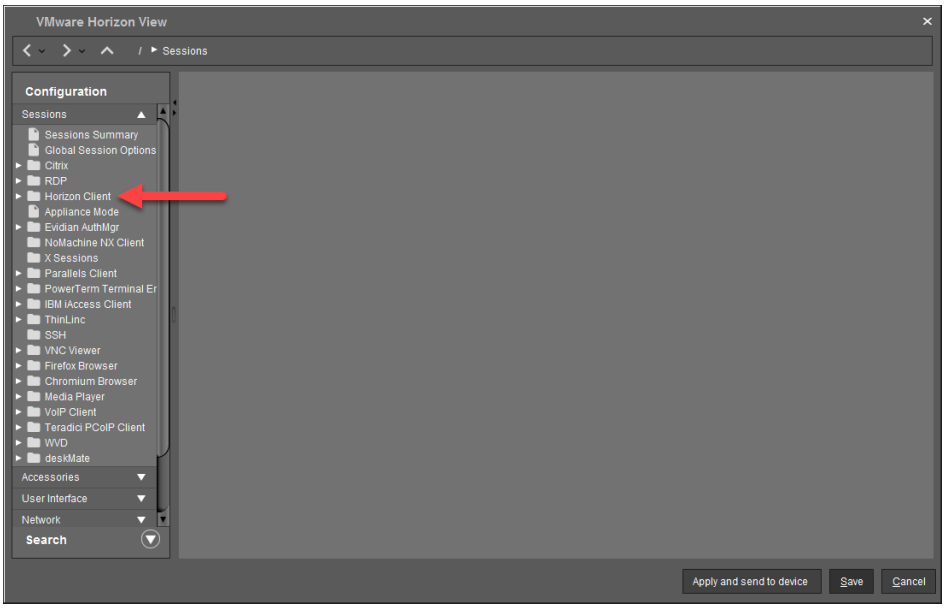
3. The profile window opens, and you are presented with templates for typical configurations, although you are far from limited to what is listed. The UMS has over 7,000 possible settings!

   In this example, you are creating a session to a VMware Horizon environment, click the **Sessions** down arrow to expand the node.

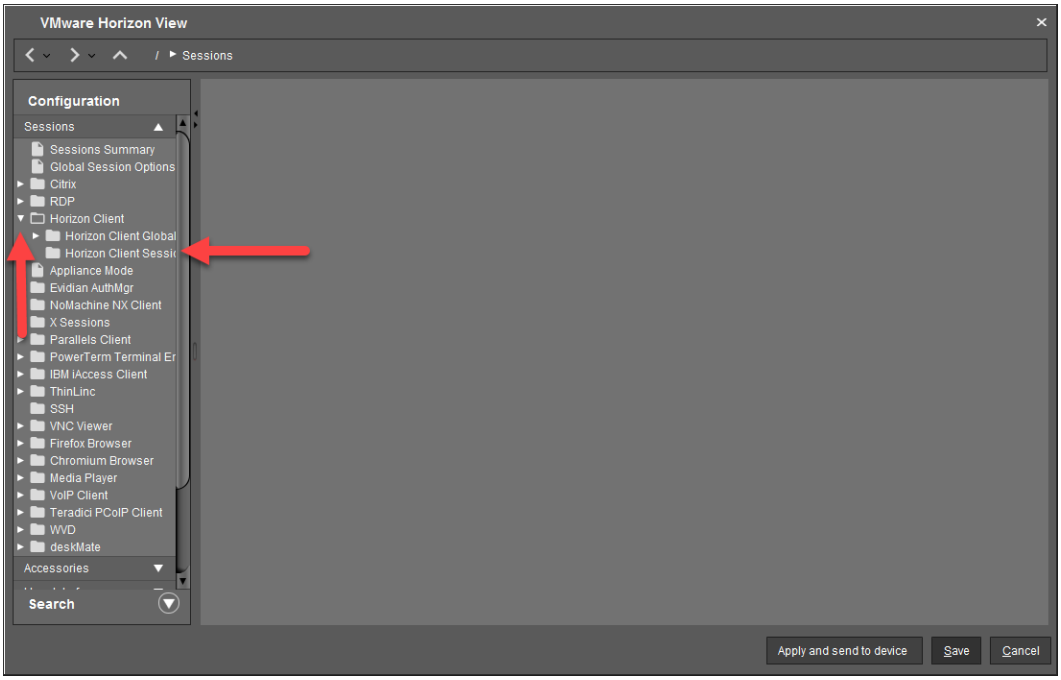


4. You are presented with all the possible sessions you can configure. Take a second or two to browse through this list. You will find sessions, such as Citrix XenApp, XenDesktop, Microsoft RDP, SSH, VNC Viewer, Firefox browser, Multimedia Player, and so much more. The possibilities never cease to amaze me.

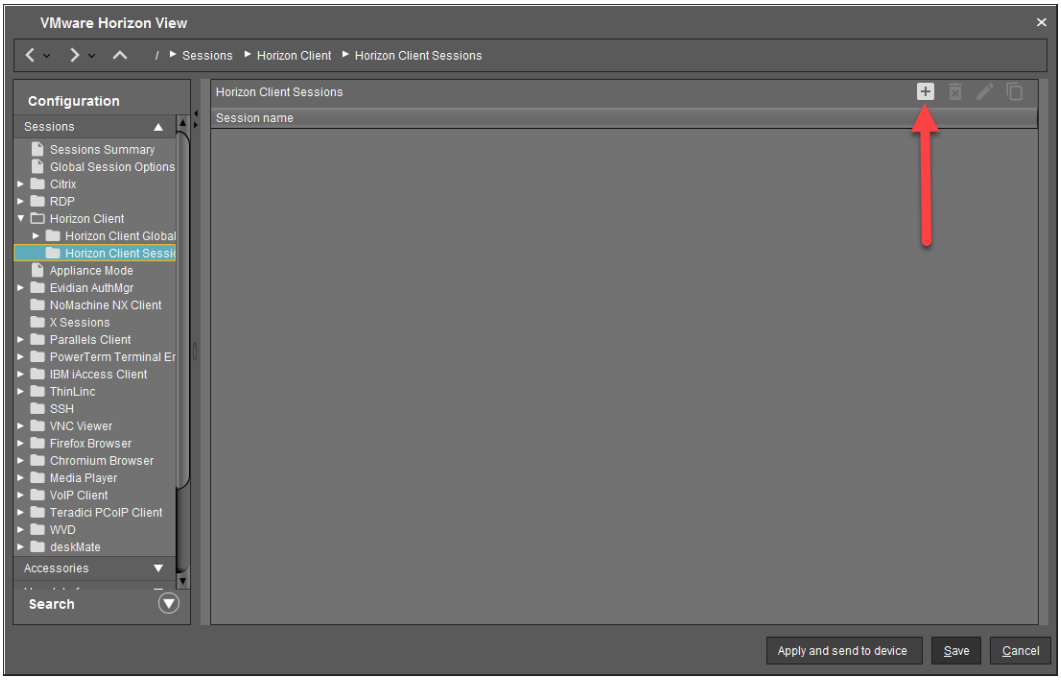
   Click **Horizon Client** to expand the node.



5. Click the **Horizon Client Session** item.



6. Click the + icon located on the top right of the window.

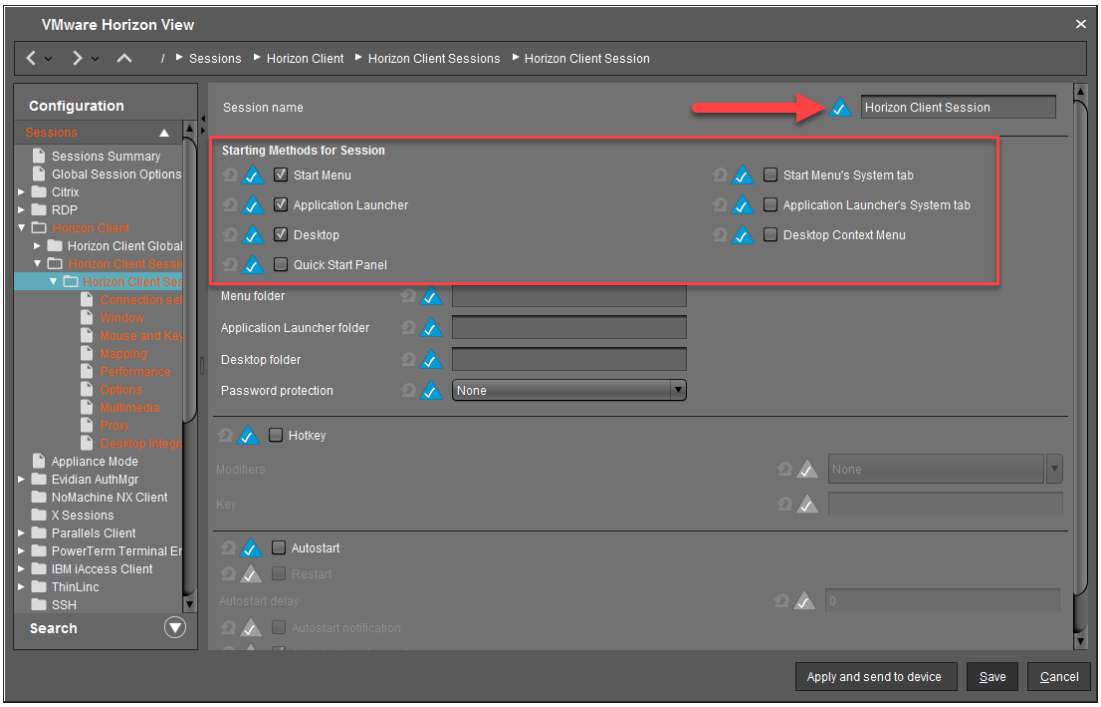


7. The **Desktop Integration** page opens. This is the same screen you will see if you click the **Desktop Integration** link at the bottom of the list. This screen is important as it allows you to define where and how it is presented to the user.

   You can specify the name in the **Session Name** field.

   You can also define where the session will be displayed. For example, you can configure the system to place an icon on the user's desktop, the start menu, or maybe add it to the context menu displayed when the user right-clicks on the desktop. It is all up to you.

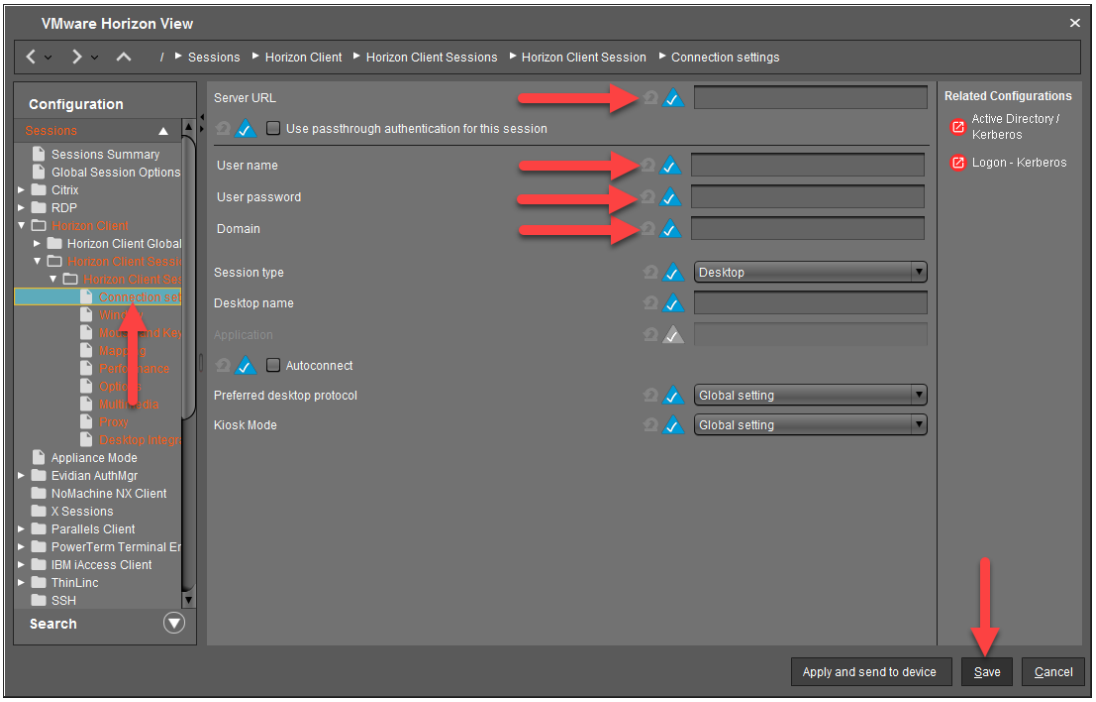
   Define where you would like the session's application icon to be displayed by clicking on the desired settings blue triangle to enable editing each setting.



8. You are presented with a big list of the settings and configurations for the VMware Horizon Client. Feel free to browse the list to familiarize yourself with them.

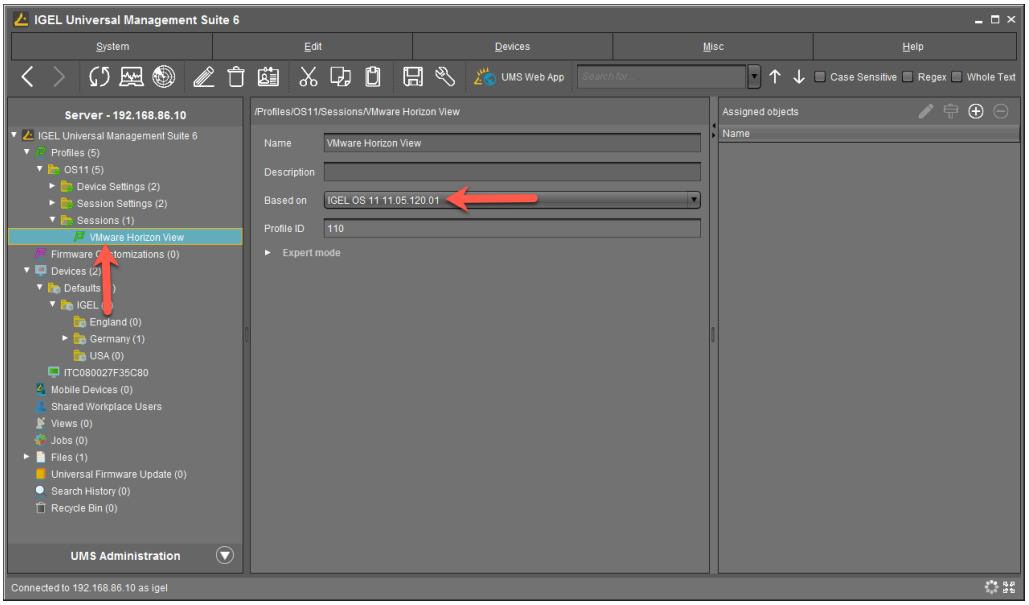
   To create a simple connection, you need to configure only a couple of sections. Click on the **Connection Setting** node. At the least, you are required to set the **Server URL**, **User Name**, **Password**, and **Domain**.

   When finished, click the **Save** button to save the new profile.

