



IGEL SOFTWARE PLATFORM

STEP-BY-STEP GETTING STARTED GUIDE



This page is blank on purpose.

NOTICE

Copyright

International copyright laws protect this publication. All rights reserved. With the exception of documentation kept by the purchaser for backup purposes, no part of this manual – including the products and software described in it – may be reproduced, manipulated, transmitted, transcribed, copied, stored in a data retrieval system or translated in any form or by any means without the express written permission of IGEL Technology GmbH.

Copyright © 2017-2018 IGEL Technology GmbH. All rights reserved.

Trademarks

IGEL is a registered trademark of IGEL Technology GmbH.

Any other names or products mentioned in this manual may be registered trademarks of the associated companies or protected by copyright through these companies. They are mentioned solely for explanatory or identification purposes and to the advantage of the owner.

Disclaimer

The specifications and information contained in this manual are intended for information use only, are subject to change at any time without notice and should not be construed as constituting a commitment or obligation on the part of IGEL Technology GmbH. IGEL Technology GmbH assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual, including any pertaining to the products and software described in it. IGEL Technology GmbH makes no representations or warranties with respect to the contents thereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose.

IGEL Endpoint Management. 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 it!

Authors

This document is a labor of love by the IGEL Community. The following fine folks put fingers to keyboard to make this resource a reality. This project would not be possible if not for the help of the following fabulous folks.

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

The Experts:

Christian Drieling - drieling@igel.com

Fredrik Brattstig - Brattstig@igel.com

Sébastien Pérusat - perusat@igel.com

Timco Hazelaar - t.hazelaar@thipc.com

Christian Drieling & Fredrik Brattstig - #1 thanks must be given to Fredrik and Christian as this document 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 true ROCK STARS. Thank you both so very much!

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

Timco Hazelaar – One of the harder items to document is SSL, but not for Timco. Without being told, he took it upon himself to help by contributing the ‘**How to Use a DigiCertificate SSL Certificate with ICG**’ section of this document. Much 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.

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 a lot of designers, but I’ve never worked with one I’ve appreciated and respected as much as Abie! Truly one of the best!

Very 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!

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

Thomas Poppelgaard

Guido Jakobs

Benjamin Crill

Mattias Jacobsson

Henk-Jan Eiten

Sébastien Pérusat

Andrew Wood

Rob Beekmans

Dieter Boonen

Douglas DeCamp

Ian Anderson

Chris Calaf

Fredrik Brattstig

René Bigler

Christian Drieling

Timco Hazelaar

Gamal Attia

Carl Behrent

Falk Heiland

Daniel Ugarte

Martijn van Tricht

Abigail Arcilla

If you are interested in seeing your name in lights, or more appropriately, helping your fellow techie by contributing to this resource, please contact us! After all, **together we are better!**

Changelog

This project is a work in progress. Below is the list of changes added in each version:

Date	Version	Description of Changes
12/7/2017	1.0 Public Draft 1	<ul style="list-style-type: none"> First public draft version, includes IGEL OS and UMS.
1/11/2018	1.0 Public Draft 2	<ul style="list-style-type: none"> Added ICG section Fixed misc. grammar and spelling issues Added misc. feedback from IGEL community members
1/29/2018	1.0	<ul style="list-style-type: none"> Added 'How to Use a DigiCertificate SSL Certificate with ICG' section. Contributed by Timco Hazelaar Fixed misc. grammar and spelling issues Added final misc. feedback from community members Finalized look and feel of the document
4/24/2018	1.5	<ul style="list-style-type: none"> New cover artwork from the amazing 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	<ul style="list-style-type: none"> Updated eDocs links to point to new kb.igel.com.

Roadmap!

The following items are currently scheduled to be added to future versions of this project. If you would like to make a recommendation for this list or are interested in contributing, please contact us at igelcommunity@igel.com.

- How to install the UMS on Linux
- How to install the ICG Virtual Appliance
- How to install the ICG on Linux
- How to backup and restore the UMS
- How to upgrade the UMS and ICG
- How to install and configure Virtual Box for use as an IGEL demo lab
- How to install and configure deviceTRUST with the IGEL Platform.
- Enhance the Configuration and Management section.

Table of Contents

INTRODUCTION.....	10
1. Project Overview	11
2. Introduction to the IGEL Software Platform	12
INSTALLATION.....	16
1. Infrastructure Considerations.....	17
2. Download IGEL Software	19
3. Install IGEL Universal Management Suite (UMS)	22
3.1. UMS System Requirements	23
3.2. How to Install the IGEL UMS	24
3.3. How to Open Firewall Ports Required by UMS	33
3.4. How to Install the UMS Console on Remote PC	34
4. Install IGEL Cloud Gateway (ICG)	37
4.1. ICG System Requirements	39
4.2. How to Create an AWS Instance for ICG	40
4.3. How to Open Firewall Ports Required by ICG	51
4.4. Create Required DNS Records.....	54
4.5. Download IGEL Cloud Gateway Software.....	55
4.6. How to Create an SSL Certificate for ICG	58
4.7. How to Add Certificates to UMS.....	66
4.8. How to Install the IGEL ICG Software.....	76
4.9. How to License the IGEL ICG.....	86

5.	Install IGEL OS Universal Desktop Converter (UDC)	98
5. 1.	UDC 3 System Requirements	99
5. 2.	How to Create a Bootable USB Drive	100
5. 3.	How to Install the UDC.....	103
5. 4.	How to Find IGEL OSes	112
5. 5.	How to License the IGEL OS UDC	117

CONFIGURATION & MAINTENANCE..... 128

1.	UMS Profiles Overview.....	129
1. 1.	How to Create a Basic Folder Structure	130
1. 2.	How to Create Basic UMS Profiles	134
2.	Customize the IGEL OS Look and Feel	144
2. 1.	How to Customize the Start Button	146
2. 2.	How to Customize the Start Menu Icon	152
2. 3.	How to Customize the Desktop Wallpaper	158
2. 4.	How to Customize UI Theme Colors	164
2. 5.	How to Customize the Screensaver.....	176
2. 6.	How to Customize the Bootsplash Image	182
2. 7.	How to Customize Session Icons	187
2. 8.	How to Lockdown the IGEL OS.....	197
3.	IGEL OS Firmware Updates.....	205
3. 1.	IGEL OS Firmware Versions Explained.....	206
3. 2.	Update IGEL OS Firmware via the UMS	208
3. 3.	Update IGEL OS Firmware via the ICG	219
3. 3. 1	Download IGEL OS Firmware	220
3. 3. 2	Create Firmware Repository	223
3. 3. 3	How to Create a Firmware Update Profile	250

3. 4.	How to Deploy a Firmware Update	258
3. 4. 1	How to Manual Deploy from UMS	259
3. 4. 2	How to Automate Updates on Shutdown.....	261
3. 4. 3	How to Schedule Updates using Jobs & Views.....	263
3. 5.	How to Update Existing Profiles.....	275
APPENDIX.....		278
1.	How to Use a DigiCertificate SSL Certificate with ICG	279
2.	How to Import Project Customizations.....	286
3.	IGEL-Getting-Started-Guide.zip Files Explained	296
4.	Additional Resources	298
5.	Last Words	300

Introduction

1. Project Overview

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

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

When finished, you will have a fully working IGEL End-Point Management Platform consisting of the IGEL Universal Management Suite (UMS), IGEL Cloud Gateway (ICG) and at least one IGEL OS installed, connected and centrally managed! That sounds great to me!

All this, screen-shot by screen-shot. No more guesswork!

If you are reading the printed version of this document, we recommend you also download the PDF version so to take advantage of all the links found in this resource.

This project is a work in progress. Thanks to so many incredible contributions and due to the changing face of software-defined, this document will grow. To stay up to date with what’s new with this project and what’s technically new at IGEL, please join the IGEL Community and our very active [Slack](#) group.

If you have questions and would like to contribute, please email me directly. I would love to hear from you!

It is that easy. Thanks for downloading and on with the show.

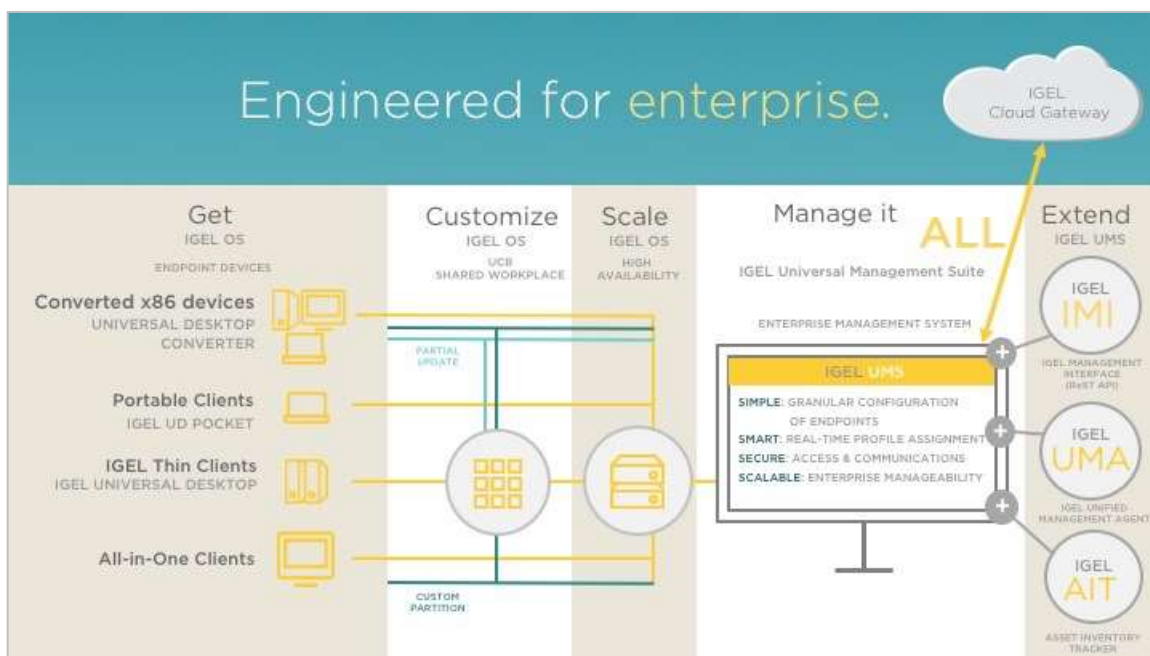


Douglas A. Brown
Global Technology Evangelist
brown@igel.com



2. Introduction to the IGEL Software Platform

The IGEL Software Suite is a platform that consists of three core components, the IGEL OS, Universal Management Suite (UMS) and the optional IGEL Cloud Gateway (ICG). Each component works together to allow you to efficiently manage, deploy, and maintain secure end-points anywhere, at any time.



IGEL OS

The genius behind the IGEL solution is the IGEL client operating system. No matter the client hardware, unless you are running Windows Embedded or Windows IoT, you are running the same version of IGEL OS. It does not matter if the device is as small as a UD Pocket USB thumb drive or a big Quad-Core IGEL UD 7 thin client. The power is in the software.

IGEL delivers its software as firmware for the different hardware solutions and as a stand-alone operating system that can run on any x86 machine, with minimal resources. The IGEL OS is installed physically on the device, as like any other operating system, or you can boot it from a USB drive when using the IGEL UD Pocket.

The IGEL OS is delivered in the following versions to allow you the ultimate flexibility, all packed with the same operating system. The only difference is how the OS is installed on the device.

- **IGEL OS - Universal Desktop Converter (UDC)** – The UDC is designed to convert any existing x86 device to a fully managed, secure end-point running the IGEL OS. However, don't let the name fool you, the UDC is not like any other device conversion tool as it installs the full version of the IGEL OS. It is the same OS you find on any other IGEL client. The UDC is installed on the device's local hard drive and overwrites the existing OS. It is a great way to extend the life of your current hardware by adding the power of a fully managed secure end-point, without buying new.

The UDC is the version of the IGEL OS you download to install IGEL in a virtual machine environment, which works great for testing and lab scenarios.

- **IGEL OS - UD Pocket (UDP)** – The IGEL UD Pocket is designed to bring the full power of the IGEL OS to any x86 64-bit device. It allows a user to plug the UD Pocket into a device's USB port, turn the machine on, boot to the IGEL OS and login to do their work as defined by IT!

The IGEL UD Pocket does NOT interfere with the original OS currently installed on the device. Thus, making it a perfect solution for BYOD and much more. Of course, one of the benefits of the UD Pocket is to temporarily convert a fat client into a secure and managed endpoint device running the IGEL OS and changing it back by merely removing the UD Pocket and rebooting the machine.

- **IGEL OS preinstalled on IGEL Hardware** – Pre-installed on best-of-breed **IGEL thin-client hardware**.
- **IGEL OS Installed on leading 3rd party manufactures** – Leading vendors, such as Samsung, use the best of breed IGEL OS on their devices to provide their customers with the best user experience. Currently, Samsung is running the IGEL Platform on their All-in-One devices.)

IGEL Universal Management Suite (UMS) Server

The brains behind the genius of the IGEL OS is the IGEL Universal Management Suite server (UMS), and its job is to allow IT to manage all the IGEL OSes and supported operating systems easily. For example, Microsoft Windows Embedded, Windows IoT and even Microsoft Windows with a UMS add-on called **Unified Management Agent (UMA)**.

The UMS allows 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 environment with over 7,000 possible configurations. While scripting is not required, it is still possible with firmware customizations or through the **IGEL IMI software** add-on.

The UMS is scalable! For example, IGEL has a case study customer with over 30,000 devices in over 5,000 global locations. Two people manage all this, and they do not even log in to the UMS but once or twice a month. That is what I call scalable!

IGEL does not stop there. I am only touching on the tip of the iceberg. The UMS is also extendible with such technologies as the **IGEL Cloud Gateway (ICG)**, **IGEL Management Interface (IMI)**, and **IGEL Unified Management Agent (UMA)** as discussed above.

IGEL Cloud Gateway (ICG) - (Optional)

The IGEL Cloud Gateway (ICG) is an optional component designed to allow the IGEL OS to communicate from anywhere and anytime securely, without the requirement of a VPN. The ICG is NOT required but adds considerable benefits to IT when utilizing remote IGEL OSes. For example, the IGEL UD Pocket.

Before we get too far into the ICG, I must say, trying to document such a product is complicated. There is a lot to be discussed around design, security, etc. My goal for this document and hence the ICG section itself is to give you the tools to do a basic installation of the suite, not to master every possible configuration.

To document the ‘How to Install the ICG’ section, I kept this as the goal and used an Amazon EC2 Free Tier Instance to host the ICG software. You are not limited to AWS but can install ICG in a cloud instance or on-prem. ICG is delivered as an installable Linux application and a pre-configured virtual appliance. It is up to you! The ICG is very flexible.

For a complete walkthrough of setting up an ICG deployment, please refer to the **ICG documentation eDocs home** page and the **Best Practice Installing and Configuring the IGEL Cloud Gateway** resources.

This page is blank on purpose.

Installation

1. Infrastructure Considerations

Let's get started, the goal of this document is to allow you to setup the IGEL Software Suite in your lab or for a simple proof-of-concept. For this purpose, you are not required to worry about high availability, 3rd party databases, etc. We will discuss the basics and link you to learn more.

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

- One physical, cloud instance or virtual server to host the IGEL UMS software.
- An AWS account and ability to create a free tier Linux server instance to host the IGEL Cloud Gateway software (optional)
- x86 64-bit device to convert using the IGEL OS UDC. For a lab environment, you can install the UDC in a virtual machine, no physical device required.

IGEL provides excellent and very detailed documentation and support articles at <https://kb.igel.com>. This document 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 Virtual Box or VMware Workstation virtual environment. For my lab, I have installed the UMS in a Virtual Box virtual machine, and my 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 from outside your physical network. It acts as the secure broker to allow the UMS to connect with the IGEL OS, without the requirement of using a VPN. Thus, by installing the ICG, you can thoroughly test the IGEL solution and roam throughout the world with your UD Pocket and any IGEL OS based device.

If you do not already have a UD Pocket to play with, please join the www.igelcommunity.com and message me. One just might find its way to your door.

To successfully install the IGEL software platform, you are required to perform the following high-level steps:

- Download IGEL Software
- Install IGEL Universal Management Suite (UMS)
- Open Firewall Ports Required by UMS
- Create an AWS Instance for ICG
- Open Firewall Ports Required by ICG
- Create Required DNS Records
- Create and install an SSL Certificate to ICG
- Install the IGEL ICG Software
- License the IGEL ICG
- Install IGEL OS Universal Desktop Converter (UDC)
- Add IGEL Devices to the UMS
- License the IGEL OS UDC
- Create Basic Folder Structure
- Create Basic UMS Profiles
- Configure Custom Desktop Wallpaper

2. Download IGEL Software

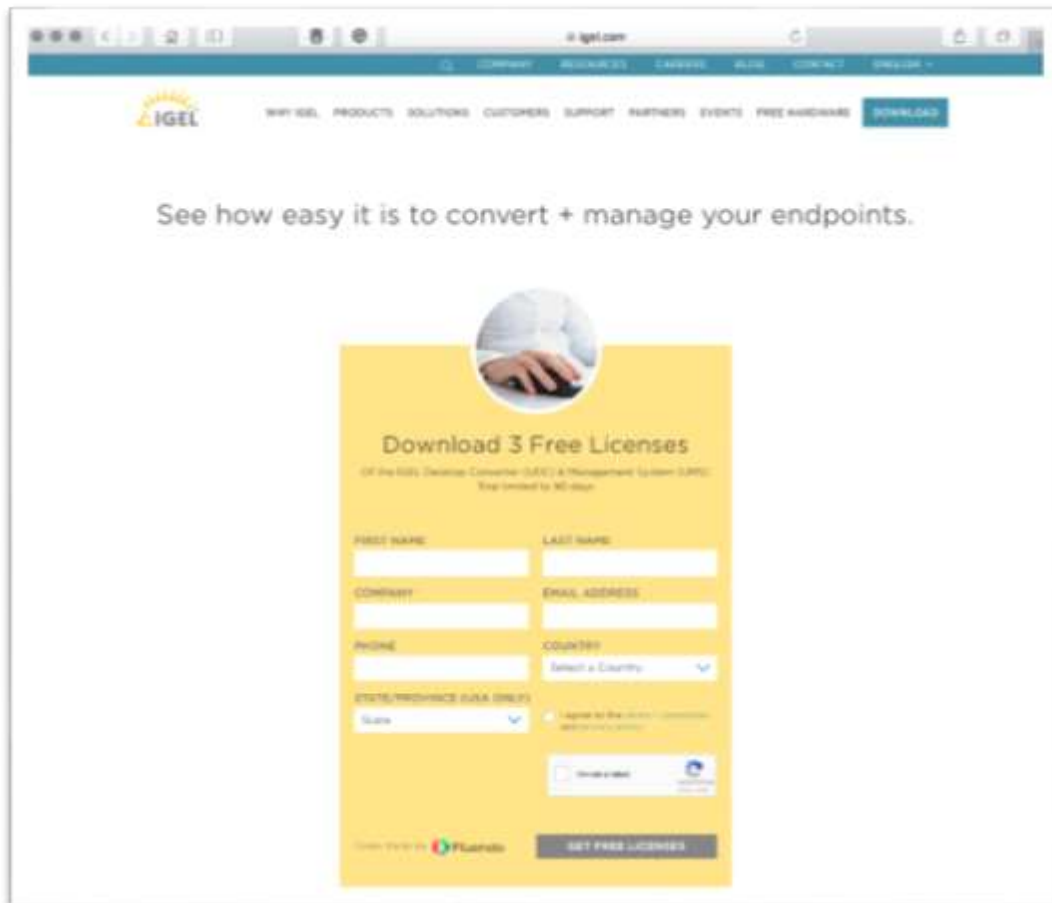
The first step is to get your hands on the latest IGEL software and a license. No worries, IGEL makes this easy. For your testing enjoyment, IGEL provides you with three free licenses for the IGEL OS and the Universal Management Suite (UMS).

The following steps walk you through downloading the IGEL Software Platform, consisting of the IGEL OS, UMS, and 3 FREE licenses:

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

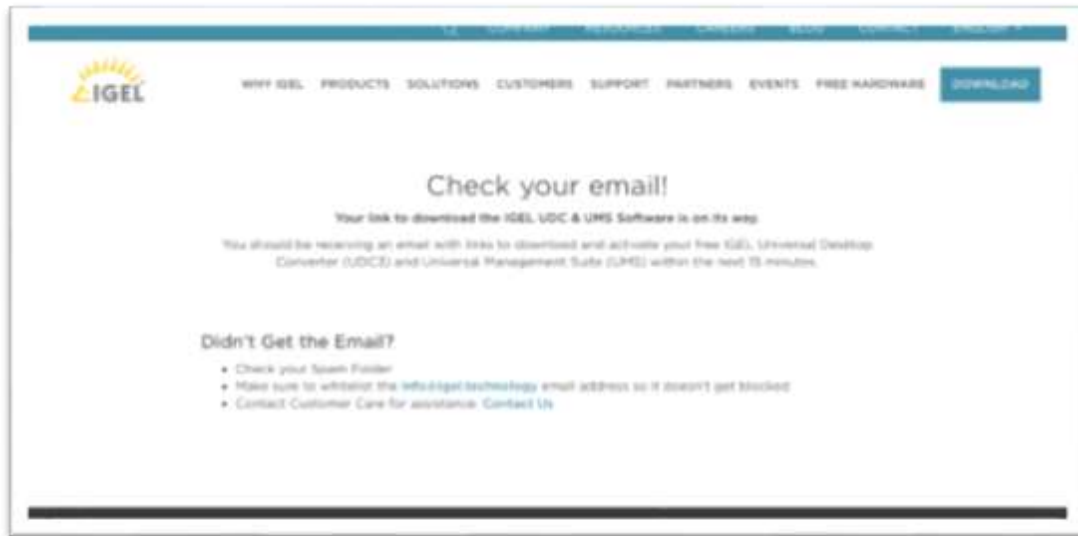
1. Open your favorite browser and browse to <https://www.igel.com/download/>.
2. You are brought to the **IGEL 3 Free Licenses** download page. Fill out the required text boxes, click to check the **I agree to the terms + conditions and privacy policy** check box, click the **I'm not a robot** checkbox and comply with the captcha question(s).

Once finished, click the **Get Free Licenses** button.

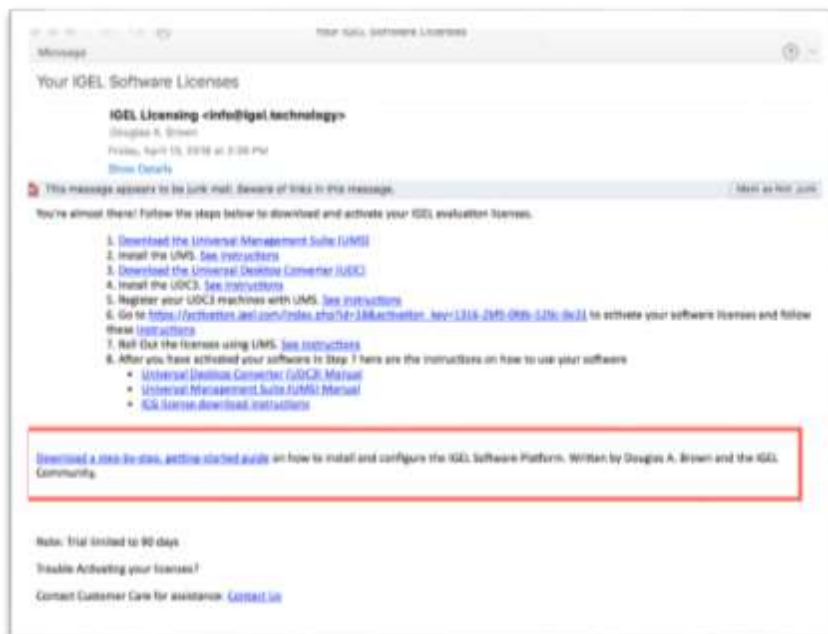
The image is a screenshot of a web browser displaying the IGEL website's 'Download 3 Free Licenses' page. The browser's address bar shows 'www.igel.com'. The website's header includes the IGEL logo and navigation links: 'COMPANY', 'RESOURCES', 'CASES', 'BLOG', 'CONTACT', and 'SPEAKER'. Below the header, a secondary navigation bar lists 'WHY ISEL', 'PRODUCTS', 'SOLUTIONS', 'CUSTOMERS', 'SUPPORT', 'PARTNERS', 'EVENTS', 'FREE HARDWARE', and a 'DOWNLOAD' button. The main content area features the headline 'See how easy it is to convert + manage your endpoints.' followed by a circular image of a hand. Below this is a yellow box titled 'Download 3 Free Licenses' with the subtitle '(Of the IGEL Desktop Converter (IGEL) & Management System (UMS))' and a note 'This limited to 30 days'. The form contains several input fields: 'FIRST NAME', 'LAST NAME', 'COMPANY', 'EMAIL ADDRESS', 'PHONE', and 'COUNTRY' (a dropdown menu). There is also a 'STATE/PROVINCE/CITY/COUNTRY' dropdown menu. At the bottom of the form, there is a checkbox for 'I agree to the terms + conditions and privacy policy' and a 'GET FREE LICENSES' button. The footer of the page includes the IGEL logo and the text 'GET FREE LICENSES'.

- After completing the signup process, 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.



- 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 the process as pleasant and straightforward as eating pie! After all, who does not love a piece of pie?



5. In the above email, there are two links you should concern yourself with:

- **IGEL UMS** - Click the **Download the Universal Management Suite (UMS)** link in the email above to download the IGEL UMS Windows installer package. As discussed, the IGEL UMS is the brains of the operation. You are installing it shortly.
- **IGEL UDC** - Click the **Download the Universal Desktop Converter (UDC)** link in the email above. The IGEL UDC download provides the IGEL OS ISO image that is used to install the IGEL OS into a virtual machine and onto a USB thumb drive that is used to convert an existing/new x86 based PC into a fully managed IGEL endpoint.

Great, you are ready to install the IGEL Universal Management Suite (UMS).

Let's get going! The fun is just getting started!

3. Install IGEL Universal Management Suite (UMS)

The first thing you need to do is install the IGEL Universal Management Suite (UMS). The IGEL UMS is a server application that is installed on either Linux or Windows.

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

UMS on Linux

In the following document, we have documented how to install the UMS on Windows. Although you are not limited to Windows, you can install the UMS on Linux.

The following IGEL eDocs article details the system requirements for installing the UMS on Linux <https://kb.igel.com/endpointmgmt/en/ums-installation-on-64-bit-systems-910970.html>.

Learn more:

- [IGEL Universal Management Suite Manual](#)
- [IGEL Universal Management Suite KB support homepage](#)

The process of installing the IGEL UMS is broken down into the following four sections:

- UMS System Requirements
- How to Install the IGEL UMS
- How to Open Firewall Ports Required by UMS
- How to Install the UMS Console on Remote PC

3. 1. UMS System Requirements

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

- IGEL UMS supports physical, virtual, and cloud instances running Microsoft Windows or Linux (x86 and x86_64).
- Minimum 1 GB RAM free memory (2 GB highly recommended)
- Minimum 1 GB free storage space (by default, your database is installed on the server running the UMS. Storage requirements vary depending on the size of the UMS database, 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 reachable via a routed network you are required to use the IGEL Cloud Gateway.

Learn more at <https://kb.igel.com/endpointmgmt/en/installation-requirements-910311.html>

No matter the size of deployment, 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 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 device 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/en/creating-a-backup-910837.html>.

3. 2. How to Install the IGEL UMS

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

1. First, you need to configure the network to allow the client devices to find the IGEL UMS without user interaction automatically. When an IGEL OS device boots it attempts to establish a connection with a UMS server. The client looks for the UMS server by the DNS 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>"

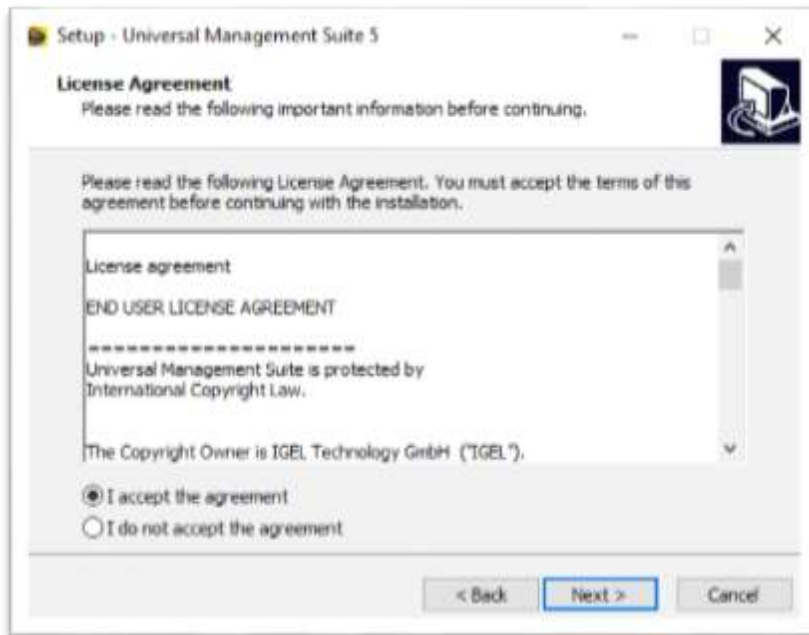
The above step is not required, although highly recommended. Learn more at <https://kb.igel.com/endpointmgmt/en/ums-installation-on-64-bit-systems-910970.html>.

2. Copy the IGEL UMS installation program you downloaded earlier in this document to the Window server you wish to install the UMS and double-click it to execute the installation program.

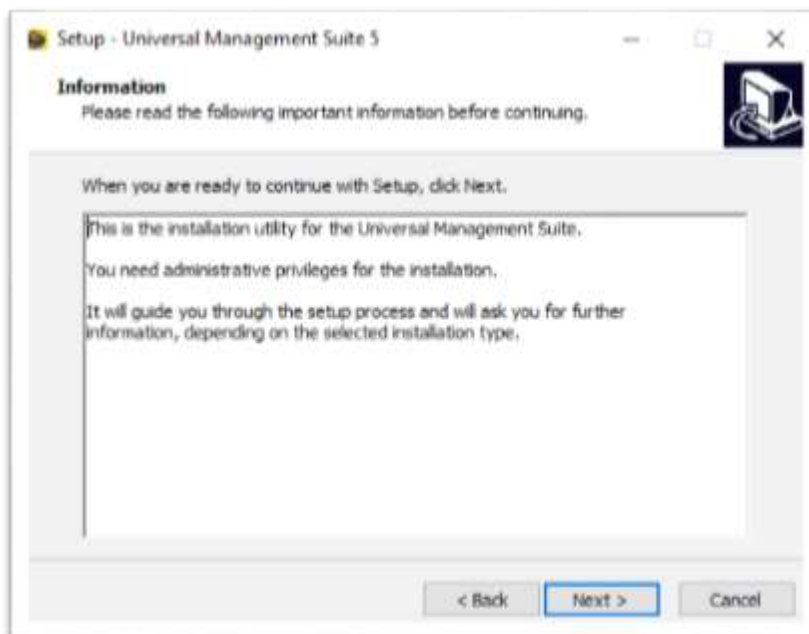
Click **Next** to continue.



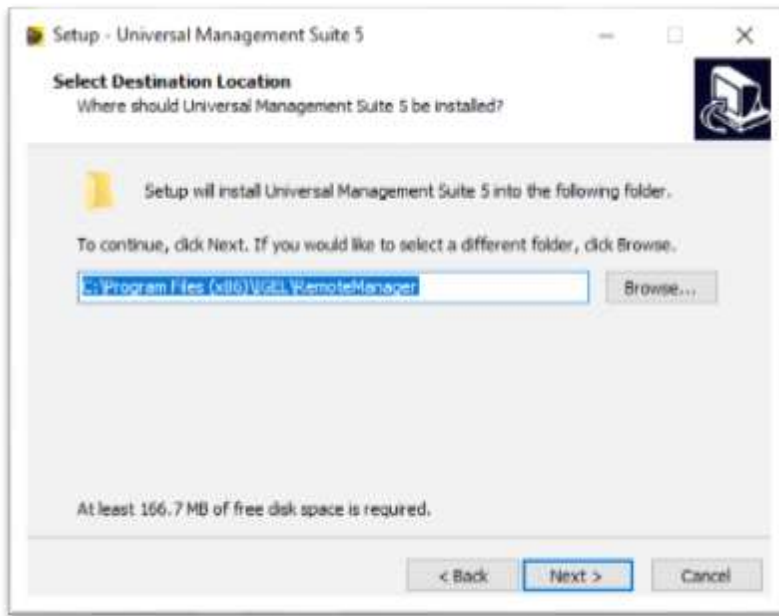
3. Read and agree to the IGEL UMS License Agreement. Click to select the **I accept the agreement** checkbox. Click the **Next** button to continue.



4. Click **Next** to continue.



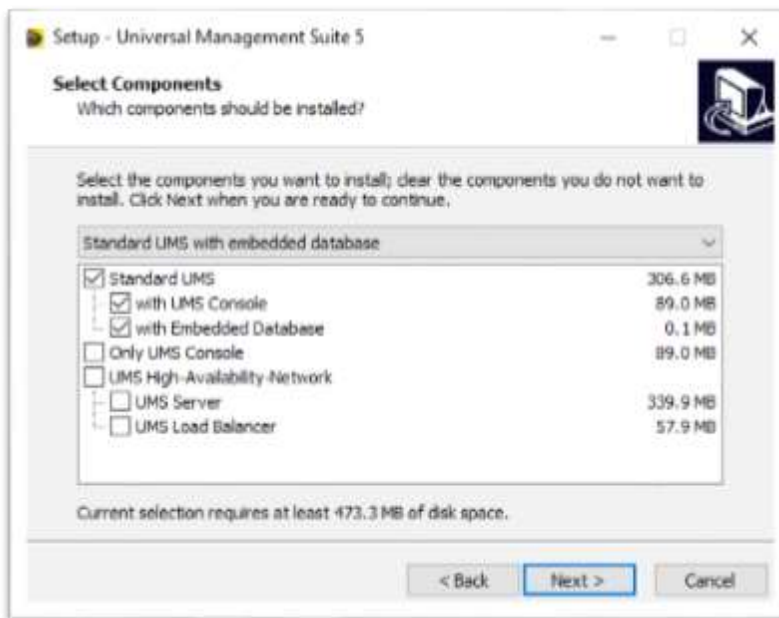
5. Enter the desired location to install the UMS system files and click **Next** to continue.



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

Learn more about the different components at <https://kb.igel.com/endpointmgmt/en/installation-on-windows-910881.html>.

Click **Next** to continue.

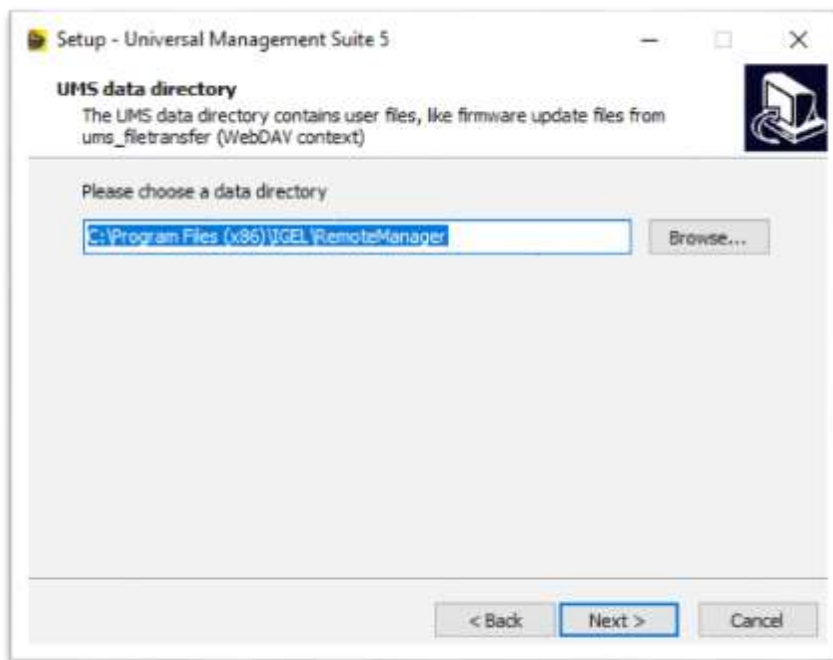


7. Enter the location you wish to store the UMS data directory. The data directory is where large files, such as firmware, are stored.

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

For a default installation, the UMS require approximately 500M in the beginning. It grows over the lifespan of the UMS deployment. 2 GB would be fine for even the biggest 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 new **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 just might find yourself running out of disk space.

Click **Next** to continue.

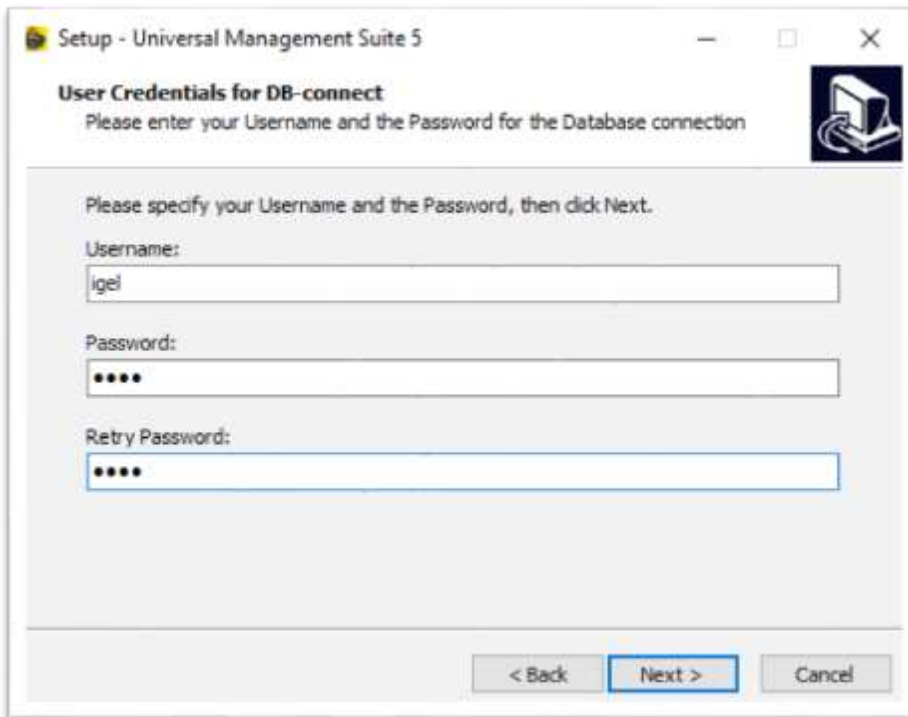


8. Next, you are required to create the database's superuser account. The superuser account is used to login to the UMS for the first time and has full access to the UMS' database. It is not a Windows user account, but a user created specifically for the IGEL UMS.

Username and passwords are important. 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 gain the keys to your IGEL kingdom.

Both UseRnaMe and PaSswOrd are Case Sensitive.

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



Setup - Universal Management Suite 5

User Credentials for DB-connect
Please enter your Username and the Password for the Database connection

Please specify your Username and the Password, then click Next.

Username:

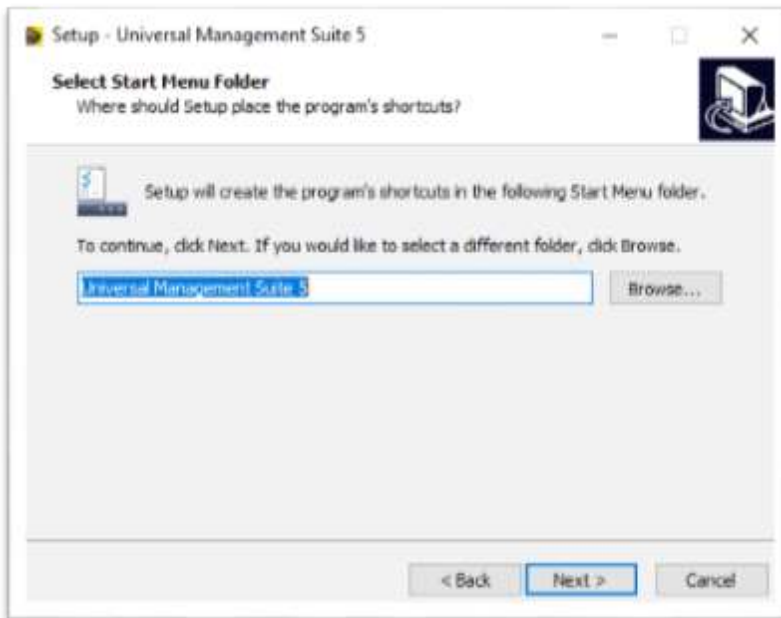
Password:

Retry Password:

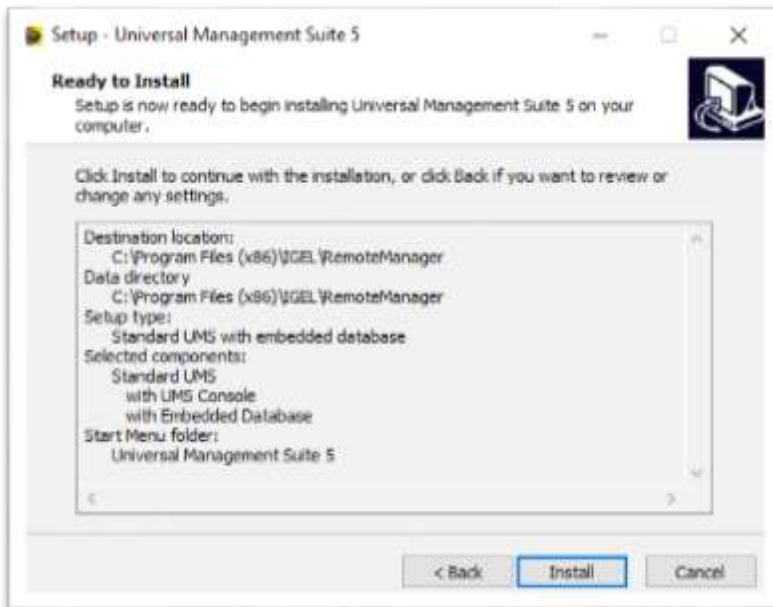
< Back **Next >** Cancel

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.

9. You are prompted to define the location that setup places the shortcut to the IGEL UMS server's console. Enter the desired location and click **Next** to continue.

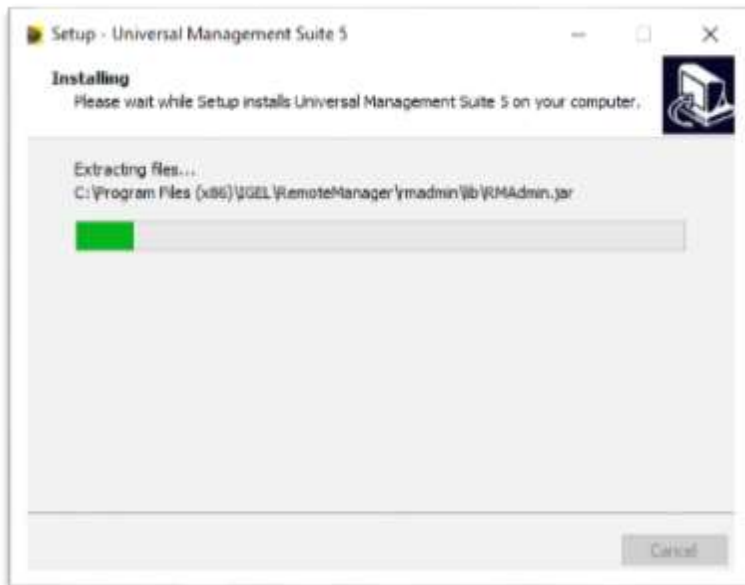


10. Please verify the settings are correct and click the **Install** button for setup to install the IGEL UMS.



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

It is possible that your Anti-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.



12. 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.

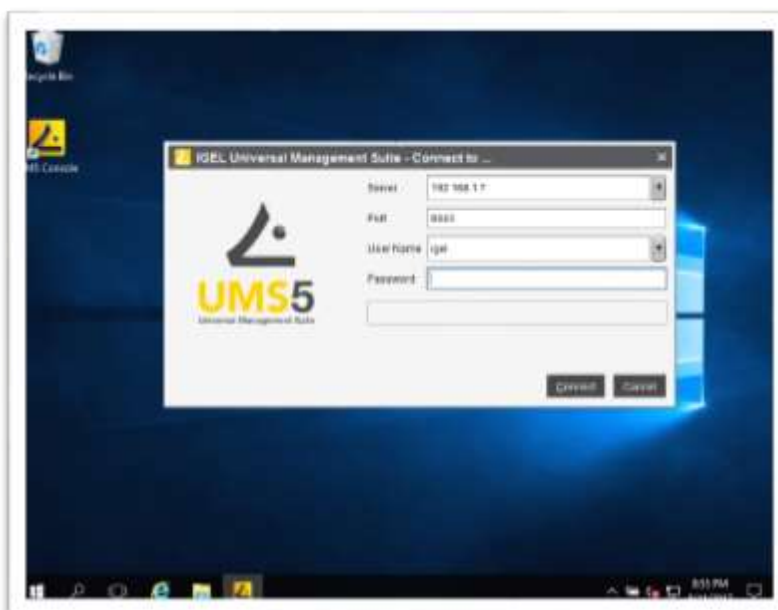


13. You notice the IGEL UMS Console's shortcut on the server's desktop or the location you specified during installation. Go ahead and double-click it to launch the UMS Console and login for the first time!

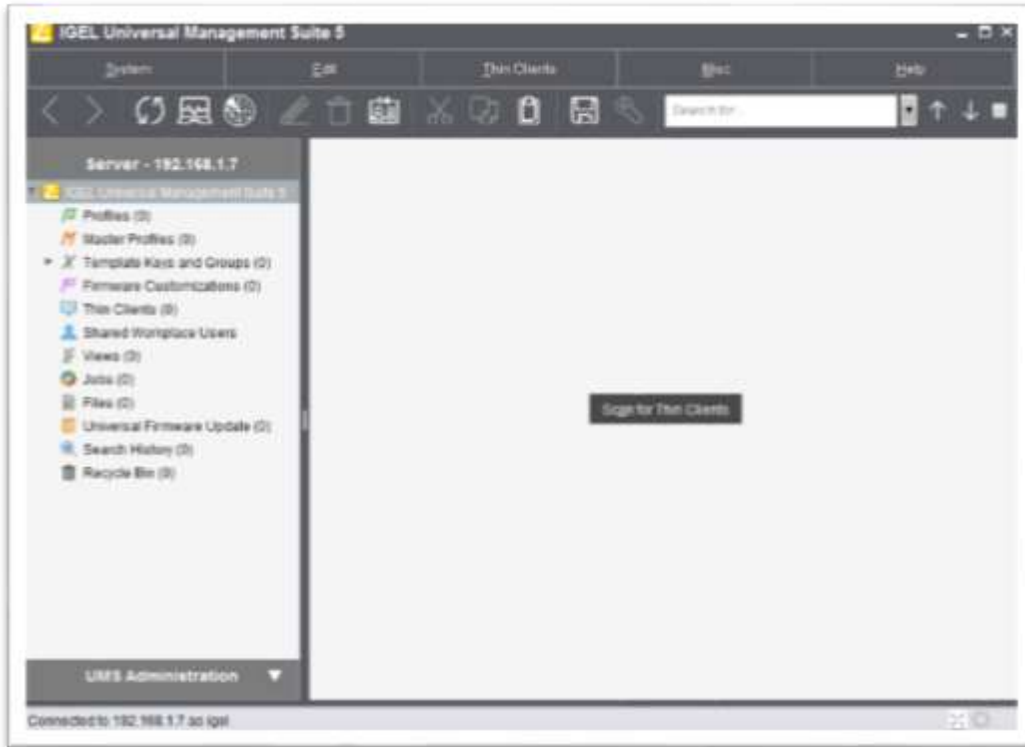


14. You are presented with the **UMS Connect To** screen. Since you are running the UMS Console from the server, there is no requirement to enter the server IP/DNS as it defaults to the local machine. If you previously created the '**igelrmserver**' DNS record, use this Server: **igelrmserver**.

Enter the default port number (8443), username and password, as configured in step 8 above. Click the **Connect** button to connect to the UMS.



15. If the stars aligned or you correctly followed the previous steps, you should see the UMS Console 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 Open Firewall Ports Required by UMS

You are required to configure any firewalls, including the Windows Firewall and AWS Security Group, to allow the UMS to communicate with the IGEL OS.

By default, the Windows firewall is configured with the following basic rules:

- Inbound Connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

The Windows firewall is configured to allow all outgoing connections. Hence, you are not required to create any outbound rules. However, inbound connections are blocked. These rules are needed to be created for the desired network ports.

Usually, the UMS installer should do this for the UMS Windows Server, but it is highly recommended you verify the required ports are open.

The following ports are required for proper network communications. The defined ports and protocols must have the ability to communicate from client to the server.

Service	Port	Type	Usage	Changeable in UMS
Server / High Availability	30001 30002	TCP/UDP	Communication between UMS server and thin client (30001). If server and load balancer are running together on one system, the server switches to port 30002 and load balancer uses 30001.	Yes
UMS Agent on TC	30005	TCP/UDP	The UMS component on the thin client (UMS Agent) is waiting for UMS server input on this port.	No
GUI Server	8443	TCP	Communication between GUI server and UMS console and file transfer with https.	Yes
IGEL Management Interface (IMI)	8443	TCP	REST API for UMS (subscription required)	Yes

The above table only lists the ports required open for a basic deployment. For a complete list of IGEL ports, please refer to the following support article <https://kb.igel.com/endpointmgmt/en/ums-communication-ports-910971.html>.

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

During the installation of the IGEL UMS the Administrator Console is installed on the server, as shown above, but if you would like to install it remotely, you can. This comes in handy if you wish to log into the UMS remotely. For example, if the UMS server is running on Linux or a cloud instance (AWS, Azure).

The IGEL UMS Management Console remote install has the following system requirement:

- Minimum 512 MB RAM (1 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.

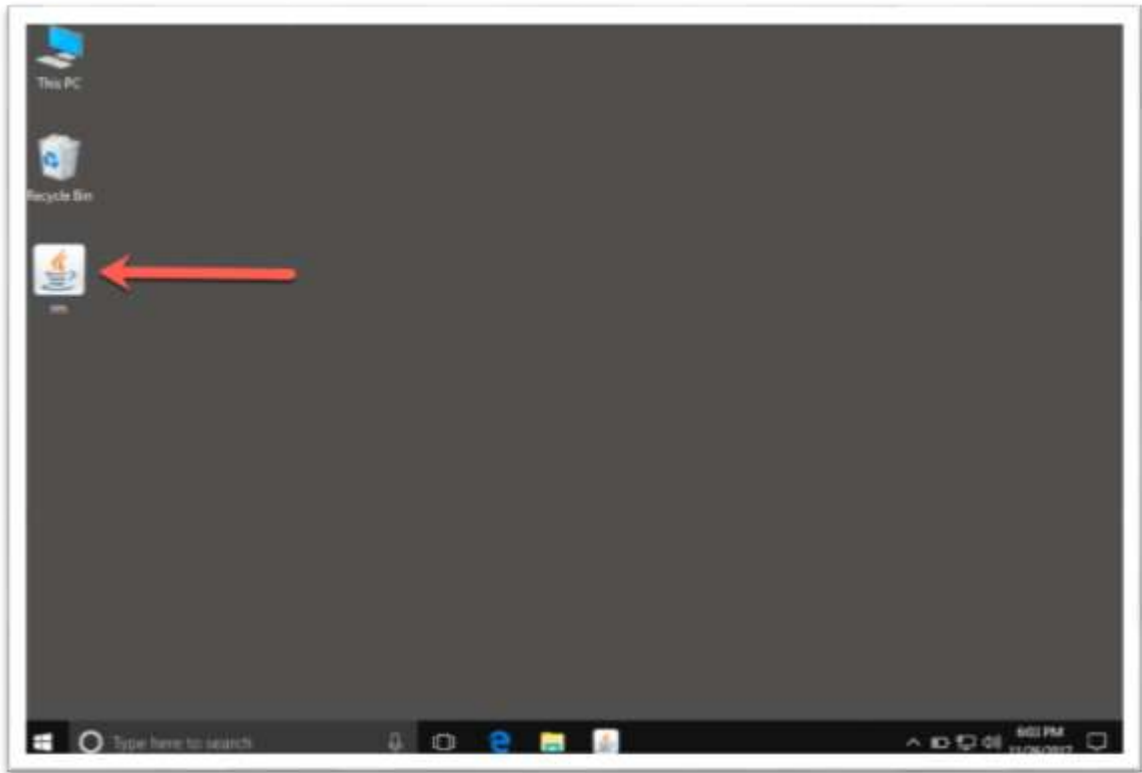
If you did not create the ‘**igelrmserver**’ DNS or DHCP setting as documented above, you are required replace ‘**igelrmserver**’ with the server name or IP address of the IGEL UMS server.



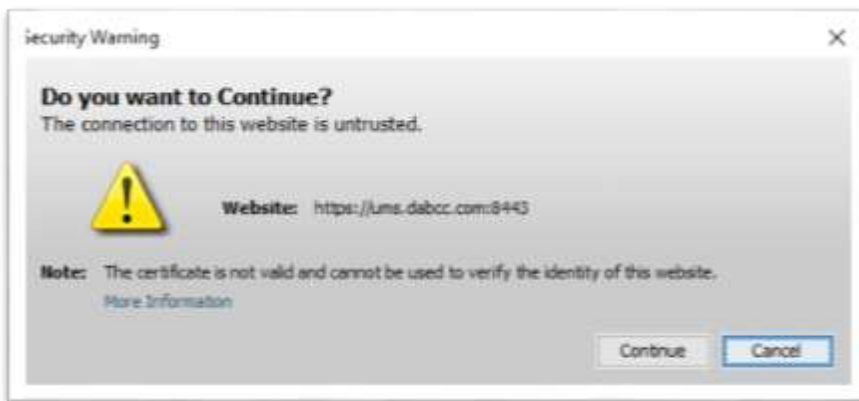
2. Click the **Start IGEL Universal Management Suite Console** link and click the **Save As** button to save the Java applet to the desired location.



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.



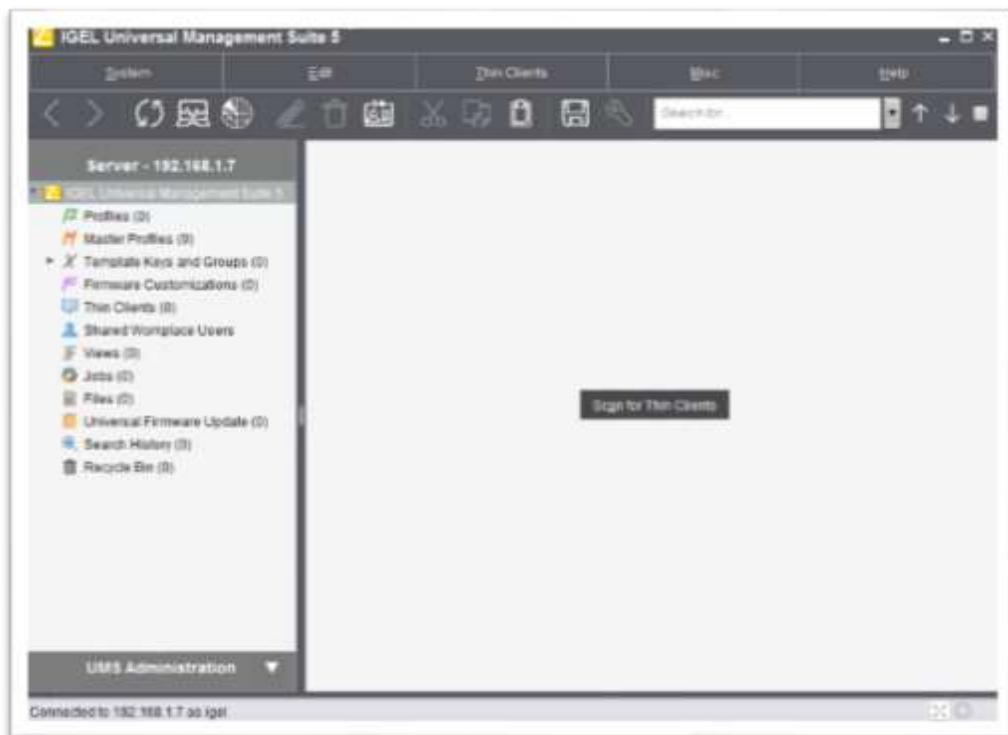
5. Enter the UMS server address in the **Server** text box, use 'igelrmserver' if you created the DNS or DHCP setting, as recommended above.

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

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



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



4. Install IGEL Cloud Gateway (ICG)

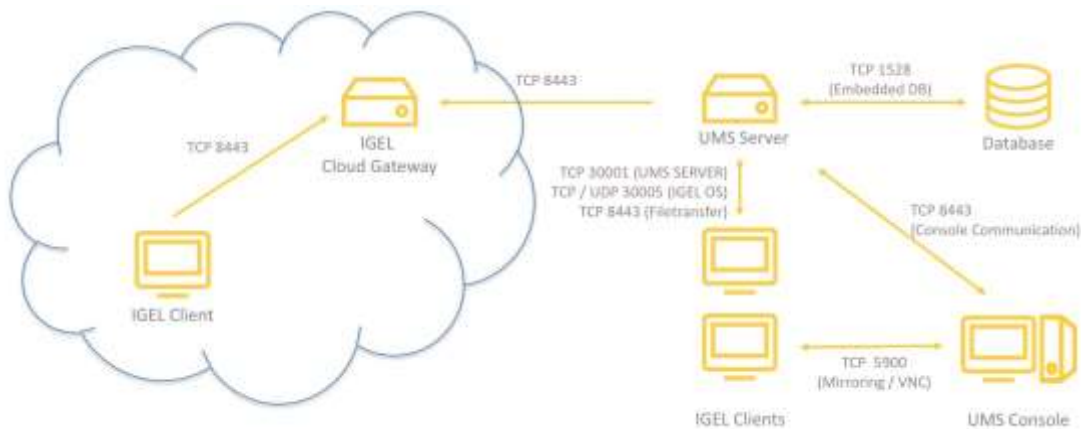
If desired, you are ready to install the IGEL Cloud Gateway (ICG). The ICG enables the Universal Management Suite (UMS) to manage endpoint devices outside the company network, securely.

It is not required to install an ICG server to test the IGEL OS and UMS. Though, 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 end-points 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



Licensing

As you are installing the IGEL software platform using the free licenses you received from the IGEL website, downloaded earlier in this document, you might notice you do not have a license to run the ICG. It does not come with the trial version. Don't worry; this is a problem we can solve.

If you want to take the plunge, you are required to procure an ICG license.

For your testing enjoyment and as a benefit of being a reader of this document, IGEL is happy to provide you with a free license. All you need to do is email ICGdemo@igel.com and let them us you are reading this guide and would like your free ICG license.

Learn more:

- [IGEL Cloud Gateway Manual](#)
- [IGEL Cloud Gateway eDocs support homepage](#)

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

- ICG System Requirements
- How to Create an AWS Instance for ICG
- How to Open Firewall Ports Required by ICG
- Create Required DNS Records
- Download IGEL Cloud Gateway Software
- How to Generate a CSR File
- How to Create an SSL Certificate for ICG
- How to Add Certificates to UMS
- How to Install the IGEL ICG Software
- How to License the IGEL ICG

4. 1. ICG System Requirements

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

ICG Virtual Appliance

- The ICG Virtual Appliance version 1.03.100 is supported on VMware ESXi, VMware Workstation or Oracle Virtual Box.

Manual Software Installation

The ICG software can be manually installed on virtual or physical hardware meeting the following requirements:

- Requires x86 64-bit architecture running Ubuntu 16.04 or Debian 8.
- Recommended 2 GB RAM for production environments.

Though, for a test/lab environment, you should be able to get away with using 1GB RAM. By following this document, you are installing 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.

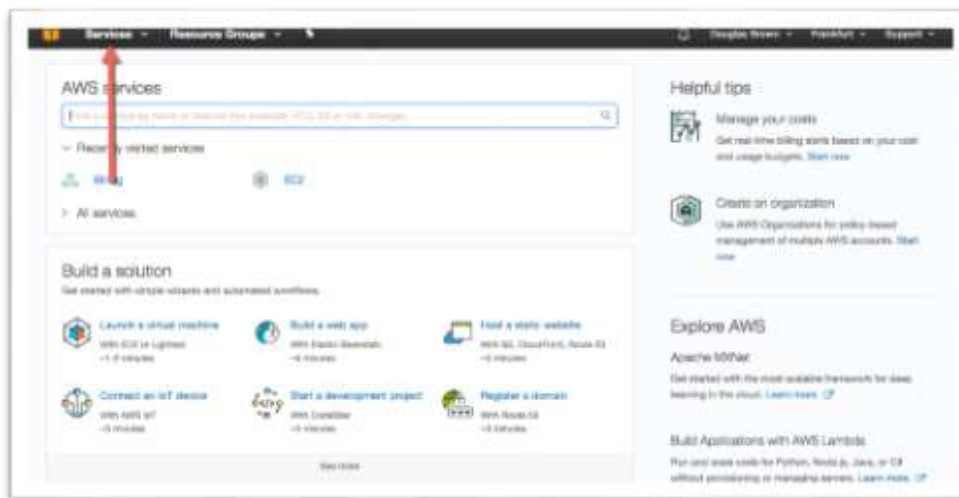
- The following packages are required: *dialog*, *uuid-runtime*, *super*, *unzip*, *realpath*.
- UMS (Universal Management Suite) in version 5.07.100 or newer.
- IGEL OS in version 10.03.100 or newer.

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

As you are using a free tier AWS EC2 instance for this project, you are required to set up an AWS account. Browse to <https://aws.amazon.com/> and create your free account.

The following details how to install the ICG on an AWS EC2 Cloud Instance:

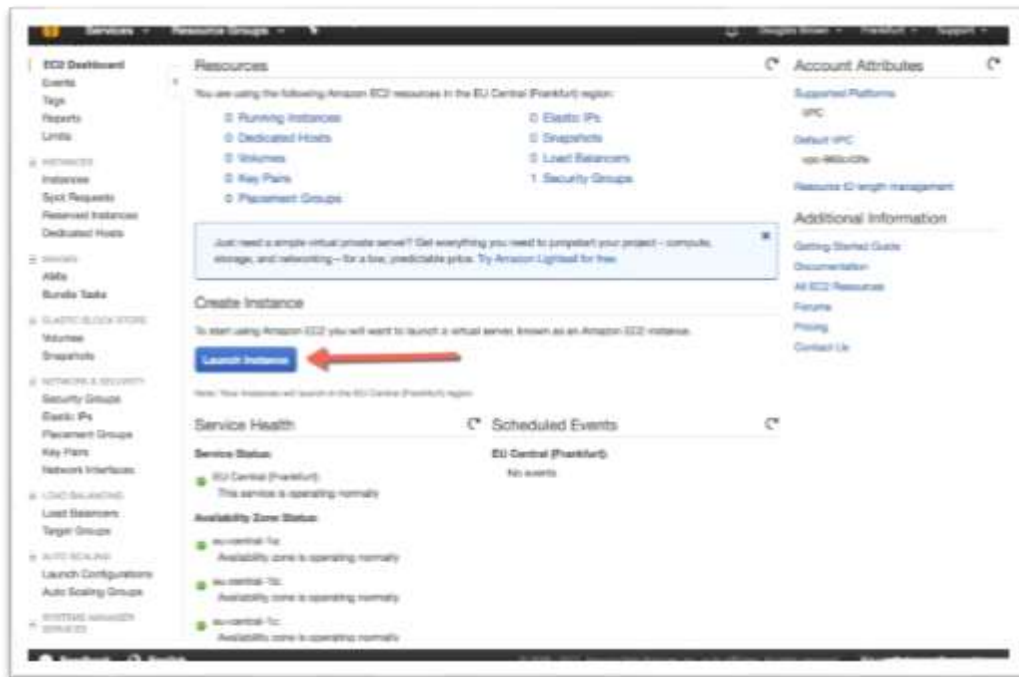
1. Login to your AWS account and click on the **Services** link located in the top menu bar.



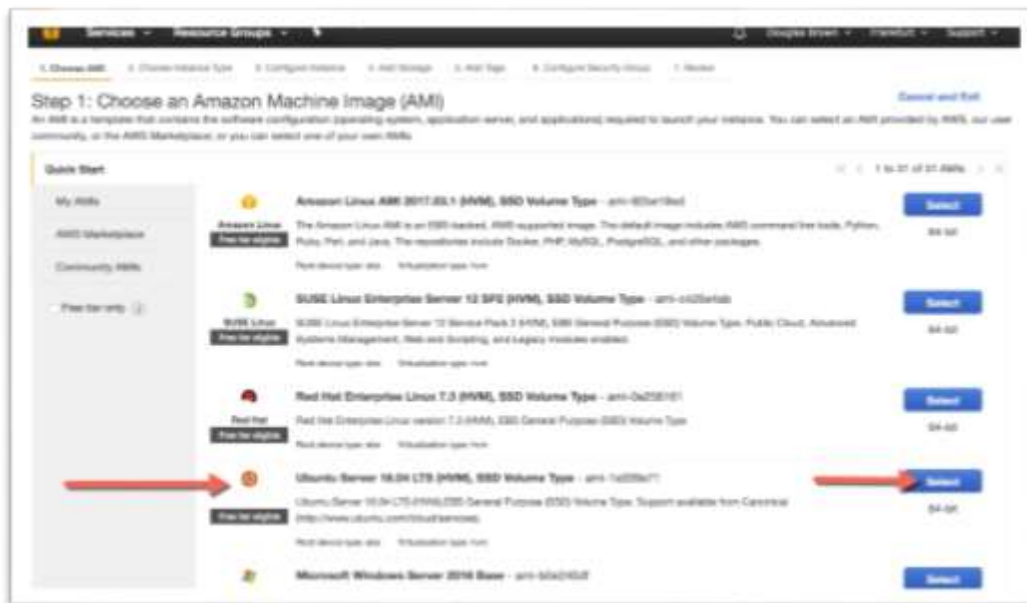
2. Click the **EC2** link.



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

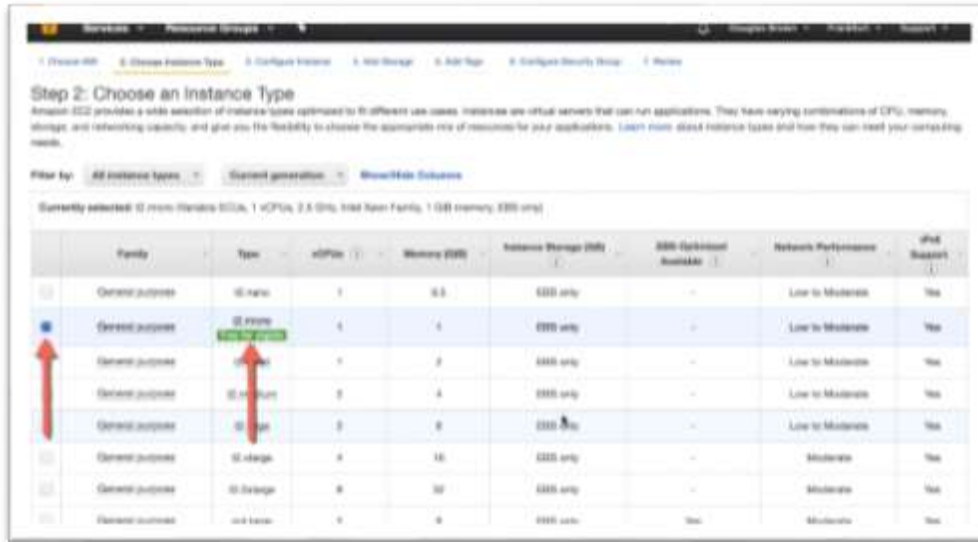


- Click the **Select** button for the **Ubuntu Server 16.04 LTS (HVM), SSD Volume Type**.

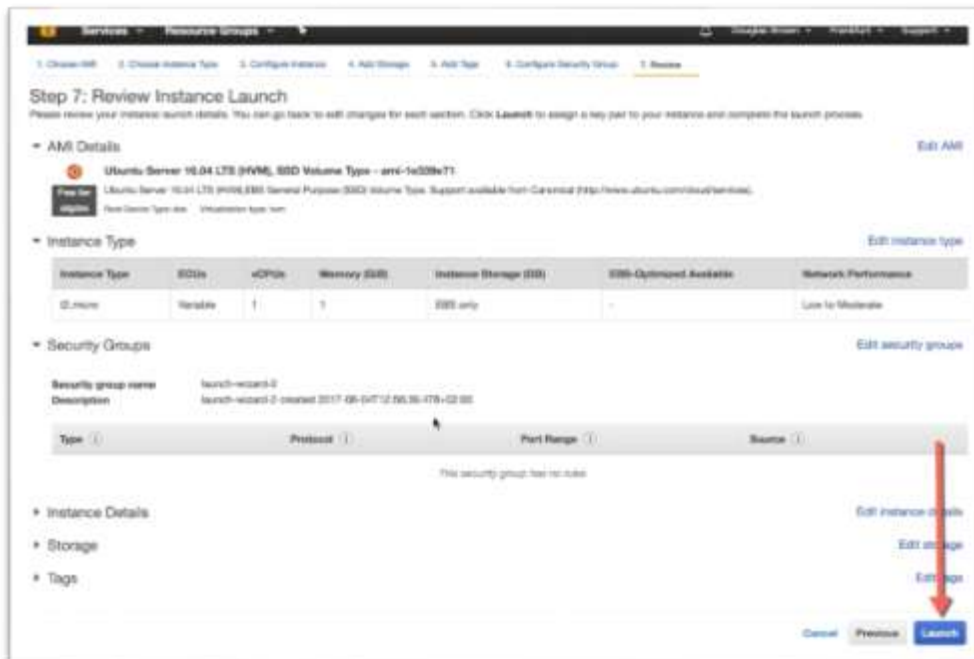


- You are prompted to pick the type of instance to deploy. The amount of CPUs and RAM depends heavily on how many users you are required to support. For this example, you are creating a personal demo environment. The AWS Free Tier works fine for this use case.

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

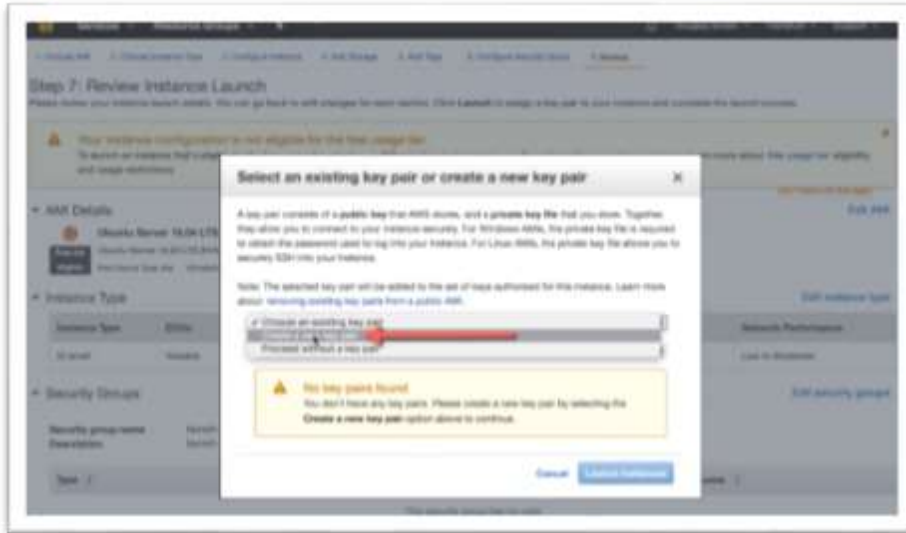


- Confirm you selected the correct Instance and click the blue **Launch** button to start the virtual machine.



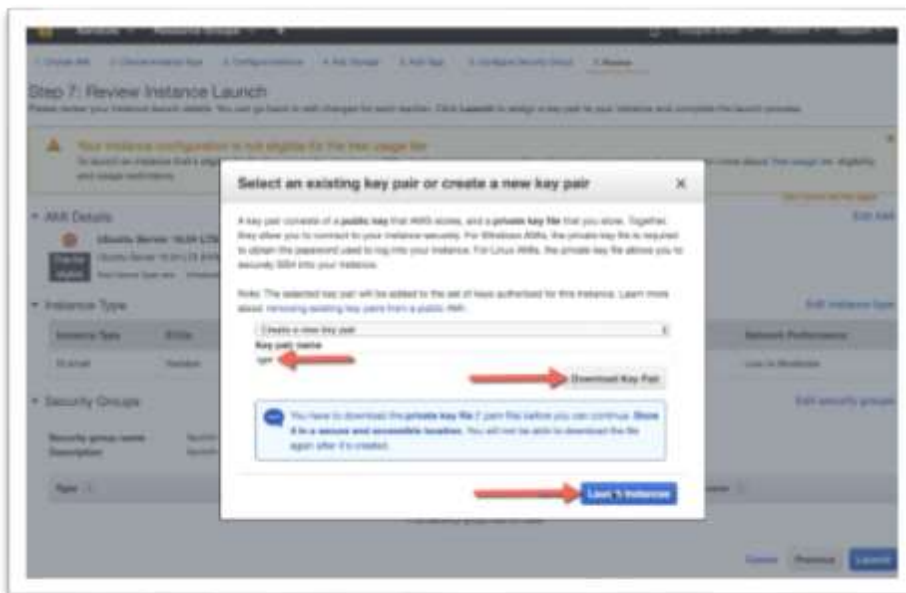
- You are prompted to create a new key pair. Later this key is used to connect to the ICG server via SSH and FTP.

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



- Enter a name for your key pair in the **Key pair name** textbox 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, but one accessible as it is used in a bit.

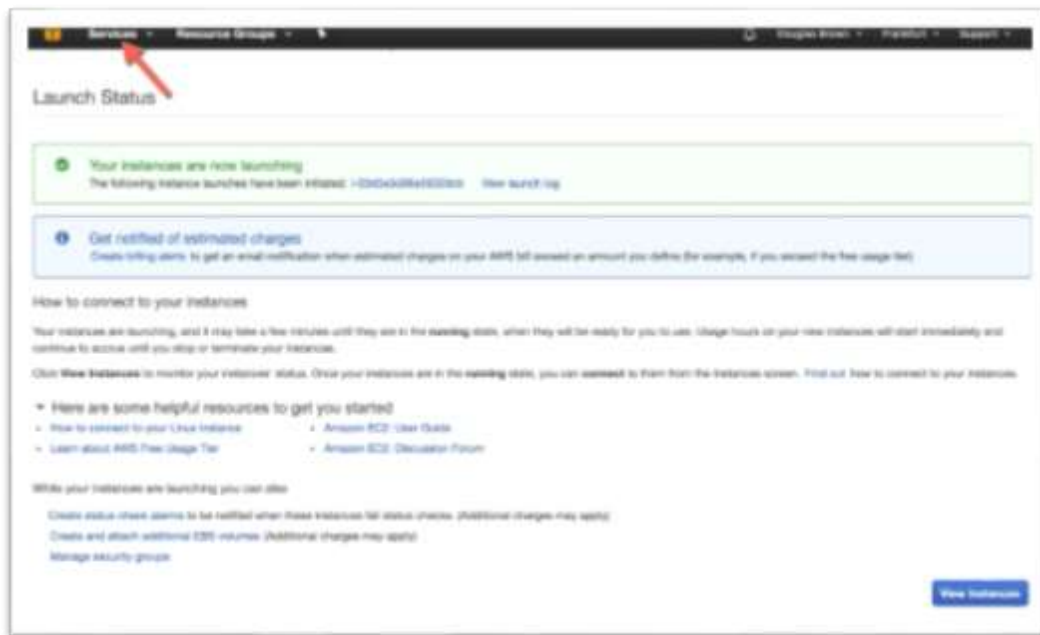
Once you have successfully downloaded the key, please click the blue **Launch Instances** button.



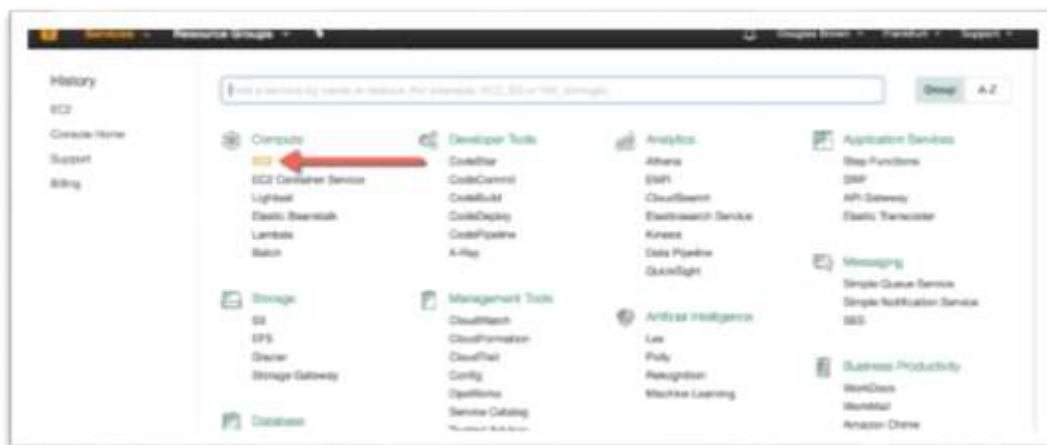
9. The file download looks something like the following, depending on your OS type.



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

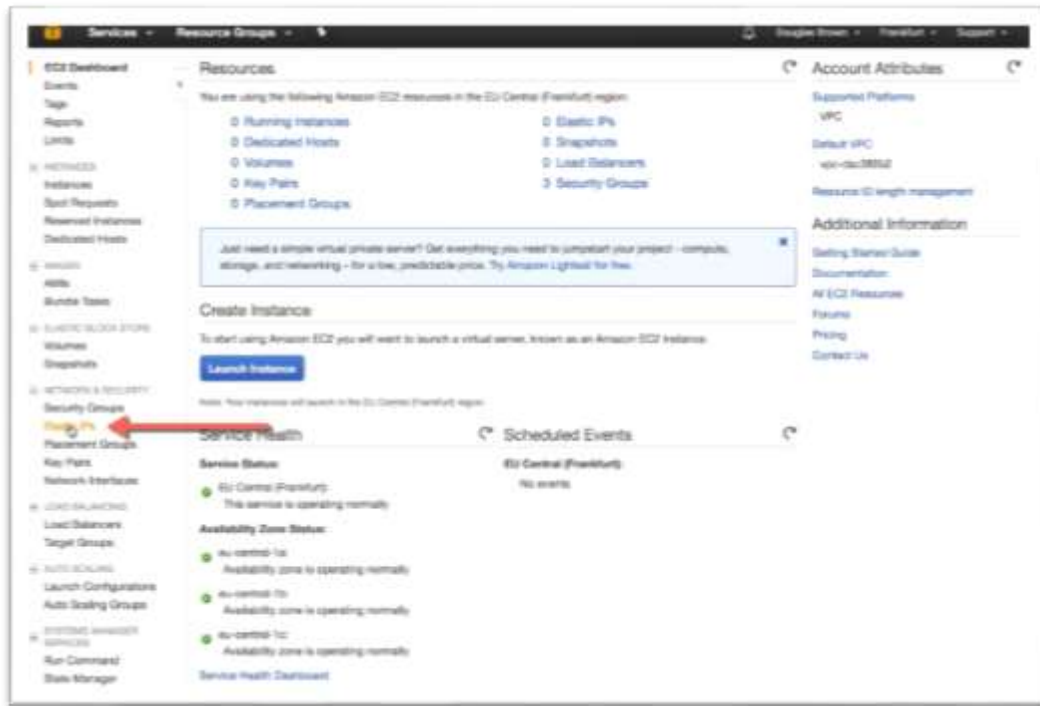


11. Click the **EC2** link.



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 blue **Allocate new addresses** 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.

Click the blue **Close** button to continue.



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



17. Click the **Instances** item located in 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.



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

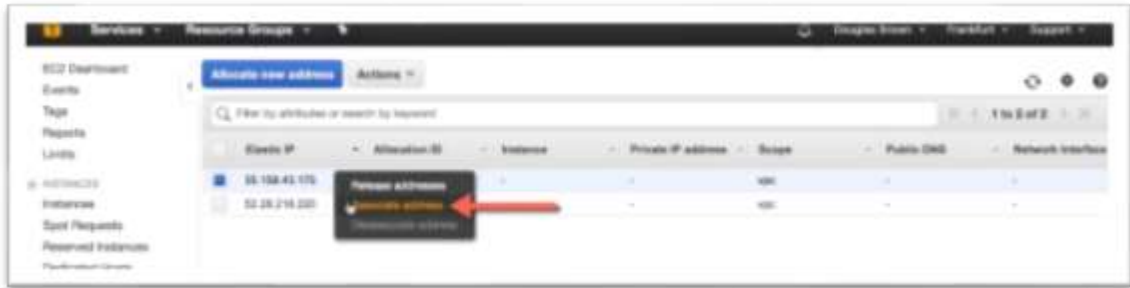
Click on the **Elastic IPs** link located in the left menu.



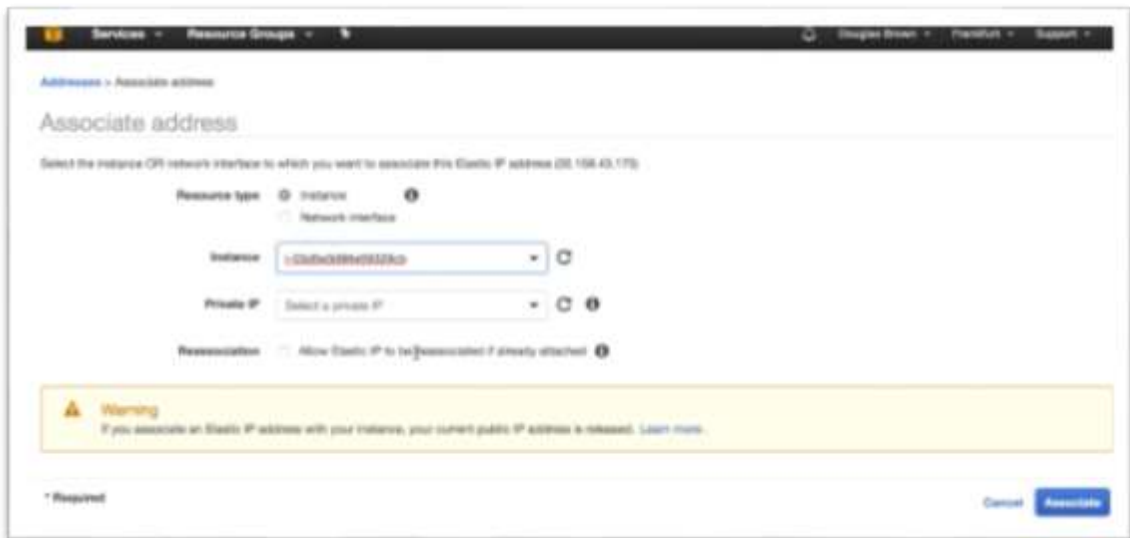
19. You are brought to the list of IP addresses issued, as seen above.



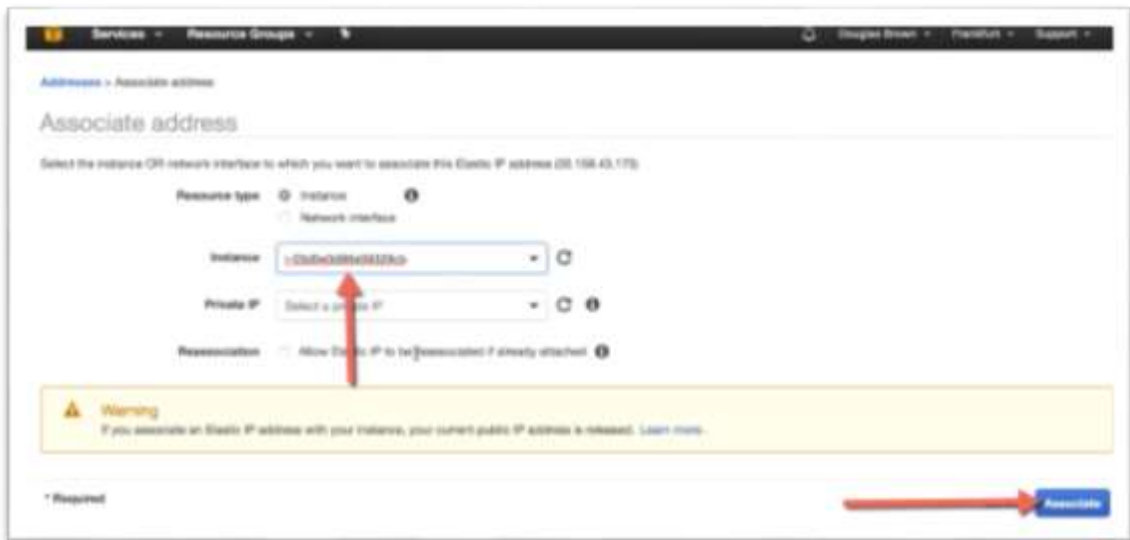
20. Right-click on the IP address you wish to assign to the ICG instance and click the **Associate address** menu item to link the selected IP address to the newly created Instance.



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



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



23. Click the **Close** button to continue.



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



25. Before you move too far, it is always good housekeeping to give your instances names anyone can understand.

Click on the **Instances** link in the left menu and select the instance you wish to change the name of and click the **pencil-shaped icon** for the desired Instance.



26. Type the new name for the Instance. For this example, please name it ICG. Hit the enter key or click the round checkbox on the bottom right of the popup.



The new IGEL Cloud Gateway instance is up and running with a working IP address and a friendly name. You are ready to configure the required firewall changes and install the ICG software itself.

