

Single KeyScaler Instance Stack - Install Guide 6.7.3

	Document Name	KeyScaler 6.7.3 Installation Single Tenant
	Host	Red Hat Enterprise Linux Server 7.9
	Version	Published
	Date Published	October 2021
	Classification	External Document
	Author	Nirmal Misra

© 2021 Device Authority

This document contains proprietary and confidential information of Device Authority and shall not be reproduced or transferred to other documents, disclosed to others, or used for any purpose other than that for which it is furnished, without the prior written consent of Device Authority. It shall be returned to the respective Device Authority companies upon request.

The trademark and service marks of Device Authority, including the Device Authority mark and logo, are the exclusive property of Device Authority, and may not be used without permission. All other marks mentioned in this material are the property of their respective owners.

Table of Contents

- [Table of Contents](#)
- [1. Introduction](#)
 - [1.1 Document Version Control](#)
 - [1.2 Assumptions](#)
 - [1.3 Constraints](#)
 - [1.2 Terms and Definitions](#)
 - [1.3 Related Documentation](#)

- 2. KeyScaler Installation
 - 2.1. Install Pre-requisites
 - 2.1.1 Verify dfactor service is running
 - 2.1.2 Add Hosts Entries
 - 2.2 Installation Wizard
 - 2.2.1 Run the KeyScaler Setup Wizard
 - 2.2.2 Welcome Page
 - 2.2.3 Database Configuration
 - 2.2.4 Apache Kafka Configuration
 - 2.2.4.1 Update server.properties
 - 2.2.4.2 Start Zookeeper as daemon
 - 2.2.4.3 Start Apache Kafka as daemon
 - 2.2.5 KMS Deployment
 - 2.2.5.1 KeyStore Initialization
 - 2.2.5.2 KMS Configuration
 - 2.2.5.3 KMS Deployment
 - 2.2.6 KMS Message Queue Service Deployment
 - 2.2.6.1 Host Information
 - 2.2.6.2 KMS Message Queue Deployment
 - 2.2.7 Memcached Configuration
 - 2.2.8 Account Creation
 - 2.2.8.1 Master Account Creation
 - 2.2.8.2 Tenant Account Creation
 - 2.2.8.3 Download DAE Account Public Keys
 - 2.2.9 System License
 - 2.2.9.1 Import System License
 - 2.2.10 DAE Deployment
 - 2.2.10.1 Host Information
 - 2.2.10.2 Configuration
 - 2.2.10.3 Deployment
 - 2.2.11 Message Queue Service Deployment
 - 2.2.11.1 Message Queue Host Info
 - 2.2.11.2 Deployment
 - 2.2.12 CP Deployment
 - 2.2.12.1 Configuration
 - 2.2.12.2 Deployment
 - 2.2.13 Setup Complete
 - 2.3 Configure Licenses
 - 2.4 Deploy DDKGs
 - 2.5 CP Access
 - 2.5.1 Tenant Control Panel
 - 2.5.2 Master Control Panel
 - 2.5.3 Post-installation activities

- 3 Service Access Controller Installation
 - 3.1 Overview
 - 3.2 Install on Same Server
 - 3.2.1 Unpack the SAC Zip file
 - 3.2.2 Configure the SAC
 - 3.2.3 Deploy service-access-controller.war
 - 3.2.4 Restart the KeyScaler DFactor Service
 - 3.2.5 Connectivity Test
 - 3.3 Install SAC on Standalone Server
 - 3.3.1 Pre-requisites
 - 3.3.1.1 Java Runtime Environment (JRE) 1.8
 - 3.3.1.2 Apache Tomcat 7
 - 3.3.1.3 Communicating over HTTPS
 - 3.3.2 Install Instructions
 - 3.3.2.1 Transfer the Service Access Controller Package to Your Server
 - 3.3.2.2 Unpack the sac.tar.gz file
 - 3.3.2.3 Create Service User
 - 3.3.2.4 Create Necessary Directories
 - 3.3.2.5 Copy Tomcat to /var/lib
 - 3.3.2.6 Symbolic link
 - 3.3.2.7 Configure Tomcat and Service Access Controller
 - 3.3.2.8 Install service-access-controller.war into Tomcat
 - 3.3.2.9 Set permissions
 - 3.3.2.10 Configure Tomcat SSL Connector
 - 3.3.3 DNS Entry
 - 3.3.4 Connectivity Tests
 - 3.3.4.1 Curl from local computer to SAC

- 4 End to End Sanity Tests
 - 4.1 Helpful Information
 - 4.2 Post-Installation Activities
 - 4.2.1 Account Settings
 - 4.2.1.1 General Settings
 - 4.2.1.2 Email URIs for PC Devices
 - 4.2.1.3 Manage Notifications
 - 4.2.1.4 Configure Outgoing Mail
 - 4.2.1.2 Manage Administrators
 - 4.2.1.3 Tenant Account Setup
 - 4.2.1.3.1 Account Settings
 - 4.2.1.3.1.1 URI Setup - for PC Devices
 - 4.2.1.4 Manage Notifications
 - 4.3.1.5 Manage Administrators
 - 4.2.1.6 Manage DAE API Settings
 - 4.2.2 Other Configuration Customization's
 - 4.2.2.1 Blocking the Wizard from General Access
 - 4.2.2.2 Installing DFACTOR Tools
 - 4.2.3 Master Account Setup
 - 4.2.4 DAE And CP Configuration
 - 4.2.5 KeyScaler-Securing Certs and Best Practice
 - 4.2.5.1 Securing SAN Certs
 - 4.2.5.2 Keeping only the necessary certificates
 - 4.3 Orientation to your KeyScaler System
 - 4.3.1 Database
 - 4.3.2 Linux User
 - 4.3.1 Log files
 - 4.3.2 Tomcat
 - 4.3.3 Helpful Commands
 - 4.3.3.1 Start KeyScaler
 - 4.3.3.2 Stop KeyScaler
 - 4.3.3.3 Check If KeyScaler is running
 - 4.3.3.4 Run NA Tool - used to configure your KeyScaler license
 - 4.3.3.5 Check to see if KeyScaler is running via Browser
 - 4.4 Troubleshooting
 - 4.4.1 Oh Snap! Maximum status check attempts exceeded
 - 4.3.1.1 Fix – Update hosts file