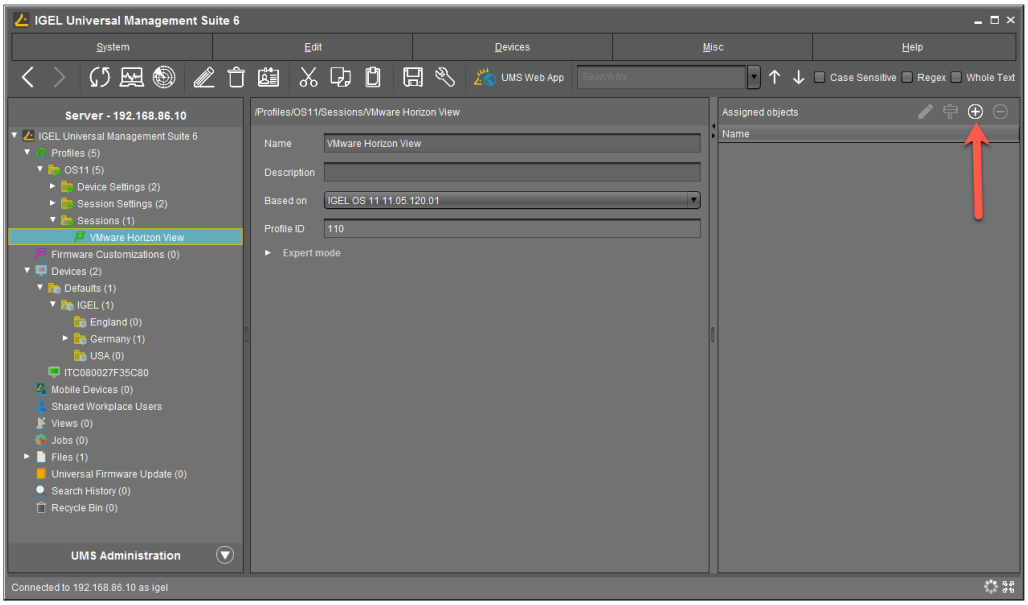


9. You are brought back to the UMS, and the VMware Horizon View client is listed in the list of profiles.

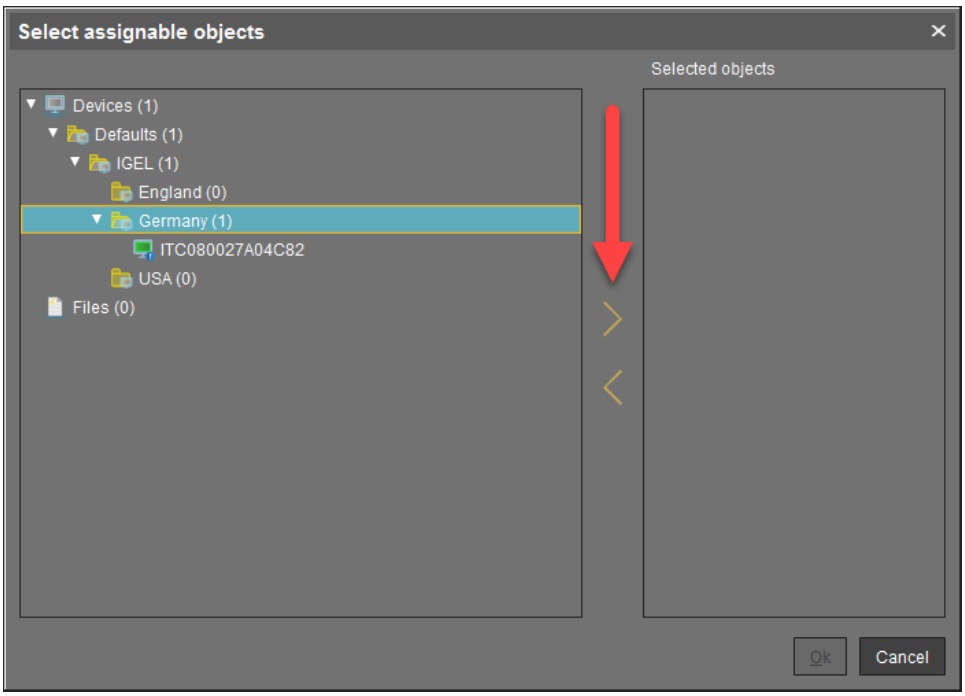
   To deploy a profile, you are required to assign the profile to the desired IGEL OS devices. You can do this by dragging the profile and dropping it on top of an IGEL OS in the Devices node or a folder of the IGEL OS device. This is up to you. You can also do it by clicking the arrow on the right side of the screen to expand the **Assigned Objects** pane of the UMS.



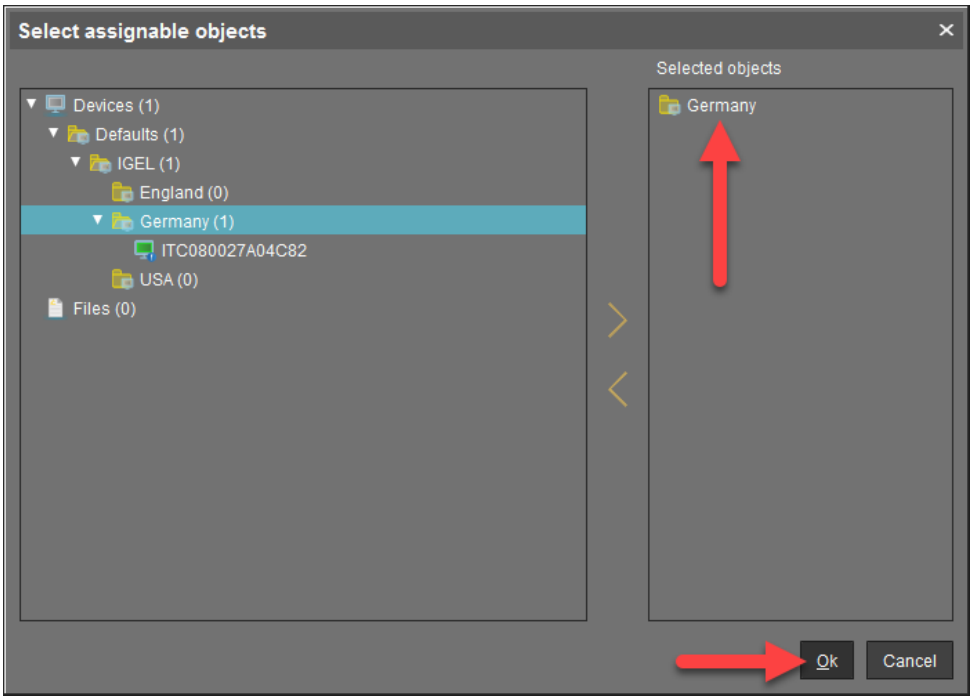
10. Click on the + icon on the top right of the UMS.



11. The **Select assignable objects** window opens. Here you can select folders of IGEL OS devices or even an IGEL OS itself to assign it to the selected profile. Select the desired folders or clients and click the > arrow to move it to the **Selected objects** section.

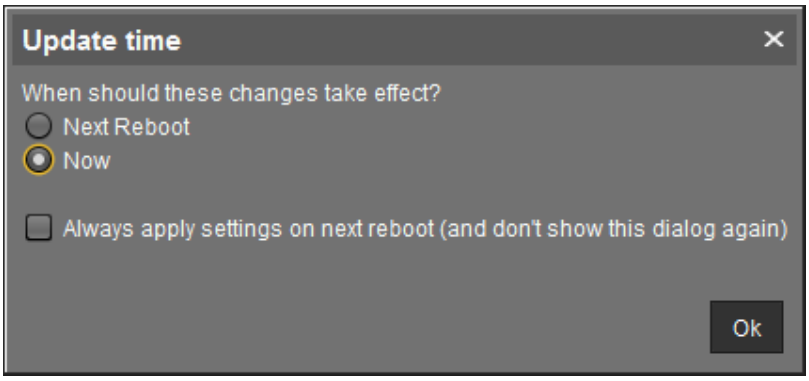


12. Once you have defined the objects to assign to the profile, you can click the **Ok** button to save it.

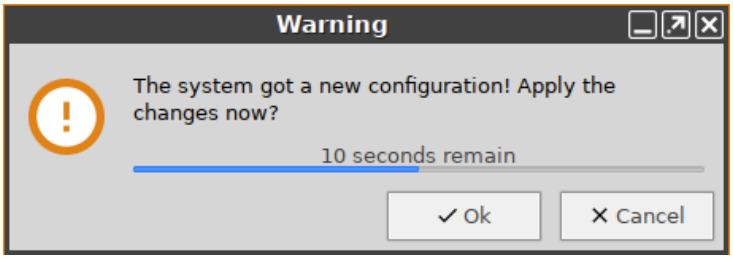


13. You are prompted to specify at what time the new settings will take effect. You can have the profile take effect the next time the user reboots the OS, or you can make the changes take effect right NOW! Yes, it is that powerful: real-time changes, no reboots required! This is up to you and your organizational policies.

    For this example, click the **Now** radio button and click **Ok** to apply this change in real-time.



14. Look at the device running the IGEL OS, and you might see a popup informing you a new configuration is going to be applied, or you might notice the policy has taken effect. In this case, the **Horizon Client Session** icon is added to the desktop and/or wherever you configured it to be placed.



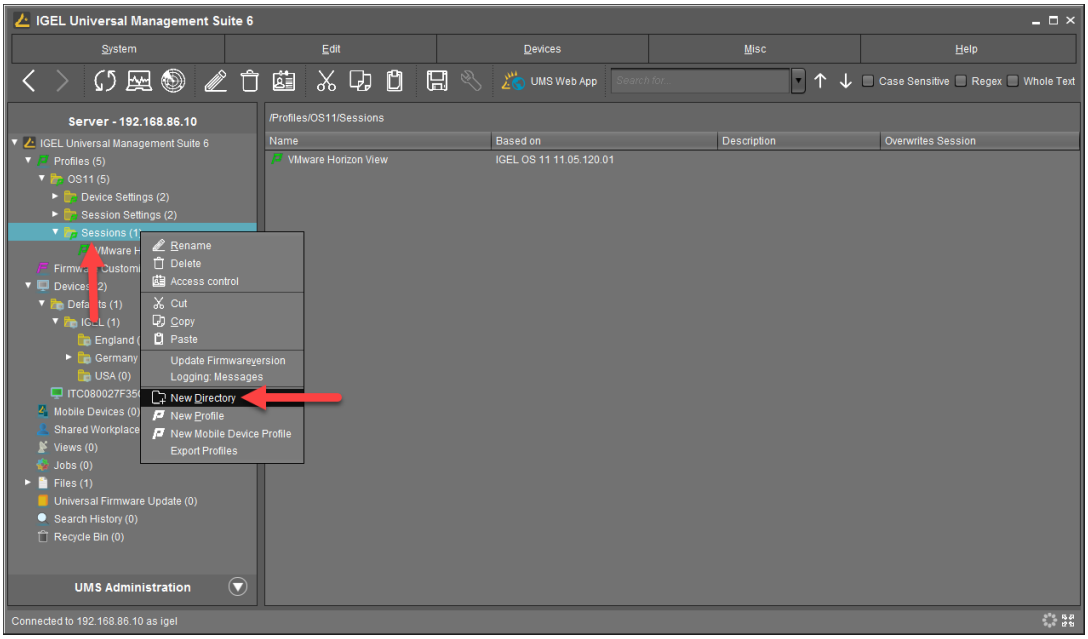
It’s that simple! This is the POWER of the IGEL Software Suite! Trust me, you can do almost anything, so have some fun and play around with profiles.

1. 3. How to Create a Chromium Session

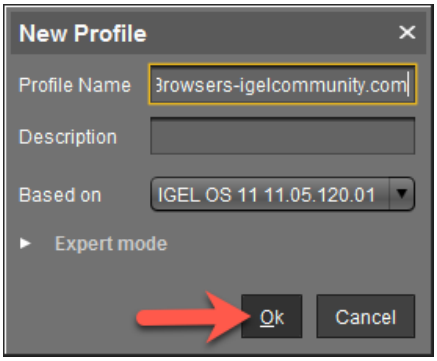
The IGEL OS ships with the Chromium Web browser. This will come in handy for typical web browsing, your corporate SaaS applications, and connecting to services such as Citrix.

The following section details how to deploy the Chromium Web browser to the IGEL OS device:

1. Open the IGEL UMS and expand the **Profile** node. Then right-click the **Sessions** folder and click the **New Profile** link.

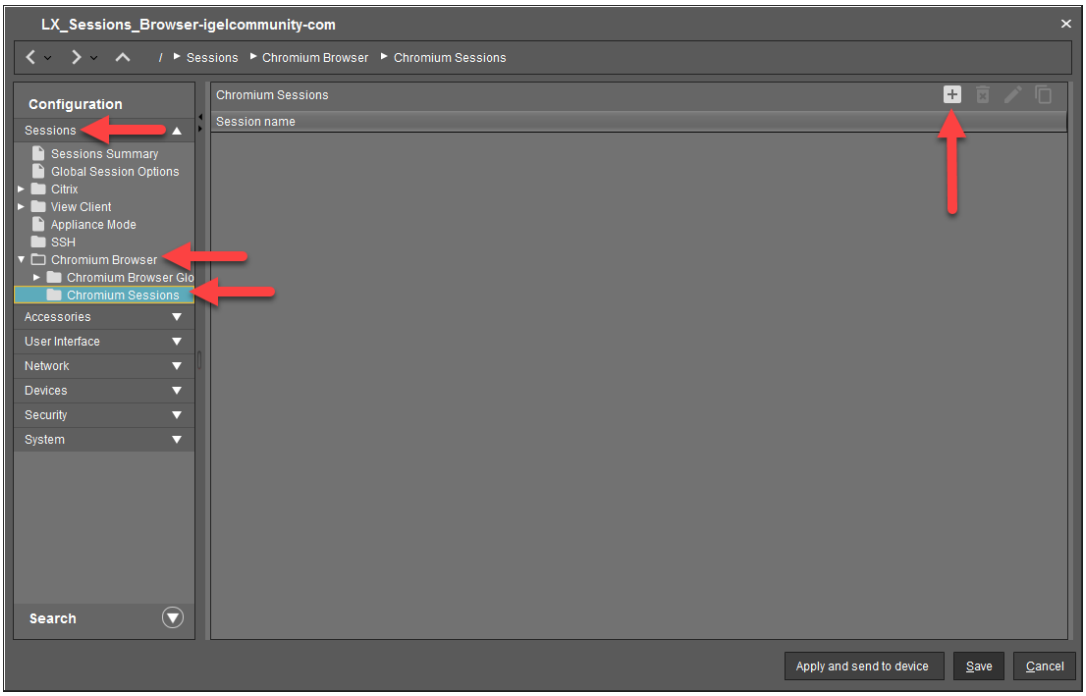


2. Enter a descriptive name for the profile in the **Profile Name** text box. Click to open the **Based On** combo box and click to select the desired IGEL OS version, in our example, **IGEL OS 11 11.05.120.01** entry. Once finished, click the **Ok** button to continue.



3. The profile settings window opens, and you are ready to add and configure the Chromium browser. From the left menu, click to expand the **Sessions** node, click to expand the **Chromium Browser** node, and select the **Chromium Sessions** item.