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

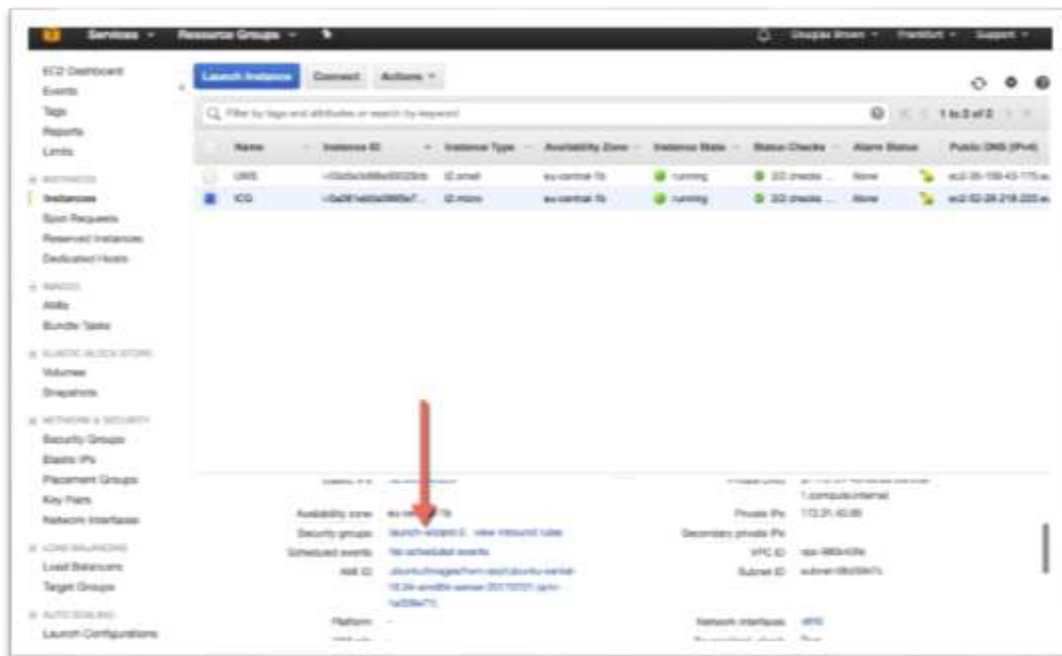
The ICG communicates with the UMS over port 8443. Thus you are required to configure the AWS firewall with the proper rules to allow access.

The following details how to open the required ports:

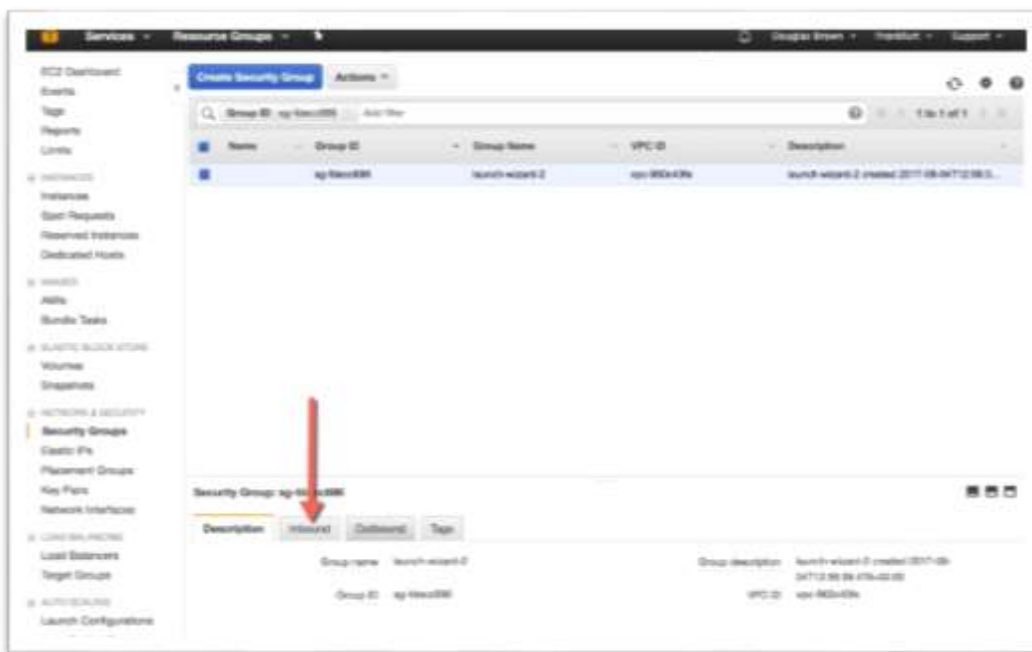
1. Click the **Instances** link, located in the left menu.



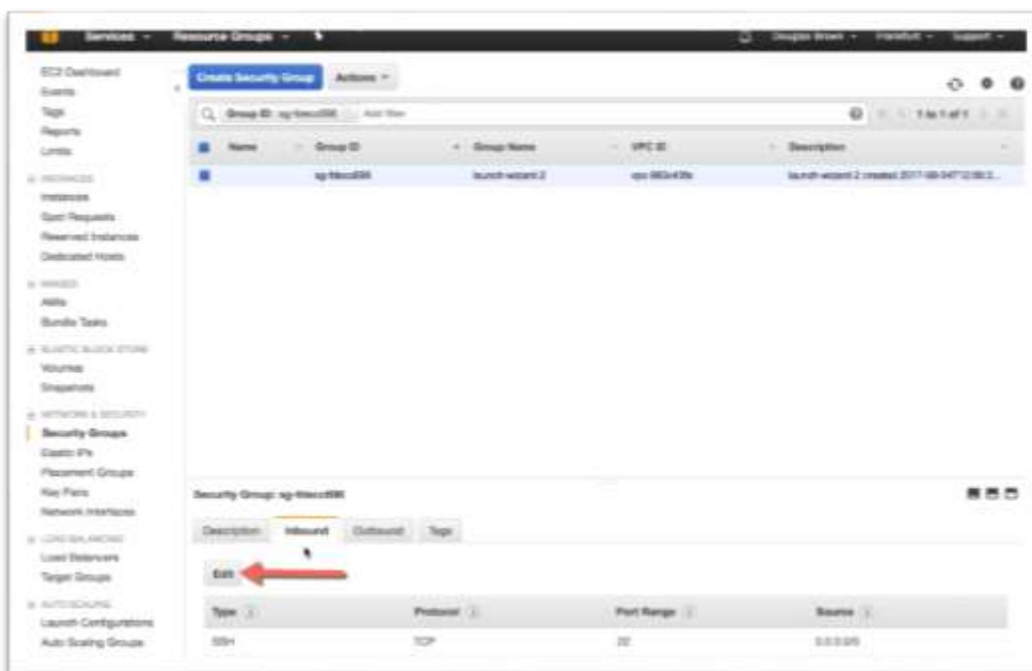
2. Click to select the newly created ICG instance and scroll down to **Security Groups**. Click the **launch-wizard-2** link.



- Click to select the **Inbound** tab.

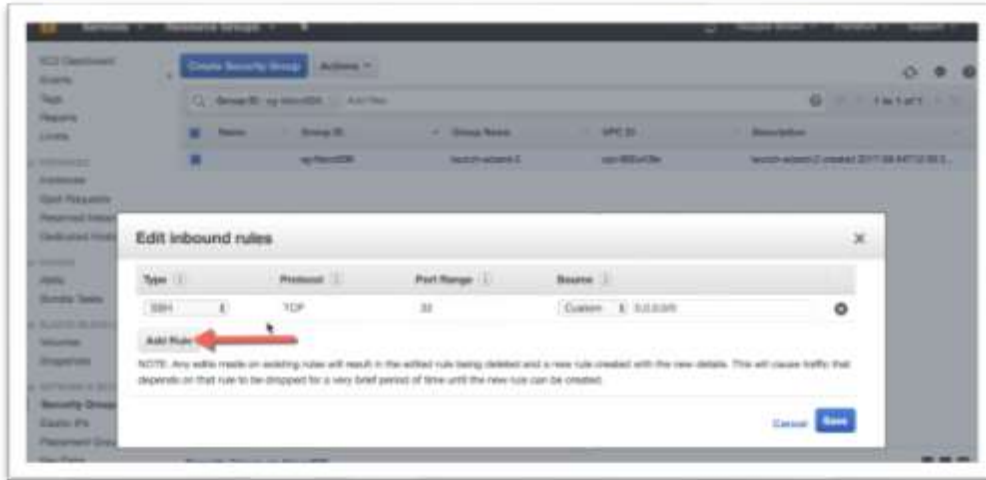


- Click the **Edit** button.



- 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.



- Configure the new rule as follows:

- **Type: Custom TCP**
- **Protocol: TCP**
- **Port Range: 8443**
- **Source: Anywhere**

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



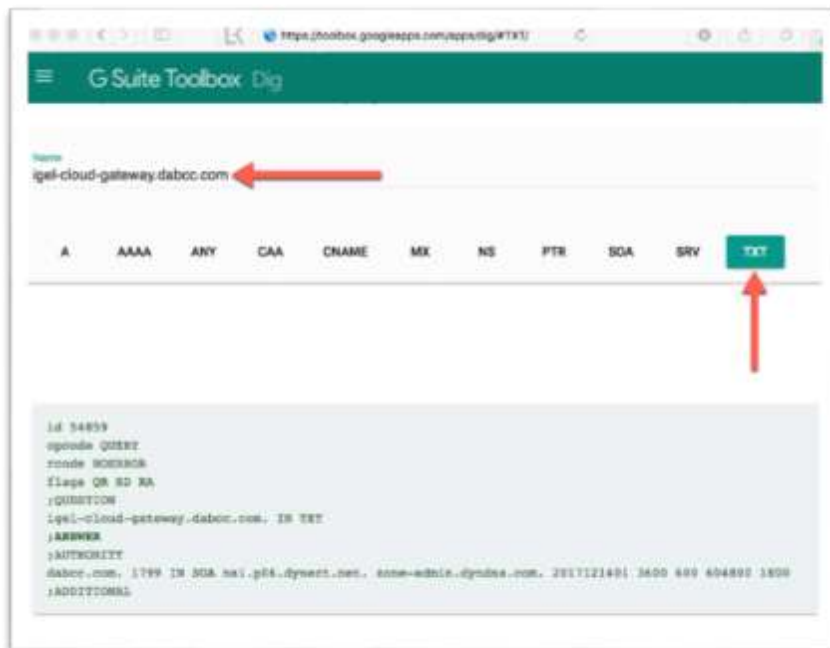
4. 4. Create Required DNS Records

The Internet runs on IP addresses, but users sure love their catchy names. It is time to create the required DNS entries for your new IGEL Cloud Gateway.

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

You can use a tool like **Google's G Suite Toolbox Dig** to verify your TXT entry is setup 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.



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.

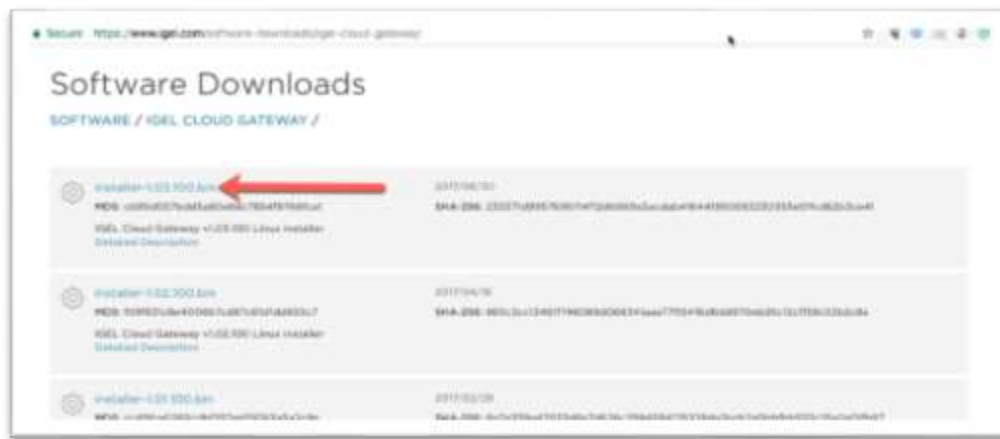
Depending on your DNS host, it could take up to 24 hours for your DNS changes to take effect across the globe. To verify the required DNS entries are active you can use the **DNS Propagation Checker**.

4. 5. Download IGEL Cloud Gateway Software

Before you install IGEL Cloud Gateway, you are required to download and copy it to the ICG server. The ICG software is currently not delivered in the evaluation package you downloaded above. You are required to download it manually now.

The following details how to download and copy the ICG software to your AWS Cloud instance:

1. Browse to the IGEL Software downloads web page to download the ICG software at <https://www.igel.com/software-downloads/igel-cloud-gateway/>.



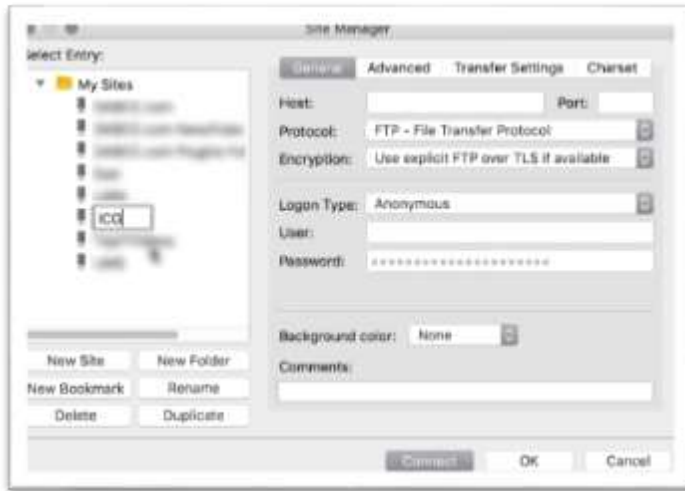
2. Once downloaded, you are required to copy the ICG bin file to the ICG server's hard drive. You do this using your favorite FTP Client.

In this example, we are using the free version of FileZilla at <https://filezilla-project.org/>.

If you are using FileZilla, open it and click the **Site Manager** button of the top left of the FileZilla menu bar

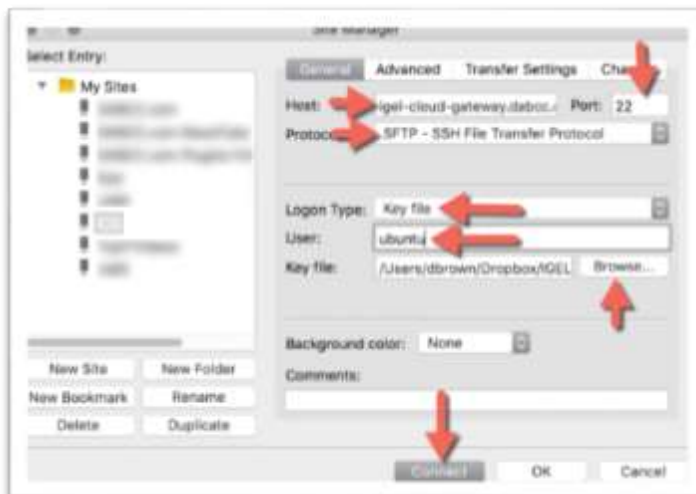


- The **Site Manager** window opens allowing you to create a new connection. Click the **New Site** button. Add a friendly name for your new connection, such as ICG.

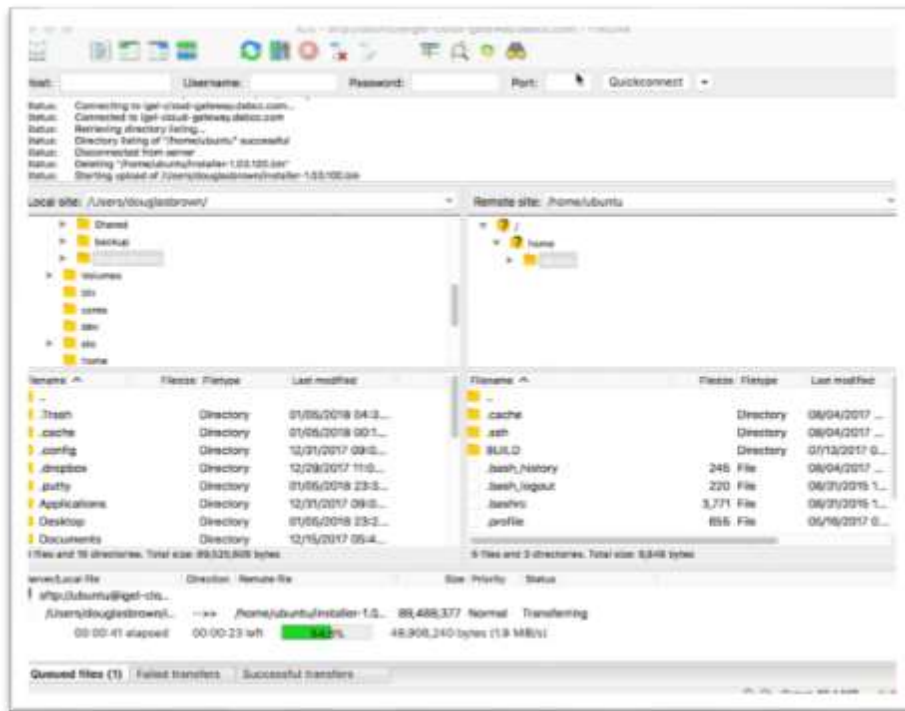


- You are required to enter the connection details for the ICG server. Configure the following sections:
 - Host** – Enter the DNS name of the ICG server
 - Port** - Enter **22**
 - Protocol** – Select **SFTP – SSH File Transfer Protocol**
 - Login Type** – Select **Key File**
 - User** – Enter the username
 - Key File location** – Click the **Browse** button to select the key file (igel.pem) you created above.

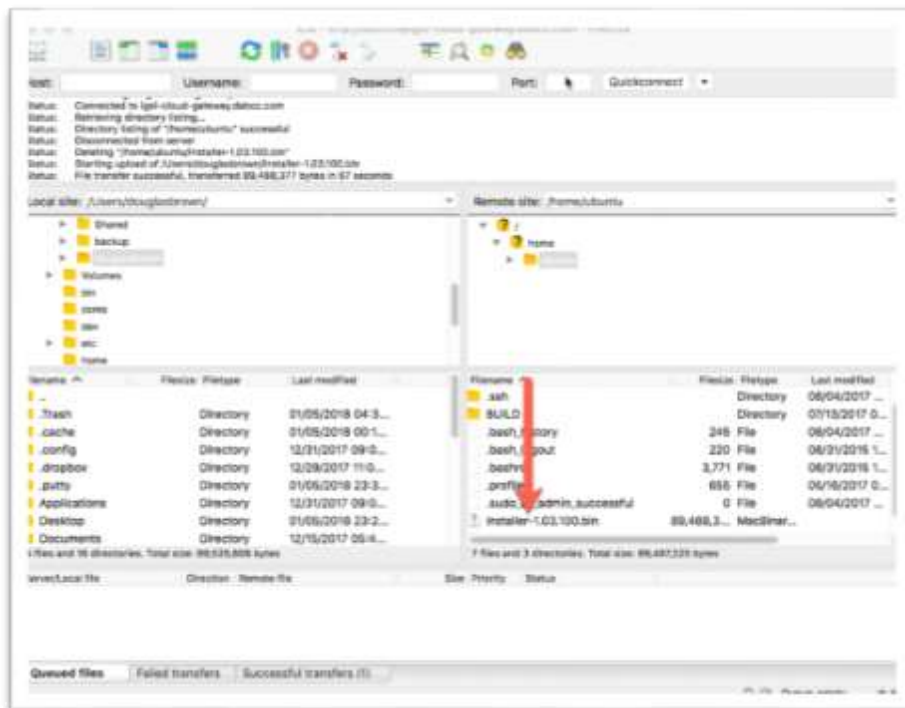
Once finished, click the **Connect** button.



- FileZilla logs in to the ICG server's file system via FTP, as shown below. Find the ICG install package download and drag and drop it onto the ICG root folder.



- If all goes well, you should find the uploaded IGEL binary in the list of files.



4. 6. 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, both public and private certificate authorities also. Although, to take full advantage and the best 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 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 fine for our use case and more than 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](#) section to learn how to deploy a certificate from <http://www.digicert.com>.

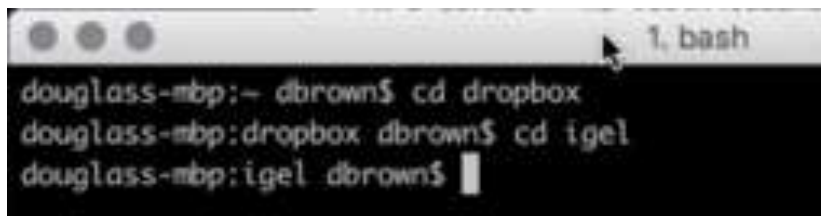
One of the main benefits of a public certificate is that you are not required to enter the part of the certificate fingerprint while connecting the IGEL OS to the ICG. Not to mention, it is always more secure when using a trusted certificate authority as there is a piece of mind that comes with knowing the certificate was vetted prior

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

1. 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 can do it from its command line.

To do this, you are required 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**.

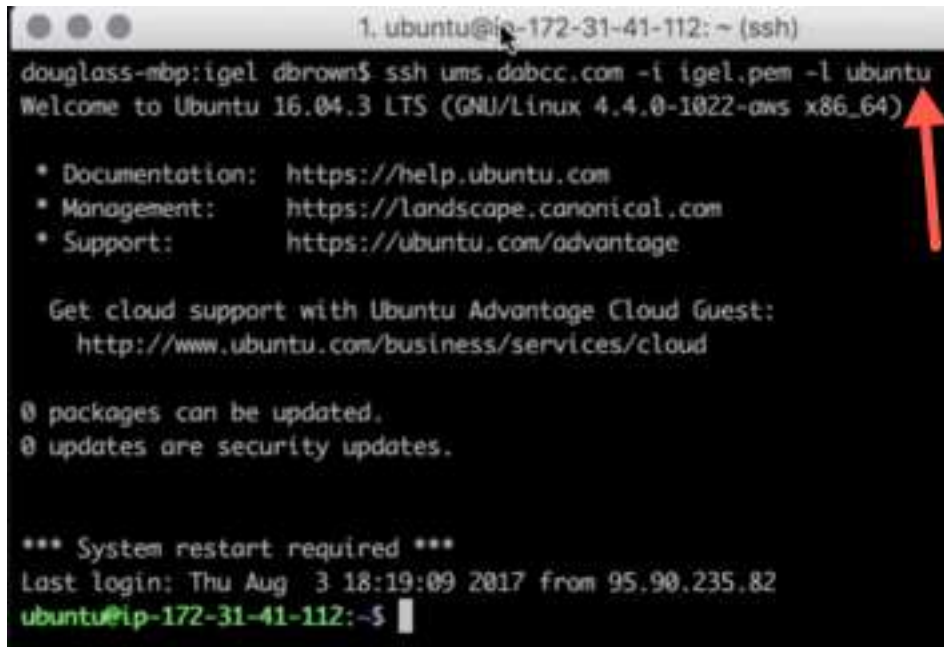


```

1. bash
douglass-mbp:~ dbrown$ cd dropbox
douglass-mbp:dropbox dbrown$ cd igel
douglass-mbp:igel dbrown$
  
```

2. Login to the remote ICG instance by typing the following:

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

A terminal window titled '1. ubuntu@ip-172-31-41-112: ~ (ssh)' shows the command 'ssh ums.dabcc.com -i igel.pem -l ubuntu' being executed. The output displays the Ubuntu 16.04.3 LTS welcome message, including documentation, management, and support links. It also shows that 0 packages can be updated and 0 updates are security updates. A red arrow points to the 'Welcome to Ubuntu' line. The prompt changes to 'ubuntu@ip-172-31-41-112:~\$'.

3. 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
```

A terminal window titled '1. ubuntu@ip-172-31-41-112: ~ (ssh)' shows the command 'openssl req -new -newkey rsa:2048 -nodes -keyout igel-cloud-gateway.dabcc.com.key -out igel-cloud-gateway.dabcc.com.csr' being executed. The prompt is 'ubuntu@ip-172-31-41-112:~\$'.

4. You will be asked a bit of information that is incorporated into your certificate request. It is important for this information to be valid as the Certificate Authority will verify it before issuing you a certificate.

Enter your information until the CSR is successfully created.

```

1. ubuntu@ip-172-31-41-112: ~ (ssh)
.....
..+++
.....+++
writing new private key to 'igel-cloud-gateway.dabcc.com.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DE
State or Province Name (full name) [Some-State]:Bremen
Locality Name (eg, city) []:Bremen
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IGEL Technology
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:igel-cloud-gateway.dabcc.com
Email Address []:brown@igel.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
ubuntu@ip-172-31-41-112:~$

```

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

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

```
ubuntu@ip-172-31-41-112:~$ cat igel-cloud-gateway.dabcc.com.csr
```

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

[illegible]

7. Browse to <http://www.psw.net/> and click the **SSL Certificate** link on the top left of the page.



8. Scroll Down until you find the **Positive SSL** certificate and click either the 30 day or 1-year link, this is up to you.

Representation (certificates)	Secured by PositiveSSL	Secured by PositiveSSL	Secured by PositiveSSL	Secured by PositiveSSL	Secured by PositiveSSL	Secured by PositiveSSL
Intermediate certificate (SSL 128-bit) (SSL 128-bit)	Yes	Yes	Yes	Yes	Yes	Yes
Issuing CA	Comodo	Comodo	Comodo	Comodo	Comodo	Comodo
Product	PositiveSSL	PositiveSSL	PositiveSSL	PositiveSSL	PositiveSSL	PositiveSSL
Root certificate	Comodo Intermediate CA Root	Comodo Intermediate CA Root	Comodo Intermediate CA Root	Comodo Intermediate CA Root	Comodo Intermediate CA Root	Comodo Intermediate CA Root
Validation	Email Based	Email Based	Email Based	Email Based	Email Based	Email Based
Validation in (public values) 1	10 min	10 min	10 min	10 min	10 min	10 min
Free exchange 1	Yes	Yes	Yes	Yes	Yes	Yes
Additional physical machines	Yes of charge	Yes of charge	Yes of charge	Yes of charge	Yes of charge	Yes of charge
Recommended for	Admin panel	Admin panel	Admin panel	Admin panel	Admin panel	Admin panel
ORDER CERTIFICATES DIRECTLY						
Individual certificates:						
30 days	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
1 year	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
2 years	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
3 years	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
Wildcard certificates:						
Wildcard 1 year	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
Wildcard 2 years	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €
Wildcard 3 years	15,00 €	20,00 €	25,00 €	30,00 €	35,00 €	40,00 €

9. From the **Would you like to order with CSR** combo box, select the **Yes, I would like to order with CSR** entry.

PSW GROUP

Telephone support +49 661 480 276 10

SECURITY

SSL Certificates | E-mail Certificates | Code Signing | Become a partner | IT security

SSL Tools | Individual certificates | Multi domain | UC Certificates | Wildcard Certificates | ECC certificates | EV SSL certificates

COMODO Lite (PositiveSSL)

1 General information | 2 Certificate order | 3 Technical order | 4 Accounting/Invoice | 5 Certificate information | 6 Order overview

General information

You can continue the ordering process with a certificate request (CSR) already generated on your server, or you can submit it later.

Please note:
The issuance of your certificate is only possible after the transmission of the CSR!

Our support team will be happy to help you create a certificate request. Book [here](#) our installation service.

Would you like to order with CSR?

Yes, I would like to order with CSR

No, I am going to get a CSR at a later date

Your selection

COMODO
Lite (PositiveSSL)

Duration:
1 year

Payment:
Purchase on account

Price: 15,00 €
(including 19% VAT)

Note for UK: →

10. Paste the text from the CSR you created above.



The screenshot shows the PSW GROUP web interface. At the top, there is a header with the PSW GROUP logo, a menu icon, and a phone number +49 661 480 276 10. Below the header, there is a section titled "Problems with your certificate request? Check your CSR here". The main content area is divided into two columns. The left column contains a large text area labeled "CSR" where the generated CSR text is pasted. A red arrow points to this text area. The right column contains a form with fields for "CN", "OU", "OU", "OU", "OU", and "OU", each with a dropdown menu. Below the form, there is a "CONTINUE" button. At the bottom of the page, there is a note: "The order is only sent to us by clicking on the button 'Buy' in step 6 of the ordering process".

11. Select **Tomcat** from the Server software combo box.



The screenshot shows the PSW GROUP web interface. At the top, there is a header with the PSW GROUP logo, a menu icon, and a phone number +49 661 480 276 10. Below the header, there is a section titled "Problems with your certificate request? Check your CSR here". The main content area is divided into two columns. The left column contains a large text area labeled "CSR" where the generated CSR text is pasted. The right column contains a form with fields for "CN", "OU", "OU", "OU", "OU", and "OU", each with a dropdown menu. Below the form, there is a "CONTINUE" button. At the bottom of the page, there is a note: "The order is only sent to us by clicking on the button 'Buy' in step 6 of the ordering process".

14. We will spare you my data as you are more than capable of following the COMODO Lite Positive SSL registration wizard. Click the green **Paying Order** button to order your SSL cert.

The screenshot shows the COMODO Lite Positive SSL registration wizard. At the top, there is a header with the COMODO logo, a menu icon, and a phone number +49 661 480 276 10. Below the header, there is a section for 'Billing address' with the following details: Name: Technology, Company: Technology, Street: 12345, City: 12345, Country: 12345, Phone: 1234567890, Fax: 1234567890. There is a 'to change' link next to the address. Below this, there is a section for 'Physical Address' with the following details: Confirmation Address: technology@12345.com, City: 12345, Country: 12345. There is a 'to change' link next to the address. Below this, there is a section for 'Terms and Conditions' with a 'I agree to the general terms and conditions of COMODO Group & Co. AG.' checkbox. There is a 'to change' link next to the terms. At the bottom, there is a green 'Paying Order' button. A red arrow points to the button.

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

- 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.dabcc.com.key`

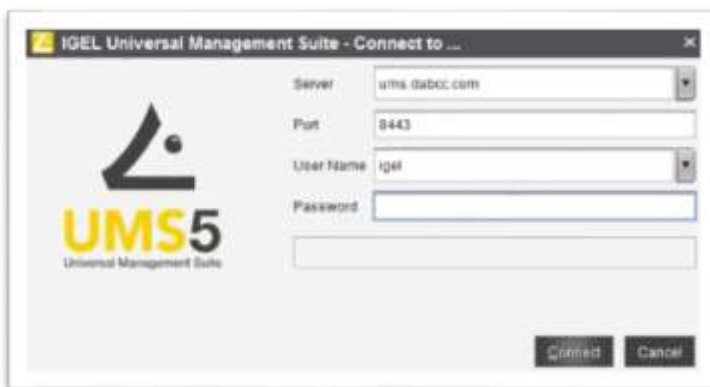
```
ubuntu@ip-172-31-41-112:~$ cat igel-cloud-gateway.dabcc.com.key
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQQGwVJD8xob+jVj
GohiQac9rnxsSQeORii0qKVOTOivYpKyslgj7Ee+JWPib2/t2BeRj88ZDIN70EpD
fEJp8lNrgENeFPyRuz2AvYNNnjAKzMF/LlYQWBrzZq408ma8OeWWIUXWZ49P+m
S4BDji7DrErSc6f0Nj1R2PG1JiYXa2qQnvB094ABhObXlmoXIjOgl8cp3BWZwpX
NwtBHFUkqVAa7m8/KkG9vite1UEWqrYMTudKn+BkNqv13E4Zu82n0erhmLBglGiO
eAL+ryFfql07Dfbxgw2UqUKxB9amxs14GbU86ws8n3l9L+3xh95TWLmgZAu1H1S
Og+HvYBxAgMBAEECggEAAZ4foK9YV0aGaEae0h3Afh7fORDHAW+Ob2MPsZ98QqxI3
IXAxxqu3q0qasZuquEAp9r7sZ+Xmz6XuKT0e80UxQvwrG2TfM6JPJTKSpOnTqKyG
YRWqDljvuvf8sm5Px/c8qnlmgYNpNaqIxuNEqOLpI2o4/su77w+aS4SggMB4RU9
lox4NfLpTlWuqp7lY4qL4mQ00pTtTx0/d0XdxLMTLreJ5V0UPexyen0t5vImDSU
yl4q0mZouz3nSfNYhy1HU7FY5lDrMj4qBcX1EnufVJl9de7DP6NQBdC1Vz+IOyzH
```

- 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 cert.txt. You import it into the UMS soon.

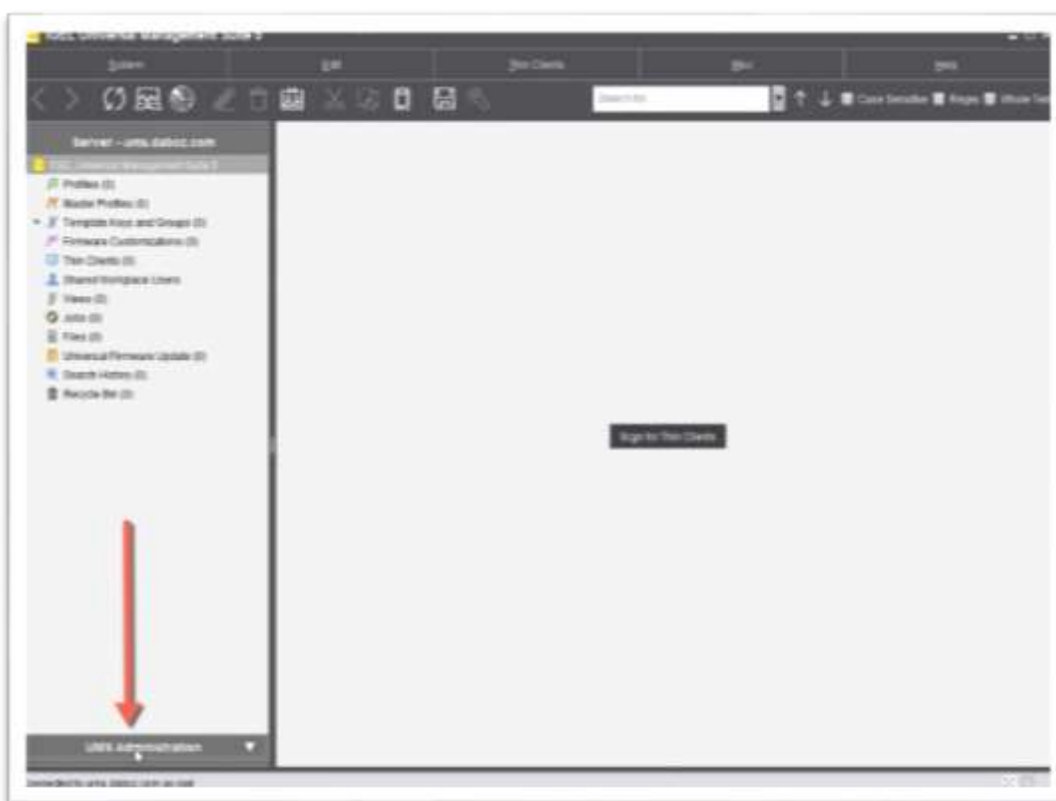


```
c - Notepad
File Edit Format View Help
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCwggSjAgEAAoIBAQQGwVJD8xob+jVj
GohiQac9rnxsSQeORii0qKVOTOivYpKyslgj7Ee+JWPib2/t2BeRj88ZDIN70EpD
fEJp8lNrgENeFPyRuz2AvYNNnjAKzMF/LlYQWBrzZq408ma8OeWWIUXWZ49P+m
S4BDji7DrErSc6f0Nj1R2PG1JiYXa2qQnvB094ABhObXlmoXIjOgl8cp3BWZwpX
NwtBHFUkqVAa7m8/KkG9vite1UEWqrYMTudKn+BkNqv13E4Zu82n0erhmLBglGiO
eAL+ryFfql07Dfbxgw2UqUKxB9amxs14GbU86ws8n3l9L+3xh95TWLmgZAu1H1S
Og+HvYBxAgMBAEECggEAAZ4foK9YV0aGaEae0h3Afh7fORDHAW+Ob2MPsZ98QqxI3
IXAxxqu3q0qasZuquEAp9r7sZ+Xmz6XuKT0e80UxQvwrG2TfM6JPJTKSpOnTqKyG
YRWqDljvuvf8sm5Px/c8qnlmgYNpNaqIxuNEqOLpI2o4/su77w+aS4SggMB4RU9
lox4NfLpTlWuqp7lY4qL4mQ00pTtTx0/d0XdxLMTLreJ5V0UPexyen0t5vImDSU
yl4q0mZouz3nSfNYhy1HU7FY5lDrMj4qBcX1EnufVJl9de7DP6NQBdC1Vz+IOyzH
-----END PRIVATE KEY-----
```

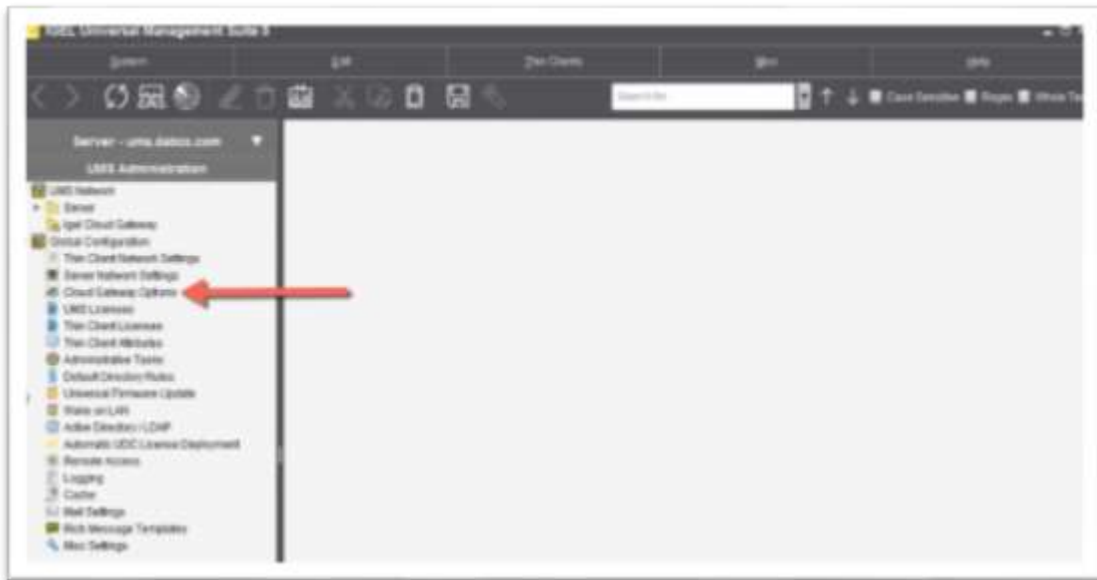

- From the UMS server's desktop, double-click the UMS shortcut and log in.



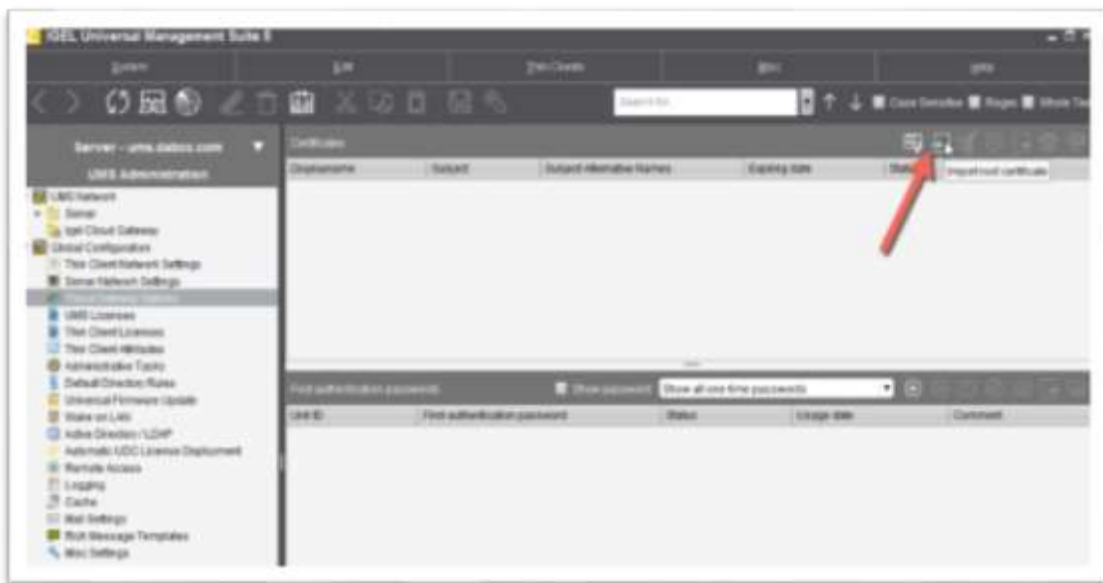
- Click to select the **UMS Administration** link at the bottom of the left menu.



- Click the **Cloud Gateway Options** link in the left menu,

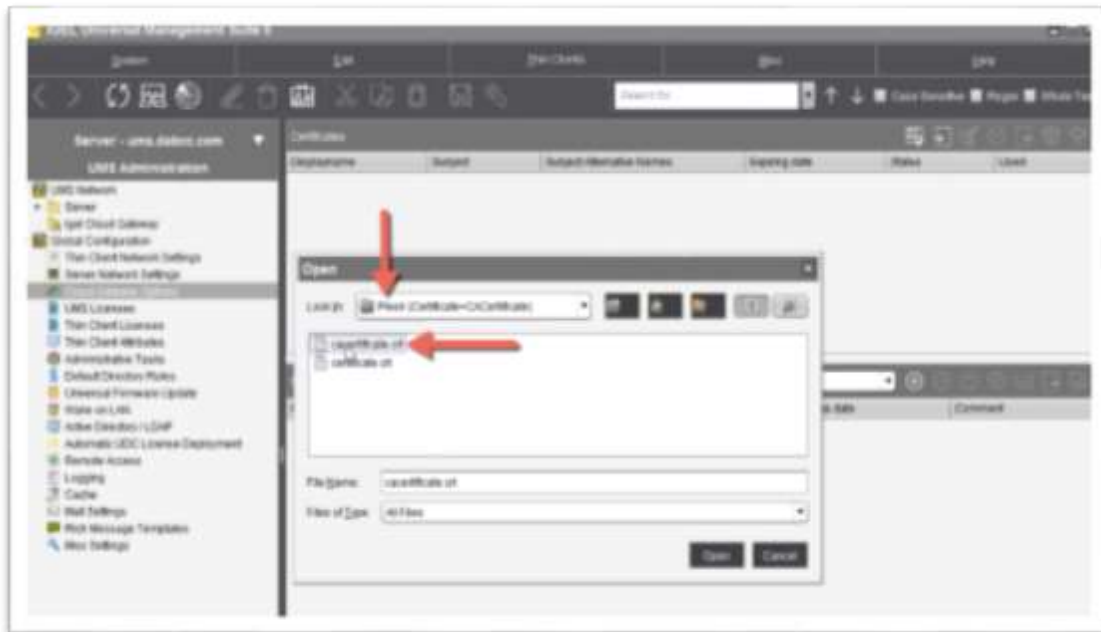


- You are ready to import the public certificate and private key for the cert.
Click the **Import root certificate** button on the top right of the UMS menu bar.

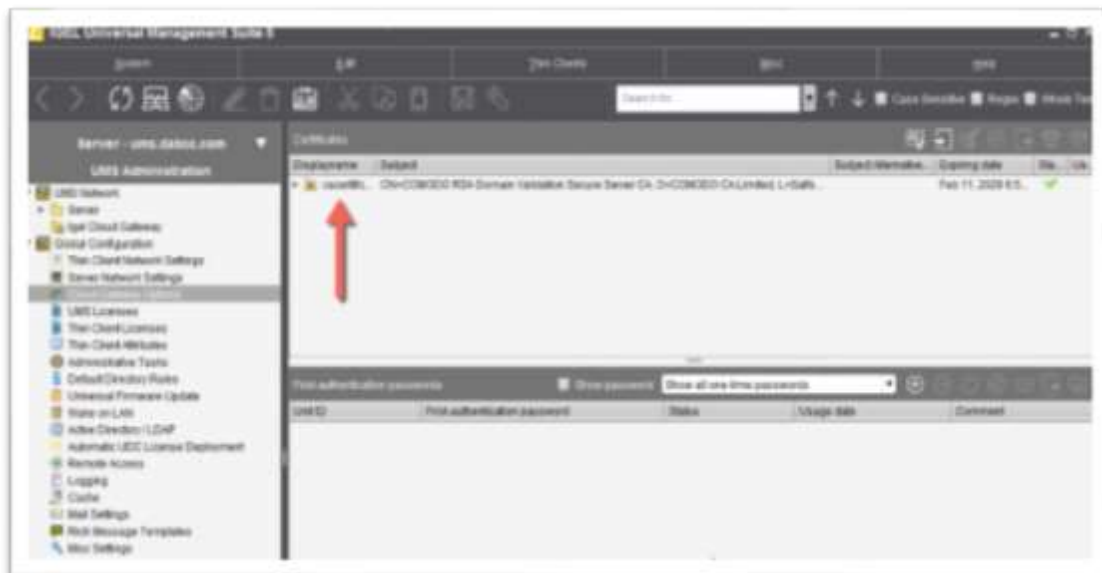


8. You are prompted to select the certificate file you received via email. Browse to the location of the .crt file, select the certificate and click the **Open** button to continue.

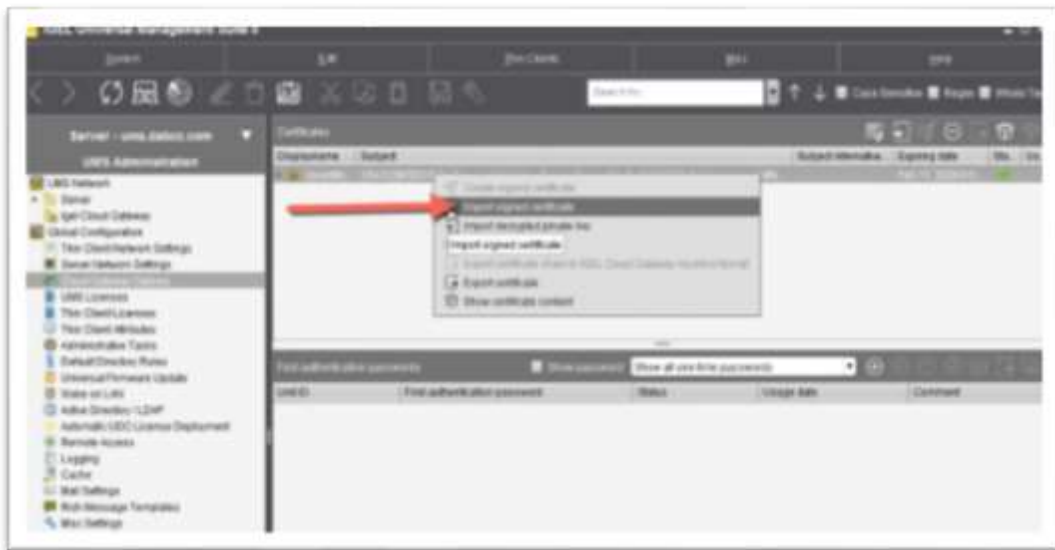
If you received your certificate from pw.net, use the **Certificate.crt** file located in the **Plesk (Certificate_CA Certificate)** folder of the unzipped certificates.zip file you received above.



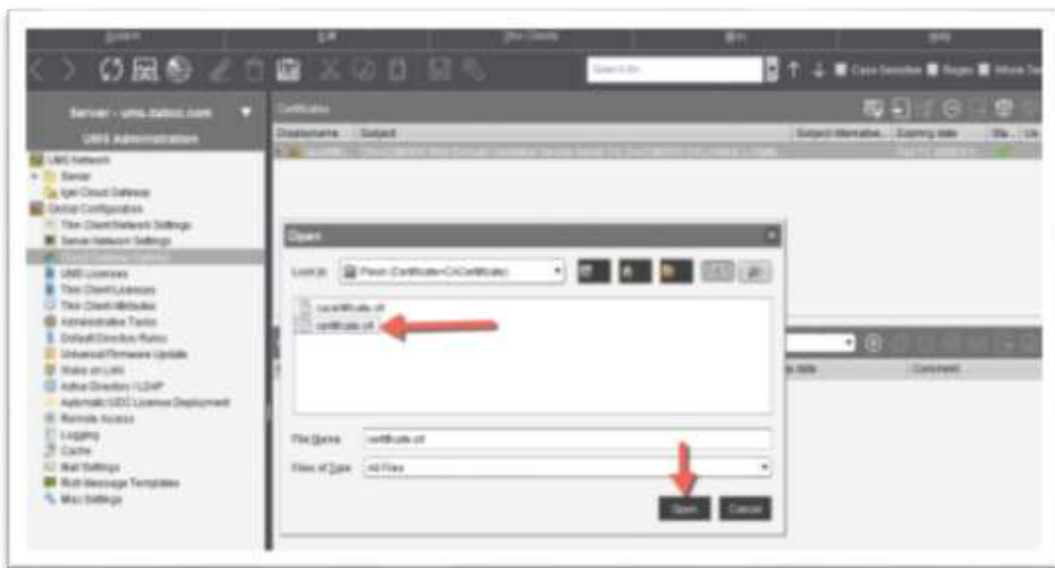
9. The certificate is imported and added to the list of ICG certificates.



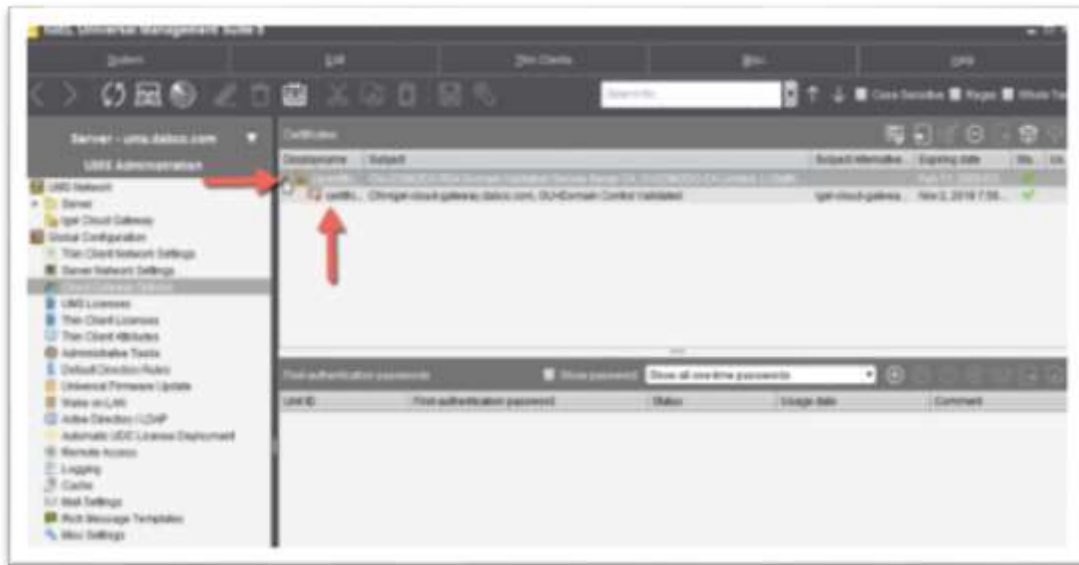
10. Right-click on the newly added certificate and click the **Import signed certificate** entry.



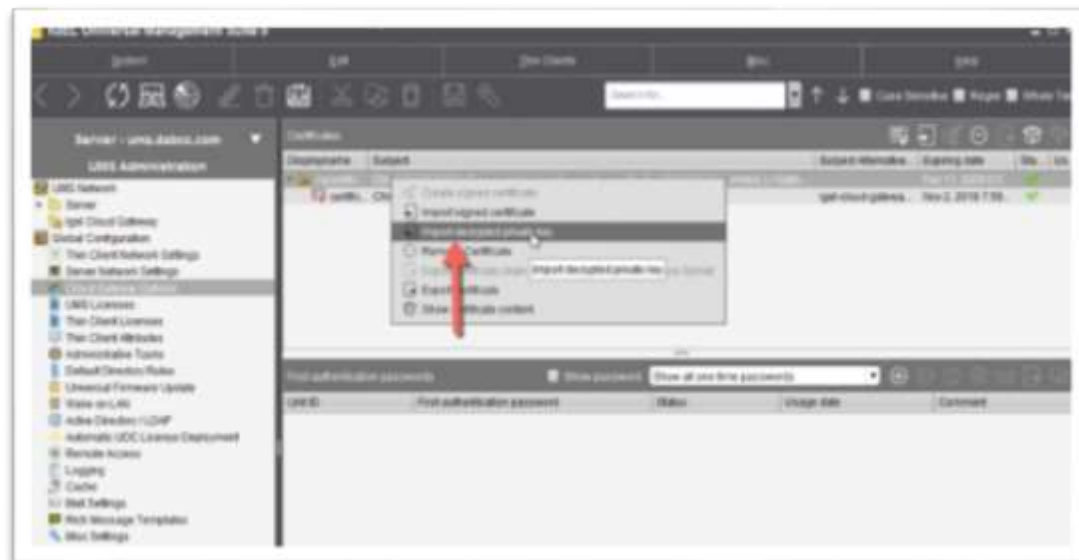
11. Browse to the location of the **.crt** file, select the certificate and click the **Open** button to continue.



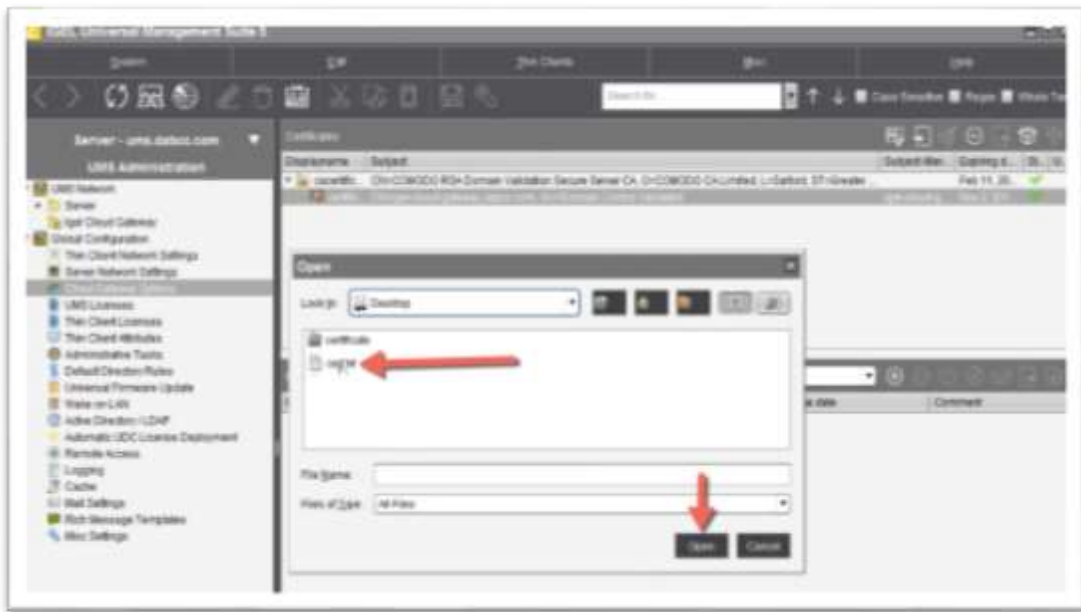
12. You should see your new SSL certificate listed.



13. Right-click on the newly added certificate, this time click the **Import decrypted private key entry**.



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

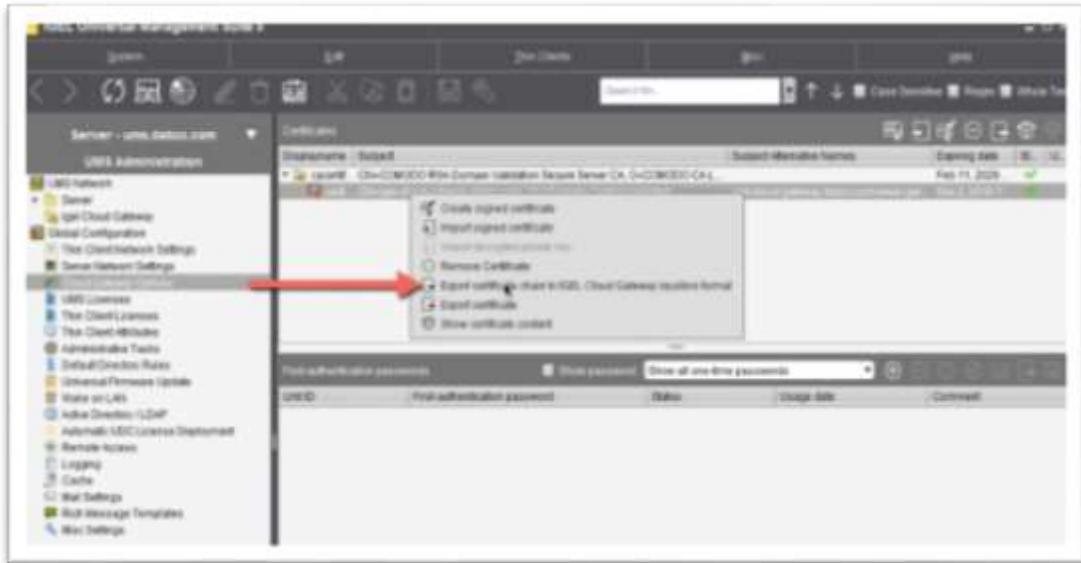


15. If all goes as expected, you are prompted that your private key was imported successfully!
Click the **OK** button to continue.

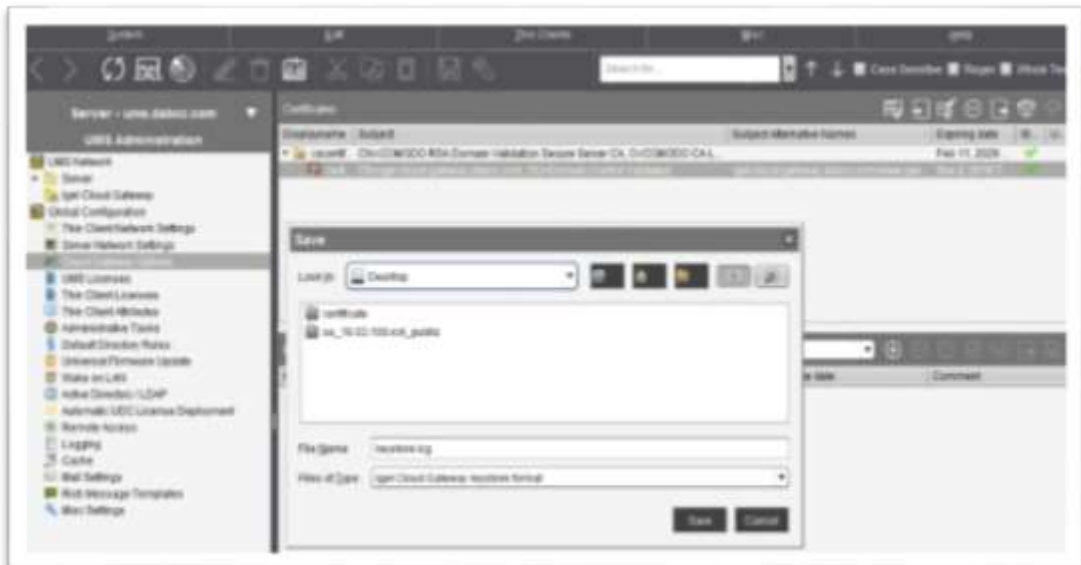


16. You have imported the certificate delivered to you from the public CA and imported the private key for your certificate that allows the UMS to create the key store files for the IGEL Cloud Gateway.

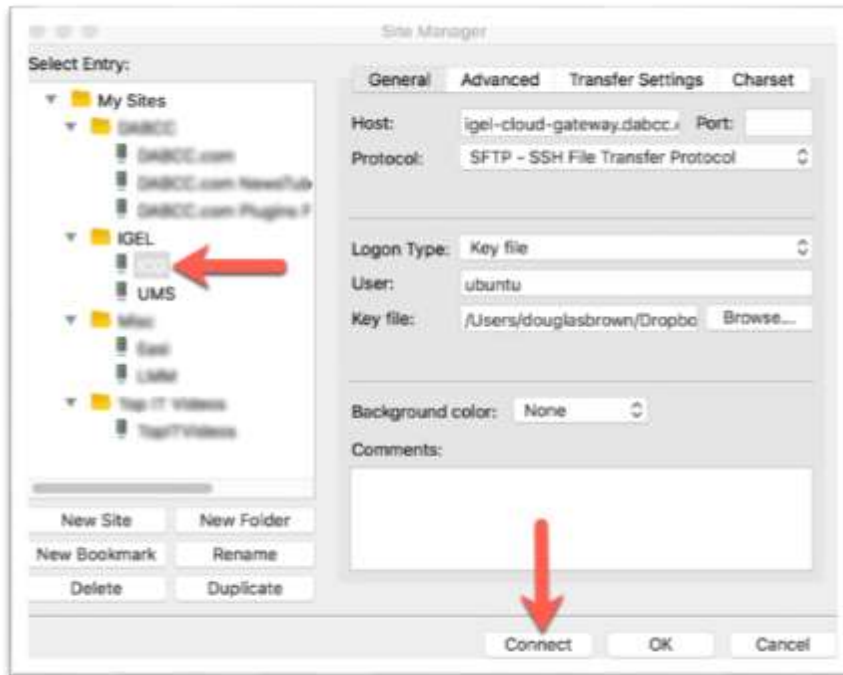
Click the **Export certificate chain to IGEL Cloud Gateway keystore format** entry.



17. Save the file to a location of your choosing.

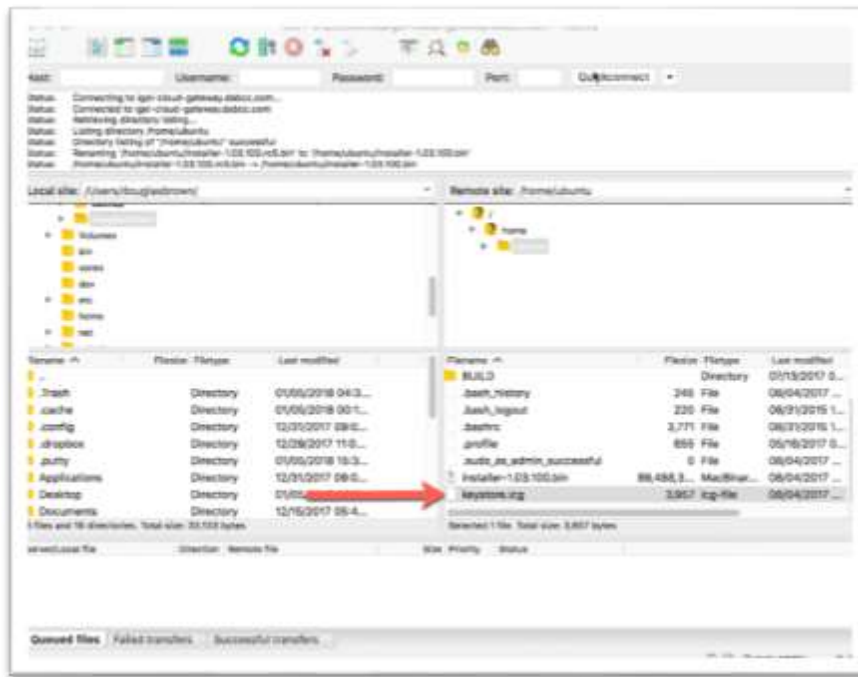


18. Open **FileZilla** and connect to the ICG server.



19. Drag and drop the **keystore.icg** file you downloaded above to the root of the ICG server.

If all goes well, you see the **keystore.icg** file located in the file list.



4. 8. How to Install the IGEL ICG Software


The environment is set up, signed and ready for you to finally install the IGEL Cloud Gateway software onto your new ICG AWS instance.

The following details how to install the ICG software:

1. The first step is to create an SSH connection to the ICG's server. Open your favorite Terminal software and connect to your ICG's AWS instance.

Type the following:

```
ssh igel-cloud-gateway.<yourdomain.com> -i igel.pem -l
ubuntu
```



```
Last login: Fri Aug  4 12:51:55 on ttys001
douglass-mbp:~ dbrown$ cd dropbox
douglass-mbp:igel dbrown$ ssh igel-cloud-gateway.dabcc.com -i igel.pem -l ubuntu
```

2. Type **yes** and hit **enter** to continue.



```
Last login: Fri Aug  4 12:51:55 on ttys001
douglass-mbp:~ dbrown$ cd dropbox
douglass-mbp:igel dbrown$ ssh igel-cloud-gateway.dabcc.com -i igel.pem -l ubuntu
The authenticity of host 'igel-cloud-gateway.dabcc.com (52.28.218.220)' can't be established.
ECDSA key fingerprint is SHA256:S4C/E8yZgu/zQk171L/rFLG5Gri80TPdo/FKjmYkgo8.
Are you sure you want to continue connecting (yes/no)?
```

3. You are logged in to the ICG terminal.

```
The authenticity of host 'igel-cloud-gateway.dabcc.com (52.28.218.220)' can't be established.
ECDSA key fingerprint is SHA256:S4C/E8yZgu/zQkl71L/rFLG5Gri80TPdo/FKjmYkgo8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'igel-cloud-gateway.dabcc.com,52.28.218.220' (ECDSA) to the list of
known hosts.
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1022-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-43-99:~$
```

4. It is always important to update your servers with the latest updates, fixes, and security patches.

Type the following:

```
sudo apt-get update
```

```
The authenticity of host 'igel-cloud-gateway.dabcc.com (52.28.218.220)' can't be established.
ECDSA key fingerprint is SHA256:S4C/E8yZgu/zQkl71L/rFLG5Gri80TPdo/FKjmYkgo8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'igel-cloud-gateway.dabcc.com,52.28.218.220' (ECDSA) to the list of
known hosts.
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.4.0-1022-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

0 packages can be updated.
0 updates are security updates.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-43-99:~$ sudo apt-get update
```

- Next, you upgrade the server components.

Type the following:

```
sudo apt-get upgrade
```

```
,232 B]
Get:13 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [
598 kB]
Get:14 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/main Translation-en [
241 kB]
Get:15 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 Packag
es [512 kB]
Get:16 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/universe Translation-
en [199 kB]
Get:17 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/multiverse amd64 Pack
ages [15.5 kB]
Get:18 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-updates/multiverse Translatio
n-en [7,540 B]
Get:19 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-backports/main Sources [3,312
B]
Get:20 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-backports/universe Sources [4
,400 B]
Get:21 http://eu-central-1.ec2.archive.ubuntu.com/ubuntu xenial-backports/universe amd64 Pack
ages [5,804 B]
Get:22 http://security.ubuntu.com/ubuntu xenial-security/main Sources [84.3 kB]
Get:23 http://security.ubuntu.com/ubuntu xenial-security/restricted Sources [2,604 B]
Get:24 http://security.ubuntu.com/ubuntu xenial-security/universe Sources [37.4 kB]
Get:25 http://security.ubuntu.com/ubuntu xenial-security/multiverse Sources [1,144 B]
Get:26 http://security.ubuntu.com/ubuntu xenial-security/main amd64 Packages [323 kB]
Get:27 http://security.ubuntu.com/ubuntu xenial-security/main Translation-en [137 kB]
Get:28 http://security.ubuntu.com/ubuntu xenial-security/universe amd64 Packages [152 kB]
Get:29 http://security.ubuntu.com/ubuntu xenial-security/universe Translation-en [77.9 kB]
Fetched 11.9 MB in 2s (5,259 kB/s)
Reading package lists... Done
ubuntu@ip-172-31-43-99:~$ sudo apt-get upgrade
```

- If all goes well, the updates are applied, and you should see a happy screen like the one below.

```
Processing triggers for ureadahead (0.100.0-19) ...
Setting up libapt-inst2.0:amd64 (1.2.24) ...
Setting up apt-utils (1.2.24) ...
Setting up grub-common (2.02-beta2-36ubuntu3.12) ...
update-rc.d: warning: start and stop actions are no longer supported; falling back to default
s
Setting up grub2-common (2.02-beta2-36ubuntu3.12) ...
Setting up grub-pc-bin (2.02-beta2-36ubuntu3.12) ...
Setting up grub-pc (2.02-beta2-36ubuntu3.12) ...
Installing for i386-pc platform.
Installation finished. No error reported.
Generating grub configuration file ...
Found linux image: /boot/vmlinuz-4.4.0-1022-aws
Found initrd image: /boot/initrd.img-4.4.0-1022-aws
done
Setting up open-iscsi (2.0.873+git0.3b4b4500-14ubuntu3.4) ...
Setting up kmod (22-1ubuntu5) ...
Setting up sudo (1.8.16-0ubuntu1.5) ...
Setting up apt-transport-https (1.2.24) ...
Setting up libdrm2:amd64 (2.4.76-1-ubuntu16.04.1) ...
Setting up unattended-upgrades (0.90ubuntu0.7) ...
Setting up python3-distupgrade (1:16.04.22) ...
Setting up python3-update-manager (1:16.04.7) ...
Setting up ubuntu-release-upgrader-core (1:16.04.22) ...
Setting up update-manager-core (1:16.04.7) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for initramfs-tools (0.122ubuntu8.8) ...
update-initramfs: Generating /boot/initrd.img-4.4.0-1022-aws
W: mdadm: /etc/mdadm/mdadm.conf defines no arrays.
ubuntu@ip-172-31-43-99:~$
```

7. You are ready to install the ICG software. The first step is to make the ICG install binary file executable. Type the following:

```
chmod a+x installer-1.03.100.bin
```

```
ubuntu@ip-172-31-43-99:~$ chmod a+x installer-1.03.100.bin
```

8. Install the ICG software! Type the following:

```
sudo ./installer-1.03.100.bin keystore.icg
```

```
ubuntu@ip-172-31-43-99:~$ sudo ./installer-1.03.100.bin keystore.icg
```

9. If you receive the following error message notifying you of missing packages, don't fret, you fix it in the next step.

If you did not receive the below error message, please skip to step 12.

```
Some packages are missing: dialog super unzip realpath. Please install them first
For logging messages see /var/log/icg_install.log
ubuntu@ip-172-31-43-99:~$
```

10. To fix this issue, all you need to do is install the missing packages. Type the following:

```
sudo apt-get install dialog super unzip realpath
```

```
Some packages are missing: dialog super unzip realpath. Please install them first
For logging messages see /var/log/icg_install.log
ubuntu@ip-172-31-43-99:~$ sudo apt-get install
```

```
ubuntu@ip-172-31-43-99:~$ sudo apt-get install dialog super unzip realpath
```

The OS communicates with the central software repository to install the missing files.

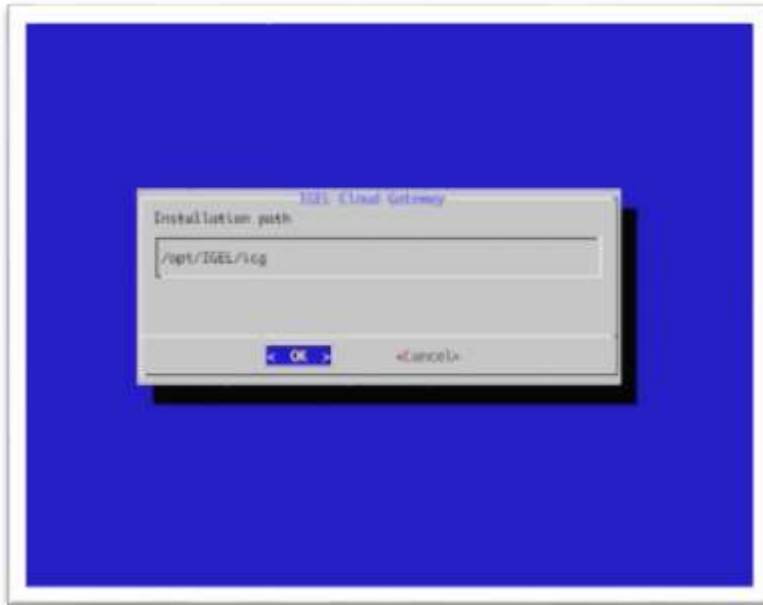
```
Unpacking unzip (6.0-2ubuntu1) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for mime-support (3.59ubuntu1) ...
Setting up dialog (1.3-20160209-1) ...
Setting up realpath (8.25-2ubuntu3~16.04) ...
Setting up super (3.30.0-7) ...
Setting up unzip (6.0-2ubuntu1) ...
ubuntu@ip-172-31-43-99:~$
```

11. Let's try installing ICG again, type the following:

```
sudo ./installer-1.03.100.bin keystore.icg
```

```
ubuntu@ip-172-31-43-99:~$ sudo ./installer-1.03.100.bin keystore.icg
```

12. The IGEL Cloud Gateway install wizard opens. Click the **OK** button to accept the defaults.



13. Enter port **8443** and click the **OK** button



14. The ICG installation program installs the ICG software...

During the ICG Installation, sometimes this screen might echo something like 'CCCCCCCCC'... Don't worry if your installation window is not shown as seen below; the will installation continues fine.



15. If you receive the following message, don't worry. Click **Yes** to continue.

If you do receive this error, it is probably due to the fact you are using a server with only 1 GB RAM. You can ignore it.



16. Once finished, the ICG install wizard closes and you return to the terminal. Verify everything started successfully and be proud. You have an ICG server up and running. However, there is still a bit more configuration required, let's keep going.

```

ener - Code ICGTCS1
Installer log file /var/log/icg_install.log:
'/home/ubuntu/BUILD/resources/uninstall.sh' -> '/opt/IGEL/icg/uninstall.sh'
DBG: Extract tomcat and java
INFO: Configure tomcat...
DBG: Copy keystore from /tmp/icg/keystore.jks to /opt/IGEL/icg/apache-tomcat-8.0.41/keys/key
store.jks
DBG: Try to copy /tmp/icg/truststore.jceks truststore to /opt/IGEL/icg/apache-tomcat-8.0.41/co
nf/truststore.jceks
DBG: Create new truststore
DBG: new truststore: f003045edb26c0b9c57562a891679e0e /opt/IGEL/icg/apache-tomcat-8.0.41/co
nf/truststore.jceks

Keystore type: JCEKS
Keystore provider: SunJCE

Your keystore contains 0 entries

DBG: Create new USG ID
INFO: Success!\nStarting tomcat...
Synchronizing state of tomcat.service with SysV init with /lib/systemd/systemd-sysv-install..
.
Executing /lib/systemd/systemd-sysv-install enable tomcat
inserv: warning: script 'tomcat' missing LSB tags and overrides
update-rc.d: error: tomcat Default-Start contains no runlevels, aborting.
DBG: Waiting for tomcat: timeout
DBG: Waiting for tomcat: Refresh timeout
INFO: Starting tomcat...
DBG: Tomcat started successfully
ubuntu@ip-172-31-43-99:~$

```


17. It is recommended to verify the ICG Process is running through the Tomcat Daemon (Service). If the Tomcat daemon is not running, it means that your ICG will not work either. To verify you can use the **systemctl status tomcat** command to see if it is running and if not try to restart it with the **systemctl restart tomcat** command.

Type the following to display the status of the Tomcat daemon:

```
systemctl status tomcat
```

Verify the State displays **running**.

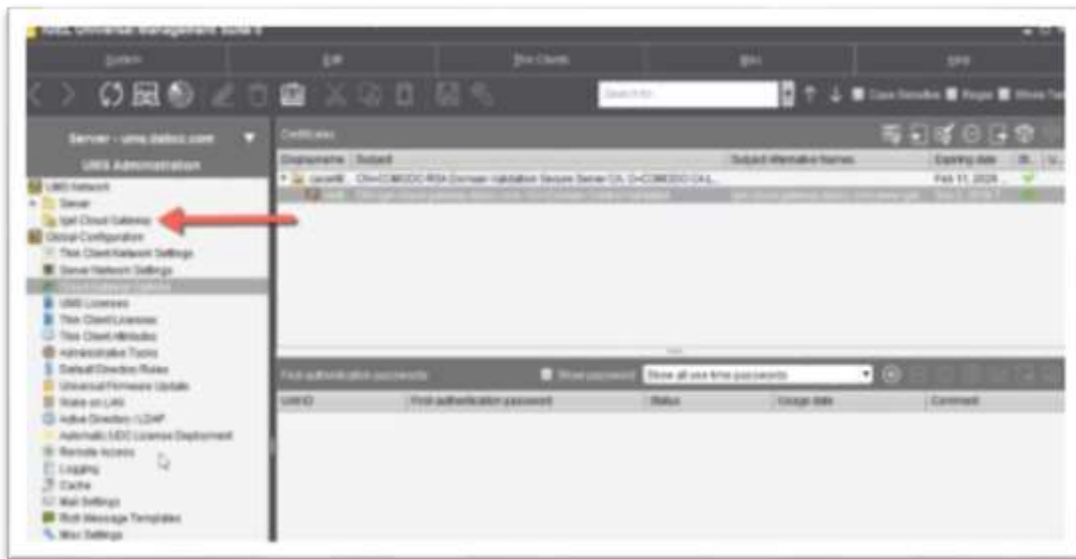
```
ubuntu@ip-172-31-43-99:~$ systemctl status
• ip-172-31-43-99
  State: running
  Jobs: 0 queued
  Failed: 0 units
  Since: Fri 2017-08-04 10:57:15 UTC; 5 months 23 days ago
  CGroup: /
    └─init.scope
      └─1 /sbin/init
    └─system.slice
      └─mdadm.service
        └─1150 /sbin/mdadm --monitor --pid-file /run/mdadm/monitor.pid --
      └─dbus.service
        └─1053 /usr/bin/dbus-daemon --system --address=systemd: --nofork
      └─cron.service
        └─1104 /usr/sbin/cron -f
      └─lvm2-lvm2metad.service
        └─416 /sbin/lvm2metad -f
      └─iscsid.service
        └─16334 /sbin/iscsid
        └─16335 /sbin/iscsid
      └─networking.service
        └─918 /sbin/dhclient -1 -v -pf /run/dhclient.eth0.pid -lf /var/li
      └─accounts-daemon.service
        └─1105 /usr/lib/accountsservice/accounts-daemon
      └─system-serial\x2dgetty.slice
        └─serial-getty@ttyS0.service
          └─1243 /sbin/agetty --keep-baud 115200 38400 9600 ttyS0 vt220
      └─atd.service
        └─1071 /usr/sbin/atd -f
```

18. If the Tomcat state is not running, try to restart it using the following command:

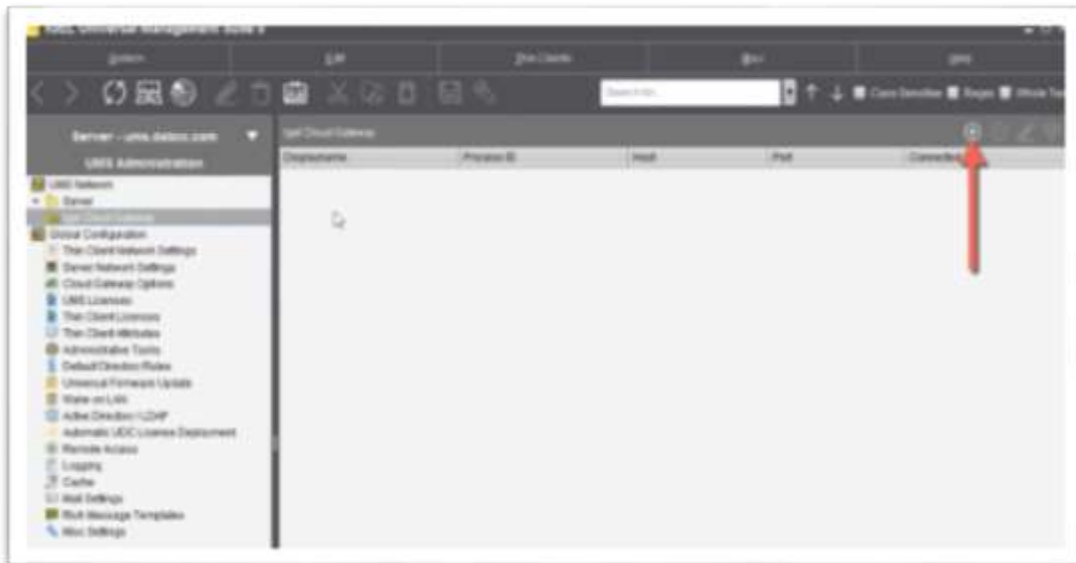
```
systemctl restart tomcat
```