1. Introduction

1.1 Document Version Control

Version	Description	Date	Author
1.0	Initial Document Creation	20 th October 2018	Frode Nilsen
2.0	Updated for KS 6.7.0	18 th Sept 2020	Nirmal Misra
2.1	Securing Certs - Best Practice	7 th October	Nirmal Misra
2.2	Updated for KS 6.7.3	October 2021	Nirmal Misra

Item 1 - Document Version Control

1.2 Assumptions

No	Description
1	Document tested on Redhat7 and CentOS7.X

Item 2 - Assumptions

1.3 Constraints

No	Description

Item 3- Constraints

1.2 Terms and Definitions

Term	Meaning
KMS	Key Management Store
DAE	Device Authority Engine
CP	Control Panel
DDKG	Dynamic Device Key Generator
SAC	Service-Access-Controller
DA	Device Authority
KS	KeyScaler

Item 4 - Terms and Definitions

1.3 Related Documentation

Doc #	Title	Comment
[1]	DAKS-6.7.0-INST-KEYSCALER.docx	KeyScaler Installation document
[2]	Single Tenant - Prerequisites KS 6.7.2 CentOS 7.5	KeyScaler Installation Prerequisites document

Item 5 – Related Documentation

2. KeyScaler Installation

2.1. Install Pre-requisites

2.1.1 Verify dfactor service is running

Check to see that the [dfactor](#) service is running:

```
[root@test ~]# service dfactor status
DeviceAuthority D-Factor (pid 16535) is running...
```

Item 6 – Start dfactor Service

2.1.2 Add Hosts Entries

The following host names will be used by KeyScaler throughout installation. Resolve these by adding entries to **/etc/hosts** on the server on which KeyScaler is being installed.

```
[root@ip-172-31-47-94 cert]# vi /etc/hosts
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6

127.0.0.1 kms.keyscaler-672-001.com
127.0.0.1 kafka.keyscaler-672-001.com
127.0.0.1 dae.keyscaler-672-001.com
127.0.0.1 queue.keyscaler-672-001.com
127.0.0.1 cp.keyscaler-672-001.com
127.0.0.1 sac.keyscaler-672-001.com
```

Item 7 – KeyScaler Server – This domain name keyscaler-6.7 matches the one set when creating the wildcard certificate in the pre-requisite document. Please update this to match your own domain name.

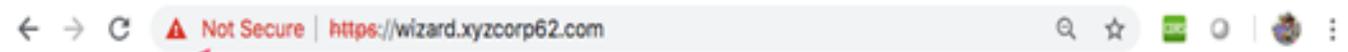
```
51.132.8.93 wizard.keyscaler-672-001.com
51.132.8.93 tenant.keyscaler-672-001.com
51.132.8.93 master.keyscaler-672-001.com
51.132.8.93 sac.keyscaler-672-001.com
```

Item 8 - Your Computer /etc/hosts (replace IP address to match your own environment)

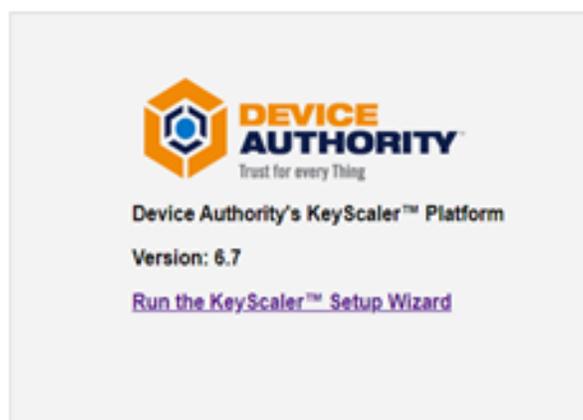
2.2 Installation Wizard

2.2.1 Run the KeyScaler Setup Wizard

<https://wizard.keyscaler-672-001.com:8443/>

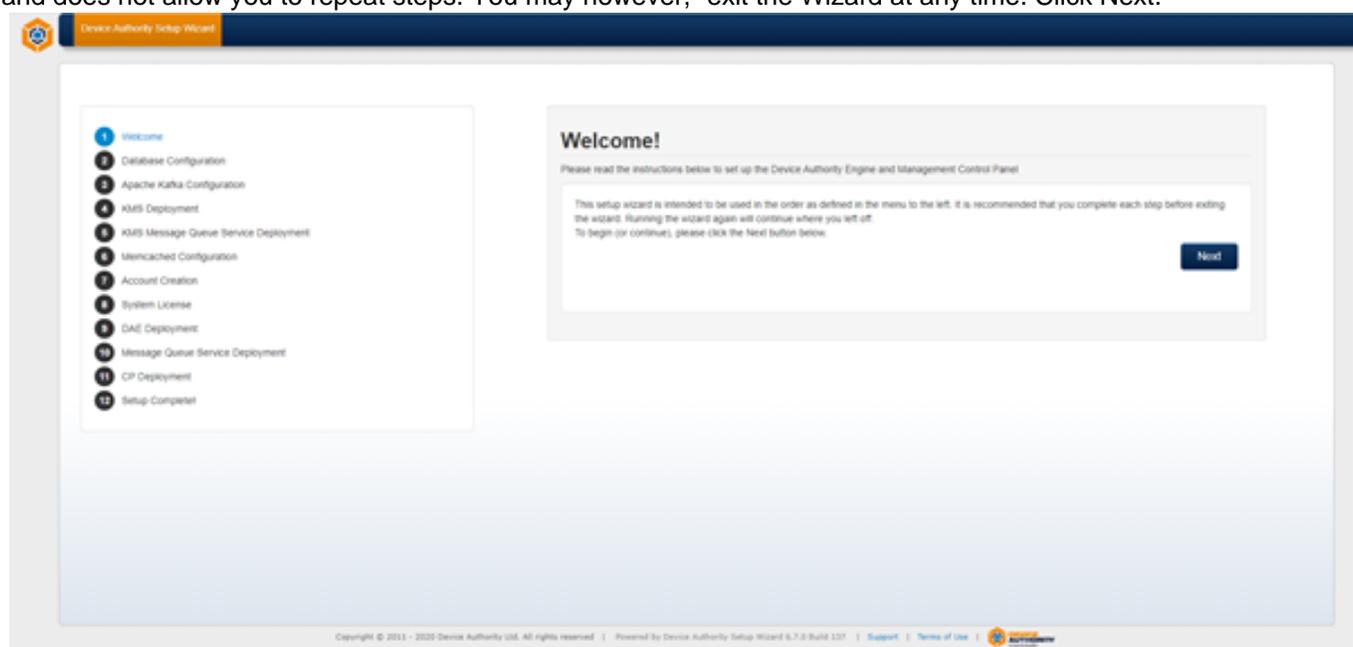


Please note: If you use self-signed cert you may see this warning message.