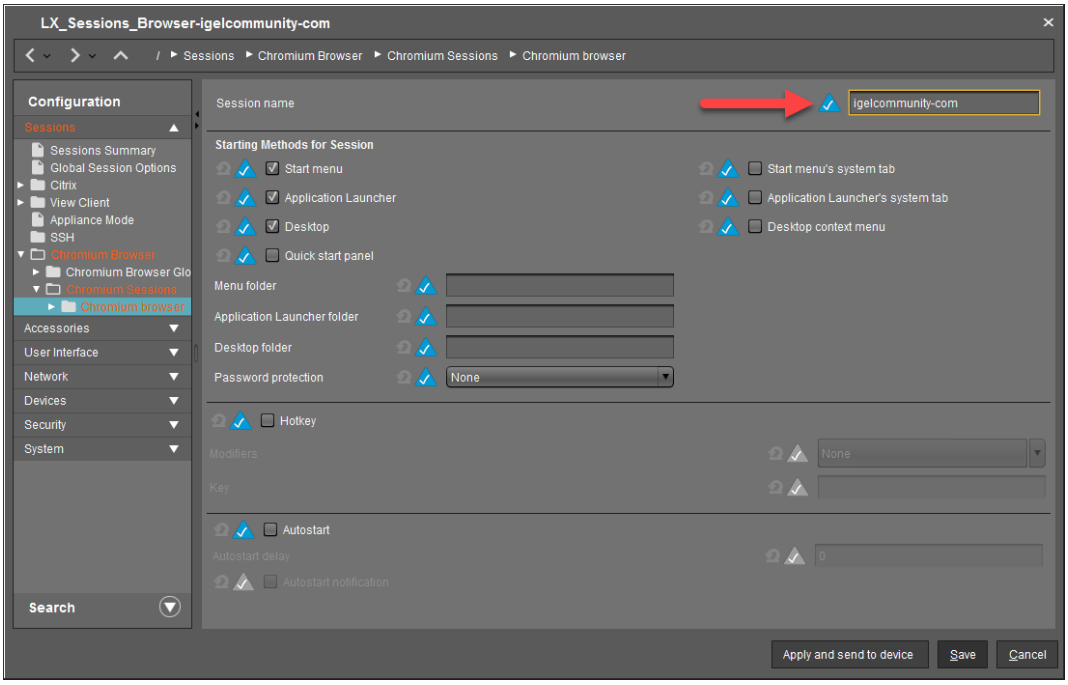
   To create a Chromium Browser, click the **+** button on the top right of the page.



4. A new node named **Chromium browser** is added below the **Chromium Sessions** node. If you desired only a Chromium browser added to the IGEL OS desktop, you could click the **Save** button now, but you might want to make some modifications. The IGEL UMS has many configurations available.

   By default, the Chromium browser is the default name assigned already, but you might want to change this to something else. In this example, we have changed it to igelcommunity.com as we will be preconfiguring the browser to use the igelcommunity.com webpage as the browser's home page. It is up to you if you would like to enter a custom name in the **Session name** text box. This name will appear under the Chromium icon on the IGEL OS desktop.

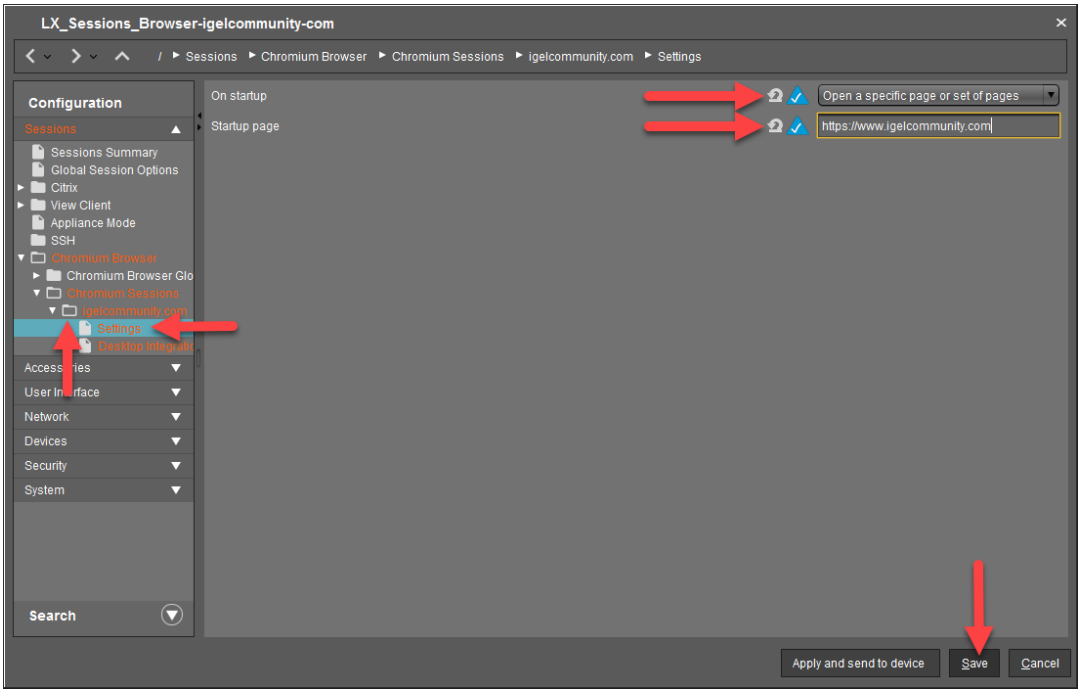
   You can also define where the session will be displayed. For example, you can configure the system to place an icon on the user's desktop, the start menu, or maybe add it to the context menu displayed when the user right-clicks on the desktop. It is all up to you. Play around and have fun. As with everything IGEL does, the sky is the limit.



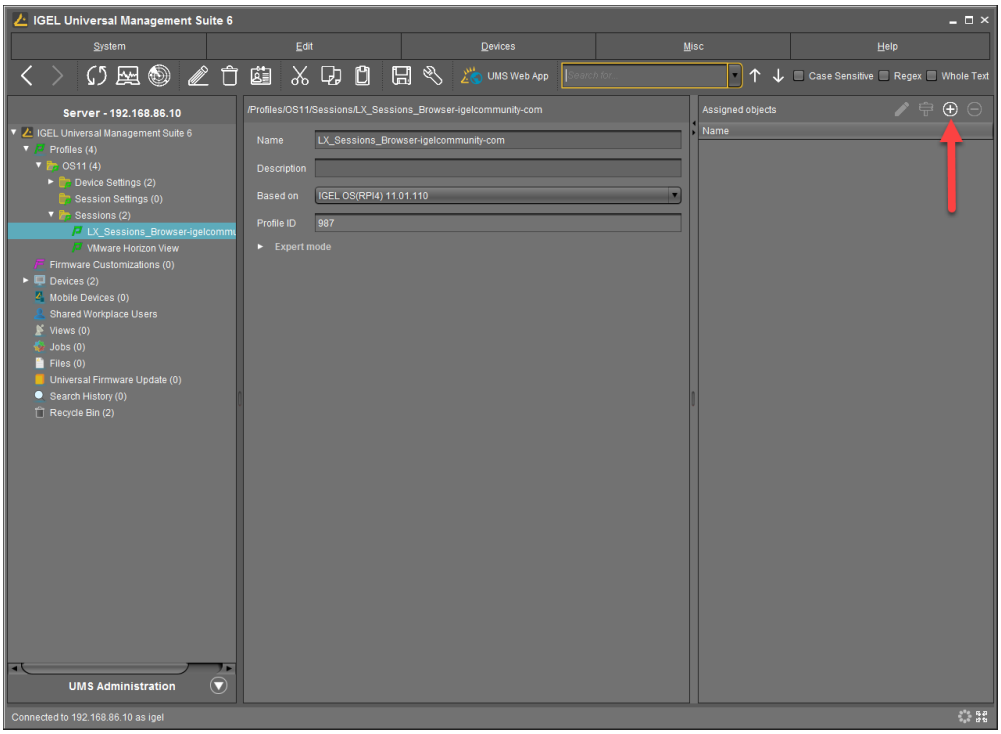
5. The next step is to choose the startup page. This is the web page that will be loaded when the browser is started. To configure a startup web page, click to expand the node named with the session name you defined above and click to select the **Settings** node.

   Click to open the **On startup** combo box and select **Open a specific page or set of pages** item. In the **Startup page** text box, enter the URL of the web page you wish to set as your home page/startup page.

   Once finished, click the **Save** button. Your Chromium Browser is ready to be assigned, deployed, and used!

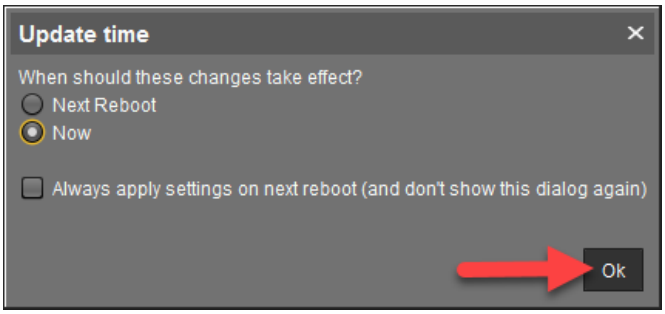


6. You are brought back to the IGEL UMS. Click the **+** icon located on the top right of the screen.



7. The **Select assignable objects** window opens. Please select the desired folders or clients and click the **>** button to move it to the **Selected objects** section. Once you have defined the objects to assign to the profile, you can click the **Ok** button to save it.

8. You are prompted to specify at what time the new settings will take effect. For this example, click the **Now** radio button and click **Ok** to apply this change in real-time.



9. The browser is configured, flip over to your IGEL OS device, and you should see the Chromium icon.

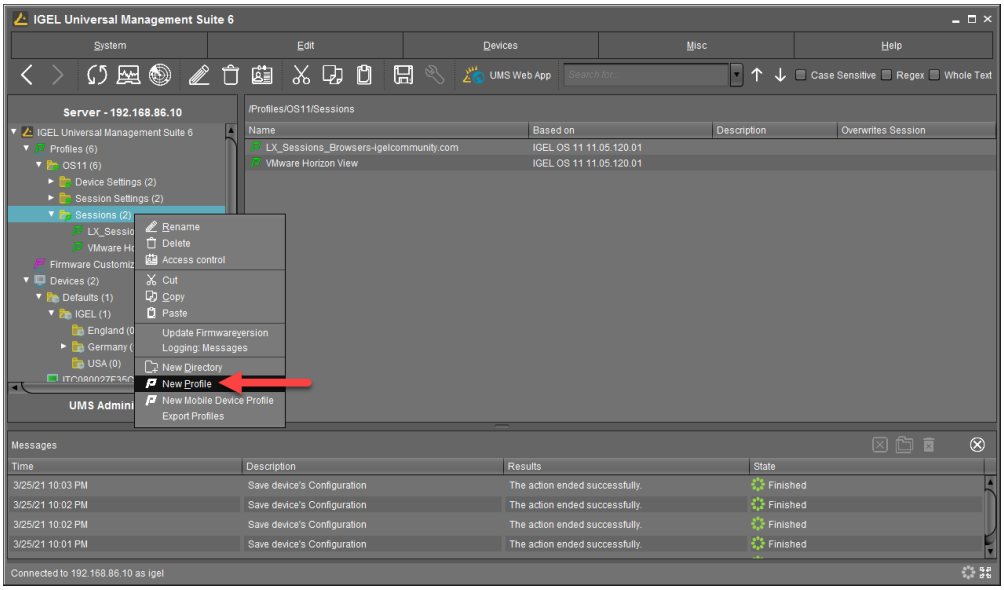
1. 4. How to Create a Chromium Kiosk Session

The IGEL OS device works great in many use cases. For example, a check-in terminal, web kiosk, and even in-store displays for signage. That said, you might find you wish to configure the Chromium browser to perform as a locked-down browser in kiosk mode. No Problem, we got you covered.

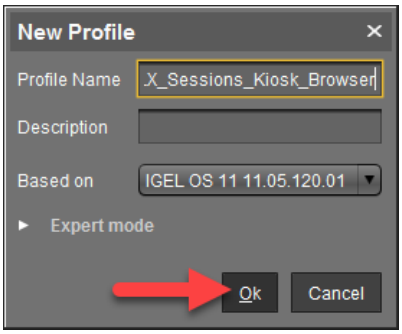
Learn more about **Chromium Browser Global** settings **https://kb.igel.com/igelos-11.05/en/chromium-browser-global-42011078.html**.

The following steps detail how to create a Chromium kiosk session:

1. From the IGEL UMS, expand the **Profiles** node, right-click on the **Sessions** folder, and click the **New Profile** link.

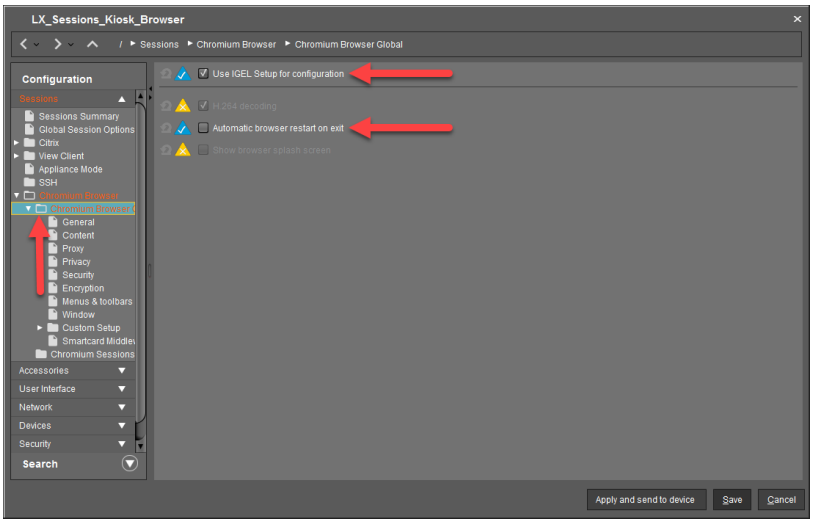


2. Enter a descriptive name for the profile in the **Profile Name** text box. Click to expand the **Based On** combo box and click to select the desired IGEL OS version, in this case, **IGEL OS 11 11.05.120.01** entry. Once finished, click the **Ok** button to continue.

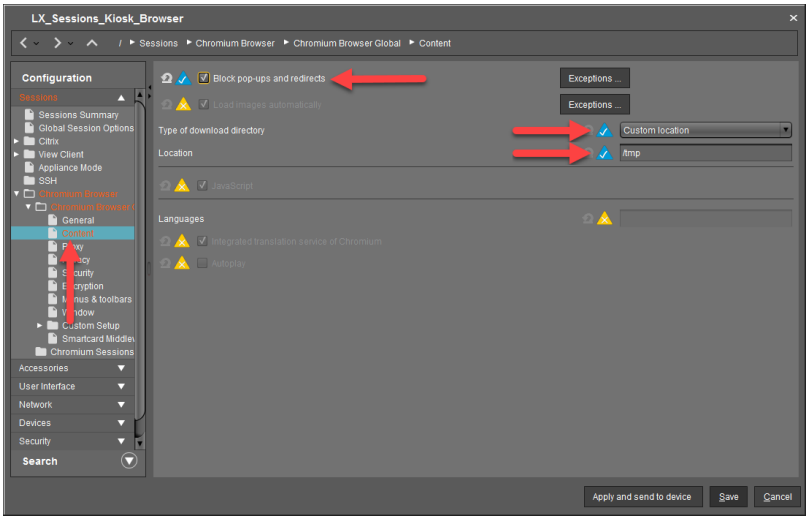


3. The profiles properties window opens, and you are ready to do some configuring. Click to expand the **Sessions** node, click the **Chromium Browser** node, and click the **Chromium Browser Global** entry.