```
ubuntu@ip-172-31-43-99:~$ systemctl restart tomcat
```


19. Open the IGEN UMS. From the **UMS Administration** section click to select the **IGEL Cloud Gateway** node, located at the top of the left menu.



20. Click the + icon to add your ICG server.



21. You receive the following error message as you have yet to install the ICG license.
Click **OK** to continue.



22. The **Connect new IGEL Cloud Gateway** connection window opens. Enter a custom description, host DNS name, and port of 8443.
Click **Connect** to add your ICG server to the UMS.

This is the critical step. If you experience problems, in most cases, it is related to the certificate you imported. Please verify you completed the above steps correctly and try again.



23. If all goes well, you see your ICG server listed. Congratulations, you have successfully installed the IGEL Cloud Gateway. Next step is to license it.



4. 9. How to License the IGEL ICG

Once you receive your ICG license from IGEL, you need to install it.

If you have not applied for your free ICG license yet, please do it now. Email ICGdemo@igel.com and let us know you are reading this document and would like your free ICG license.

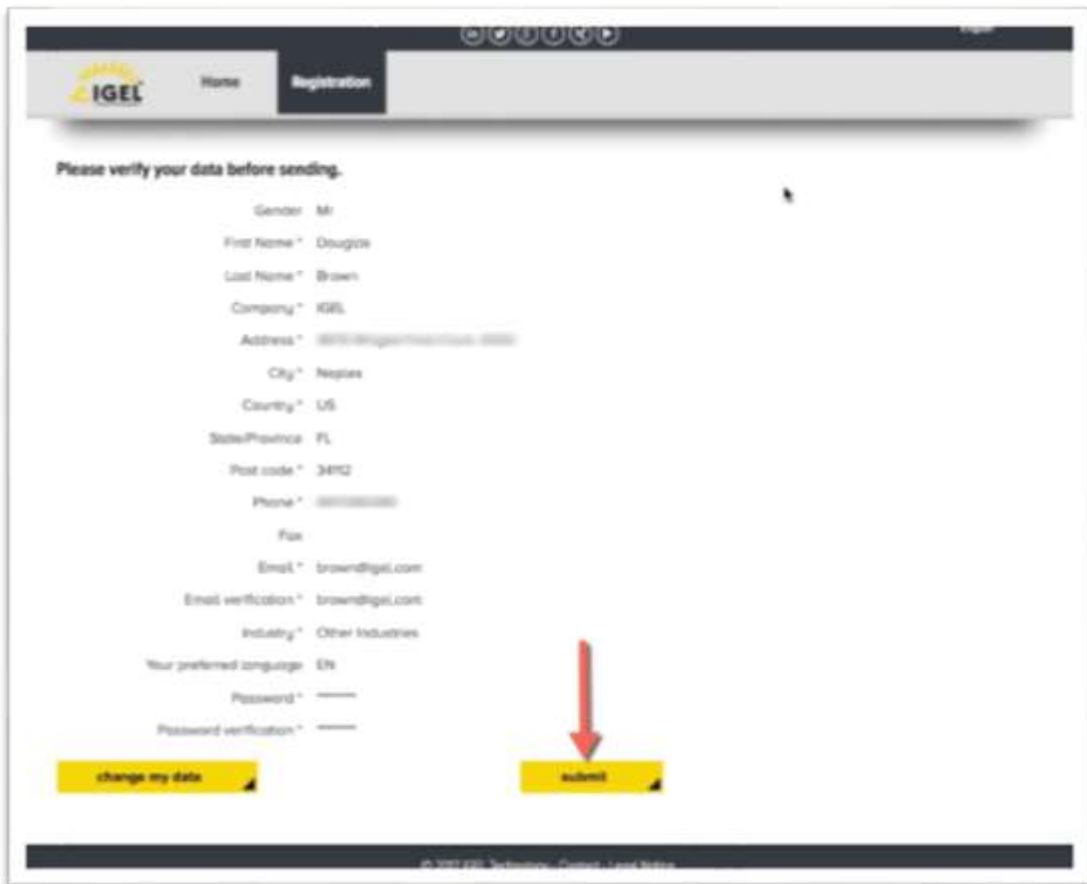
The following details how to license your IGEL ICG server:

1. Once you receive your activation key from IGEL via email, you are required to activate and download the ICG license file into the UMS.

Browse to <http://activation.igel.com/> and click the **Register** button to continue.

2. Enter your bio information, comply with the CAPTCHA and click the **Submit request** button.

3. One last chance, verify all your information is correct and click the **Submit** button to create your account.

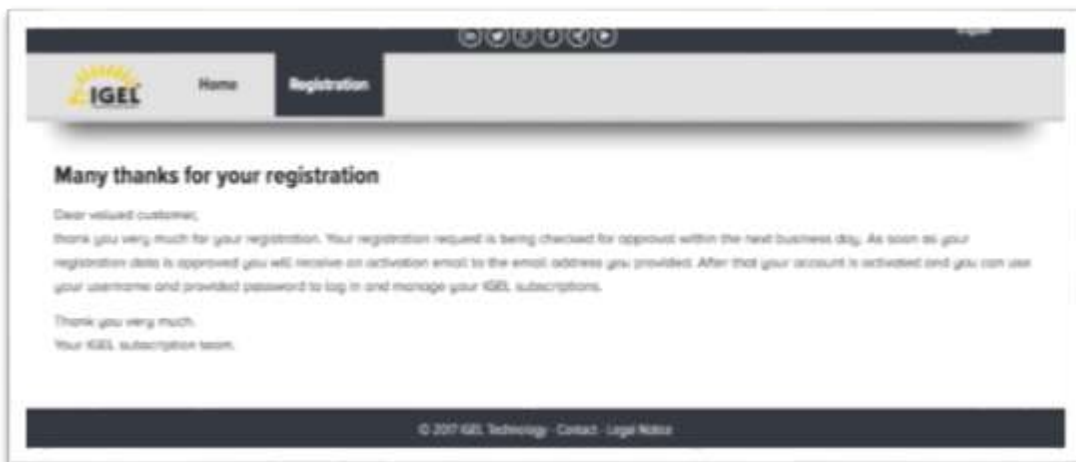


The screenshot shows the IGEL registration page. At the top, there is a navigation bar with the IGEL logo, a 'Home' link, and a 'Registration' link. Below the navigation bar, the text 'Please verify your data before sending.' is displayed. The form contains the following fields and values:

- Gender: Mr
- First Name: Douglas
- Last Name: Brown
- Company: IGEL
- Address: 18750 Douglas Highway - 08801
- City: Naples
- Country: US
- State/Province: FL
- Post code: 34112
- Phone: (813) 233-1111
- Fax:
- Email: brown@igel.com
- Email verification: brown@igel.com
- Industry: Other Industries
- Your preferred language: EN
- Password: [redacted]
- Password verification: [redacted]

At the bottom of the form, there are two buttons: 'change my data' and 'submit'. A red arrow points to the 'submit' button. The footer of the page contains the text '© 2017 IGEL Technology - Contact - Legal Notice'.

4. Your request is processed, and you will receive an email with your login information. This process is automated but might take up to an hour, in most cases.



The screenshot shows the IGEL registration confirmation page. At the top, there is a navigation bar with the IGEL logo, a 'Home' link, and a 'Registration' link. Below the navigation bar, the text 'Many thanks for your registration' is displayed. The page contains the following text:

Dear valued customer,

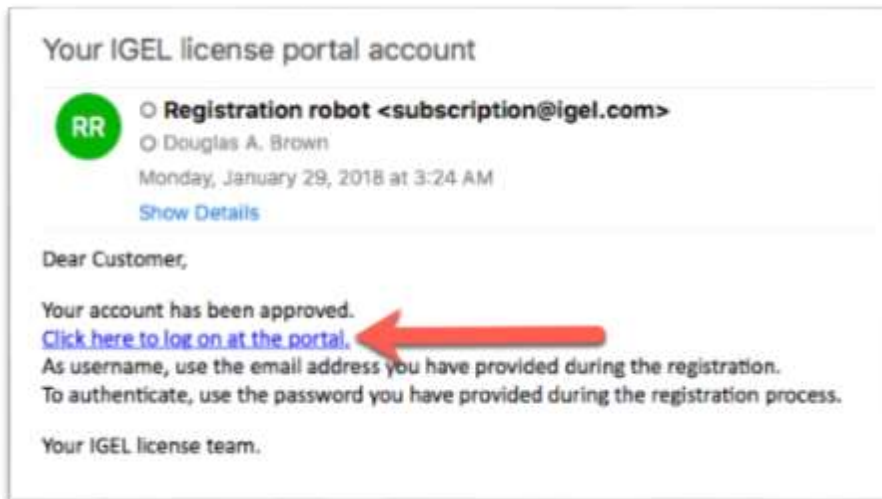
Thank you very much for your registration. Your registration request is being checked for approval within the next business day. As soon as your registration data is approved you will receive an activation email to the email address you provided. After that your account is activated and you can use your username and provided password to log in and manage your IGEL subscriptions.

Thank you very much.

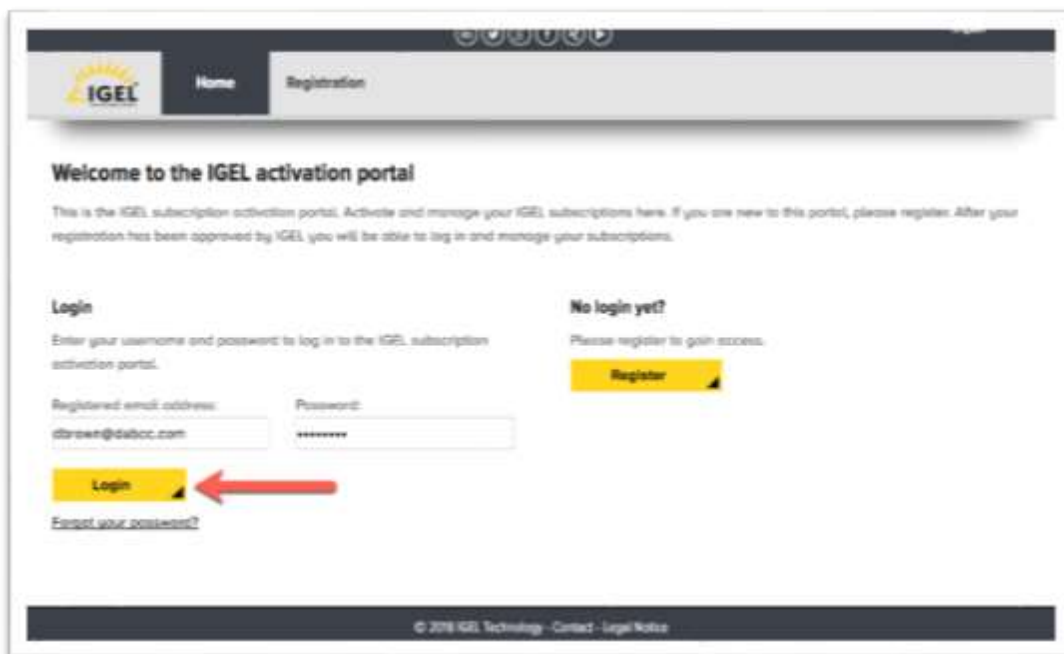
Your IGEL subscription team.

The footer of the page contains the text '© 2017 IGEL Technology - Contact - Legal Notice'.

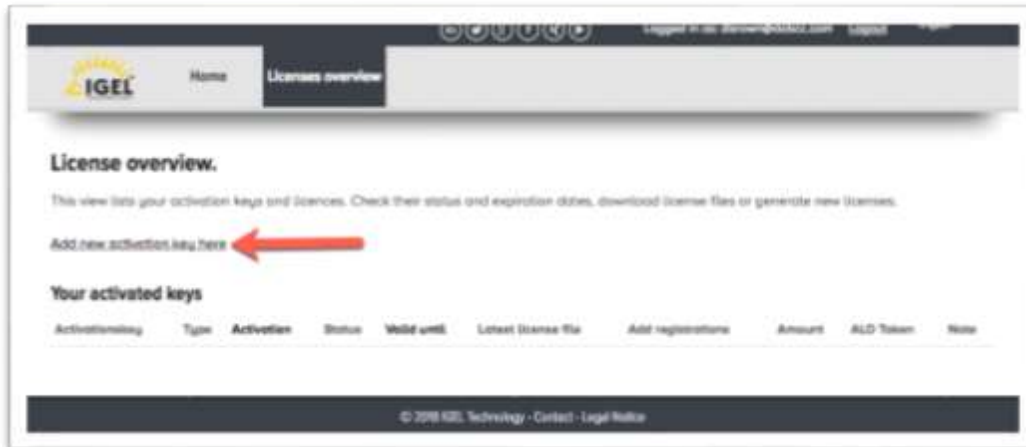
- Once you receive the email from the IGEL Activation Portal that your account has been created successfully, click on the link in the email to log on to the portal.



- Log in to the IGEL activation portal using the username and password you configured above. Click the **Login** button to log on.



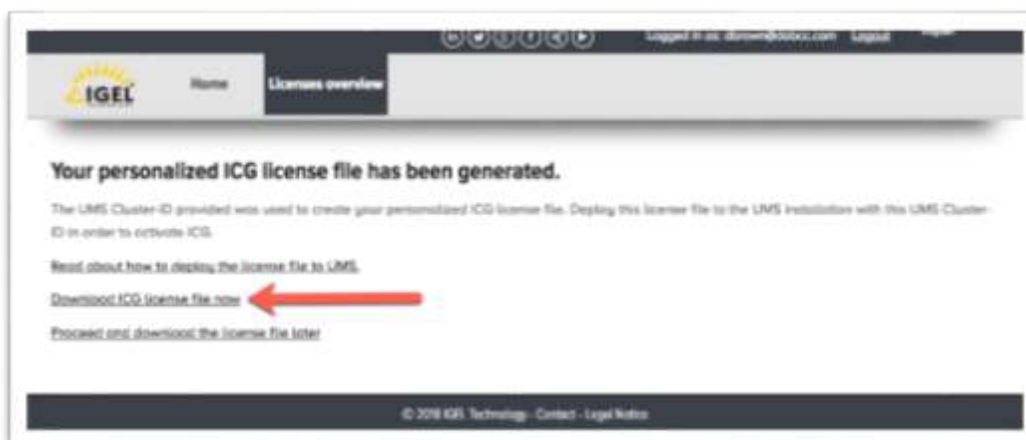
7. Once logged in, you are presented with the License overview screen. You need to add your license. Click the **Add new activation key here** link.



8. Enter the **Activation Key** you received from IGEL via email. Click the **Submit** button.



9. Click the **Download ICG license file now** link to download the license file that you import into the UMS in the coming steps.



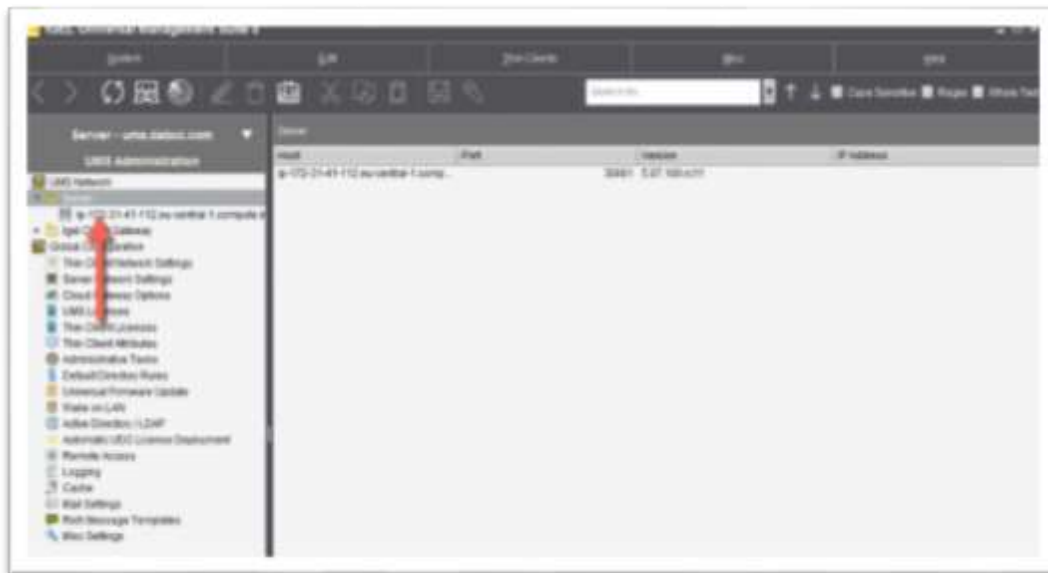
10. Find your newly added license in **Your activated keys** section and click the **register add licenses** link.



11. To create the ICG license, you need to obtain the **Cluster ID** of your UMS server. You retrieve the Cluster ID from the UMS. Minimize your browser and flip back to the UMS console.

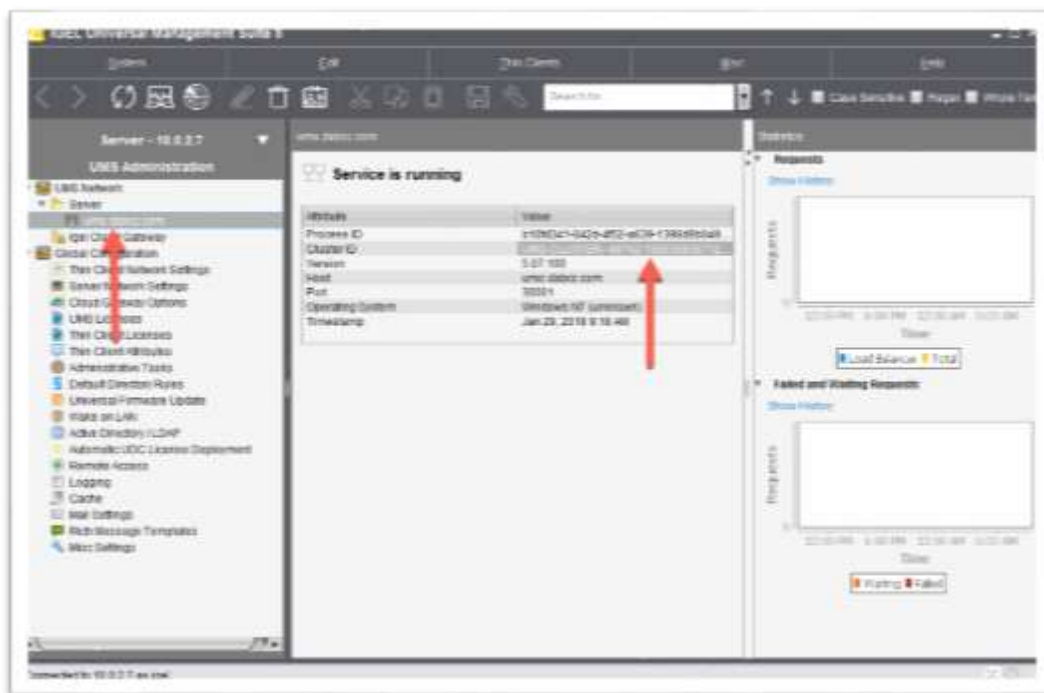


12. Click to expand the **Server** node, located in the left menu. Click to select your UMS server from the list.



13. The UMS information is presented to you along with the status and a few stats about the performance of your instance.

Although, you are only interested in one thing, the **Cluster ID**. Find your Cluster ID, highlight it and copy it to your clipboard using Control C. It is used it to create your license file in a few steps.



14. Click on the **Cluster ID** and hit CTRL C on your keyboard to and copy it to your notes. You need this when activating your license.

Attribute	Value
Process ID	24bb3ec8-23a5-44ed-a96b-c97fb500...
Cluster ID	UMS-CLUSTER-44857-15017858152
Version	5.07.100.m.1
Host	ip-172-31-12.eu-central-1.comput...
Port	30001
Operating System	Linux
Timestamp	Aug 4, 2017 7:19 AM

15. Once you have entered your activation key, you are prompted to associate it with a UIMS server. To do this, you use the Client ID you just copied to your clipboard above.

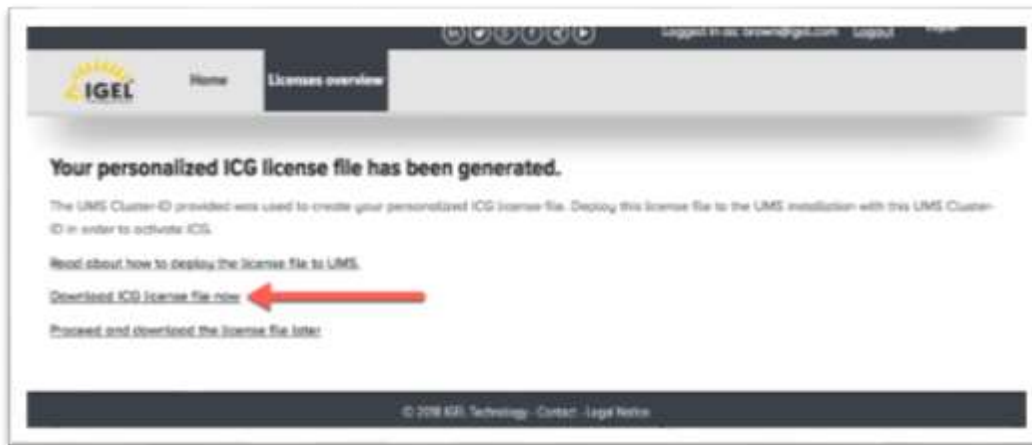
Paste the **UMS Cluster ID** into the **Enter your UMS Cluster ID** text box and click the **Submit** button.

Be careful that the double dash in the middle was not changed to a big dash

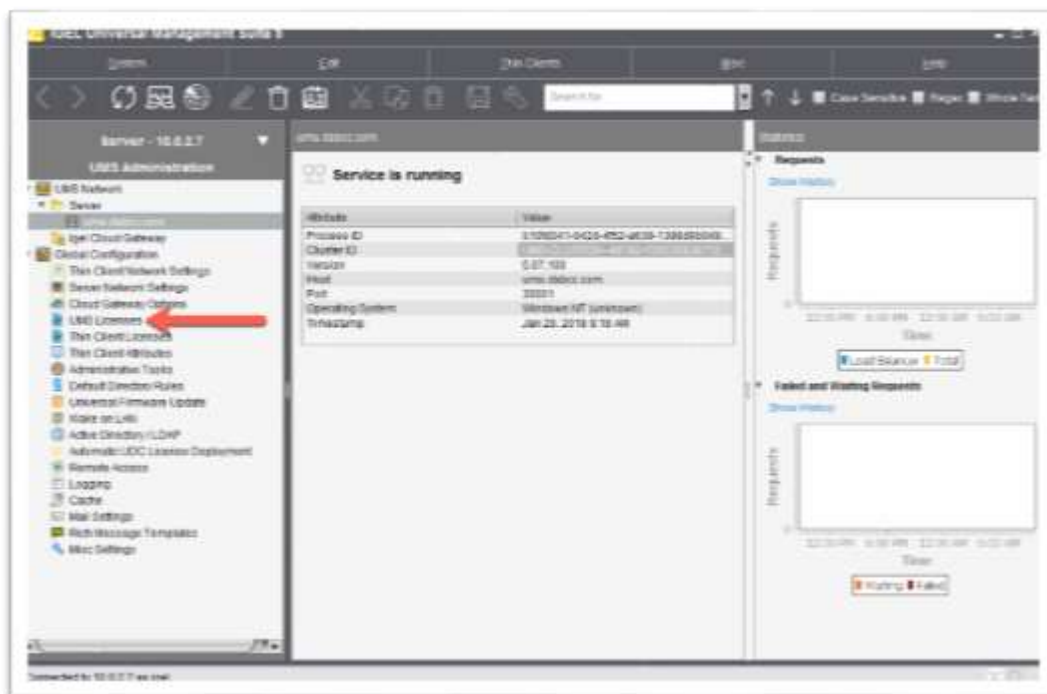
The screenshot shows the IGEL 'Licenses overview' page. The main heading is 'Activate the ICG subscription for your UMS installation'. Below this, there is instructional text: 'You need to provide the UMS Cluster-ID in order to generate an ICG-subscription license file, as the license will be tied to your UMS installation or cluster. Read here about how to find your UMS Cluster-ID. Make sure to enter the correct UMS Cluster-ID. The ID is case sensitive and cannot be modified later.' There is a text input field labeled 'Enter your UMS Cluster-ID:' and a yellow 'Submit' button. The footer of the page reads '© 2016 IGEL Technology - Contact - Legal Notice'.

16. The license file is issued, you can download the ICG License file now.

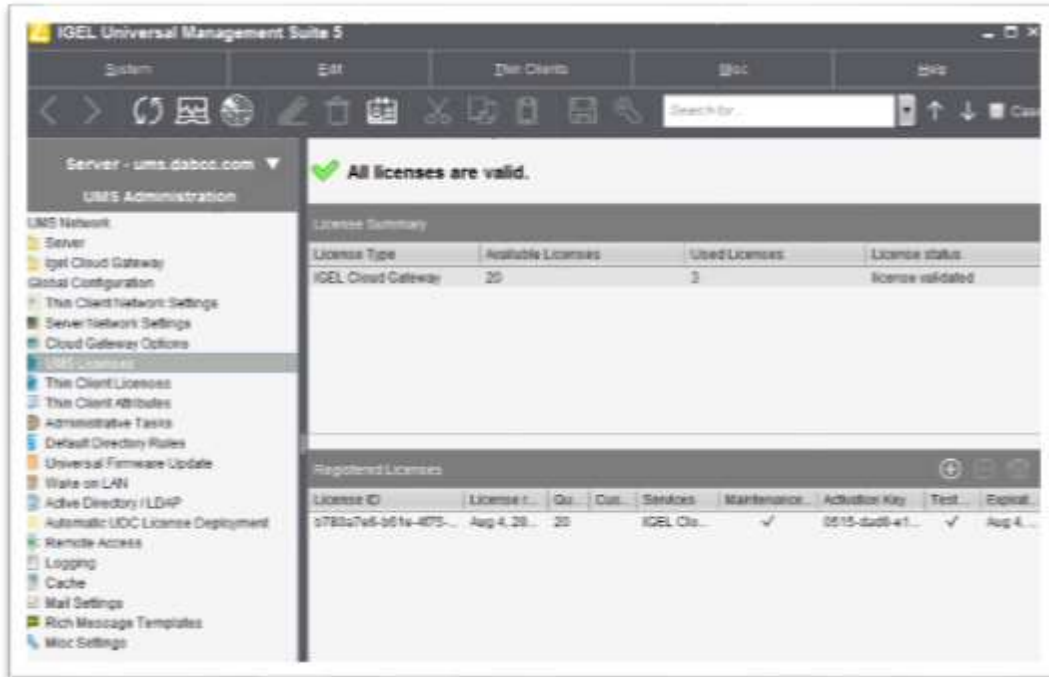
Click the **Download ICG license file now** link.



17. Return to the UMS and click the **UMS Licenses** node from the left menu.

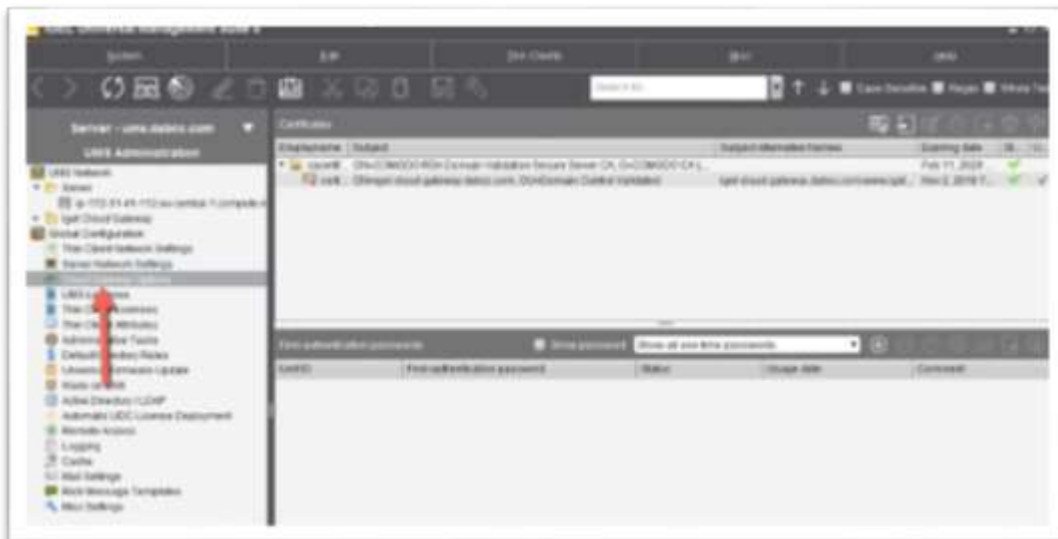


20. Yippee! All licenses are valid! You are almost there!

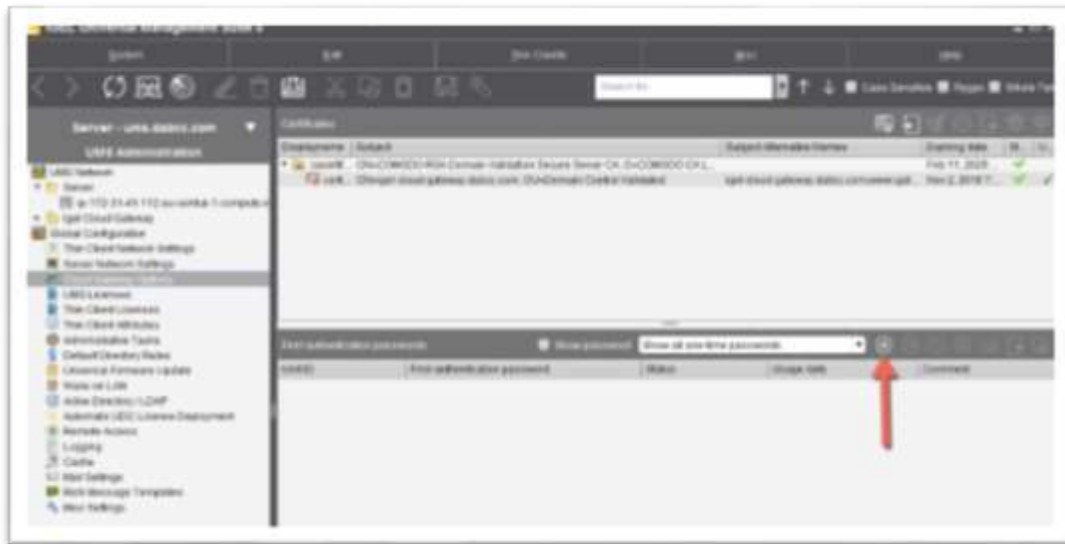


21. You need to assign a password to your ICG server. This password is used by end-users when registering their new IGEL OS to the UMS via the ICG.

Click the **Cloud Gateway Options** node in the left menu.

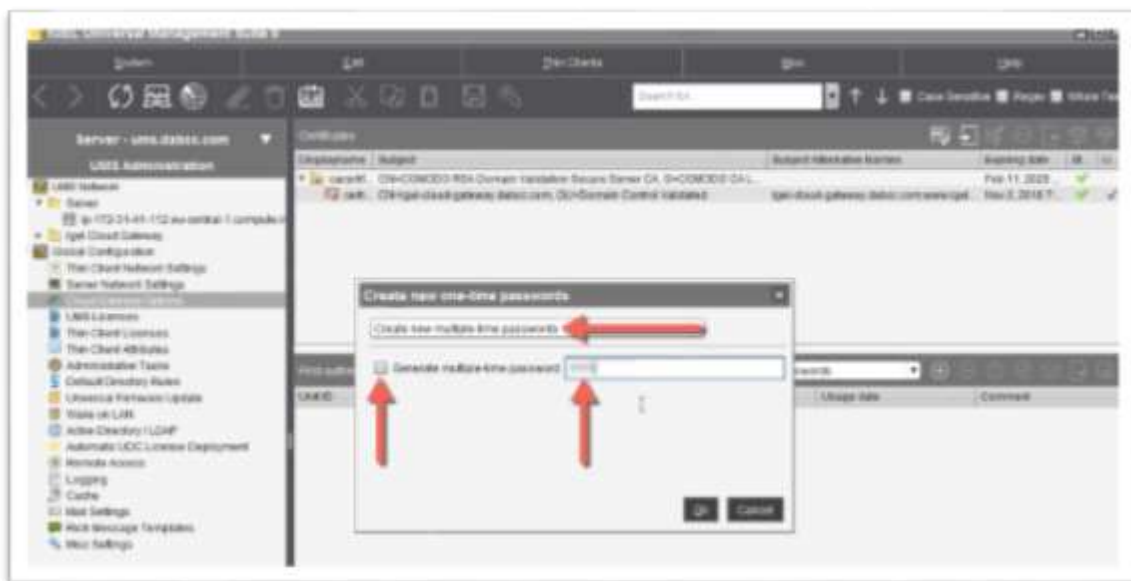


22. Click the + icon located in the **First-authentication passwords** box.

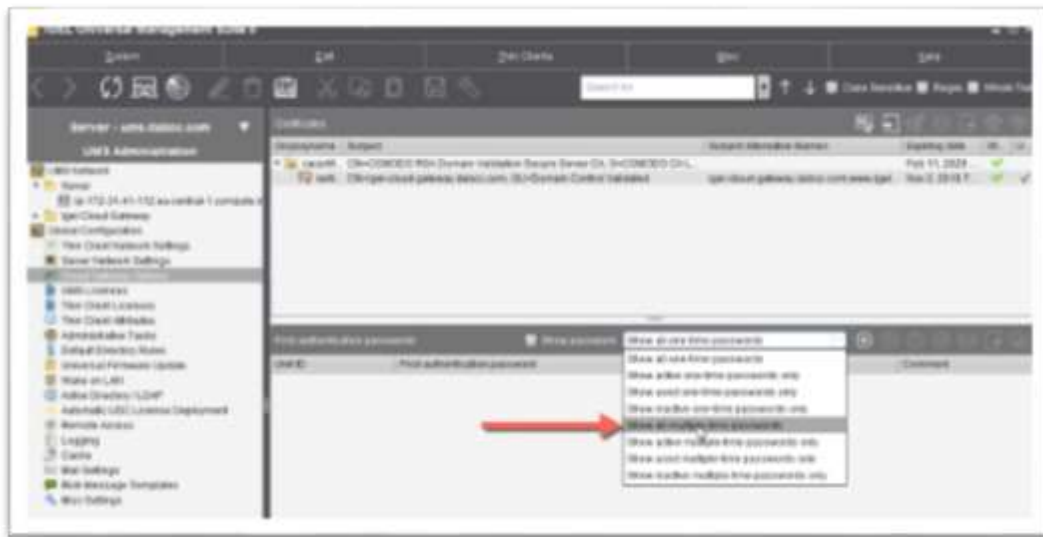


23. The **Create new one-time passwords** window opens. Select **Create** new multiple-time passwords from the dropdown list. Enter the desired password to be used to connect to the ICG. Click **OK** to continue.

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

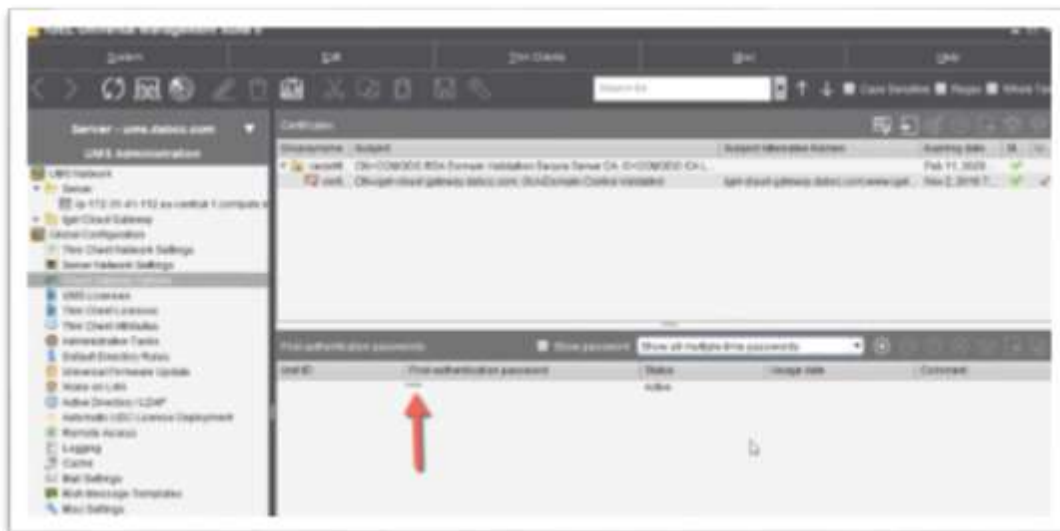


24. From the drop-down box on the top of the **First-authentication** passwords section select **Show all multiple-time passwords**.



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

Another cool feature of the ICG is that the login credentials can be sent via email if a mail relay is configured in the UMS. For more information, please refer to the IGEL Cloud Gateway eDocs support page <https://kb.igel.com/igelicg/en/igel-cloud-gateway-icg-2271354.html>.



Your IGEL Cloud Gateway server is up and running. It is time to install your first IGEL managed device!

5. Install IGEL OS Universal Desktop Converter (UDC)

The IGEL solution for installing the IGEL OS on an x86 computer is called Universal Desktop Converter (UDC). However, don't let the name fool you, this is not just a device conversion tool, but it installs the full version of the IGEL OS.

IGEL OS fully supports being run in an Oracle Virtual Box 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 Tech video on how to install the IGEL OS in a Virtual Box environment <https://www.youtube.com/watch?v=odsHIfrfAJM>.

Learn more:

- [IGEL Universal Desktop Converter 3 \(UDC3\) Manual](#)
- [IGEL Universal Desktop Converter 3 \(UDC3\) KB Support Homepage](#)

The process of installing, licensing and configuring the IGEL OS is broken down into the following five steps:

- UDC 3 System Requirements
- How to Create a Bootable USB Drive
- How to Install the UDC
- How to Find IGEL OSes
- How to License the IGEL OS UDC

5. 1. UDC 3 System Requirements

To successfully install the IGEL OS (UDC) operating system the target device must meet the following requirements:

- Any 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 are using 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/>.

- 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 UDC inside a virtual machine.
- Ethernet or wireless adapter.

Installing the IGEL OS operating system via UDC3 destroys all data on the target device's hard drive. Please be careful and do not accidentally delete the hard drive of the client machine you wish to maintain.

In the 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 a BYOD scenario.

5. 2. How to Create a Bootable USB Drive

If you are using IGEL OSes device converter solution (UDC) to convert existing hardware to a fully managed IGEL OS, you are required to boot to the UDC's installer software on the target device. This is done in two ways, 1) burning a DVD using the ISO image provided in the download package 2) creating a bootable USB thumb drive with the UDC's installer image on it. This USB drive is used to install the IGEL OS firmware and software onto the target devices' hard drive.

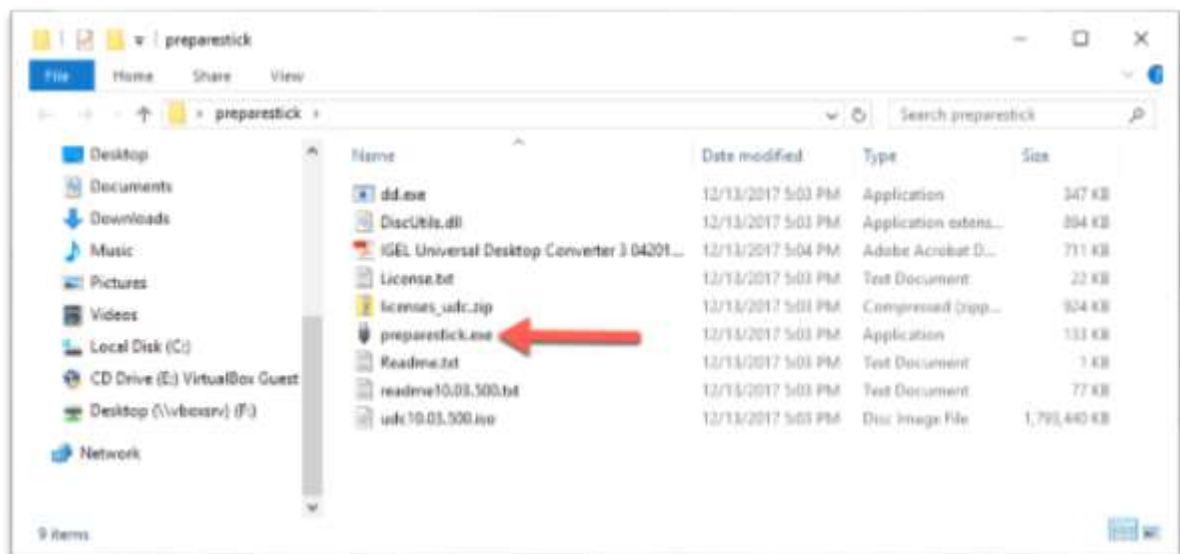
The following steps detail how to create a bootable USB drive with the IGEL OS UDC installer:

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

Double-click the **preparestick** executable.

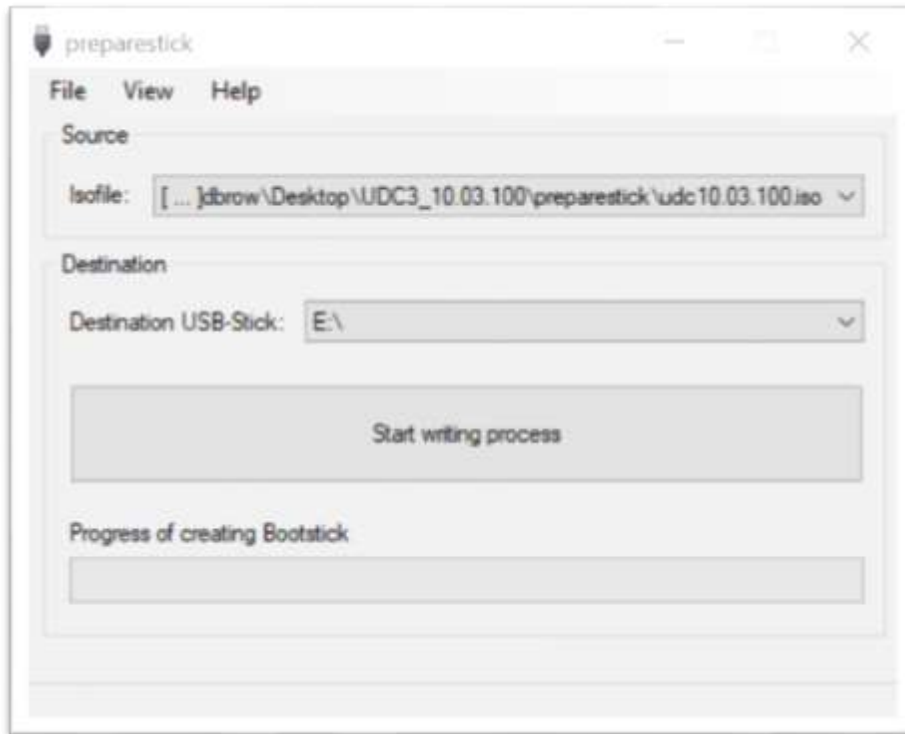
It is required to run the **preparestick** application with administrative context, or the app may fail.

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 UDC on a USB drive, but it is important to understand you can also utilize this ISO image and install the UDC in a virtual machine or burn a CD / DVD image.



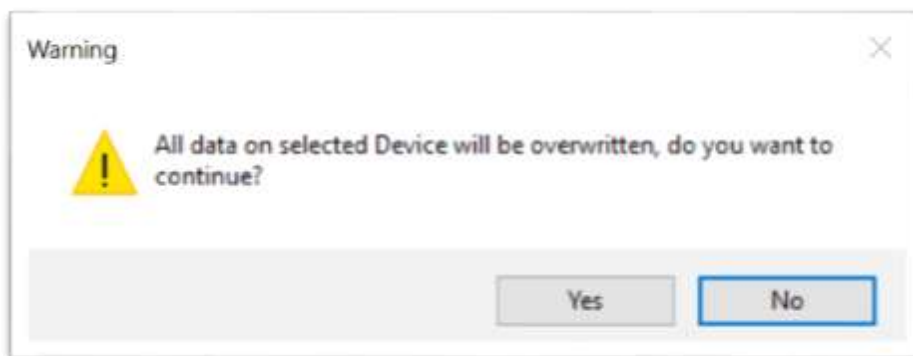
3. The **preparestick** application opens and presents you with the IGEL OSes source location (the ISO image discussed above) and destination you wish to install the IGEL OS software too, in this case, a USB thumb drive.

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

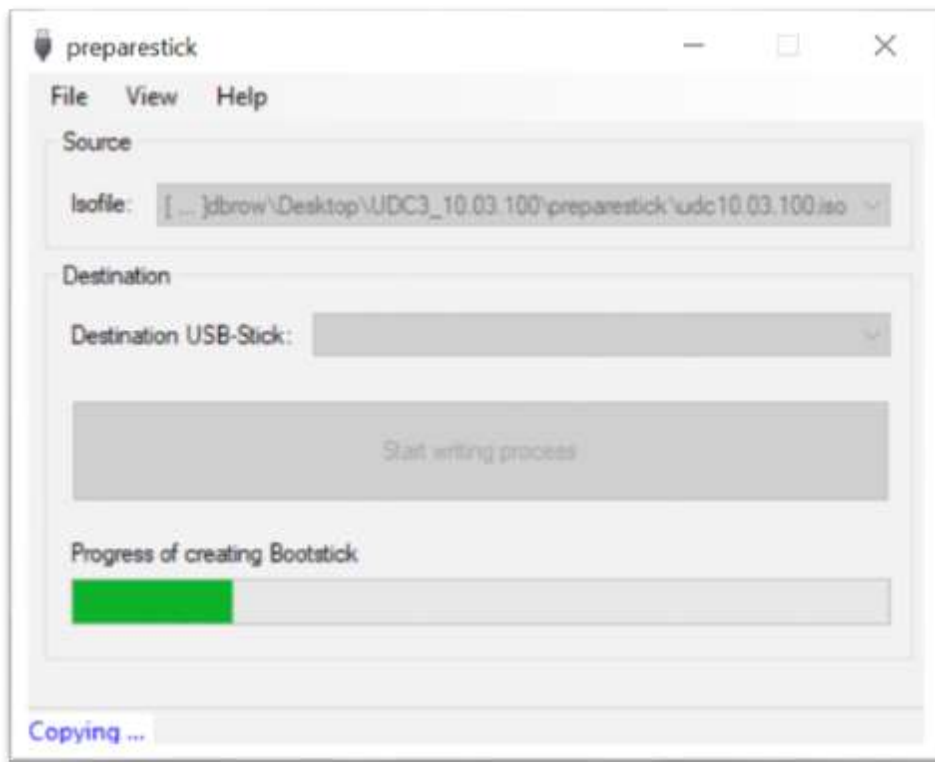


4. Beware, this tool formats the USB stick, thus any data on the drive is lost. Please be careful and double-check to make sure you do not delete the wrong hard-drive by accident.

Click **Yes** to continue.

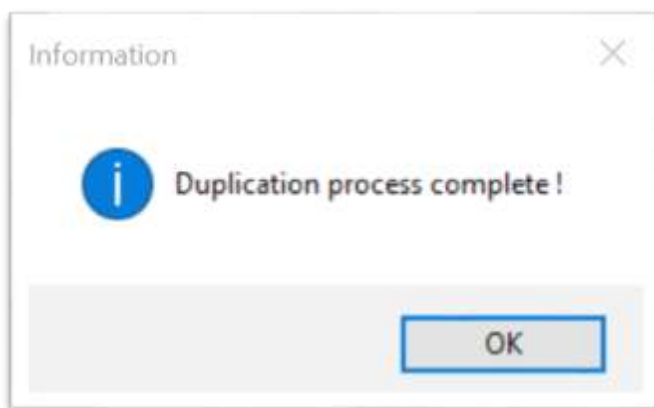


5. The preparestick program copies the IGEL OSes installation program to the USB drive and makes it bootable.



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

Click **OK** to continue.



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

5. 3. How to Install the UDC

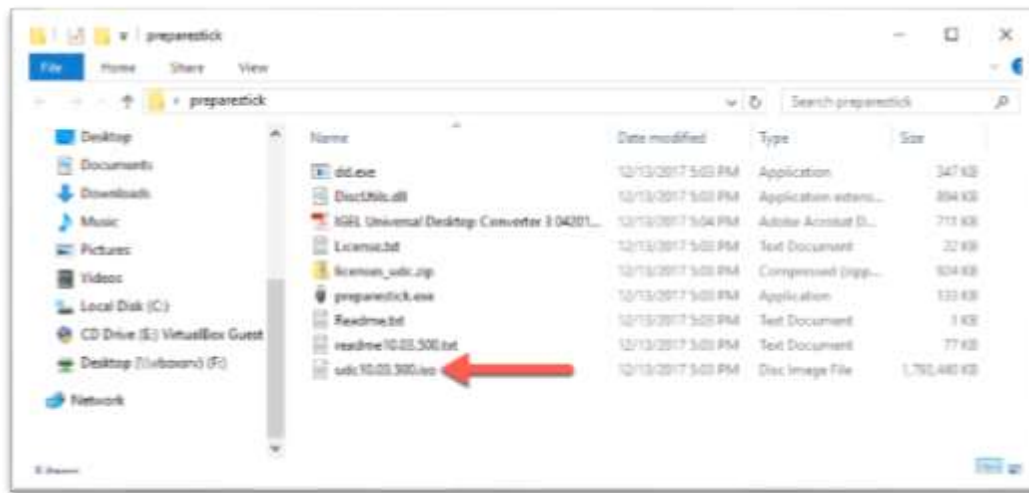
The following details how to install and configure the IGEL OS Universal Desktop Converter (UDC) software:

As stated above, IGEL fully supports Oracle's Virtual Box. Installing the UDC in a virtual machine only takes a couple of minutes and is a great way to test new configurations. Please refer to the following IGEL Tech video on how to install the IGEL OS in a Virtual Box environment

<https://www.youtube.com/watch?v=odsHlfrfAJM>.

1. From the device, you wish to install the IGEL OS too, 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 UDC in a virtual machine, you configure Virtual Box to boot from the **udc10.03.500.iso** image (file name varies depending on OS version) located in the **preparestick** folder of the extracted UDC download.



Before starting the installation, make sure 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 be able to boot the operating system.

2. Once you have successfully booted to the IGEL UDC, you are presented with the following list of options.

Click the **UDC Installation** entry.



3. The IGEL Universal Desktop Converter wizard walks you through installing the IGEL OS.

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



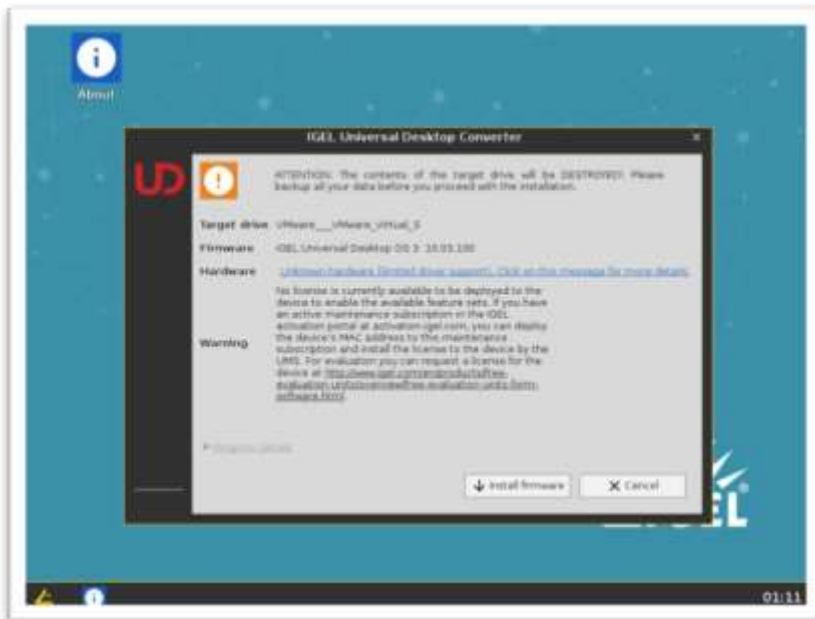
4. Click the **Yes** button to accept the IGEL license agreement.



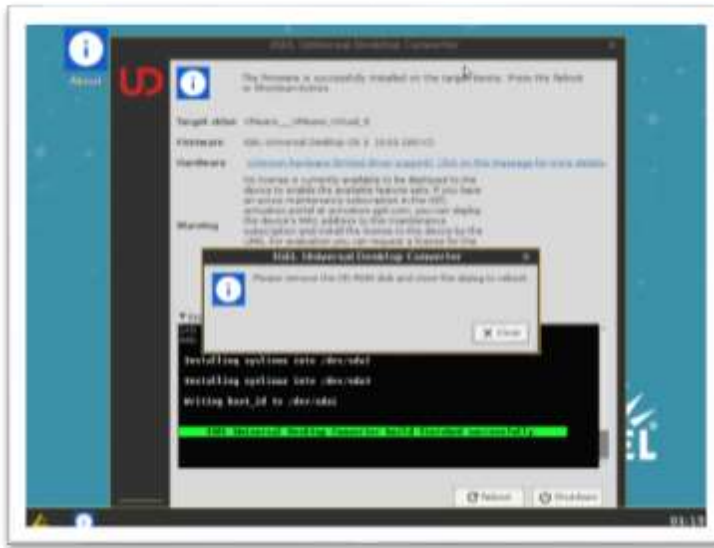
5. **IMPORTANT!** Verify you are installing to the correct hard drive as once you click the **Install Firmware** button the selected disk is erased without any way to restore it.

Pay close attention to “unknown hardware” details. Although, if there are unknown hardware noted, generally it works fine.

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



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



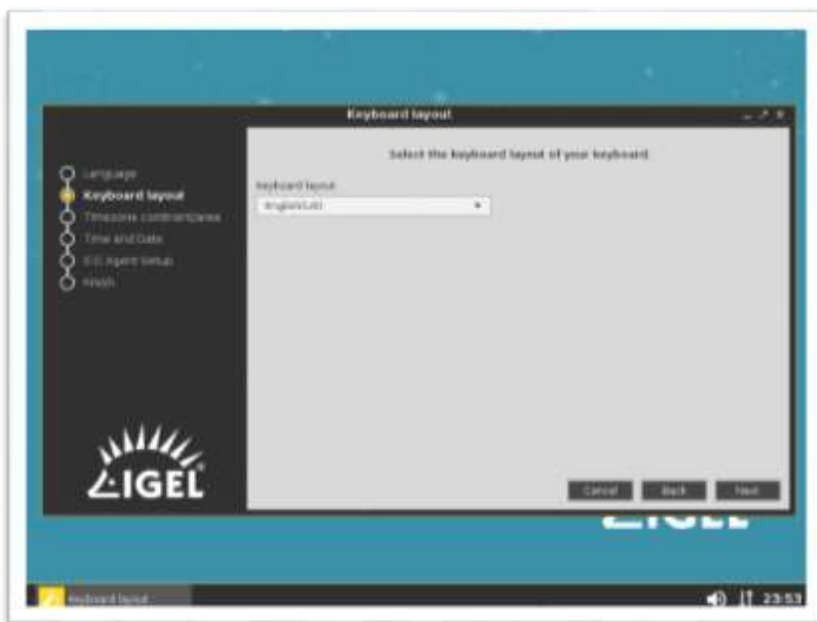
9. After the machine has restarted, you are logged in to the IGEL OS desktop. If you successfully configured the 'igelrmserver' DNS or DHCP entry the **Welcome Wizard** will not run. You are ready to skip to the next section of this document. If not, you are presented with the following **Welcome Wizard**.

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. Though do not continue until the **Welcome Wizard** appears, it is required if you are not using the 'igelrmserver' configuration for registration.

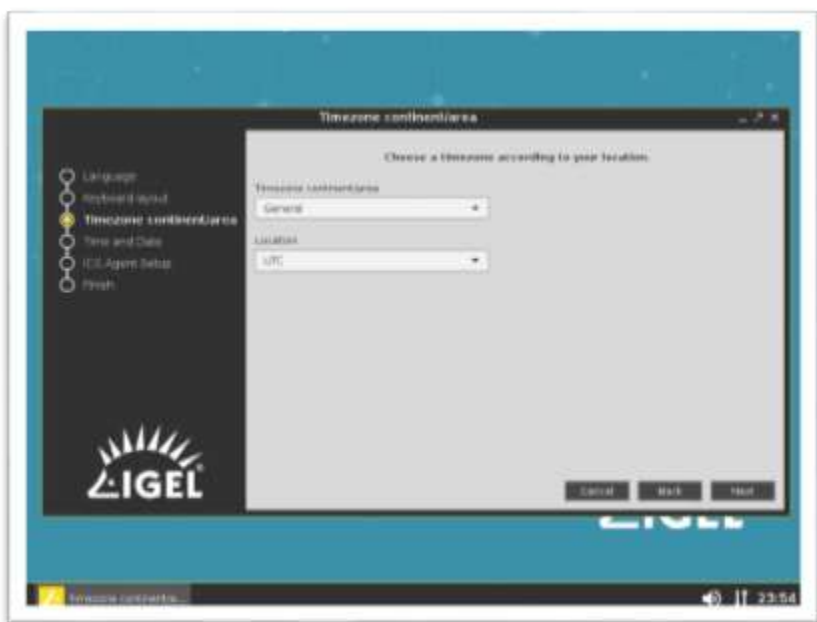
Select your desired language and click **Next** to continue.



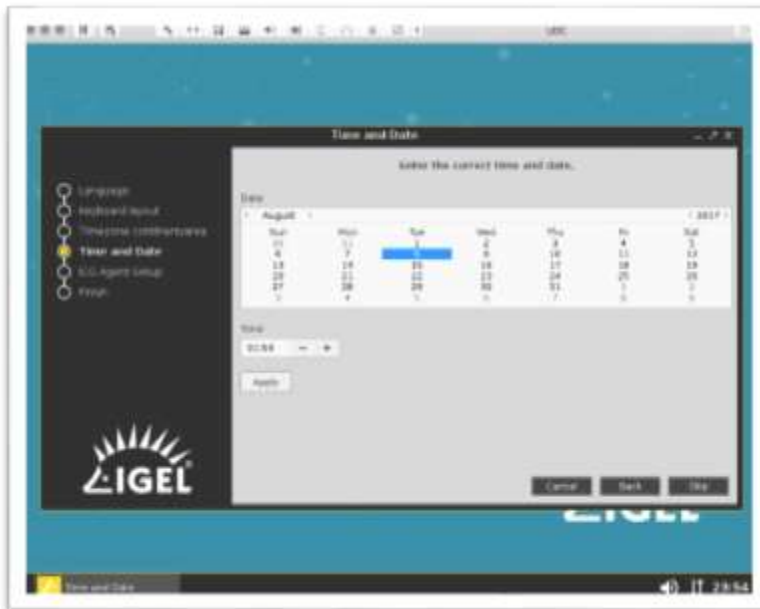
10. Select the desired keyboard layout and click **Next** to continue.



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



12. Enter the desired time and date and click the **Next** button to continue.



13. You are prompted for the address of the IGEL Cloud Gateway (ICG) server. If you have installed an ICG server, please enter the DNS name in the **Address** text box.

Click the **Connect** button to test the connection and connect the IGEL OS to the UMS via the ICG.

If you do not have an ICG server at your disposal, you can skip this step and connect directly to the UMS via a routable IP address. In this case, click the **Skip** button to continue and skip to step 16.



14. Enter the one-time password you created above and click the **Login** button to continue.

If there is a self-signed certificate, you are challenged to enter part of the fingerprint. The four-part fingerprint is found in the **UMS Administration > Cloud Gateway** and then click on the connected **Cloud Gateway**.



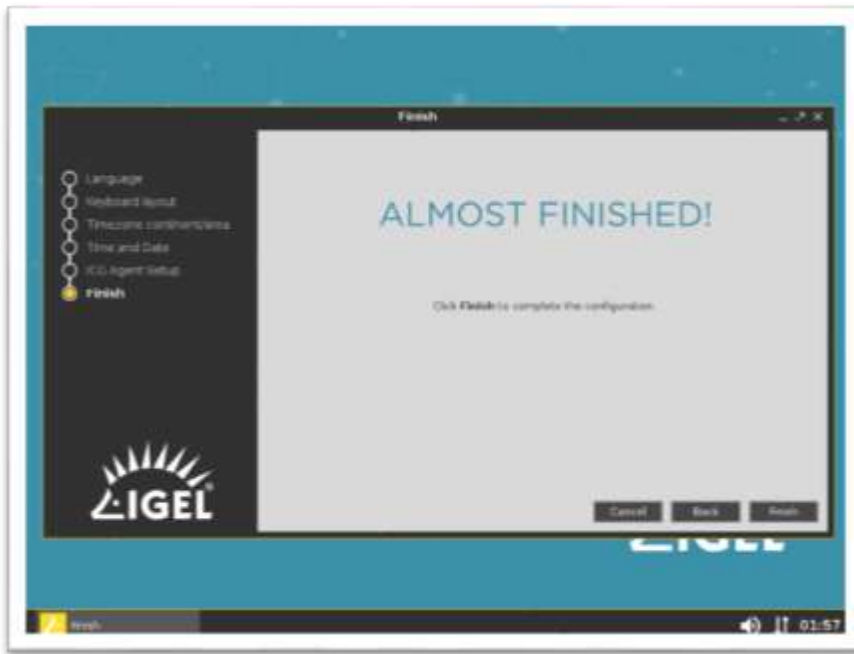
15. If all goes as desired, you will see the **ICG connection ready!** text on the screen as shown in the following image.

This is a happy moment. If everything is working, you have successfully connected to your ICG server. I love it when a plan comes together.

Click **Next** to continue.

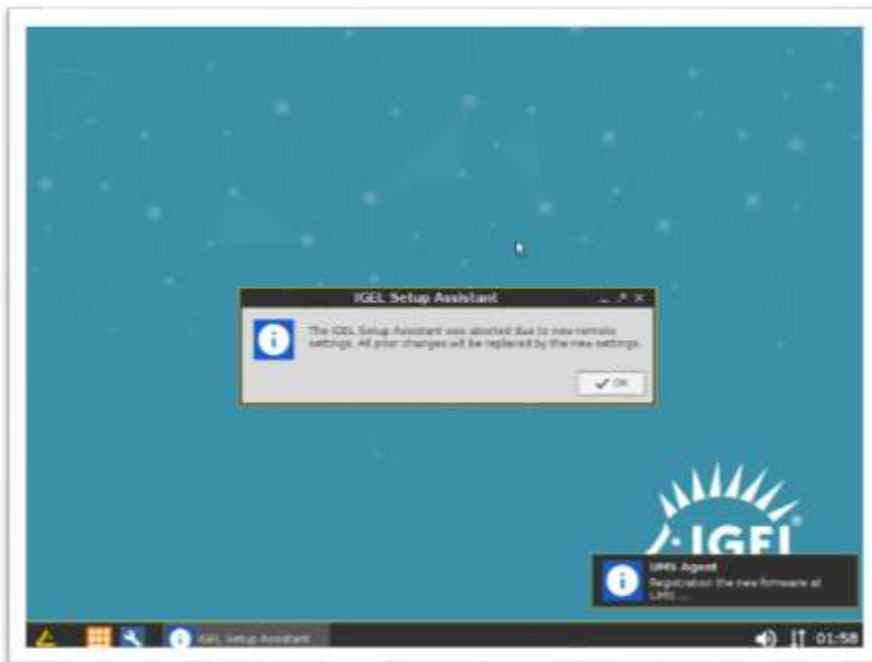


16. You are done! Click the **Finish** button to close the startup wizard.



17. If you receive the following message, you can ignore it.

The UMS Agent notification popup on the bottom right of the screen. It is telling you the IGEL OS has successfully registered with the UMS. Joy to the world!



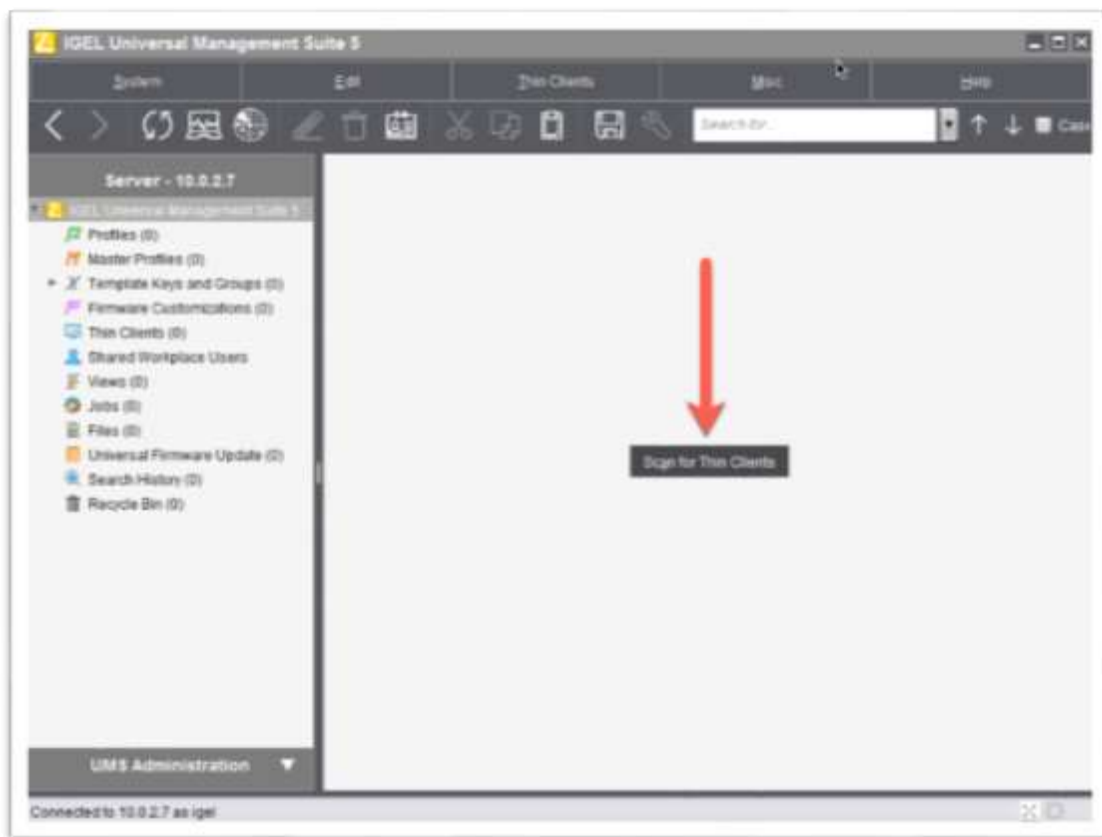
5. 4. How to Find IGEL OSeS

You have a working IGEL UMS, and your first IGEL OS end-point installed. If you did not register the IGEL OS via the ICG, then the next step is to configure the UMS to find any available IGEL OSeS and import them.

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

1. On the UMS's **IGEL Universal Management Suite 5** page, you see a big button allowing you to scan for thin clients, thus look for IGEL OSeS.

Click the **Scan for Thin Clients** button to continue.



2. The **Scanning for Thin Clients** window opens allowing you to select the network you wish to scan.

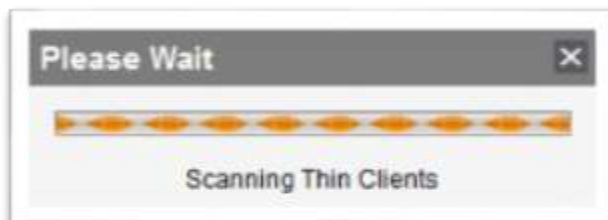
For more information on importing and managing IGEL thin clients, please refer to the following IGEL Tech video:

<https://www.youtube.com/watch?v=MfMXw4UUhQ>

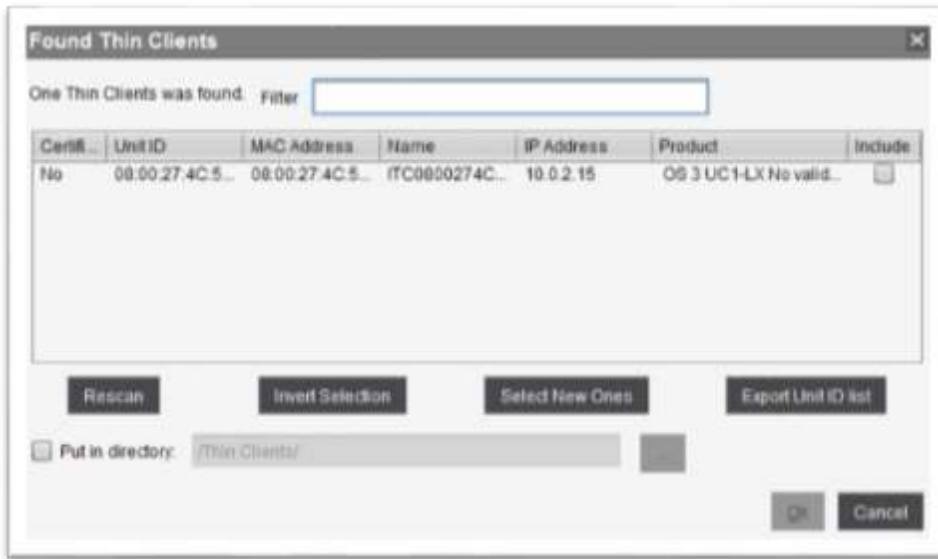
If the UMS experiences problems finding your clients, please verify you have connectivity between hosts. UDP should be open between the IGEL OS and UMS. Try TCP scan for figuring out if this is the problem. Also working without UDP when TCP Scan is checked and try scanning in a specific IP Range.



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



4. The **Found Thin Clients** windows list all IGEL OSES that are found.



5. Click to check the **Include** checkbox of the IGEL OSES 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.



7. 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.

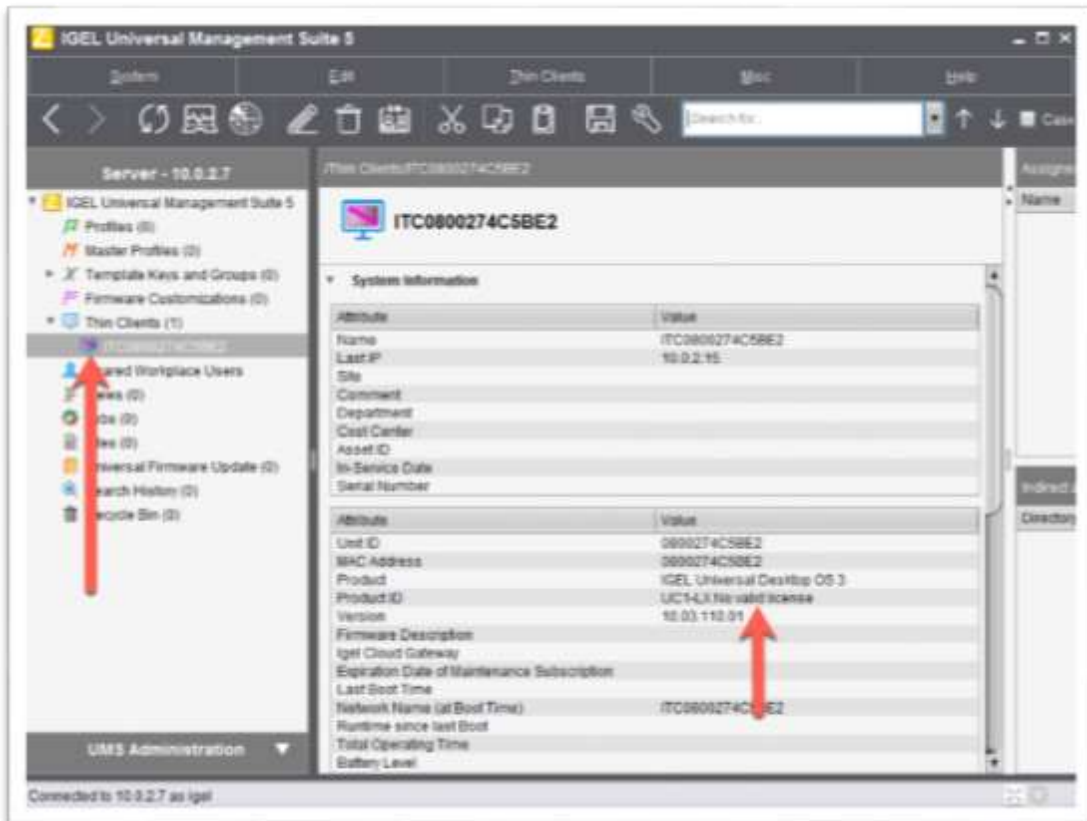
For more information on troubleshooting this issue, please refer to <https://kb.igel.com/endpointmgmt/en/registration-of-a-thin-client-fails-911003.html>.

Click the **OK** button to continue.



8. You should see your newly found and registered devices in the **Thin client** section of the UMS, as seen below.

Do note the **Product ID** section of the **System Information** area. It will read, **No valid license**. Don't worry; you are ready to install the license you obtained when downloading the IGEL OS trial software.

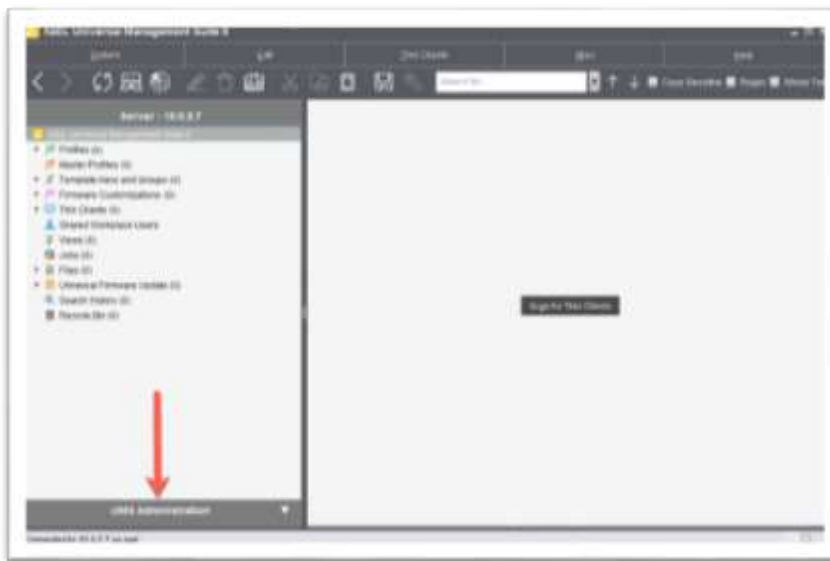


5. 5. How to License the IGEL OS UDC

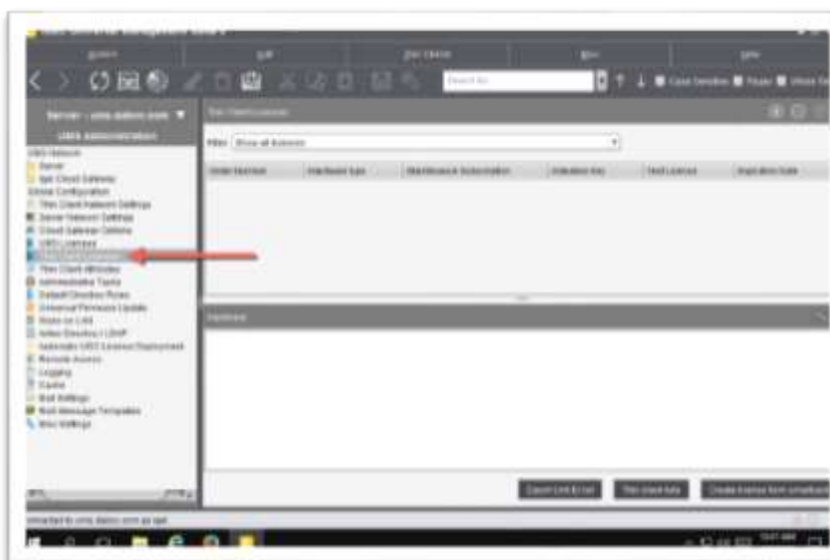
Now that you have successfully registered your first IGEL OS (UDC in this case) to your newly created UMS, you are ready to procure a license file and apply it to the UMS.

The following defines how to download your free UDC licenses and apply them to the IGEL UMS:

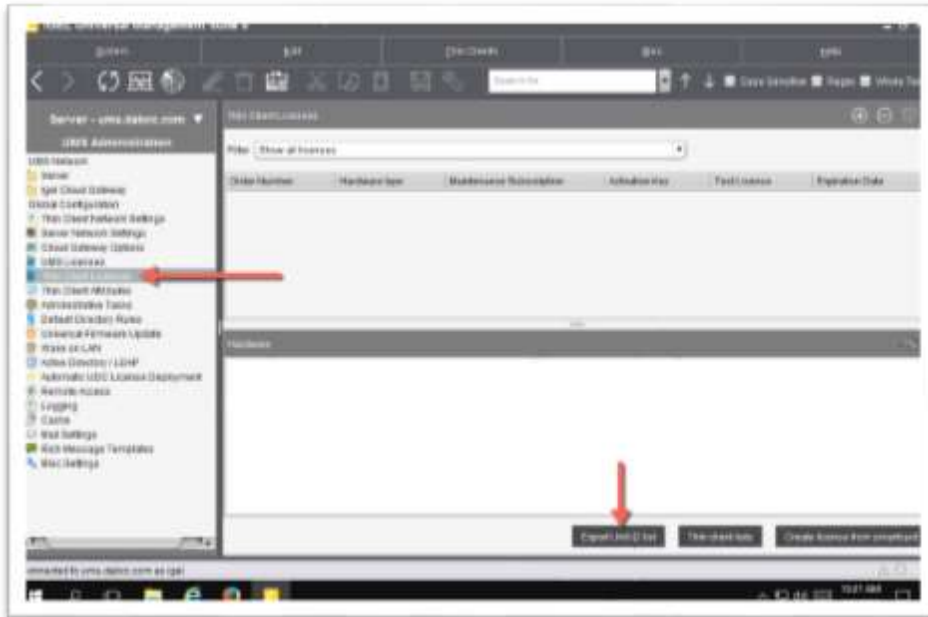
1. Click the **UMS Administration** button at the bottom of the left menu.



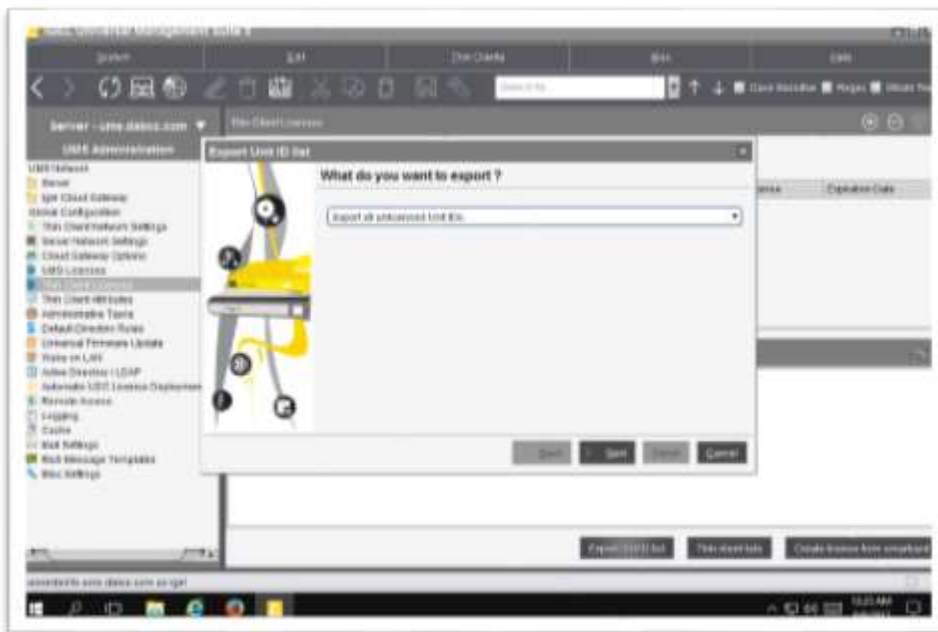
2. Click the **Thin client Licenses** node in the left menu.



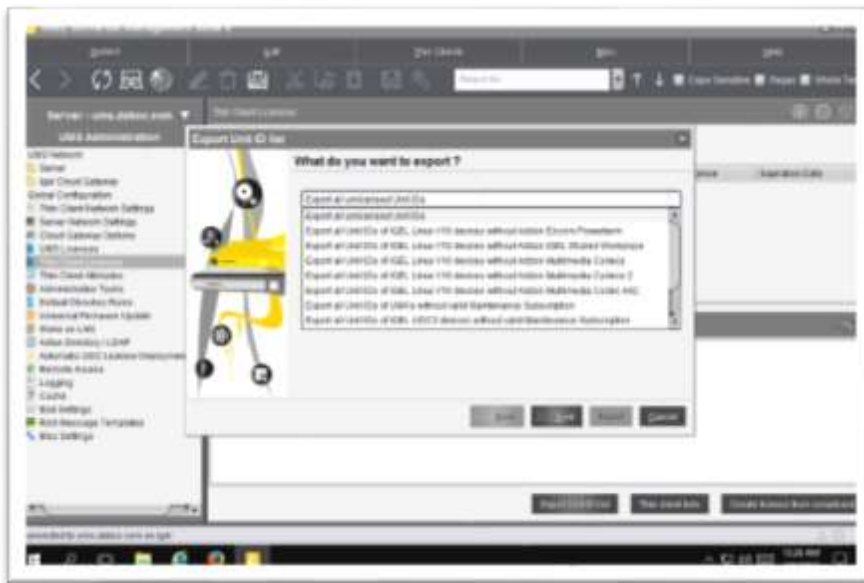
3. Click the **Export Unit ID List** button.



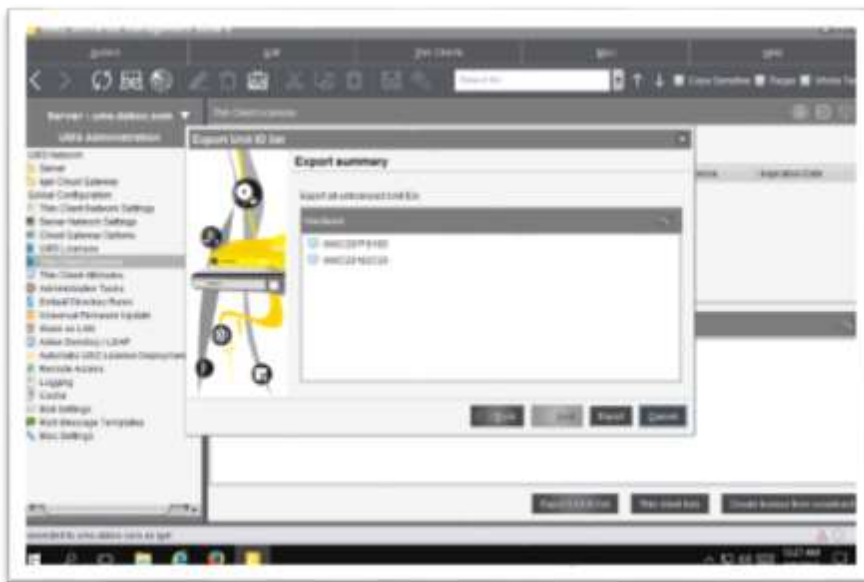
4. The **Export Unit ID List** wizard opens. This wizard will allow you to export a list of hardware identifiers (MAC addresses). This list is required to create the license file.



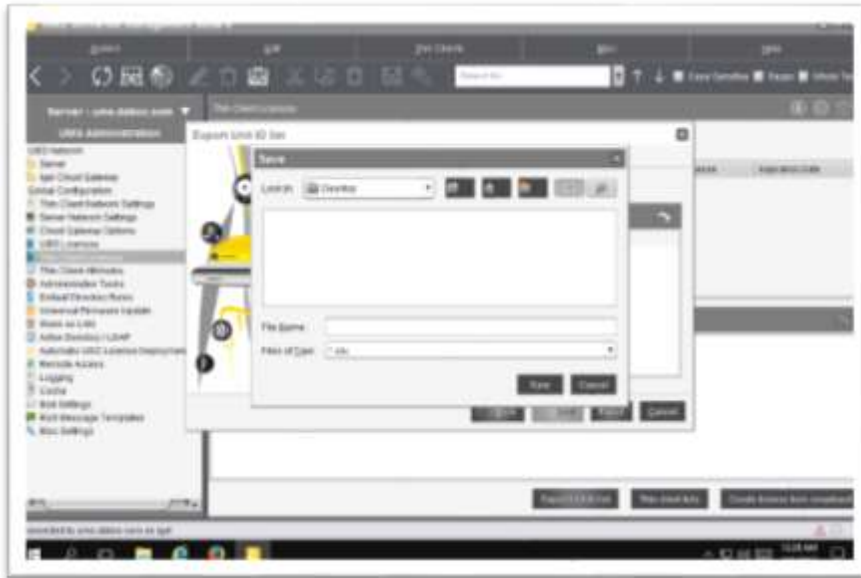
5. Select the **Export all unlicensed Unit IDs** list from the dropdown list and click **Next** to continue.



6. You are presented with a list of all the Unit IDs of the newly added IGEL OSes. Verify you are not missing any and click the **Export** button to continue.



7. Browse to the location you wish to save the Unit IDs .CSV file and click the **Save** button. I like to place it on my desktop as it is convenient, but this is up to you!



8. Refer to the email you received when downloading the IGEL software. In this email, you will find a link that looks something like this:

Go to https://activation.igel.com/index.php?id=y1u8&activation_key=521rv315-dadfdd-0ddwf3f-a3sdd1-35dfd75 to activate your software licenses and follow these instructions.

Click the above link to start the process of obtaining your free license.

9. Your default Internet Browser will open, and you are taken to the **IGEL UDC Demo Activation Portal**. Click the **Browse** button.

IGEL Home Registration

Activate UDC DemoIT License

Activate your UDC DemoIT licenses to start your trial period