2.2.2 Welcome Page

Start the Wizard by using a browser window to navigate to e.g. <https://wizard.keyscaler-672-001.com> (replacing organization as appropriate). The Device Authority Setup Wizard is intended to be used in a start-to-finish manner and does not allow you to repeat steps. You may however, exit the Wizard at any time. Click Next.

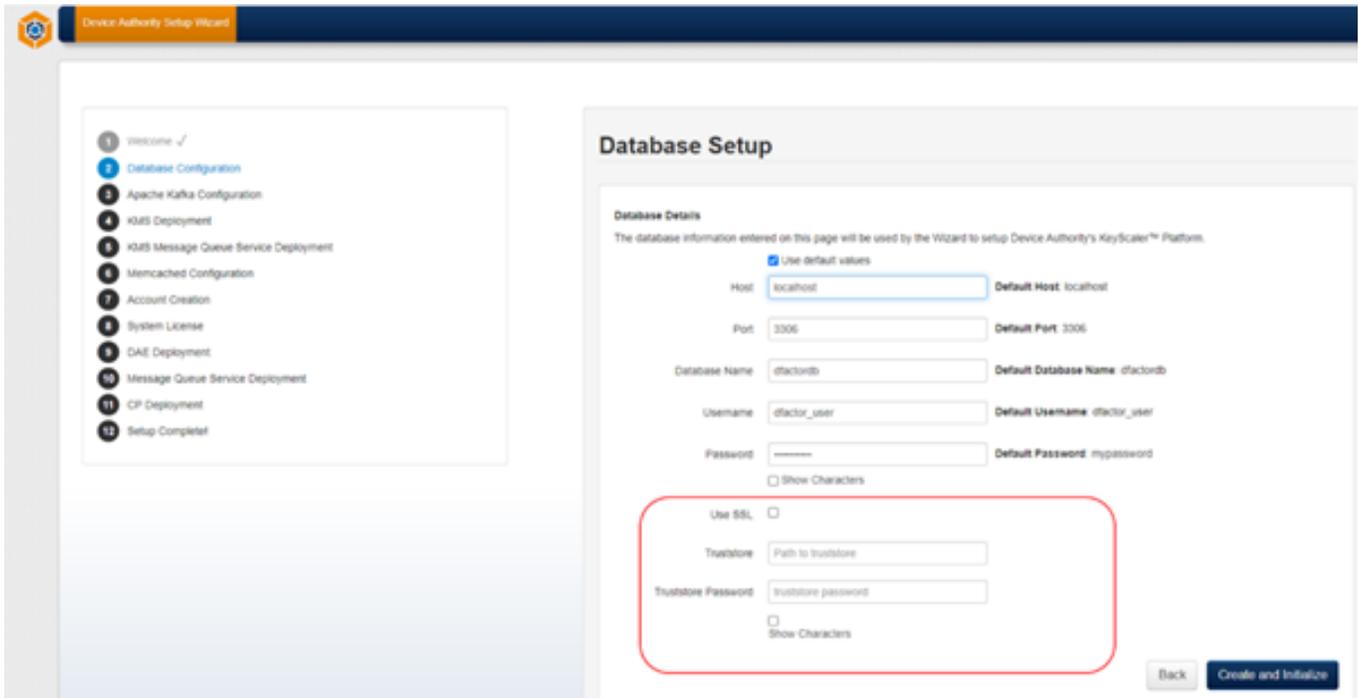


2.2.3 Database Configuration

The database details used when creating your database during the installation of MySQL are provided for you.

The database host name must be the same as used when granting table permissions in the database configuration step. This was set to "*localhost*" by the install script.

- The database port number is set to the default of **3306** which is recommended.
- The default Database Name is **dfactordb**
- The default database username is **dfactor_user**.
- The default password is **mypassword**, change this to the password used in the pre-requisite guide, e.g. ! **Passw0rd!**



For 'Truststore' configuration - Please refer to APPENDIX XX

2.2.4 Apache Kafka Configuration

2.2.4.1 Update [server.properties](#)

```
[root@ config]# vi /opt/kafka_2.11-1.0.0/config/server.properties
```

Item 12 – Configure Apache Kafka

Update the following line `listeners=PLAINTEXT://kafka.keyscaler-672-001.com:9092` to match your domain.

```
# The address the socket server listens on. It will get the value returned from
# java.net.InetAddress.getCanonicalHostName() if not configured.
# FORMAT:
# listeners=listener_name://host_name:port
# EXAMPLE:
# listeners=PLAINTEXT://your.host.name:9092
listeners=PLAINTEXT://kafka.keyscaler-672-001.com:9092
```

Item 13 – Update Kafka `server.properties`. Please ensure that the domain `keyscaler-672-001.com` is swapped for your own domain name

2.2.4.2 Start Zookeeper as daemon

```
[root@host ~]/opt/kafka_2.11-1.0.0/bin/zookeeper-server-start.sh -daemon /opt/kafka_2.11-1.0.0/config/zookeeper.properties
```

Item 14 – Start Zookeeper as a daemon

2.2.4.3 Start Apache Kafka as daemon

```
[root@host ~]# /opt/kafka_2.11-1.0.0/bin/kafka-server-start.sh -daemon /opt/kafka_2.11-1.0.0/config/server.properties
```