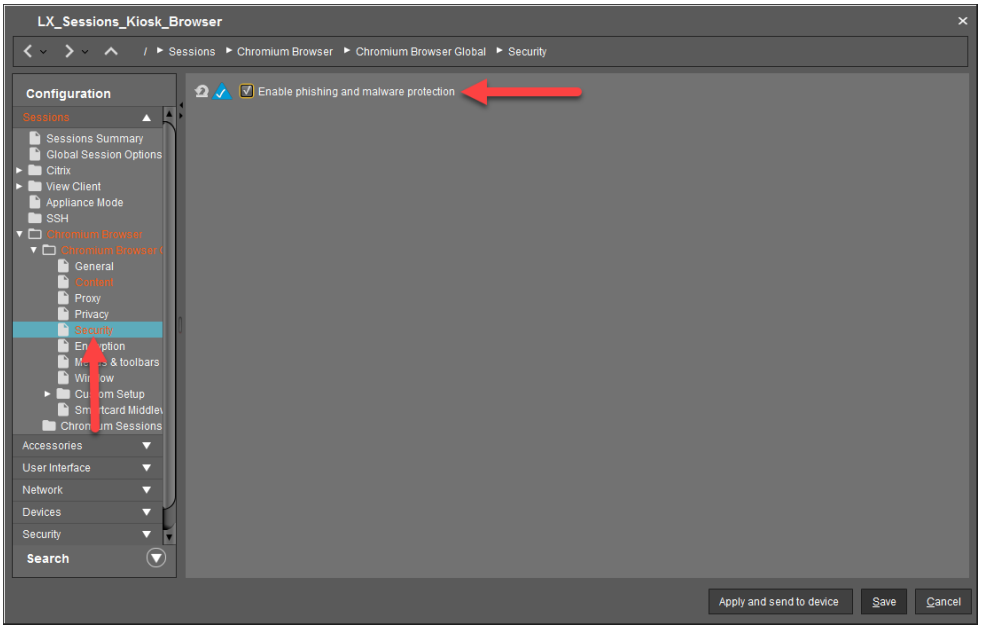
   Click the yellow triangle to change it to blue (configurable) and then click the **Use IGEL Setup for configuration** checkbox. This allows you to configure the below settings. You can now configure a few items, such as H.264 decoding, the ability to restart the browser if it is closed and to show the browser splash screen when Chromium is started. Configure the settings as desired.



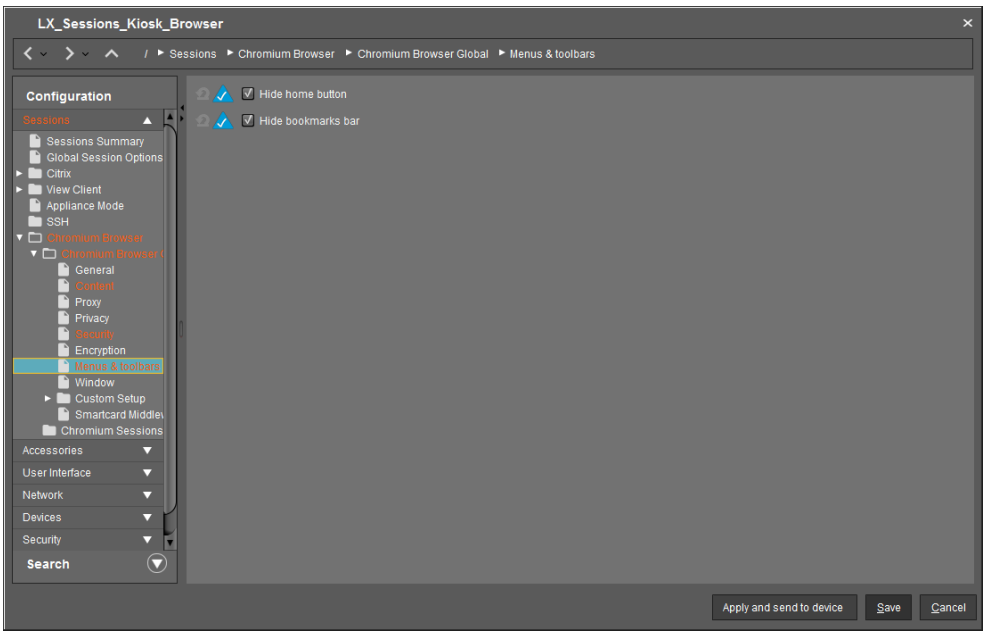
4. Click the **Content** link located below the **Chromium Browser Global** folder. On this page, you can configure how content is treated. For example, you can block pop-ups and redirects, load or disable images automatically, configure the location of the Java library and browser language settings. In this case, you will want to click the yellow triable to enable editing and then click to check the **Block pop-ups and redirects** and to set the download directory, as shown below.



5. Click to select the **Security** link under the **Chromium Browser Global** folder and click the yellow triable to enable editing. Next, click to check the **Enable phishing and malware protection** checkbox. This is always a best practice and will help secure your environment from potential lurking bad guys on the dark web.

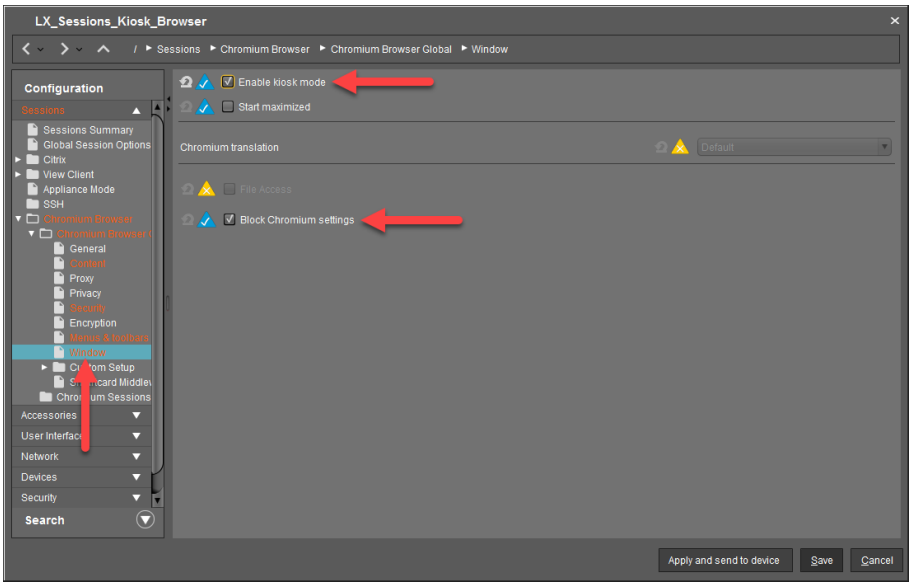


6. Click to select the **Menus & toolbars** link under the **Chromium Browser Global** folder. Here you can configure if the home button is viewable and if you wish to hide the bookmarks bar or not. Since we are creating a kiosk, it is best to hide both. Click the yellow triangle next to both settings and check the checkboxes, if so desired.



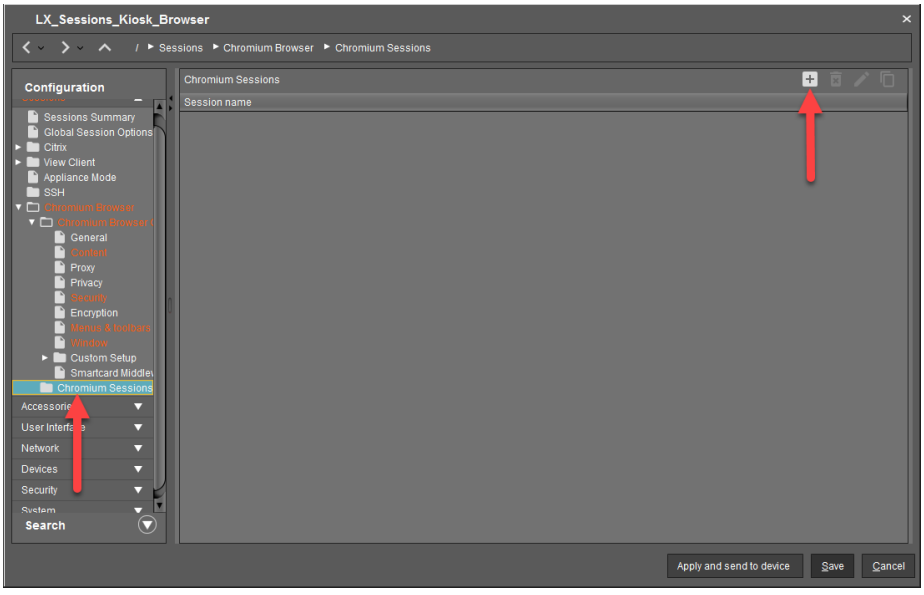
7. Now you can configure how the browser opens. Next, click the **Window** link below the **Chromium Browser Global** folder. Here you can either configure Chromium in kiosk mode by checking the **Enable kiosk mode** checkbox or start the browser in full-screen mode by checking the **Start maximized** checkbox or startup the browser as a windowed app by unchecking both.

   Next, click the **Block Chromium settings** checkbox to disable the Chromium menu accessibility.

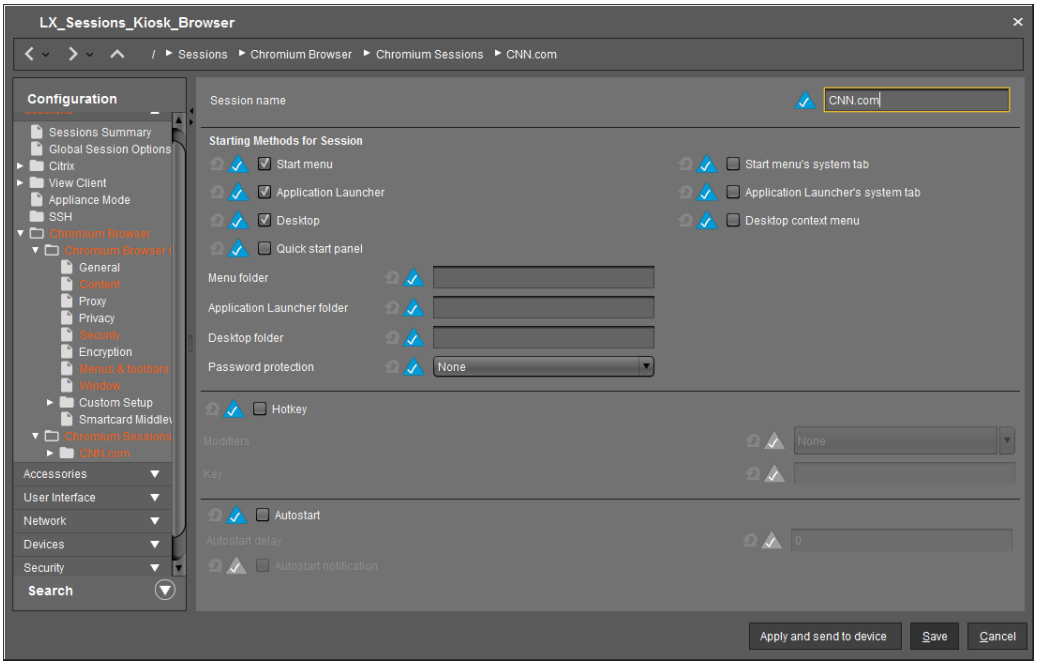


8. You have successfully locked the browser down, and now you are ready to deploy the Chromium browser.

   Click to select the **Chromium Sessions** link under the **Chromium Browser** folder in the left menu, and then click the **+** button on the top right of the IGEL UMS.

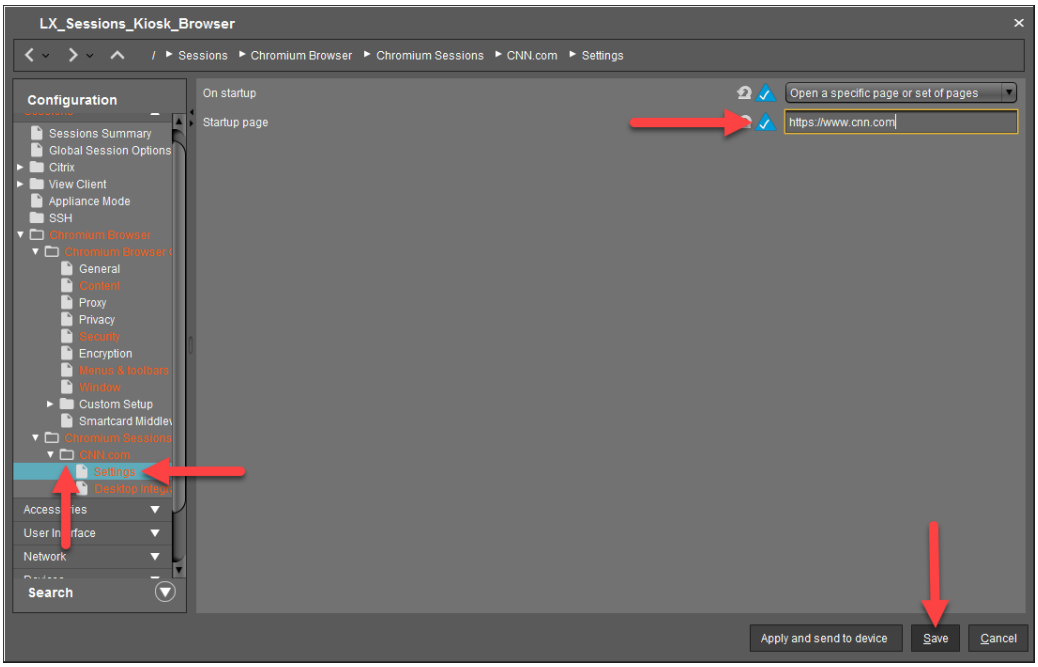


9. Enter the name of the kiosk browser in the **Session name** text box.

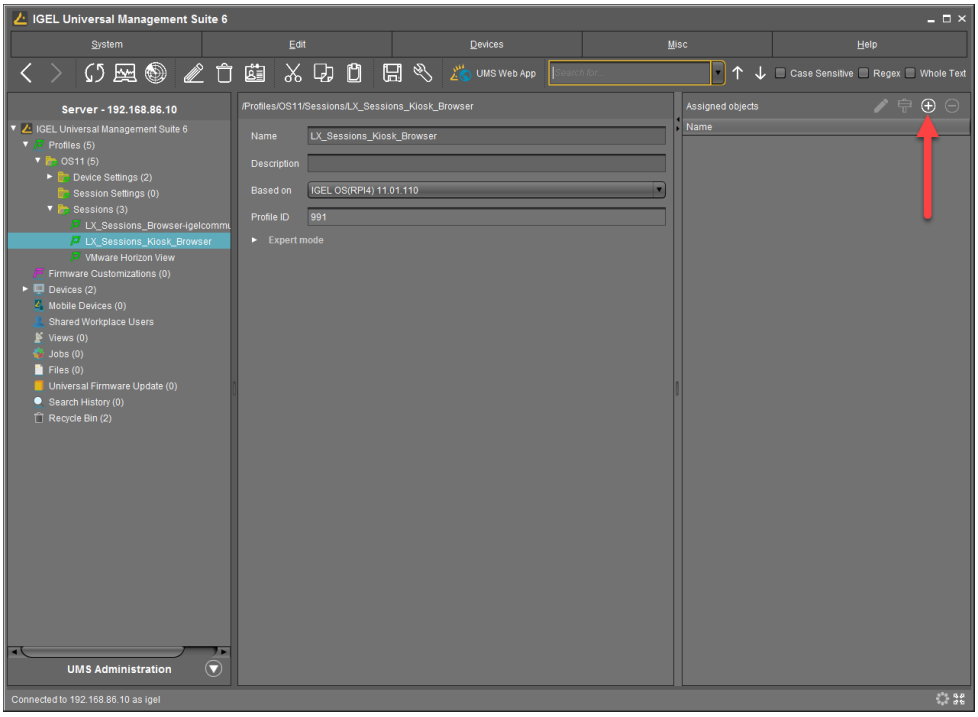


10. Click to expand the newly created cnn.com link and click the **Settings** link. Click to open the **On startup** combo box and select **Open a specific page or set of pages** item. Enter the URL of the website to open upon starting the browser in the **Startup page** textbox.