You need to provide a list of MAC addresses in order to generate a UDC license file for the devices with these addresses. [Read about how to use UMS to generate the MAC address list file in CSV format.](#)

You need not generate licenses for all your MAC addresses in one run. Generate as many as you need each time until the licenses tied to your activation key are used up. The trial period, however, begins when generating the first license.

Make sure the list only includes MAC addresses of devices you really want to license UDC trial for. You cannot remove any devices from a license offer it has been generated on this portal.

Upload a CSV file with a list of MAC addresses. **Browse...** **Submit**

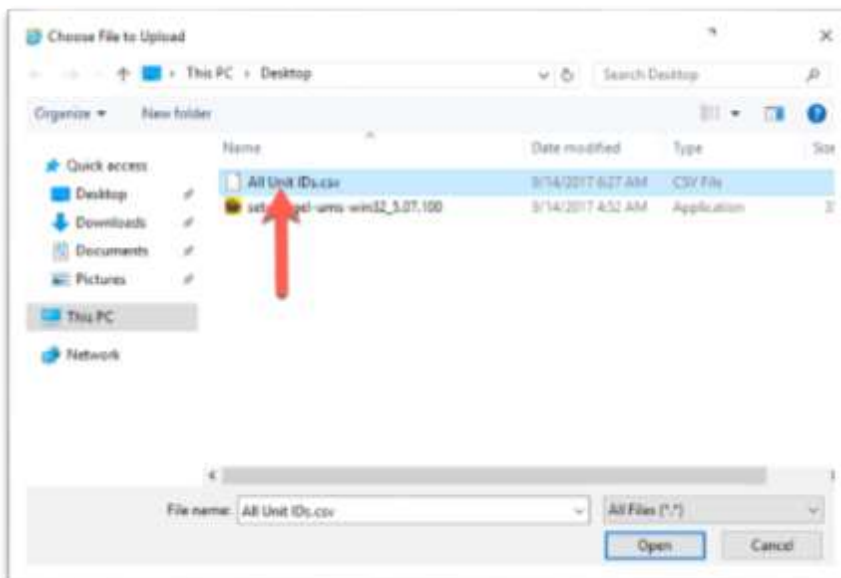
Or input addresses in field(s) below

Tips about input format

- MAC addresses are allowed with - or - as delimiters. Can be provided without delimiters as well. Letters can be provided in any case. Valid examples: R22:33:ab-cd-ef, R22:33:ab-cd-ef, R2233abcdEF

You are allowed to register 3 MAC addresses with this UDC license. Already registered: 0

10. The **Choose File to Upload** window opens prompting you to select the CSV file you saved above. Browse to the location you saved the file and click to select. Click the **Open** button to upload your CSV file to the activation portal.



11. You are brought back to the activation portal's main page. Click the **Submit** button to submit your Unit IDs.

Activate UDC DemoIT License

Activate your UDC DemoIT licenses to start your trial period

You need to provide a list of MAC addresses in order to generate a UDC license file for the devices with these addresses. [Read about how to use UDC to generate the MAC address list file in CSV format.](#)

You need not generate licenses for all your MAC addresses in one run. Generate as many as you need each time until the license list to your activation key are used up. The trial period, however, begins when generating the first license.

Make sure the list only includes MAC addresses of devices you really want to license UDC trial for. You cannot remove any devices from a license after it has been generated on this portal.

Upload a CSV file with a list of MAC addresses. *

[C:\Users\Administrator\Desktop\All 1](#) [Browse...](#)

Submit

Or input addresses in field(s) below

Submit

Tips about input format

① MAC addresses are allowed with - or - as delimiters. Can be provided without delimiters as well. Letters can be provided in any case. Valid examples: 02:23:ab:cd:ef, 02-23-ab-cd-ef, 0223abcdEF

You are allowed to register 3 MAC addresses with this UDC license. Already registered: 0

© 2017 IGEL Technology - Contact - Legal Notice

12. Verify the Unit IDs (MAC addresses) are correct and if you would like to add another manually, please do. Remember, you get three free licenses!

Click the **Submit** button to continue.

Activate UDC DemoIT License

UDC MAC addresses preview

Following new (not yet registered with current UDC license) MAC addresses were found in provided CSV file

You are allowed to register 3 MAC addresses with this UDC license. Provided (already registered + found in uploaded file): 2

New MAC addresses

You can provide additional addresses

Tips about input format

① MAC addresses are allowed with - or - as delimiters. Can be provided without delimiters as well. Letters can be provided in any case. Valid examples: 02:23:ab:cd:ef, 02-23-ab-cd-ef, 0223abcdEF

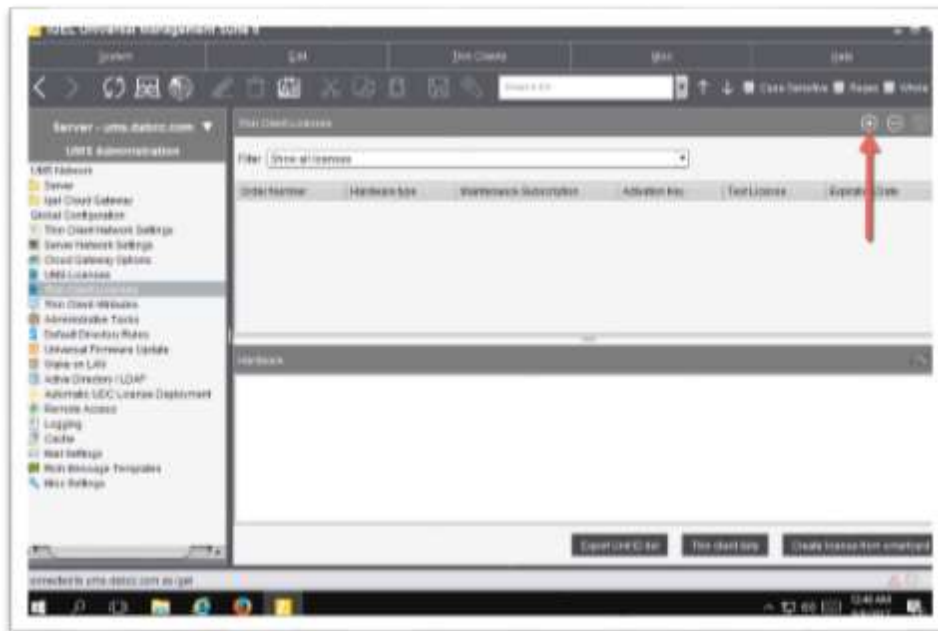
Submit

© 2017 IGEL Technology - Contact - Legal Notice

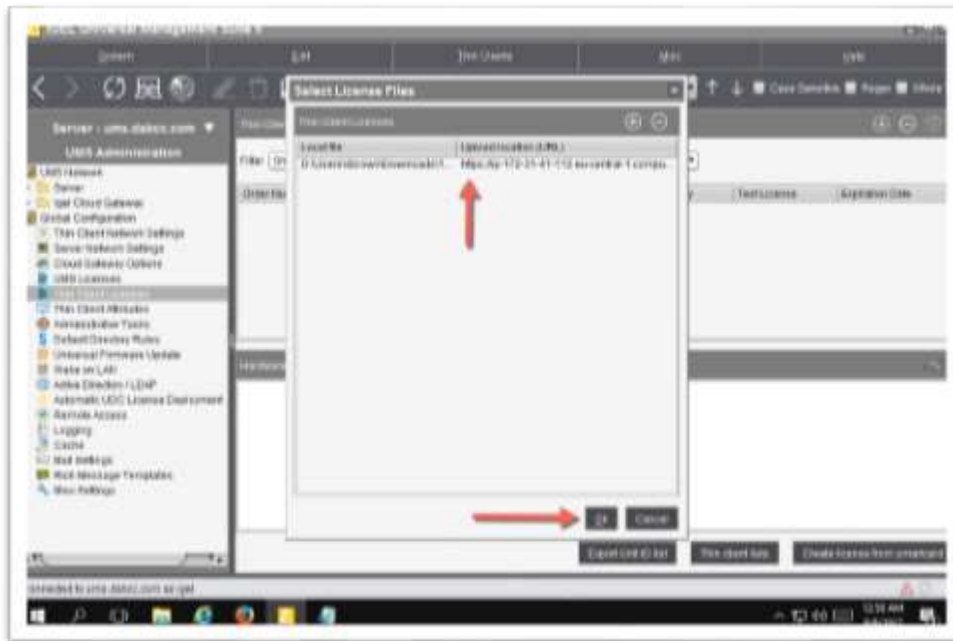
13. The activation portal has successfully created your license file. Please click the **Download UDC License file now** link to download your newly created license file.



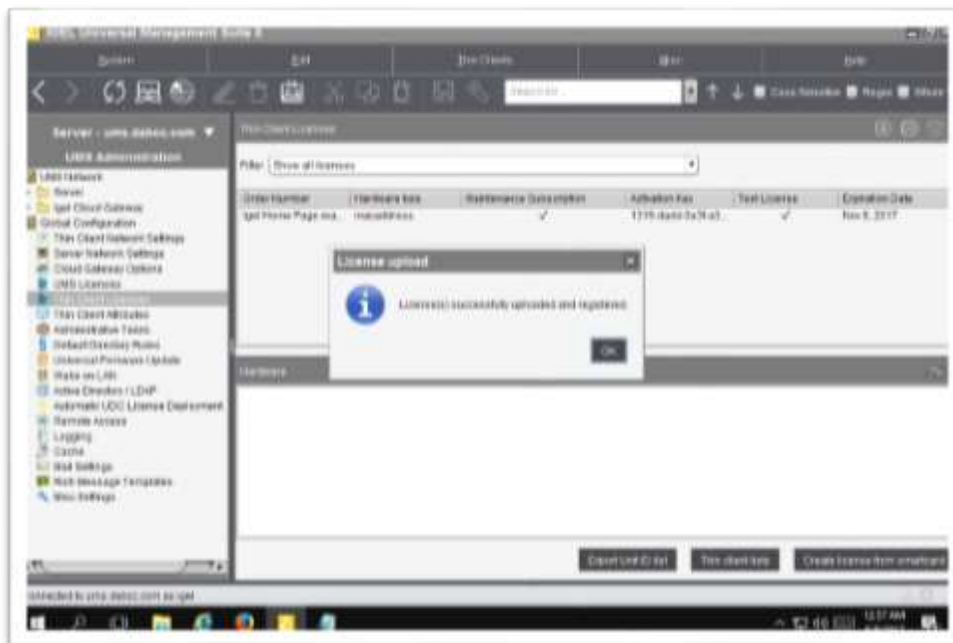
14. You are ready to import your license. Flip back to the UMS and from **Thin client Licenses** screen click the + button located at the top right of the right panel.



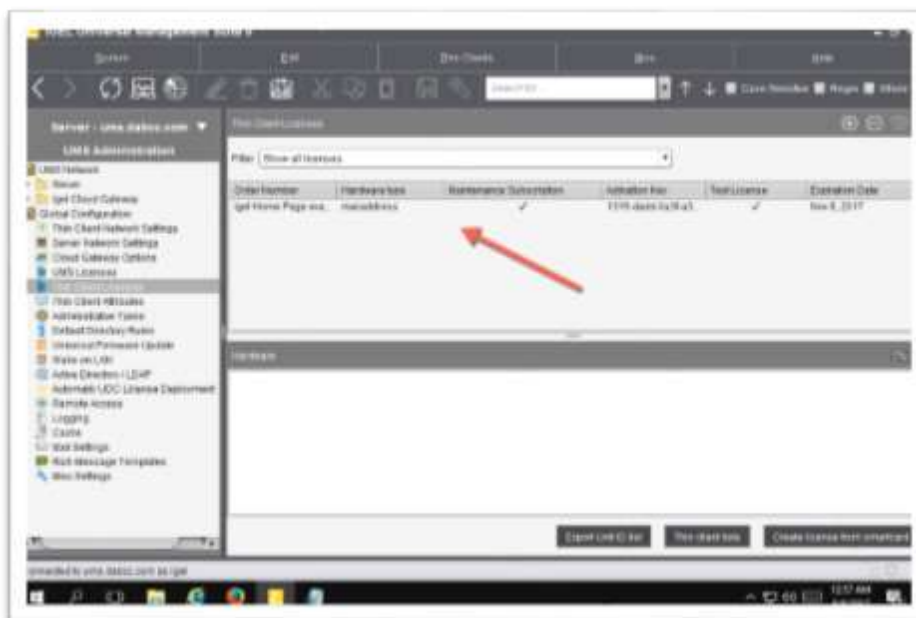
17. Verify your license was imported correctly and if all looks good, click the **OK** button to continue.



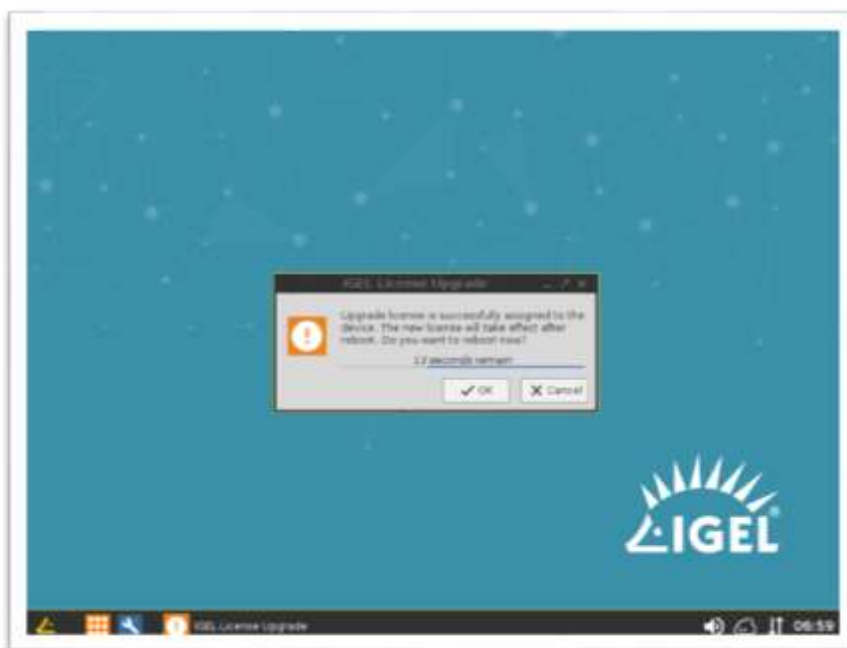
18. If all goes well, you will be presented with a fancy popup window informing you the new licenses were successfully uploaded and registered!
- Click the **OK** button to close the popup window.



19. Your new license file will be listed in the top pane of the **Thin client Licenses** page, as shown below.



20. If you refer to the device running the IGEL OS UDC you might notice a message box telling you the newly added license has successfully been assigned to the device!



You have successfully installed the IGEL Software Suite and have successfully licensed it. You are ready to create policies to configure the look and feel of the IGEL. You are rolling, don't look back!

This page is blank on purpose.

Configuration & Maintenance

1. UMS Profiles Overview

Profiles are where you configure the settings of the IGEL OS, everything from the look and feel to the applications and sessions the user will have access. 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 part of the different versions of the IGEL OS. For example, as IGEL releases updates they might add new profile settings. Hence profiles are tied to OS versions. In fact, if you did not follow this document 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 enabled by the different versions of the IGEL OS registered to the UMS on which you are creating the profiles.

It is recommended to create profiles to be used per feature, and not to have a single profile for EVERY feature/setting.

Profiles are so powerful and vast that we could write an entire document on the subject and IGEL has! For a detailed reference on IGEL profiles, please refer to the **IGEL UMS 5 Profiles Reference Manual**

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. Though, 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.

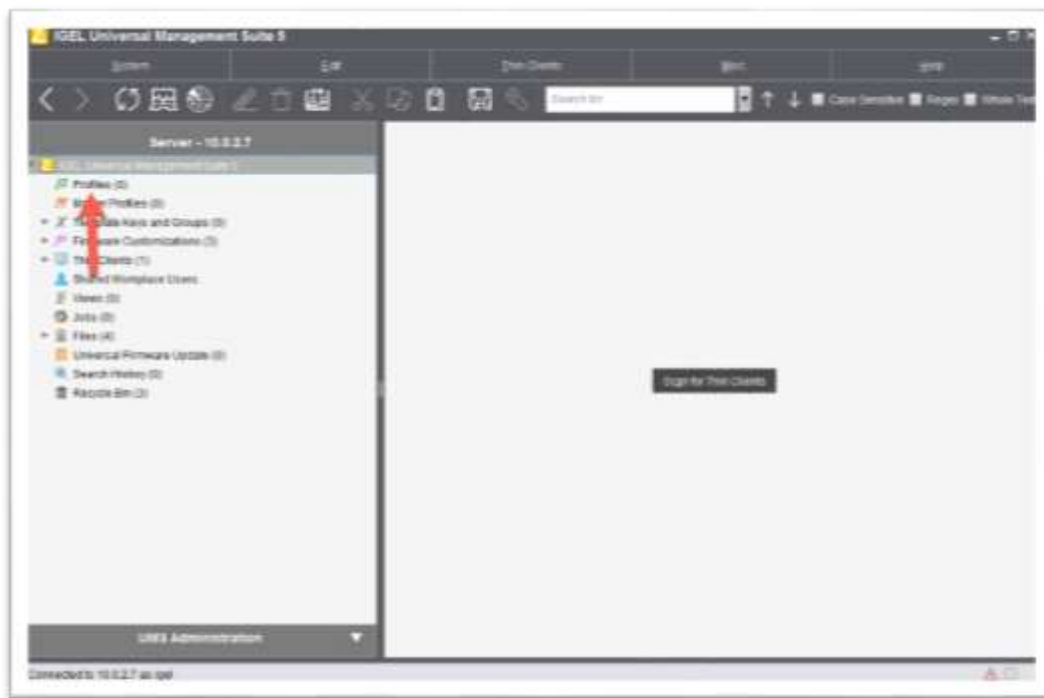
Learn more about profile folder structure at

<https://kb.igel.com/endpointmgmt/en/creating-profiles-910899.html>

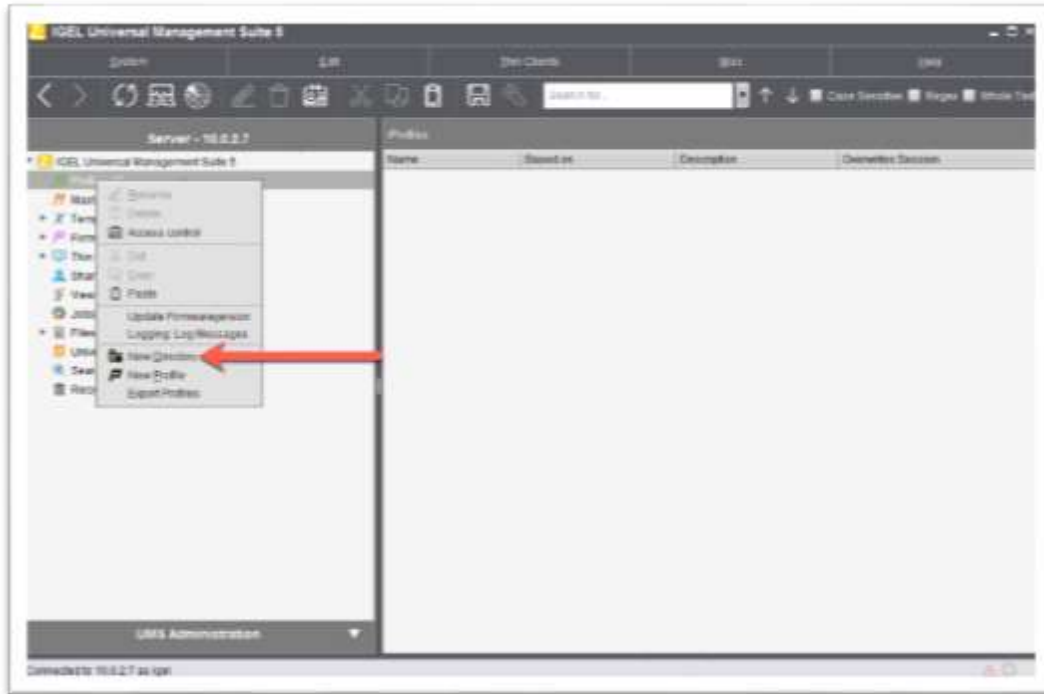
Learn more about Thin client device structure at [Creating Thin client Structures](#)

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. IGEL UMS profiles are based IGEL OS firmware versions. Since, in this example, you are installing the IGEL OS UDC you are using the LX firmware. Enter **LXv10**, for IGEL OS firmware LX version 10, in the **Directory Name** text box and click **OK** to create the new folder.



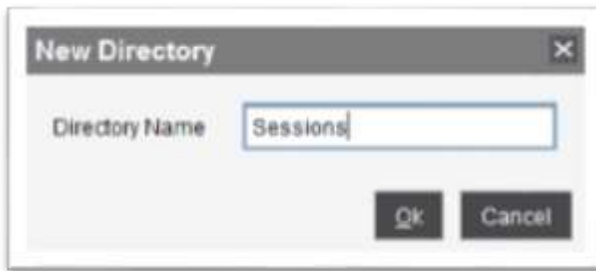
4. Under the OS firmware version directory, created above, you will create your child folders for the different type of Profiles and settings you will be creating.

Repeat the above two steps and this time name the new folder **Thin client Settings**.

This folder will be used to store profiles that control how the local operating system should look and behave.



5. As above, create a new folder named **Sessions**. This folder will be used to store the different type of sessions you will be deploying to the IGEL OS.



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



7. Once finished, you will see a folder structure that looks like the following image.
You are ready to create your first profile so let's get to it!

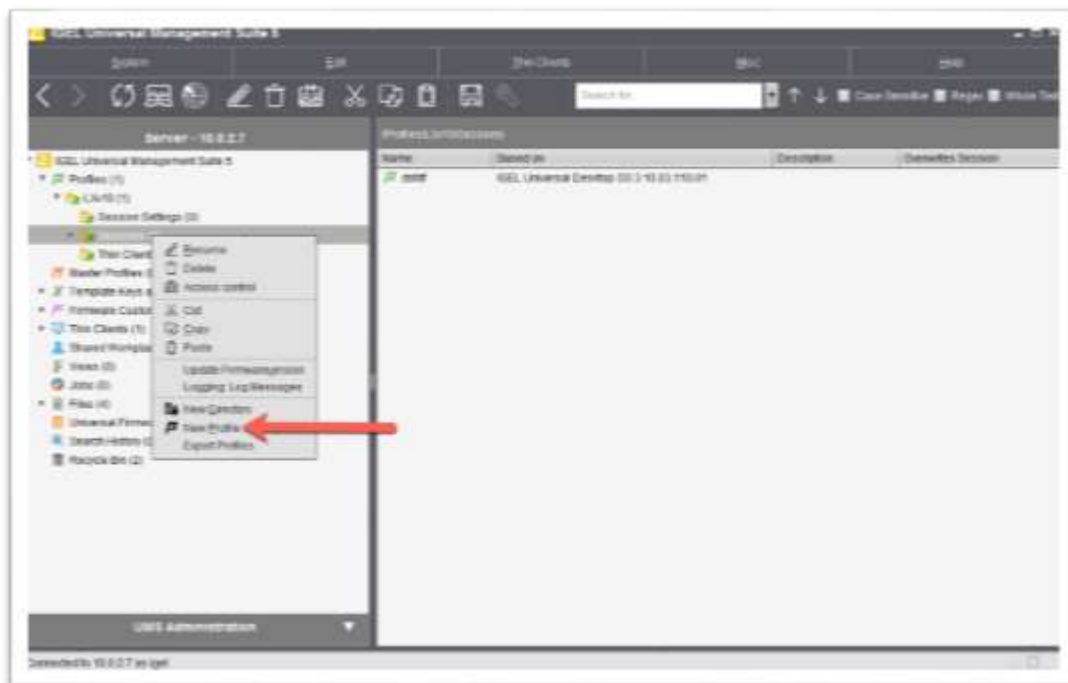


1. 2. How to Create Basic UMS Profiles

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

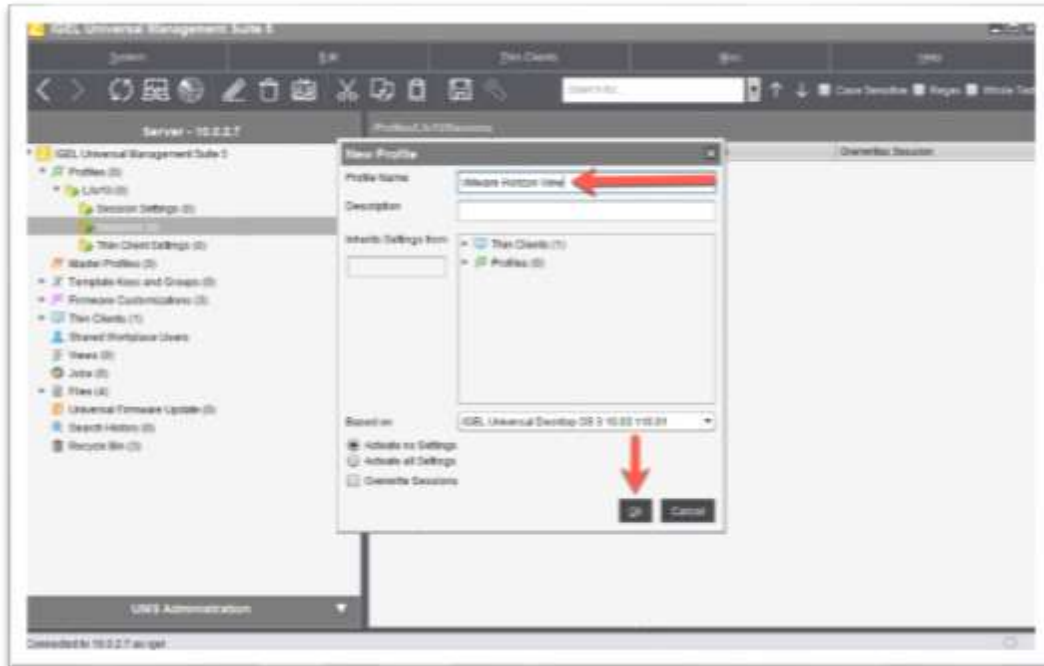
The follow steps detail how to create a basic profile and assign it to client devices running the IGEL. In this example, you will be configuring the **VMware Horizon View client**.

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**.



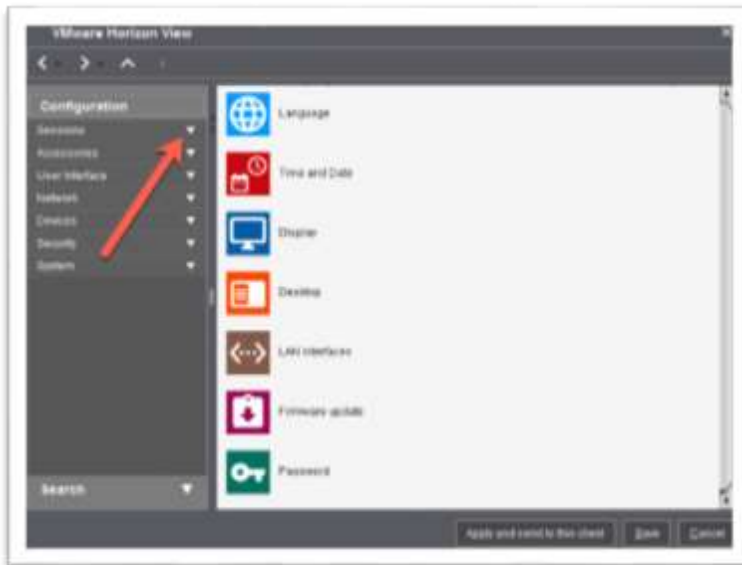
2. The **New Profile** window opens. Enter the name of the profile in the **Profile Name** text box. Make this title descriptive, so you and others understand its purpose. For example, **VMware Horizon View Client**.

Click the **OK** button to continue.



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

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

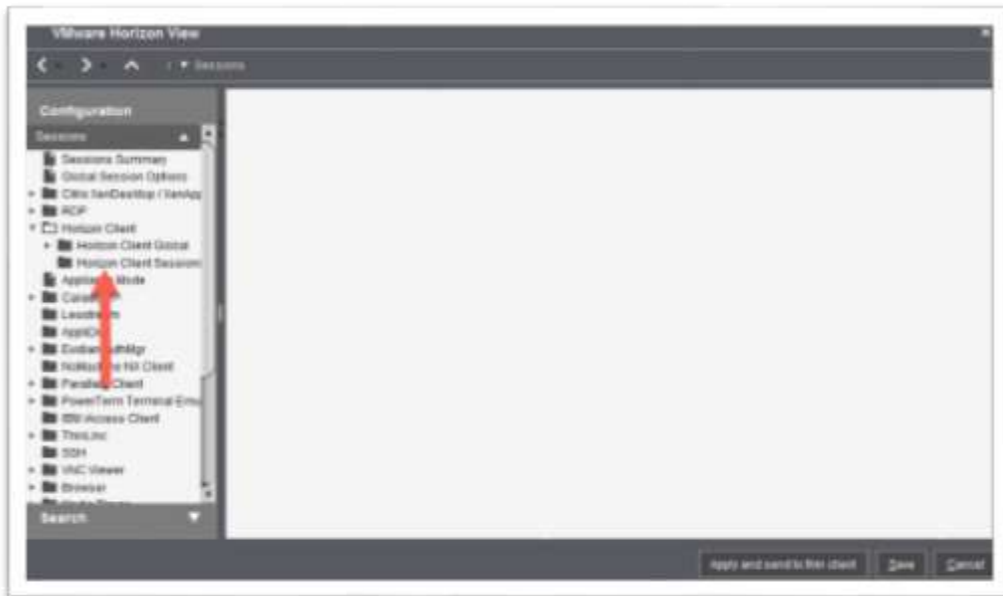


- You are presented with all the possible sessions you can configure. Take a second or two to browse through this list. You will find sessions, such as Citrix XenApp, XenDesktop, Microsoft RDP, SSH, VNC Viewer, Firefox browser, Multimedia Player and so much more. The possibilities never cease to amaze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

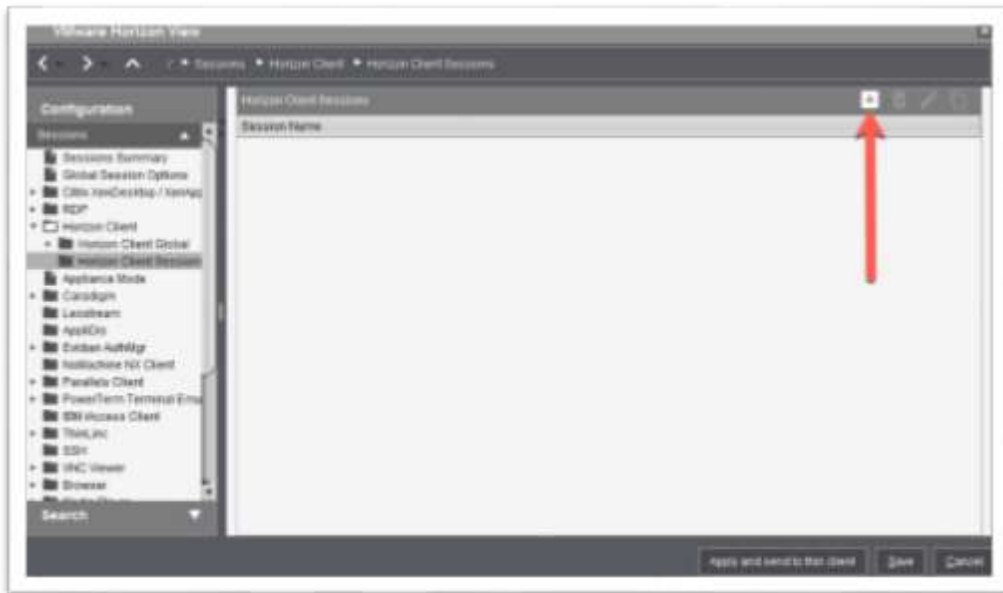
Click **Horizon Client** to expand the node.



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



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

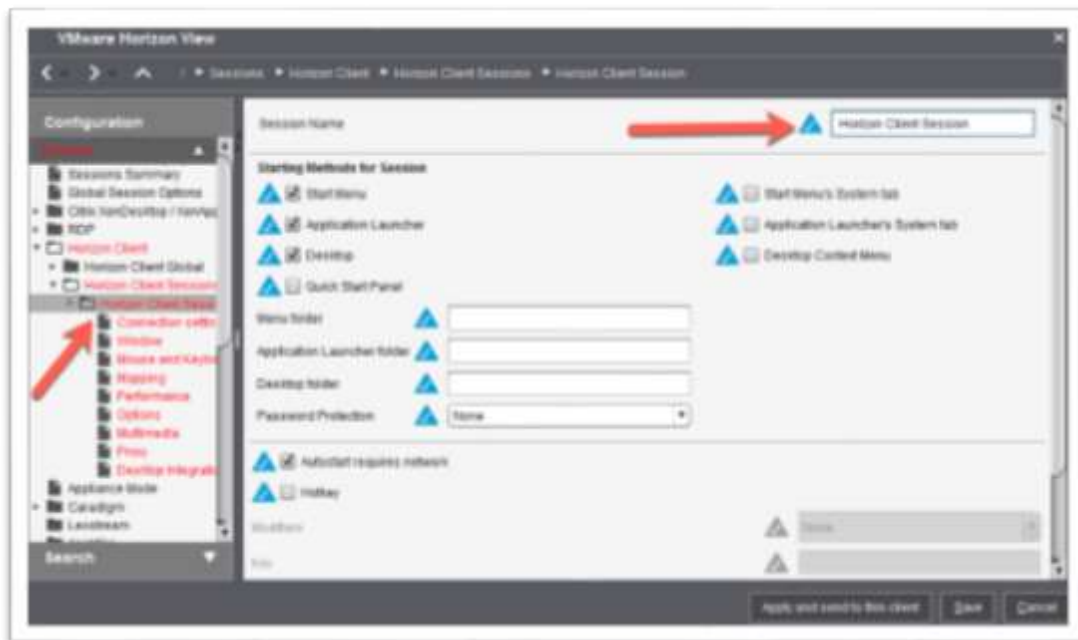


7. The **Desktop Integration** page opens. This is the same screen you will see if you click the **Desktop Integration** link located at the bottom of the list. This screen is important as it allows you to define where and how the session is presented to the user.

You can specify the name in the **Session Name** field and 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 that is displayed when the user right-clicks on the desktop. It is all up to you.

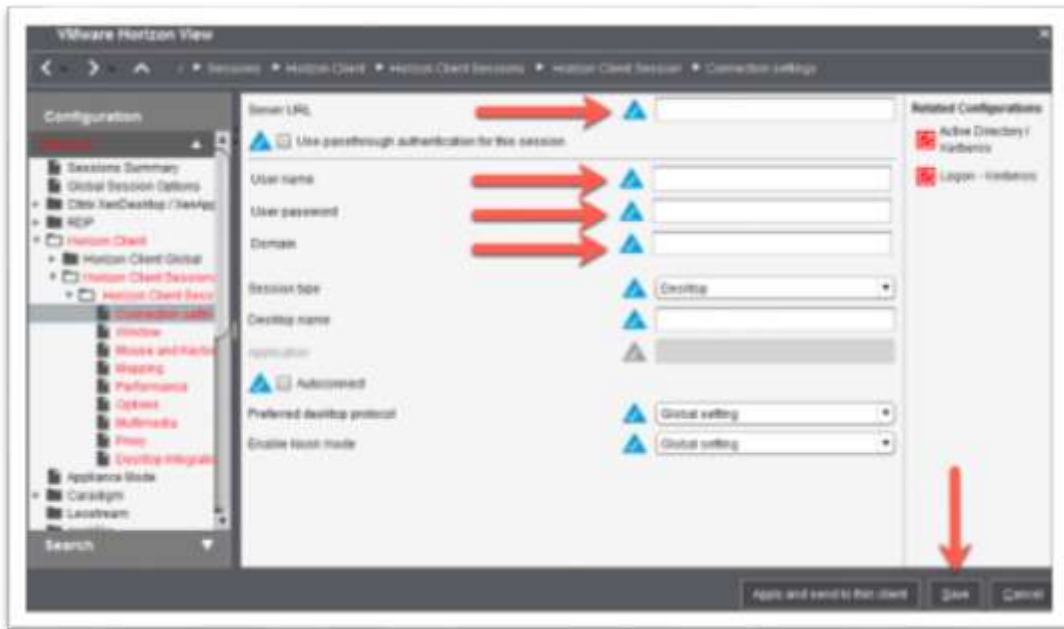
Define where you would like the session's application icon to be displayed by clicking on the desired settings blue triangle to enable editing each setting.



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 with them.

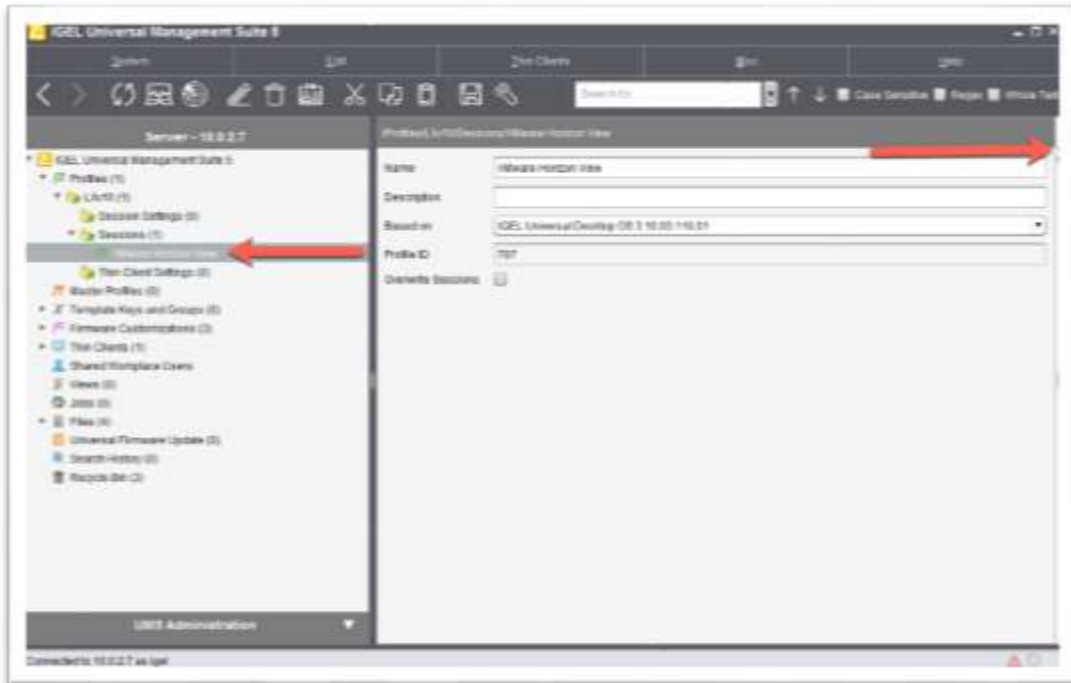
To create a simple connection, you need to configure only a couple sections. Click on the **Connection Setting** node. At the least, you are required to set the **Server URL**, **User Name**, **Password**, and **Domain**.

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

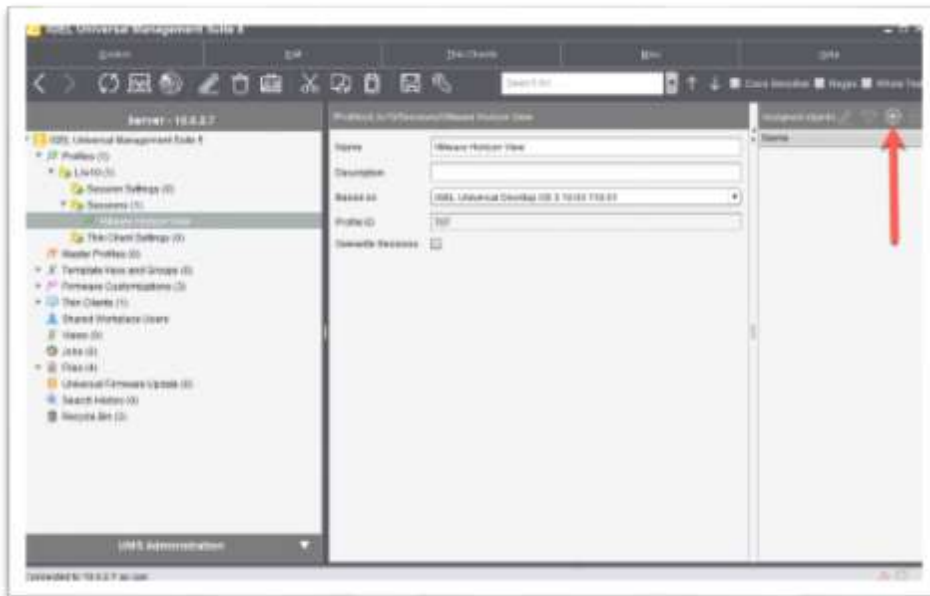


9. You are brought back to the UMS, and the VMware Horizon View client is listed in the list of profiles.

To deploy a profile, you are required to assign the profile to the desired IGEL OS thin clients. You can do by dragging the profile and dropping it on top of an IGEL OS in the Thin client node or a folder of IGEL OSEs. 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 thin clients 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.

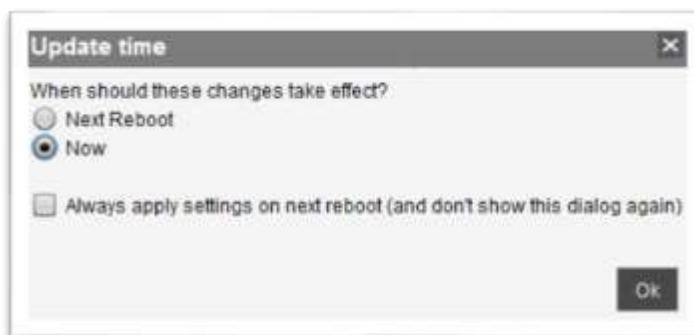


12. Once you have defined the objects, you would like to assign the profile so you can click the **OK** button to save it.



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 to the device running the IGEL OS, and you will notice the policy has taken effect and, in this case, the **Horizon Client Session** icon has been added to the desktop, and/or wherever you configured it to be placed above.

It's that simple! This is the POWER of the IGEL Platform! Trust me, you can do almost anything so have some fun and play around with profiles. Refer to the [UMS 5 Profiles Reference Manual](#) for detailed information on the UMS profile engine.



2. Customize the IGEL OS Look and Feel

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 amazing designs Apple has given us, IGEL believes that beauty is in the eye of the beholder and 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!

The Process of customizing the IGEL OS is performed using UMS Profiles and Firmware Customizations. You might find overlap as a customization might be found in both a profile and firmware customization. In this document, we have tried to use the easiest and most verbose method possible. Though, this is up to you!

To learn the finer details on Firmware Customization, please refer to

<https://kb.igel.com/endpointmgmt/en/firmware-customization-910517.html>.

This chapter is broken down into the following eight sections, when finished you will have given your users a custom, branded, and beautiful experience of their own! Even better than Apple!

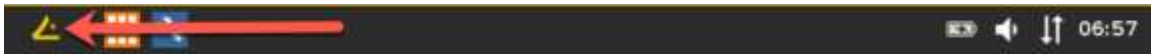
- [How to Customize the Start Button](#)
- [How to Customize the Start Menu Icon](#)
- [How to Customize the Desktop Wallpaper](#)
- [How to Customize the UI Theme Colors](#)
- [How to Customize the Screensaver](#)
- [How to Customize the Bootsplash Image](#)
- [How to Customize Session Icons](#)
- [How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

The images, icons, profiles and firmware customization created in this document can be found in the **IGEL-OS-Getting-Started.zip**, as detailed in the **IGEL-Getting-Started-Guide.zip Files Explained** Appendix section. To learn how to import the customization, please refer to the **How to Import Project Customizations** also found in the Appendix

2. 1. How to Customize the Start Button

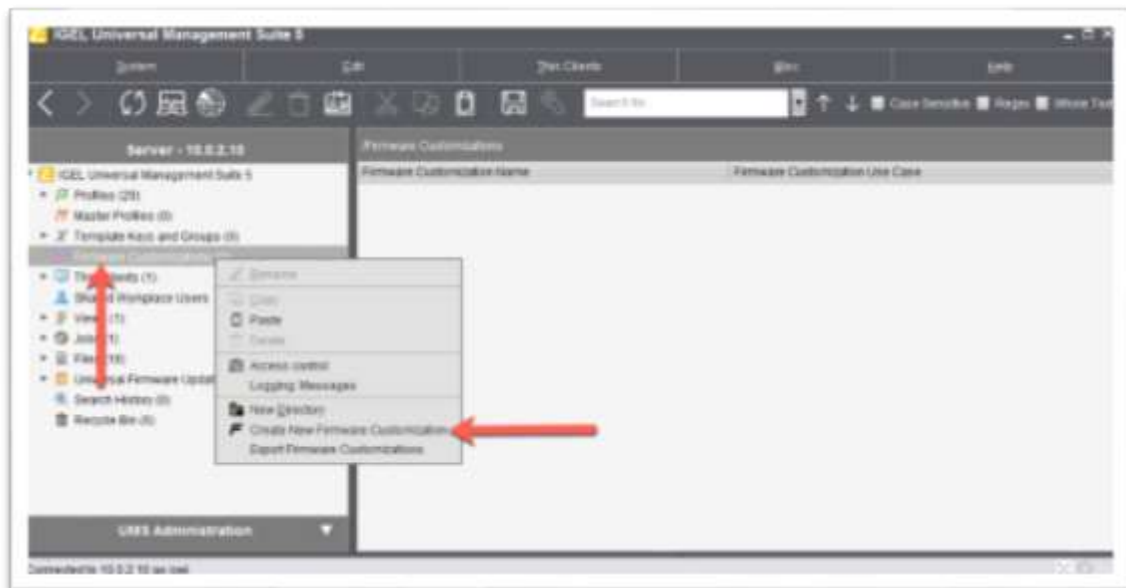
The first step in your quest to make the IGEL OS truly yours is to customize the Start button's icon. By default, IGEL uses the nose of the IGEL Hedgehog logo and who does not love a hedgehog, but this is up to you.

By default, the start menu icon is as shown below:



The following defines how to customize the start button with your company logo or an icon of your choosing:

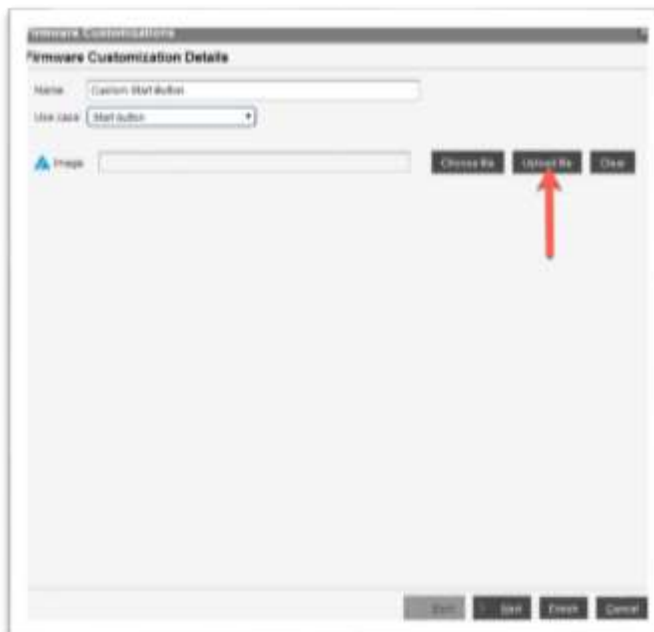
1. From the UMS, right-click the **Firmware Customizations** link in the left menu and click to select the **Create New Firmware Customization** link.



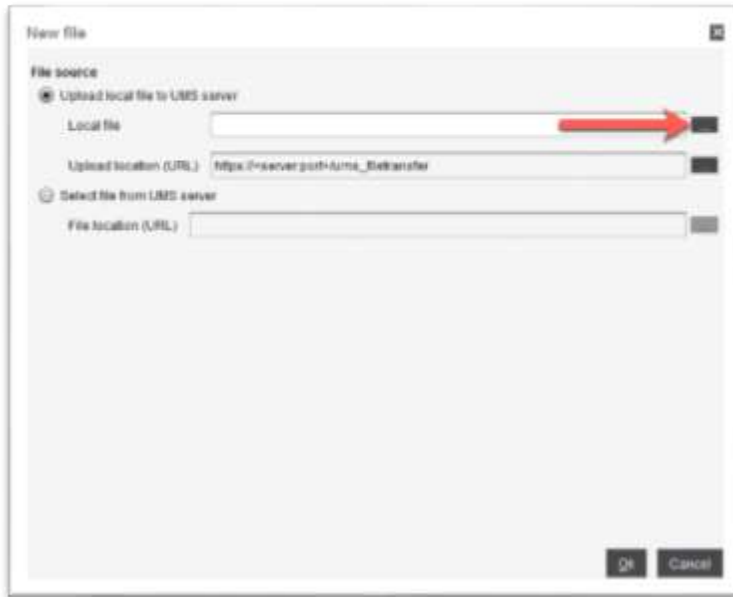
2. The **Firmware Customization Details** wizard opens. Enter a detailed name in the **Name** text box and then click to open the **Use case** combo box. You will notice the different types of firmware customizations you can configure. Click to select the **Start button** link.



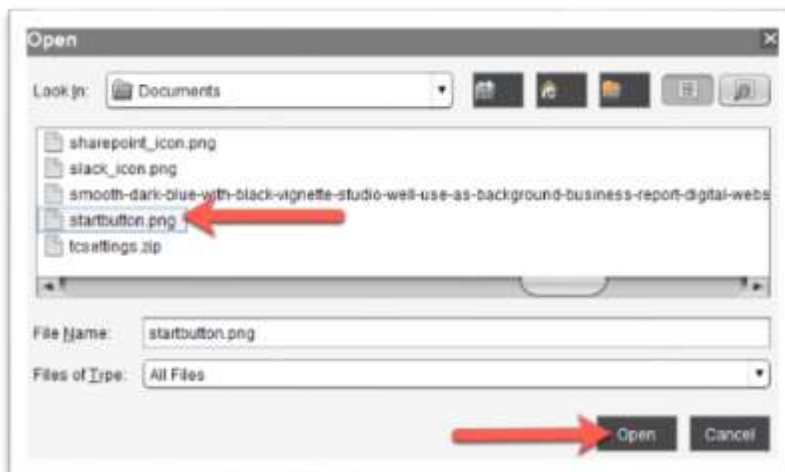
3. You are required to select the image you wish to use for the start button. You have two choices, to choose a file you have already uploaded or upload a new file now. Since this is our first customization, you will upload the image. Click the **Update file** button to continue.



4. The **New File** window opens. Click the ... button, located just to the right of the **Local File** text box to continue.



5. The **Open** window appears prompting you to select the file you wish to upload. Find the file, highlight it and click the **Open** button to continue.



6. You are brought back to the **New file** window. Verify the correct file was uploaded and click the **OK** button to continue.

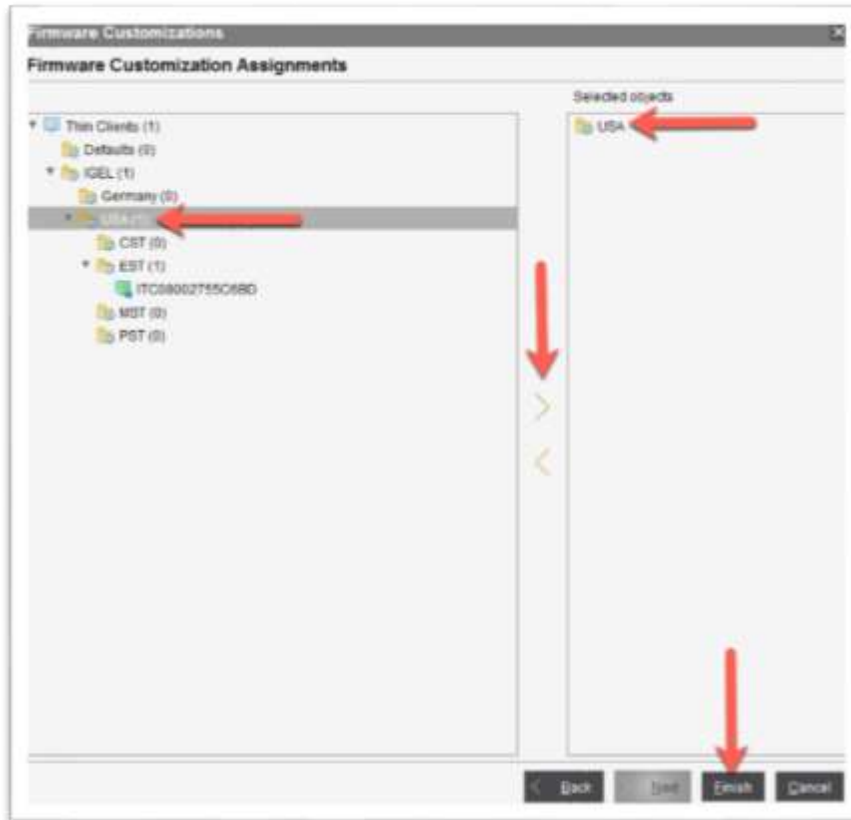


7. The new file will appear in the image text box. Click the **Next** button to continue.

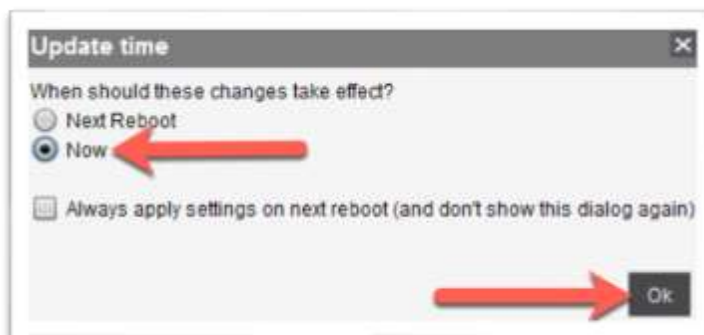


8. The **Firmware Customization Assignments** window opens prompting you to assign the firmware customization to the desired devices. A firmware customization can be assigned to a thin client or a directory. Firmware customizations take priority over profiles and are overridden by master profiles.

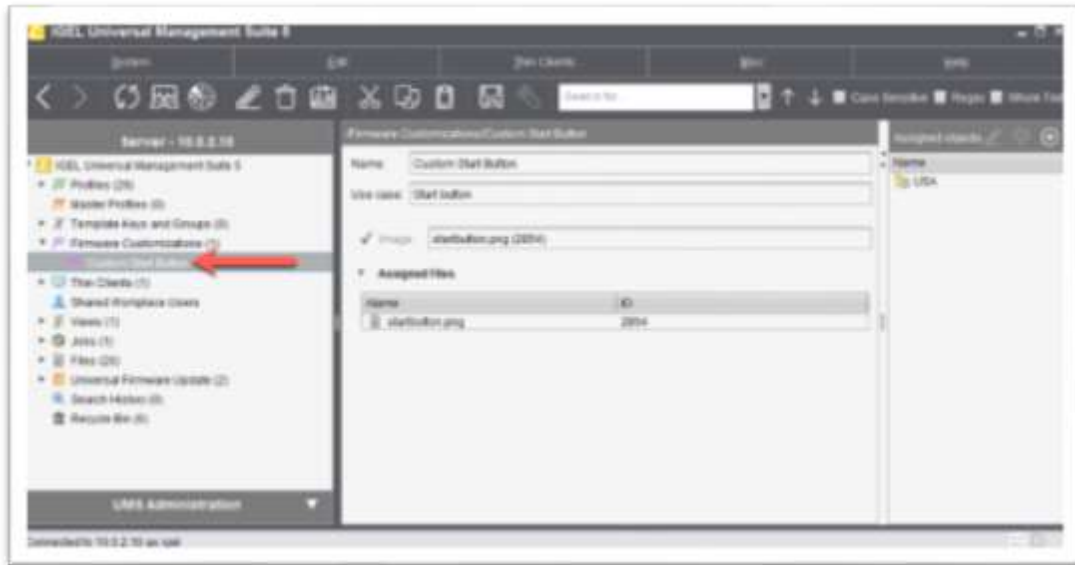
Click to select the device(s) or directories you wish to assign the firmware customization to and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign your new firmware customization



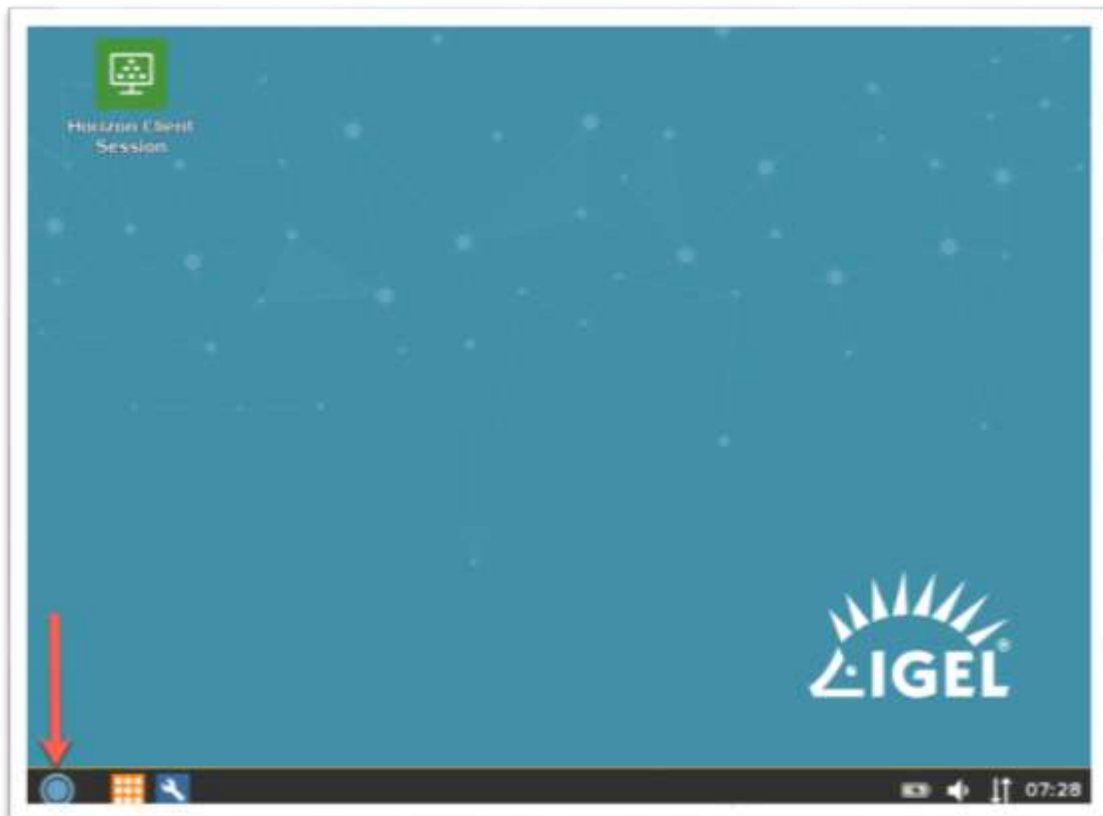
9. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



10. The firmware customization window is closed, and you are brought back to the UMS where you will see your new firmware customization listed.



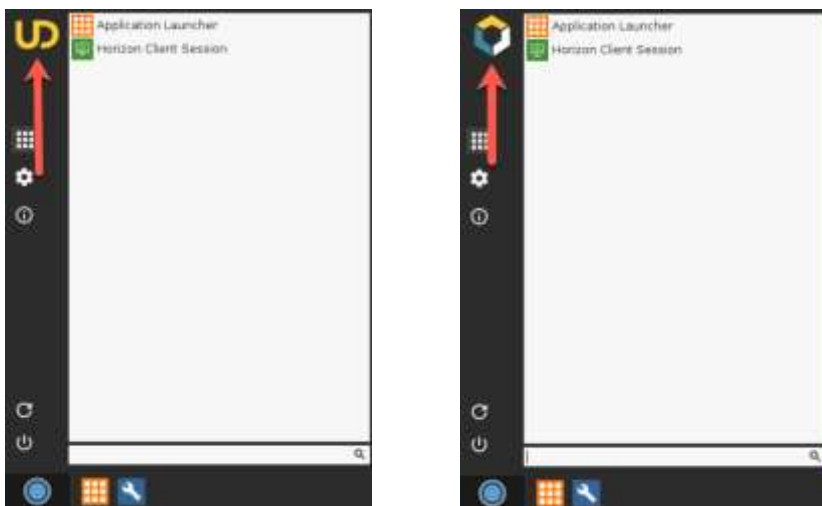
11. If you look at a managed device, you will notice the new icon has been added! Starting to look good but a few more steps to go!



2. 2. How to Customize the Start Menu Icon

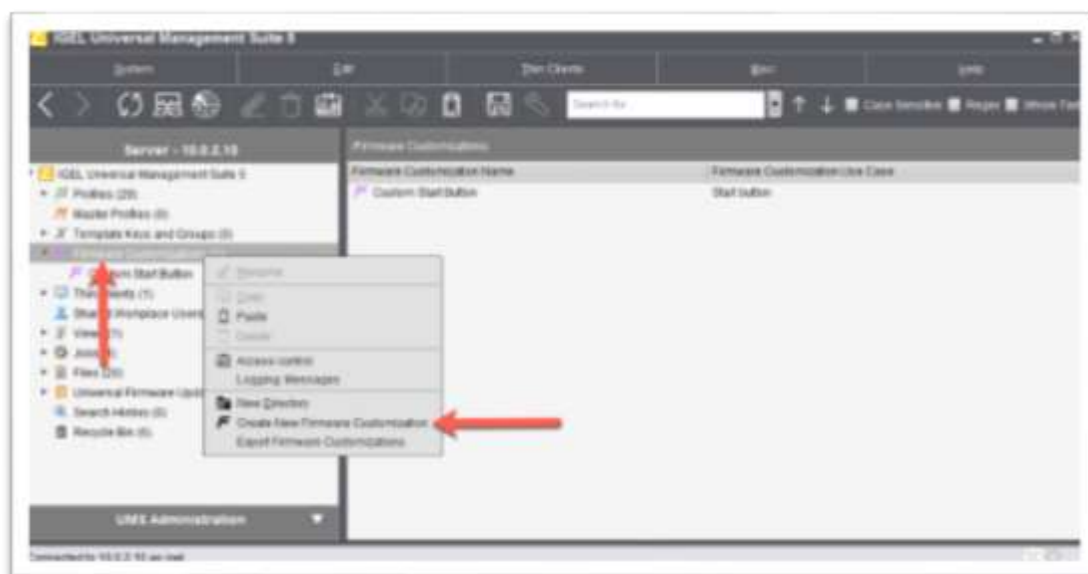
As we said, with the IGEL OS, you can customize about everything. The next item you will configure is the Start Menu icon. By default, it displays the IGEL OS Universal Desktop icon (UD), but you might want to swap it with your company logo, or possibly the IGEL Community logo, as seen below.

The following are before and after images. You will notice the beautiful IGEL Community logo has replaced the default IGEL UD image.

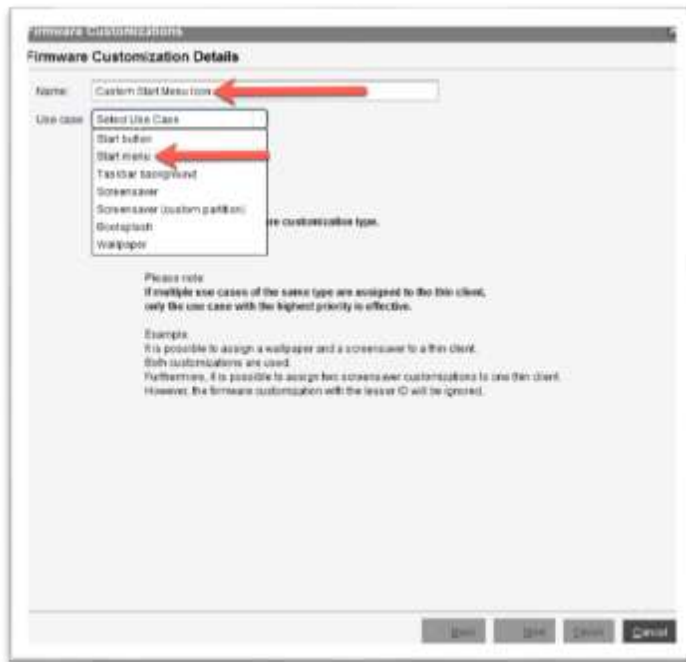


The following defines how to customize the start menu's icon:

1. From the UMS, right-click the **Firmware Customizations** link in the left menu and click to select the **Create New Firmware Customization** link.



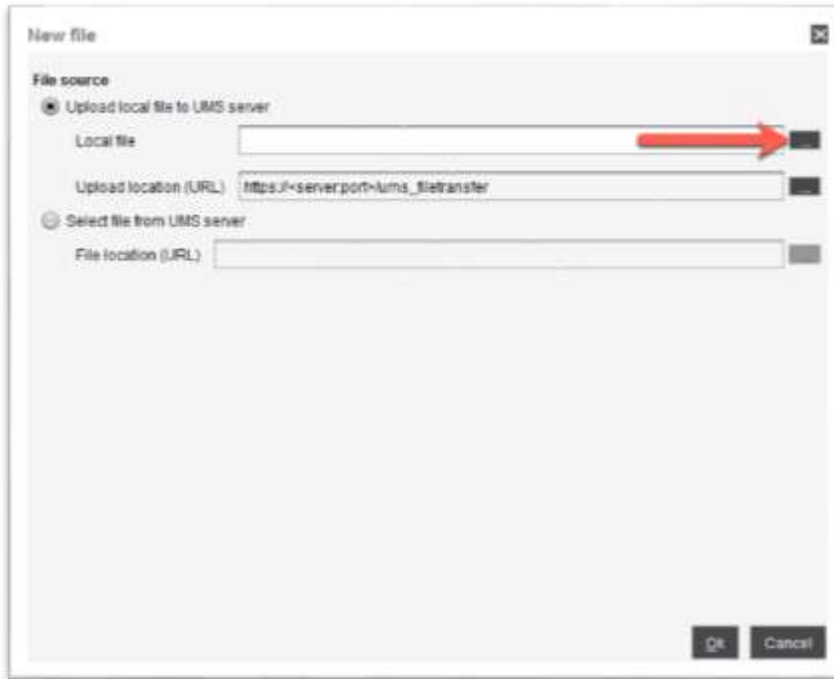
2. The **Firmware Customization Details** wizard opens. Enter a detailed name in the **Name** text box and then click to open the **Use case** combo box. Click to select the **Start Menu** link.



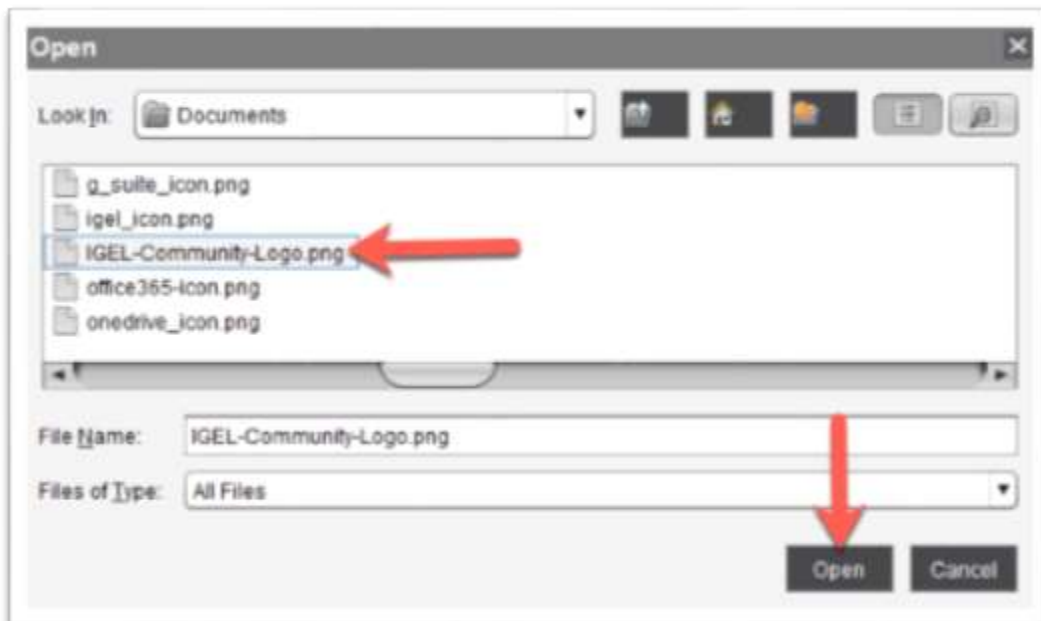
3. Next, you will select the image you wish to use for the start button. You have two choices, to choose a file you have already uploaded or upload a new file now. Click the **Update file** button to continue.



4. The **New File** window opens. Click the ... button, located just to the right of the **Local File** text box to continue.



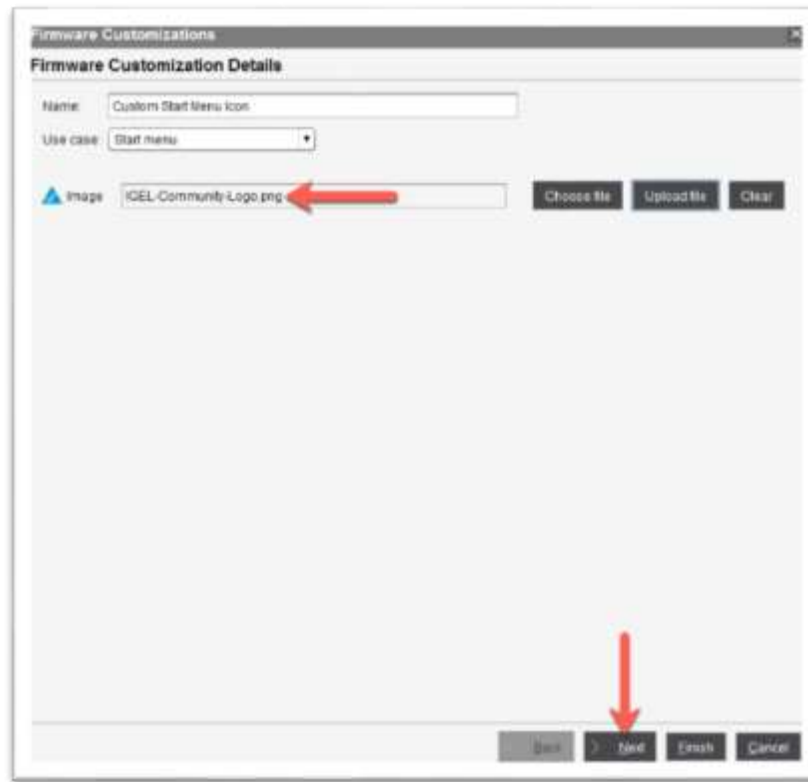
5. The **Open** window opens prompting you to select the file you wish to upload. Find the file, highlight it and click the **Open** button to continue.



6. You are brought back to the **New file** window. Verify the correct file was uploaded and click the **OK** button to continue.



7. The new file will appear in the image text box. Click the **Next** button to continue.

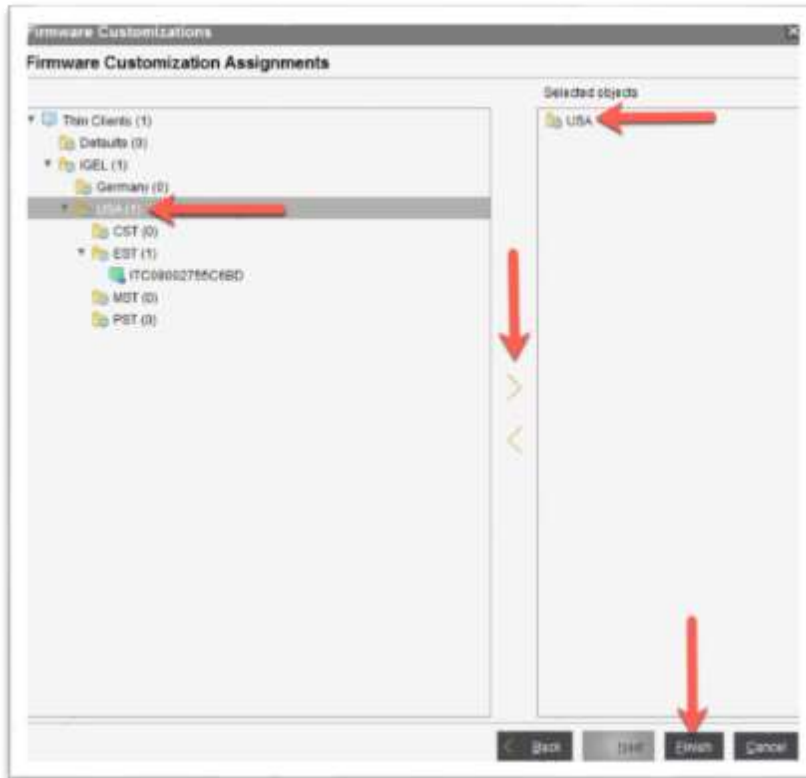


8. **Firmware Customization Assignments** window opens prompting you to assign the firmware customization to the desired devices.

Click to select a device(s) or directories you wish to assign the firmware

customization to and click the > arrow to move it to the **Selected objects** pane.

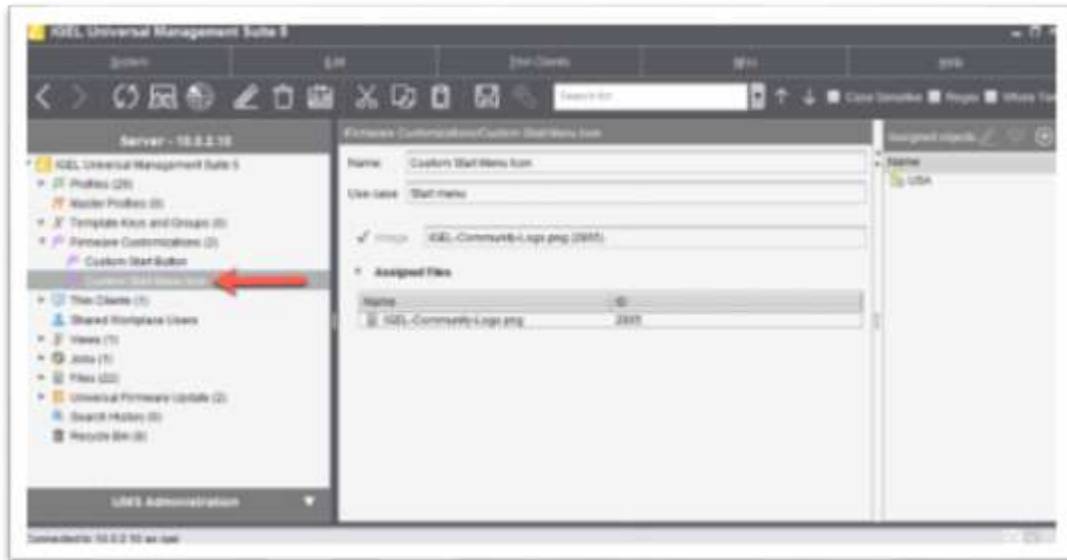
Once finished, click the **Finish** button to assign your new firmware customization.



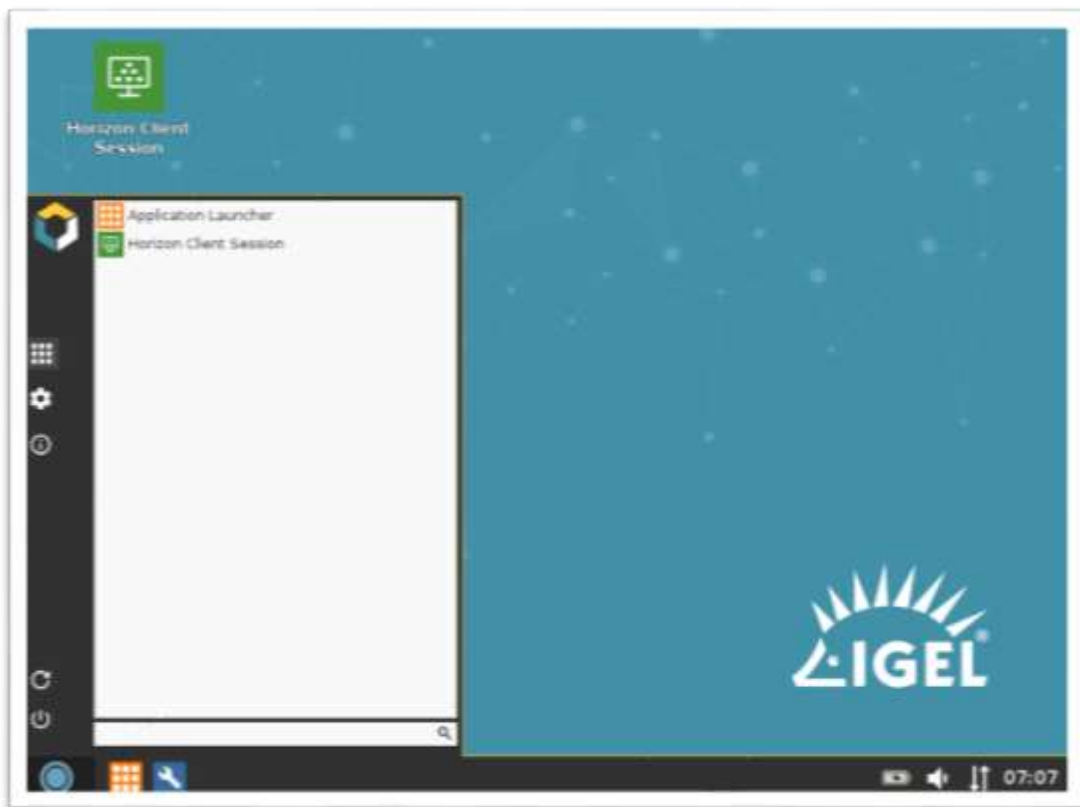
9. You are prompted to select when you would like the changes to take effect. Select the desired setting and click **OK** to continue.



10. The firmware customization window is closed, and you are brought back to the UMS where you will see your new firmware customization listed.



11. Flip over to a managed device and you will see the nice new image, as shown below.



2. 3. How to Customize the Desktop Wallpaper

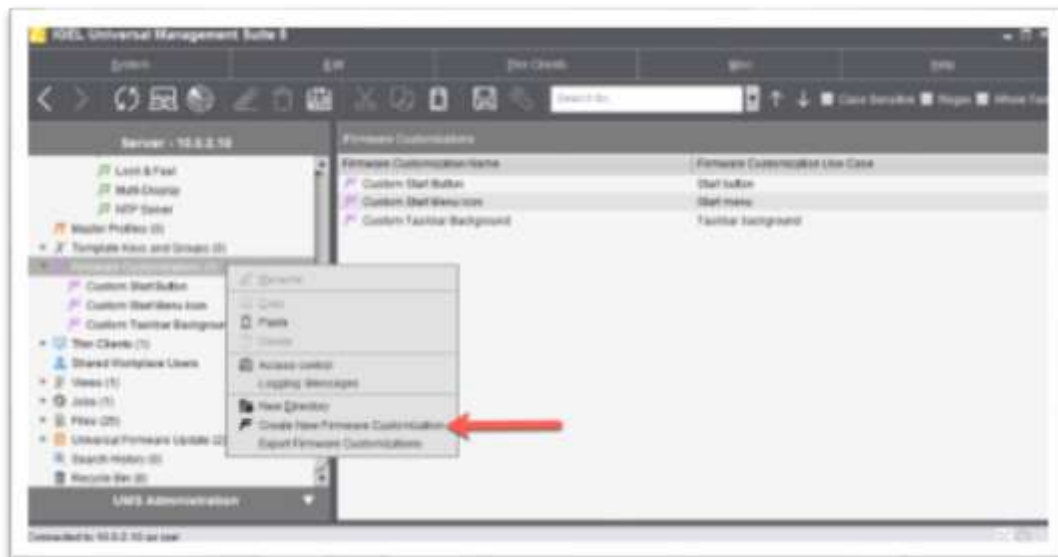
The next step in designing a beautiful user experience is to customize the wallpaper. You might want to brand it with your corporate logo or a picture of the the IT department, or maybe not that but worth a shot. No matter what image you choose, applying custom wallpaper for your users is up to you!

The following are before and after images. Notice the difference? It's starting to look good!



The following defines how to add a custom desktop wallpaper:

1. From the UMS, click on the **Firmware Customizations** link in the left menu. Click the **Create New Firmware Configuration** link in the popup menu.



- The new **Firmware Configurations** wizard opens and asks you to define the use case of the newly created rule. Enter a descriptive name in the **Name** text box and click the **Wallpaper** entry from the **Use Case** dropdown list. Click **Next** to continue.

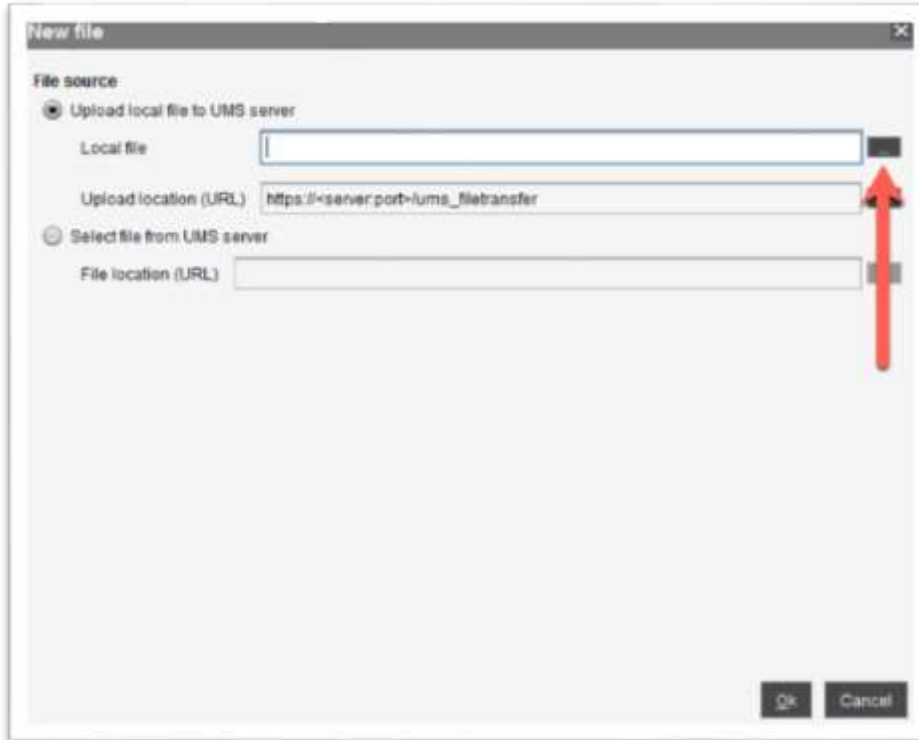


- You are prompted to select the monitors you would like to assign the new wallpaper too. As you can see, you can configure custom wallpaper for up to 8 monitors. In this case, let's configure just one. Click the **Upload File** button to continue.

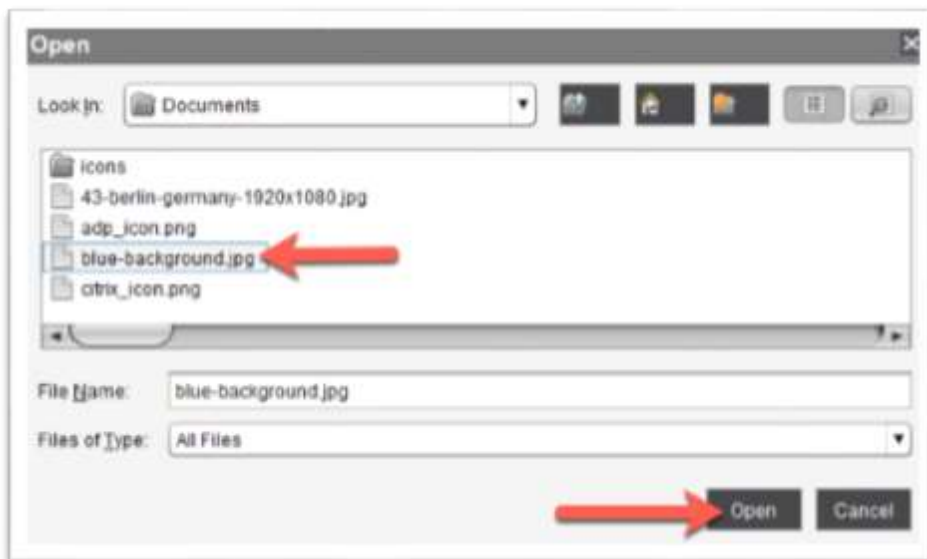


4. The **New File** window opens allowing you to upload the new image or pick one that was previously uploaded to the UMS server, maybe via FTP.

Click the ... button to upload a file from the local filesystem.



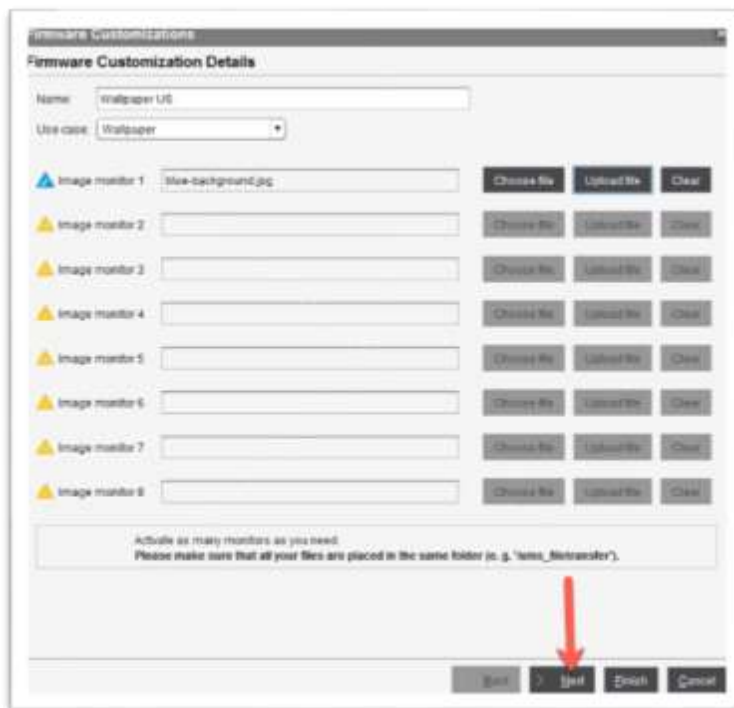
5. Browse to the location of your background image and click the **Open** button.



6. Verify your desired image file location is correct and click the **OK** button to continue.

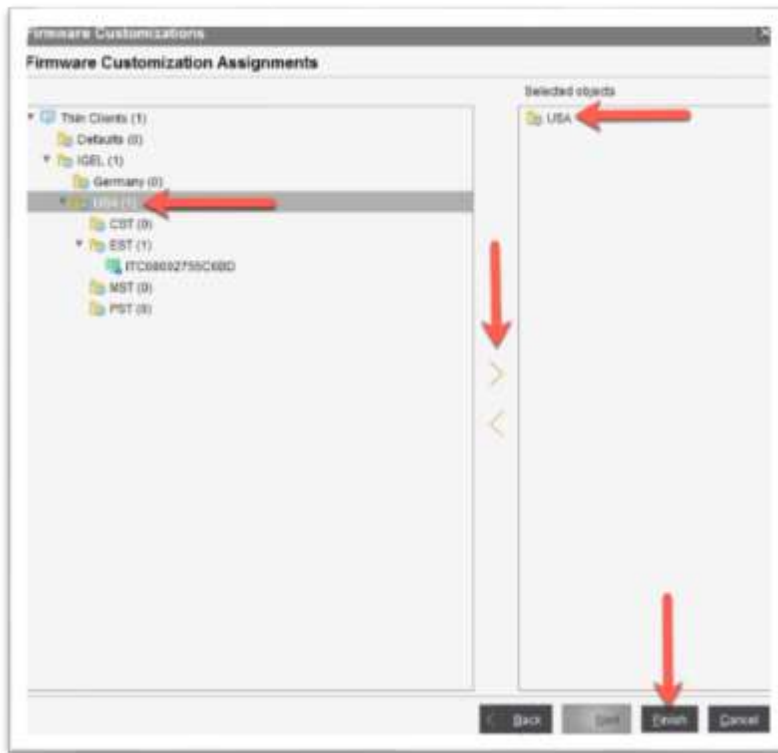


7. If you would like to assign additional images, either click the **Upload File** button to upload a new image or you can click the **Choose File** button if you have the desired image already on the server. Click **Next** to continue.

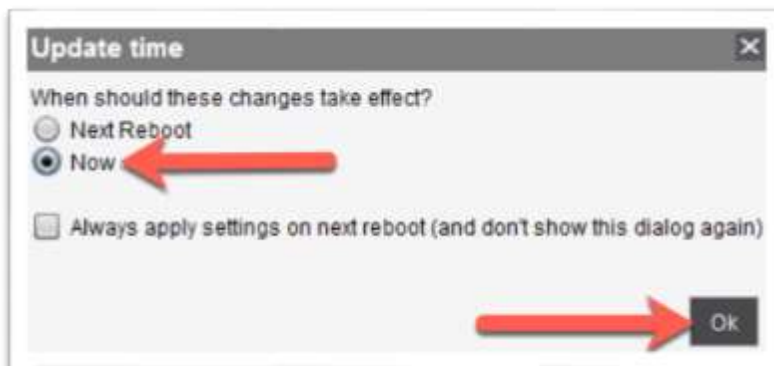