Item 15 – Start Apache Kafka as daemon

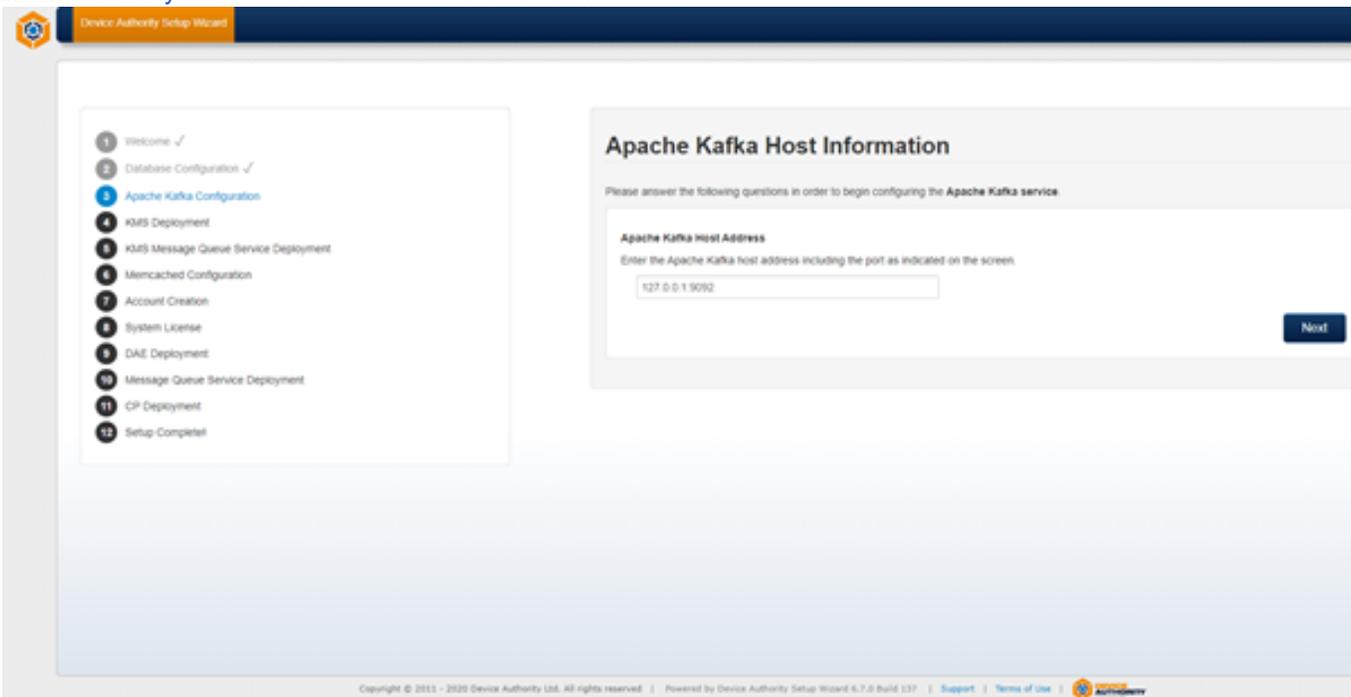
Verify that Kafka is running indicated by output shown in Item 17. If there is no output, please ensure that you have correct entry in hosts file (Item 7)

```
[root@host ~]# ps ax | grep -i 'kafka.Kafka'
```

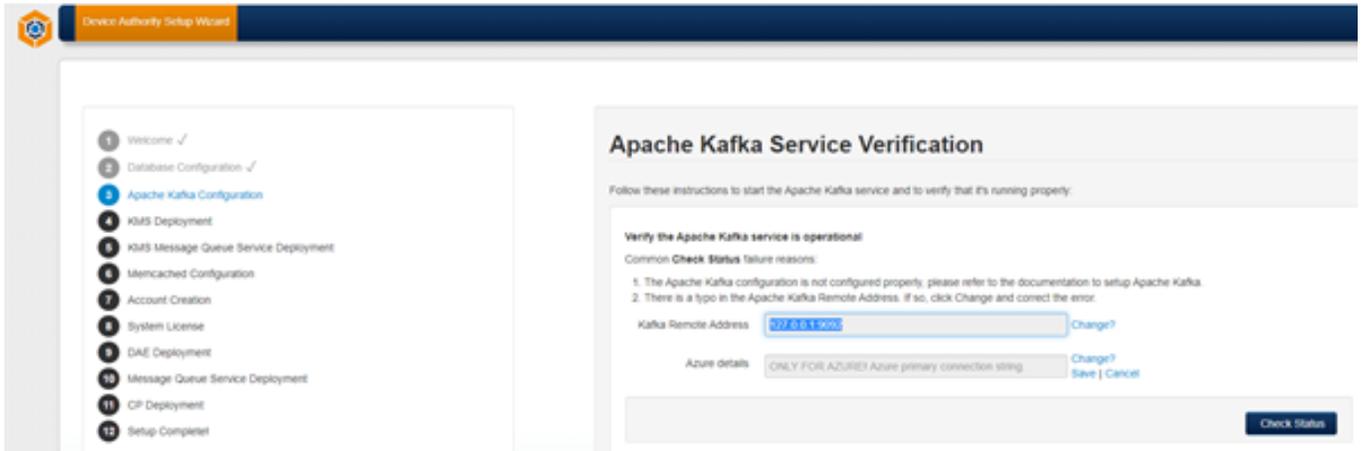
Item 16 – Check if Kafka is running. If there is no output, it is not running. If there is output (Item 17), kafka is running.



Enter kafka.keyscaler-672-001.com:9092 and click **Next**



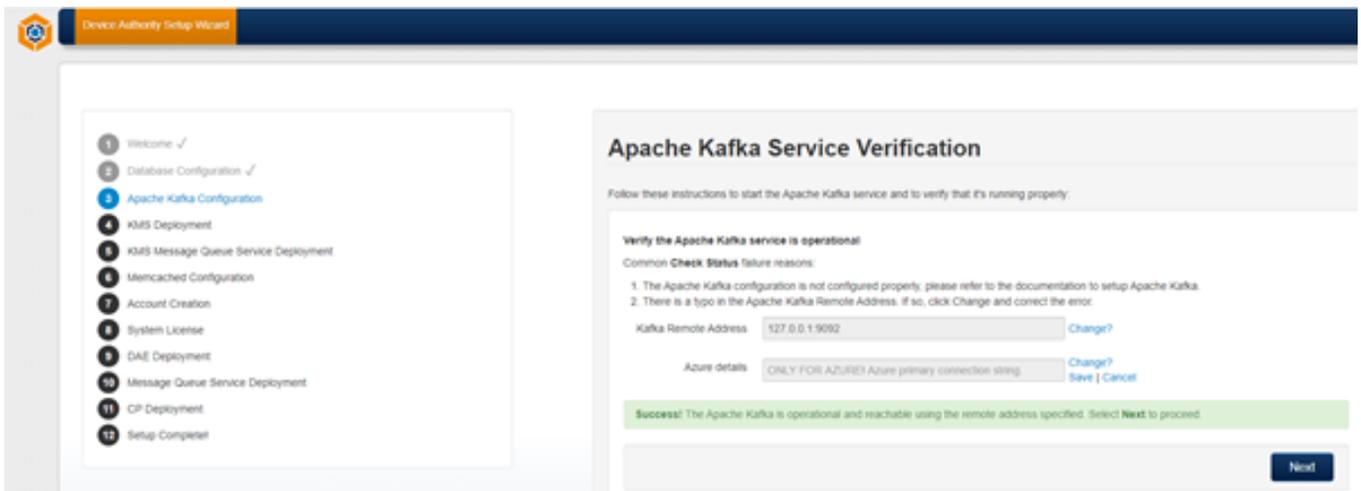
Click on the **Check Status** button.