    You are done. Click the **Save** button to save the profile.

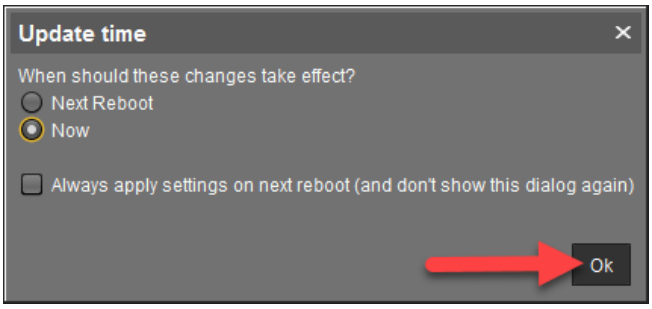


1. The Chromium kiosk profile is created, you are ready to assign it to your devices. Click the **+** button located in the top right of the UMS.



2. The **Select assignable objects** window opens. Select the desired folders or clients and click the **>** button to move it to the **Selected objects** section. Once you have defined the objects to assign to the profile, you can click the **Ok** button to save it.

3. You are prompted to specify at what time the new settings will take effect. For this example, click the **Now** radio button and click **Ok** to apply this change in real-time.



4. Flip over to the IGEL OS device, and you should see the new kiosk browser icon has been added to the desktop.

1. 5. How to install a CA Root Certificate on IGEL OS

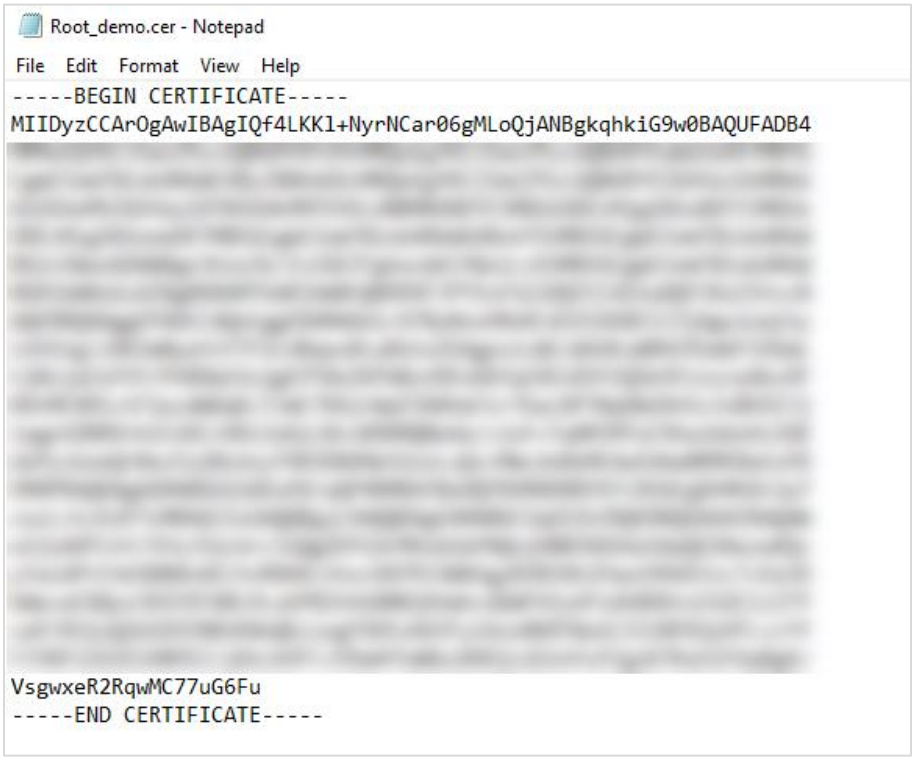
Now that you have learned how to deploy the Chromium browser, it is time to use it to launch Citrix sessions. To do this, the same process you learned above is used. All you need to do is replace the URL to your Citrix StoreFront or Citrix ADC (NetScaler) address.

The following steps detail how to enable Citrix access via the Chromium browser on IGEL OS:

1. The first step is to procure the Certificate Authority Certificates that will be uploaded to the IGEL UMS. If you have trouble getting your Certificate Authority Certificates, please be aware that this process might be best achieved with your PKI / Certificate Management administrator.

   Note: Root Certificate Authorities and/or SubCAs need to fit in BASE64 format.

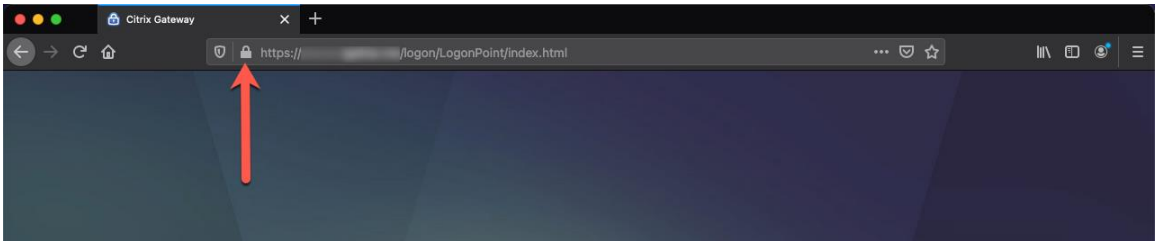
   It is imperative, once you procure the certificate, you will want to make sure it valid. The following is an image of how a certificate should look when you open it using a text editor.



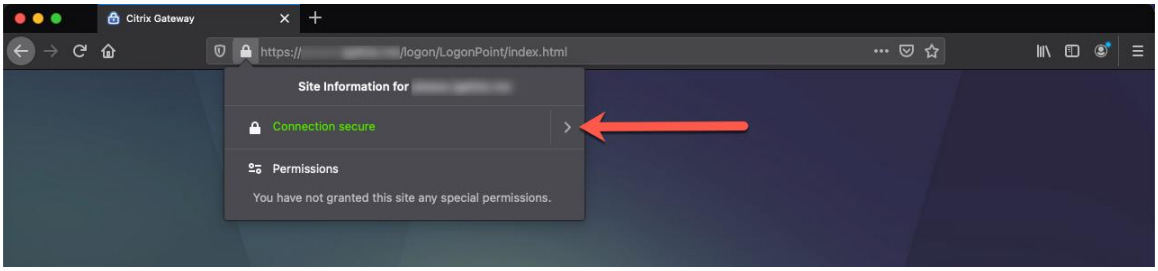
The following is an image of how a certificate should NOT look. If your certificate looks like this, get another as it will NOT work.

2. If you wish to procure the root certificate yourself, a straightforward way is to use Firefox (or any other Browser that can export Certificates in BASE64) and follow the next few steps.

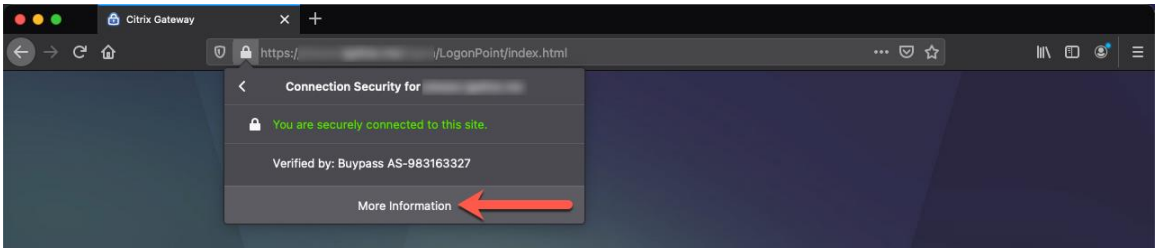
   Browse to the StoreFront or Citrix ADC login page and click on the padlock to the URL's left.



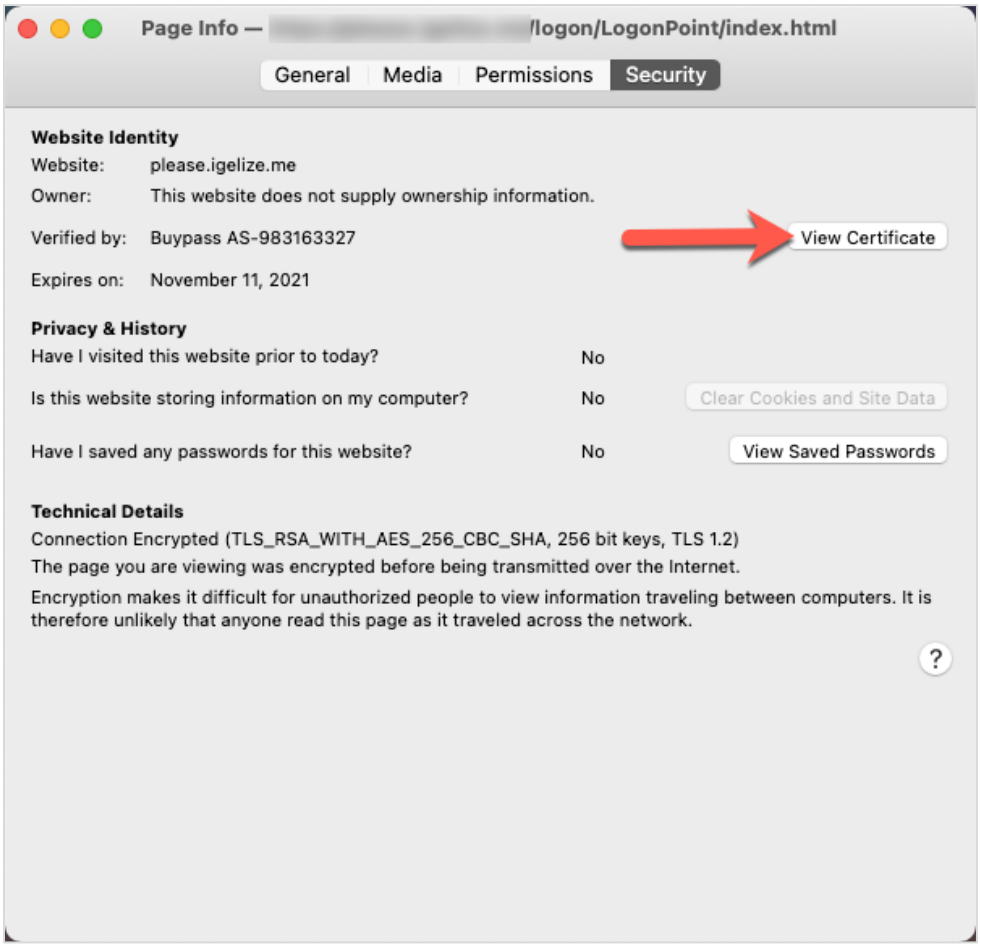
3. If you are using Firefox, click the **>** icon to the right of the **Connection secure** link.



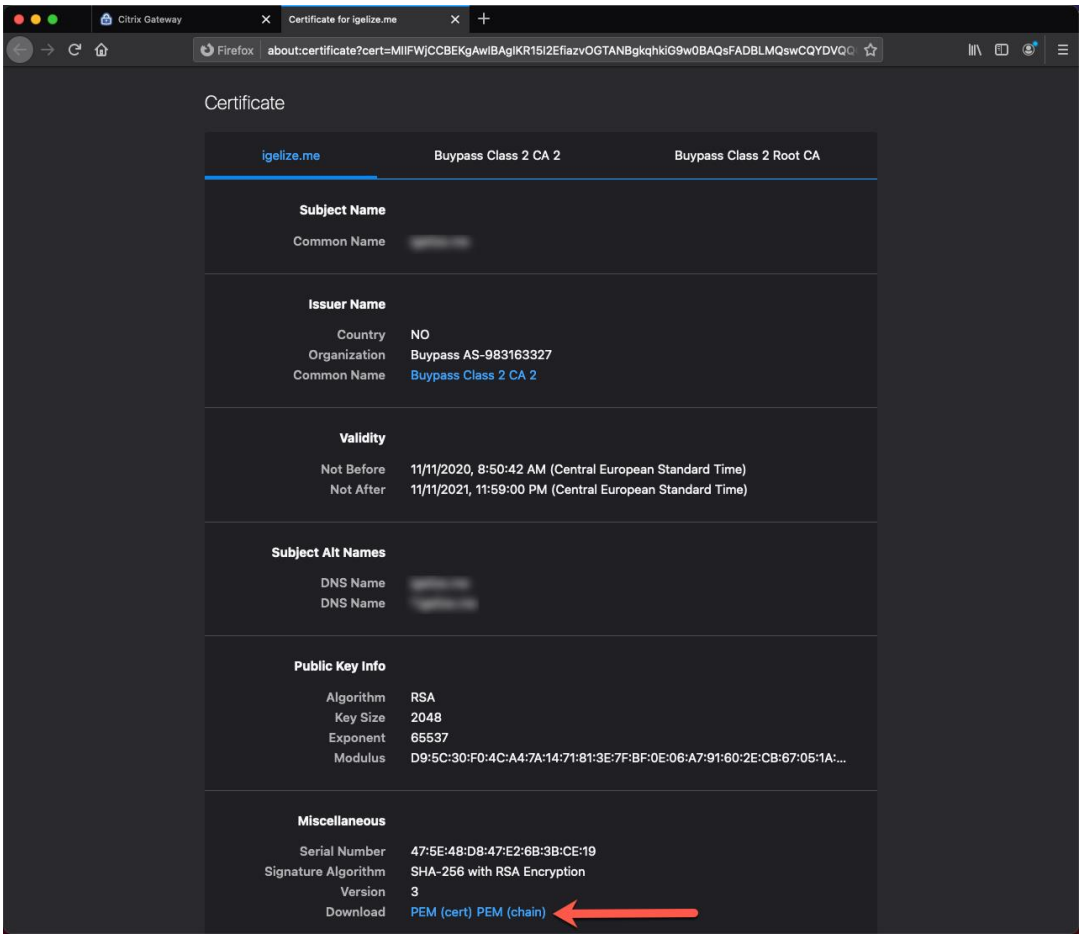
4. Click the **More information** link at the bottom of the dropdown.



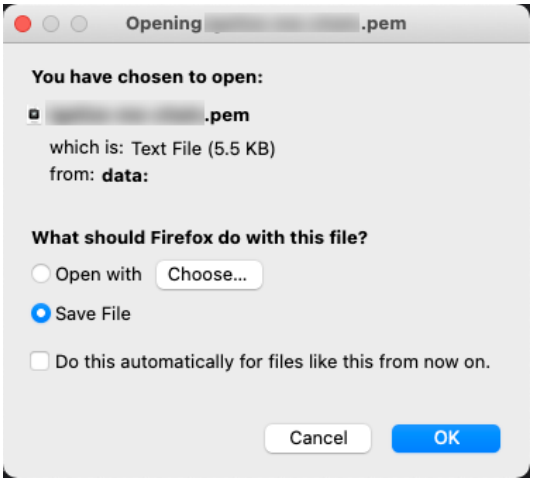
5. The **Page info** screen will open. Depending on the OS you are using, it should look something like the following. Make sure you are on the **Security** page and click the **View Certificate** button.