8. You are ready to apply the customization to your devices. Depending on the folder structure you have or have not created you can assign this policy accordingly. Click to select the folder and click the > arrow to move it to the right column, thus assigning the desired folder to the new customization.

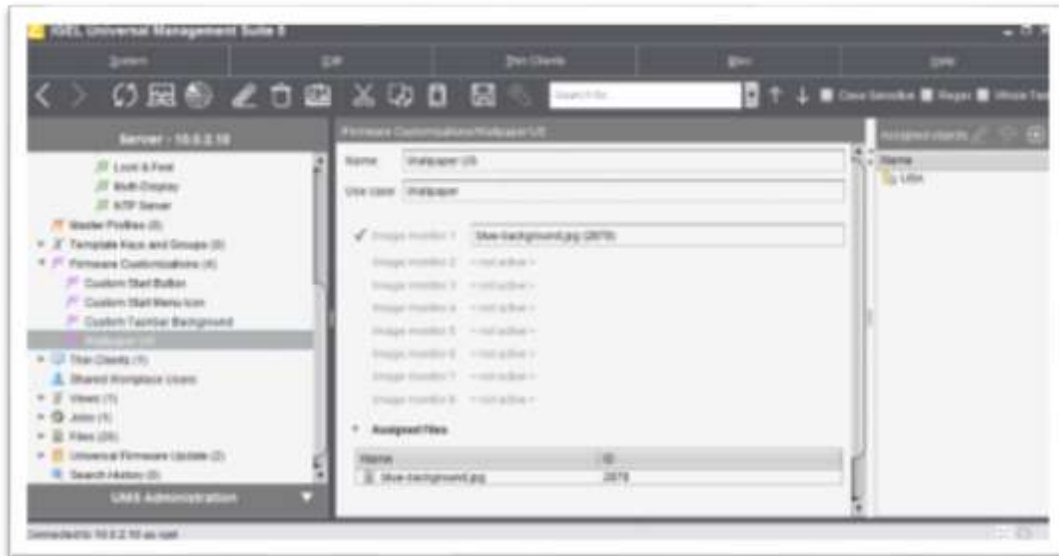
Repeat this step to apply the customization to multiple folders. Click the **Finish** button to assign the firmware customization to the desired devices.



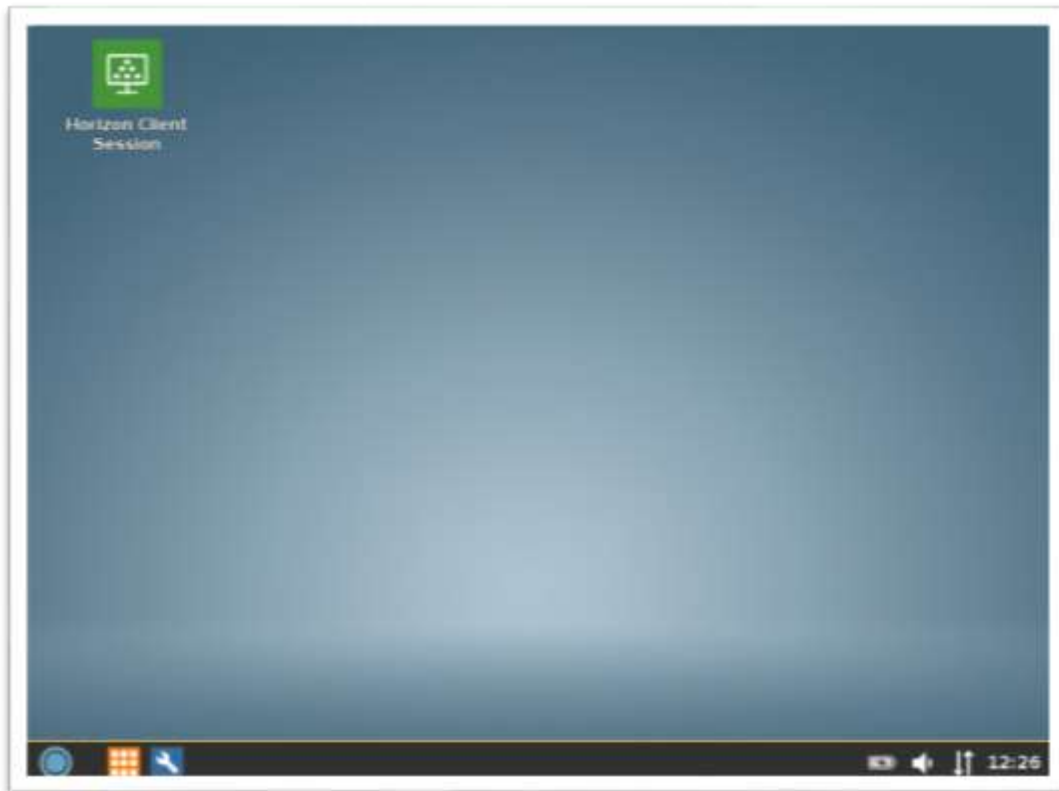
9. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



10. The **Firmware Customization** properties page appears listing the details of the specific customization.



11. Head on over to your managed IGEL OS, and you might notice it is starting to look beautiful! Now I would be proud to use such a look and feel!

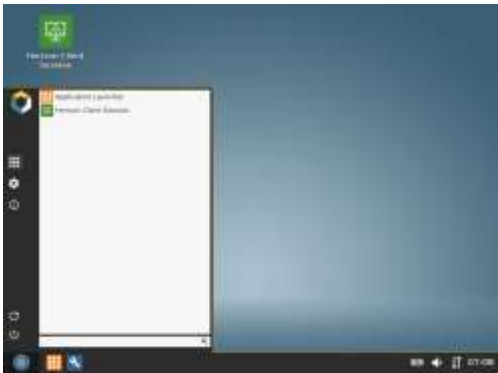


2. 4. How to Customize UI Theme Colors

The user-interface (UI) is starting to look good. Next step is to match the UI theme colors with the background color. This process is best done using a UMS profile as it gives you the most flexibility.

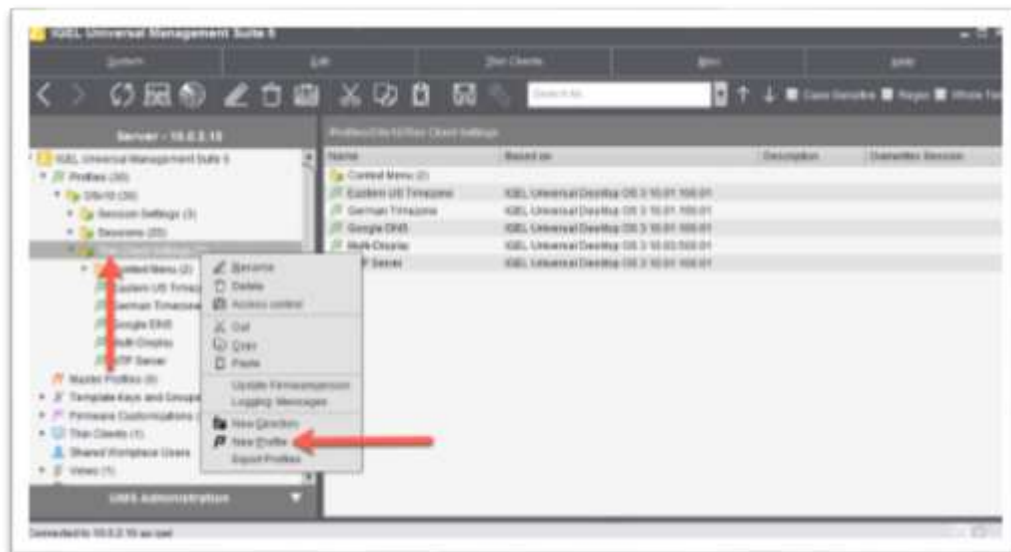
In this section, you will not only configure the UI base and highlight colors but also the color of the taskbar itself. Configuring the taskbar background can also be done using a firmware customization, as you might have noticed. Though this process is less flexible than using a profile and since you will be creating a profile to customize the UI colors it only makes sense to customize the taskbar colors at the same time.

The following are before and after images. You will notice the taskbar and start menu now match the background perfectly. Steve would be proud.

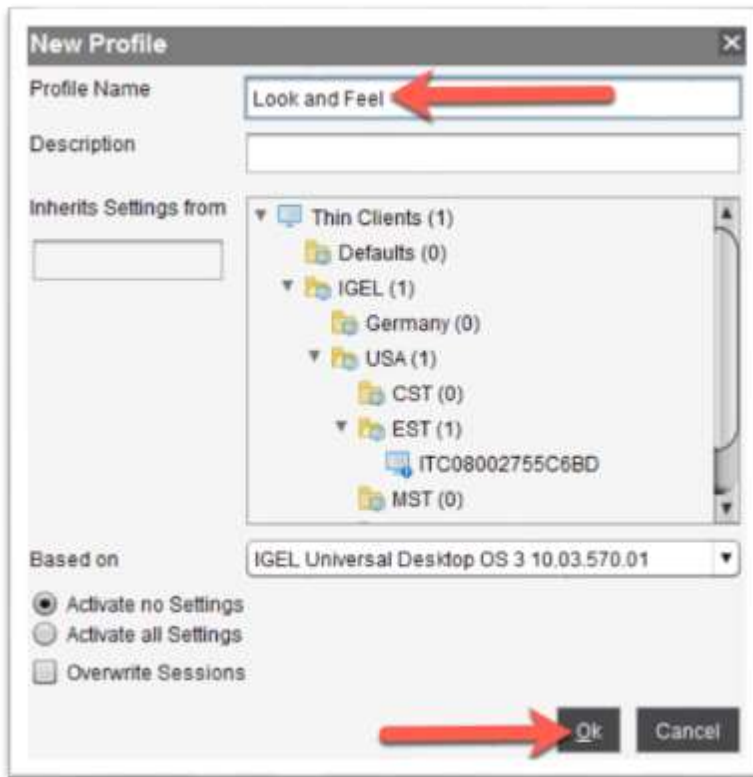


The following details how to customize the UI colors:

1. From the UMS, right-click the location you wish to store the new profile and click to select the **New Profile** link.



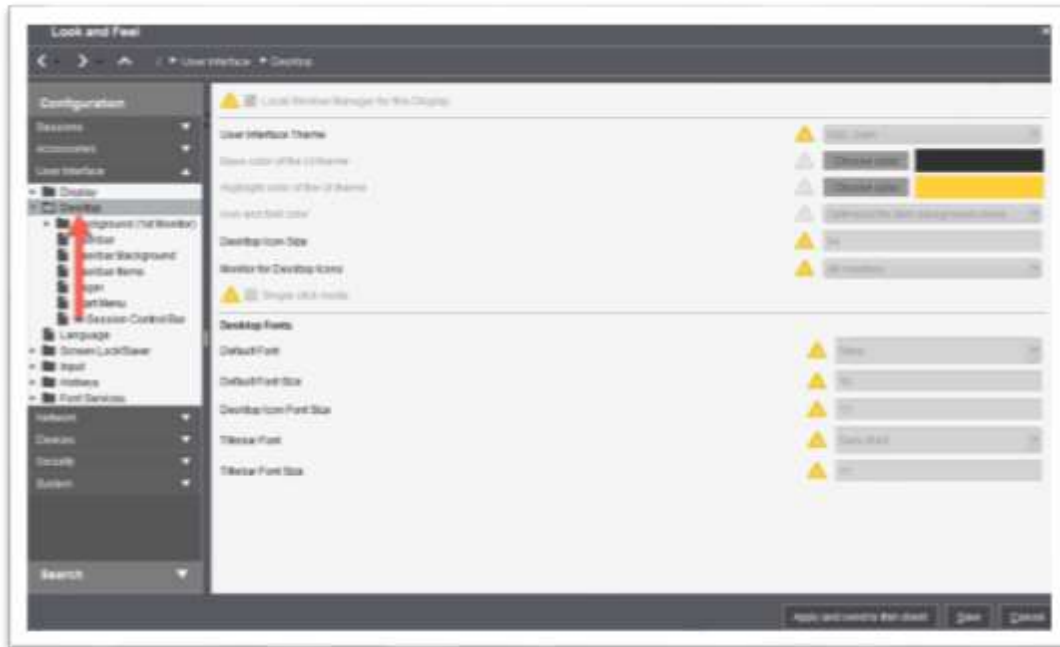
2. Enter a detailed name in the **New Profile** text box and click the **OK** button to continue.



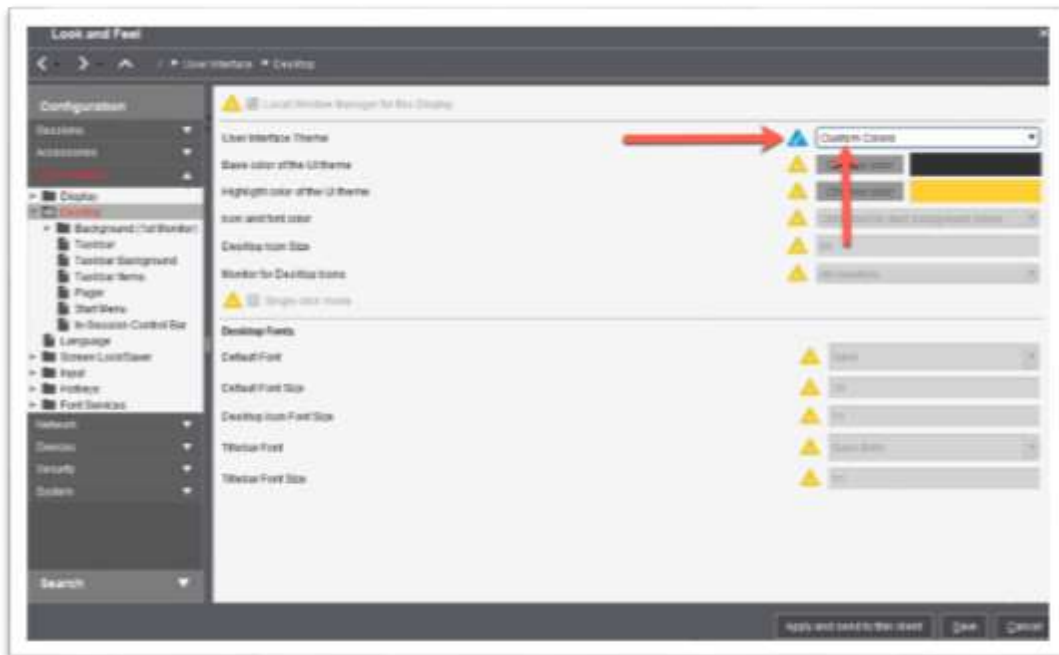
3. The new profile window opens. Click to expand the **User Interface** section



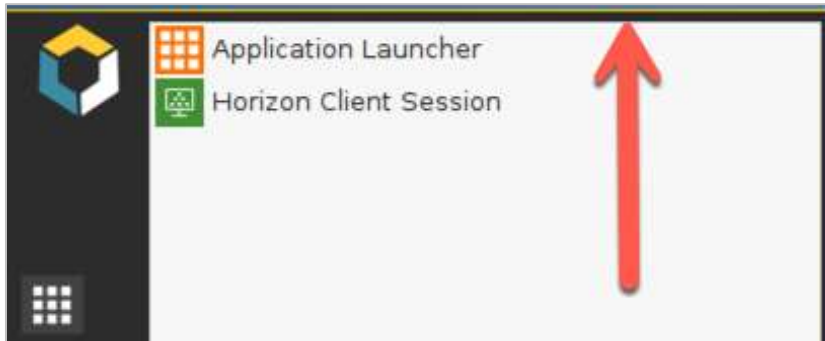
- Click to select the **Desktop** node. This is where you will customize the UI theme colors and a few other configurations.



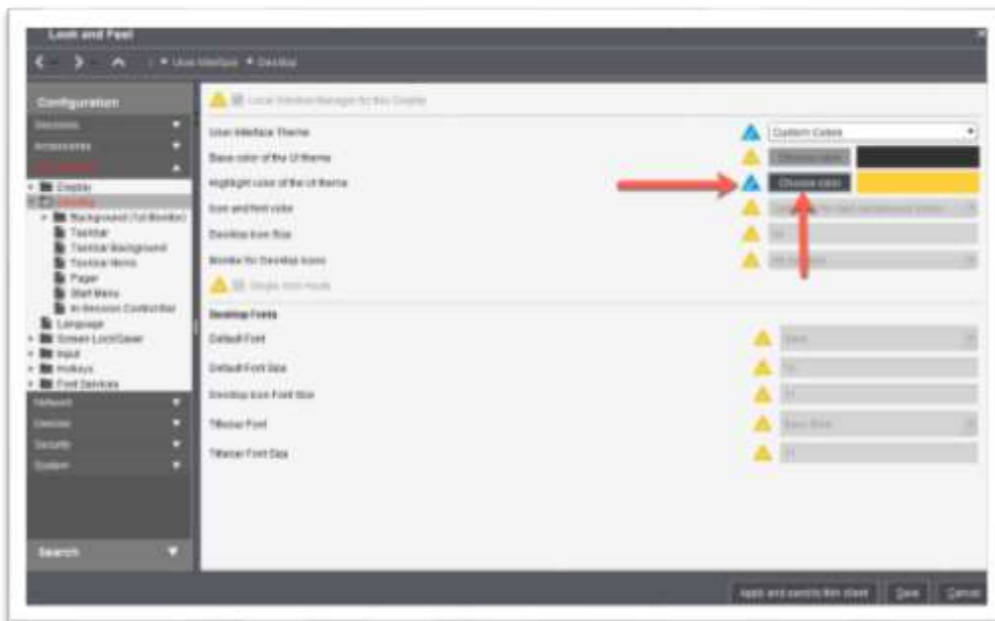
- Click the **User Interface Theme** triangle checkbox to enable it (turns blue) and then select **Custom Colors** from the drop-down combo box list.



6. The first thing you want to configure is the highlight color. This is the color that you see as a slight border color around the start menu, taskbar and other places within the IGEL OS UI.



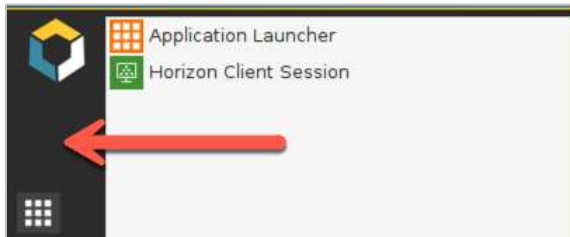
Click the **Highlight color of the UI theme** triangle checkbox to enable it (turns blue) and click the **Choose color** button.



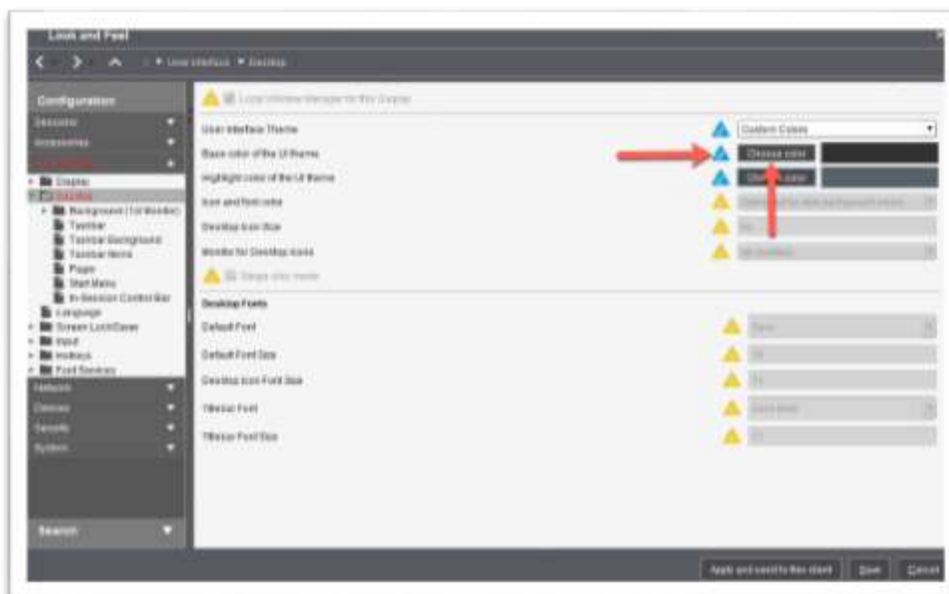
7. The **Choose color** window opens prompting you to select the color of your choosing. Enter the desired color and click the **OK** button to continue.



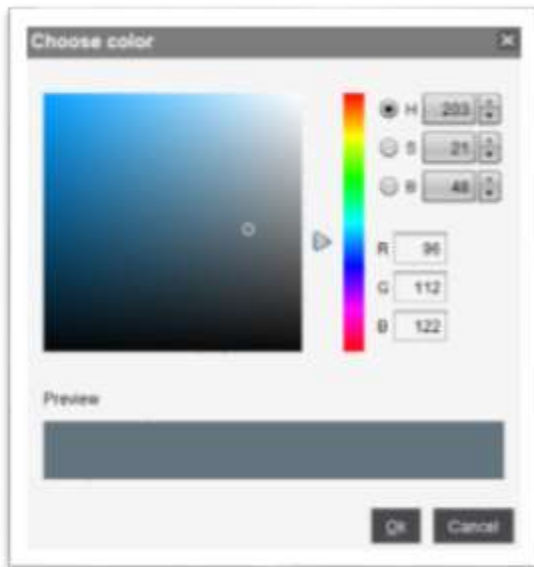
8. The next color you will want to change is the base color of the user interface.



Click the **Base color of the UI theme** triangle checkbox to enable it (turns blue) and click the **Choose color** button.

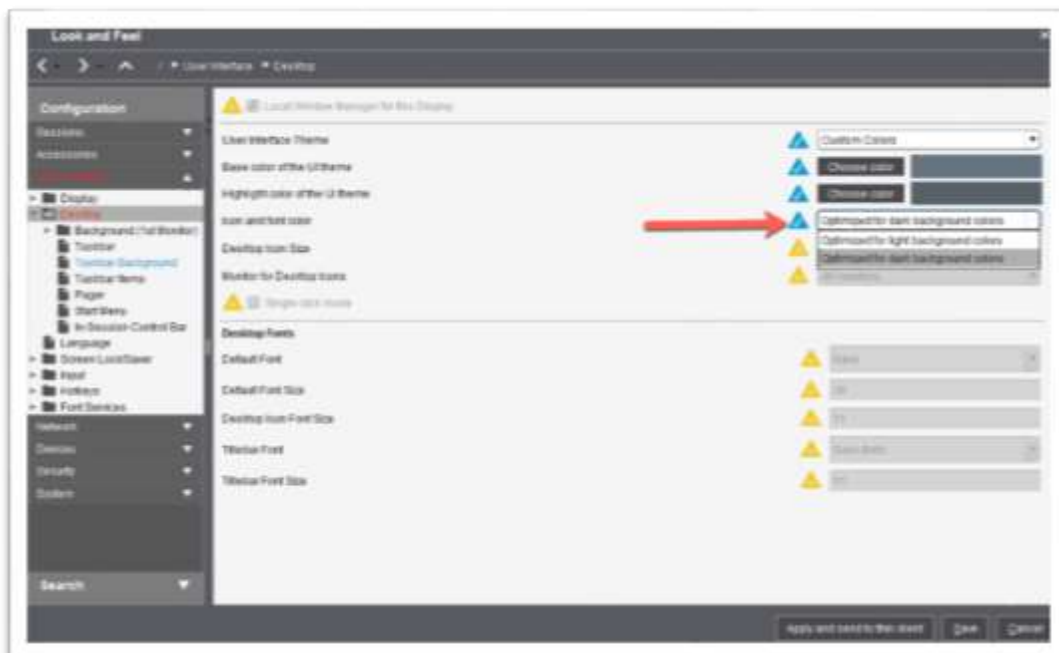


9. The **Choose color** window opens prompting you to select the color of your choosing. Enter the desired color and click the **OK** button to continue.



10. The next item in the list allows you to configure the font and icon color. This setting is used to change the color of the icons and fonts to fit with the color of the background you are using. For example, if your background is dark, you will want to use light fonts and icons. If the background color is white, then you will want to use dark fonts and icons, so they are more visible to the reader.

If this example, the default setting works great so you can skip this setting but do keep it in mind in case your background is light.

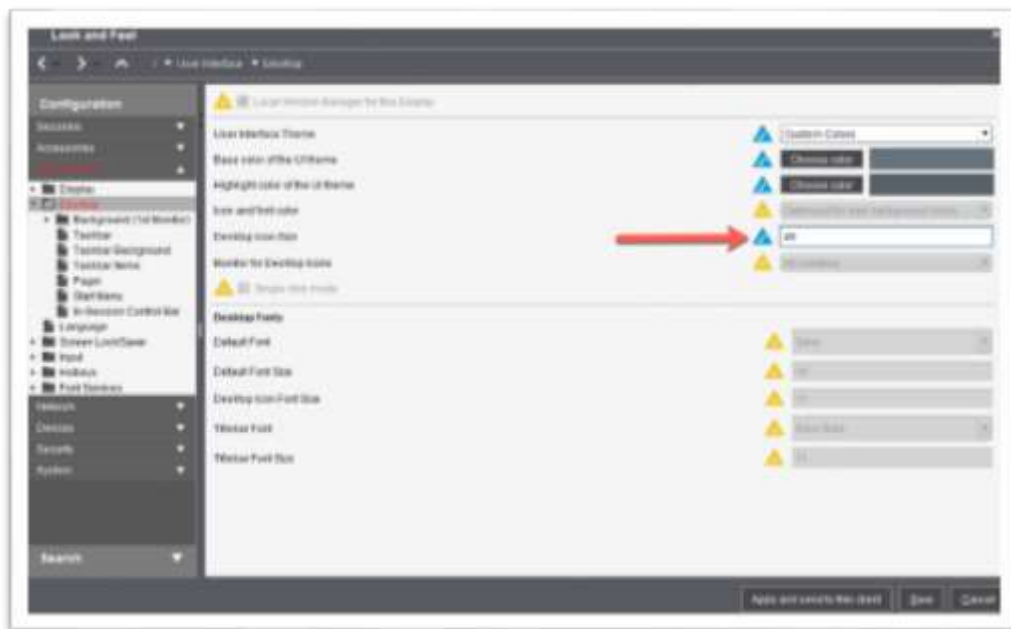


11. In design spacing is everything. Although, with the IGEL OS one of the few things that you can't do is adjust the spacing between the desktop icons. However, you can change the size of the icons, and at the same time the spacing between each icon gets a bit smaller and looks a bit better, or at least to the eyes of this author.

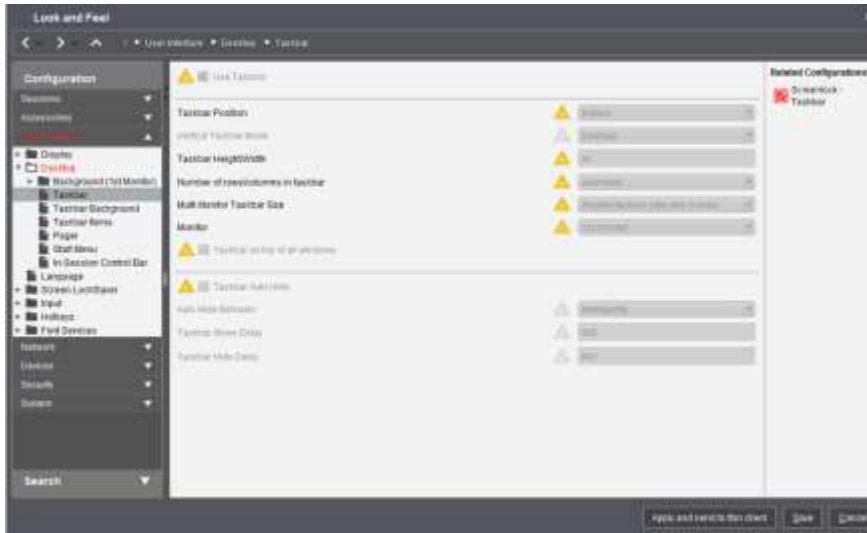
Below are before and after images of the subtle change to icon spacing when using the **Desktop Icon Size** setting. You will notice it is just a bit more appealing.



Click the **Desktop Icon Size** triangle checkbox to enable it (turns blue) and enter the desired font size. Feel free to play around with this number to find the suitable spacing to meet your design goals.



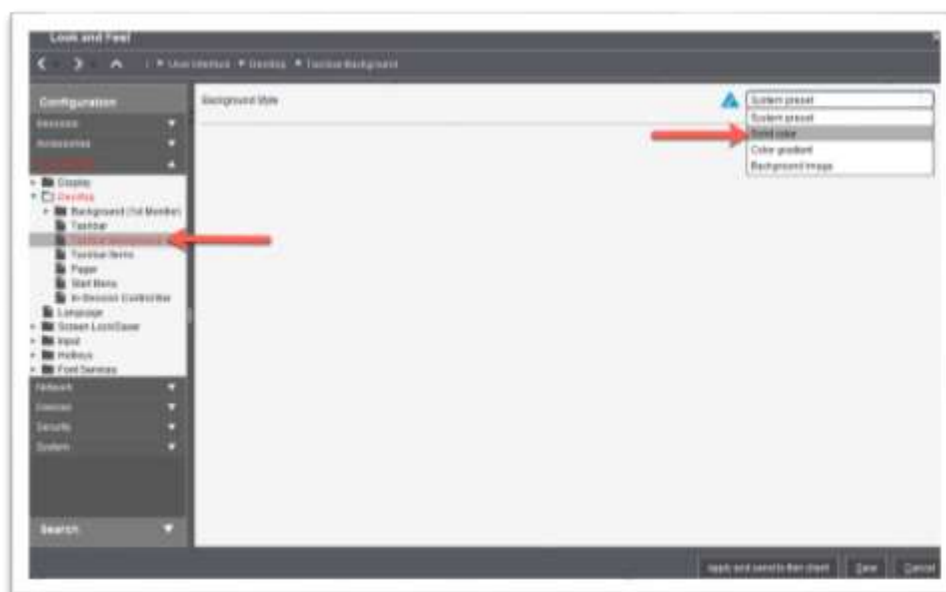
12. You are ready to configure the look and feel of the taskbar. Click to select the **Taskbar** policy node in the left menu. On this page, you will notice many different configurations you can make. For example, you can completely disable the taskbar by unchecking the **Use Taskbar** checkbox or change the height, number of rows, if it works on multiple monitors, etc. As with all configuration, please feel free to play around. For now, you can skip to the next step.



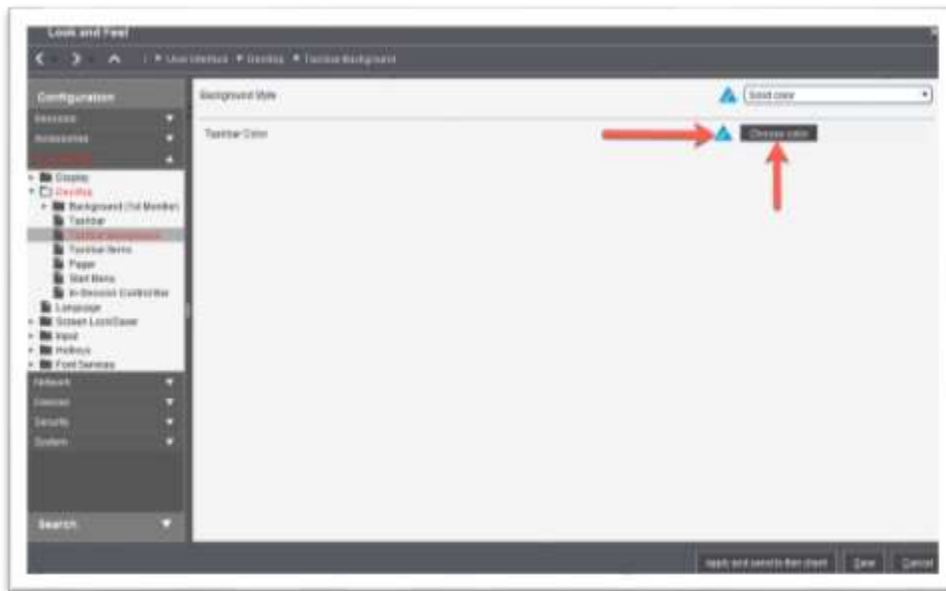
13. You are ready to change the color of the taskbar's background.



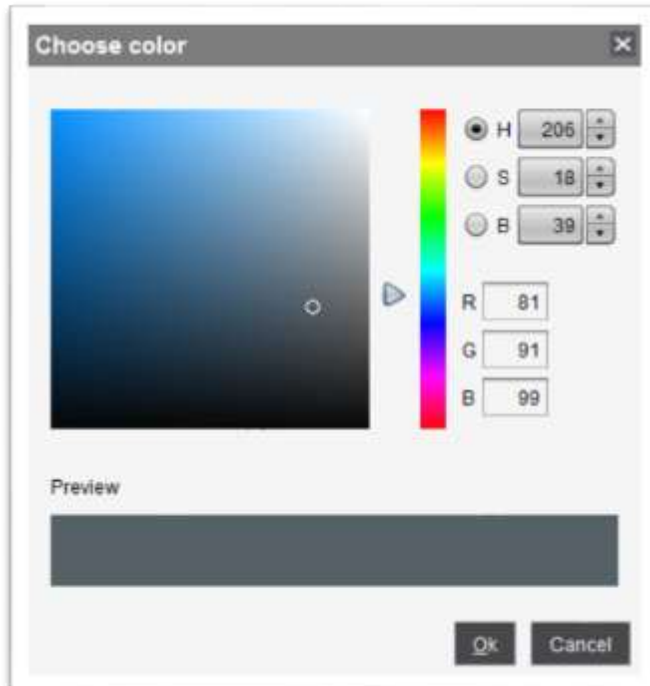
Click to select the **Taskbar Background** profile node and then click the **Background Style** triangle checkbox to enable it (turns blue) and click the **Solid color** button.



14. Click the **Taskbar Color** triangle checkbox to enable it (turns blue) and click the **Choose color** button.

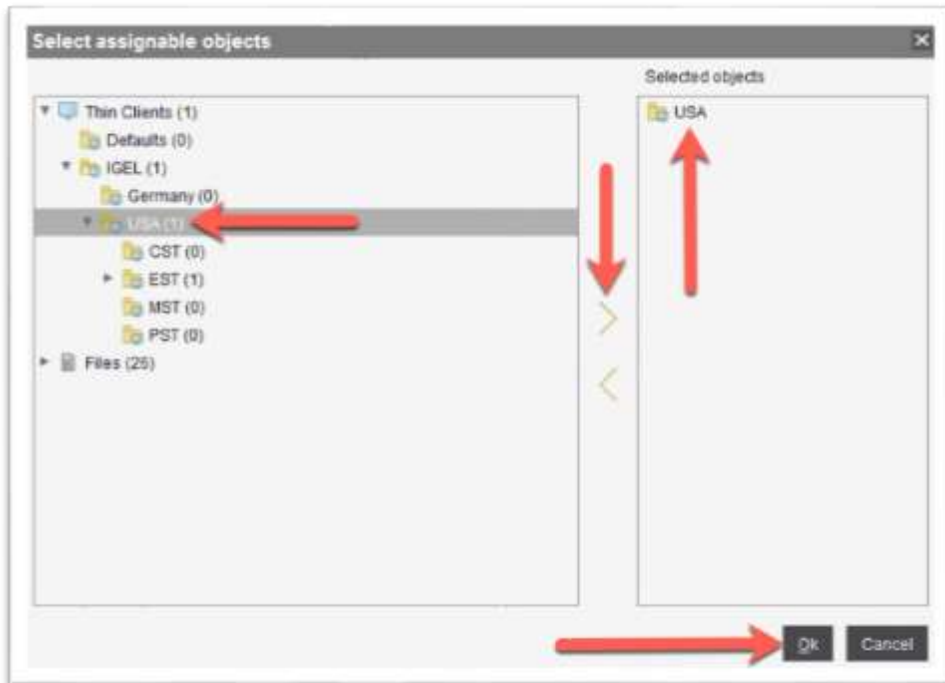


15. The **Choose color** window opens prompting you to select the color of your choosing. Enter the desired color and click the **OK** button to continue.



18. The **Select assignable objects** window opens allowing you to assign the profile to the desired folder(s) and/or device(s).

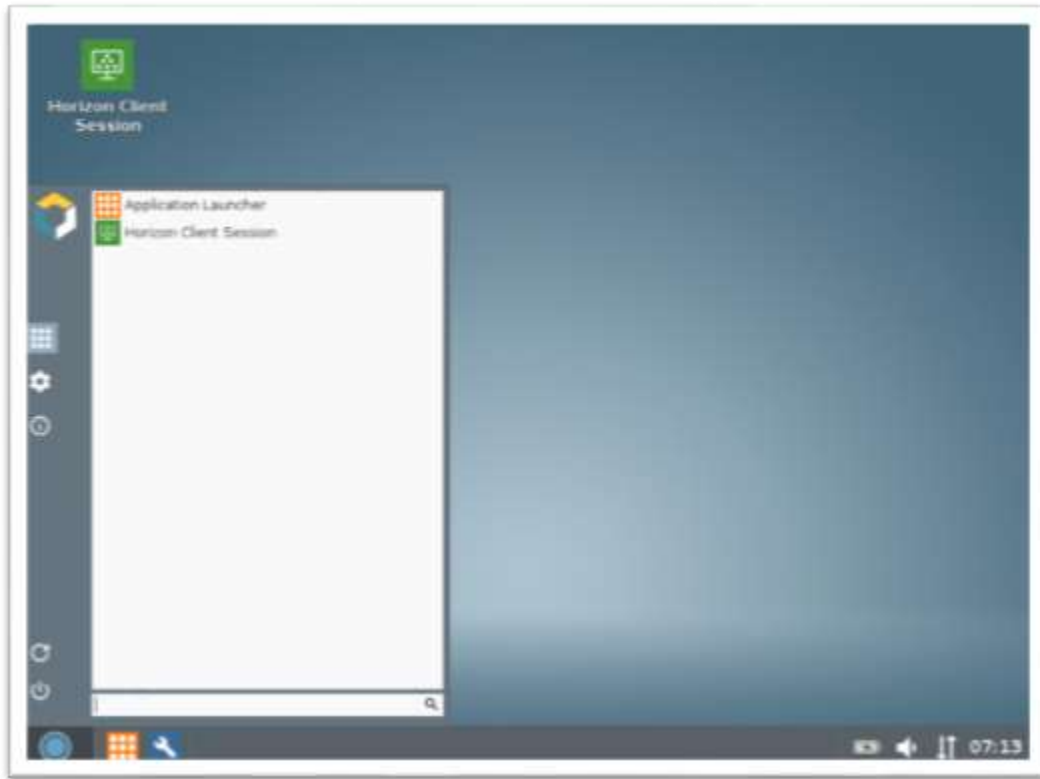
Click to select the device(s) or folder(s) you wish to assign and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign the profile.



19. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



20. Look to one of your managed devices; you will see the user interface colors of the start menu and the taskbar have been changed. Starting to look good!



2. 5. How to Customize the Screensaver

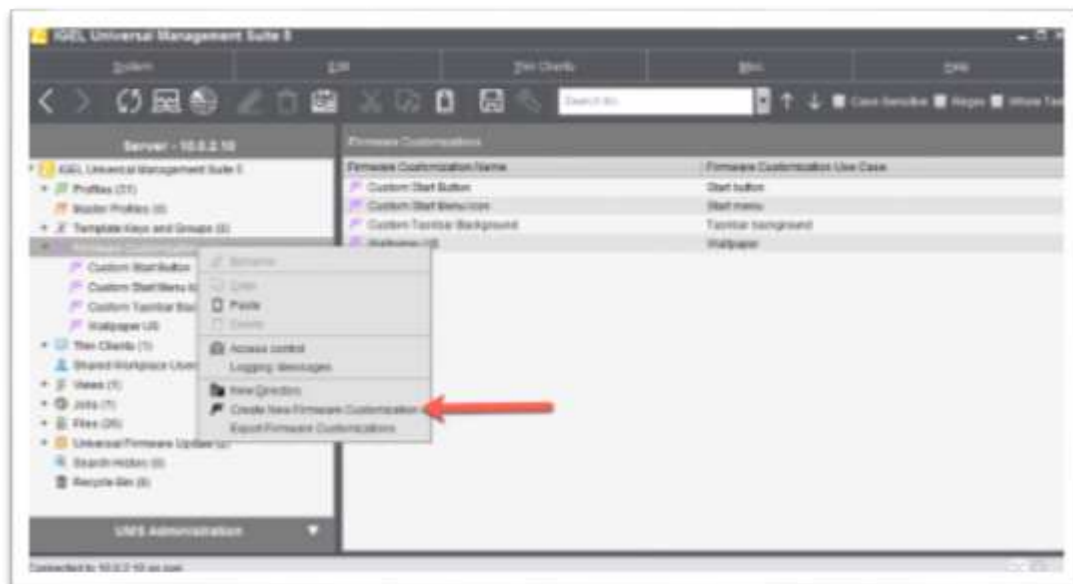
The UI is looking good! It is time to work on the fine details and round off the complete design. The next item is the screensaver. Like with the start button and background this can be done using a firmware customization.

The following are before and after images. Notice you can change the image and the background color.

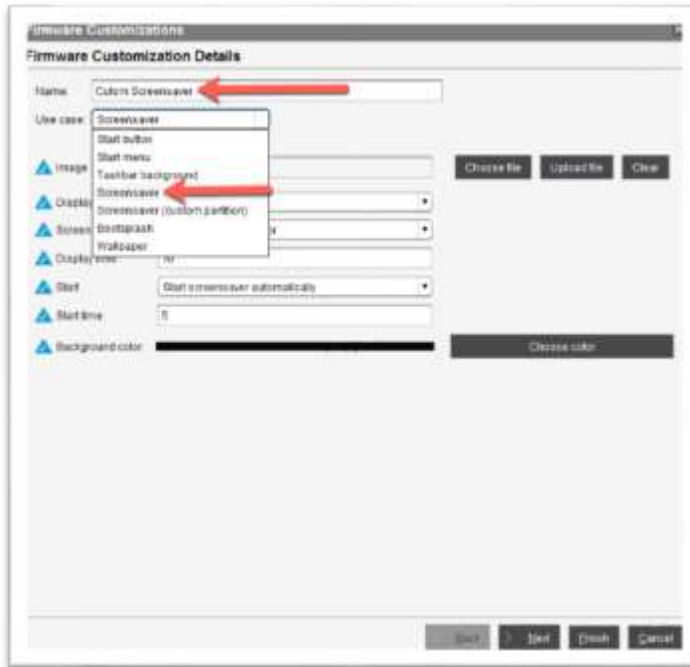


The following defines how to customize the screensaver:

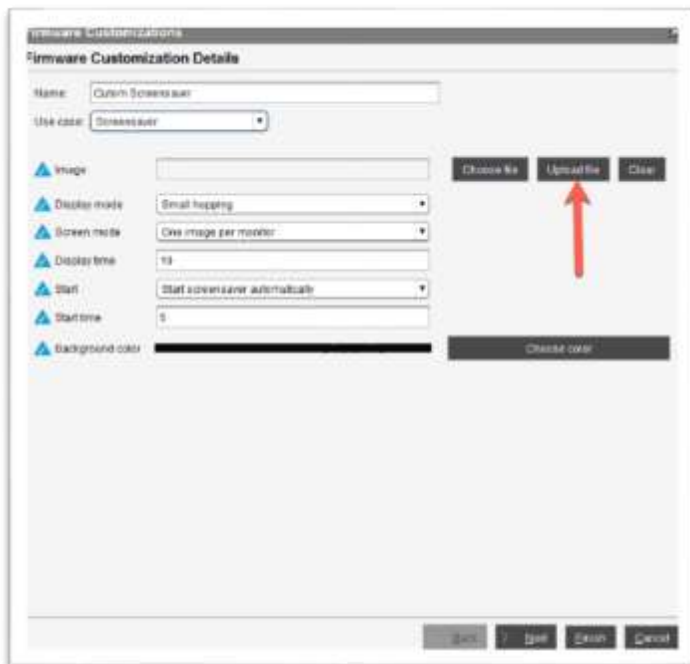
1. From the UMS, right-click the **Firmware Customizations** link in the left menu and click the **Create New Firmware Customization** link.



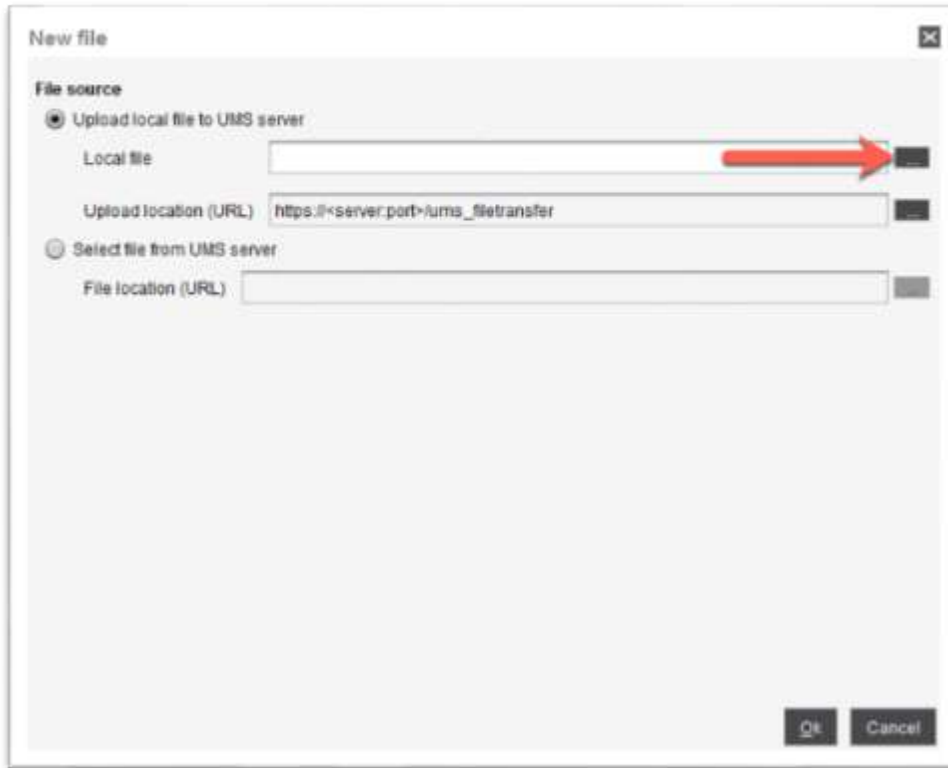
- The **Firmware Customization Details** wizard opens. Enter a detailed name in the **Name** text box and click to open the **Use case** dropdown combo box. Click to select the **Screensaver** link.



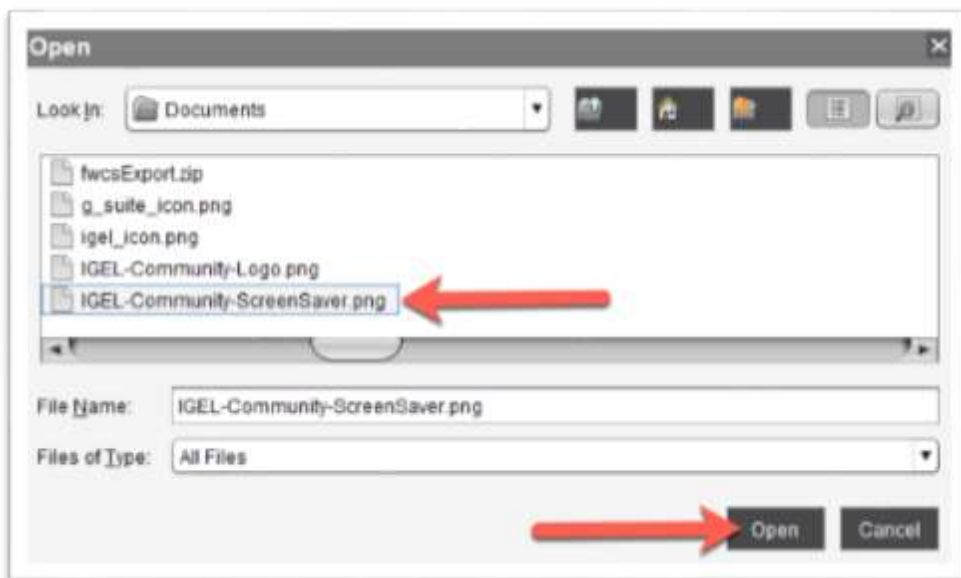
- You are required to select the image you wish to use for the screensaver image. You have two choices, to choose a file you have already uploaded or upload a new file now. Click the **Update file** button to continue.



4. The **New File** window opens. Click the ... button, located to the right of the **Local File** text box to continue.



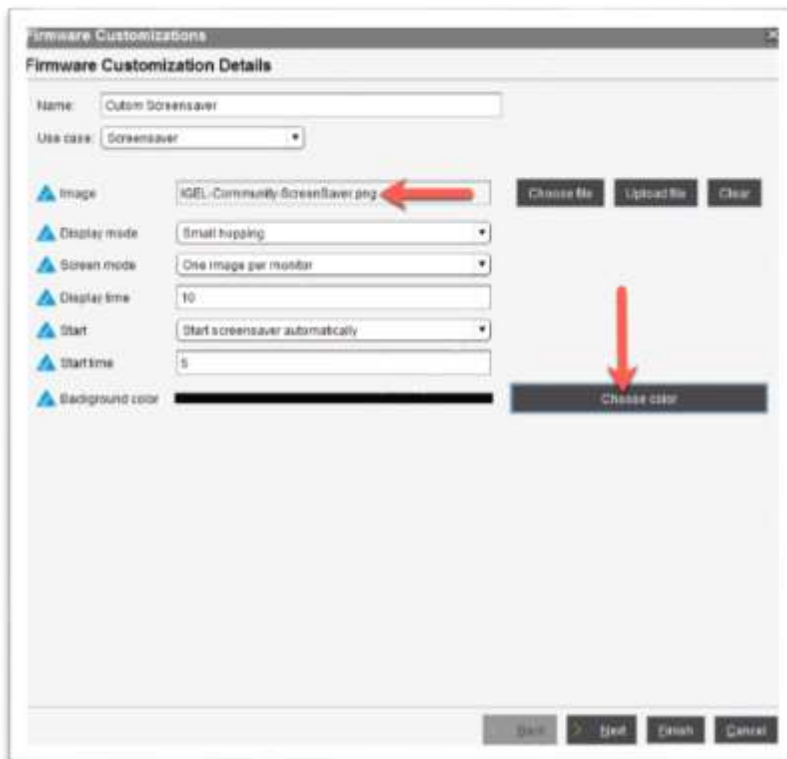
5. The **Open** window opens prompting you to select the file you wish to upload. Find the file, highlight it and click the **Open** button to continue.



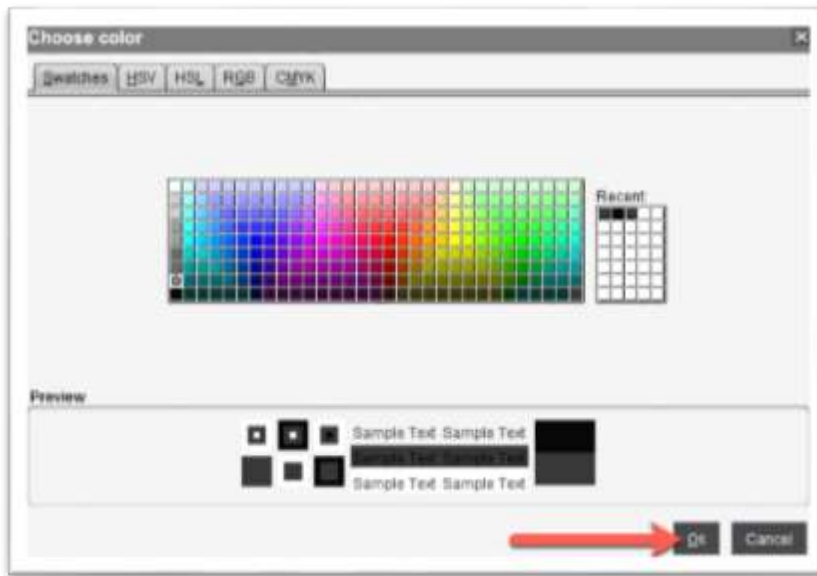
6. You are brought back to the **New file** window. Verify the correct file was uploaded and click the **OK** button to continue.



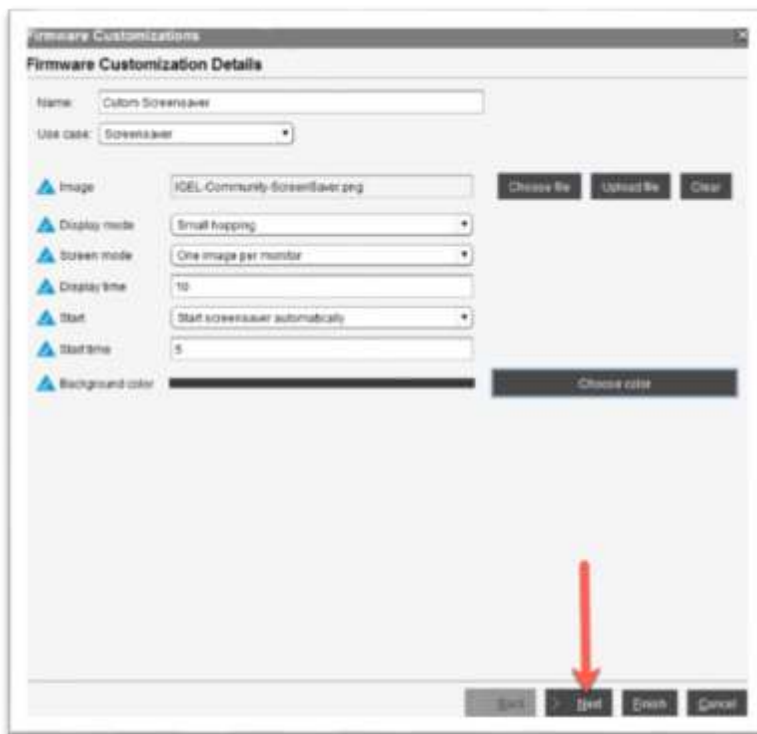
7. The new file will appear in the image text box. You are ready to change the color of the screensavers background. Click the **Choose color** button.



8. The **Choose color** window opens which gives you many different options on how to change the background color. Select the desired color and click the **OK** button to continue.

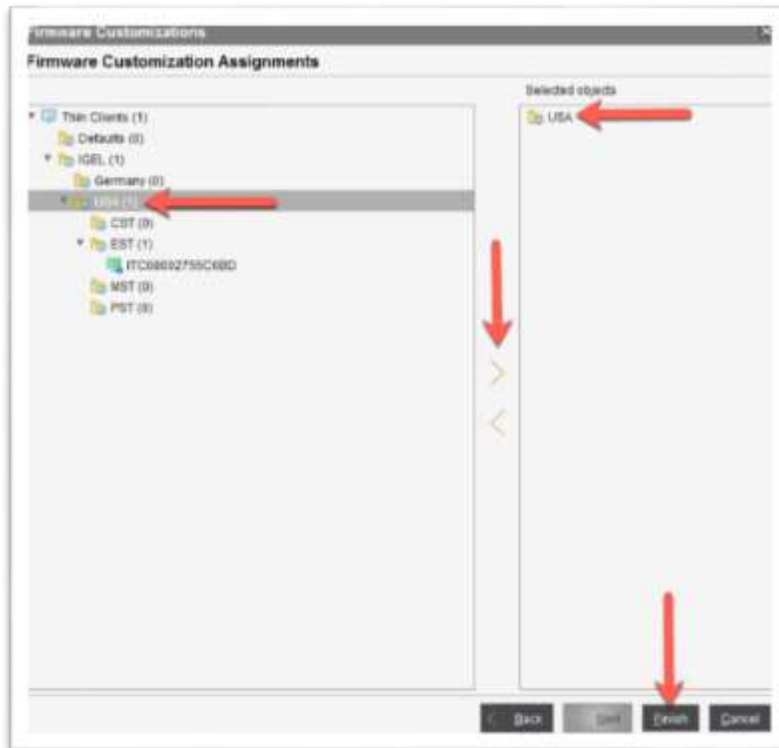


9. You are brought back to the **Firmware Customization Details** window. You will notice the new image in the **Image** text box and the color you chose is shown in the **Background color** box. If all looks good, click the **Next** button to continue.



10. The **Firmware Customization Assignments** window opens prompting you to assign the firmware customization to the desired folder(s) and device(s).

Click to select device(s) or folder(s) you wish to assign the firmware customization to and click the > arrow to move them to the **Selected objects** pane. Once finished, click the **Finish** button to assign the new firmware customization.



11. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



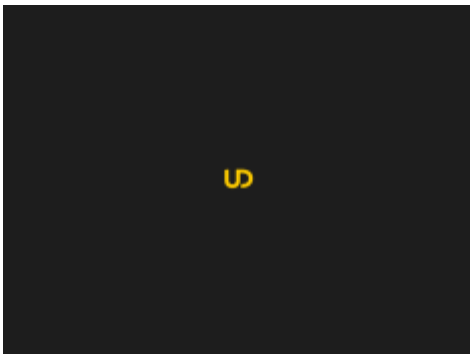
You are done, the next time the assigned IGEL OS devices go to screensaver mode, your users will see your fancy new image. The devil is in the details! This is just one of those that truly make the IGEL OS yours!

2. 6. How to Customize the Bootsplash Image

You have successfully customized the look and feel and the screensaver's image. It's time to customize the image that is displayed at boot time. This too is done using a firmware customization.

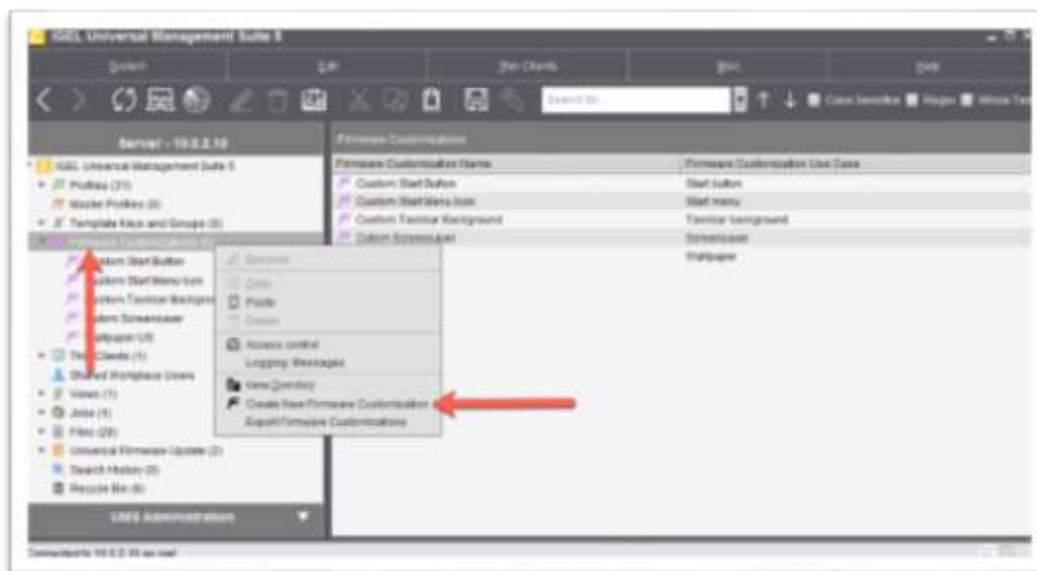
The file types BMP, JPG, GIF, TIF, PNG, and SVG are supported for a boot splash image. The aspect ratio will remain unchanged. You can position the image vertically and horizontally.

The following are before and after images. Notice the new beautiful IGEL Community logo.

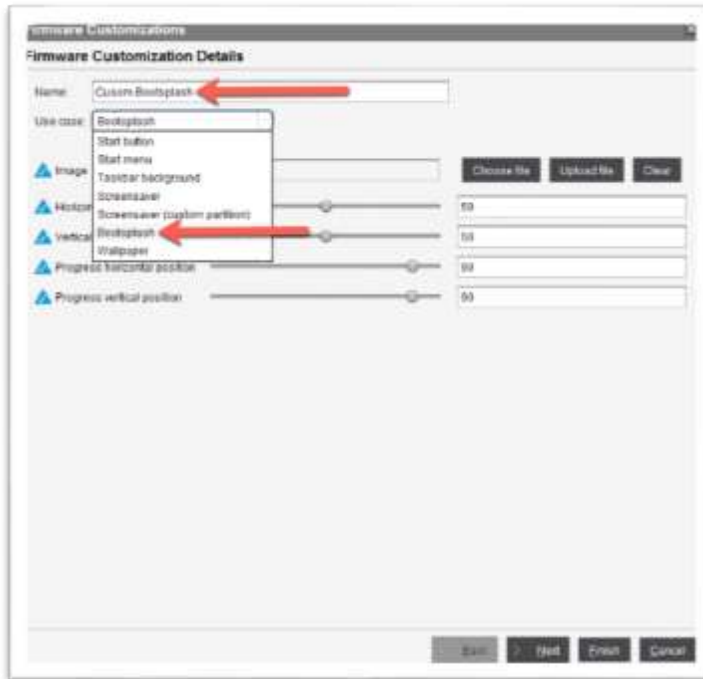


The following defines how to add a custom boot splash image:

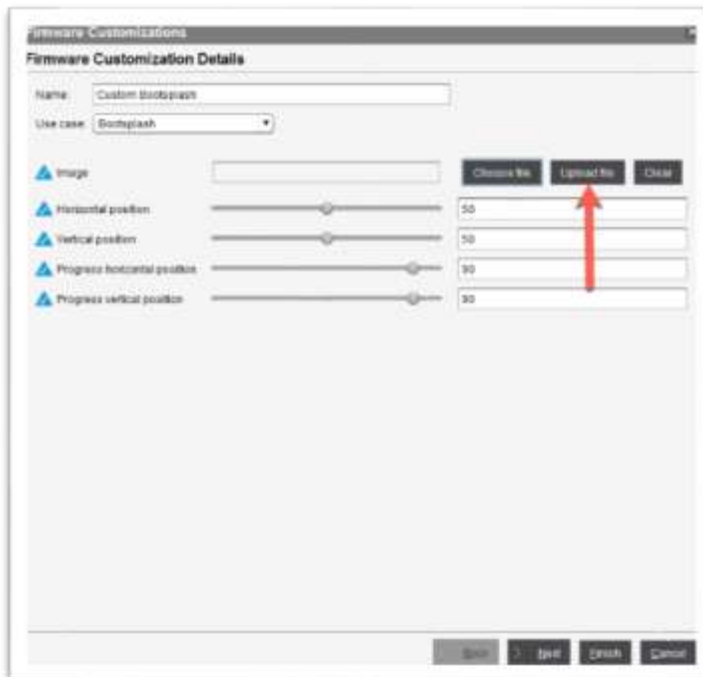
1. From the UMS, right-click the **Firmware Customizations** link in the left menu and click to select the **Create New Firmware Customization** link.



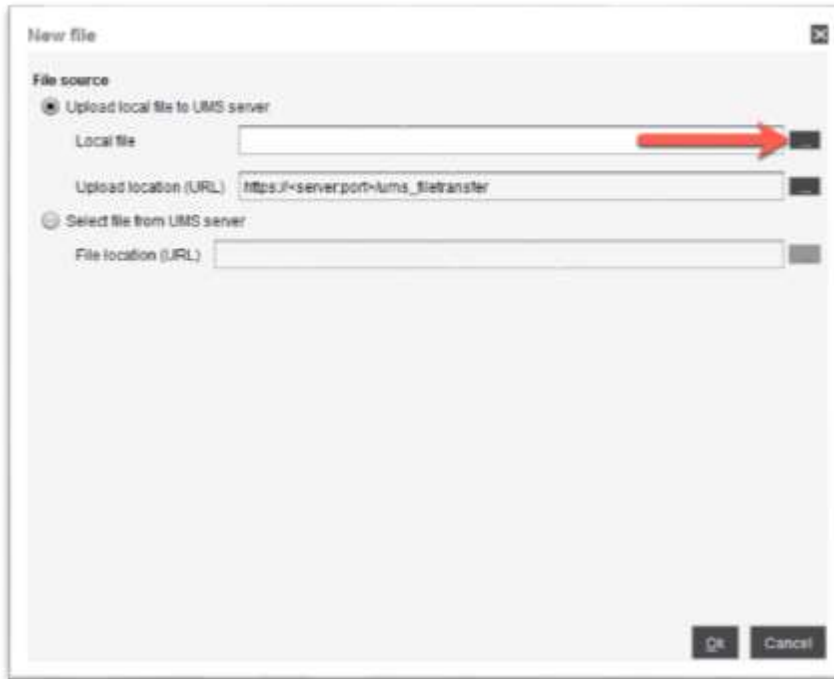
- The **Firmware Customization Details** wizard opens. Enter a detailed name in the **Name** text box and then click to open the **Use case** combo box. Click to select the **Bootsplash** link.



- You need to select the image you wish to use for the bootsplash screen. You have two choices, to choose a file you have already uploaded or upload a new file now. Click the **Update file** button to continue.



- The New File window opens. Click the ... button, located just to the right of the **Local File** text box to continue.



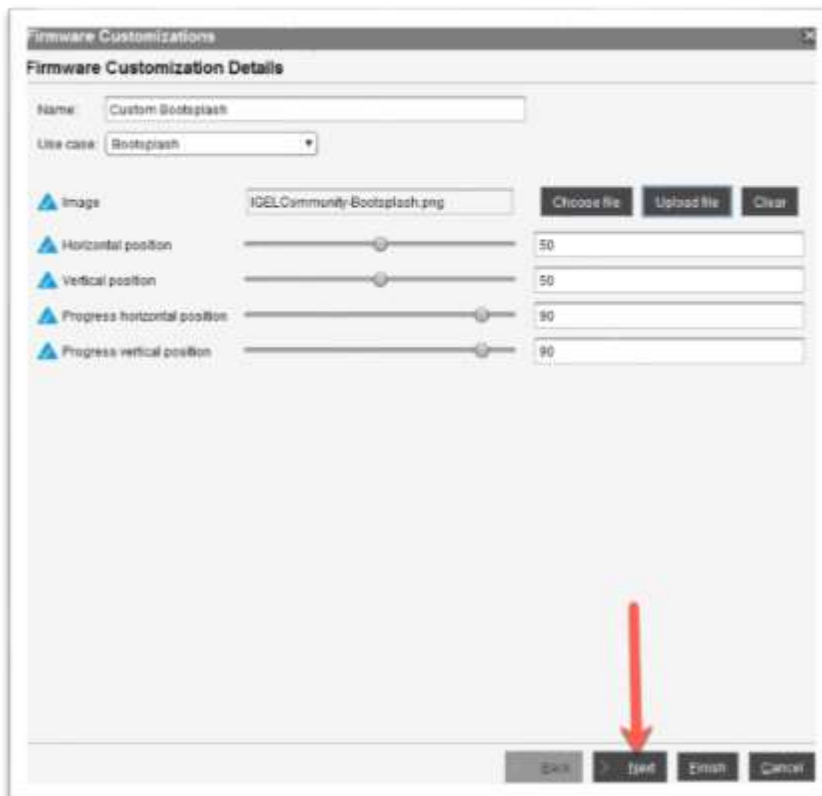
- The **Open** window opens prompting you to select the file you wish to upload. Find the file, highlight it and click the **Open** button to continue.



6. You are brought back to the **New file** window. Verify the correct file was uploaded and click the **OK** button to continue.

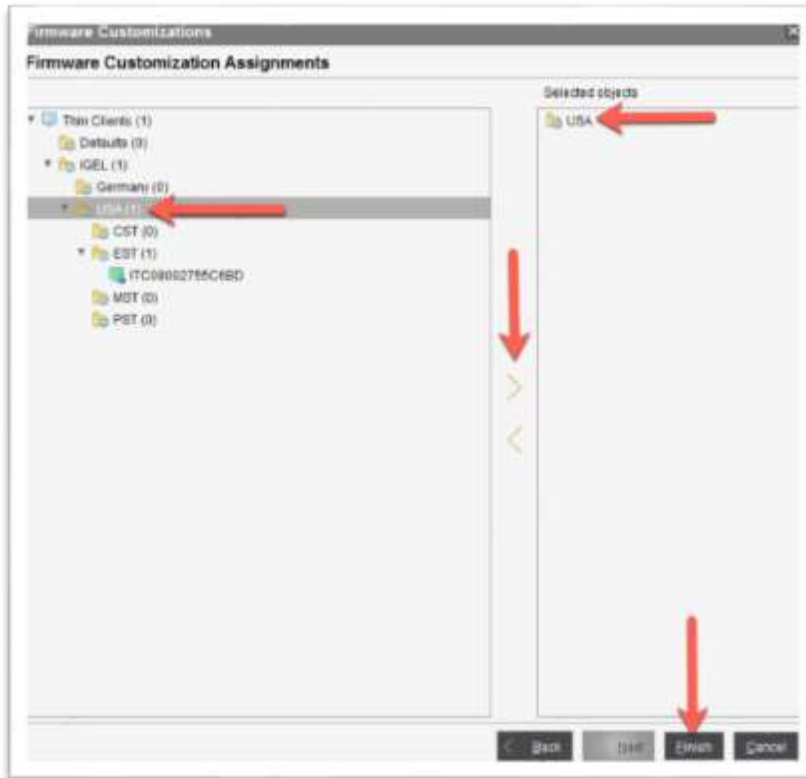


7. The new file will appear in the image text box. Click the **Next** button to continue.



8. The **Firmware Customization Assignments** window opens prompting you to assign the firmware customization to the desired devices.

Click to select device(s) or folder(s) you wish to assign the firmware customization to and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign your new firmware customization



9. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



2. 7. How to Customize Session Icons

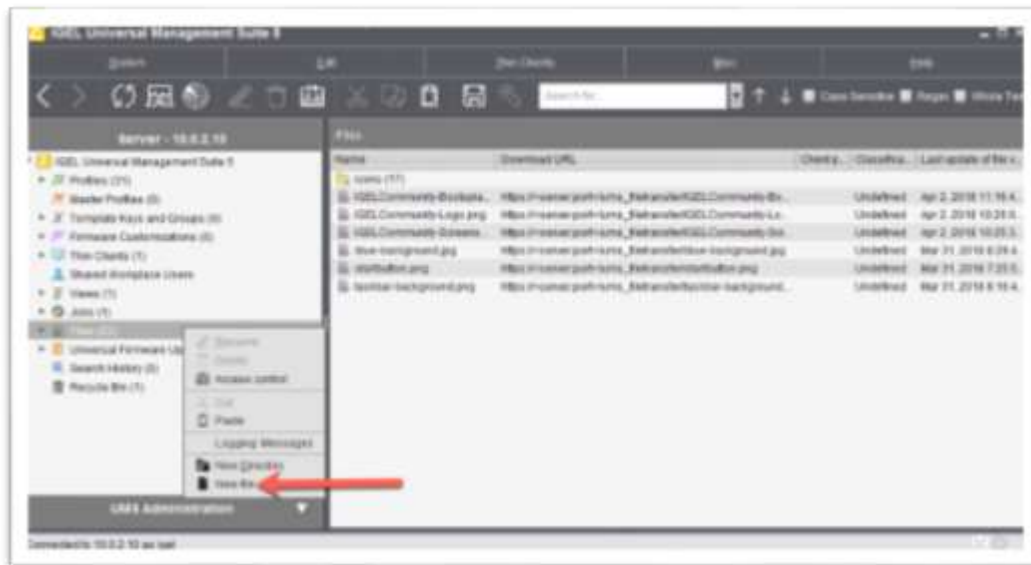
The IGEL OS ships with default icons for the different supported sessions and one for web applications. But like everything else, this too can be customized to your liking. To configure the perfect icon, you are required to upload the icon to the UMS Files repository and then customize the icon that is defined in the registry of the profile deploying each session/web app.

The following are before and after images of just a couple of the icons:

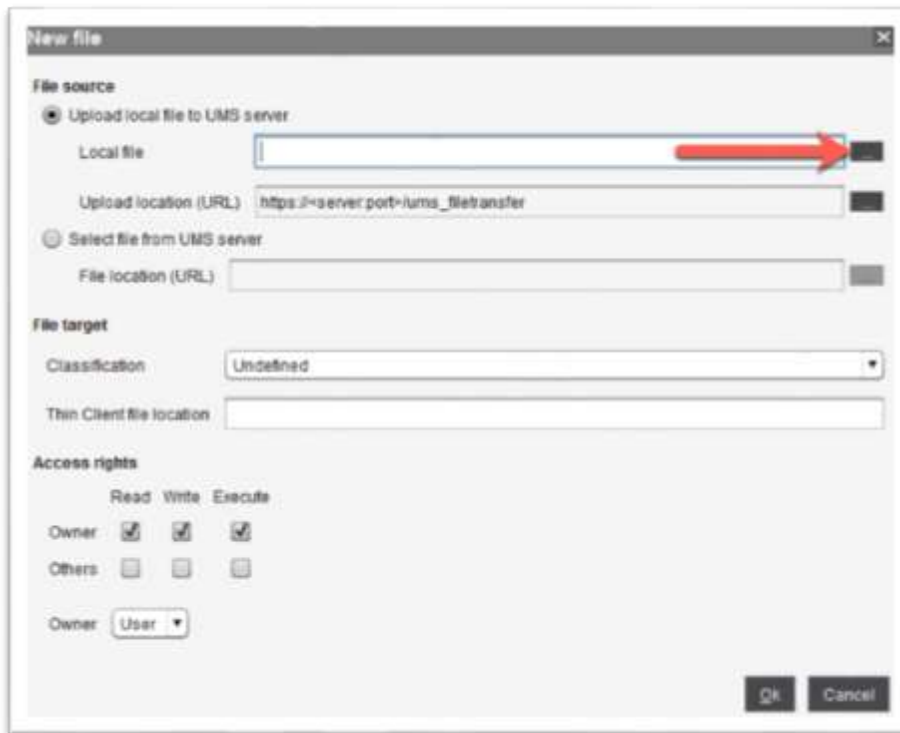


The following defines how to configure the perfect icon for your sessions:

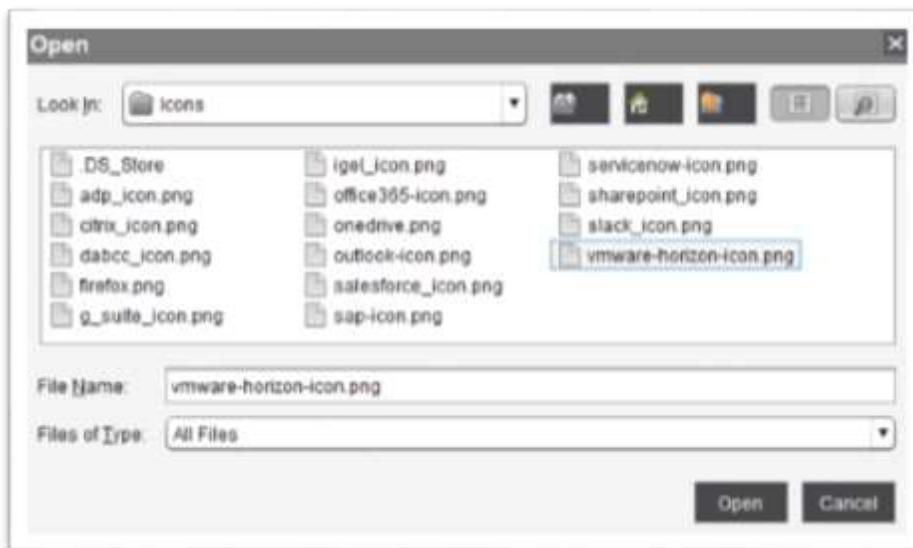
1. The first step is to upload the image you wish to assign to the session/web app. To do this, you will upload the image file to the UMS Files repository. From the UMS, right-click on the **Files** link in the left menu and click the **New file** link.



- The **New file** window opens. For this example, you are required to have the icon image located on the machine running the UMS Console. Click the ... icon located to the right of the **Local file** text box.

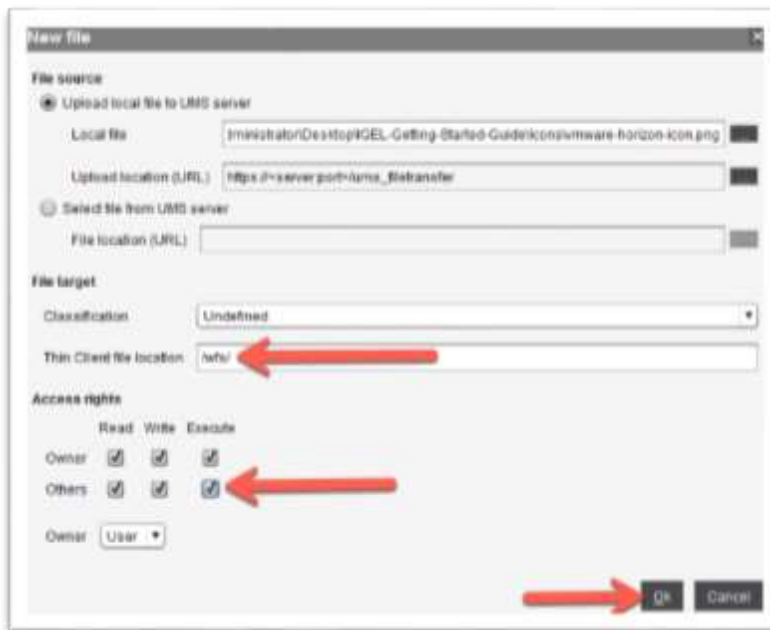


- The **Open** window open. Browse to the location you stored the icon you wish to use, click to select it and then click the **Open** button to continue.

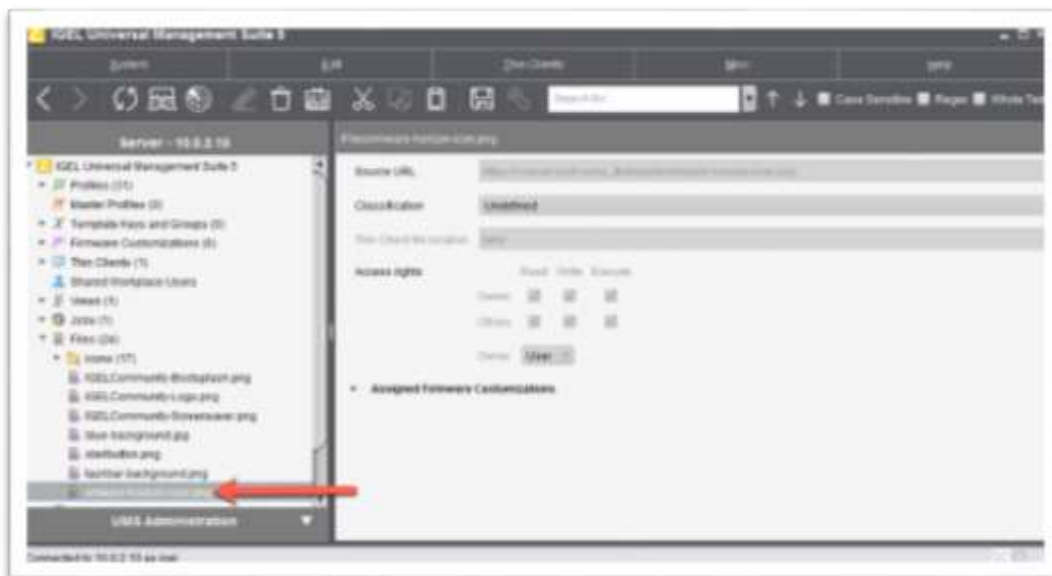


- You are brought back to the **New file** window, and you will notice the icon image is listed in the **local file** text box. The next step is to assign the location on the UMS server where the file will be uploaded. Enter **/wfs/** in the **Thin Client file location** text box. Next check the **Read**, **Write** and **Execute** checkboxes to the right of **Others**.

Click **OK** when finished to upload the image.



- You are brought back to the UMS, and you will notice your new image has been uploaded and added to UMS Files repository, as shown below.

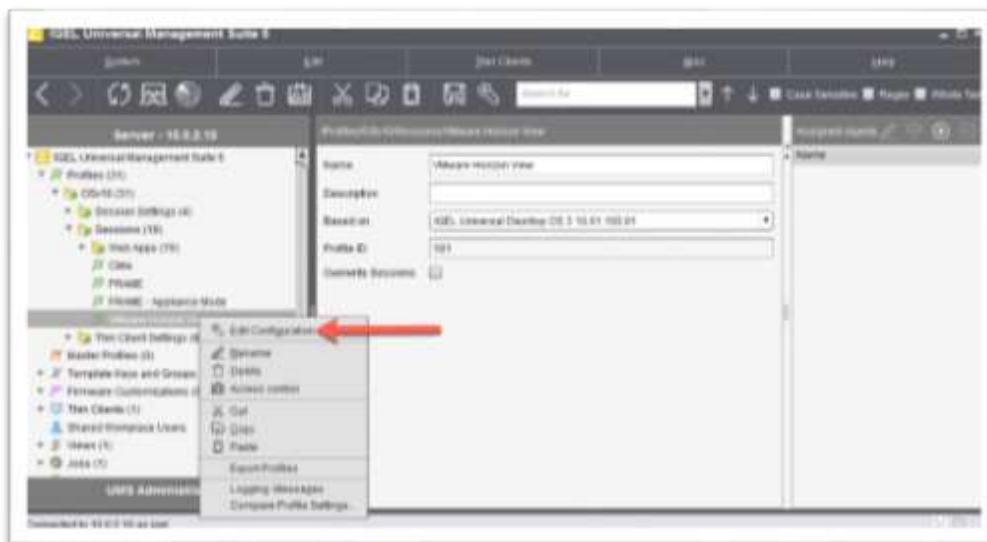


6. The next item you will need to accomplish is to assign that newly uploaded image to the folder(s) and/or device(s) you wish it to be used on. To do this, you will need to drag-and-drop the image to the desired folder(s) or device(s). It is that simple. Once you have done this the **Update time** window will open prompting you to define when you would like the image files to be copied to the desired devices. Select the desired setting and click the **OK** button.

The icon is required to be assigned to the device before you change the profiles setting below or you will receive a not so attractive image, the default image.



7. Now it is time to edit the desired session's profile to utilize the newly uploaded icon. Right-click on the desired profile and click the **Edit Configuration** link.

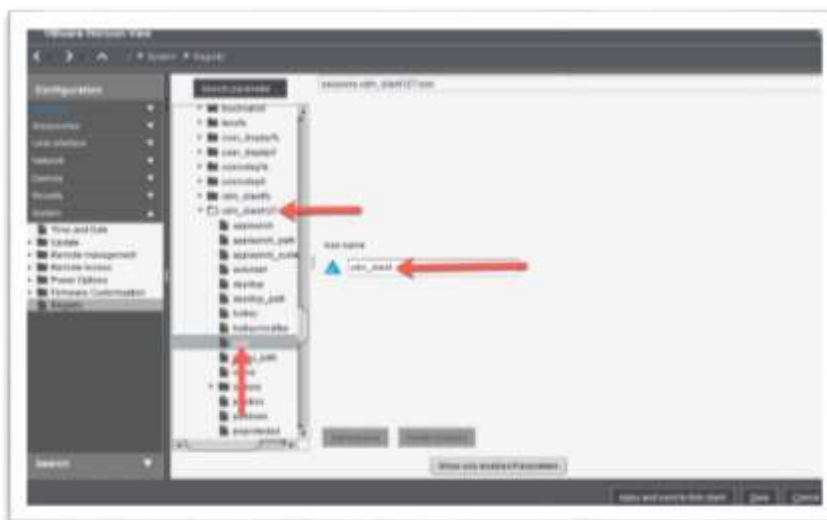


8. The profile configuration settings window opens, click the **System** profile node and click the **Registry** profile in the left menu. Click to select the **sessions** node in the right column.

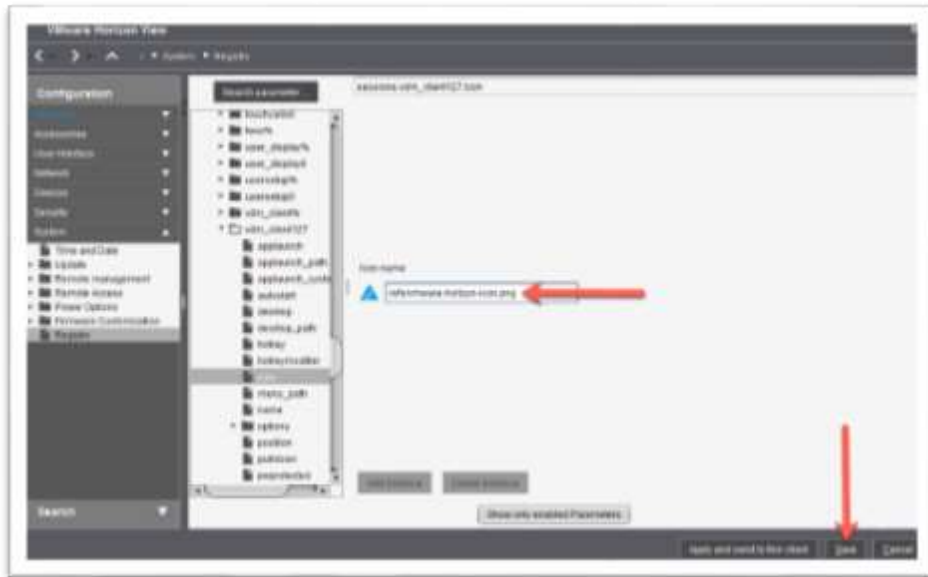


9. Depending on the session you wish to configure a custom icon for will depict which node you will click next. The rule of thumb is to use some common sense for the root of the name. For example, below you are changing the VMware Horizon client's icon, in the list, you will find a node called **vdm_client**. This makes sense. But it does get a bit tricky as two items start with **vdm_client**, a **vdm_client%**, and **vdm_client127**. It is the node with the numbers behind it that you will usually want. But trial and error will tell you if you are wrong or right.

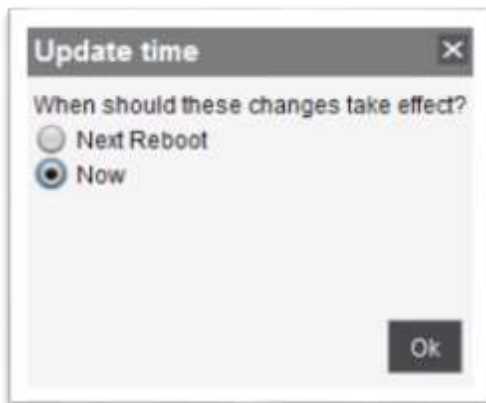
Click to select the desired node and then click to select the **Icon** profile node. You found it and will see the default icon name.



10. Enter the full path and name of the icon uploaded in step 2-4. For example, **/wfs/vmware-horizon-icon.png**. Once finished, click the **Save** button to continue.



11. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



12. Look to a managed IGEL OS, and you will see the session icon has been changed.
Now does that not just look wonderful?



13. However, above you learned how to use some common sense to find the registry node for a session, for example, VMware or Citrix client, but what if you would like to deploy a web application or change the icon of the Firefox browser. This is a bit different, so we will explain!

First, you need to deploy a Firefox session to the IGEL OS and create and copy an icon to use for your Firefox session to the UMS files repository as detailed in steps 1-5 above. In the example below, you will use the **firefox.png** from the accompanying **IGEL-Getting-Started-Guide.zip** file.



14. Open the Firefox session's profile and browse to **System > Registry > sessions** > and then browse through the list until you find the browser entries. Like with the session icon node above, you will want to look for the entry with the numbers behind it. In the example below, you will see this as **browser113**. Of course, these numbers are not the same for every session. Click to expand the **browser113** and click the **icon** node.



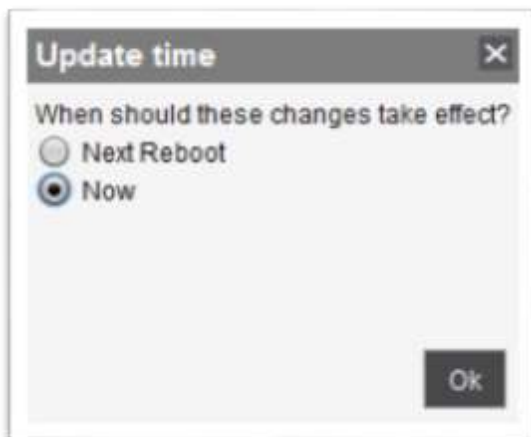
15. You see the default Firefox icon is **firefox**.



- Click to enable the triangle checkbox and enter the name of the icon you uploaded, for this example use `/wfs/firefox.png` and click the **Save** button to continue.



- You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



18. Look at one of your managed devices, and you will notice the Firefox icon has come to life with a new fancy icon! Now that is one beautiful desktop and one your users will be familiar with a very much enjoy using!



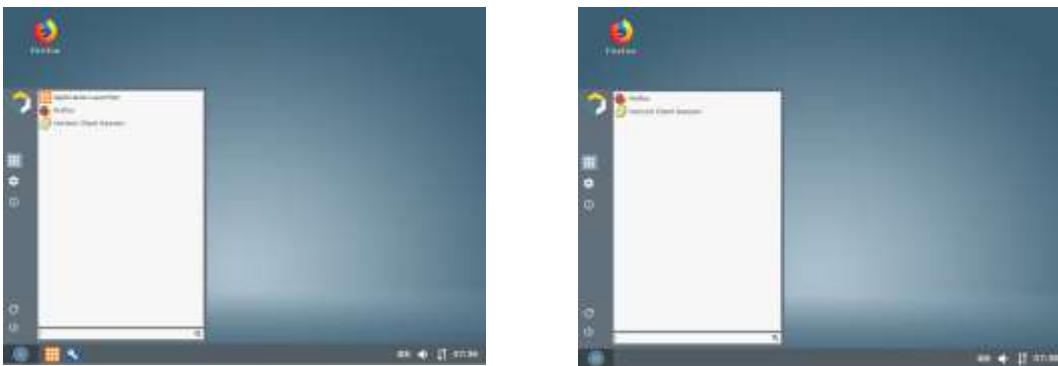
I'm happy to say; you have completed the steps required to make the IGEL OS truly your own! This is a great day for you, your users and the design world in general!

2. 8. How to Lockdown the IGEL OS

Now that you have made your IGEL OS beautiful you will want to lock it down and remove some of the unnecessary user-interface components.

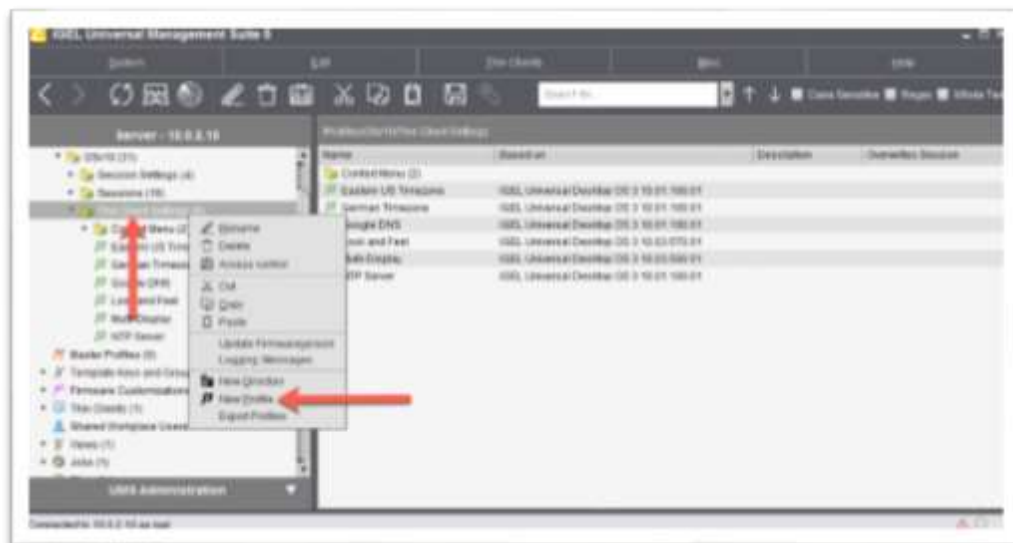
The steps in this section are very simple and not, in anyway, meant to be an inclusive guide to securing the IGEL OS by locking it down. It is a starting point to show you what can be done. To learn more about how to secure and lockdown the IGEL OS, please refer to the [How to Secure Endpoints with IGEL OS](#) white paper.

The following are before and after images showing a basic UI lockdown:

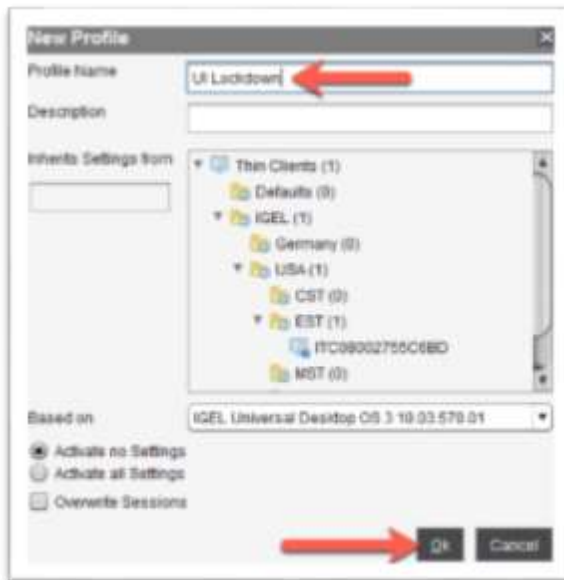


The following defines how to perform a basic UI lockdown of the IGEL OS:

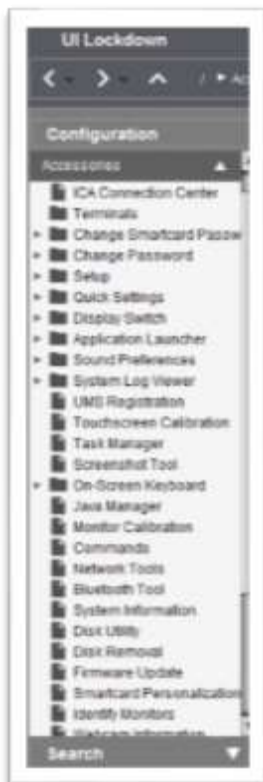
1. From the UMS, right-click the location you wish to store the new profile and click to select the **New Profile** link.



2. Enter a detailed name in the **New Profile** text box and click the **OK** button to continue.



3. The policy window opens, if you click to expand the Accessories node, you will see the different areas the IGEL OS that can be customized. As you did above, look around and play around. There is so much you can do to design and lock down your environment the way that fits your users and requirements best.

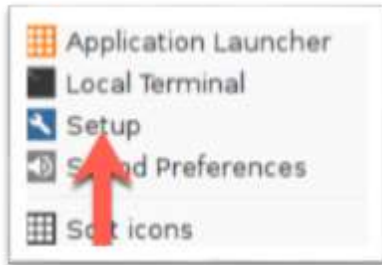


4. The first thing you might want to remove from your user's view is the IGEL Setup icon. The setup icon is shown in multiple places in an IGEL OS environment.

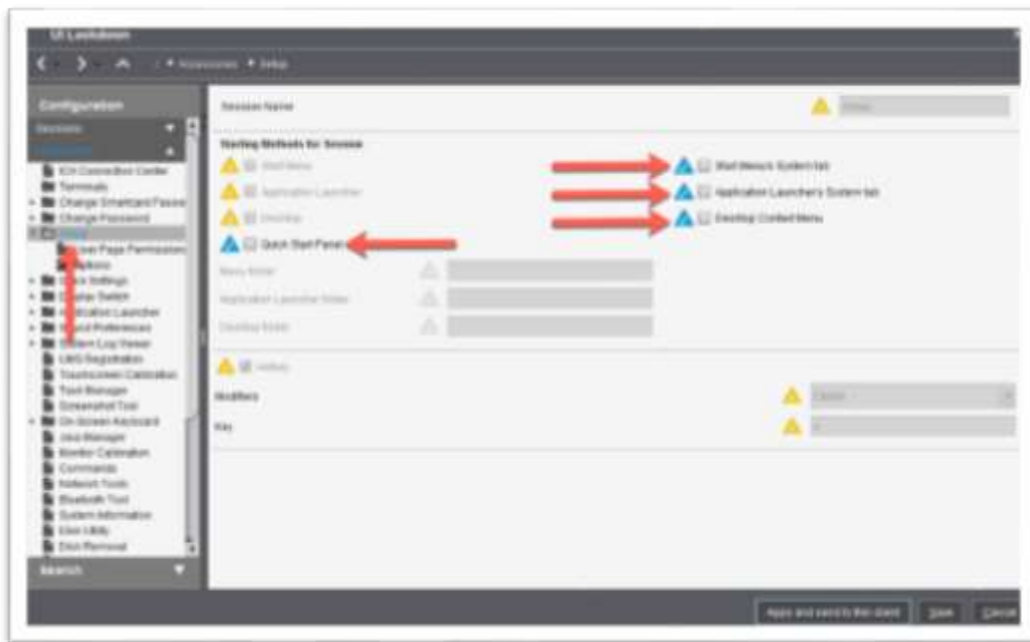
On the taskbar:



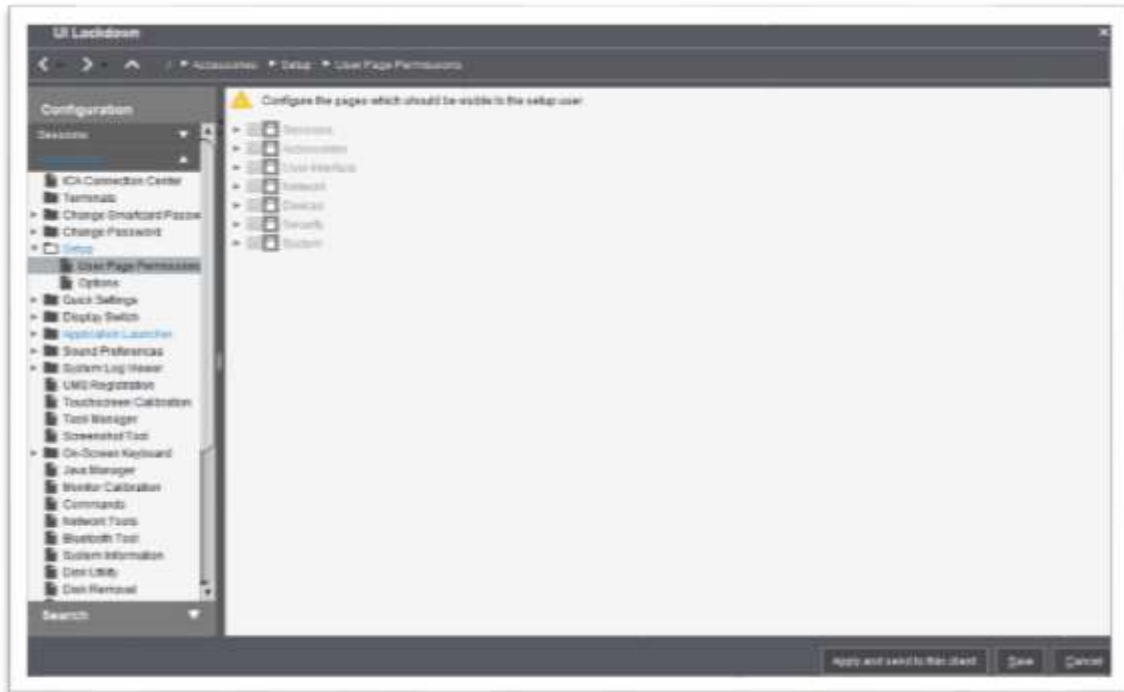
And in the context menu, a user receives when they right-click on their desktop.



If you desire to remove these, all you need to do is browse to the **Accessories** node and then click to open the **Setup** profile. In the **Starting Methods for Session** section, you are presented with the different locations the session icon is deployed. In this case, you will want to uncheck all options to remove the **Setup** applet for the user throughout the UI.



5. Click to expand the **Setup** node and click the **User Page Permissions** profile. You are presented with the different setup pages you can allow or deny visibility to your users. Since above you removed the setup icon across the all your UI you don't need to worry about these settings but do note they are there and that you don't have to remove everything but only what you desire and require. Again, this is the genius of the IGEL solution; almost everything is configurable.