⚠ If you encounter the error “Oh Snap! Ajax query failed for health check request” please check your `/etc/hosts` file that you have the correct entry and ensure that Kafka is running: `ps ax | grep -i 'kafka\.`Kafka'. If Kafka is not running, start it as shown above.

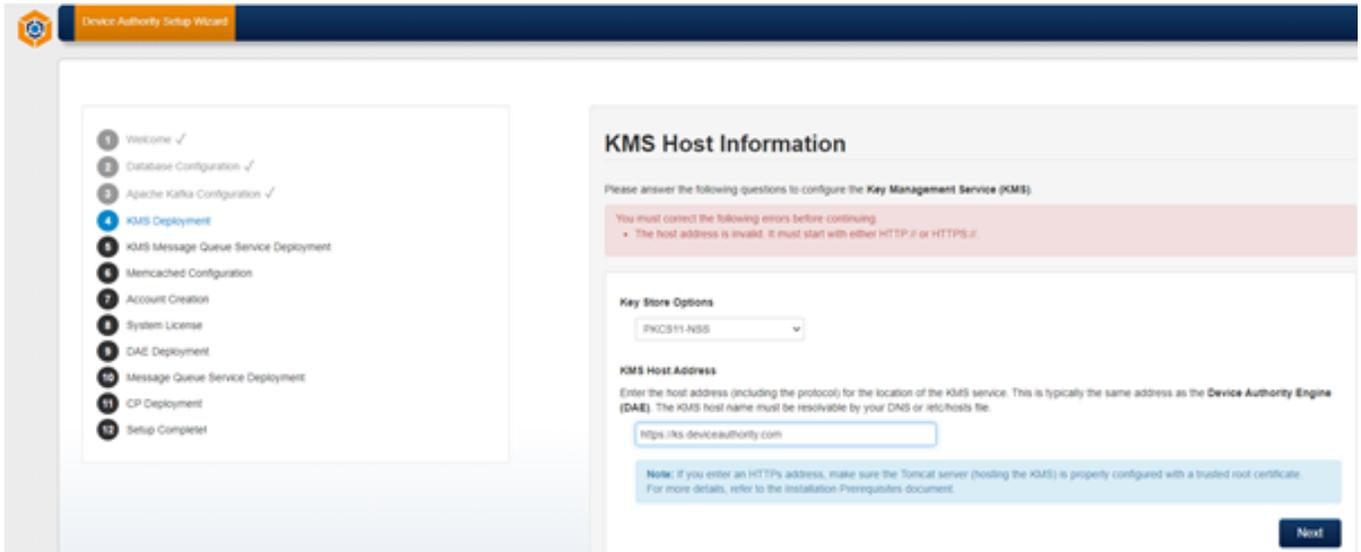
Once the wizard page shows a success message, Click **Next** as shown below:

✓ Success! The Apache Kafka is operational and reachable using the remote address specified. Select **Next** to Proceed.



2.2.5 KMS Deployment

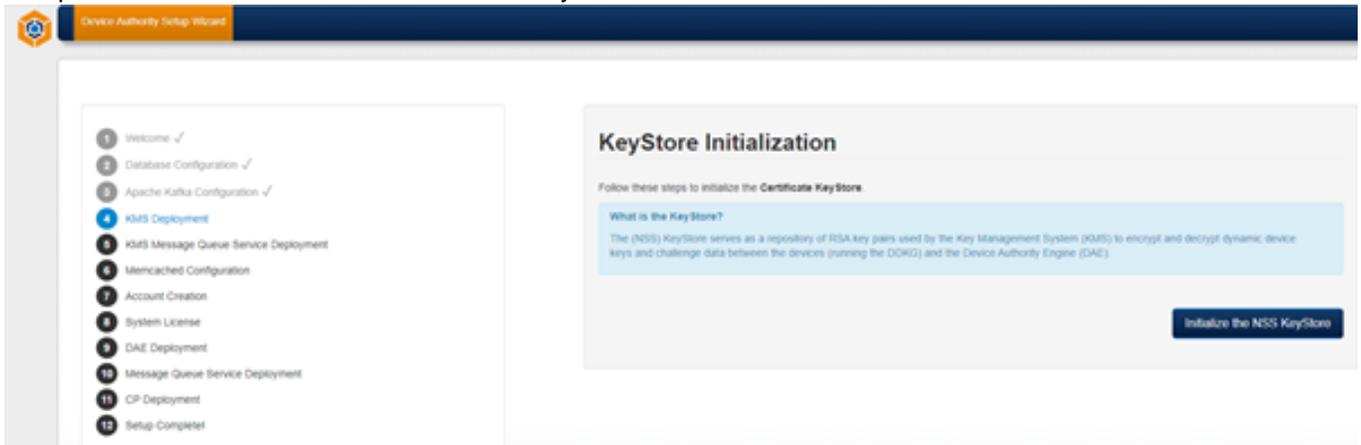
Enter URL <https://kms.keyscaler-672-001.com>



Note: Enter the protocol **https**, else you will get a message as shown above in red.

2.2.5.1 KeyStore Initialization

No input is needed other than to initialize the KeyStore.



2.2.5.2 KMS Configuration

Values entered elsewhere are displayed for your confirmation. If these are correct, click Next.