6. Your browser will open the **Certificate** page. Scroll down the page until you find the download link. Click the **PEM (chain)** link to download the certificate chain.

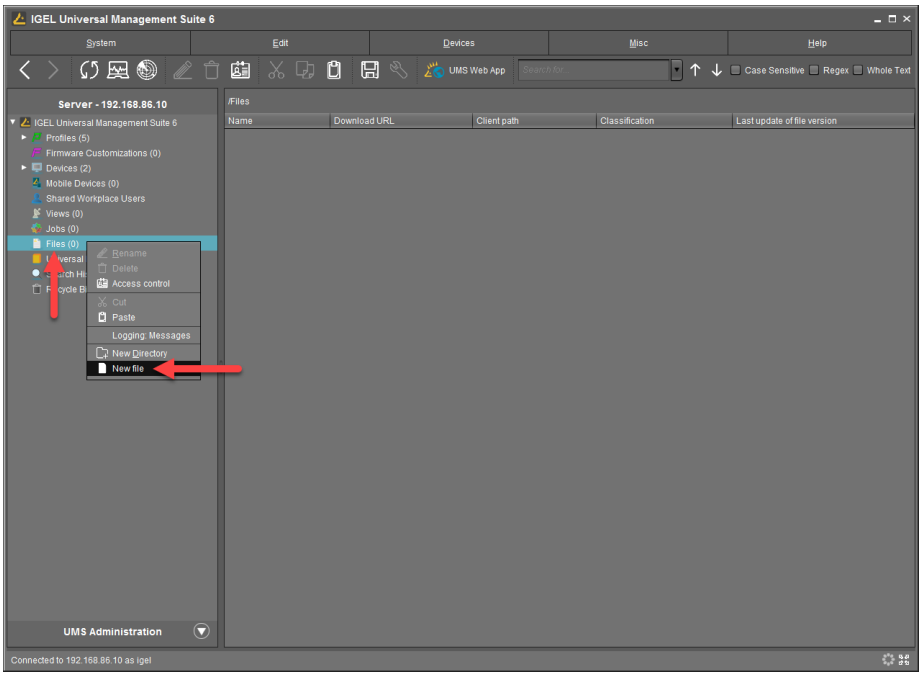


7. You are prompted to save the certificate file. Click to select the **Save File** radio button and click the **Ok** button.

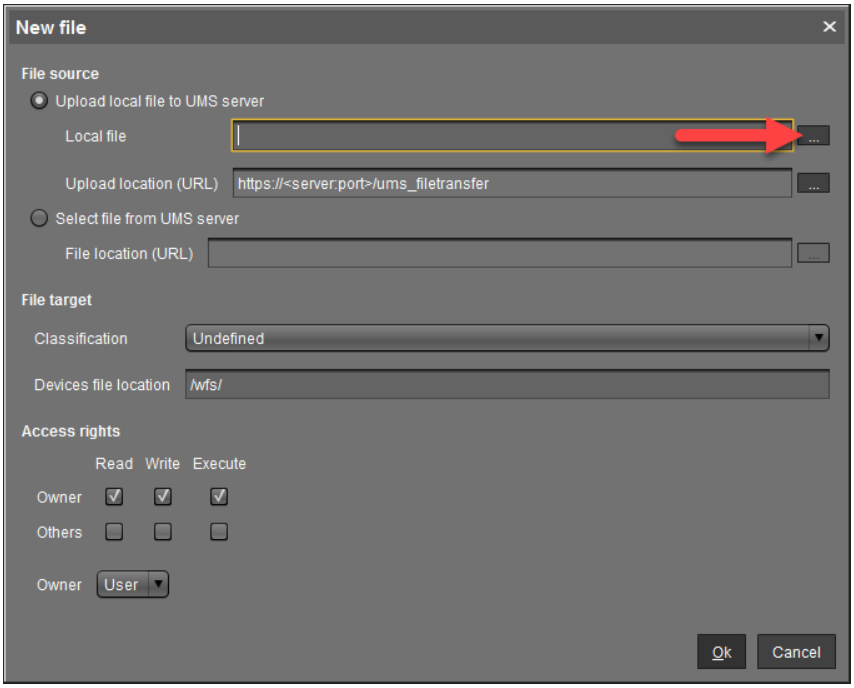


8. Once you have downloaded the certificate chain, open it in a text editor and verify it looks like the following. If not, try the above steps again or contact your Certificate administrator for help.

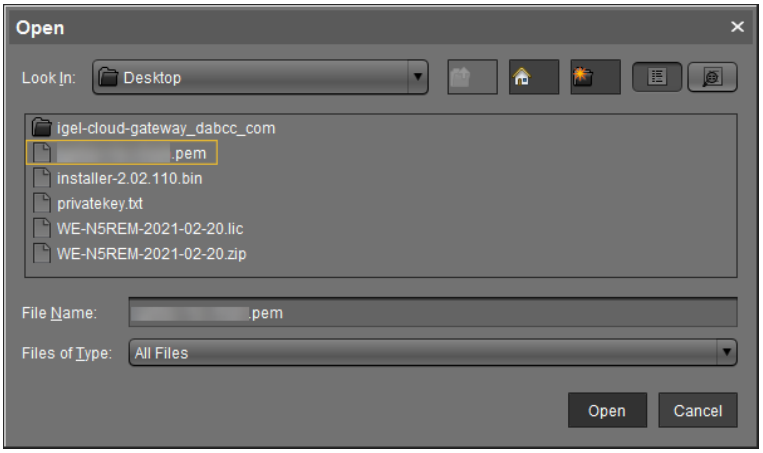
9. The next step is to upload the certificate file to the IGEL UMS. Right-click on the **Files** node in the left menu and click the **New file** link.



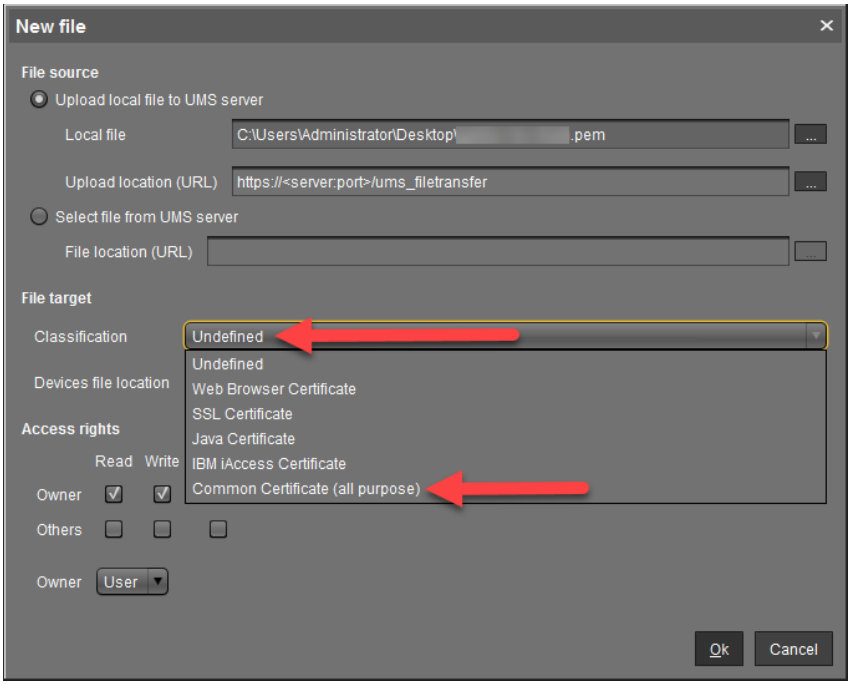
10. Click the **…** icon to the right of the local file text box.



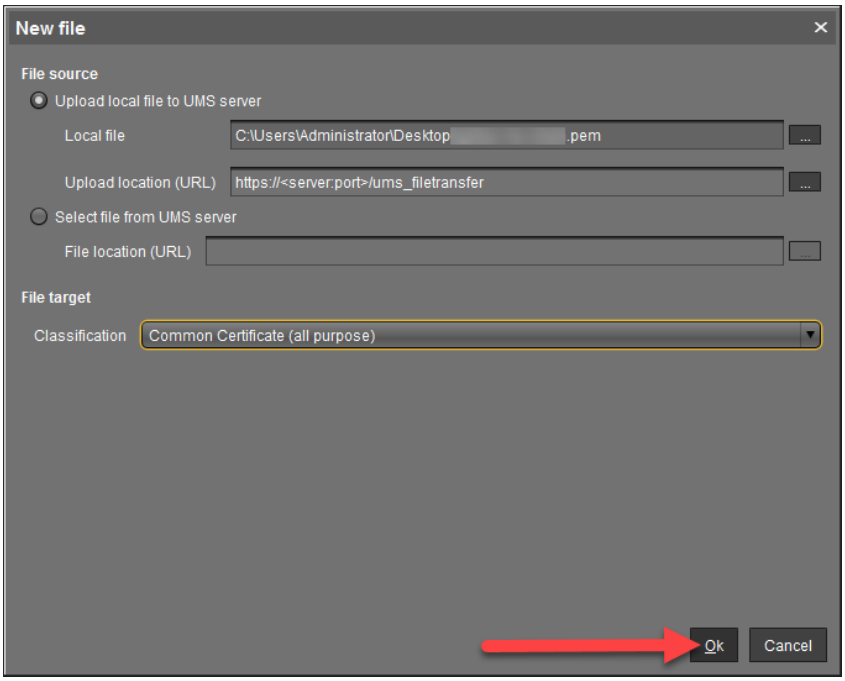
11. The **Open** window opens. Browse to the location you saved the certificate chain .pem file and click to select it. Click the **Open** button to continue.



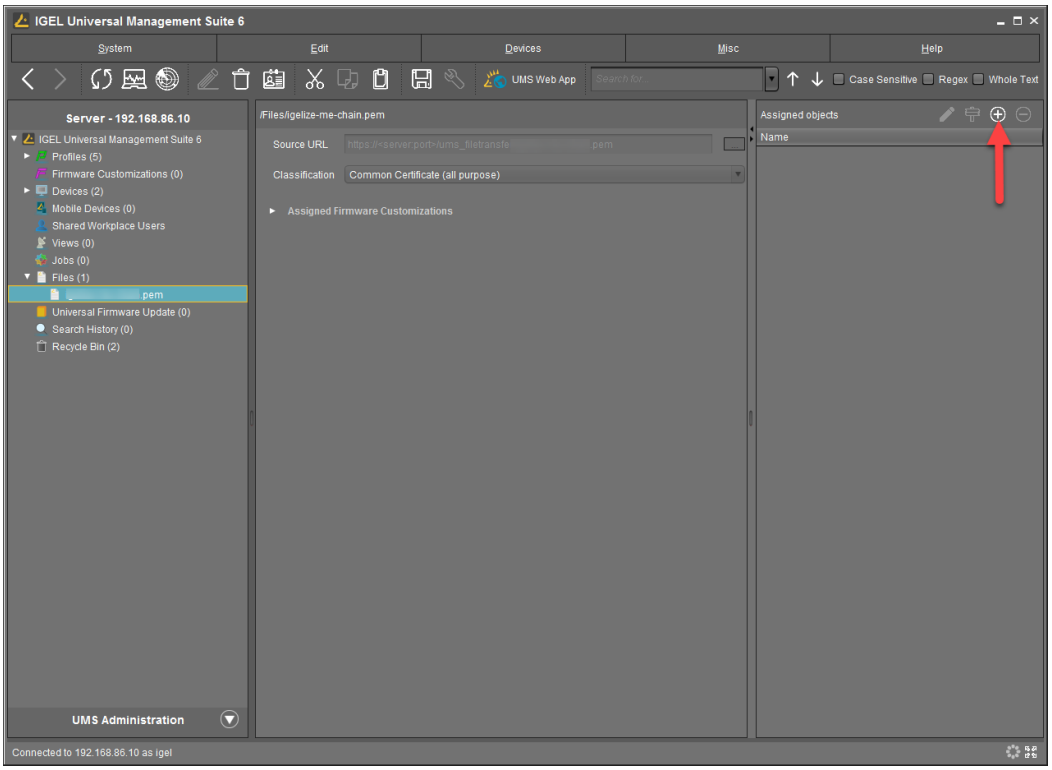
12. Next, you need to tell the IGEL UMS the type of file you are uploading. To do this, click to open the **Classification** combo box and click to select **Common Certificate (all purpose)** located at the bottom of the list.



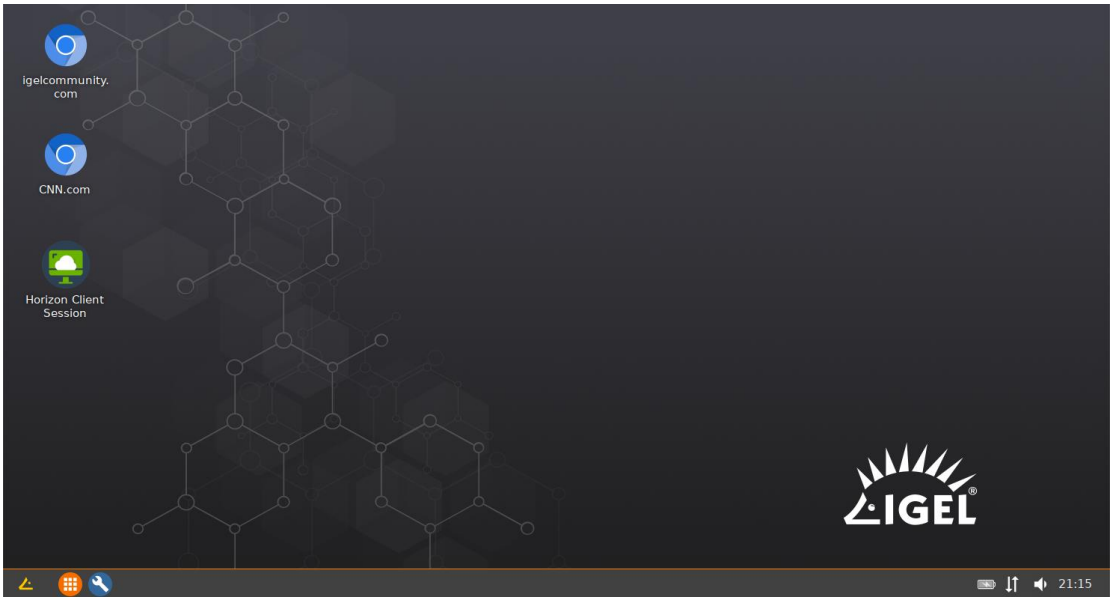
13. Your **New file** window should look like this. If all looks good, click the **Ok** button to upload the certificate to the IGEL UMS.



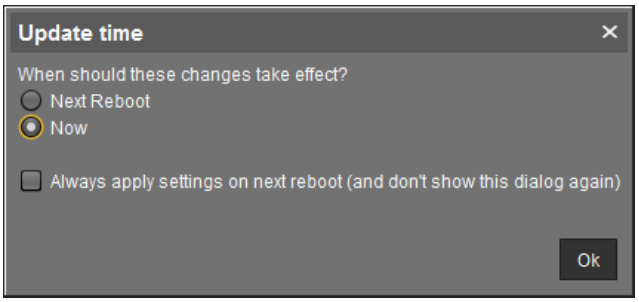
14. The certificate is uploaded, you are ready to assign it to your devices. Click the + button located in the top right of the UMS.