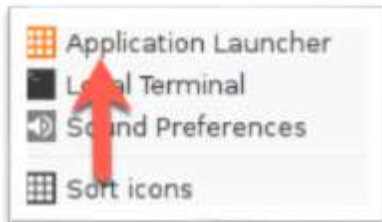


6. The next item on the chopping block is the **Application Launcher**. Of course, this is up to you. By default, your users will see the same session icons on the desktop and when clicking to open the Start button as they will within the Application Launcher. This might be overkill and hence removing the Application Launching might have the benefit of cleaning up the look and feel.

By default, the Application Launcher is located on the taskbar, as shown below:

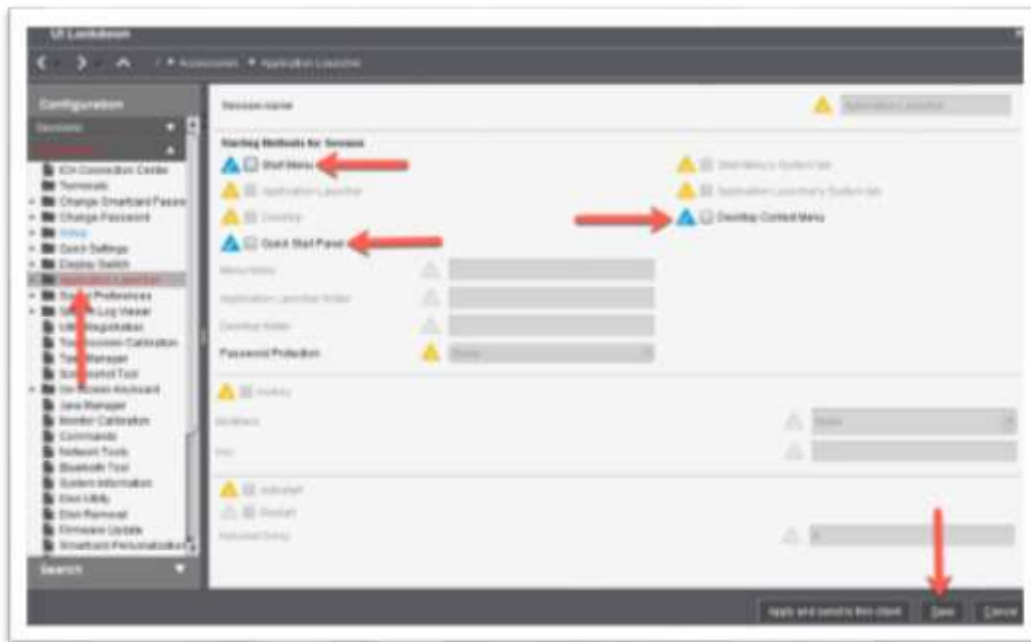


And in the context menu, a user receives when they right-click on their desktop.

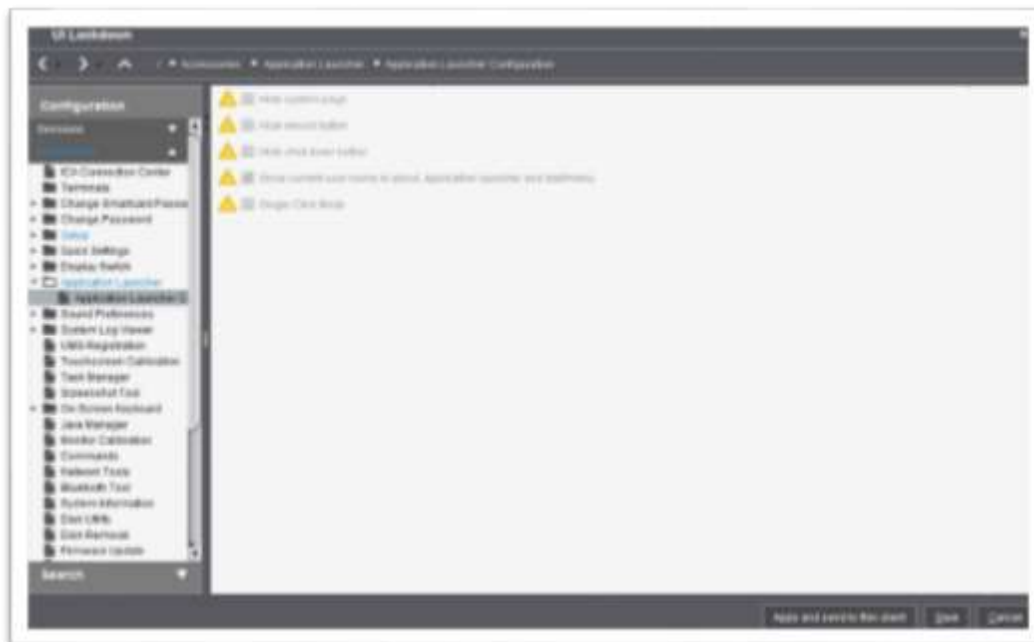


If you desire to remove the Application Launcher icon, all you need to do is browse to the **Accessories** node and then click to open the **Application Launcher** profile. In the **Starting Methods for Session** section, you will uncheck the locations you wish to hide the icon on, as you did for the setup applet.

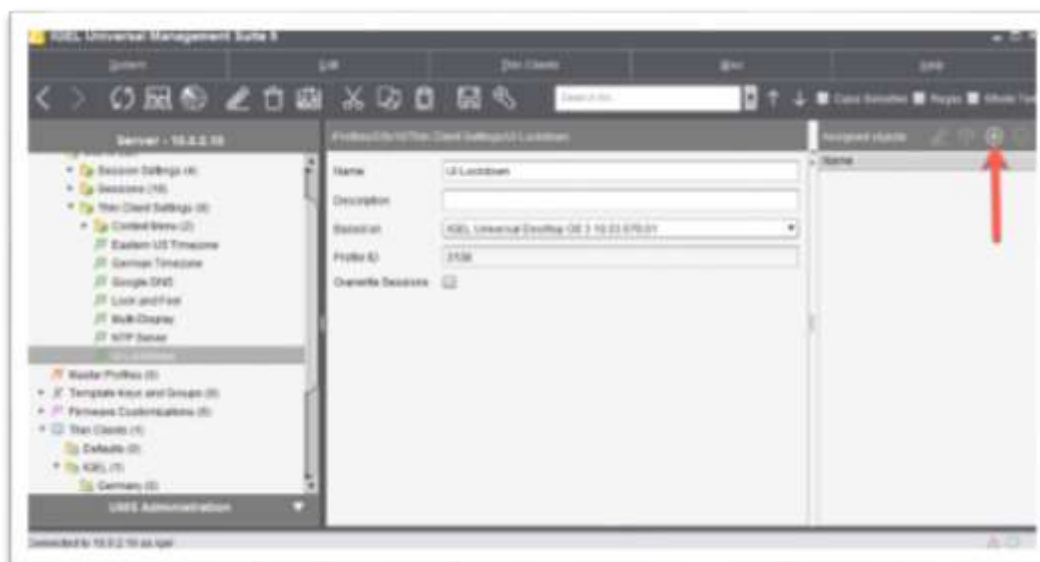
From there, you are done and can click the **Save** button. Though, feel free to look around as there are so many more configurations to be played with.



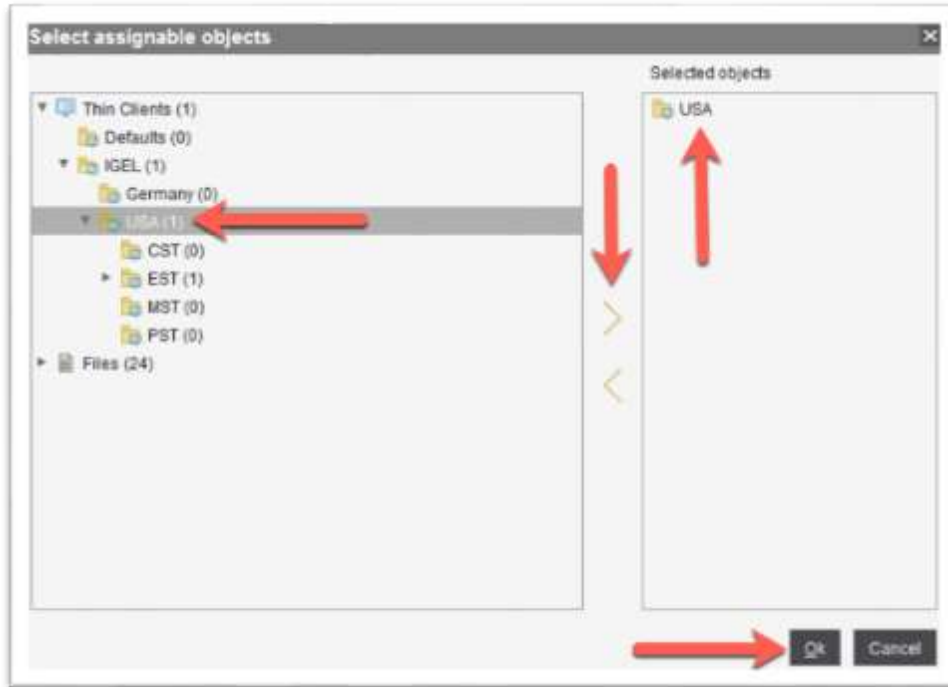
7. For example, if you click to expand the **Application Launcher** node, you will find the **Application Launcher Configuration** profile. Here you can configure items such as hiding the systems page or reboot icon. This is up to you. Have fun as the sky is your limit!



8. Once you saved your profile, you will want to assign it to the desired folder(s) and device(s). As always, you do this by clicking the + icon located at the top right of the profile page in the UMS.



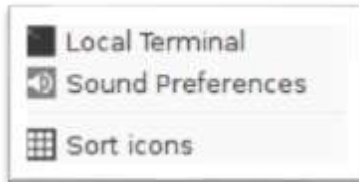
12. The **Select assignable objects** window opens prompting you to assign the profile to the desired devices. Click to select the folder(s) and device(s) you wish to assign the profile to and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign your new profile.



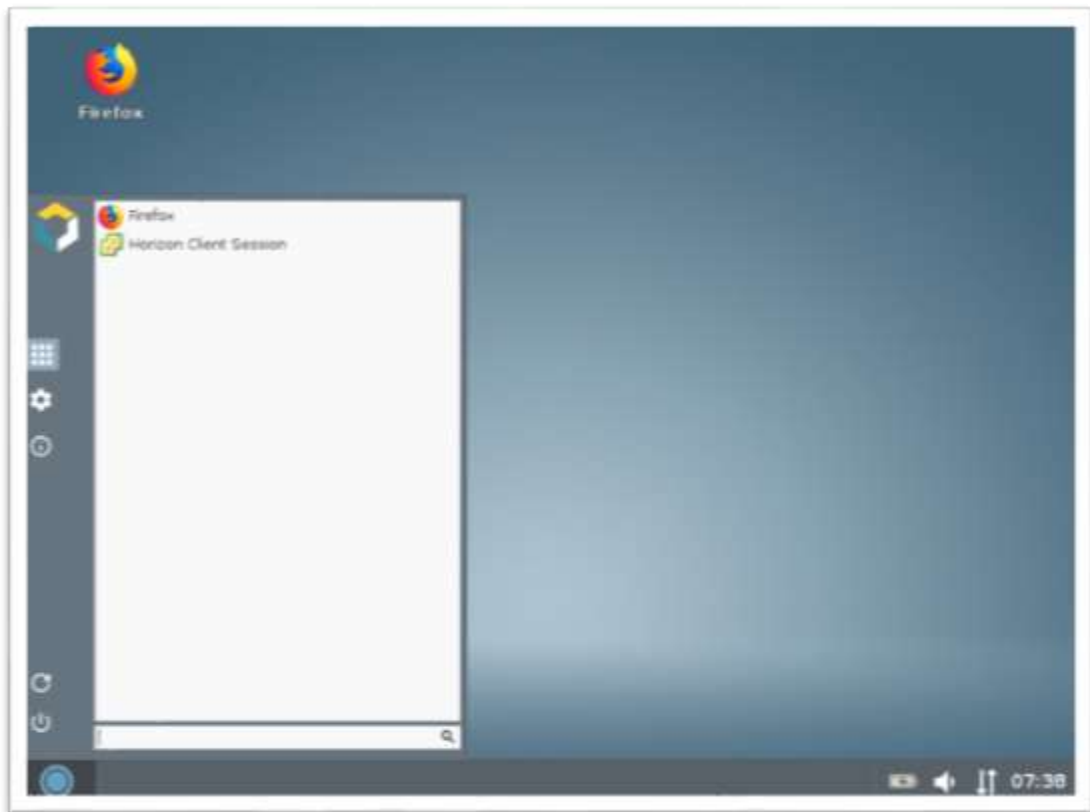
9. You are prompted to select when you would like the changes to take effect. Of course, this is up to you. Select the desired setting and click **OK** to continue.



10. If all goes as planned, the Application Launcher icon is removed from both the desktop's right-click context menu, as shown below.



And from the start menu and the taskbar!



Tell me that does not look great! Just what your users need, not too much and not too little, not too hot and not too cold. The three little pigs would be happy with you and so will your users.

Again, this just a start in locking down and customizing the IGEL OS. As we have said many times before and will say many times again, the genius of the IGEL solution is the ability to do so much with it in such an easy fashion. Have fun, play around, and design the most amazing environment just for you and your users. They will thank you, and Steve Jobs would be proud of you!

3. IGEL OS Firmware Updates

IGEL OS updates are delivered via downloadable firmware available free from the IGEL web site. 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 is connected to the UMS via the IGEL Cloud Gateway (ICG), the traditional UMS **Universal Firmware Update** feature does not work as the IGEL end-points 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 the IGEL OS when connecting to the UMS via an ICG server:

- [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](#)
- [How to Deploy a Firmware Update](#)

3. 1. IGEL OS Firmware Versions Explained

Currently, IGEL ships different versions of the IGEL OS firmware based on the different types of devices you own. This can be somewhat confusing as to why but it comes down to the device drivers included in each image. This allows IGEL to ship the smallest, yet most complete image possible.

Today, there are mainly three types of firmware versions you would be interested in, Windows, LX, and OS. Of course, the Windows version is the Microsoft Windows 10 IoT version whereas the LX and OS version is the IGEL OS Linux operating system. Both the LX and OS firmware contain the same feature sets. The LX 10.03.500 is the same as OS 10.03.500; the only difference is the type of device it is deployed on. LX is used on IGEL hardware-based thin clients, and the OS version is used on the IGEL UDC and UD Pocket.

You will also notice a reference to v5 and v10. The v5 version is a legacy version of the IGEL OS, and it reached end-of-life in fall 2017. IGEL supports all EOL firmware for up to three years from the EOL date. **The current version of IGEL OS Linux operating system (LX+OS) is v10.**

The following table lists the current in-use firmware versions:

Prefix	Usage
LX	IGEL hardware-based thin clients running the Linux version of the IGEL OS. If you are running an IGEL hardware-based thin client and it is not running Windows, it is a good bet this is the firmware you use to upgrade your device(s). Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX/
IZ	Software license locked down version of the LX operating system. It is the same IGEL OS, running on the same hardware, the feature sets are just locked away. There are three different versions of IZ device, Citrix, Microsoft RDS, and VMware Horizon. Download at http://www.myigel.biz/index.php?dir=IGEL_ZERO/
OS	IGEL Universal Desktop Converter (UDC) and IGEL UD Pocket. Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_CONVERTER/
W10	IGEL hardware-based thin clients running Windows 10 Enterprise IOT. Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W10/

The following table lists the legacy firmware versions:

Prefix	Usage
CE	Windows CE based version (not supported any longer) Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/CE/
ES	Windows Embedded Standard 2009 (XP) Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/ES/
LX_Soc	Legacy ARM-based IGEL thin clients (not supported any longer) Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/LX_SoC/
W7	IGEL hardware-based thin clients running Windows 7 Embedded Standard. Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7/
W7+	IGEL hardware-based thin clients running Windows 7 Embedded Standard with larger storage adapter than the 4GB in W7. This is the same version of Windows 7 Embedded as in the W7 firmware expect the size of the image is larger to accommodate the larger storage sizes of some devices. Download at http://www.myigel.biz/index.php?dir=IGEL_UNIVERSAL_DESKTOP_FIRMWARE/W7%2B/

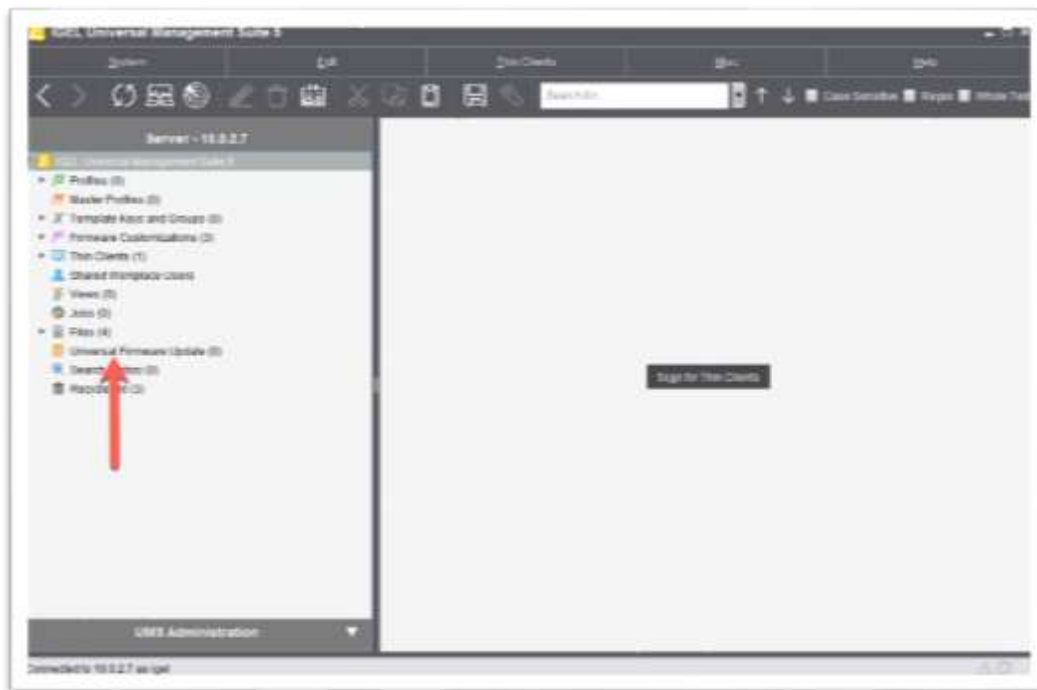
Learn how IGEL versioning works and what the identification numbering means - <https://kb.igel.com/licensesmore/what-is-the-meaning-of-igel-release-names-2271574.html>

3. 2. Update IGEL OS Firmware via the UMS

If the devices you wish to update connects to the IGEL UMS via a routable network, then you can use the UMS's **Universal Firmware Update** feature.

The following defines how to update the IGEL OS firmware using the UMS Universal Firmware Update feature:

1. Right-click the **Universal Firmware Update** node, located on the bottom left menu of the UMS.

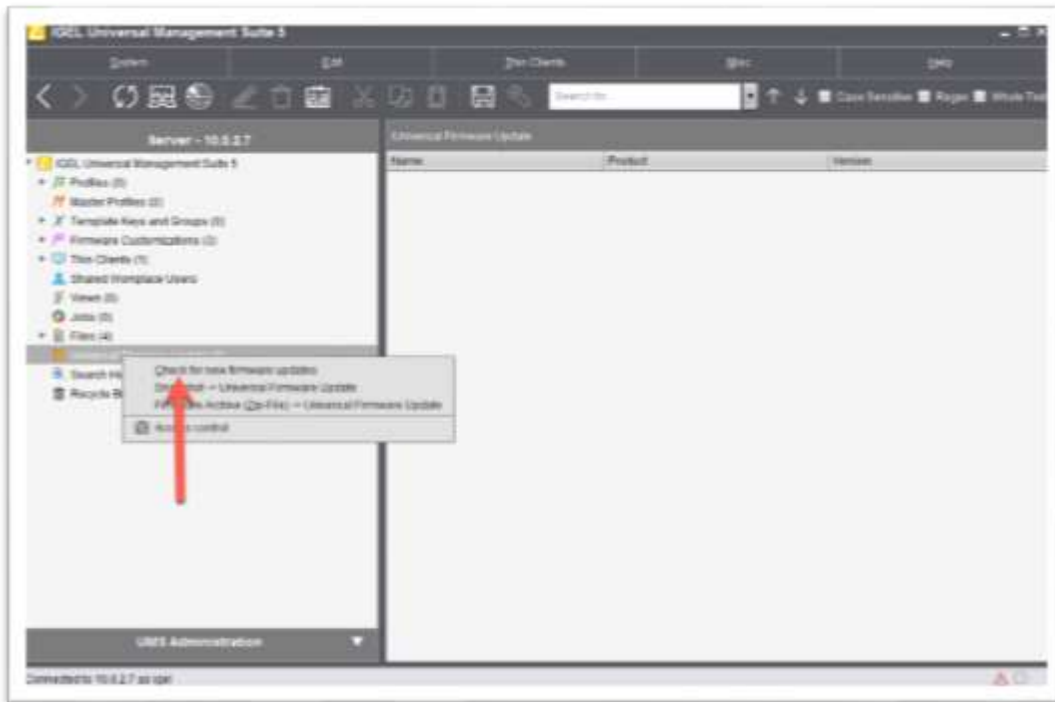


2. The UMS offers two different methods for updating the IGEL OS firmware, automatic and manual.

To automatically update the IGEL OS, the UMS is required to have a working Internet connection. The manual method does not need connectivity as you can download the firmware from IGEL's website on another machine and upload it manually to the UMS.

If you chose to update the UMS firmware repository manually, skip to step 6.

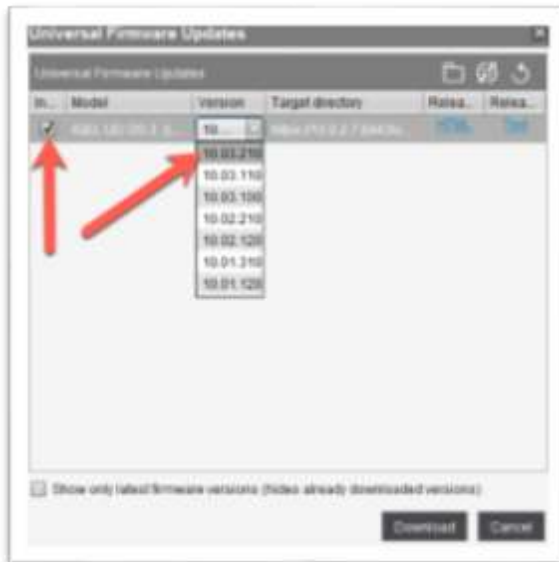
To automatically update the firmware, please click the **Check for new firmware updates** link from the dropdown list.



- The **Universal Firmware Updates** window opens, and the UMS starts a process to search for the IGEL OS firmware version families you have registered in the UMS. For example, if you have the IGEL OS UDC or UP Pockets registered, the UMS downloads the correct firmware for the corresponding IGEL OS firmware family.

Click to check the **Include** check box for the firmware model (family) and click the version dropdown list to select the version(s) you wish to add to the repository.

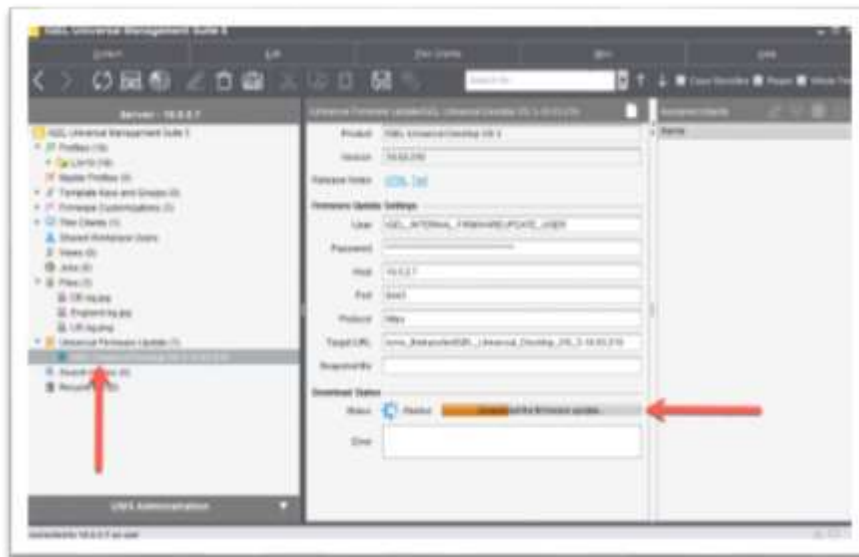
Click the **Download** button to start the download process.



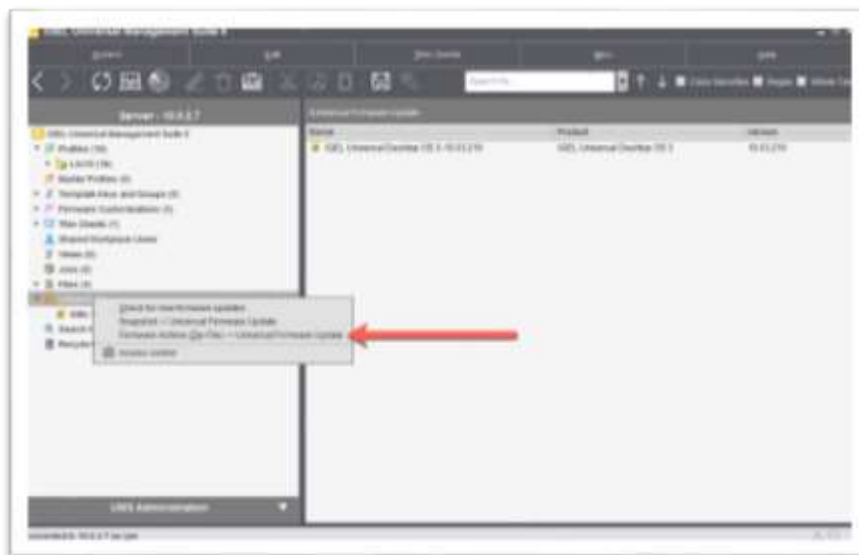
- The update process' status is changed to **Started**, you are off and running. This process could take a bit of time, so please click the **OK** button to continue.



- You are brought back to the UMS. The new firmware is added to the list of possible updates in the left menu as it continues to download. Keep an eye on the **Download Status** section, but don't worry if the status bar does not move, it IS working, trust us.

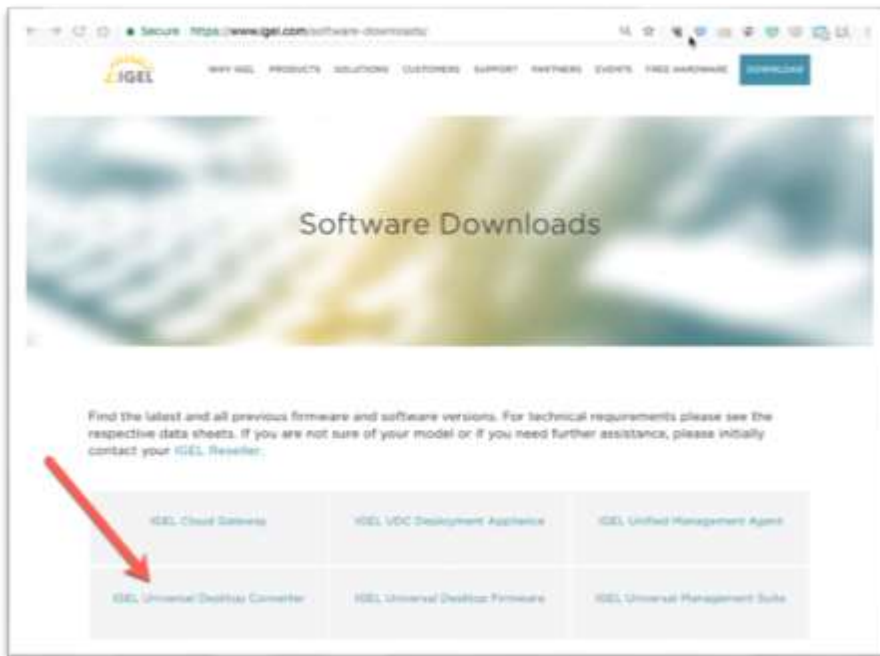


- If you would like to download the IGEL OS firmware manually, right-click on **Firmware Archive (Zip-File) -> Universal Firmware Update**. Though, before you go to the next step, you need to download the firmware from the IGEL web site. Let's do that now, and then you can flip back to the UMS to continue.

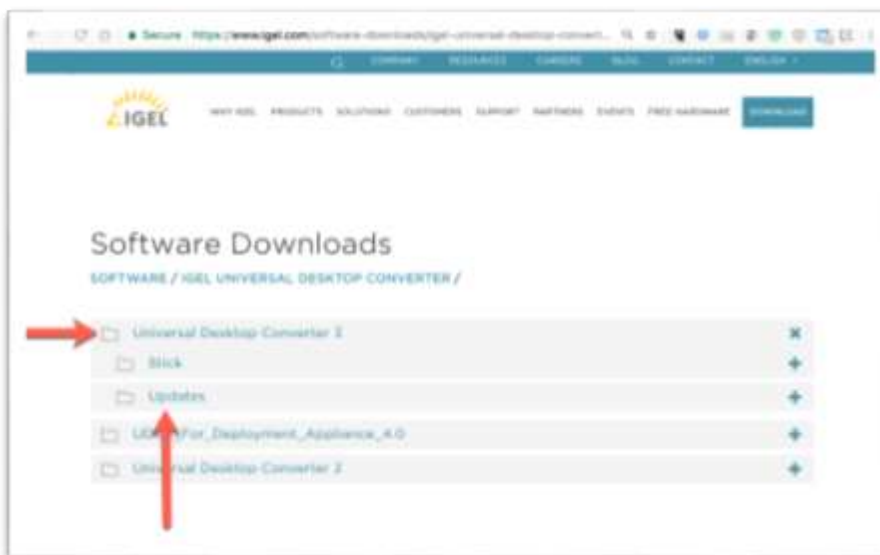


7. Browse to <https://www.igel.com/software-downloads/> to download the desired IGEL OS firmware version. Notice the different software downloads available. Depending on which devices you own will define which firmware you download and then add to the UMS update file repository.

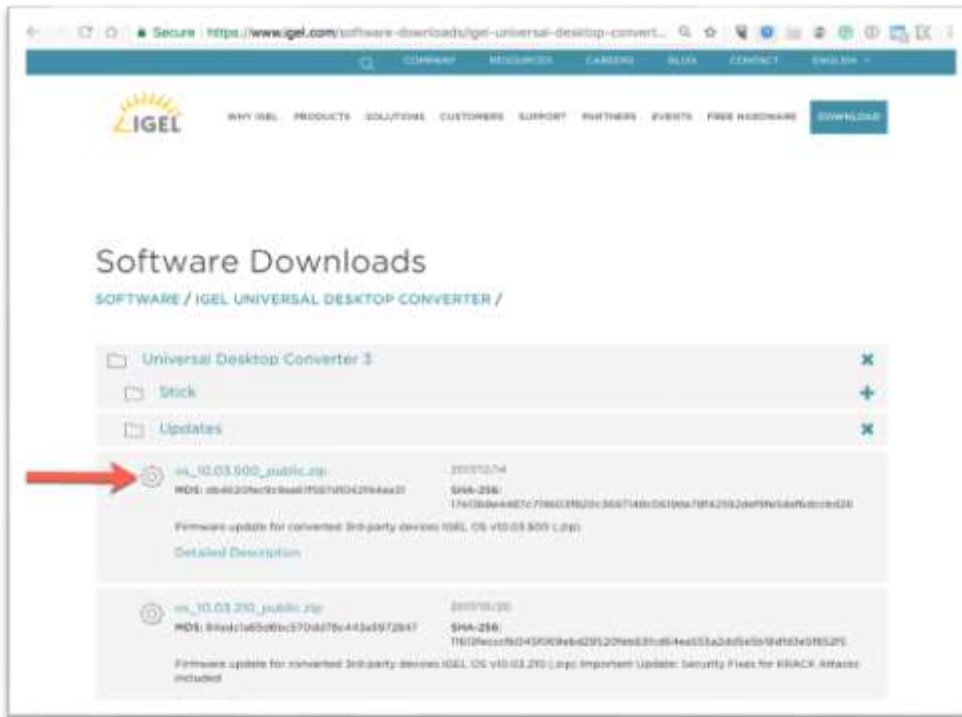
In this case, you want to update the IGEL OS for the UDC. Click the **IGEL Universal Desktop Converter** link to continue.



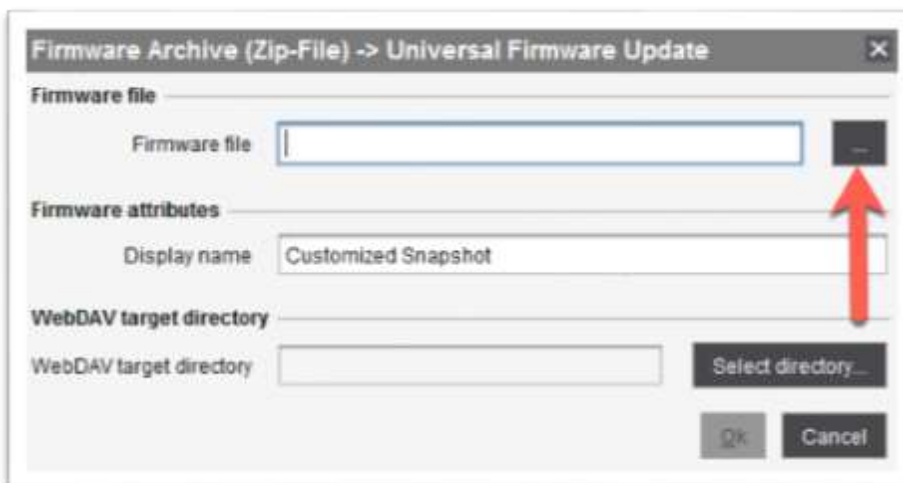
8. Click to expand the **Universal Desktop Converter 3** folder and click the **Updates** folder link.



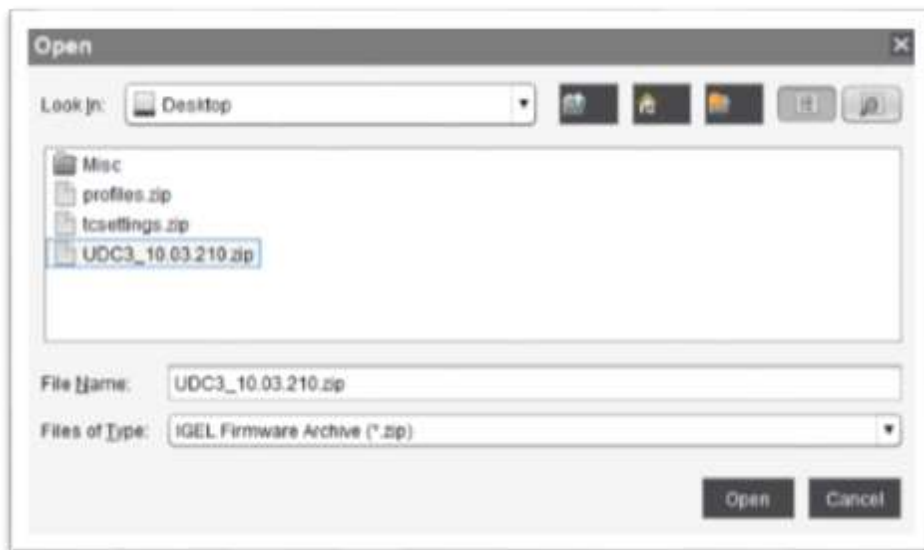
9. Click to download the desired firmware versions and save it to a location where it is accessible. If you are doing this on your local machine, you are required to copy the firmware file to UMS server to be imported into the UMS Firmware Repository.



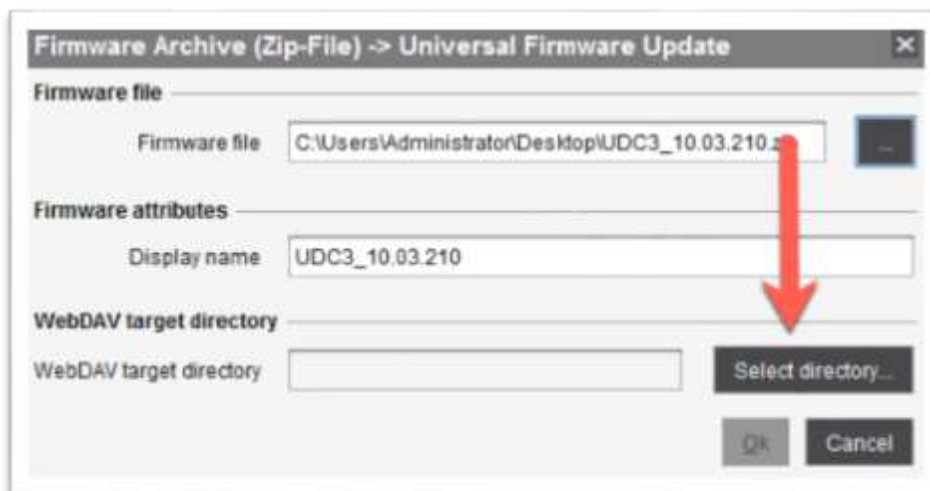
10. Once you have downloaded and copied the desired firmware file to the UMS server, you can flip back to the UMS. The **Firmware Archive (Zip-File) -> Universal Firmware Update** window opens. Click the ... button to start the process of uploading the IGEL OS firmware image you downloaded above.



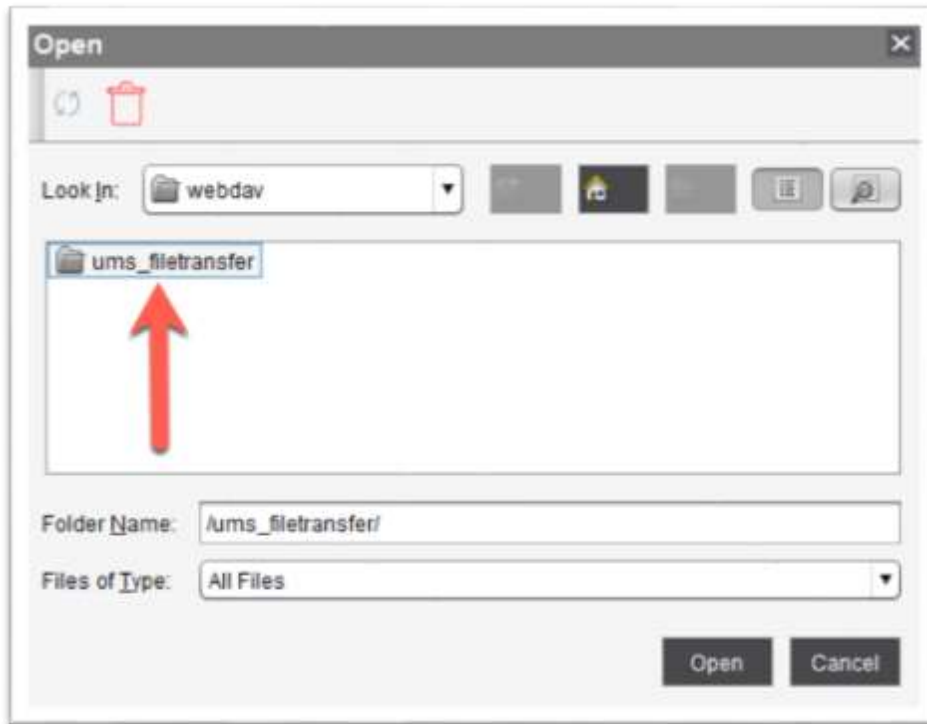
11. You are brought to the **Open** window. Browse to the location of the downloaded firmware, select it and click the **Open** button to continue.



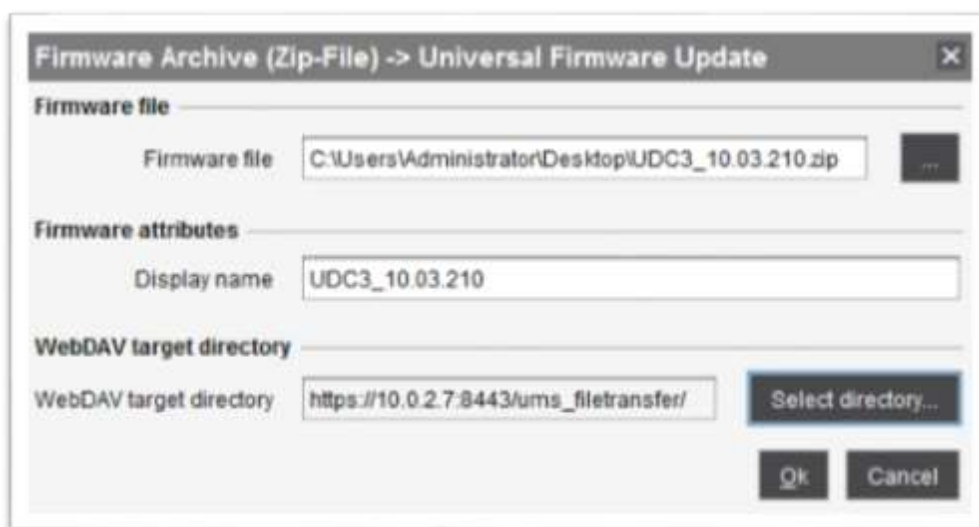
12. You are brought back to the **Firmware Archive (Zip-File) -> Universal Firmware Update** window where you can change the name that is displayed in the UMS for this particular firmware update in the **Display name** text box. It is highly recommended to give it a friendly name so that it can be easily be identified.
- Next, you are required to enter the directory where the firmware upload is to be stored. Click the **Select directory** button to continue.



13. The UMS ships with a built-in web server for numerous uses, one being the deployment of the IGEL OS firmware images. Select the **ums_filetransfer** entry and click the **Open** button to continue.

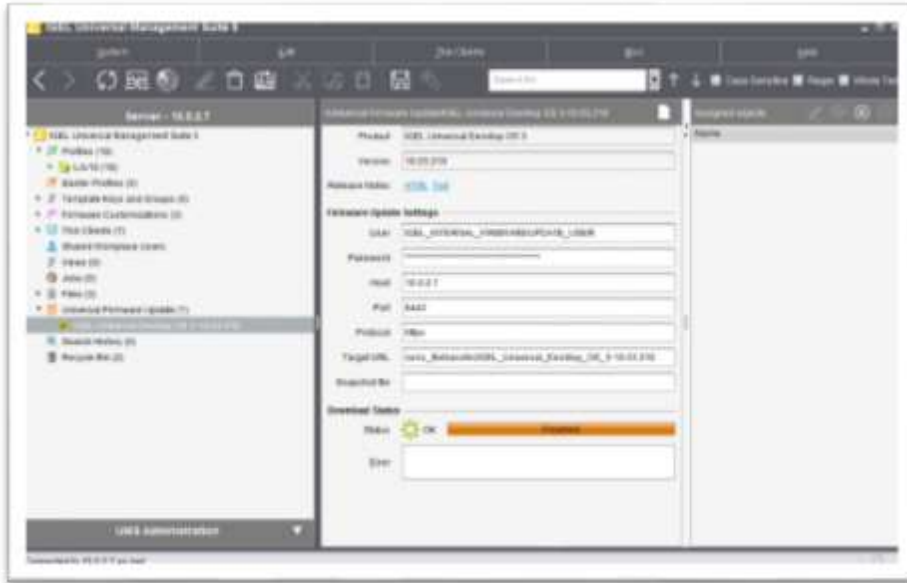


14. You are brought back to the **Firmware Archive (Zip-File) -> Universal Firmware Update** window. Verify all the settings are as desired and click the **OK** button to start the process of uploading the firmware.

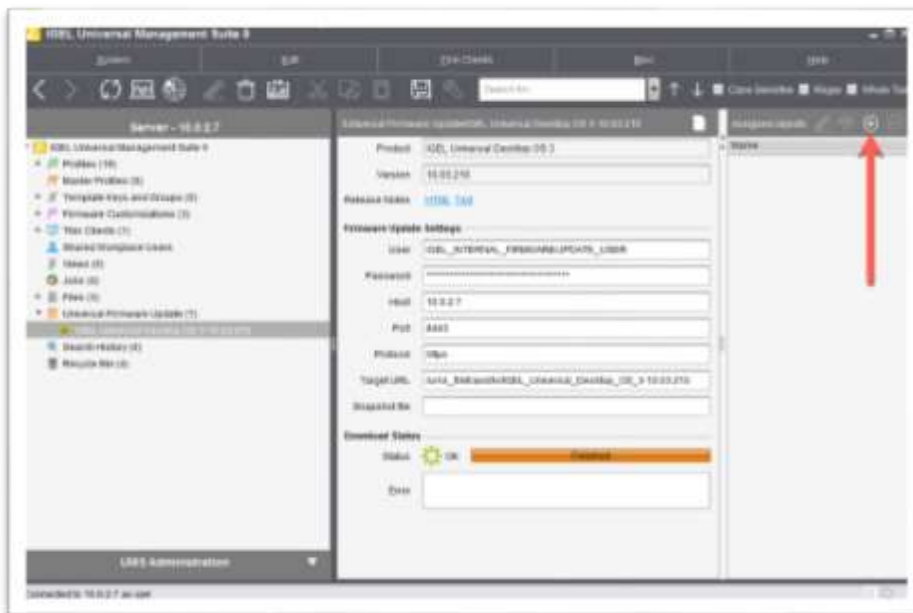


15. The UMS start the process of uploading the selected firmware files. Hit the F5 Key or the **Refresh** button to update the progress bar.

The download status button is not that great as it does not accurately show the progress. Trust us; it will finish, if not you will see **Failed** as the status. A failed download could happen for a few reasons, lack of storage space and failure to communicate with the IGEL web site.



16. The next step is to assign the uploaded IGEL OS firmware to the devices you wish to update. Click the + icon in the **Assigned objects** pane.



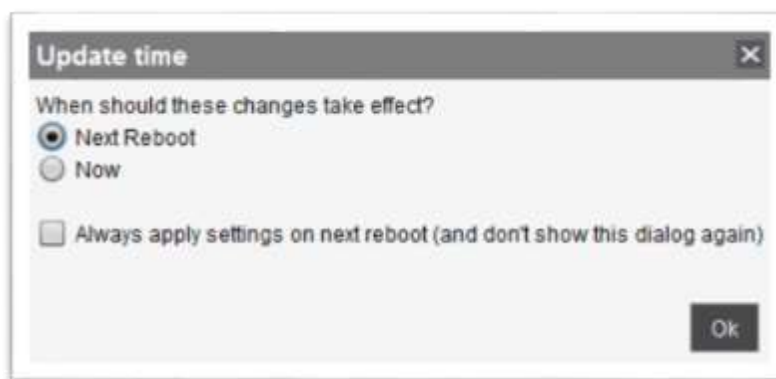
17. The **Select assignable objects** window opens allowing you to select the devices you want to update. You can assign firmware to single devices or folders of devices within the directory structure. Click the desired folders or devices you want to upgrade and click the > button to move them to the **Selected objects** pane.

Once finished, click the **OK** button to continue.

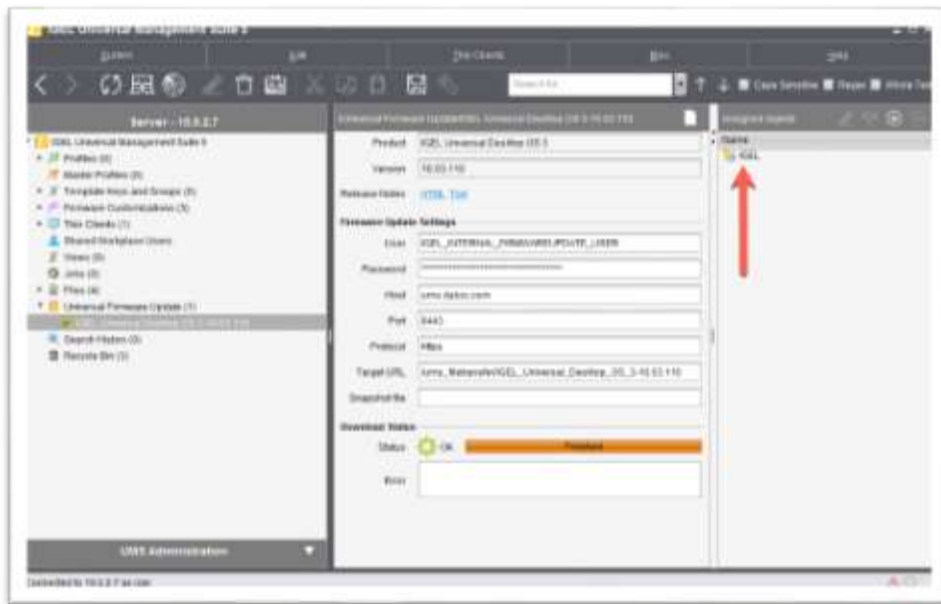


18. As with profiles, you can define at which time you wish to push the instruction set to configure the device to download the firmware when triggered.

Select the desired radio button and click the **OK** button to continue.



19. You are brought back to the UMS and will notice the folders and devices you assigned to the selected IGEL OS firmware are listed in the **Assigned objects** pane.



You have successfully configured the firmware update. The next step is to define how and when you wish the firmware to be deployed to the desired IGEL OS devices. Please skip to the [How to Deploy a Firmware Update](#) section.

3. 3. Update IGEL OS Firmware via the ICG

As discussed above, if you have IGEL devices connected to the IGEL UMS via the ICG you are not able to use the traditional **Universal Firmware Update** UMS feature. You are required to deploy the updates using a UMS profile. The firmware update files are required to be stored in a location that your devices can connect to and download from.

The first thing you need to decide upon is where to store the IGEL firmware files. As stated above, the data is required to be accessible from the client. You can place them in any location that allows the IGEL OS to download them directly. IGEL supports FTP, SFTP, HTTP, HTTPS, FTPS, or File. In this document, we have detailed how to store the firmware updates on AWS S3, Citrix ShareFile, or a traditional FTP server, in this case, a Microsoft IIS FTP server.

Once you have created the required firmware file repository, you are required to develop a simple UMS profile and then assign it to the devices you wish to update. It is just that simple.

This section is broken down into the following steps, depending on your desired configuration:

- **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**
- **How to Deploy Firmware Update**
 - [How to Manual Deploy from UMS](#)
 - [How to Automate Updates on Shutdown](#)
 - [How to Schedule Updates using Jobs & Views](#)
- **How to Update Existing Profiles**

3. 3. 1 Download IGEL OS Firmware

Before you get too far, you need to download the appropriate firmware version for the type of device(s) you wish to update. Please refer to the previous section for more information on which firmware version is right for you.

For this document, we are updating the IGEL UDC or UD Pocket thus the **OS** firmware family is the correct version for this use-case.

The following defines how to download the IGEL OS firmware for the UDC/UD Pocket:

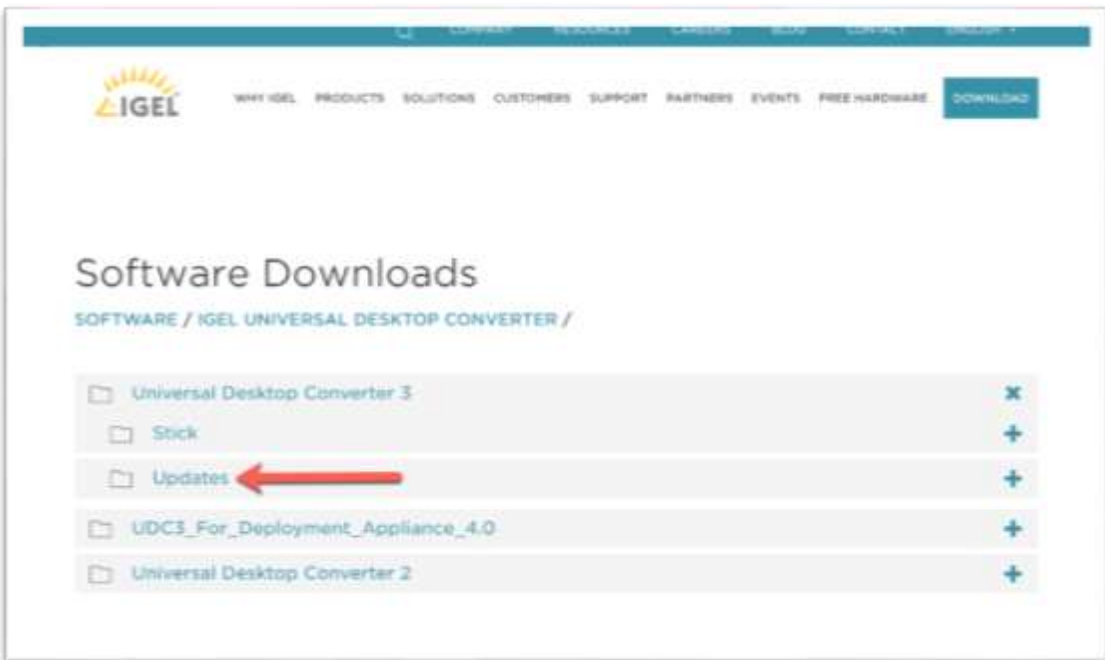
1. IGEL has recently updated the IGEL website and the Software Downloads section. To download the latest OS version firmware, browse to the following web page <https://www.igel.com/software-downloads/> and click the **IGEL Universal Desktop Converter** link.



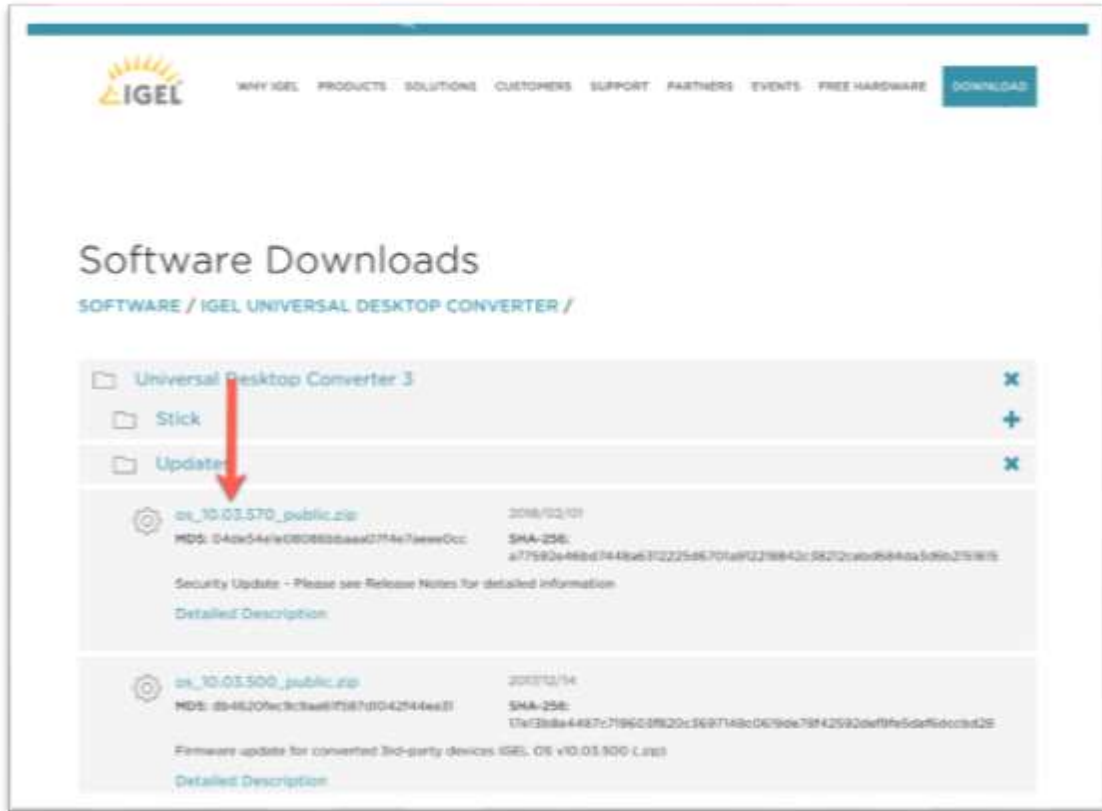
2. Click to expand the **Universal Desktop Converter 3** link.



3. Click to expand the **Updates** link



4. You are presented with a list of the most recent versions of the IGEL OS firmware. Click to download the desired version(s) and save them to a location accessible as you will extract and copy the firmware files to the desired download location in a bit.



3. 3. 2 Create Firmware Repository

For the IGEL OS to download the required firmware files, they need to be accessible. This can be done using FTP, SFTP, HTTP, HTTPS, or FTPS. That is up to you.

For this document, we have tried to detail how to use the most common solutions, AWS, Citrix ShareFile, and a standard FTP server. You only need to choose one.

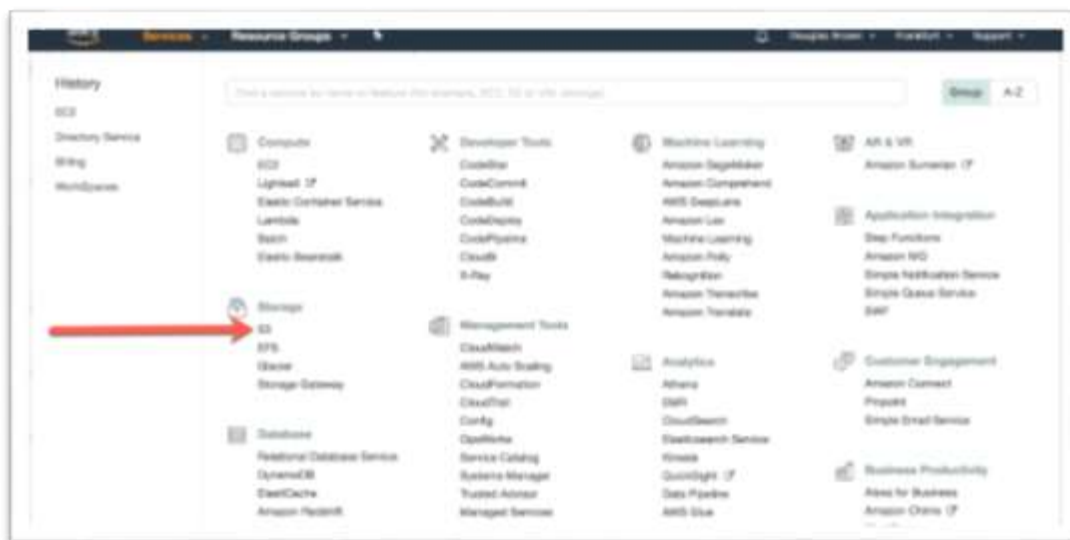
The following section is broken down into the following options:

- [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](#)

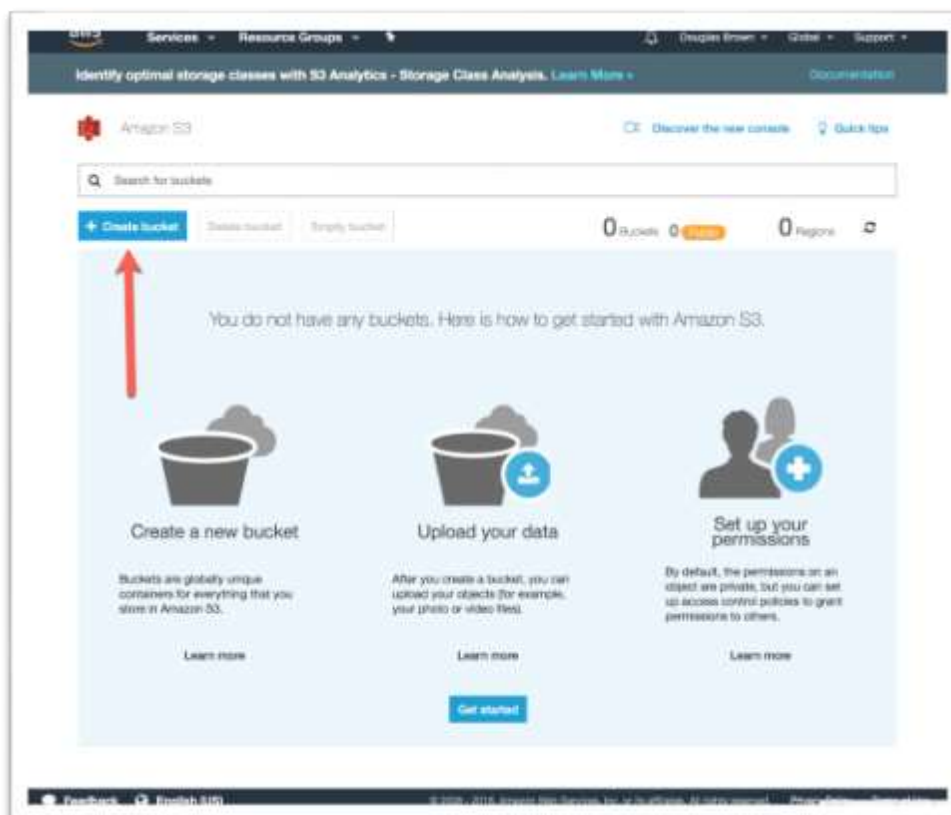
How to Configure AWS S3 as the Firmware Repository

If you have chosen to use AWS S3 as the firmware repository, please follow the steps below to configure a new AWS S3 Bucket:

1. Browse to the AWS portal and log in. From the **Services** menu click the **S3** link.



2. Click the **Create bucket** button to continue.



- The next step is to create the S3 Bucket. You are required to enter a bucket name. The Bucket name needs to be a unique DNS-compliant name. This name must be unique across all existing bucket names in Amazon S3. After you create the bucket, you cannot change the name. This name is visible in the URL that points to the objects that you are going to put in your bucket, so please choose wisely.

For more information about naming buckets, please refer to the [Rules for Bucket Naming](#) in the **Amazon Simple Storage Service Developer Guide**.

Next, select the Region the firmware files are stored. If you have IGEL devices located across the globe, you will want to create multiple buckets and thus numerous profile configurations for each region. For now, select the region that is closest to your devices.

Click the **Create** button to create the new S3 storage Bucket.

The screenshot shows the 'Create bucket' dialog box in the AWS Management Console. The dialog has a blue header with the title 'Create bucket' and a close button. Below the header is a progress bar with four steps: 1. Name and region, 2. Set properties, 3. Set permissions, and 4. Review. The first step, 'Name and region', is currently selected. The main content area is dark blue and contains the following fields and options:

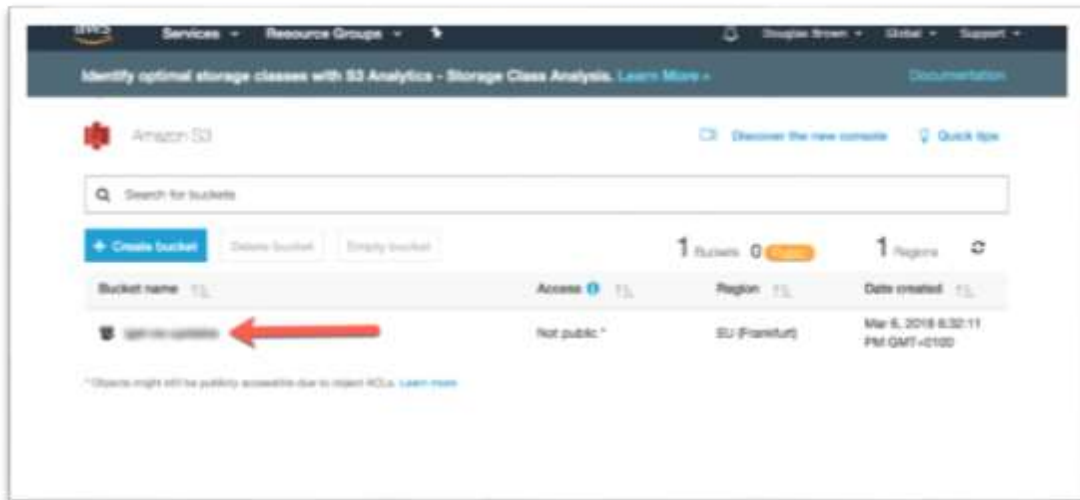
- Name and region**: A section header.
- Bucket name**: A text input field with a red arrow pointing to it.
- Region**: A dropdown menu with 'EU (Frankfurt)' selected and a red arrow pointing to it.
- Copy settings from an existing bucket**: A section header.
- You have no buckets**: A text box indicating no existing buckets are available for copying settings.
- 0 Buckets**: A dropdown menu showing the count of existing buckets.

At the bottom of the dialog, there are three buttons: 'Create' (with a red arrow pointing to it), 'Cancel', and 'Next'.

4. Your new bucket is created, and you will see it in the list of S3 Buckets.

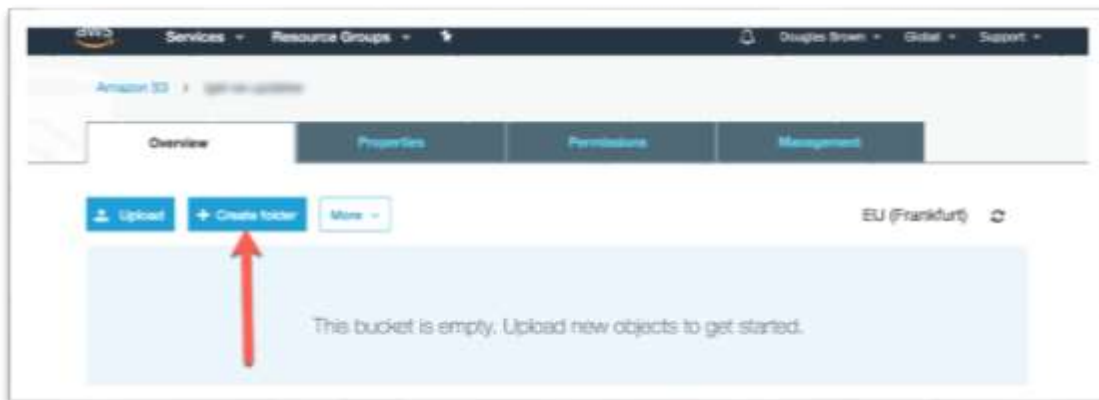
You will notice, we have blurred the name of the bucket. This is due to the fact the bucket name is used in the URL you will configure the IGEL OS to download the updates from. If this URL is publicly available, then anyone can use it to download their updates and thus your S3 storage bill could become rather large. You are duly warned.

Click the bucket name link to continue.



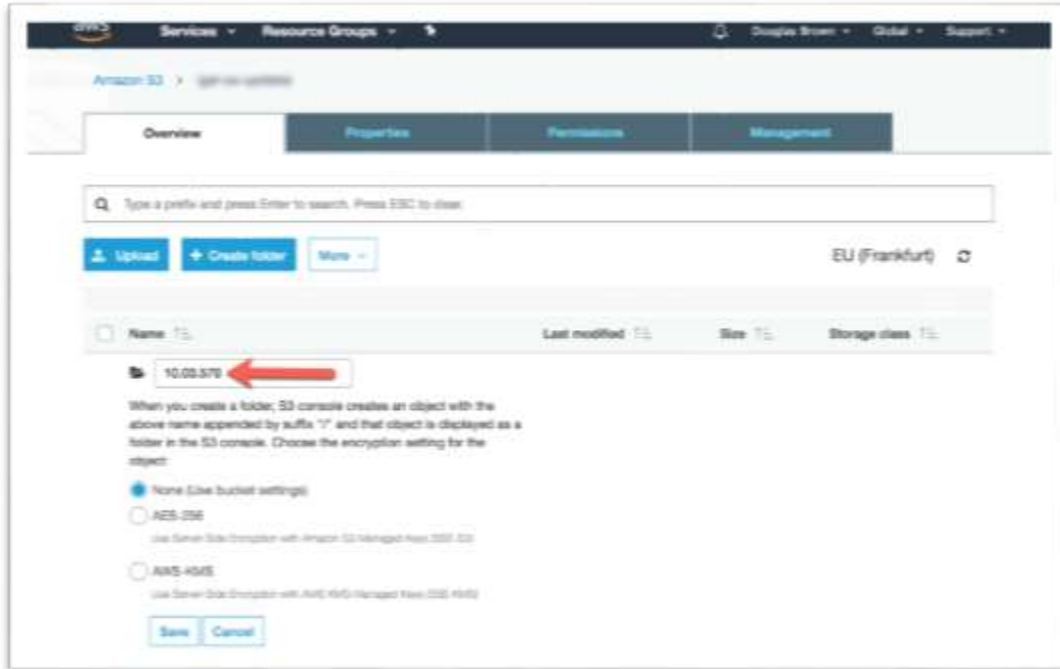
5. Over time you might find yourself with multiple firmware versions for a different type of devices and different firmware version numbers. Thus, it is recommended to create a folder for each firmware update.

Click the **Create folder** button to continue.

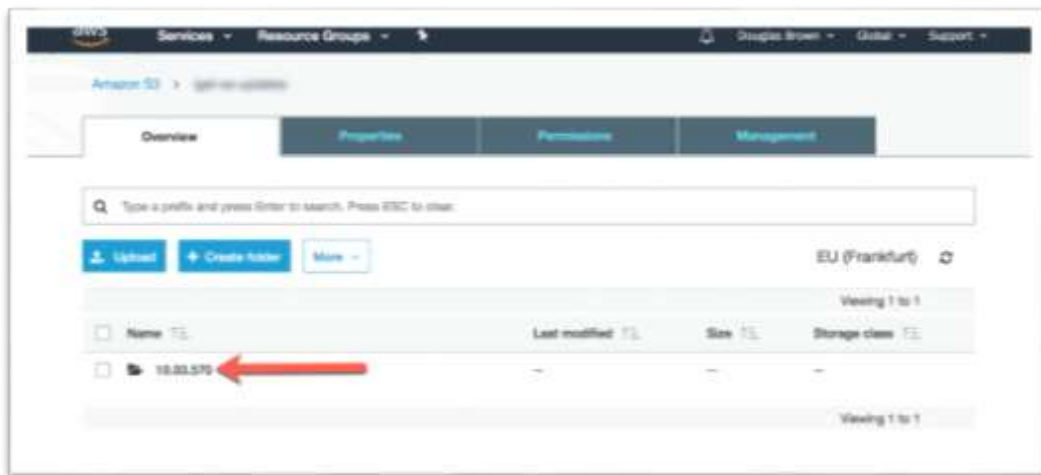


6. Enter a name for the new folder. We recommend selecting a name that reflects the firmware version.

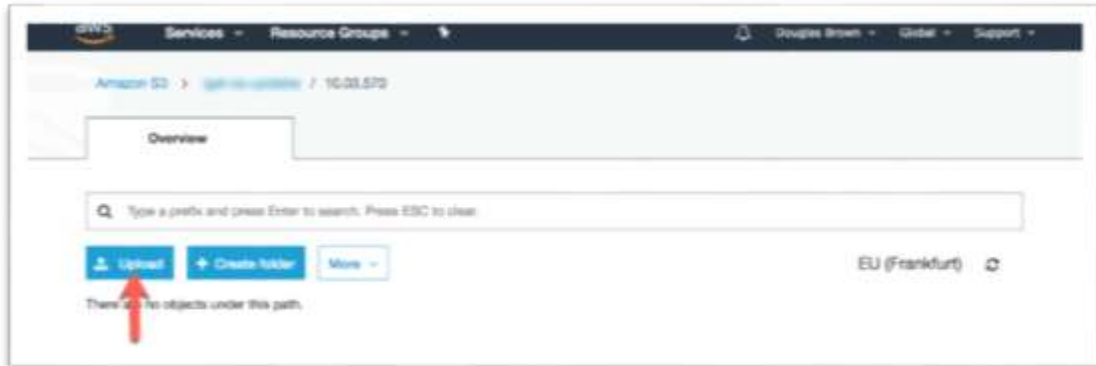
Enter the desired name and click the **Save** button to create the new folder.



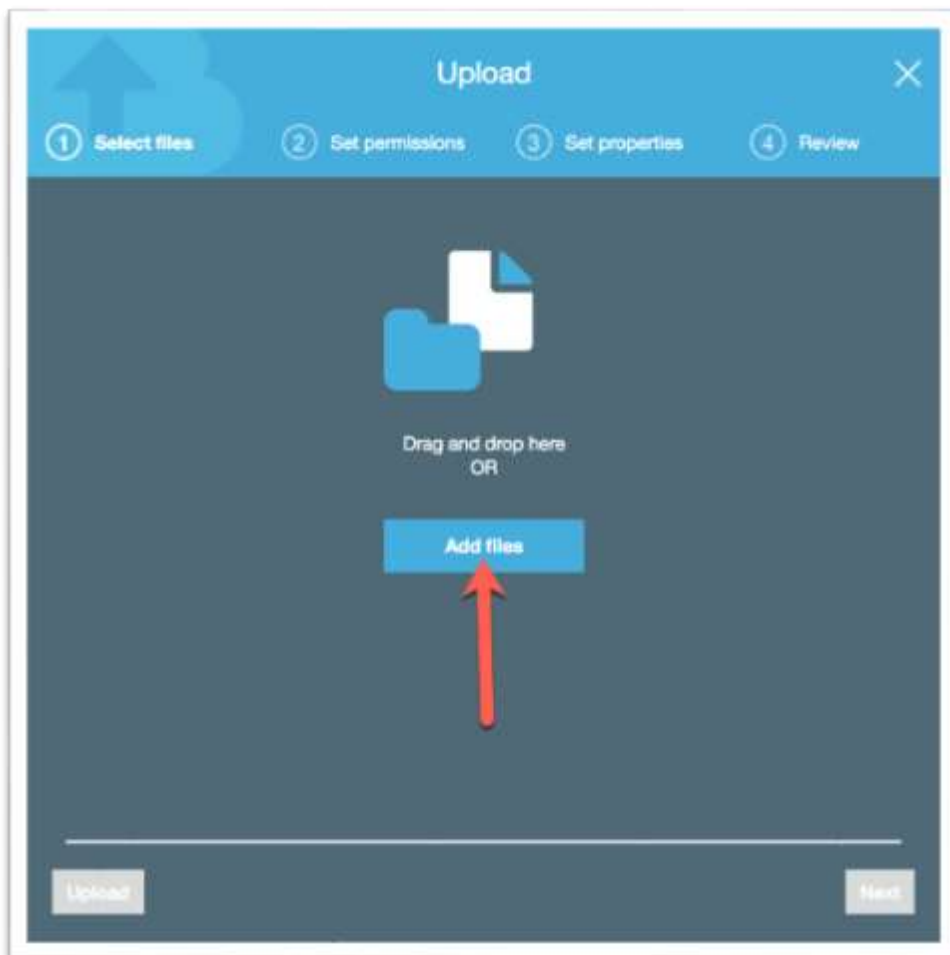
7. Click on the newly created folder to continue.



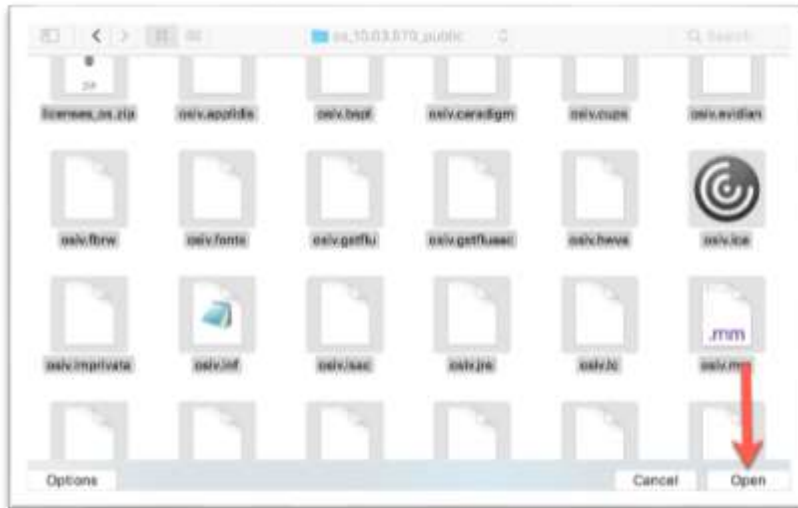
8. You are ready to upload the firmware files you downloaded above. Click the blue **Upload** button to continue.



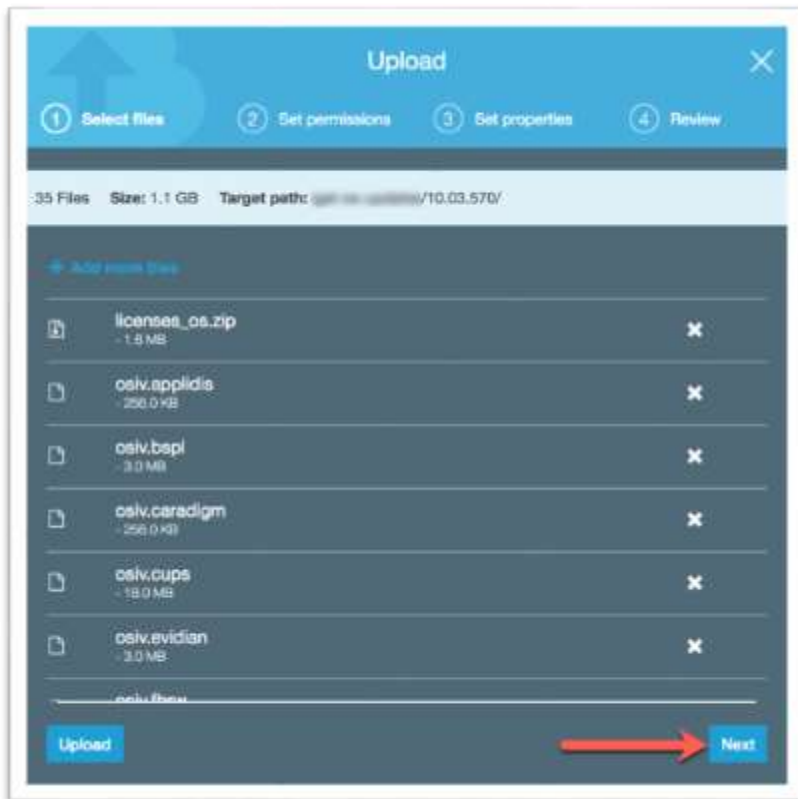
9. Click the **Add files** button to continue.



10. Browse to the location you extracted the firmware files you downloaded and hit **CTRL/Command A** (depending on OS version) to select all the files and then click the **Open** button.

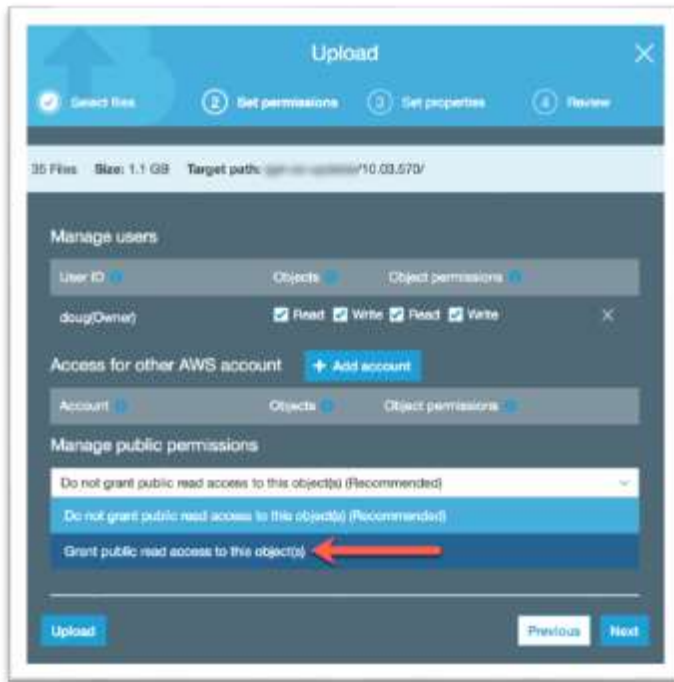


11. Click the **Next** button to continue.

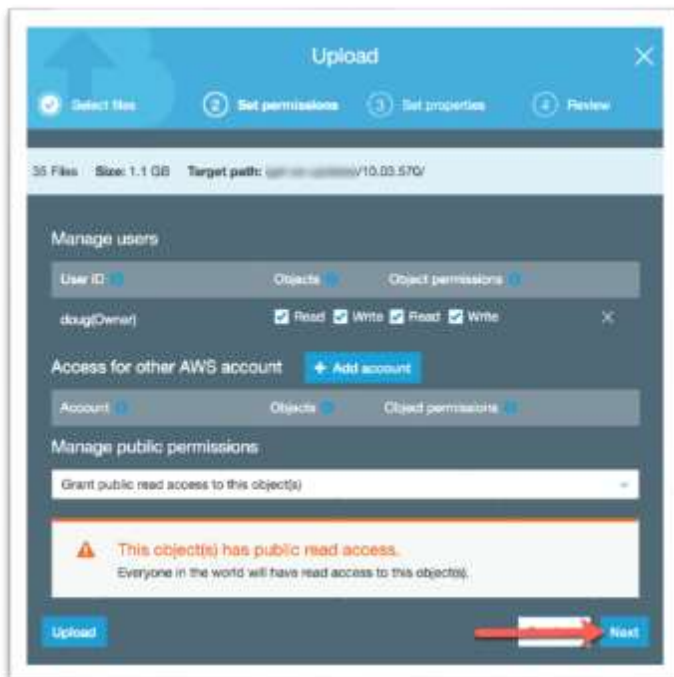