 For 'Truststore' Configuration - Please refer to APPENDIX XX

2.2.5.3 KMS Deployment

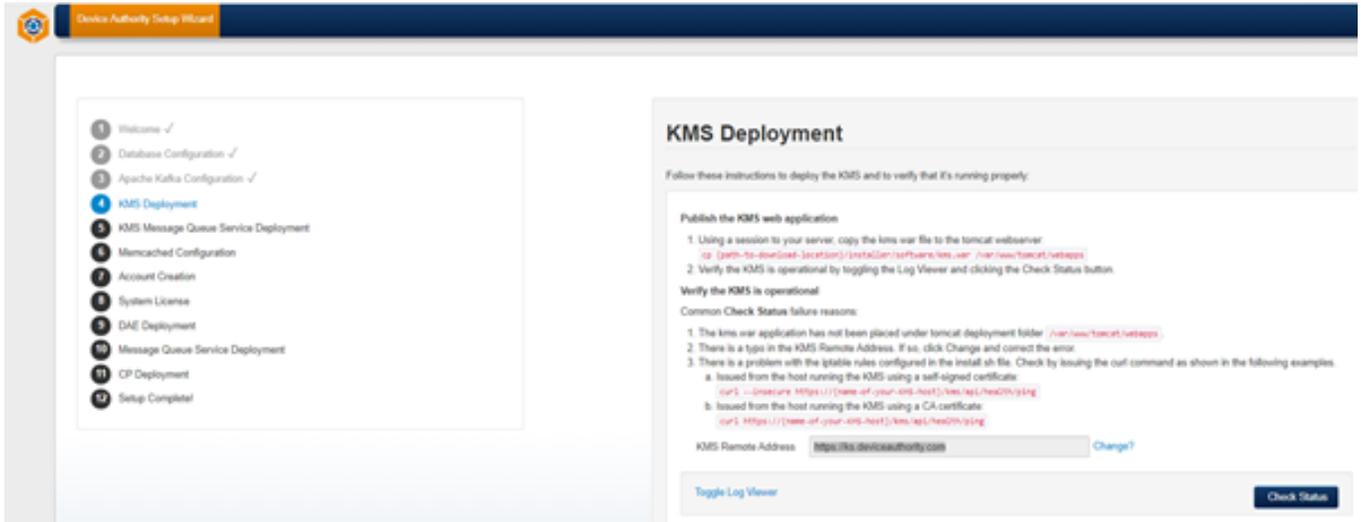
The KMS war file will be deployed in this step and assumes that all the required IP rules have been properly configured as performed by the installer script in the DAE, KMS and CP Installation Prerequisites. Follow the instructions in the Wizard to copy (deploy) the KMS war file to the tomcat webapps directory. Once deployed, click the Check Status button to verify the KMS has deployed successfully.

 **Note:** At this stage copy only the **KMS.war** file, not the other war files, as doing so will break the install procedure.

```
[root@ip-172-31-42-166 software]# cd /home/ec2-user/installer/software
```

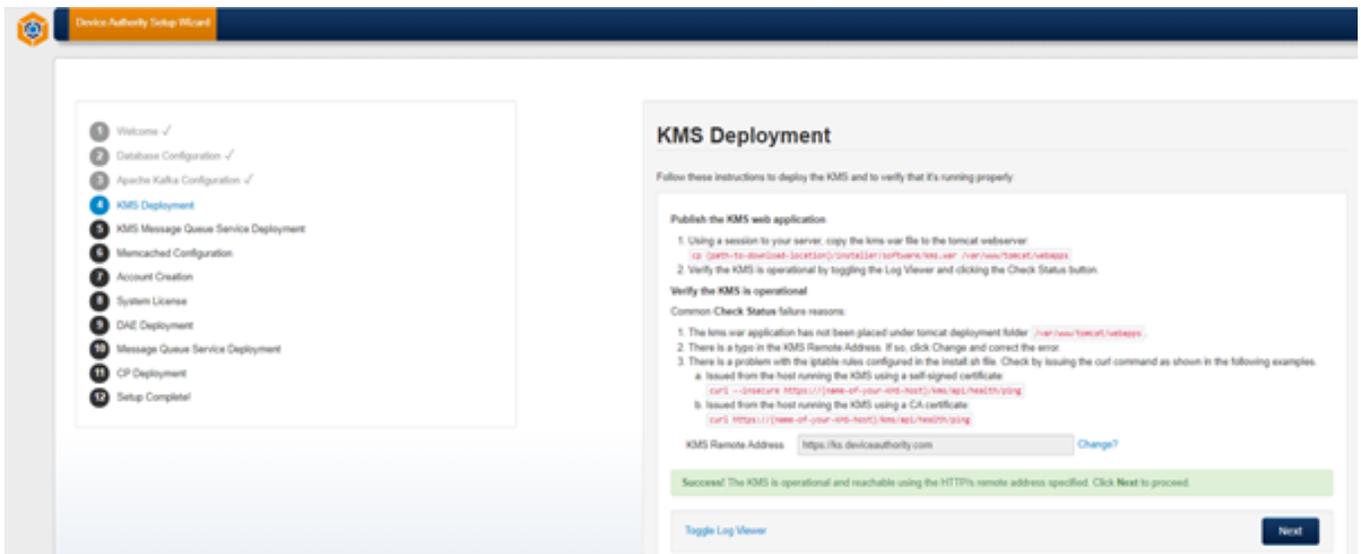
```
[root@ip-172-31-42-166 software]# cp kms.war /var/www/tomcat/webapps
```

Item 24 – Please note the user may differ from centos in which case you need to swap centos in above path with your own user



The following message indicates success:

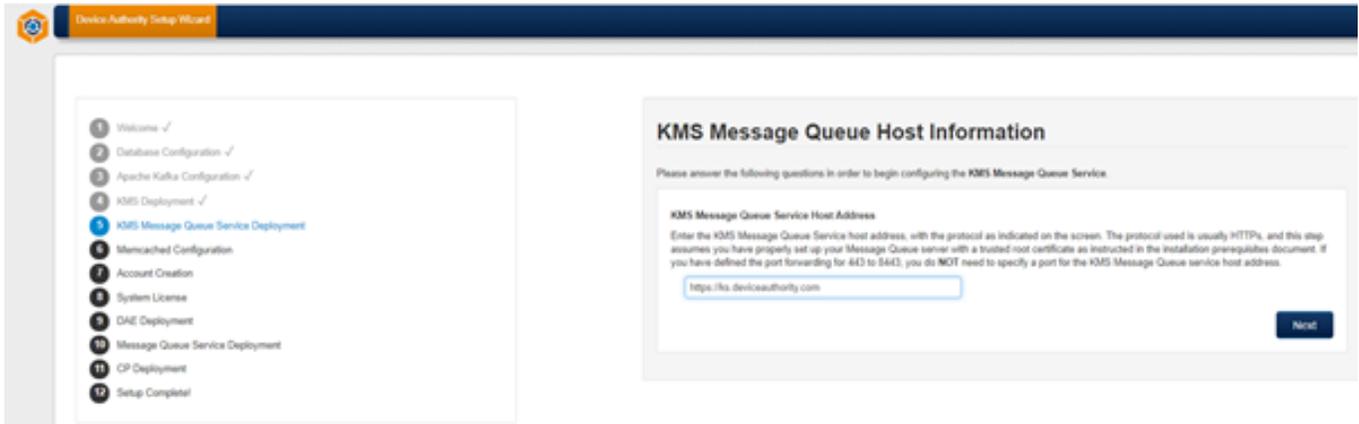
✓ Success! The KMS is operational and reachable using the HTTP/s remote address specified. Click Next to Proceed.