15. The **Select assignable objects** window opens. Please select the desired folders or clients and click the > button to move it to the **Selected objects** section. Once you have defined the objects to assign to the profile, you can click the **Ok** button to save it.



16. You are prompted to specify at what time the new settings will take effect. For this example, click the **Now** radio button and click **Ok** to apply this change in real-time.

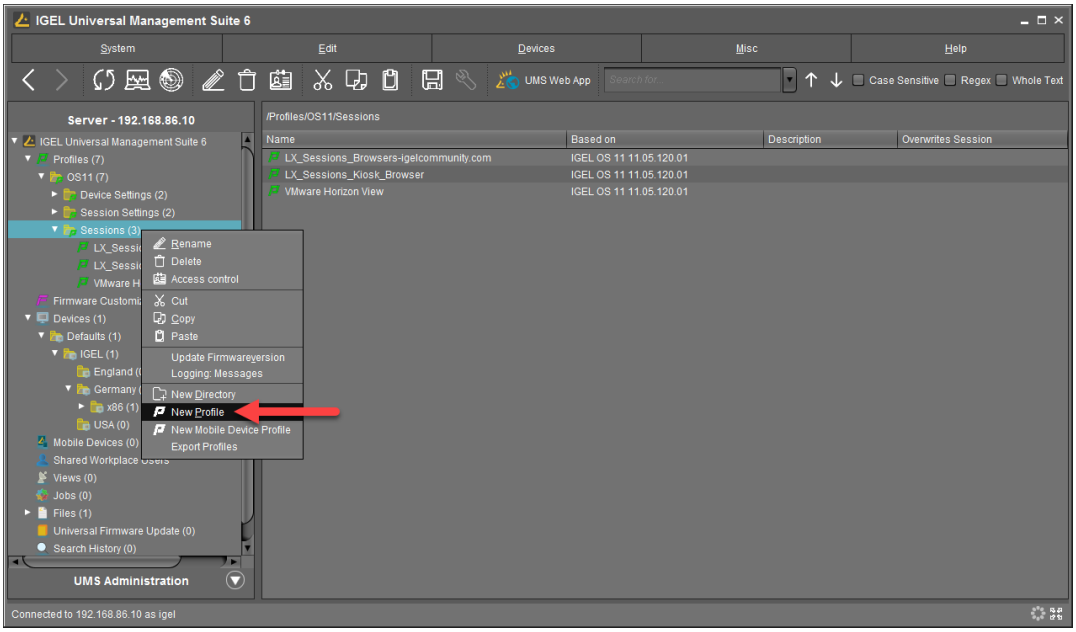


1. 6. How to Configure Citrix Access via Chromium

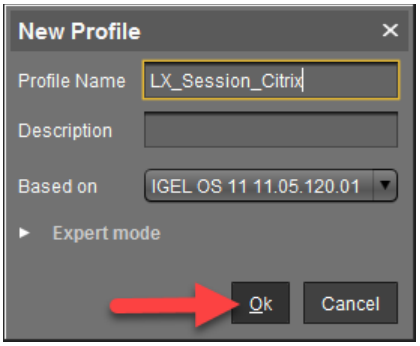
Now that you have learned how to deploy the Chromium browser, it is time to use it to launch Citrix sessions. To do this, the same process you learned above is used. All you need to do is replace the URL to your Citrix StoreFront or Citrix ADC (NetScaler) address.

1. The certificate is uploaded and deployed to the desired IGEL OS devices. You are ready to create a profile to deploy the Chromium browser pointing to your Citrix backend.

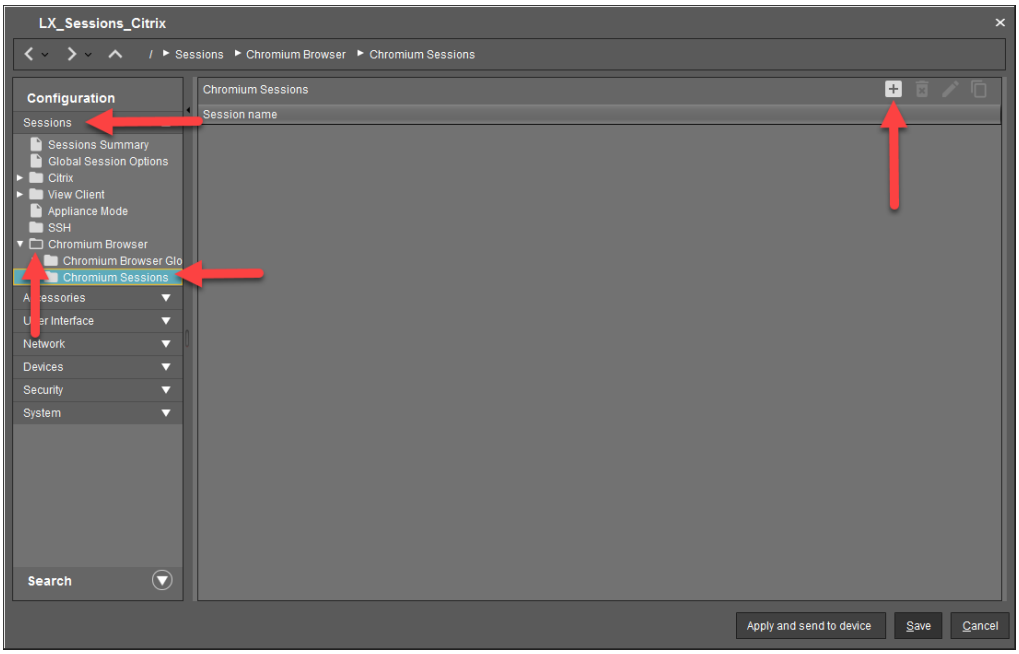
   From the IGEL UMS, expand the **Profiles** node, right-click on the **Sessions** folder, and click the **New Profile** link.



2. Enter a descriptive name for the profile in the **Profile Name** text box. Click to expand the **Based On** combo box and click to select the desired IGEL OS version, for this example, **IGEL OS 11.05.120.01** entry. Once finished, click the **Ok** button to continue.

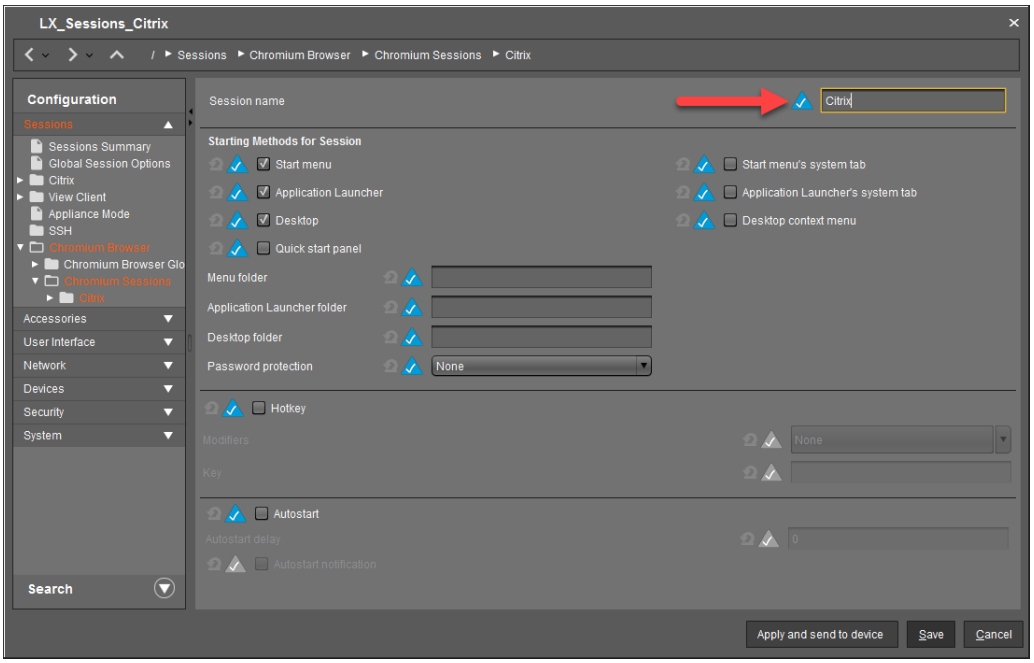


3. Click to expand **Sessions** > **Chromium Browser** and click to select the **Chromium Sessions** link. Click the **+** button located on the top right of the window.

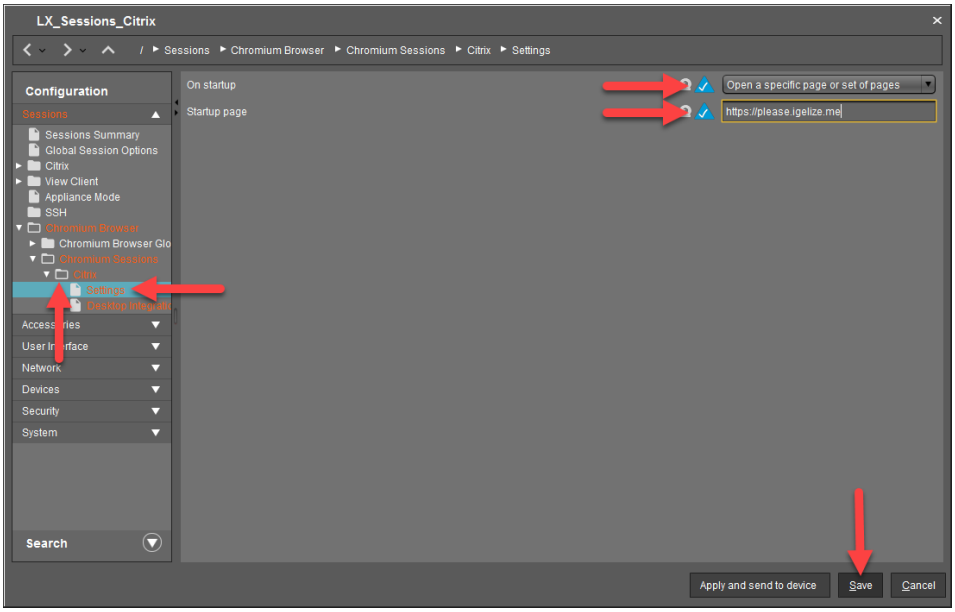


4. The Citrix profile window opens, you can give the session icon a name and select where it will be displayed on the IGEL OS. Enter a friendly name for the Citrix sessions in the **Session name** text box.

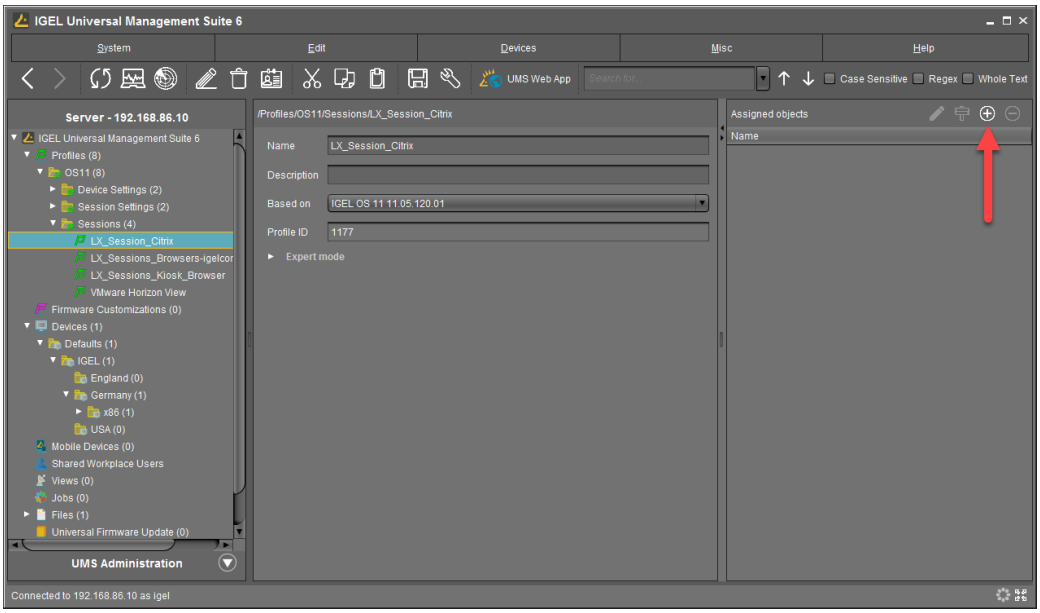
   You can also define where this session will be placed on the IGEL OS, select the desired locations. This is up to you.



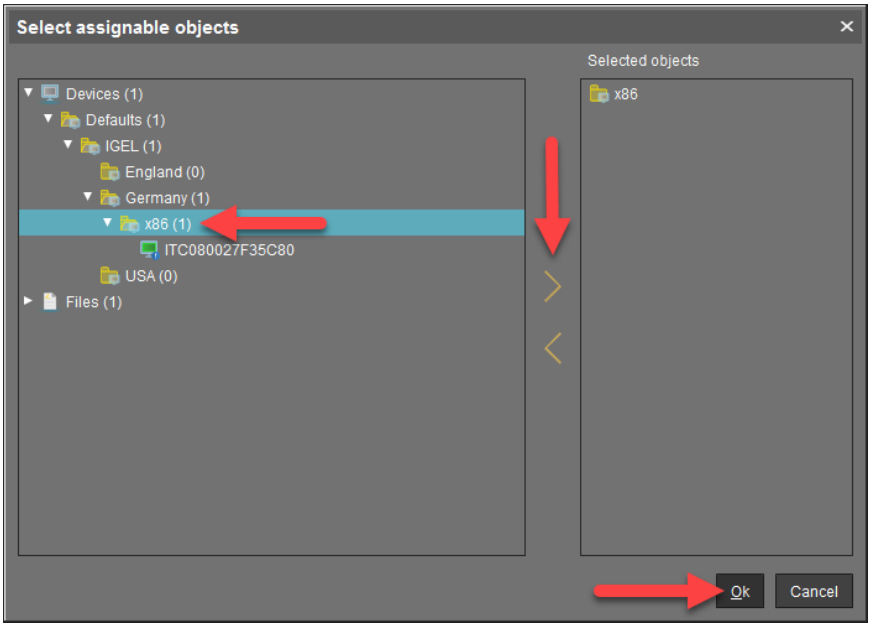
5. Click to **Settings** node below the **Citrix** folder. Here you will define the web page the browser will open upon startup. Click to open the **On startup** combo box and select **Open a specific page or set of pages** item from the list. Next, enter the URL of the Citrix login web page in the **Startup page** text box. Once finished, click the **Save** button.



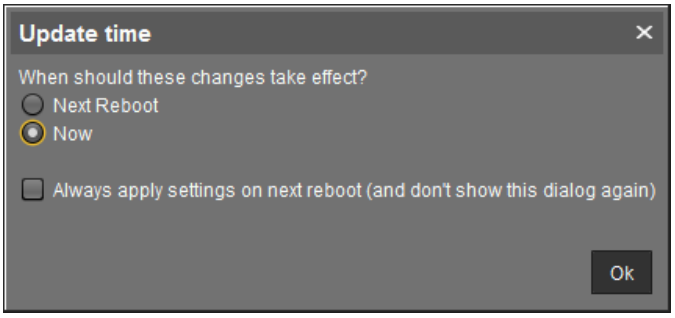
6. The profile is created, and you are ready to assign it to your devices. Click the **+** button located in the top right of the UMS.