12. You are required to make the files public, so they are accessible to be downloaded by the IGEL OS. Click to dropdown the **Manage public permissions** combo box and select the **Grant public read access to this object(s)** item.

Click **Next** to continue.



13. You are warned that everyone will have read access to your files. This is perfect, click the **Next** button to continue.



14. Click **Next** to continue.

Upload

Select files Set permissions **3 Set properties** 4 Review

35 Files Size: 1.1 GB Target path: s3://igel-ubuntu/10.03.570/

Storage class
Choose one depending on your use case, scaling and performance access requirements.

☒ Standard ☐ Standard-IA ☐ Reduced redundancy

Encryption
Protect data at rest by using Amazon S3 master key or by using AWS KMS master key.

☒ None ☐ Amazon S3 master key ☐ AWS KMS master key

Metadata
Metadata is a set of name-value pairs. You cannot modify object metadata after it is uploaded.

Header Value

Upload **Next**

15. You are ready to upload the firmware files. Click the **Upload** button to start the upload process.

Upload

Select files Set permissions Set properties **4 Review**

Files Edit

35 Files Size: 1.1 GB

Permissions Edit

2 grantees

Properties Edit

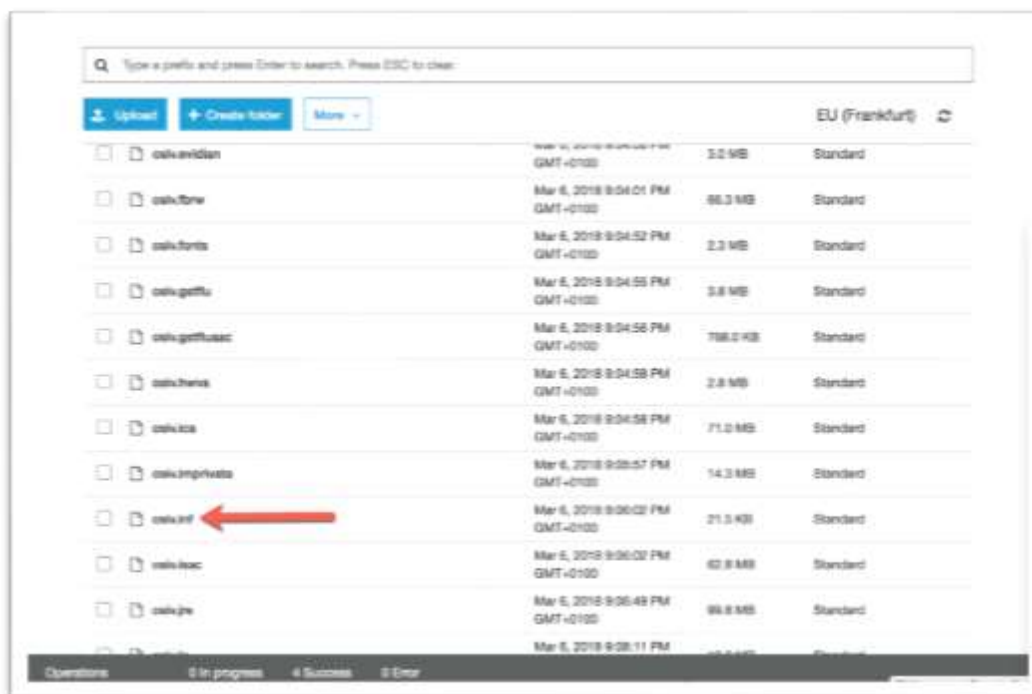
Encryption No Storage class Standard

Metadata

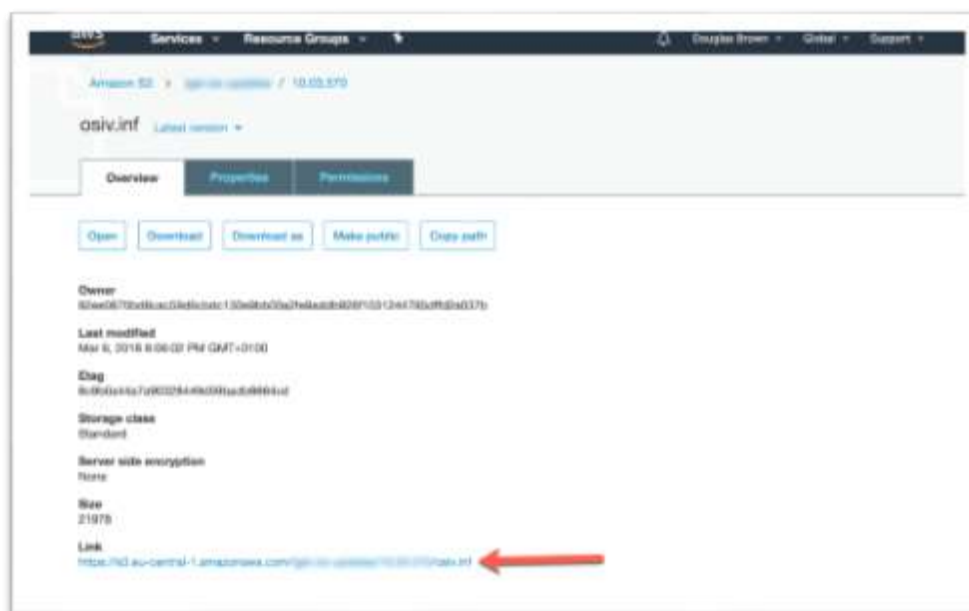
Tag

Upload

16. Once the files are uploaded, browse the list until you find the **osiv.inf** file and click to open its properties.



17. This is the file that gives you the complete path to the firmware files. Copy and paste this URL into a safe place as you will use it when creating a UMS Update profile.



You are done and can skip to the [How to Create a Firmware Update Profile](#) section to configure the IGEL OS devices to use the newly created firmware repository.

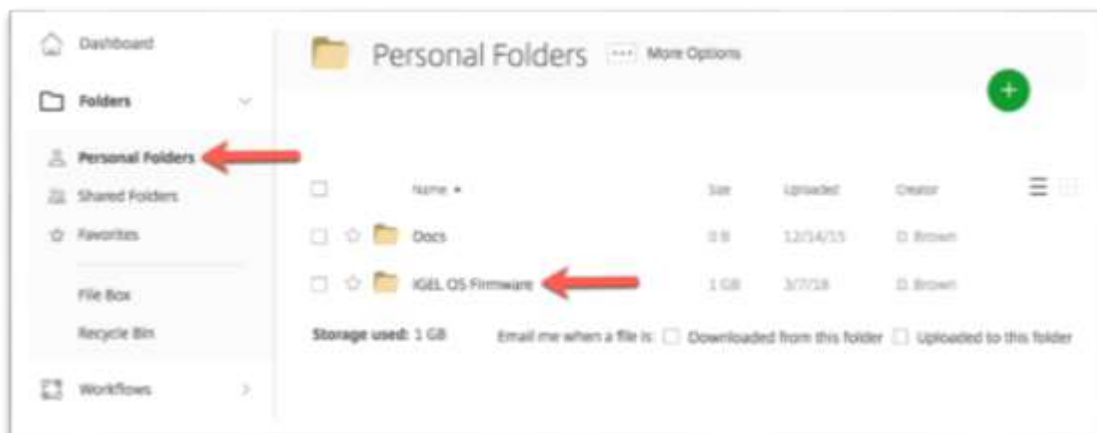
How to Configure Citrix ShareFile as the Firmware Repository

If you have chosen to use Citrix ShareFile as the firmware repository, please follow the steps below to configure ShareFile:

By default, the Citrix ShareFile FTP service only establishes nine FTP connections at a time. In this case, you would either need to set an update task to be trigger nine updates at shutdown and then repeat the process until all devices are updated, or you can try to contact ShareFile support and negotiate to change this setting on your ShareFile account, though we cannot promise they will.

1. Open your favorite Browser and browse to your Citrix ShareFile account's web page and log in.
2. Once logged in, it is recommended to create a firmware update folder structure to store the different firmware updates the IGEL OS will be downloading. You can store this in any location you like, just be mindful of the location as you will need the full path when creating the UMS Update profile in a coming step.

In this example, you have created a folder in the **ShareFile Personal Folders** called **IGEL OS Firmware**.

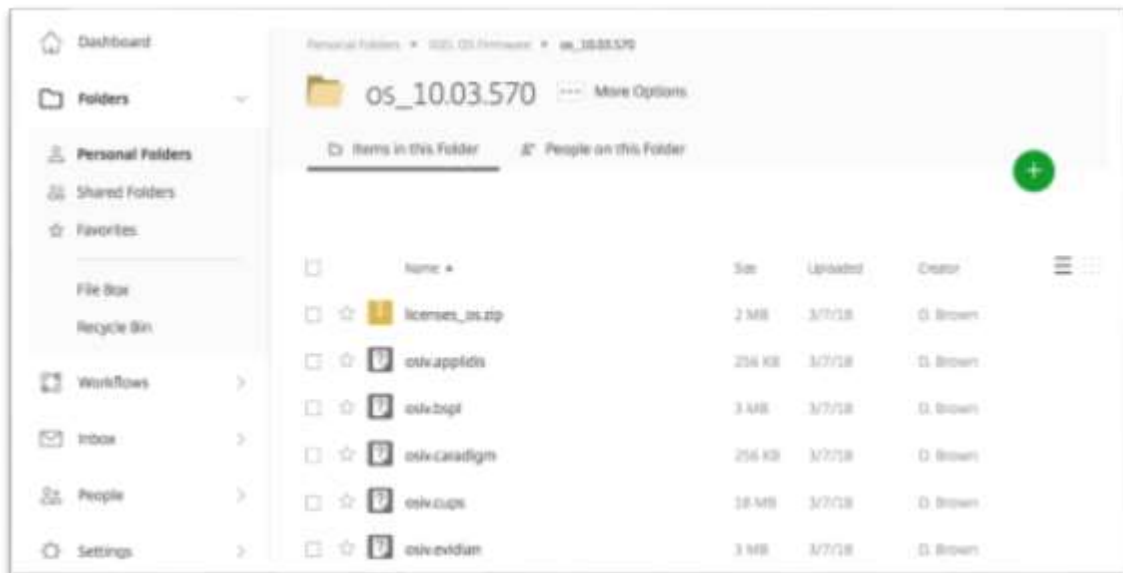


- Next, you will want to create the different folders for each firmware update. In this example, you have named it **os_10.03.570**.



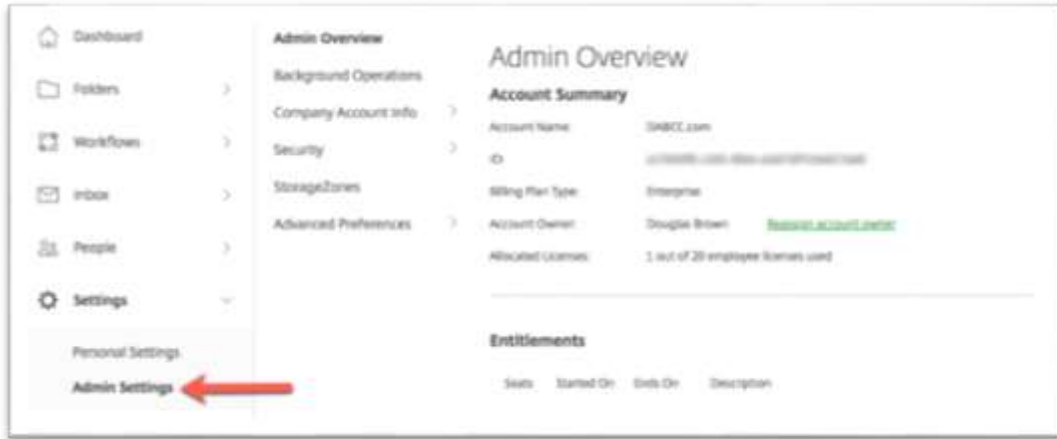
- Open the folder you created above and copy the extracted firmware files for the appropriate firmware to the newly created folder. This will take a bit of time to upload the files to the ShareFile cloud.

The upload will occur in the background; you can move forward to the next step.

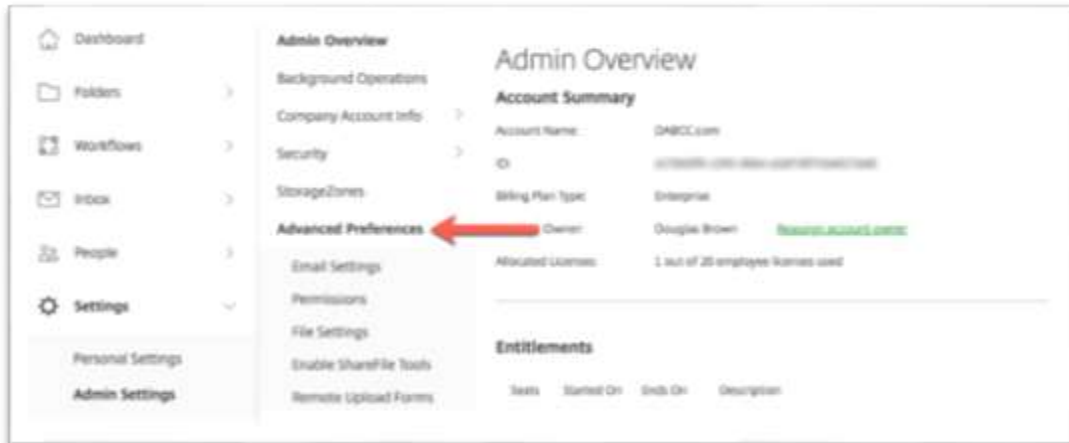


- Now that you have created your folder structure and are copying the firmware files to ShareFile you will need to configure the ShareFile service to allow the IGEL OS to download via the ShareFile FTP server.

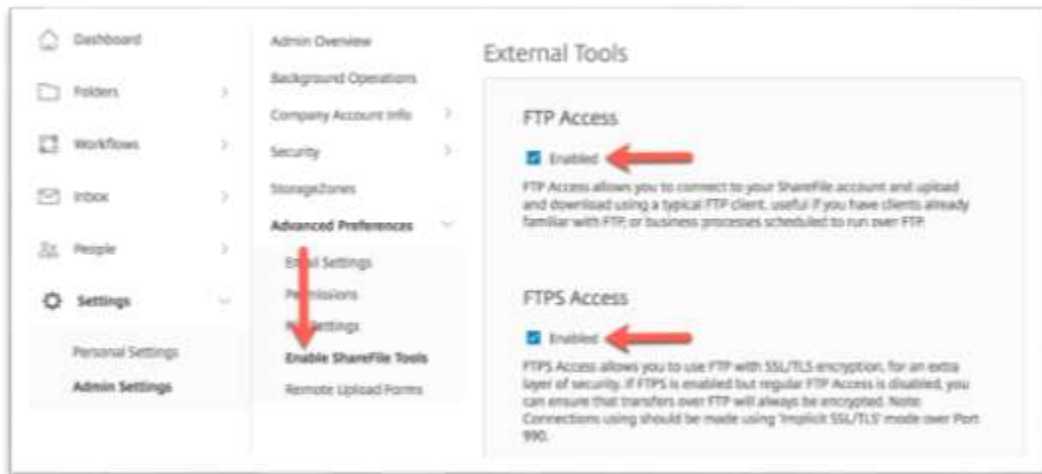
From the ShareFile web page, on the left menu, click to expand the **Settings** node and then click the **Admin Settings** link.



- Click to expand the **Advanced Preferences** node



7. Click to the **Enable ShareFile Tools** node and browse to the **External Tools** section of the page. Click to check the **FTP Access** and **FTPS Access** checkboxes to enable the FTP service.



8. From the **Settings** section of the left menu click to select the **Personal Settings** node.



- Click to select the **Advanced Connections** node and browse to the **FTP Settings** section of the page. On this page, the FTP server name and username are displayed. Make a note of the **FTP Server URL** and the **User Name** as you will use them when creating the firmware update profile in a later section below.

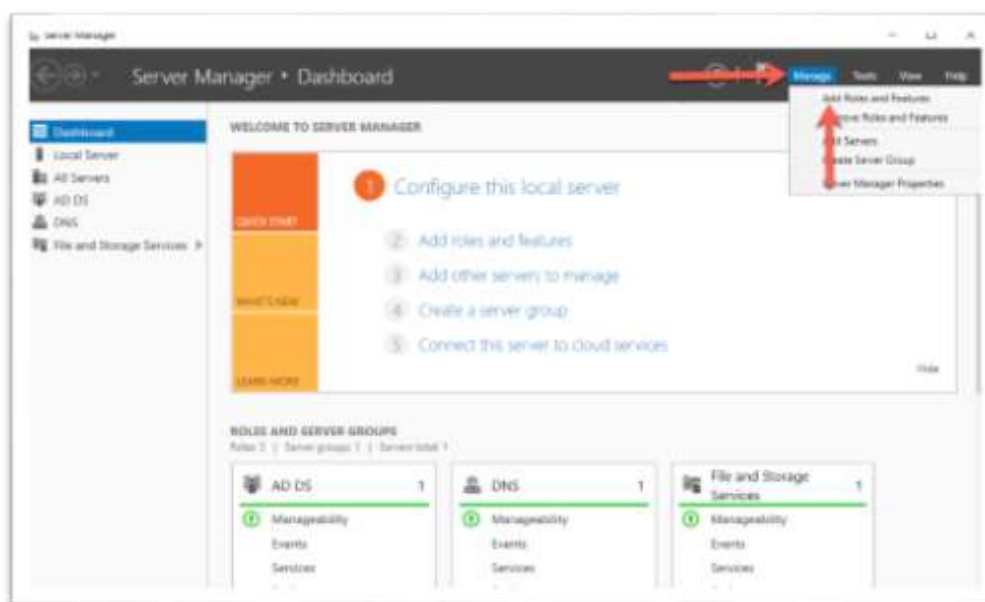


You are done and can skip to the **How to Create a Firmware Update Profile** section to configure the IGEL OS devices to use the newly created firmware repository.

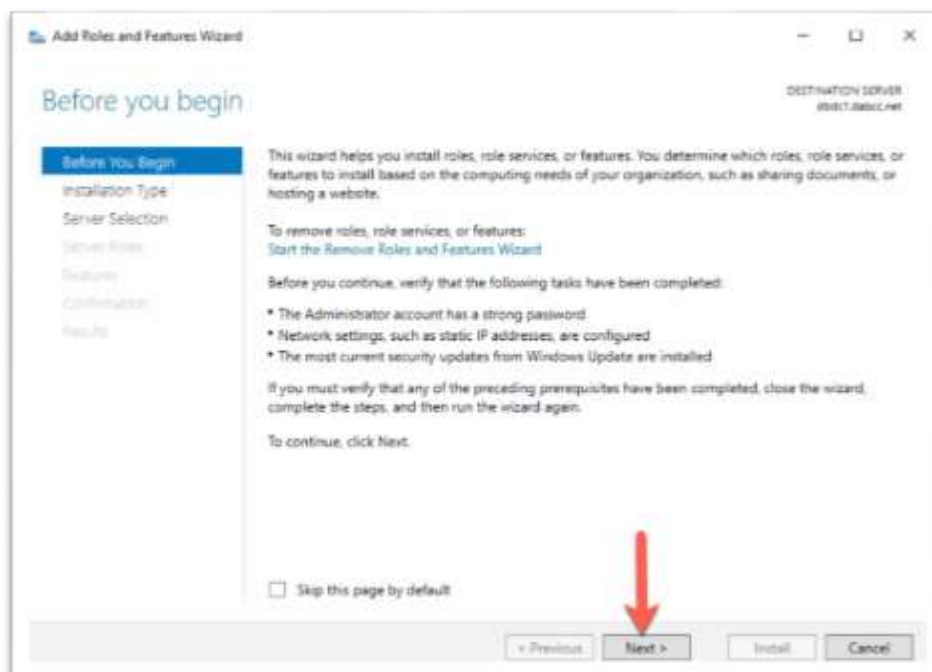
How to Configure Microsoft IIS FTP as the Firmware Repository

If you have chosen to use a Microsoft IIS FTP server as the firmware repository, please follow the steps below to create and configure the IIS FTP server:

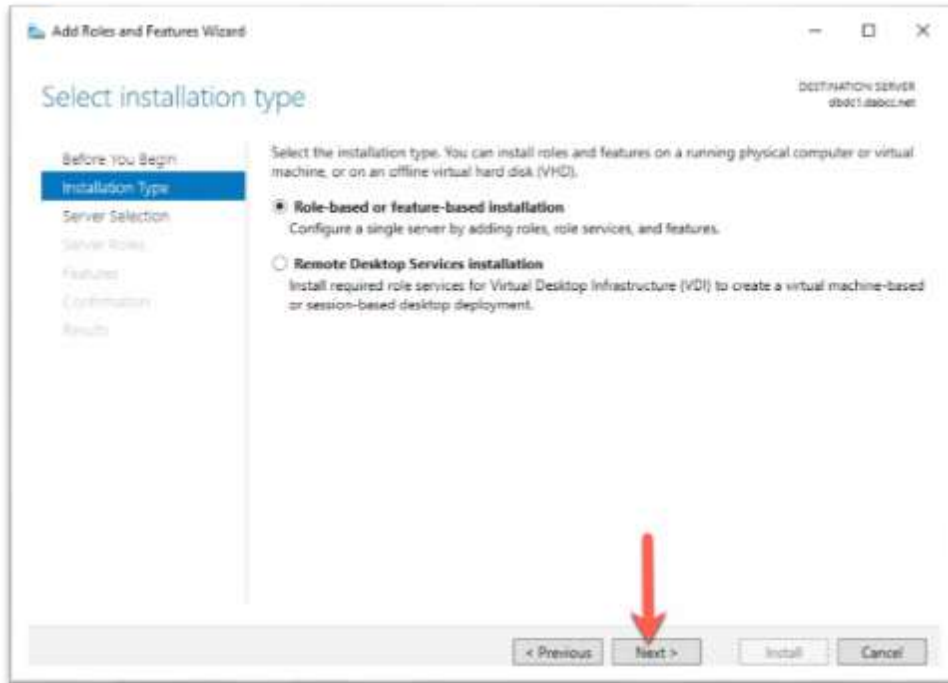
1. Open the **Server Manager** and click to expand the **Manage** menu and then click the **Add Roles and Features** link.



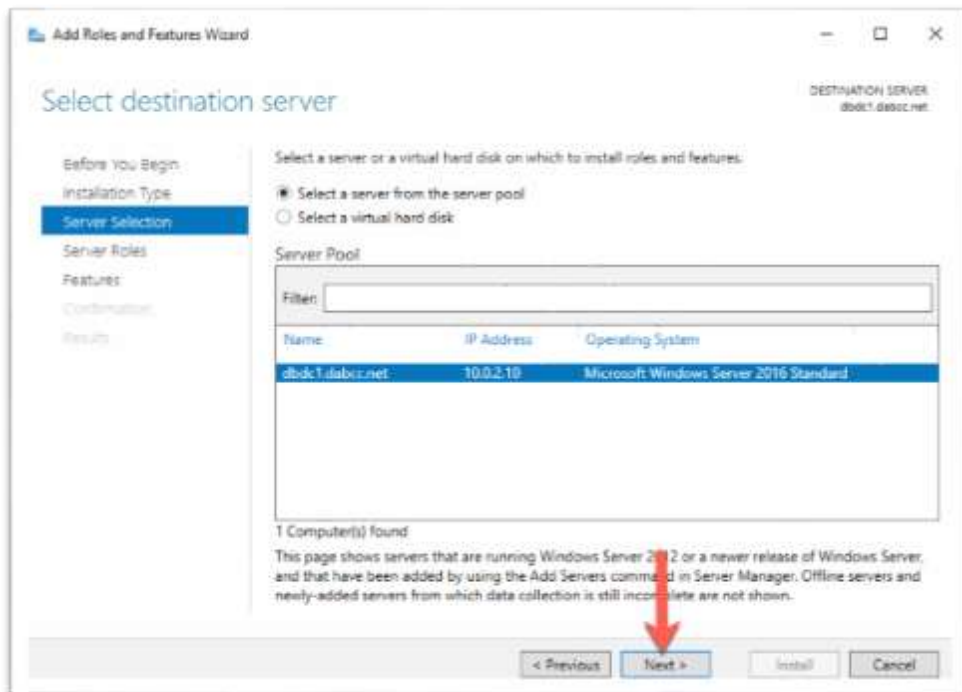
2. Click the **Next** button to continue.



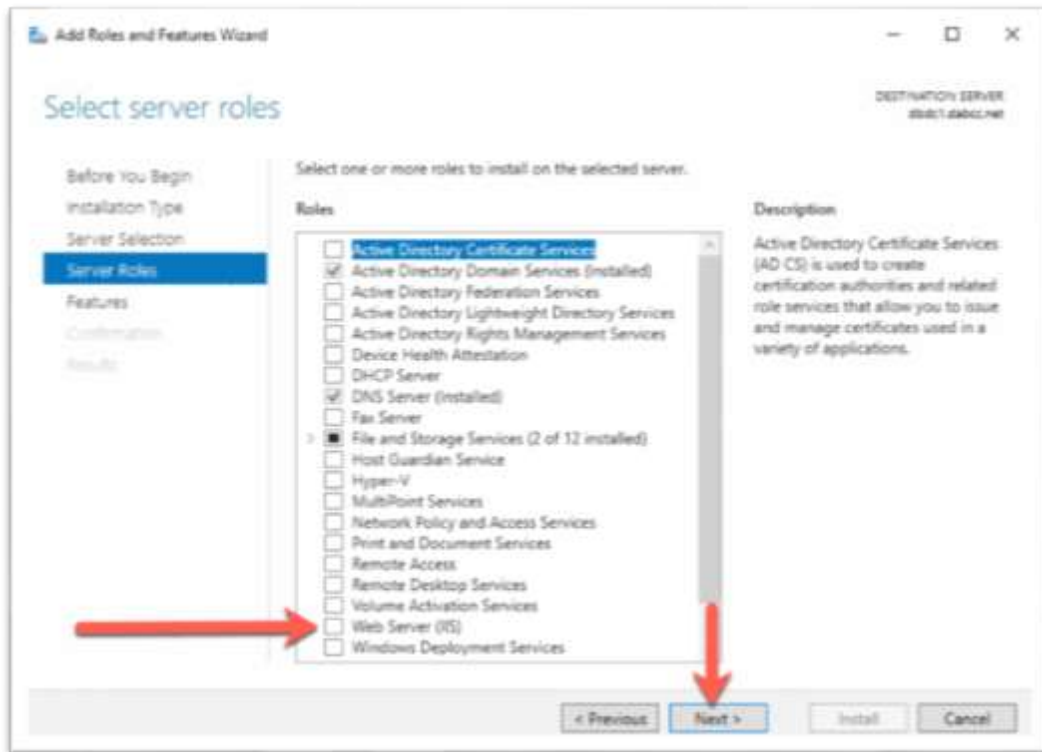
3. Accept the default **Role-based feature-based installation** and click **Next** to continue.



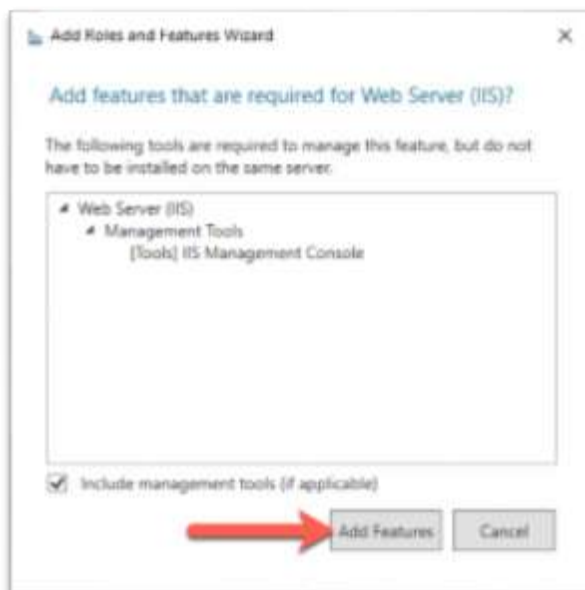
4. Accept the default **Select a server from the server pool** and click **Next** to continue.



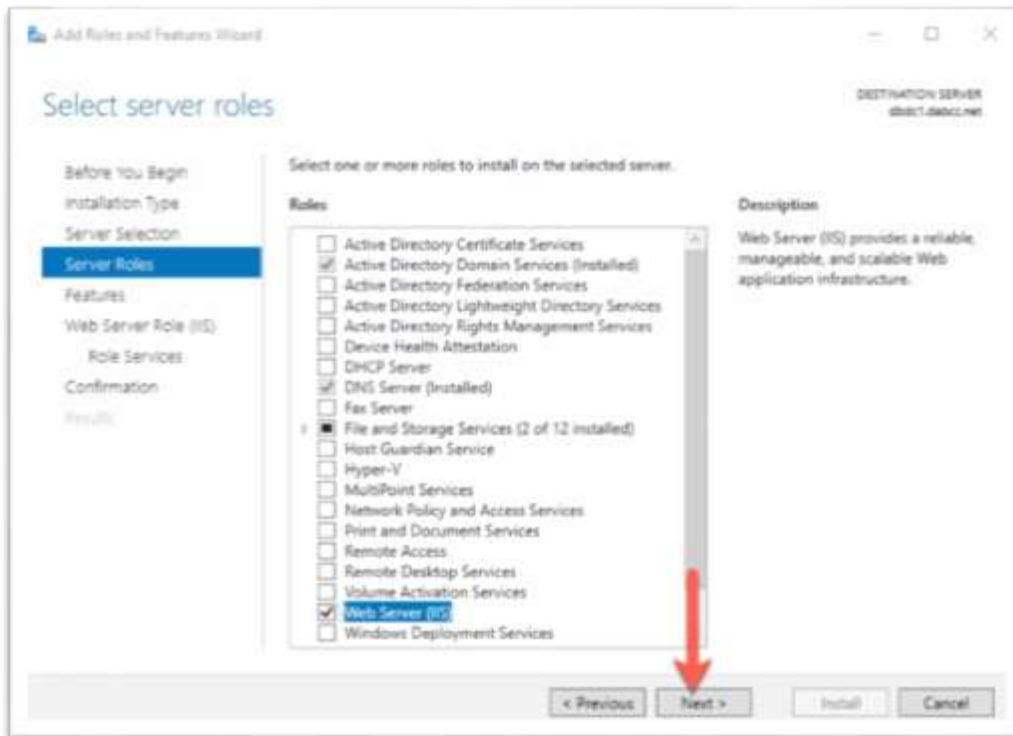
5. Click to check the **Web Server (IIS)** role and click **Next** to continue.



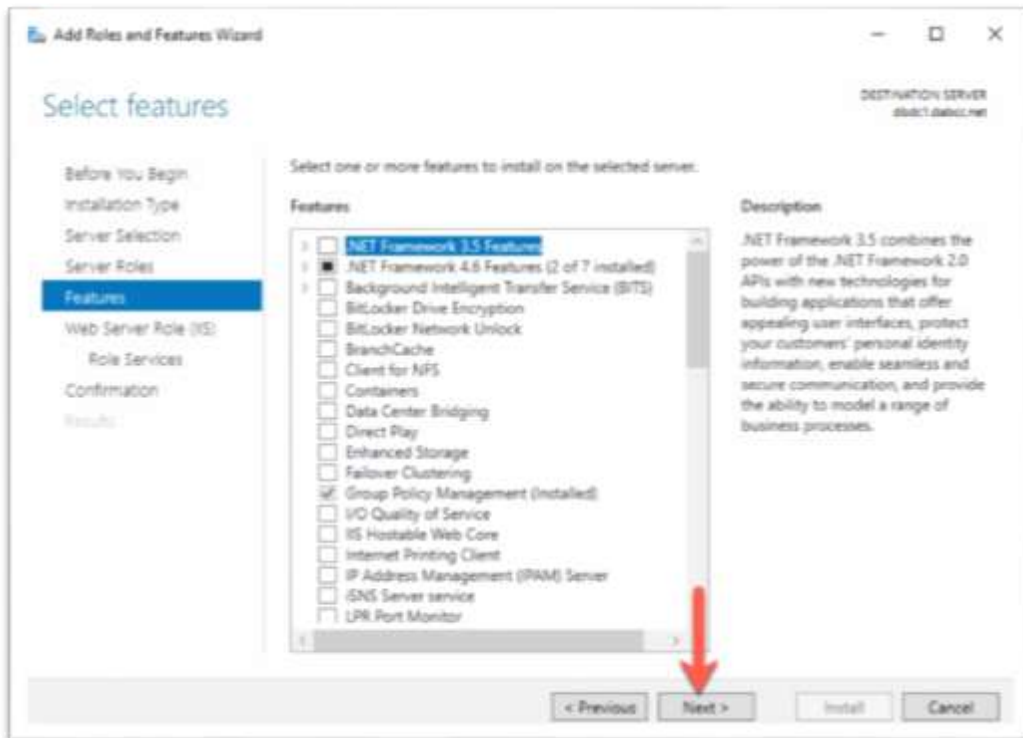
6. Click the **Add Features** button to continue.



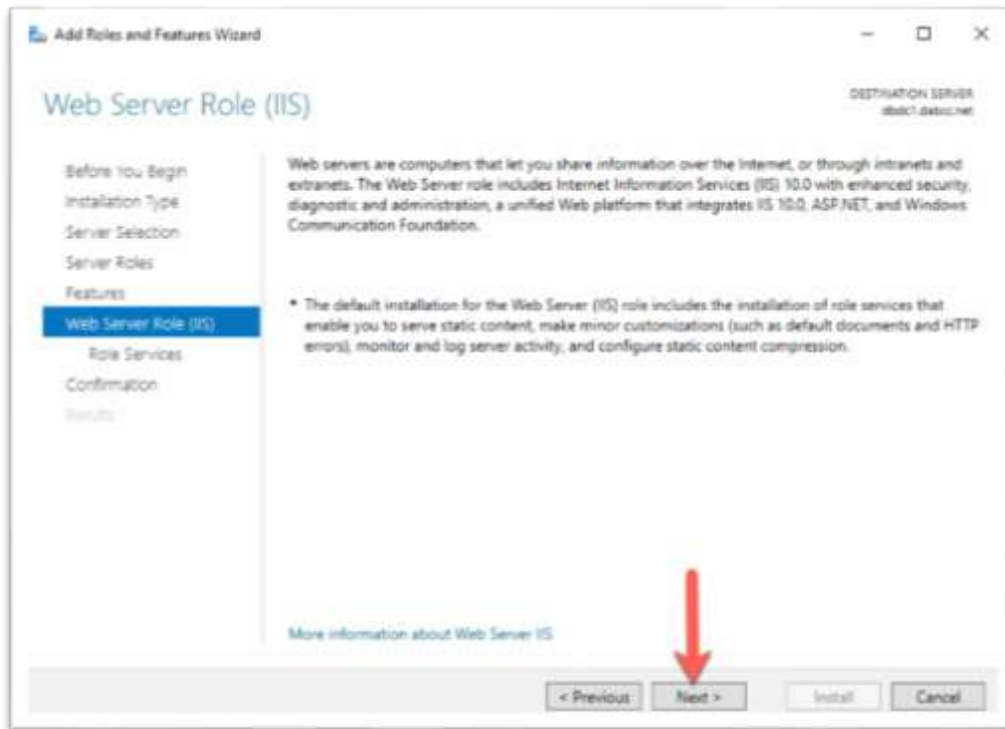
7. You are brought back to the Roles page, and you will notice the **Web Server (IIS)** checkbox is checked. Click **Next** to continue.



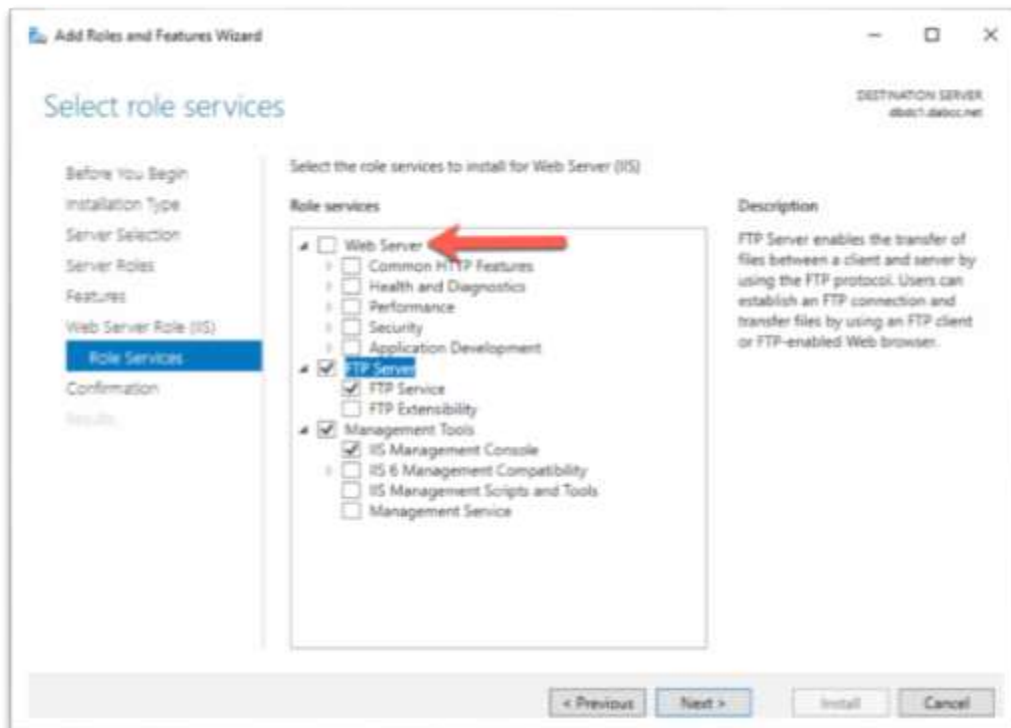
8. Click **Next** to continue.



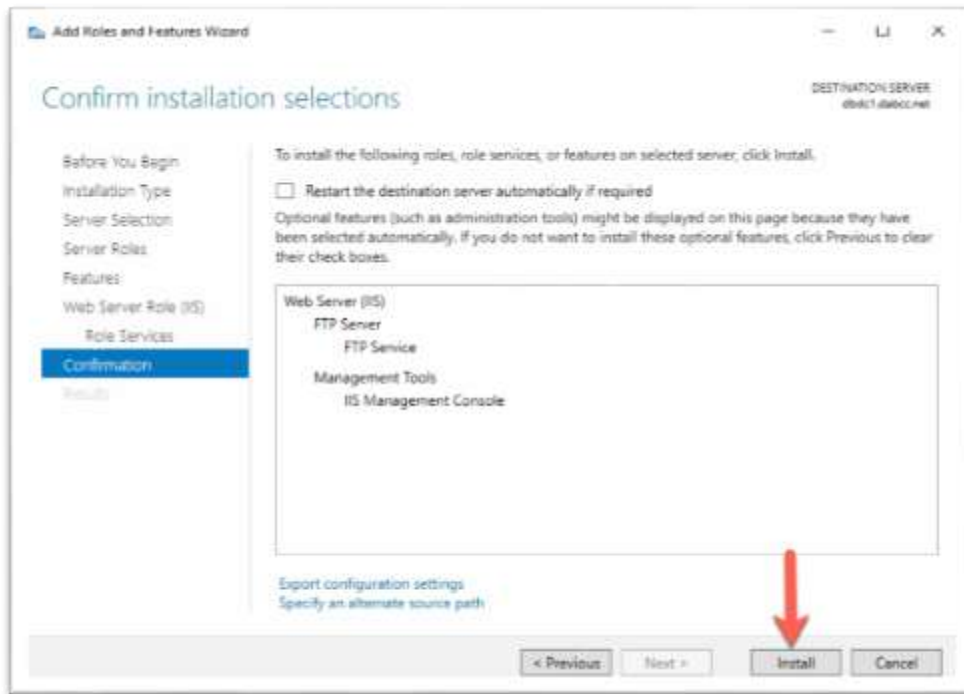
9. Click **Next** to continue.



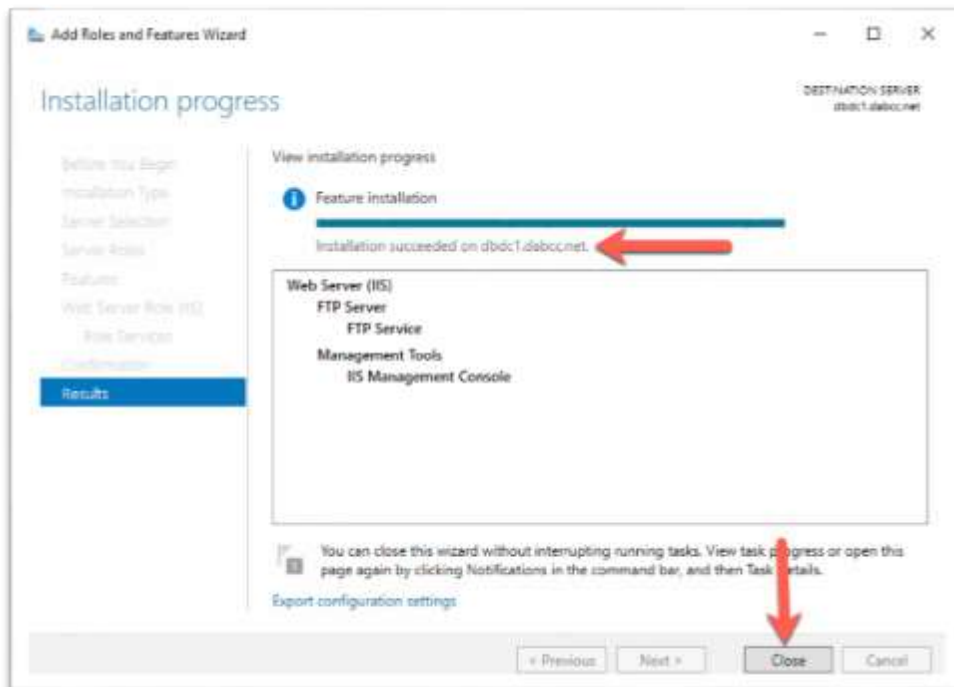
10. It is time to configure the different IIS Services you wish to install. In this use-case you are only installing the FTP Server, you can uncheck the **Web Server** checkbox and then click to check the **FTP Server** checkbox and then click **Next** to continue.



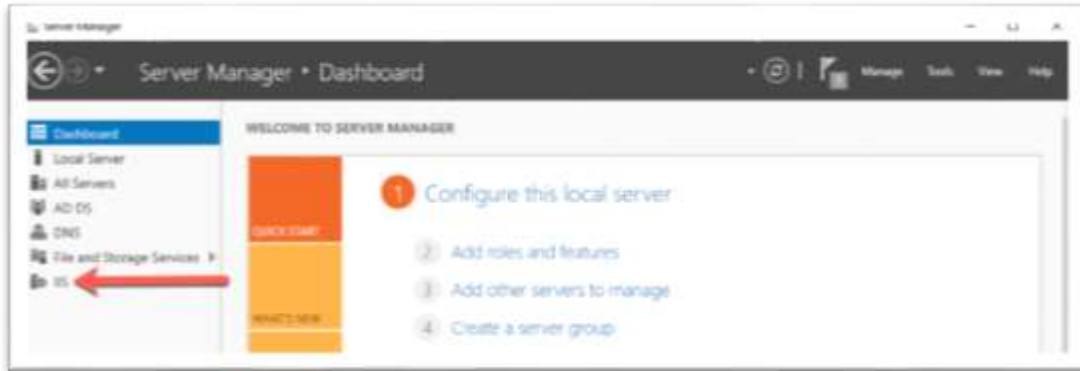
11. Verify your settings look like the screenshot below and click the **Install** button to install the FTP Server.



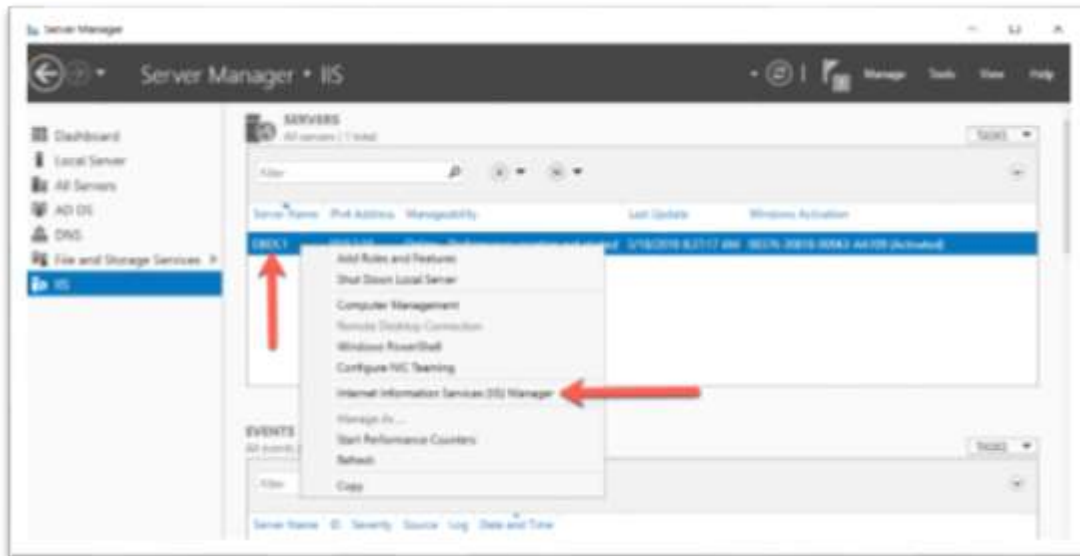
12. If all goes as planned, you are promoted that the installation succeeded. Click the **Close** button to continue.



13. You have successfully installed a Microsoft FTP server. The next step is to create the FTP site you will use to store IGEL OS firmware updates. Click the new **IIS** entry in the left menu.



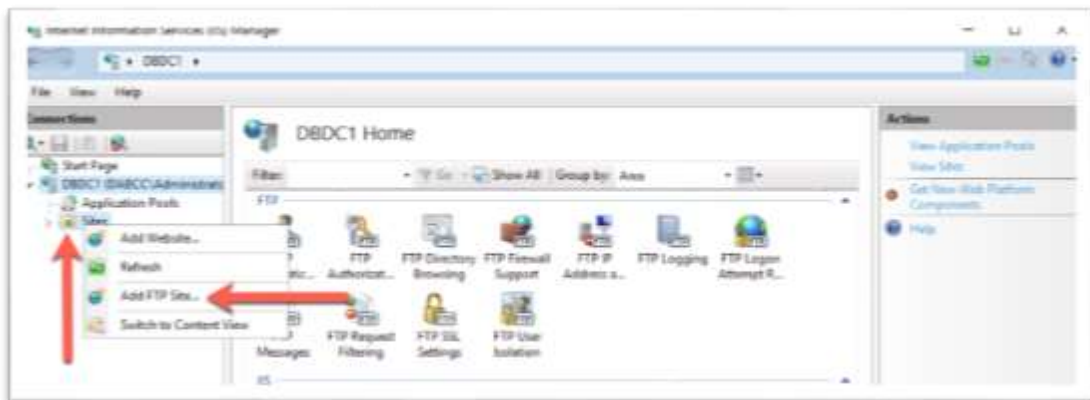
14. You should see your newly installed FTP server listed in the right pane, right-click on it to reveal the context menu. Click the **Internet Information Services (IIS) Manager** link.



15. The **Internet Information Services (IIS) Manager** opens. Click to expand the server's node in the left men.

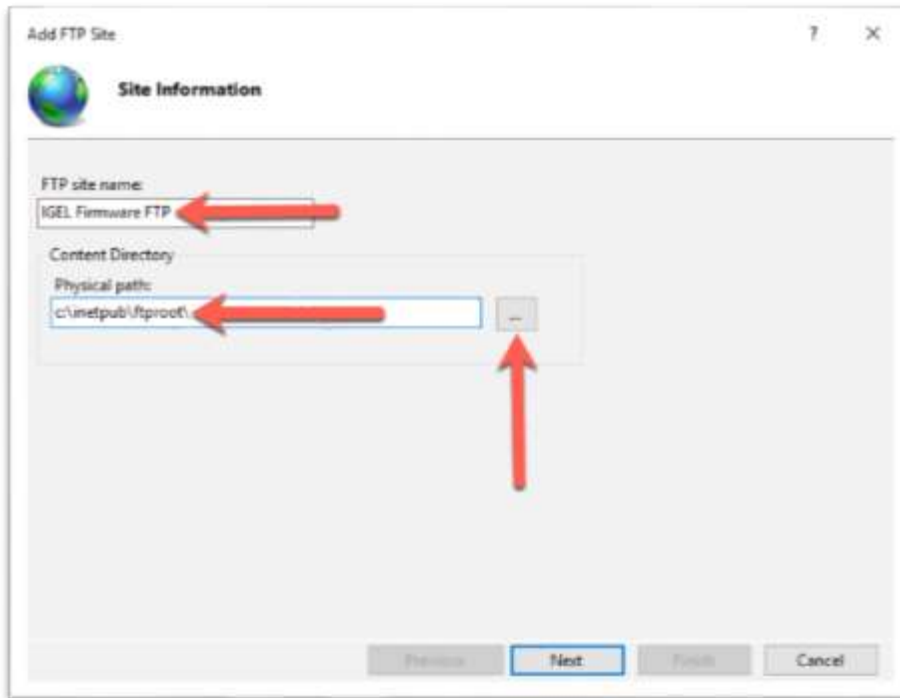


16. Right-click the **Sites** node to expose the context menu and click the **Add FTP Site** link to continue.

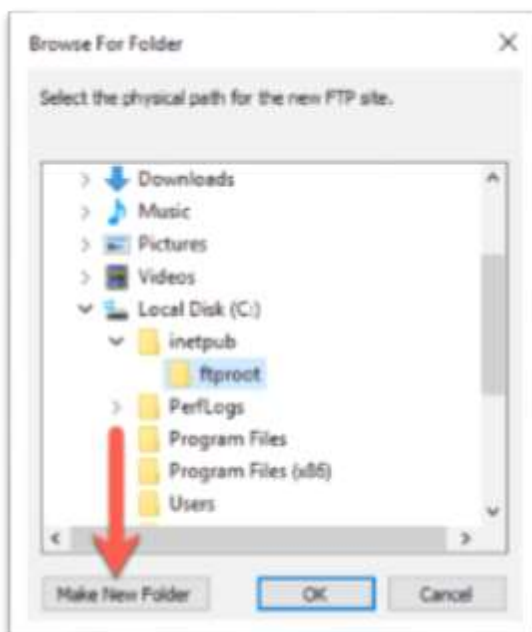


17. Enter a friendly name in the **FTP site name** text box and then enter **c:\inetpub\ftproot** in the **Physical path** text box and click the ... button to create the location you will be storing the firmware image files.

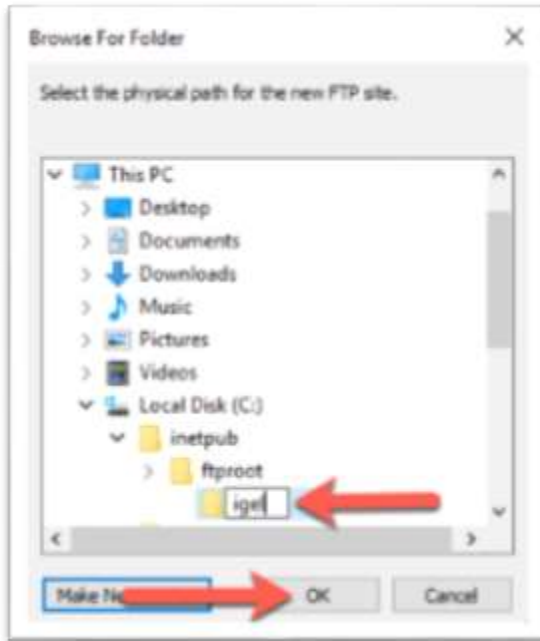
You will need to make sure you have enough disk space to store the firmware updates. Firmware updates can be rather large, greater than 1GB in size.



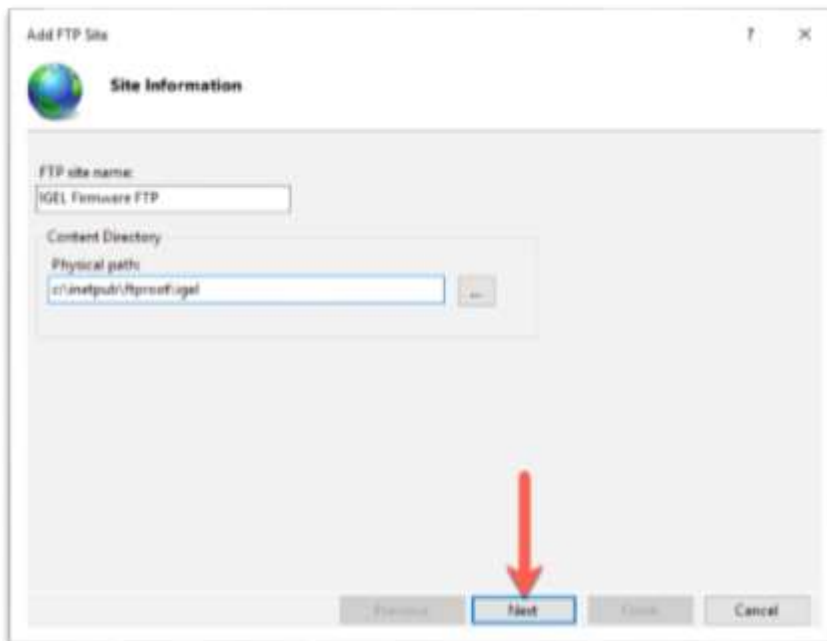
18. Click the **Make New Folder** button.



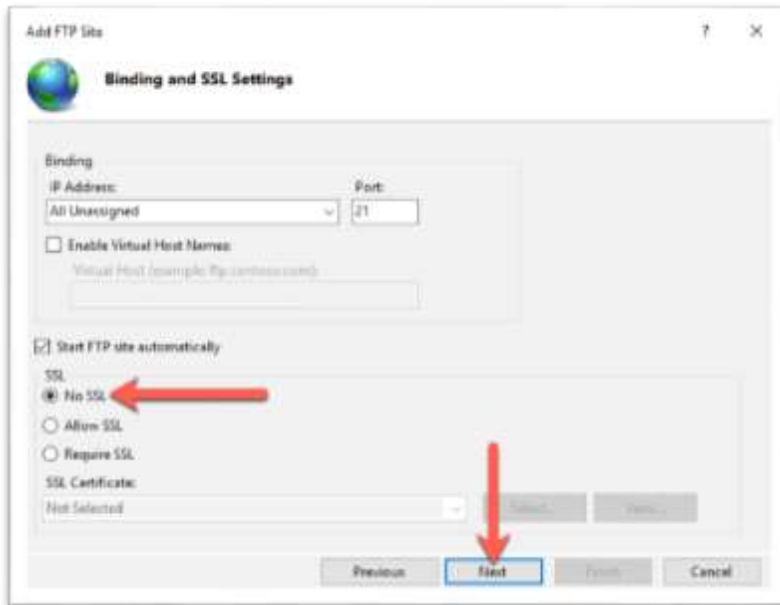
19. Enter a name for the firmware repository's root folder and click **OK** to continue.



20. Verify the settings are as desired and click **Next** to continue.



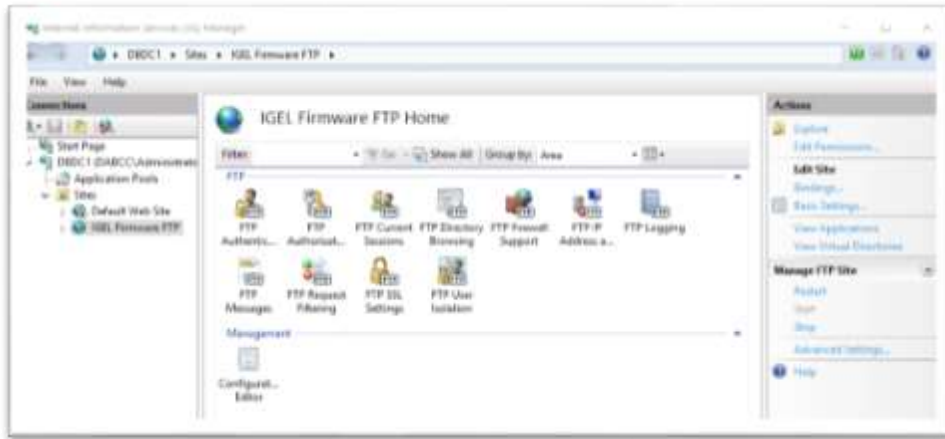
21. In this example, you are not deploying an SSL certificate and hence not using SFTP. Of course, you can do this if you desire. Click the **No SSL** radio button and click **Next** to continue.



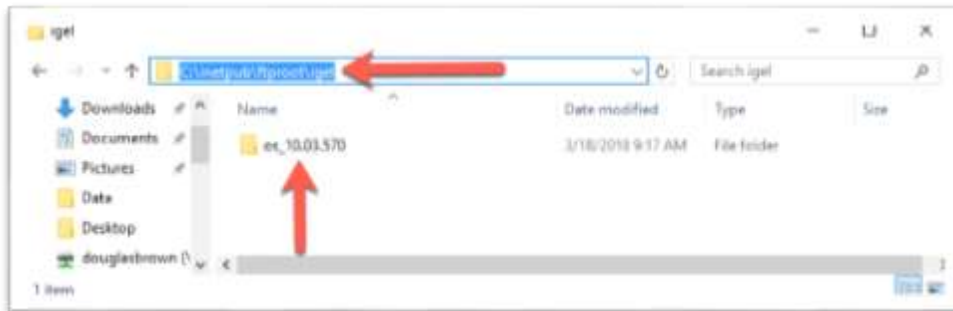
22. You are required to configure how the IGEL OS will authenticate with the FTP server to download the firmware updates. In this example, you will be using **Basic** authentication, and the permissions are set to **Read** only. You can either create a local windows user or, if your server is a domain member, you can use a Domain User account. In both cases, make sure this user account has the correct NTFS permissions on the FTP folders. Click **Finish** to continue.



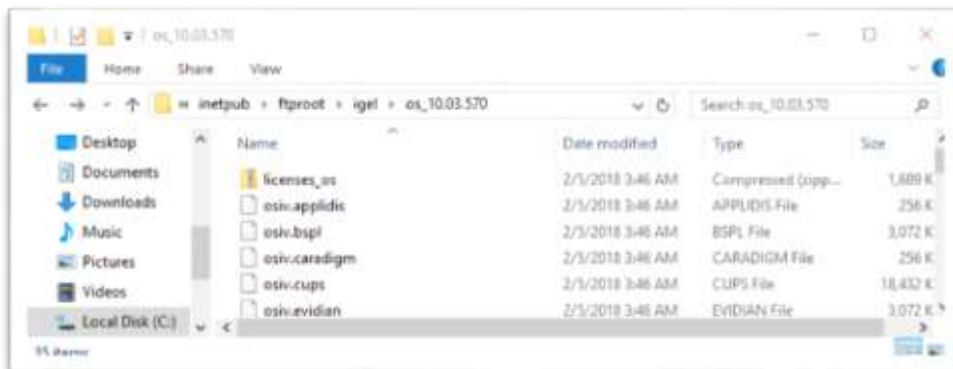
23. You are done configuring the Microsoft FTP server. You can test it by connecting to the FTP server with your favorite FTP client.



24. Now it is time to populate the FTP site with the desired firmware image files. Browse to the folder you defined in step 19 and create a new folder with a name corresponding to the desired firmware version you will be deploying. Repeat this step for every firmware version you would like to implement.



25. Open the newly created folder and copy and paste the extracted firmware image files to the folder.



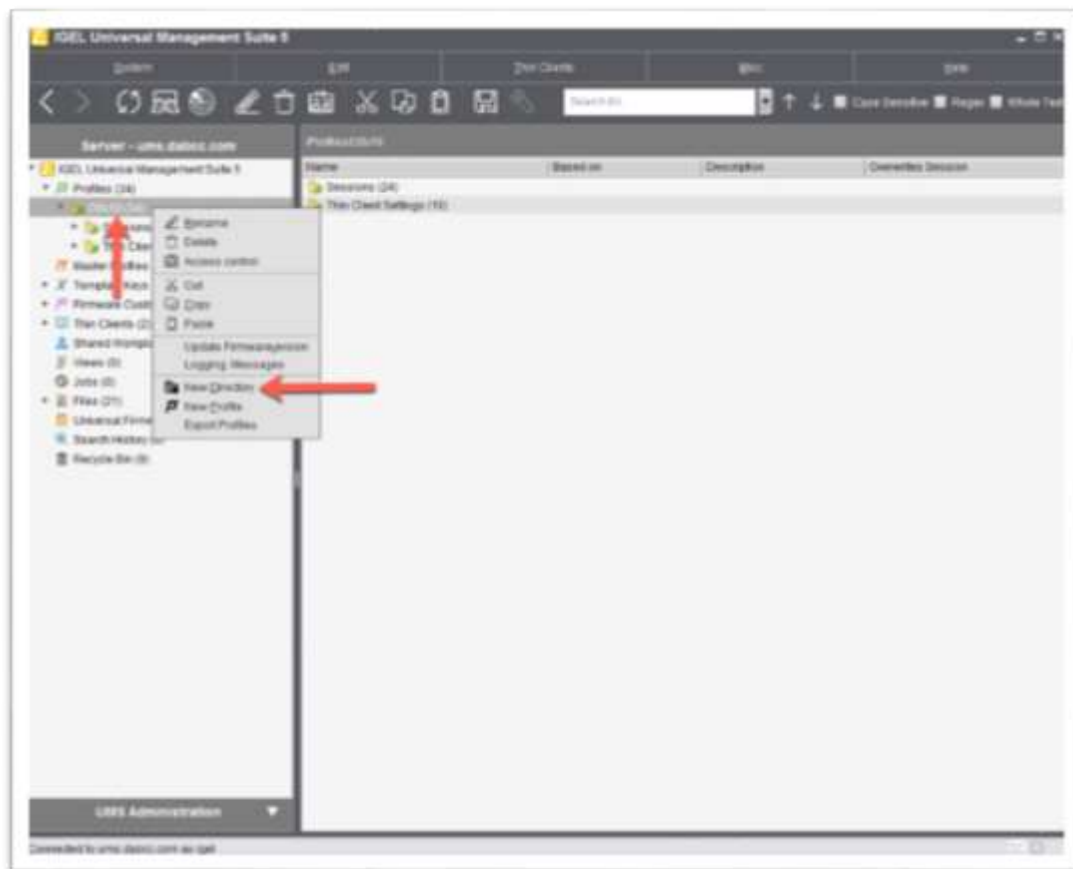
3. 3. 3 How to Create a Firmware Update Profile

Once you have created the firmware repository, you are ready to create a UMS update profile. This profile is used to configure the desired IGEL OS devices to use the newly created firmware repository settings.

The following details how to create a UMS update profile and assign it to the desired devices running the IGEL OS.

1. Login to the IGEL UMS and browse to the **Profiles** section. The first thing you will want to do is create a folder structure to house the different profiles you will be creating for each firmware version you wish to deploy.

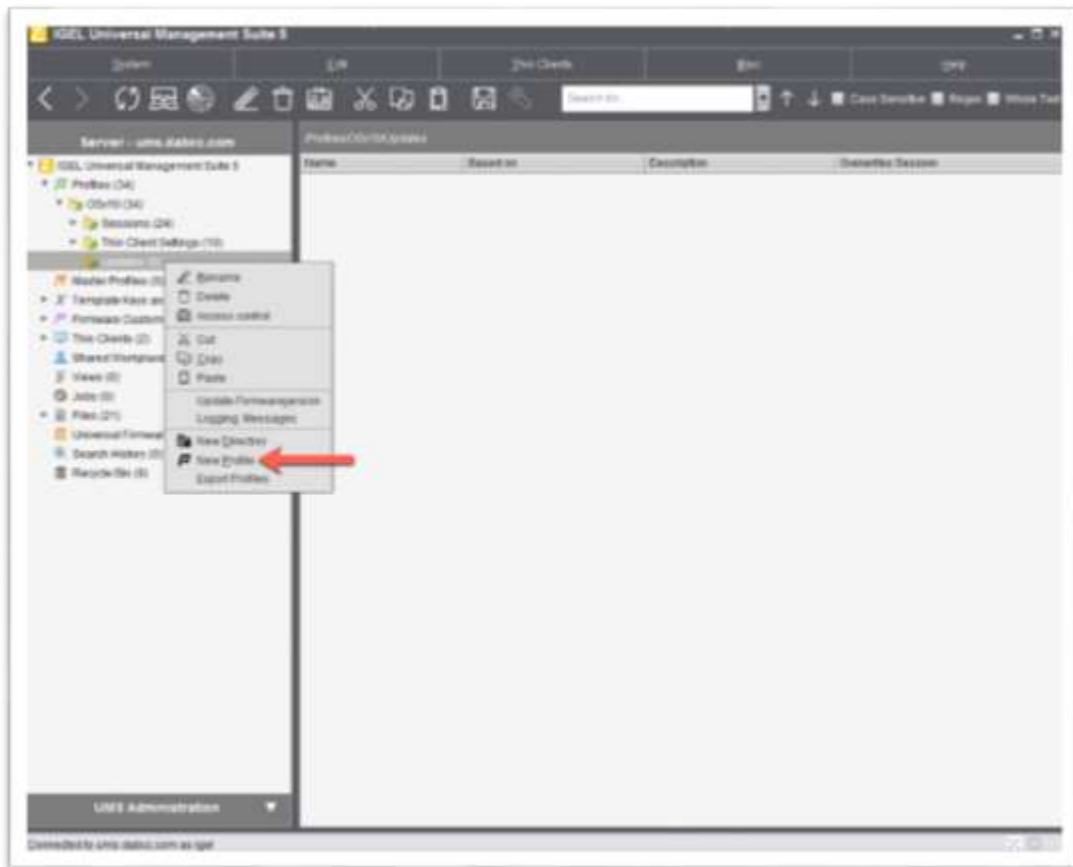
Right-click the root level folder that houses the profiles for the specific firmware family you are deploying and click the **New Directory** link.



2. Enter a name for the new directory that will house the update profiles. It is recommended to make this name descriptive. In the example below, we used the name **Updates**, though you are free to call it anything you like.



3. Right-click the newly created folder and click the **New Profile** link to start the process of creating an update profile.



4. You are required to create a specific profile for each IGEL OS firmware you wish to deploy. Enter a detailed name for the new profile in the **Profile Name** text box. As with all names, make it descriptive. In the example below, the profile is named after the firmware version being deployed. Click the **OK** button to continue.



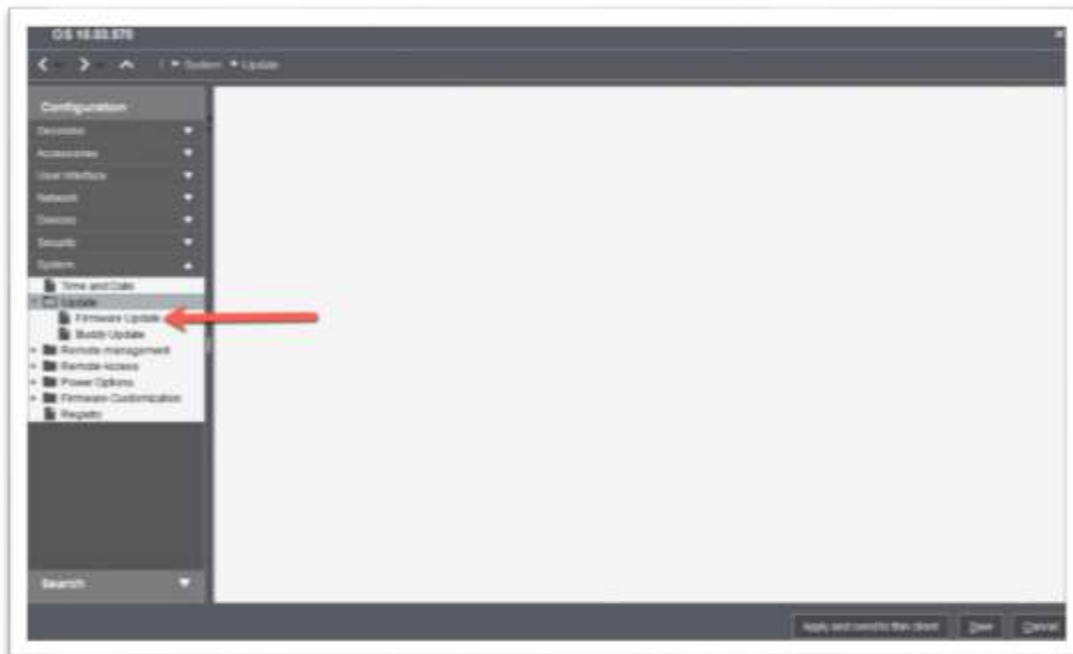
5. The profile window opens, click to expand the **System** menu item located in the left menu.



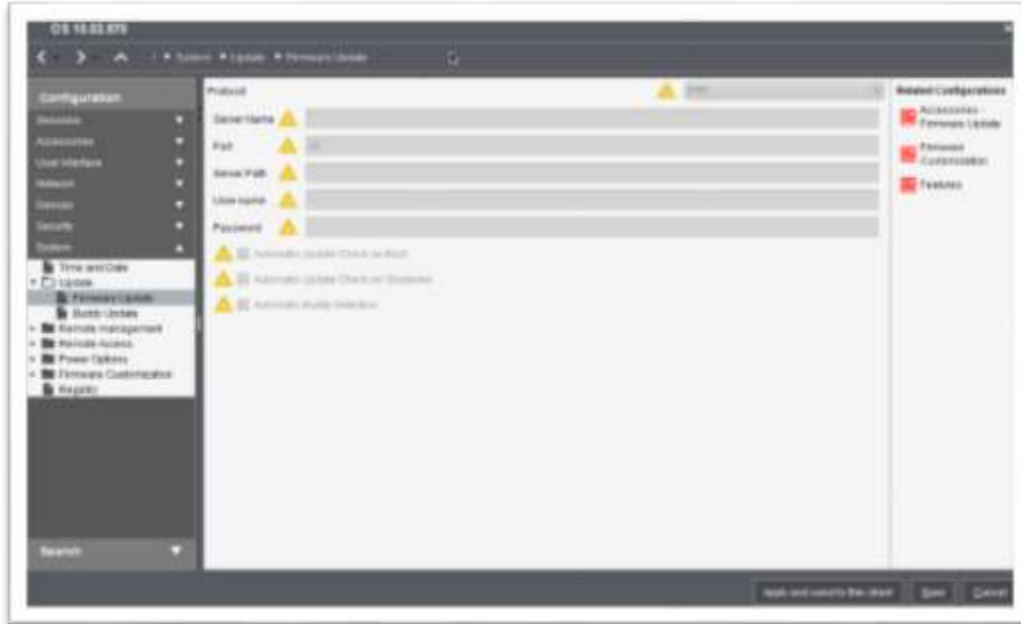
6. Click to expand the **Update** node.



7. Click the **Firmware Update** link to open the firmware update profile settings page.

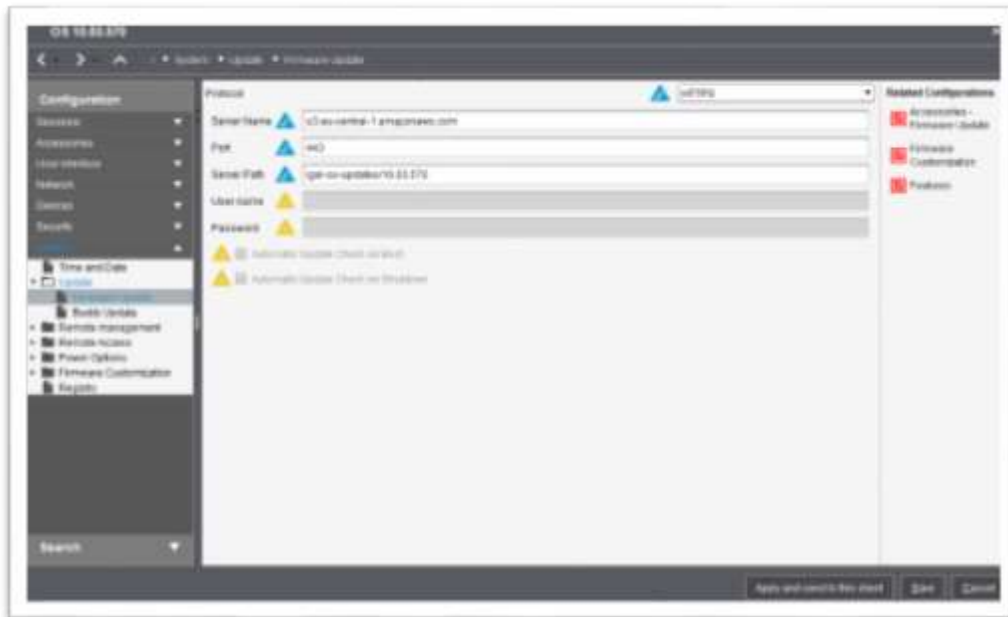


8. You are brought to the **Firmware Update Profile** properties page. This is where you will configure the IGEL OS where to download the firmware files. Depending on the firmware repository you choose to configure in the previous section will define what settings you will enter on this page.



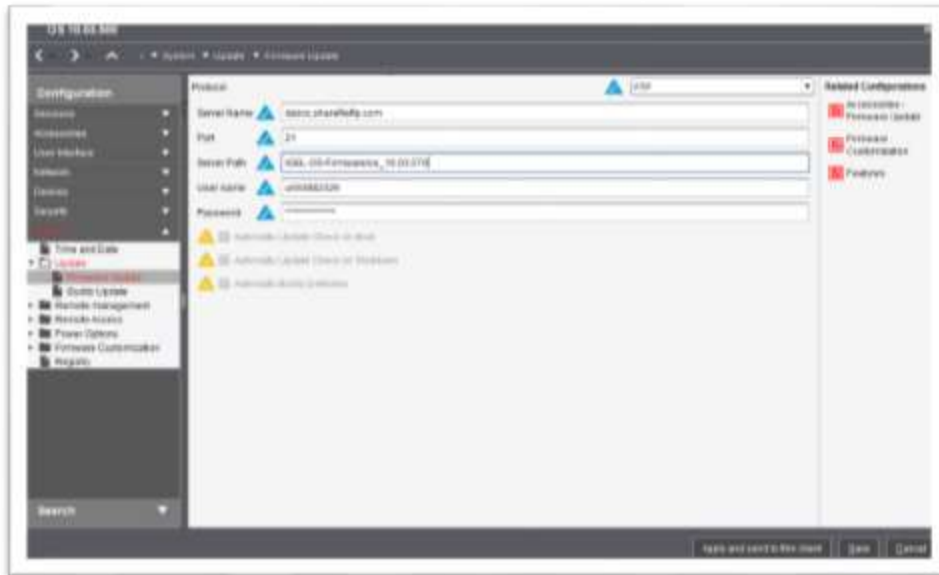
9. If you are using **AWS S3** as the firmware repository, as documented above, please refer to your notes for the specific server name, port, and server path. In the example above, it would look something like the screenshot below.

Enter your specific settings and click the **Save** button to save the new profile.



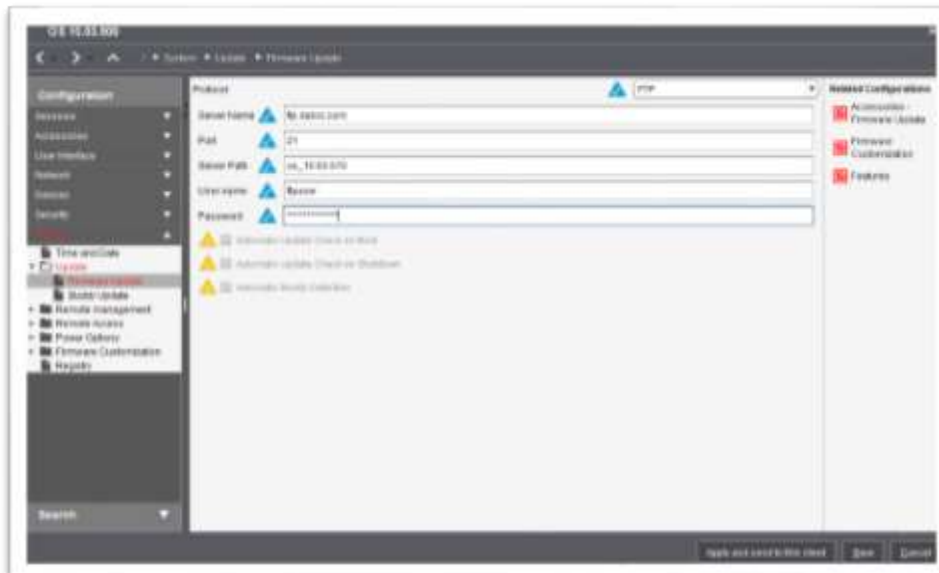
10. If you are using a **Citrix ShareFile** server as the firmware repository, as documented above, please refer to your notes for the specific server name, port, server path, username, and password. In the example above, it should look something like the screenshot below.

Enter your specific settings and click the **Save** button to save the new profile.



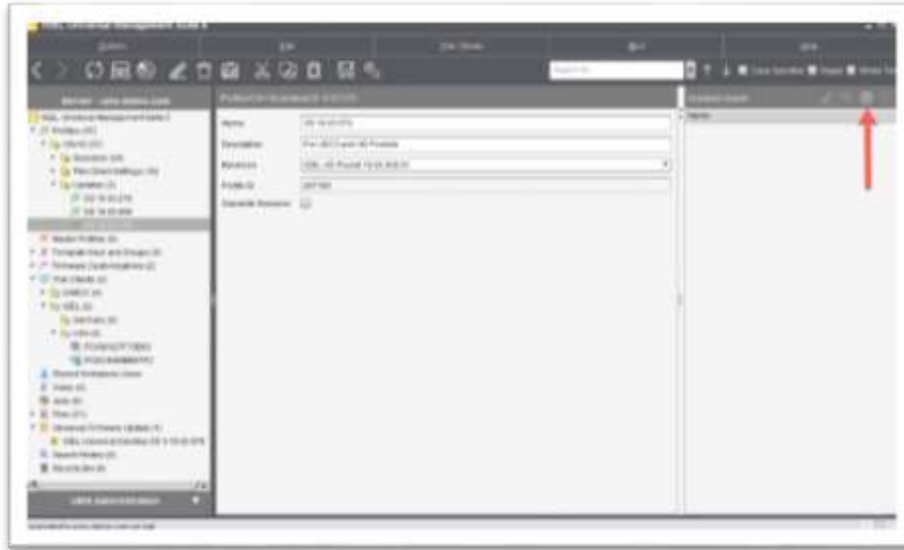
11. If you are using a **Microsoft IIS FTP** server as the firmware repository, as documented above, please refer to your notes for the specific server name, port, server path, username, and password. In the example above, it should look something like the screenshot below.

Enter your specific settings and click the **Save** button to save the new profile.



12. Now that you have created the firmware update profile you will need to assign it to the desired IGEL OS devices. This can be done in two ways, 1) you can drag and drop the newly created profile to a folder or device containing the IGEL OS devices you wish to assign the profile to, or 2) you can assign it using the **Assigned Objects** panel of the UMS.

For this example, let's assign the device using the **Assigned Objects** panel. Click the + icon located in the **Assigned Objects** section.



13. The Select assignable objects window opens, and you are presented with a tree of folders and devices to assign to the new update firmware profile. Do note that you are just assigning the firmware update settings and not triggering the update itself. In this case, it is not necessarily bad to assign the profile to all the desired devices at once. The update is relatively small and would not require a reboot.



14. Select the desired objects and click the > button to move them to the **Selected objects** pane. Repeat this step until you have assigned all the folders and devices you wish to the update firmware profile.

Click the **OK** button to when finished to assign the profile to the desired IGEL OS devices.



15. The **Update time** dialog box is opens prompting you to define when you would like the new settings to take effect. Select the desired setting and click **OK** to continue.



3. 4. How to Deploy a Firmware Update

Once you have successfully downloaded the IGEL OS firmware and configured the IGEL UMS to update the IGEL OS firmware you are required to deploy it. In simple terms, in this step, you tell the IGEL OS when to download and update the firmware. IGEL provides four different options to configure the deployment; locally, via the UMS, automatically on shutdown or startup and you can create a scheduled task to update at a specific date and time.

This section is broken down into the following three possible steps, only one is needed:

- [How to Manual Deploy from UMS](#)
- [How to Automate Updates on Shutdown](#)
- [How to Schedule Updates using Jobs & Views](#)

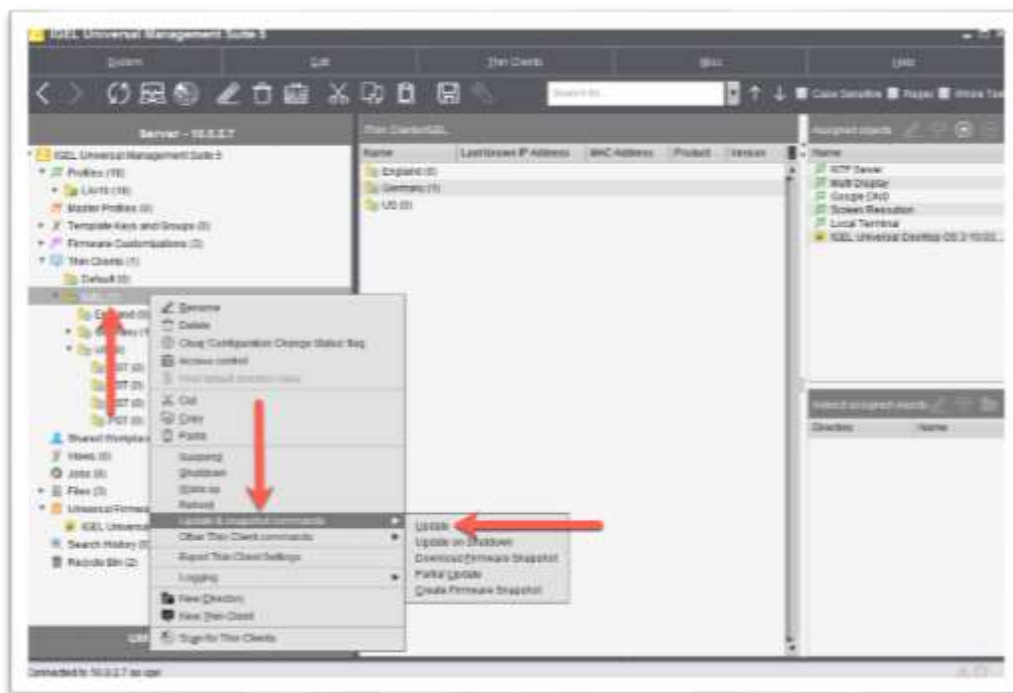
3. 4. 1 How to Manual Deploy from UMS

The following steps detail how to manually configure deployment of the IGEL OS firmware update via the UMS. This option triggers the update to occur right away, in real time.

1. To deploy the IGEL OS firmware update you will need to do that from the IGEL OS folders or the device itself.

In this example, let's trigger the update for all devices in a folder. Right-click on the desired folder and click the **Update & snapshot commands**.

Click the **Update** link to continue.



- The **Update Firmware of Thin Clients** window is opened listing the devices that will be updated. Confirm the list is correct and click the **Update** button to install the updates.



- The firmware update should have started, look at an affected device, you might notice message boxes showing the progress of the firmware update.

Once finished the device will reboot, and the new OS version will be ready to use!



3. 4. 2 How to Automate Updates on Shutdown

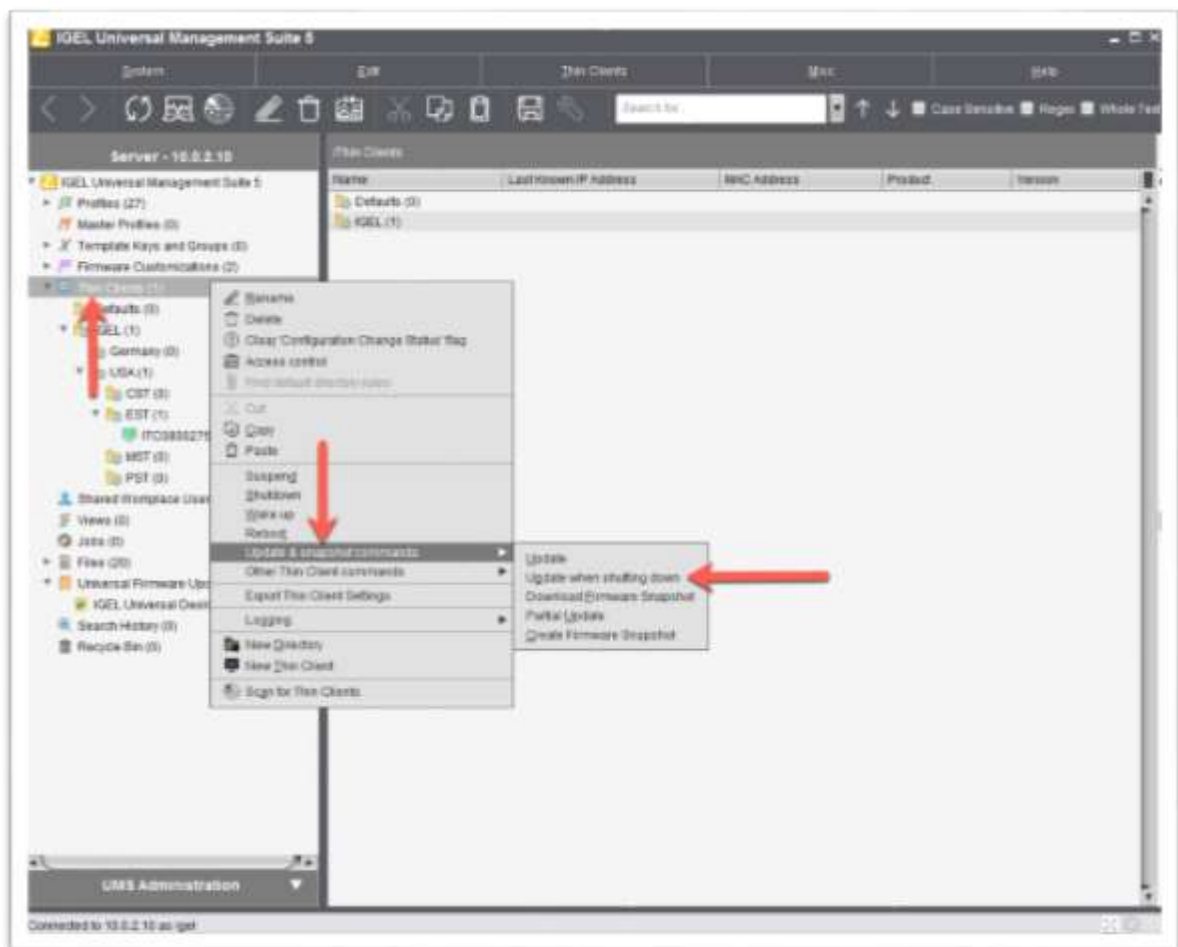
Although it is powerful to be able to deploy a new update on-demand, it might be in your best interest to deploy the update the next time the device is shutdown.

The following steps details how to manually configure deployment of the IGEL OS firmware update via the UMS the next time the desired devices are shut down.

1. To automate firmware updates the next time the IGEL OS is shutdown you need to do that from a folder containing IGEL OS device the desired device itself.

In this example, let's trigger the update for all devices in a folder. Right-click on the desired folder and click the **Update & snapshot commands**.

Click the **Update when shutting down** link to continue.



2. The **Update Firmware of Thin Clients on next shutdown** window opens listing the devices that will be updated. Confirm the list is correct and click the **Update when shutting down** button to install the updates.



It's that simple, the next time the configured IGEL OS devices are shut down, the desired firmware update will occur.

3. 4. 3 How to Schedule Updates using Jobs & Views

The IGEL UMS ships with a powerful feature for scheduling tasks called Jobs. With Jobs, you send reoccurring or one-time only commands to an IGEL OS device or a group of IGEL OS devices.

Currently, the UMS support sending the following commands via a Job:

- Update
- Shutdown
- Reboot.
- Suspend
- Update on boot
- Update on shutdown
- Wake up
- Settings TC->UMS
- Settings UMS->TC
- Download Flash Player
- Remove Flash Player
- Download Firmware Snapshot
- Partial Update
- Update desktop customization

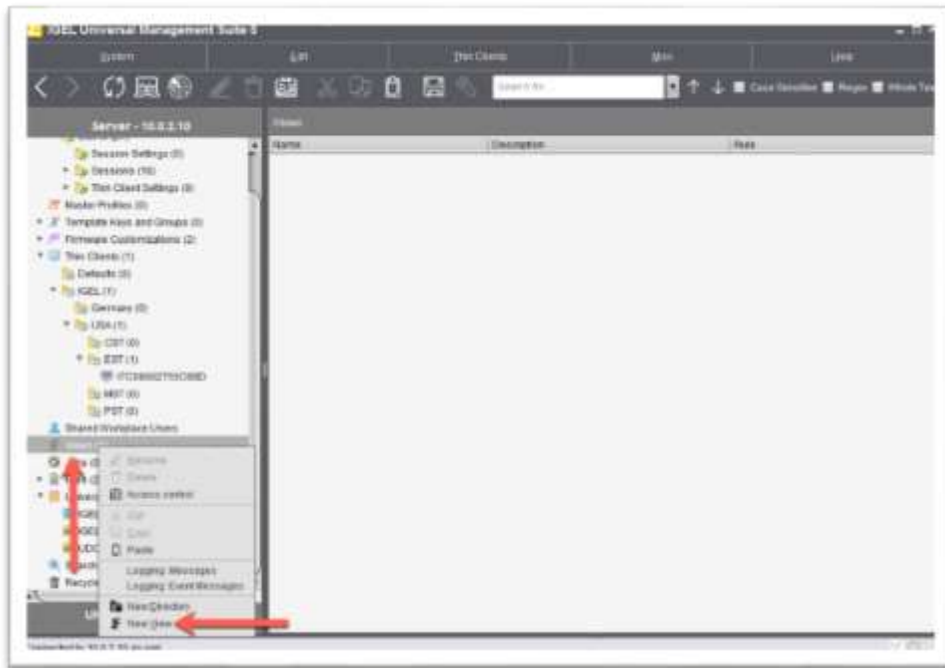
To learn more about the UMS Jobs feature, please refer to the following eDocs article:
<https://kb.igel.com/endpointmgmt/en/jobs-910606.html>.

The UMS also ships with a feature called, Views that perfectly compliment the Jobs feature. A View allows administrators to define a list of devices based on many different criteria, For example, listing all the devices that are older than a certain firmware version. Once a View is created, you can assign it to a Scheduled Job.

To learn more about the UMS Views feature, please refer to the following eDocs article:
<https://kb.igel.com/endpointmgmt/en/views-910591.html>.

The following steps detail how to schedule a firmware update using the UMS Jobs and Views features:

1. If you would like to use a View to define a list of devices based on criteria more than just a group of devices or specific devices, then a View is for you. To create a View right-click on the **Views** node in the left menu and click the **New View** link.

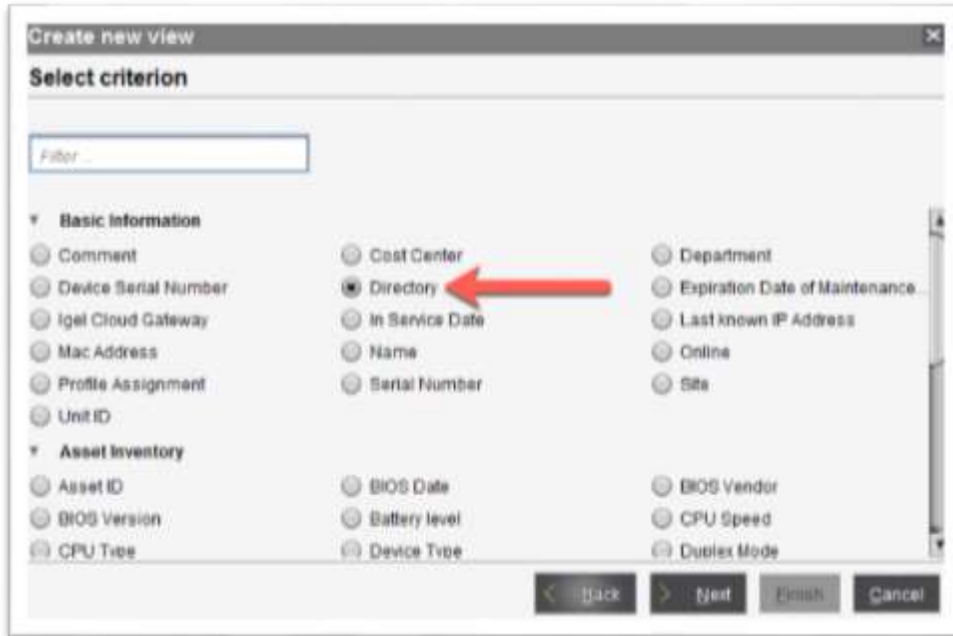


2. Enter a descriptive name in the **Name** text box and click **Next** to continue.

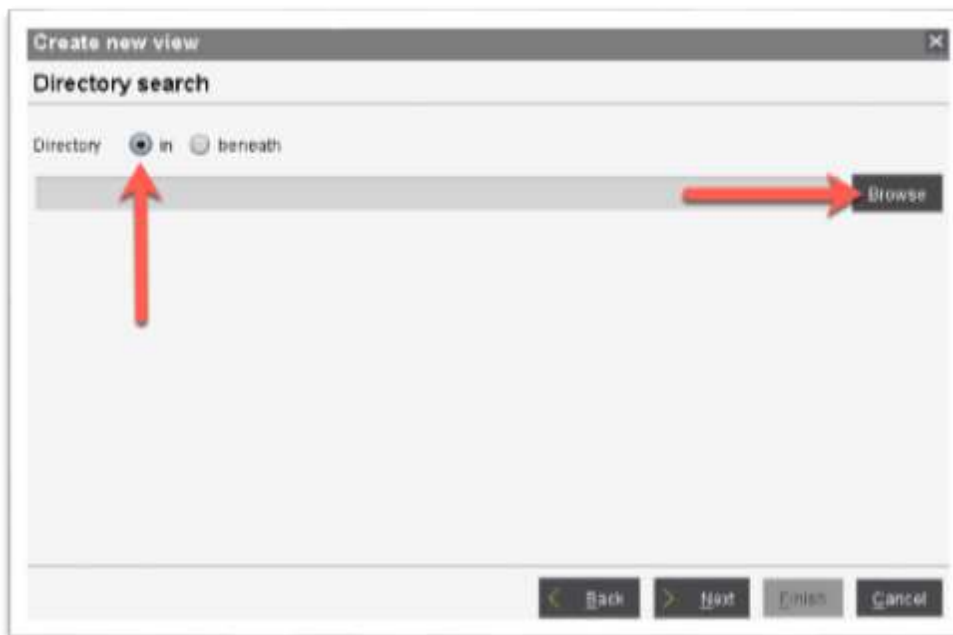


3. You are prompted to select the criteria you would like to use to make the list of devices. As you can see, there are many options to choose from. You can even filter the list by using the **Filter** text box.

For this example, click the **Directory** radio button and then click **Next** to continue.



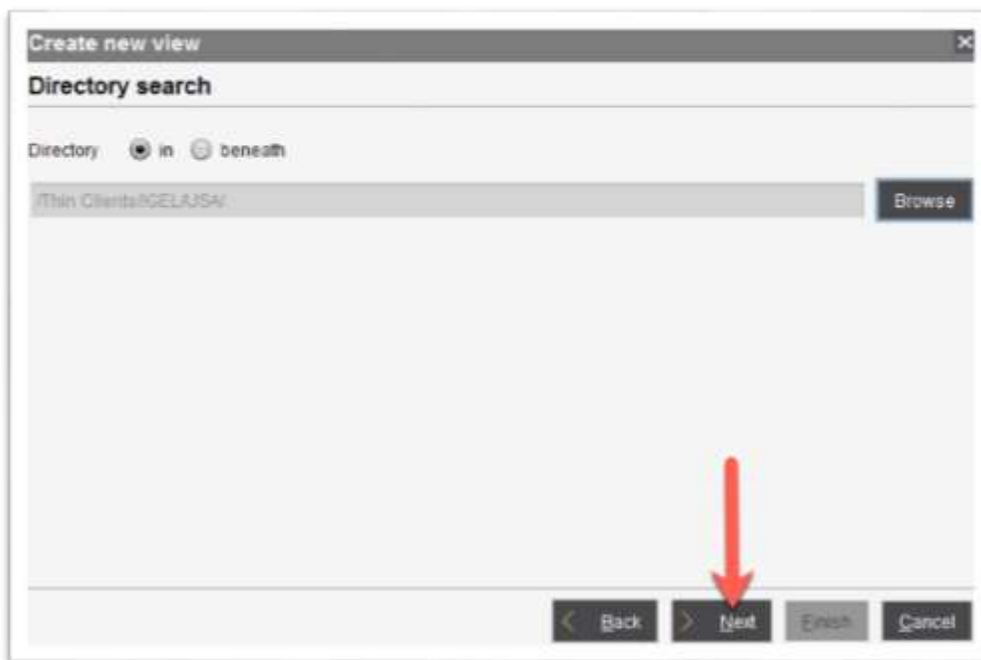
4. The **Directory Search** page allows you to define which Thin client folder you wish to narrow your search within. Click the **in** radio button and then click **Browse**.



5. Select the Thin client directory you wish to use and click the **OK** button to continue.



6. You are brought back to the **Create new view** page, click **Next** to continue.



7. You are asked if you would like to continue building your view or create additional search criteria.

For our example, click the **Narrow search criterion (AND)** radio button and then click **Next** to continue.

Create new view

Finish view creation

Name: Define_my_concerned_Endpoints_for_update

Description:

View criteria

is in the directory with ID 81

☐ Create view
☒ **Narrow search criterion (AND)**
☐ Create additional search criterion (OR)

8. The next screen allows you to define the criteria the narrow your search. In the example below, we have used the Filter function to narrow the results to the item related to firmware. Click to check the **Firmware Version** radio button and then click **Next** to continue.

Create new view

Select criterion

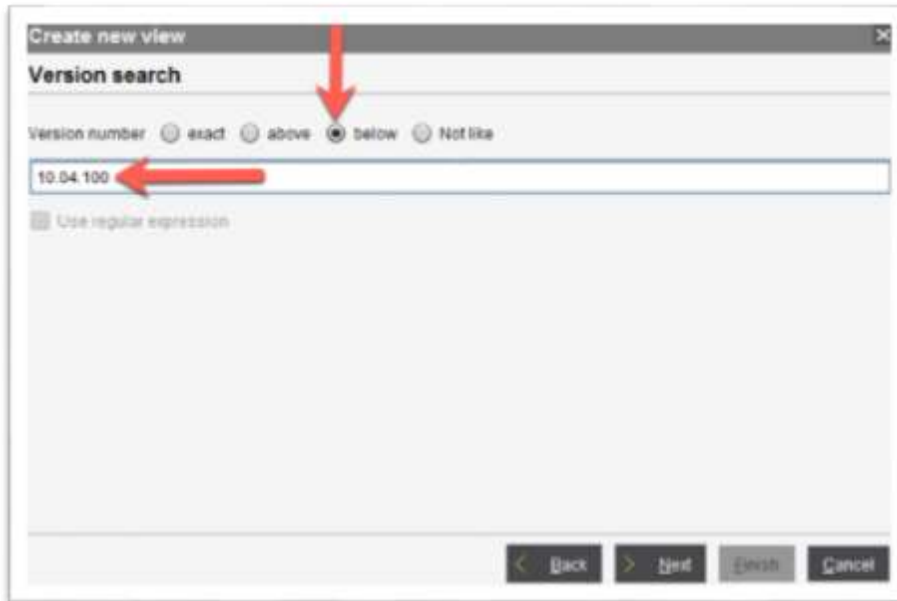