2.2.6 KMS Message Queue Service Deployment

2.2.6.1 Host Information

Please enter the following Message Queue host address, e.g. <https://queue.keyscaler-672-001.com>, as shown below and click Next.



2.2.6.2 KMS Message Queue Deployment

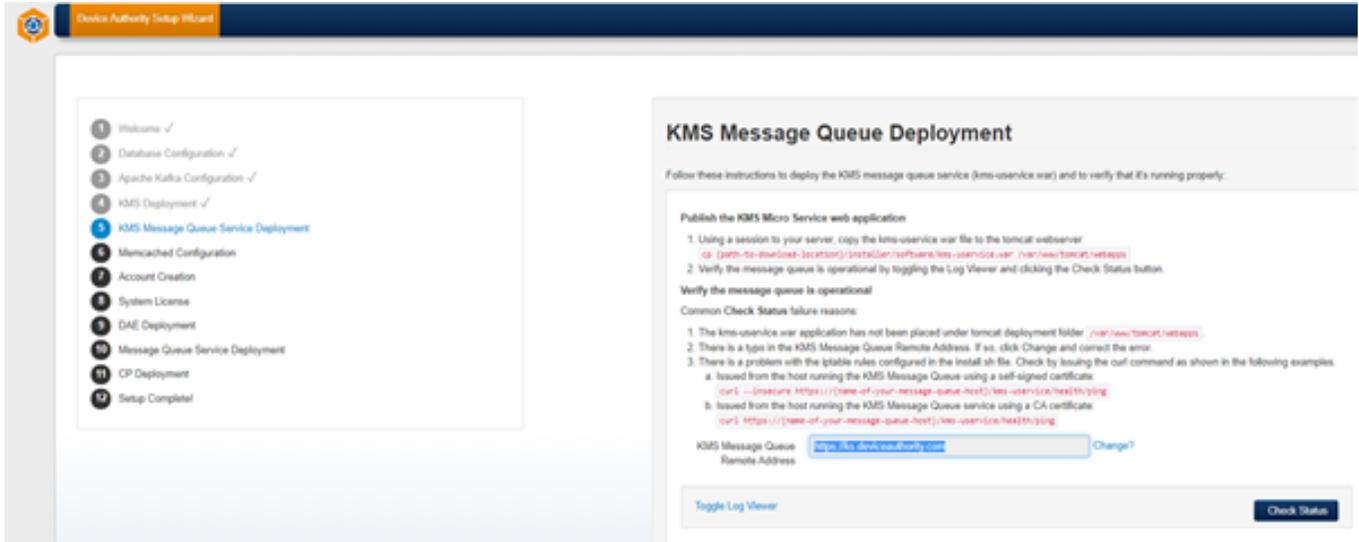
Deploy the following war file.

```
[root@ip-172-31-42-166 software]# cd /home/ec2-user/installer/software
```

```
[root@ip-172-31-42-166 software]# cp kms-uservice.war /var/www/tomcat/webapps
```

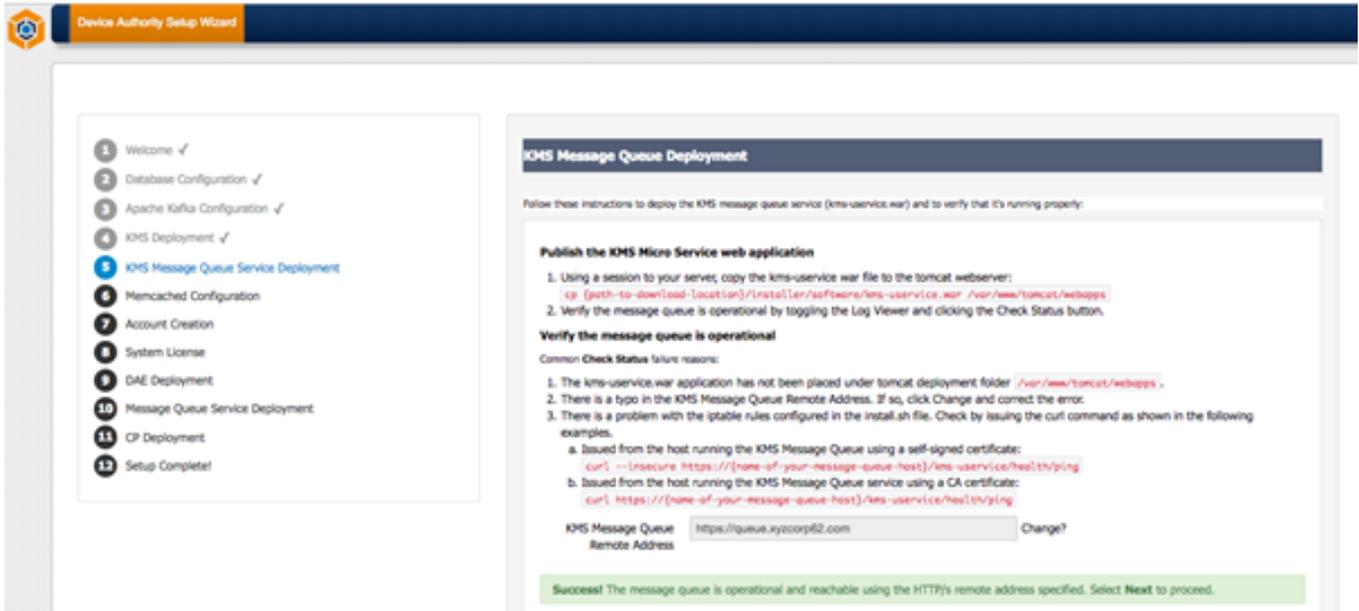
Item 28 – KeyScaler Server – Deploy KMS.war

Click the Check Status button and you should see a green success message after a couple of seconds.