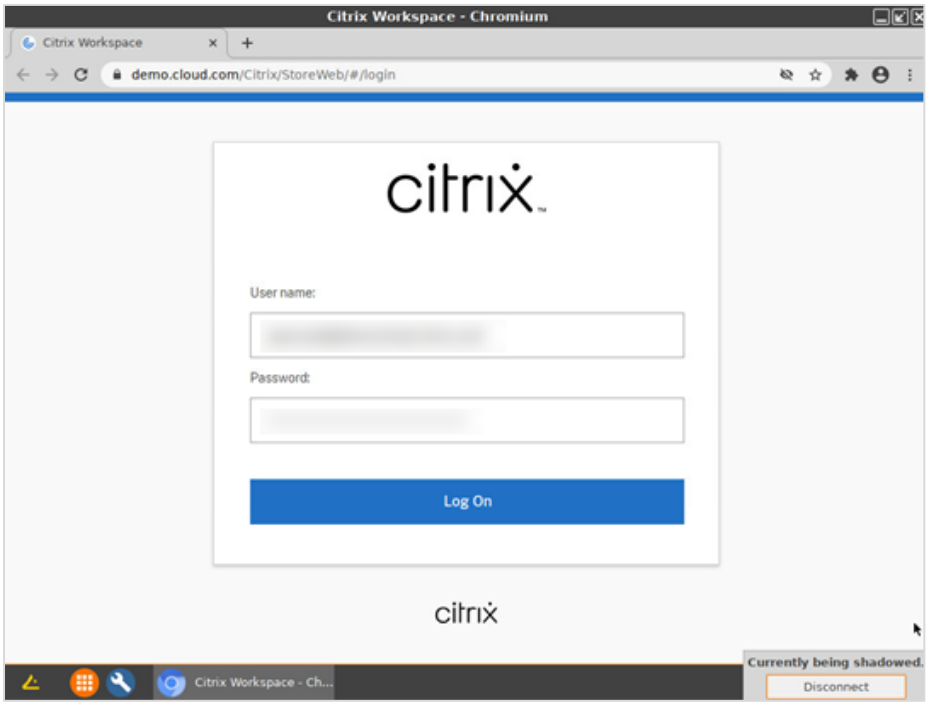
7. The **Select assignable objects** window opens. Please select the desired folders or clients and click the > button to move it to the **Selected objects** section. Once you have defined the objects to assign to the profile, you can click the **Ok** button to save it.



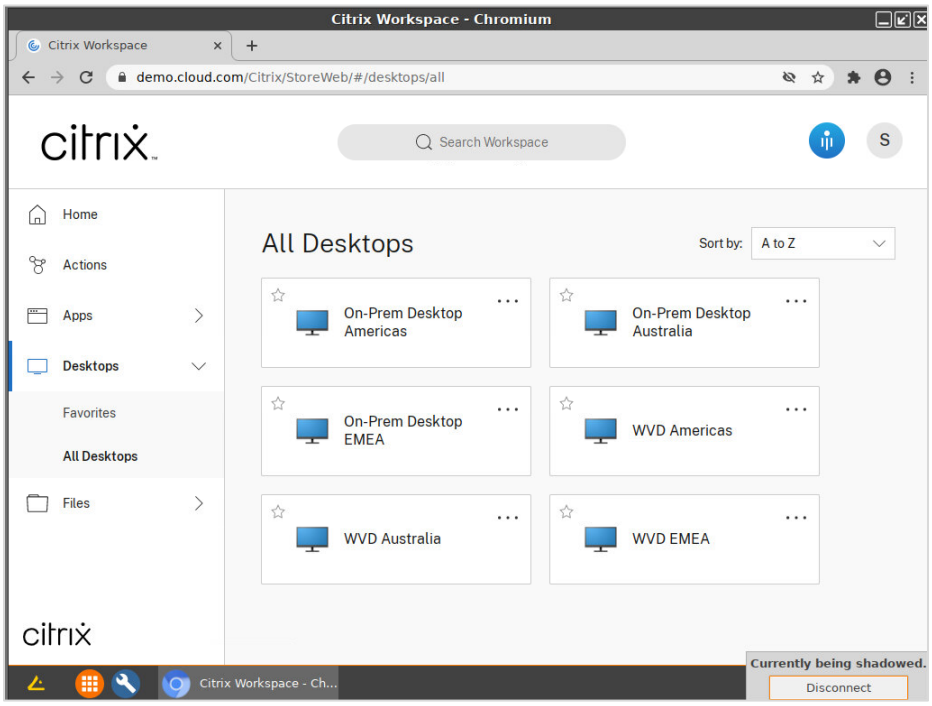
8. You are prompted to specify at what time the new settings will take effect. Select the desired setting and click **Ok** to apply the new settings.



9. You have successfully deployed access to your Citrix environment via the Chromium browser. Your desired users will see a new icon on their desktop. Once double-clicked, the Chromium browser will open to the Citrix login page.



10. Once logged in, you will see a list of resources assigned to the user.

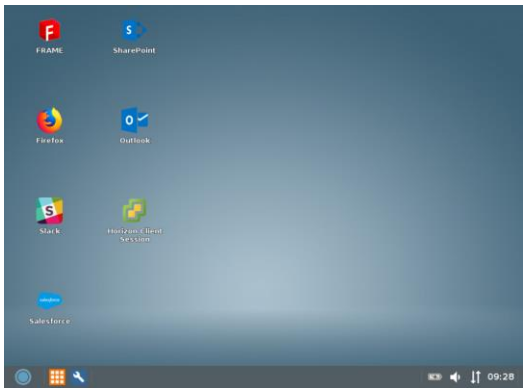


2. Customize the IGEL OS User Interface Guide

Steve Jobs once said that Apple is like a Porsche and that everyone wants to buy and drive a Porsche, but a 10-year-old used Chevy gets you from point A to point B in the same legal amount of time. Design matters.

IGEL agrees! Design does matter, but unlike the unique designs Apple has given us, IGEL believes that beauty is in the eye of the beholder. IT should have the flexibility and control to design their user's experience the way they see fit. With the UMS and IGEL OS, you have that ability, as almost everything a user sees can be customized.

The following is just an example of what can be done, the before and after picture tells the story.



Of course, when using the IGEL OS, you can customize almost every little setting, but that is way too much to try to explain, so we decided to walk you through the basics and then point you toward the other configurations to try on your own. This is just a start. As we said, you can do so much, so have fun, play around, and design something your users will truly love!

This guide is divided into the following eight sections. When finished, you will have learned how to customize, brand, and make a beautiful experience for your users! Even better than Apple!

- How to Customize the Start Button
- How to Customize the Start Menu Icon
- How to Customize the Desktop Wallpaper
- How to Customize the UI Theme Colors
- How to Customize the Screensaver
- How to Customize the Bootsplash Image
- How to Customize Session Icons
- How to Lockdown the IGEL OS

To learn how to customize the IGEL OS, download the 'Customizing IGEL OS User Interface Step-by-Step Guide' at **http://files.igelcommunity.com/Customizing-the-IGEL-OS-UI.zip**.

3. IGEL OS Firmware Updates Guide

IGEL OS updates are available for download on the IGEL website. The IGEL UMS ships with functionality to automate the process of updating IGEL devices. Depending on how your devices connect to the UMS defines how they are updated, you have two possible choices.

Updating IGEL OS devices with a direct connection to the UMS

If your IGEL OS-based devices are on a routable network and can connect directly to the UMS, you can use the **Universal Firmware Update** feature of the UMS.

The following steps details how to update the IGEL OS using the UMS **Universal Firmware Update** feature:

- **How to Update the IGEL OS Firmware via the UMS**
- **How to Deploy Firmware Update**

Updating IGEL OS devices that connect via an IGEL Cloud Gateway (ICG)

If the IGEL OS-based devices you wish to upgrade are connected to the UMS via the IGEL Cloud Gateway (ICG), the standard UMS **Universal Firmware Update** feature does not work. IGEL devices cannot download the firmware file from the UMS file repository. In this case, you are required to deploy the firmware updates in a fashion where the IGEL OS can download the files. To do this, IGEL provides the ability to create a UMS profile that allows the IGEL OS to be configured to download the firmware update via FTP, SFTP, HTTP, HTTPS, or FTPS.

The following steps detail how to update when connecting to the UMS via ICG:

- **Update IGEL OS Firmware via the ICG**
  - **Download IGEL OS Firmware**
  - **Create Firmware Repository**
    - How to Configure AWS S3 as the Firmware Repository
    - How to Configure Citrix ShareFile as the Firmware Repository
    - How to Configure Microsoft IIS FTP as the Firmware Repository
  - **How to Create a Firmware Update Profile**

Continue reading and learn the ins and outs of updating your IGEL OS devices. Download the ‘IGEL OS Firmware Updates Step-by-Step Guide’ at **http://files.igelcommunity.com/IGEL-OS-Firmware-Updates-Guide.zip**.

Appendix

1. IGEL-Getting-Started-Guide.zip Files Explained

The IGEL Step-by-Step Guide ships with a master zip file that contains all the step-by-step guides and along with the resources, artwork, profiles, and firmware customizations found in all the getting started guides. Please download it if you received the PDF only. It is filled with a wealth of goodness!

The following explains the files located in the **IGEL-Getting-Started-Guide.zip** file.

\ IGEL-Getting-Started-Guide.zip Root Folder

Filename	Description
\Customizing the IGEL OS User Interface Guide\	Folder containing the 'Customizing the IGEL OS User Interface' Step-by-Started Guide's PDF along with images, icons, UMS Profiles, and Firmware Configurations referenced in the guide.
\IGEL OS Firmware Updates Guide\	Folder containing the 'IGEL OS Firmware Updates' Step-by-Step Guide's PDF.
\ IGEL Step-by-Step Getting Started Guide.pdf	This file, the IGEL Software Suite Step-by-Step Getting Started Guide's PDF file.

\Customizing the IGEL OS User Interface Guide\ Root Folder

Filename	Description
\Firmware Customizations\	Folder containing the custom firmware customizations found in the 'Customizing the IGEL OS User Interface' Guide.
\Icons\	Folder containing all the icons referenced in the 'Customizing the IGEL OS User Interface' Guide.
\Images\	Folder containing all the images used in the 'Customizing the IGEL OS User Interface' Guide.
\Profiles\	Folder containing all UMS Profiles created in the 'Customizing the IGEL OS User Interface' Guide.
Customizing-IGEL-OS-User-Interface-Guide.pdf	The 'Customizing the IGEL OS User Interface' Step-by-Step Guide's PDF

\Customizing the IGEL OS User Interface Guide\Firmware Customizations\ Folder

Filename	Description
How-to-Customize-the-IGEL-OS-Firmware-Customization.zip	Backup file containing the Custom Firmware Customizations found in the **How to Customize the Start Button**, **How to Customize the Start Menu Icon**, **How to Customize the Desktop Wallpaper**, **How to Customize the Screensaver**, and **How to Customize the Bootsplash Image** sections of the 'How to Customize the IGEL OS User Interface' Step-by-Step Guide.

\Customizing the IGEL OS User Interface Guide\Icons\ Folder

Filename	Description
\icons\adp_icon.png	ADP icon image
\icons\citrix_icon.png	Citrix icon image
\icons\dabcc_icon.png	DABCC.com icon image
\icons\firefox.png	Firefox icon image
\icons\g_suite_icon.png	Google G-Suite icon image
\icons\igel_icon.png	IGEL icon image
\icons\office365-icon.png	Microsoft Office 365 icon image
\icons\onedrive.png	Microsoft OneDrive icon image
\icons\outlook-icon.png	Microsoft Outlook icon image
\icons\salesforce_icon.png	Salesforce icon image
\icons\sap-icon.png	SAP icon image
\icons\servicenow-icon.png	ServiceNOW icon image
\icons\slack_icon.png	Slack icon image
\icons\vmware-horizon-icon.png	VMware Horizon View icon image

\Customizing the IGEL OS User Interface Guide\Profiles\ Folder

Filename	Description
\Profiles\Look-and-Feel-Profile.zip	How to Customize the UI Theme Colors UMS profile archive zip file.
\Profiles\UI-Lockdown-Profile.zip	How to Lockdown the IGEL OS UMS profile archive zip file.

\ Customizing the IGEL OS User Interface Guide\Images\ Folder

Filename	Description
\ images\blue-background.jpg	Blue wallpaper image
\images\IGELCommunity-Bootsplash.png	IGEL Community bootsplash image
\images\IGELCommunity-Logo.png	IGEL Community logo image for the start menu
\images\IGELCommunity-Screensaver.png	IGEL Community logo image for the screensaver
\images\startbutton.png	Start button image

\ IGEL OS Firmware Updates Guide \ Root Folder

Filename	Description
\IGEL-OS-Firmware-Updates-Guide.pdf	The 'IGEL OS Firmware Updates' Step-by-Step Guide's PDF file.

2. Additional Resources

Again, this guide is meant to be a starting point in your journey in IGEL products and solutions. Please refer to the following essential IGEL technical resources to learn more.

Getting Started Guides:

- **IGEL-Getting-Started-Guide.zip**
- **All IGEL Step-by-Step Guides**

IGEL Community:

- **Join IGEL Community on Slack**
- **IGELCommunity.com**
- **IGEL Community Blog**
- **IGEL Community Tech Videos**
- **IGEL Community Message Archives**
- **IGEL Community Videos - Technical How-To Videos**
- **IGEL Community on GitHub**

Web Resources:

- **IGEL Knowledge Base**
- **IGEL OS 11 Manual**
- **IGEL Universal Management Suite (UMS) Manual**
- **IGEL Cloud Gateway (ICG) Manual**
- **IGEL Licensing**
- **Linux Third-Party Hardware Database**
- **IGEL Community HCL**
- **How to Secure Endpoints with IGEL OS White Paper**
- **How to Use a DigiCertificate SSL Certificate with ICG**

3. Last Words

To ‘somewhat’ quote one of my favorite stories, **“You’re off to great places, today is your day, your devices are waiting, so get on your way!”** - Dr. Seuss: Oh, The Places You'll Go!

You are done! You are off and running on a journey that will allow you to quickly deploy, manage and secure the most powerful operating system designed for Citrix, Microsoft, VMware, Server-based Computing, VDI, and DaaS environments today! The possibilities are close to endless. You cannot hurt it, so create more profiles and have some fun with it.

The steps within this guide provided you with the very basics to kick-start your IGEL lab environment. To learn more, please visit the resources linked to within this guide to dive deeper into a technology or configuration. If you have additional questions, please join the **IGEL Community** and use the “power of the people” to learn, interact, and grow. I cannot recommend it enough.

The **IGEL Knowledgebase** has you covered with a lengthy library of manuals, tips & tricks, support articles, and much more. The search engine is fantastic too. The KB is your friend!

Additionally, please check out the IGEL Community blog for important white papers, web resources, how-to tips, webinars, podcasts, and other great resources recommended and/or requested within the IGEL Community. It’s a helpful list of resources, and I feel you will find it useful.

Lastly, I thank you for taking the first step into the software-defined world of IGEL. The IGEL Software Suite is one fantastic piece of software, designed and developed by a fantastic group of people! You will genuinely enjoy it, and your users will too!

Thank you very much,

Douglas Brown & The IGEL Community Team!

A Splendid Time is Guaranteed for All!