firmware

☒ **Firmware Version**
☐ Firmware Description
☐ Firmware Update (Relative)

9. You are prompted to enter the version number you wish to build the list upon. You can define if the list contains all devices with the same version or the devices above/below or not like at all.

For this example, click the **below** radio button to build the list of all devices that are below the stated version number.

Enter the desired version number in the text box and click **Next** to continue.



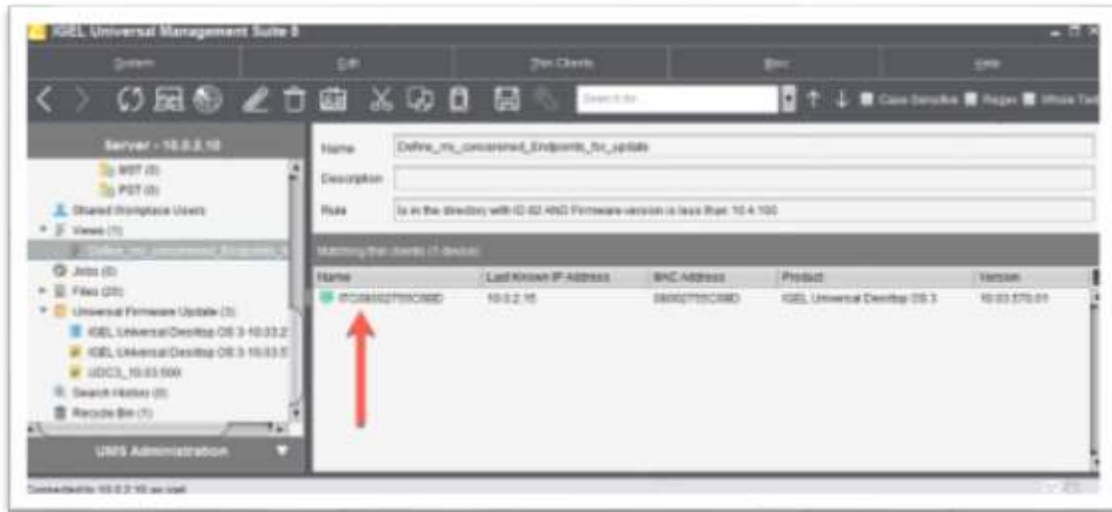
The screenshot shows the 'Create new view' dialog box with the 'Version search' tab selected. The 'Version number' field is set to '10.04.100'. The 'below' radio button is selected, and the 'exact', 'above', and 'Not like' buttons are unselected. The 'Use regular expression' checkbox is unchecked. The 'Next' button is highlighted with a red arrow.

10. You are prompted if you would like to continue building your view or create additional search criteria. Though, you are done! Click the **Finish** button to have the UMS build the View.

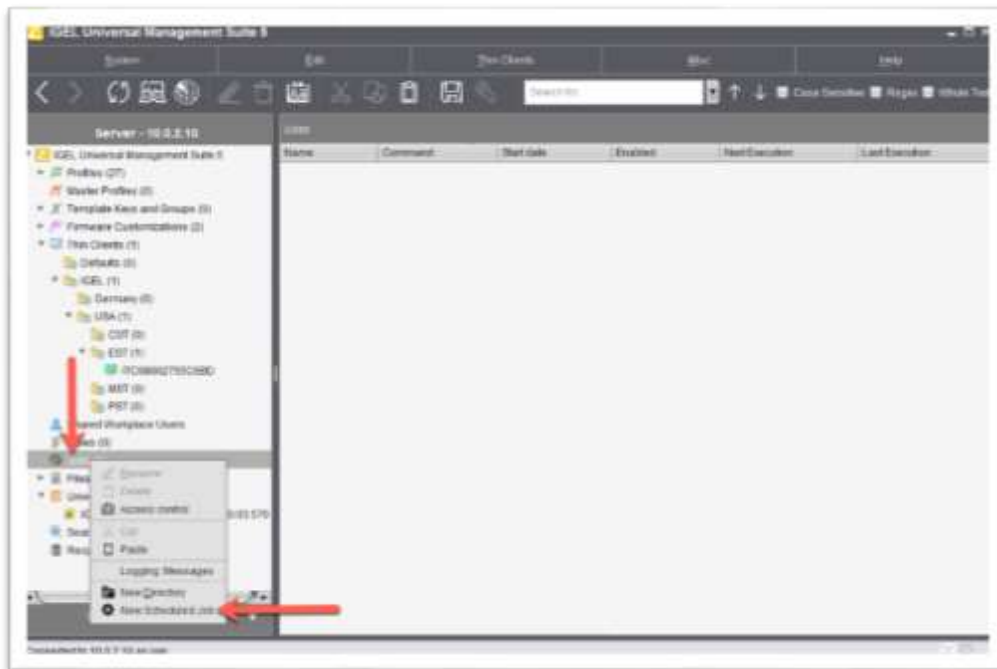


The screenshot shows the 'Create new view' dialog box with the 'Finish view creation' tab selected. The 'Name' field is 'Default_my_recommended_Endpoints_for_update'. The 'Description' field is empty. The 'View criteria' field contains the text 'Is in the directory with ID 81 AND Firmware version is less than 10.4.100'. The 'Create view' radio button is selected, and the 'Narrow search criterion (AND)' and 'Create additional search criterion (OR)' buttons are unselected. The 'Finish' button is highlighted with a red arrow.

11. You are brought back to the UMS, and your View is listed containing the client devices found. You are ready to create the Job and schedule the firmware update.



12. To trigger the IGEL OS firmware update via a UMS Job, right-click on the **Jobs** entry in the UMS' left menu and click the **New Scheduled Job** link.



13. Enter a friendly name for the new job in the **Name** text box.

New Scheduled Job

Details

Name: Update IGEL OS

Command: [Empty]

Execution time: 10:18 Start date: 2018-03-19 [Enabled]

Comment: [Empty]

Options

☒ Log results ☐ Retry next boot

Max. Threads: 98 Delay: 0 Seconds

Timeout: 30

Job Info

Job ID: [Empty]

Next Execution: [Empty]

User: [Empty]

[Back] [Next] [Finish] [Cancel]

14. Click the **Command** combo box to reveal the list of possible commands you can schedule. In this list, you will find the ability to **Update on Boot** and **Update when shutting down**.

Select the desired command.

New Scheduled Job

Details

Name: Update IGEL OS

Command: [Dropdown Menu Open]

Execution time: [Empty] Start date: 2018-03-19 [Enabled]

Comment: [Empty]

Options

☒ Log results ☐ Retry next boot

Max. Threads: [Empty] Delay: [Empty] Seconds

Timeout: 30

Job Info

Job ID: [Empty]

Next Execution: [Empty]

User: [Empty]

[Back] [Next] [Finish] [Cancel]

15. Next, configure the time you wish the command to execute in the **Execution time** text box and then select the day in the **Start date** text box. When finished, click the **Next** button to continue.

The screenshot shows the 'New Scheduled Job' dialog box with the 'Details' tab selected. The 'Name' field contains 'Update IGEL OS'. The 'Command' dropdown is set to 'Update on Boot'. The 'Execution time' is set to 18:00 and the 'Start date' is 2018-03-21. The 'Enabled' checkbox is checked. The 'Comment' field is empty. The 'Options' section includes 'Log results' (checked), 'Max. Threads' (99), 'Delay' (0 seconds), and 'Timeout' (30). The 'Job info' section shows 'Job ID' (empty), 'Next Execution' (Mar 21, 2018 6:00 PM), and 'User' (empty). At the bottom, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'. Red arrows point to the 'Execution time' and 'Start date' fields, and another red arrow points to the 'Next' button.

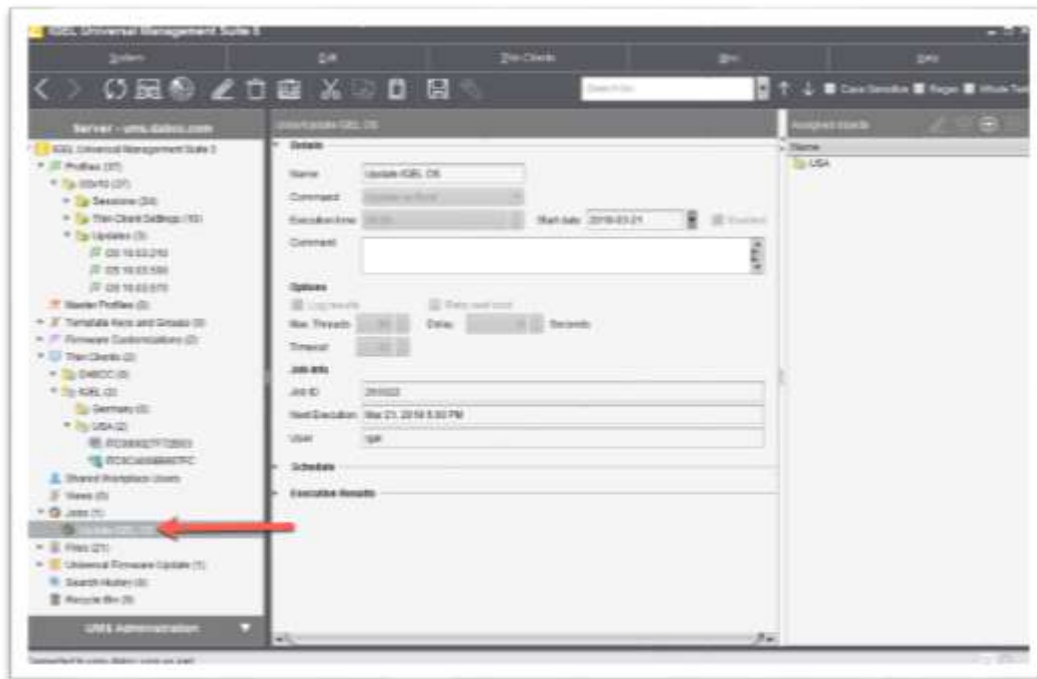
16. The next screen prompts you to define the specifics on when you would like the Job to execute. Familiarize yourself with the settings, though in our use-case all you need to do is click the **Next** button to continue.

The screenshot shows the 'New Scheduled Job' dialog box with the 'Schedule' tab selected. The 'Execution time' is 18:00 and the 'Start date' is 2018-03-21. The 'Expiration date' is empty. The 'Repeat Job' section shows 'Never' selected. Below it, there are options for 'Every' day, week, month, or year, and a list of days of the week. The 'Exclude Public Holidays' checkbox is checked. There is a table with columns 'Date' and 'Comment'. At the bottom, there are buttons for 'Back', 'Next', 'Finish', and 'Cancel'. A red arrow points to the 'Next' button.

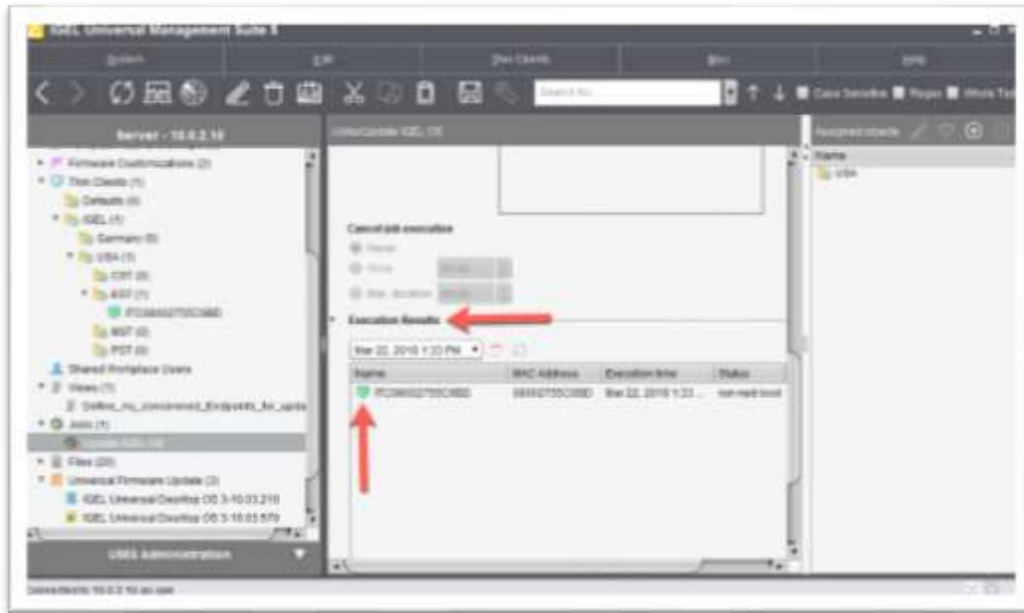
17. You are prompted to assign the desired IGEL OS devices you wish to add to the new Job. Click to select a folder, device, or View and click the top arrow button to move it to the **Selected objects** folder. Repeat this step to assign all the desired folders and devices and click the **Finish** button to create the new Job.



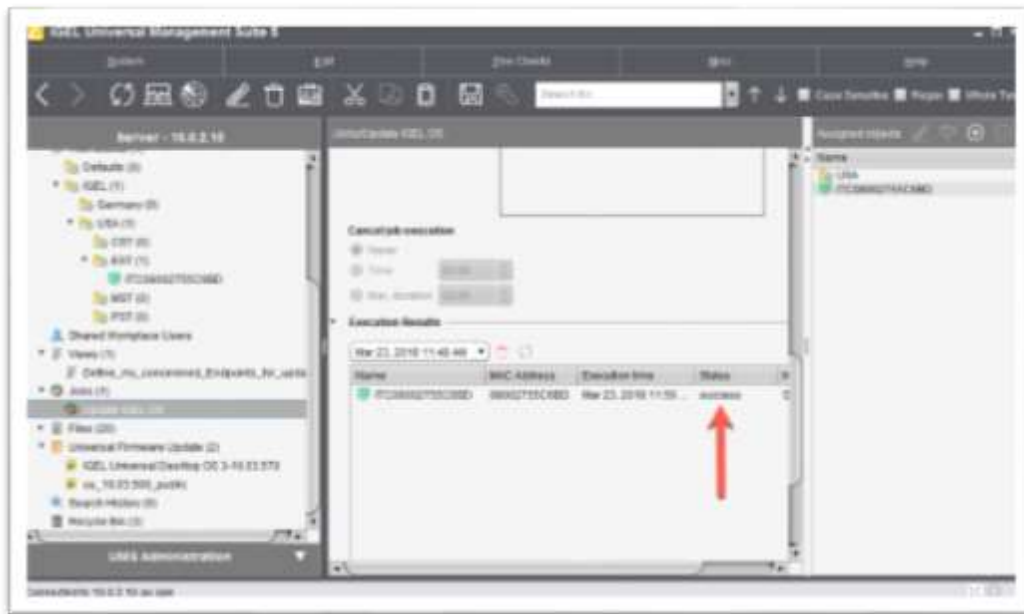
18. If all goes as planned, the Job is created, and you are presented with the Job's properties page.



19. You can view the Jobs status by scrolling down to the **Execution Results** section of the page. You are presented with a list of the devices in the Job along with the status. For example, the device in our example will run the firmware update the next time the device boots.

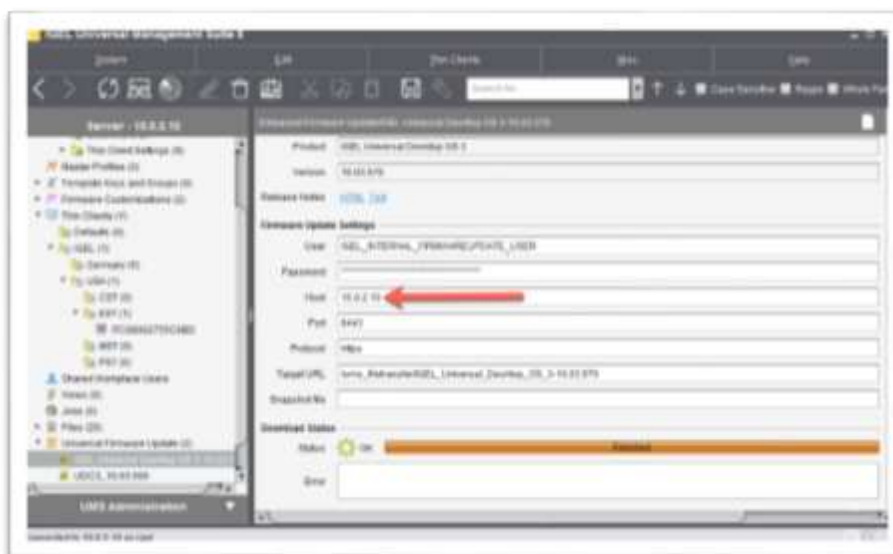


20. In the example below, you see the device was rebooted, and the firmware update was a success!

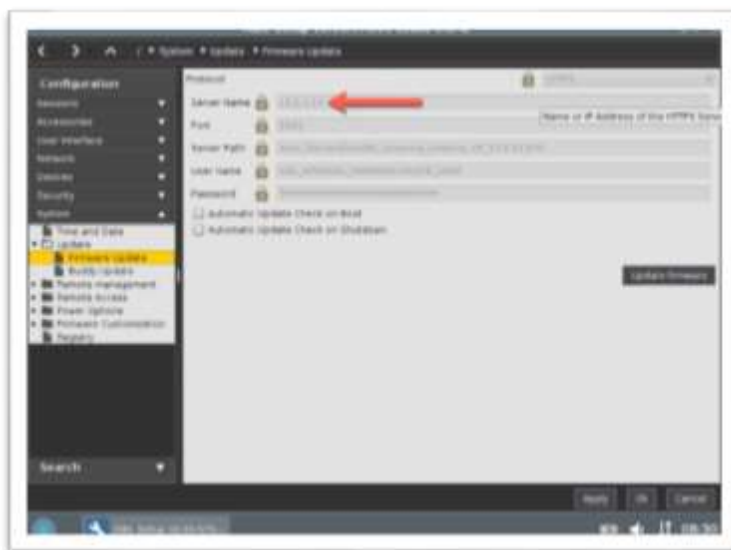


21. If you are not so lucky and the update fails, it is possible the device was not able to connect and download the firmware files. In this case, you will want to verify the host IP address is stated correctly in the Host text box of the desired firmware update.

The screenshot below works for when deploying updates via the UMS Universal firmware update feature.



22. You can also view these settings from the IGEL OS by clicking **Start > System icon > Setup**. Then click to expand the **System** node > click **Update** and then click the **Firmware Update** link to expose the firmware update settings that have been assigned to the local device. Verify the IP address is the address of the firmware repository and if not then verify you followed the above steps properly.



3. 5. How to Update Existing Profiles

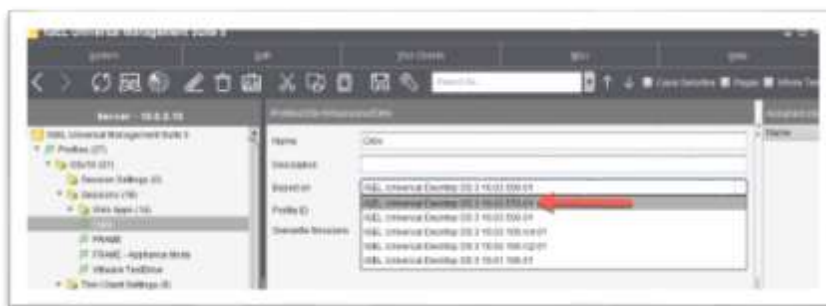
New versions of the IGEL OS might add new features and/or updates to installed applications, such as the Citrix Receiver. It is important to understand UMS profiles are specific to the firmware version they were based on, usually the latest version deployed at the time the profile was created. Thus, after you deploy firmware updates, it's recommended to go through your profiles and update the desired profiles to the latest version. Of course, this is only required if a new feature was added to the configuration you are deploying. For example, upgrading the Citrix Receiver to the latest version.

The following steps details how to update a profile to utilize the latest firmware configurations:

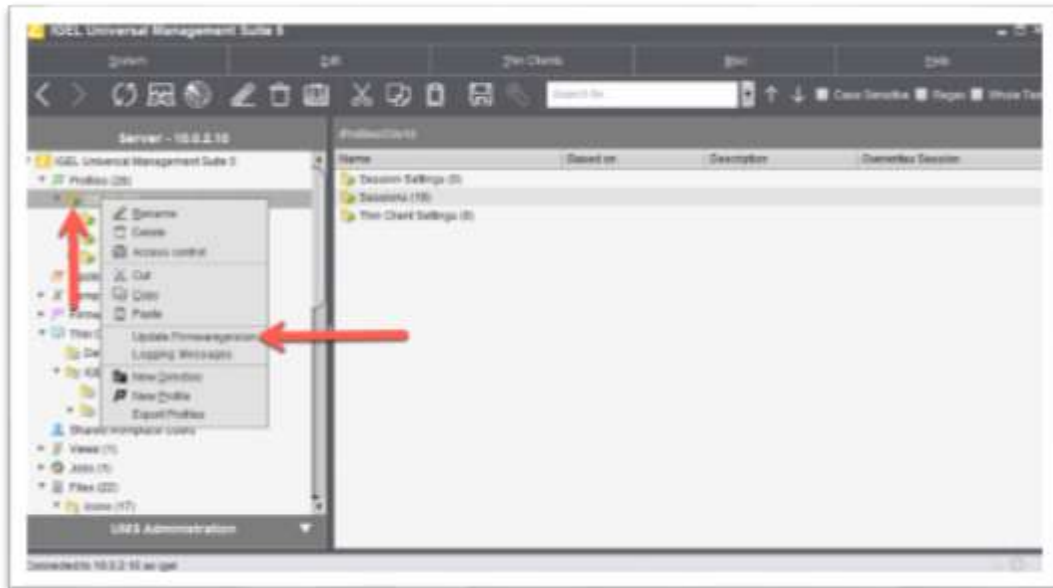
1. Browse to the desired profile and click it. You will be shown the profiles Name, Description, and Based on settings. The **Based on** combo box is the setting you need to click to upgrade to the desired firmware version.



2. Click the **Based on** combo box to expose the list of firmware versions available to assign to the profile. Select the desired version. Repeat this step for the profiles that have a new feature you wish your deployed devices to take advantage of.



3. If you have many profiles and wish you update them all to the latest firmware version at the same time, then you can use do this too. Right-click on the folder, be it the root or a subfolder and click the **Update Firmwareversion** link in the context menu.



4. The **Update profile to new firmware version** window opens allowing you to select the desired firmware version. Once selected, click the **OK** button to update all profiles at once.



5. If all goes as planned, you will be presented with the following popup telling you the update was successful! Click **OK** to continue.



For more information on how to update an existing profile and change the Citrix Receiver version, in case a new version was released, please refer to the following blog article <https://masterxen.wordpress.com/2018/03/21/post-igel-firmware-missing-new-citrix-receiver-version/>

Appendix

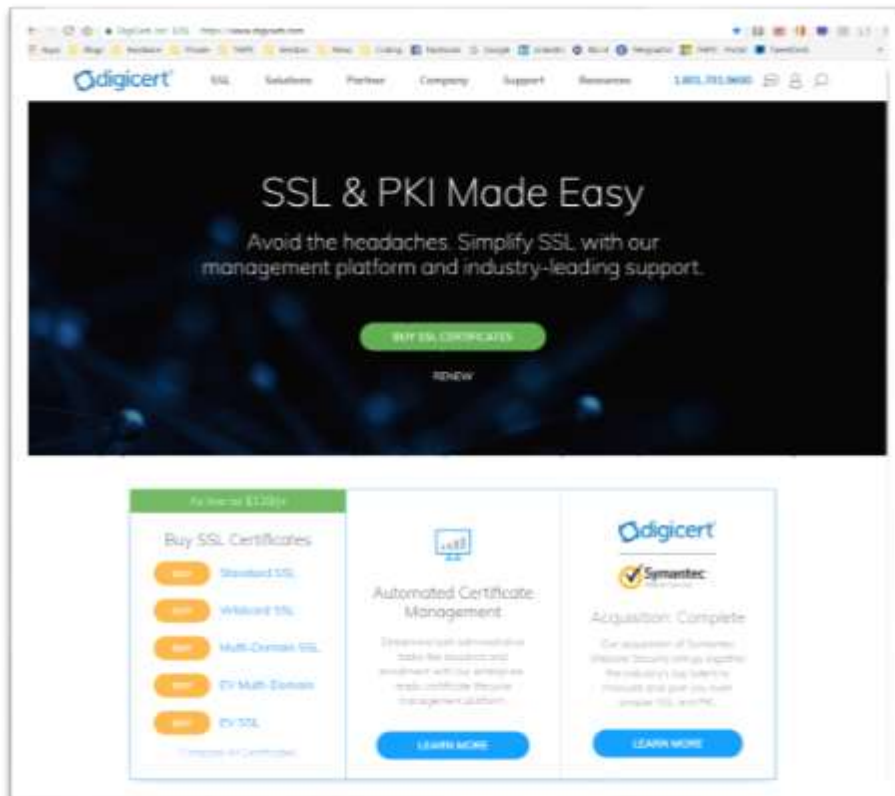
- Fill out the correct information, most important is the “Common Name,” to the actual FQDN name which is bound to the SSL Certificate.

You have two files, an SSL key file, and an SSL CSR file

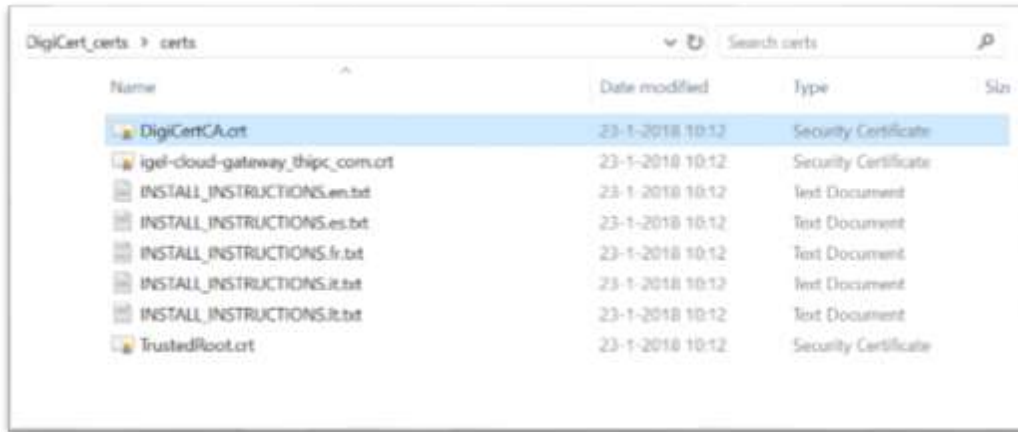


- Use a tool like WinSCP to download the **igel-cloud-gateway.thipc.com.key** from your ICG appliance and copy it over to your UMS server. This file is needed to complete the SSL Certificate configuration

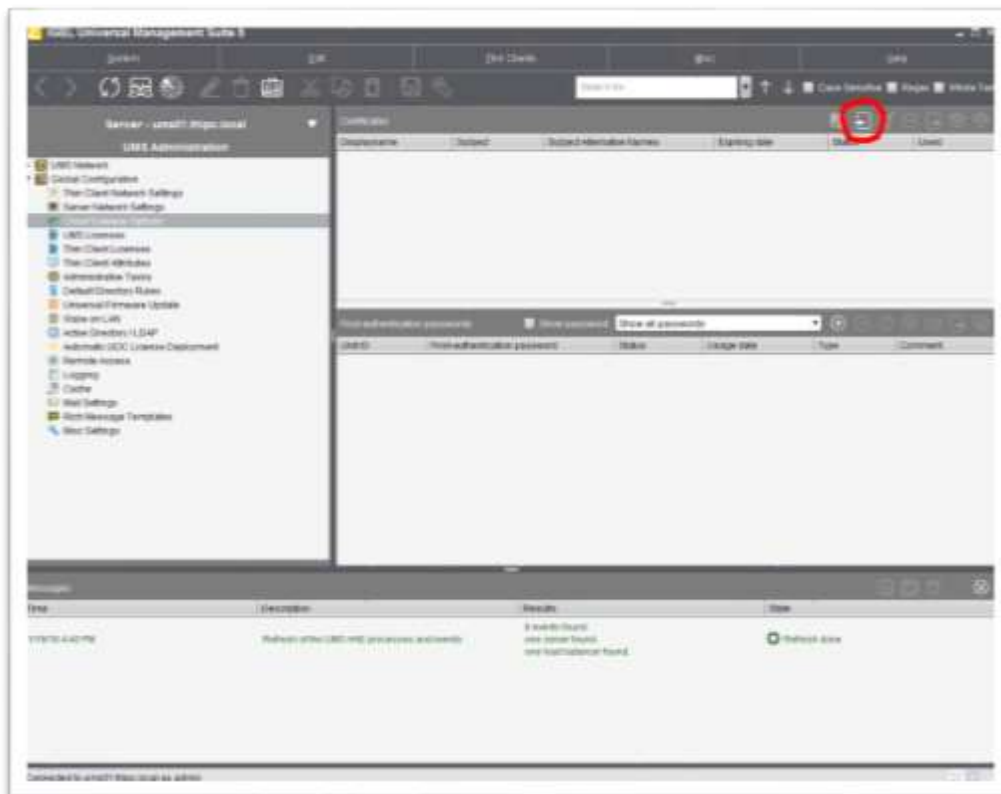
Use the CSR file to create your certificate on the [DigiCertificate website](#).



5. When you receive your SSL Certificate from DigiCert, a zip file is attached, which contains your Certificate, the root CA and intermediate certificate. Copy these files to your UMS server.



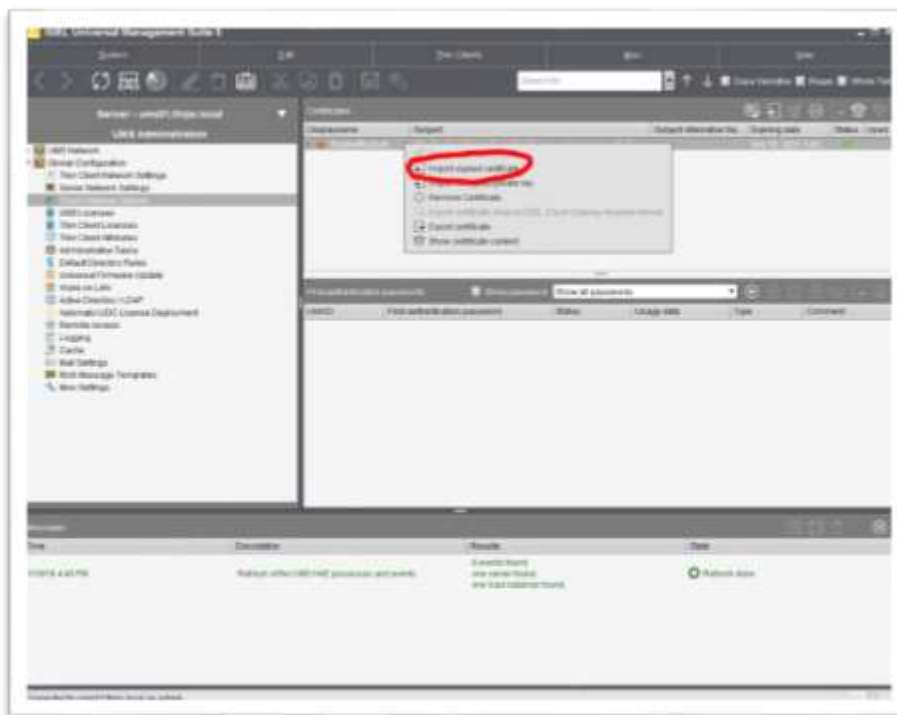
6. Go to the UMS management console, and click **Cloud Gateway Options**, choose **import root certificate**.



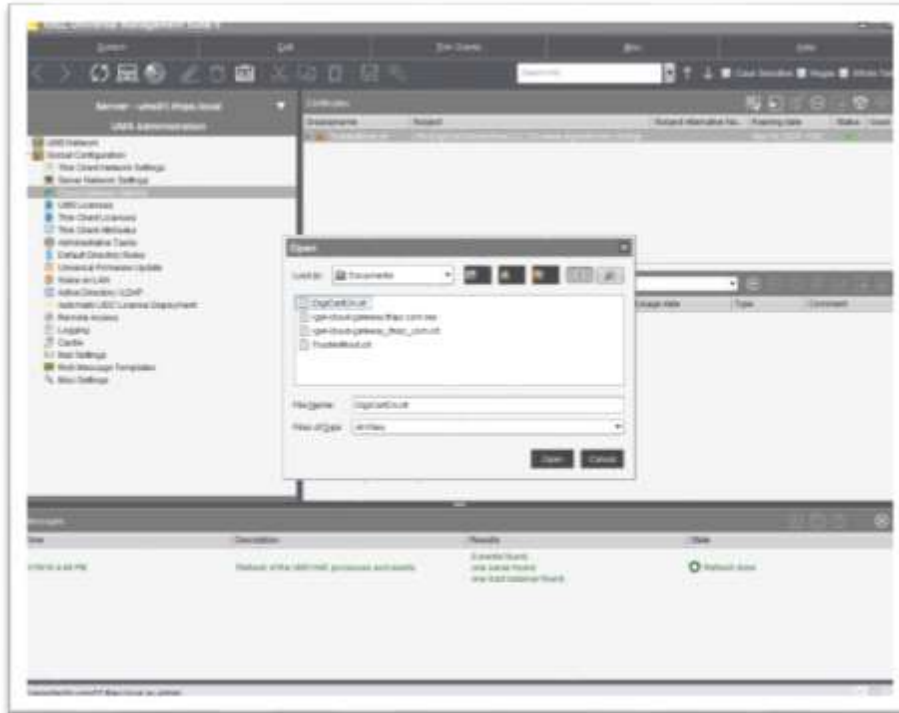
7. First import the DigiCertificate Root CA, which is **TrustedRoot.crt**



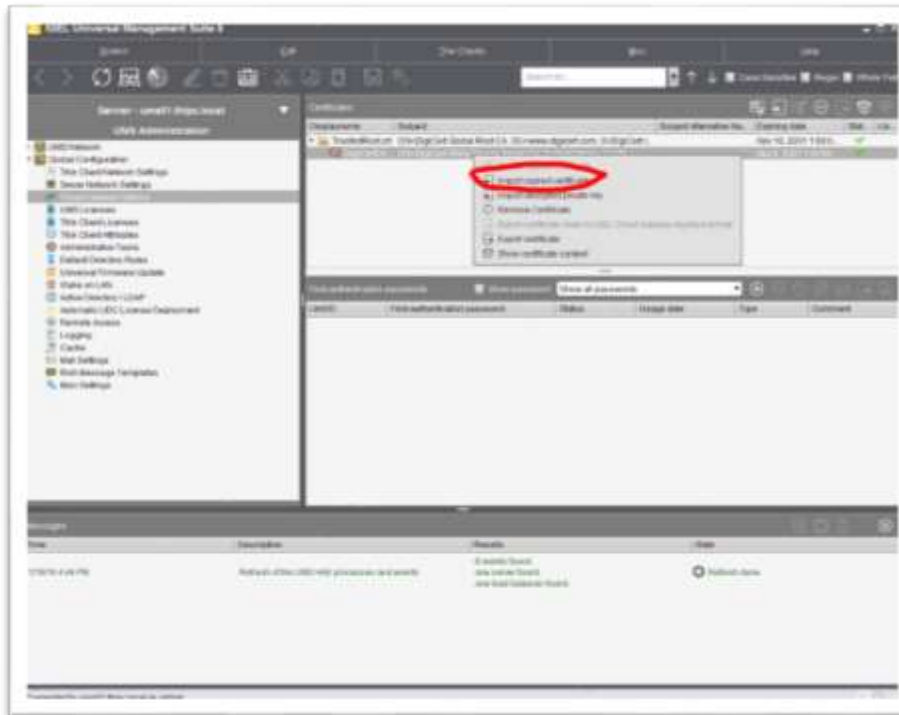
8. Right-click the imported certificate and choose **import signed certificate**.



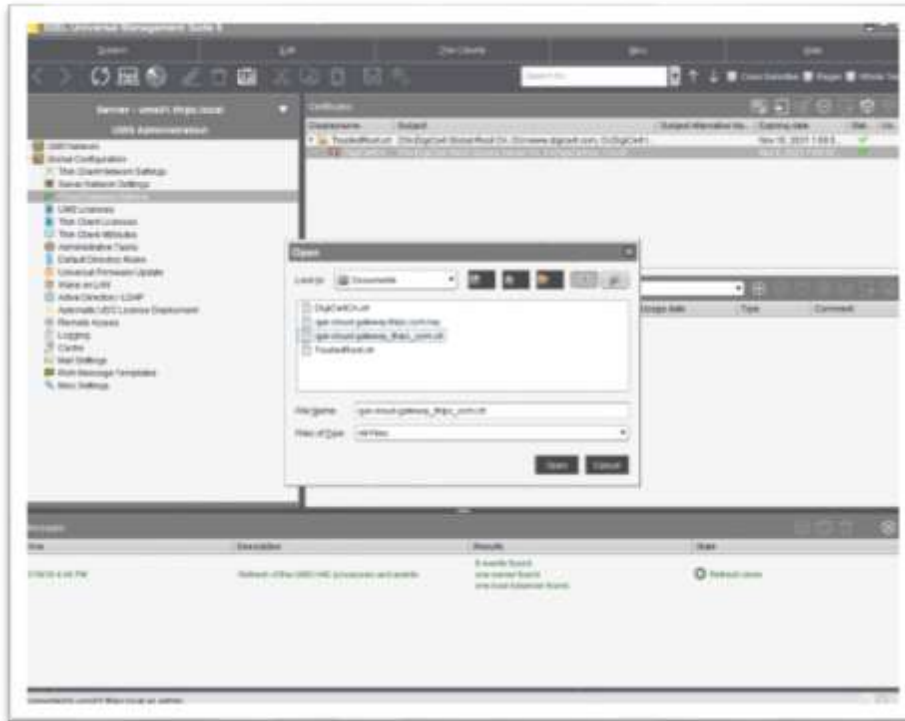
9. Choose the intermediate certificate which is **DigiCertCA.crt**



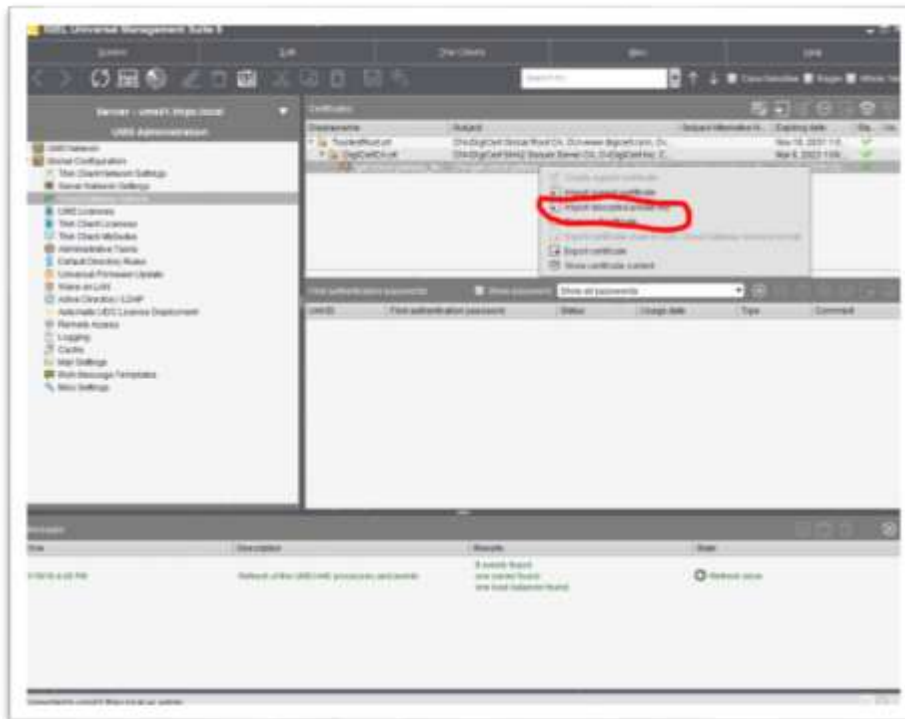
10. Right-click the certificate you just imported and choose **import signed certificate**.



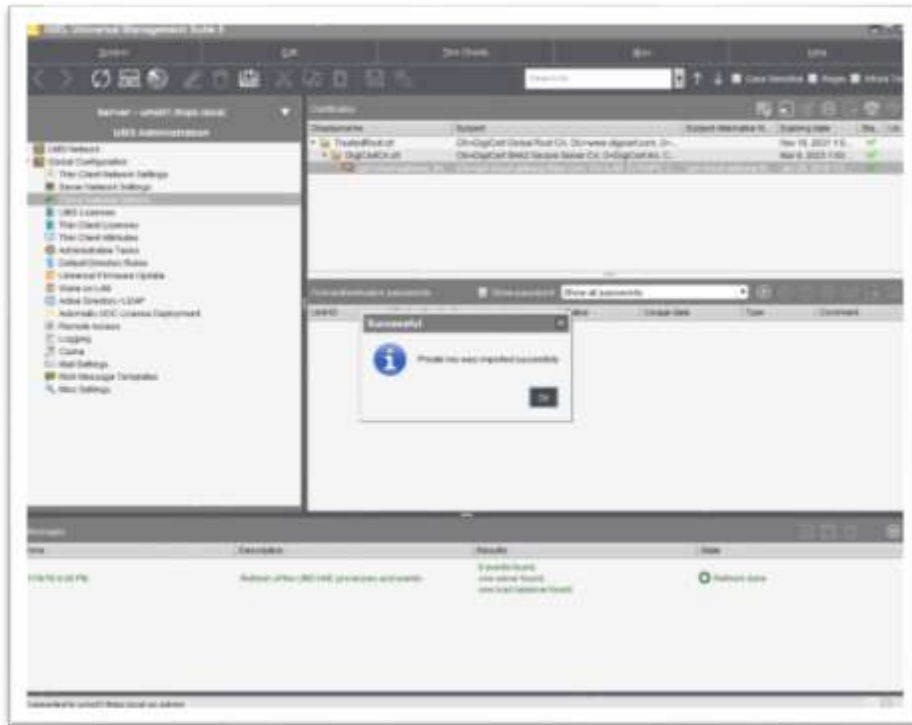
11. Choose your server certificate, in my case this is **igel-cloud-gateway-thinpc-com.crt**



12. Now right-click your server certificate and choose **import decrypted private key**. Select the key file which you generated and downloaded from your ICG appliance.



13. You have successfully installed a DigiCertificate SSL certificate on your UMS and ICG environment.

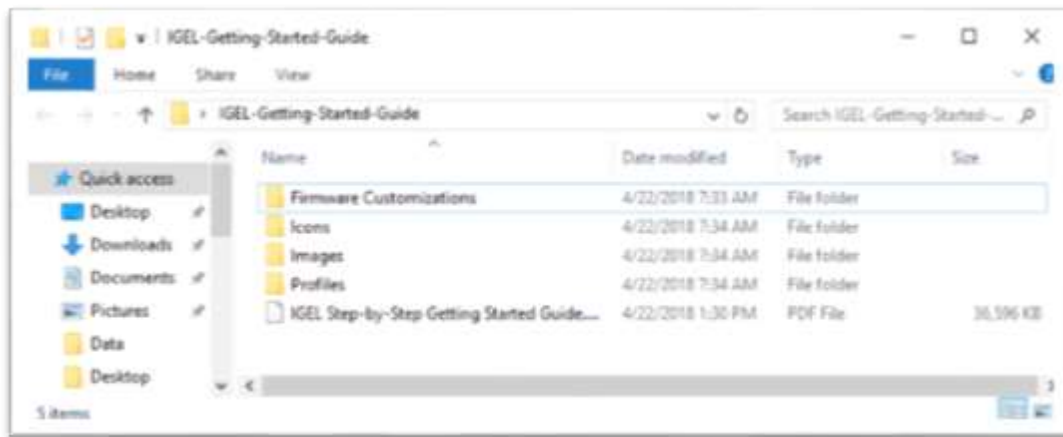


2. How to Import Project Customizations

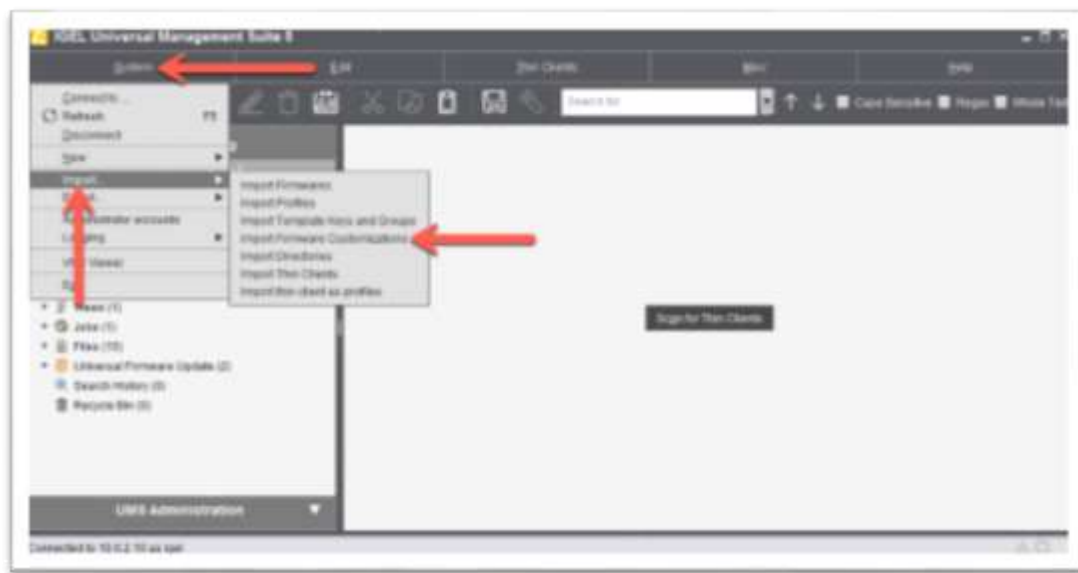
The IGEN Platform Step-by-Step Getting Started Guide is delivered with a zip file containing the UMS profiles, firmware customizations, images and icons used in the customization section.

The following defines how to import the custom customizations:

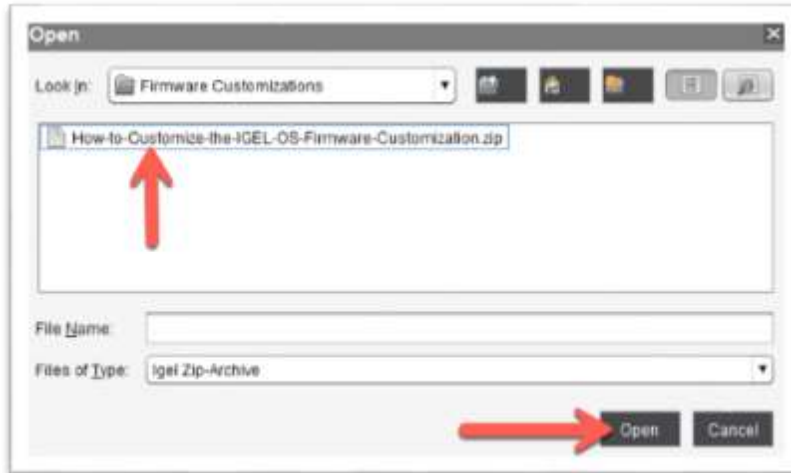
1. Extract the contents of the **IGEL-Getting-Started-Guide.zip** file to a location accessible to be uploaded to the UMS. If you are running the UMS on Windows, the desktop works great.



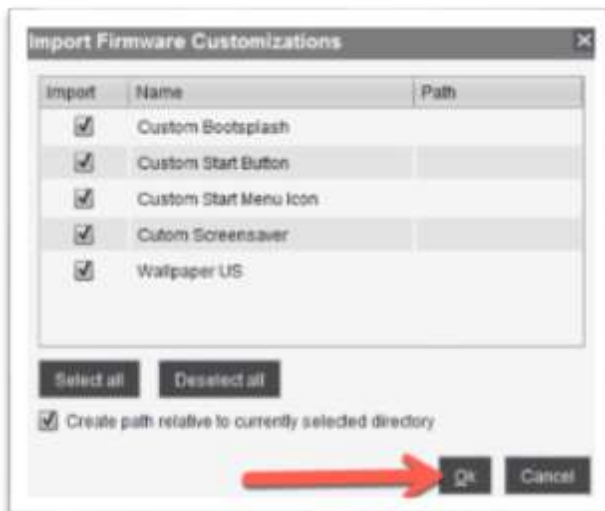
2. The first thing you will want to do is import the firmware customizations. Click the **Systems** link in the top left of the UMS, click the **Import** link in the drop-down menu and then click the **Import Firmware Customizations** item.



3. The **Open** window opens. Browse to the location you extracted the **IGEL-Getting-Started-Guide.zip** file and drilled down to the **Firmware Customizations** folder. Click to select the **How-to-Customize-the-IGEL-OS-Firmware-Customizations.zip** file and then click the **Open** button to upload it.



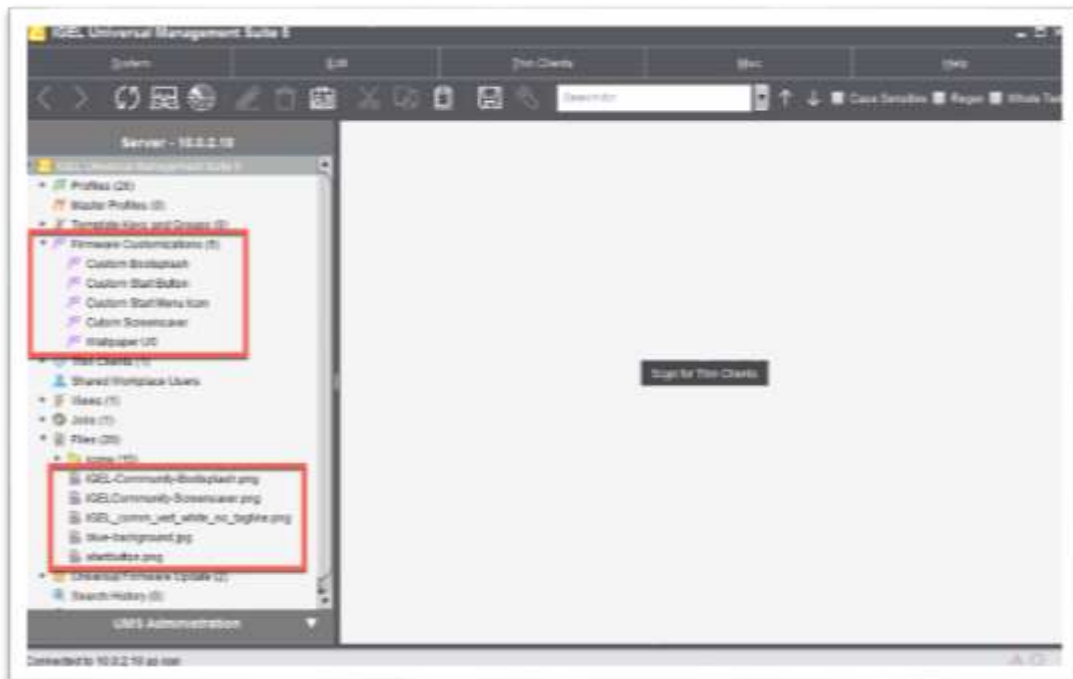
4. The **Import Firmware Customizations** window opens listing the firmware customization included in the zip file. Accept the defaults to import all the customizations and then click the **OK** button to continue.



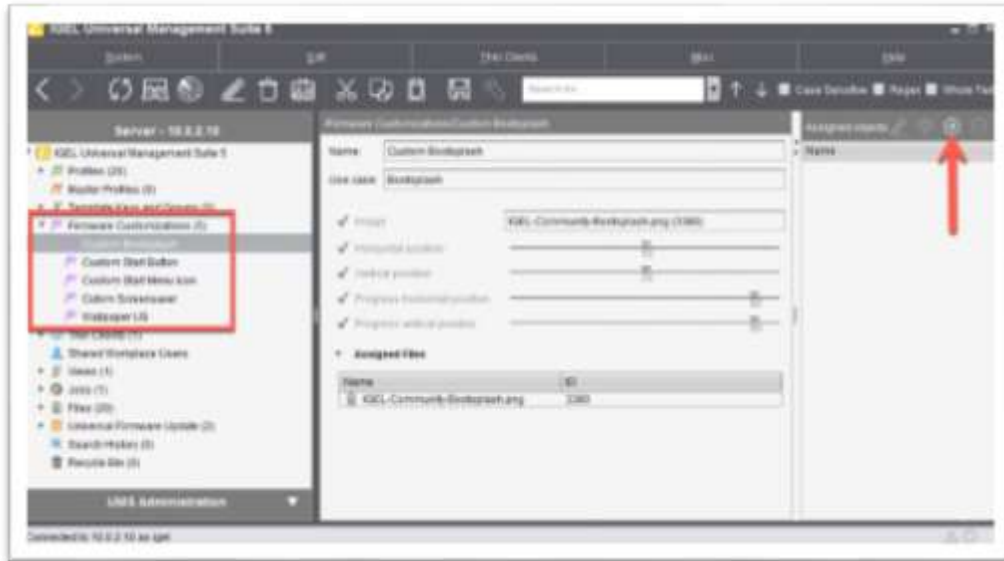
5. If life is good, you will see the following popup prompting you the import was successful. Click **OK** to continue.



6. You are brought back to the UMS, where you will notice a few new items. The first is the firmware customizations where imported and added to the **Firmware Customizations** section and the other being the images associated with each customization where added to the UMS' **Files** repository.

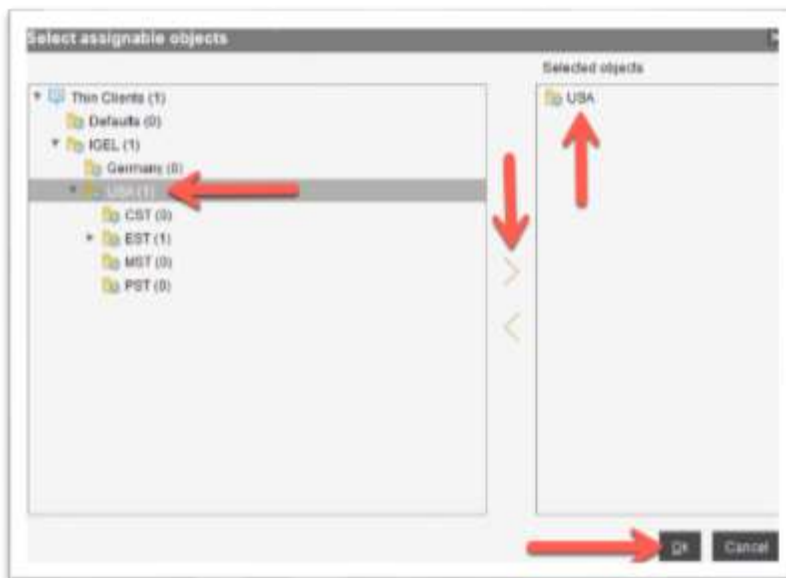


7. Once the firmware customizations are imported you are required to assign each configuration to the desired device(s). Click the desired firmware customization and click the + icon located at the top right of the UMS.



12. The **Select assignable objects** window opens prompting you to assign the firmware customization to the desired devices.

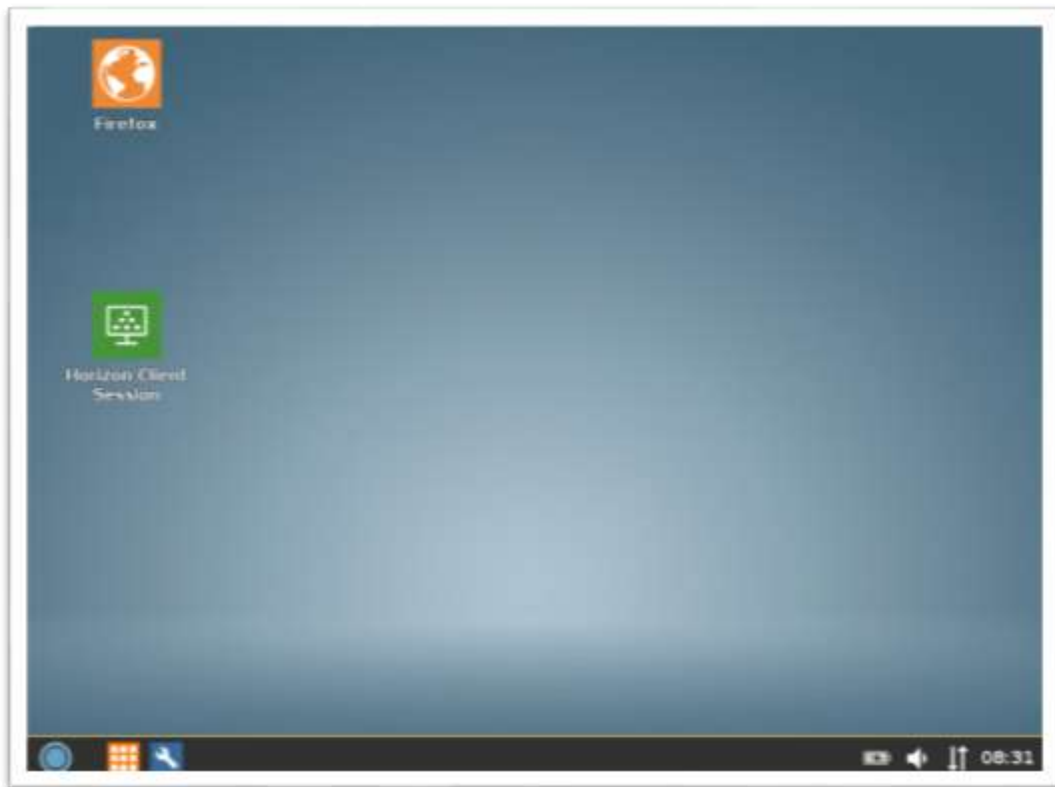
Click to select the device or directories you wish to assign the firmware customization to and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign your new firmware customization.



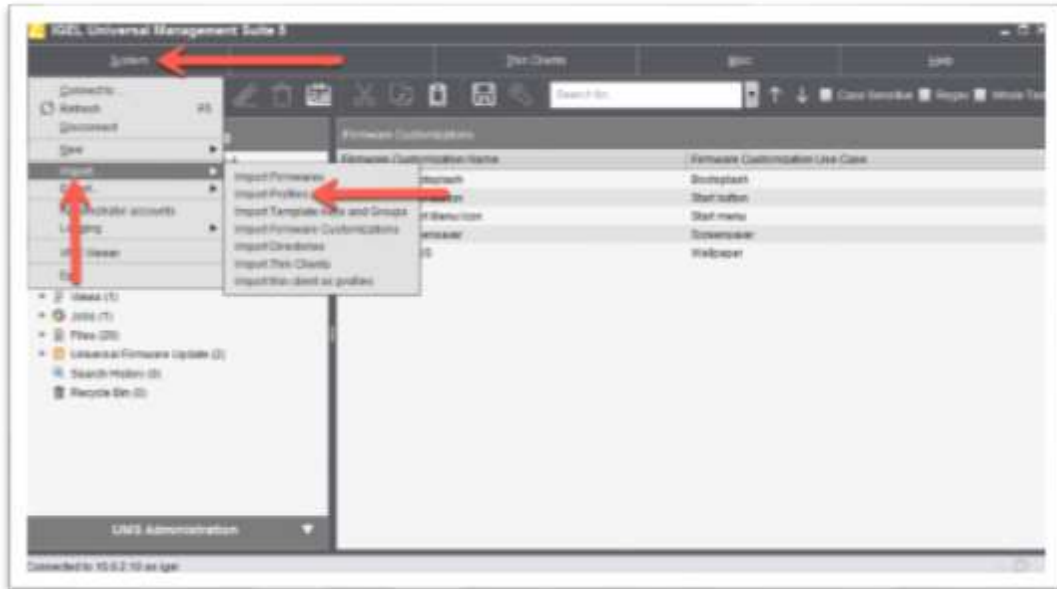
8. The **Update time** dialog box is opens prompting you to define when you would like the new settings to take effect. Select the desired setting and click **OK** to continue.



9. Look at one of your managed devices; you will notice the customization has been applied. Your desktop is starting to look like the one in this guide.



10. The next step is to import the delivered UMS profiles. Click the **Systems** link in the top left of the UMS, click the **Import** link in the drop-down menu and then click the **Import Profiles** item.



11. The **Open** window opens. Browse to the location you extracted the **IGEL-Getting-Started-Guide.zip** file, click to select the first profile from the **Profiles** directly and then click the **Open** button to upload it.



12. The **Import Profiles** window opens listing the profiles within the selected profiles zip file. Accept the defaults and click **OK** to import the profile to your UMS.

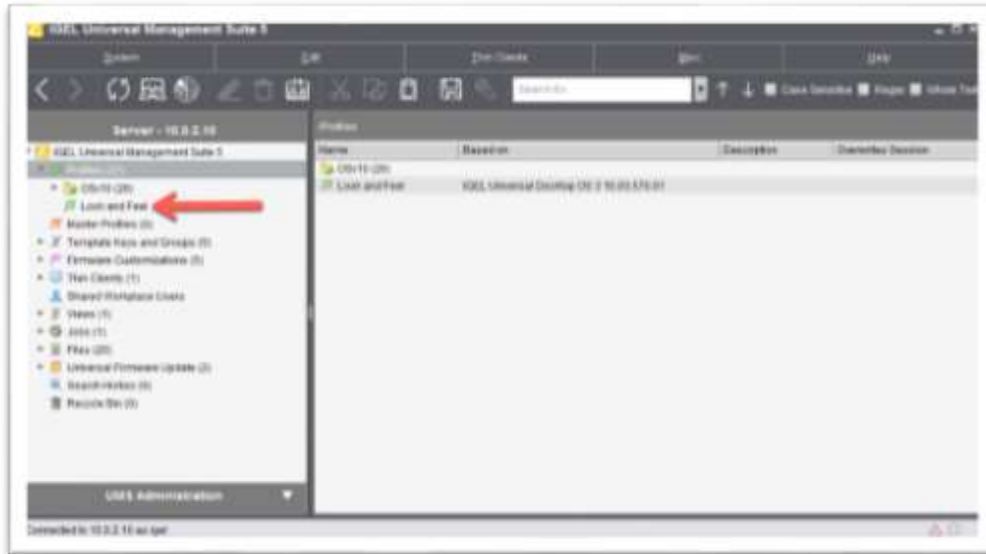


13. Click **OK** to continue.

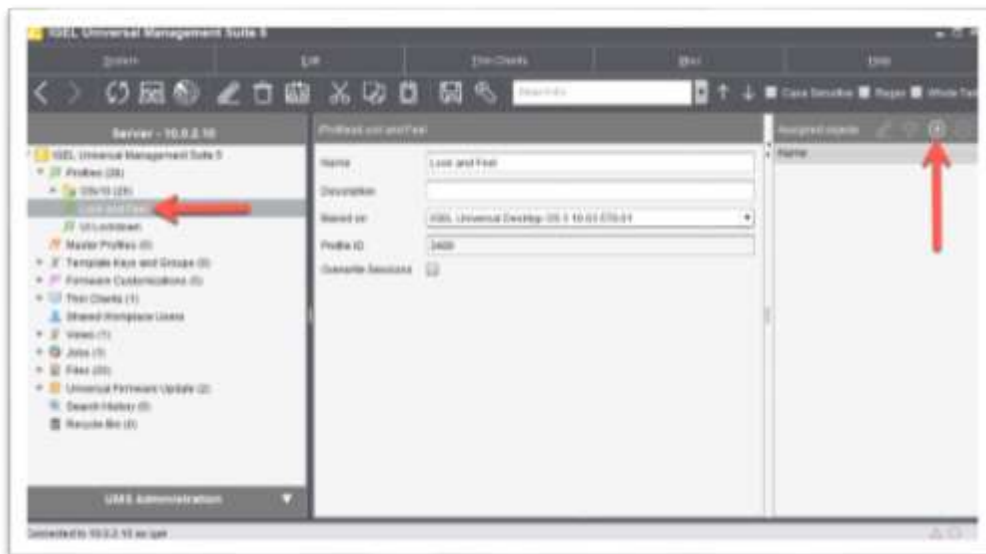


14. The profile is imported into the root of the UMS **Profiles** tree. You are free to drag and drop it into the desired folder or leave it where it sits.

Repeat steps 10-13 to import the second included profile zip file.



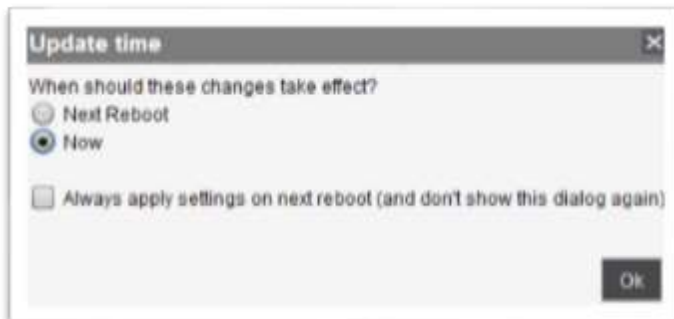
15. As with the firmware customizations you are required to assign the newly imported profile to the desired device(s). Click the desired profile and click the + icon located at the top right of the UMS.



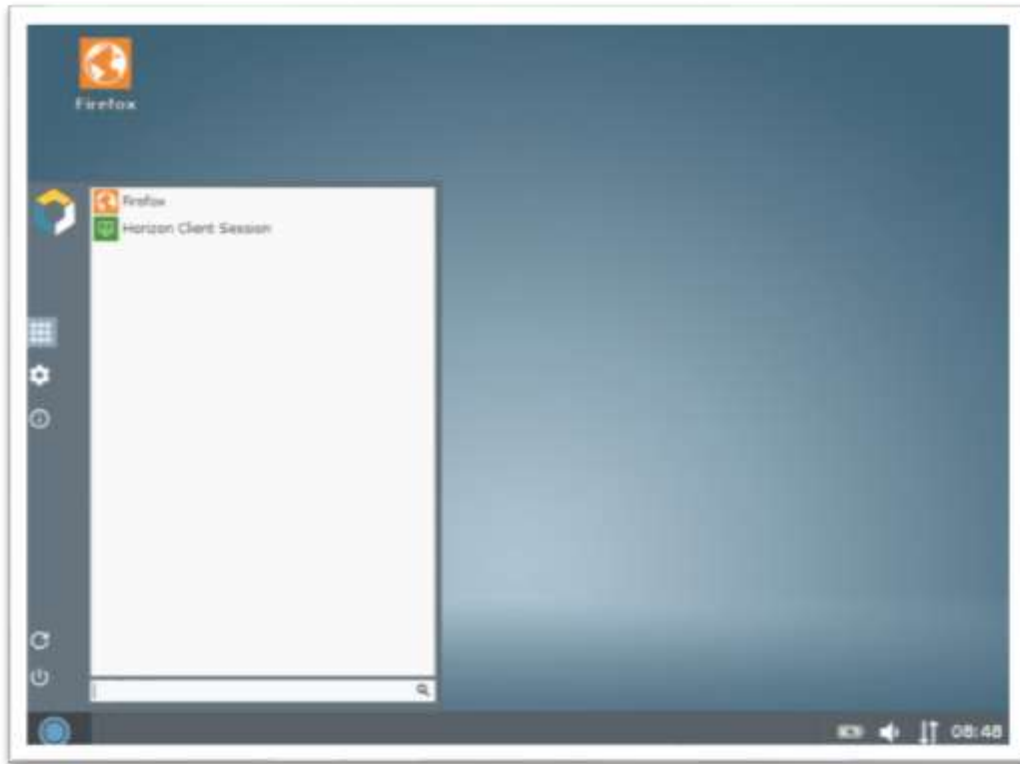
16. The **Select assignable objects** window opens prompting you to assign the profile to the desired devices. Click to select device(s) or directories you wish to assign the profile customization to and click the > arrow to move it to the **Selected objects** pane. Once finished, click the **Finish** button to assign the new profile.



17. The **Update time** dialog box is opens prompting you to define when you would like the new settings to take effect. Select the desired setting and click **OK** to continue.



18. Look at a managed IGEL OS device, and you will notice it is not fully customized and should look just like the image below.



19. You are now ready to customize the icons. Please refer to the [How to Customize Session Icons](#) section above.

You are done! It is truly a beautiful day!

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

The IGEL Platform Step-by-Step Getting Started Guide comes with a zip file containing example UMS profiles, images and icon used in the customization section. Refer to the **How to Import Project Customizations** section above to learn how to import the following configurations into your environment.

The following is a list detailing the files located in the **IGEL-Getting-Started-Guide.zip** file.

Root Folder:

Filename	Description
\ IGEL-Step-by-Step-Getting-Started-Guide-1.5.zip	This document, the main how-to install and configure the IGEL Platform Step-by-Step Getting Started Guide .

Firmware Customizations Folder:

Filename	Description
How-to-Customize-the-IGEL-OS-Firmware-Customization.zip	Backup file containing the 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.

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

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.

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

4. Additional Resources

As I mentioned in the preface, this document is meant to be a starting point in your journey in mastering the hottest secure endpoint management solution out there today! However, this is just a start, below is a list of additional resources for you to learn more about the fantastic solution we call the IGEL Software Platform!

Profile Files:

- **IGEL-Getting-Startd-Guide.zip**
<http://files.igelcommunity.com/IGEL-Getting-Started-Guide.zip>

IGEL Community:

- **LinkedIn Group**
<http://linkedin.igelcommunity.com/>
- **Slack Group**
<http://slack.igelcommunity.com/>

Web Resources:

- **IGEL Community Public Home Page**
<http://www.igelcommunity.com/>
- **IGEL Community TechChannel – Technical How-To Videos**
<https://www.youtube.com/c/IGELCommunity>
- **IGEL Support Documents**
<http://kb.igel.com/>
- **IGEL Management Interface (IMI)**
<https://kb.igel.com/igelimi-v1/en/igel-management-interface-imi-3113925.html>
- **IGEL Unified Management Agent (UMA)**
<https://kb.igel.com/uma/en/unified-management-agent-uma-2721613.html>
- **IGEL UMS High Availability (HA)**
<https://kb.igel.com/endpointmgmt/en/high-availability-ha-915934.html>
- **Linux Third Party Hardware Database**
<https://www.igel.com/linux-3rd-party-hardware-database/>
- **IGEL with Imprivata Step by Step Configuration Video**
<https://www.xentegra.com/igel-pocket-secure-rogue-workforce-ease/>

- **IGEL Cloud Gateway on Nutanix AHV**
<https://dreadysblog.wordpress.com/2017/12/25/igel-cloud-gateway-on-nutanix-ahv/>

IGEL Related Manuals

- **IGEL Universal Desktop LX 10 - User Manual**
<https://kb.igel.com/igelos/en/igel-os-manual-2719974.html>
- **IGEL Universal Management Suite v5 - User Manual**
<https://kb.igel.com/igellinux/en/igel-linux-v5-manual-2274996.html>
- **IGEL Universal Desktop Converter 3 (UDC3) - User Manual**
<https://kb.igel.com/igelos/en/udc3-manual-2721394.html>
- **IGEL UMS 5 Profiles - Reference Manual**
<https://kb.igel.com/endpointmgmt/en/profiles-910377.html>
- **How to Secure Endpoints with IGEL OS White Paper**
https://www.igel.com/wp-content/uploads/2017/07/WP_Securing-IGEL-OS-Endpoints.pdf

5. Last Words

To ‘somewhat’ quote one of my favorite stories, **“You’re off to great places, today is your day, your” thin clients “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, and VDI environments today! The possibilities are close to endless. You cannot hurt it, create more profiles and have some fun with it.

Of course, the steps within this document provided you with the very basics for you to kick-start your IGEL lab environment. Please refer to the links to eDocs support articles, white papers, videos, and 3rd party web posts found throughout this document. They will allow you to learn more about each configuration and the vast possibilities each setting brings. Don’t forget the **Additional Resources** section to read and learn more.

To stay up to date with all the latest IGEL tech resources and this project, please join the **IGEL Community**. Our goal was to create a place for the techies, the men and women who are required to support IGEL solutions, to learn more through the power of each other! Today we have hundreds of the leading names in the EUC world, along with rock star engineers from IGEL as members of our lively community.

Want proof? This document is the proof; this is an IGEL Community Project so if you would like to stay up to date with the latest changes and additions please join.

Today you can find the IGEL community in two places, a [LinkedIn Group](#), and a very active [Slack](#) group. I cannot recommend it enough.

All in all, have fun! The IGEL Platform is one fantastic piece of software designed and developed by a fantastic group of people! You will truly enjoy it and your users will too!

Thank you very much,

Douglas Brown & The IGEL Community Team!

A Splendid Time is Guaranteed for All!