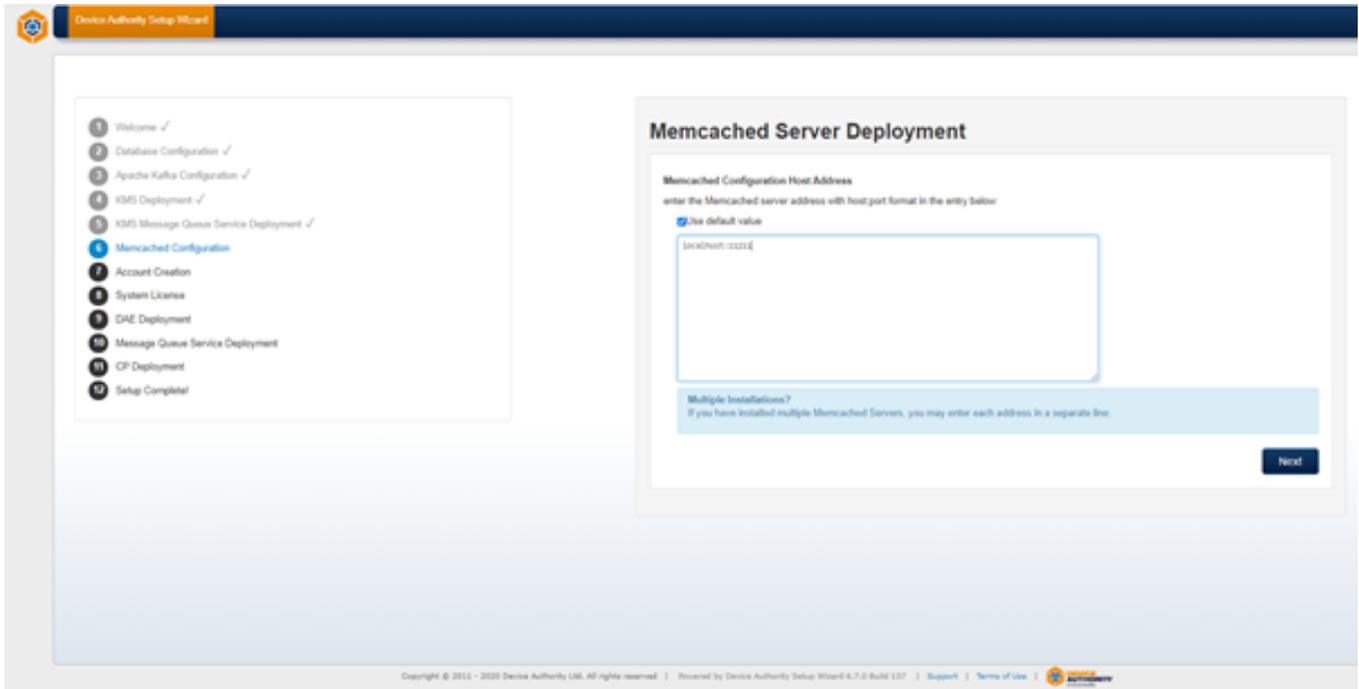
The following message indicates success:

✔ Success! The message queue is operational and reachable using the HTTP/s remote address specified. Click **Next** to Proceed.



2.2.7 Memcached Configuration

The Memcached server address is localhost:11211



2.2.8 Account Creation

The Device Authority IoT Security Platform is a multi-tenant application. You will be creating a Master account and one Tenant account.

2.2.8.1 Master Account Creation

In the Master Account Creation step, you will be defining details about the Master Account. The Master Account allows you to configure and manage system-wide settings and tenant accounts. Make note of the account information used as you'll need it to access the Management Control Panel and register your device.

The Master Tenant Sub-Domain Name will be used as the sub-domain when accessing the Management Control Panel, so choose something simple and easy to type. Common sub-domain names for the Master Account are master, or cp.

The screenshot displays the 'Device Authority Setup Wizard' interface. On the left, a progress indicator shows 12 steps, with 'Account Creation' (step 7) highlighted in blue. The main content area is divided into two sections:

- Master Account Creation:** This section contains a form for 'Organization Details' and 'Admin User Credentials'.
 - Organization Details:** Fields include Organization Name (Master Tenant), Master Subdomain Name (master), Country Name (UK), State or Province Name (BE), Locality Name (Reading), Organizational Unit Name (IT), Support Email (frode.nilsen@deviceauthority.com), and Support Contact Number (123-123-1233).
 - Admin User Credentials:** Fields include Administrator Full Name (Frode Nilsen), Administrator Email (frode.nilsen@deviceauthority.com), and Administrator Password (masked).
- Review Master Account:** This section displays a summary of the 'Organization And Admin User Details' entered, including Master Account Number (224145632), Organization Name (Master Tenant), Administrator Full Name (Frode Nilsen), and Administrator Email (frode.nilsen@deviceauthority.com). It includes 'Back - Recreate Master Account' and 'Next' buttons.

At the bottom of the wizard, a footer contains the copyright information: 'Copyright © 2011 - 2017 Device Authority Ltd. All rights reserved. | Powered by Device Authority Setup Wizard 6.2.0 Build 108 | Support | Terms of Use | Device Authority'.

2.2.8.2 Tenant Account Creation

The Tenant Account is tied to the application(s) and/or service(s) you are protecting. Make note of the account information used here as well. The Tenant Sub-Domain Name will be used as the sub-domain when accessing the Management Control Panel, so choose something simple and easy to type. For example, you could use devtenant for the Tenant Account sub-domain name.

Note: The Master and Tenant email address used for administrator access can be the same.

The screenshot shows the 'Device Authority Setup Wizard' interface. On the left is a progress list with 12 steps: 1. Welcome ✓, 2. Database Configuration ✓, 3. Apache Kafka Configuration ✓, 4. KMS Deployment ✓, 5. KMS Message Queue Service Deployment ✓, 6. Memcached Configuration ✓, 7. Account Creation (highlighted in blue), 8. System License, 9. DAE Deployment, 10. Message Queue Service Deployment, 11. CP Deployment, 12. Setup Complete!

Tenant Account Creation

In this step, we'll create the **First Tenant Account** for the Device Authority Engine. The Tenant Account is tied to the application(s) and/or service(s) you are protecting. Make note of the account information used here as well. The Tenant Sub-Domain Name will be used as the sub-domain when accessing the Management Control Panel, so choose something simple and easy to type.

Note: The Master and Tenant email address used for administrator access can be the same.

Tenant Details

The following information will be used to represent the Tenant Account information.

Organization Name:

Tenant Subdomain Name:

Support Contact Number:

Admin User Credentials

In this section, you'll enter the Tenant Account's administrator credentials. With this information, you'll be able to link your device and access the Management Control Panel (CP) once deployed.

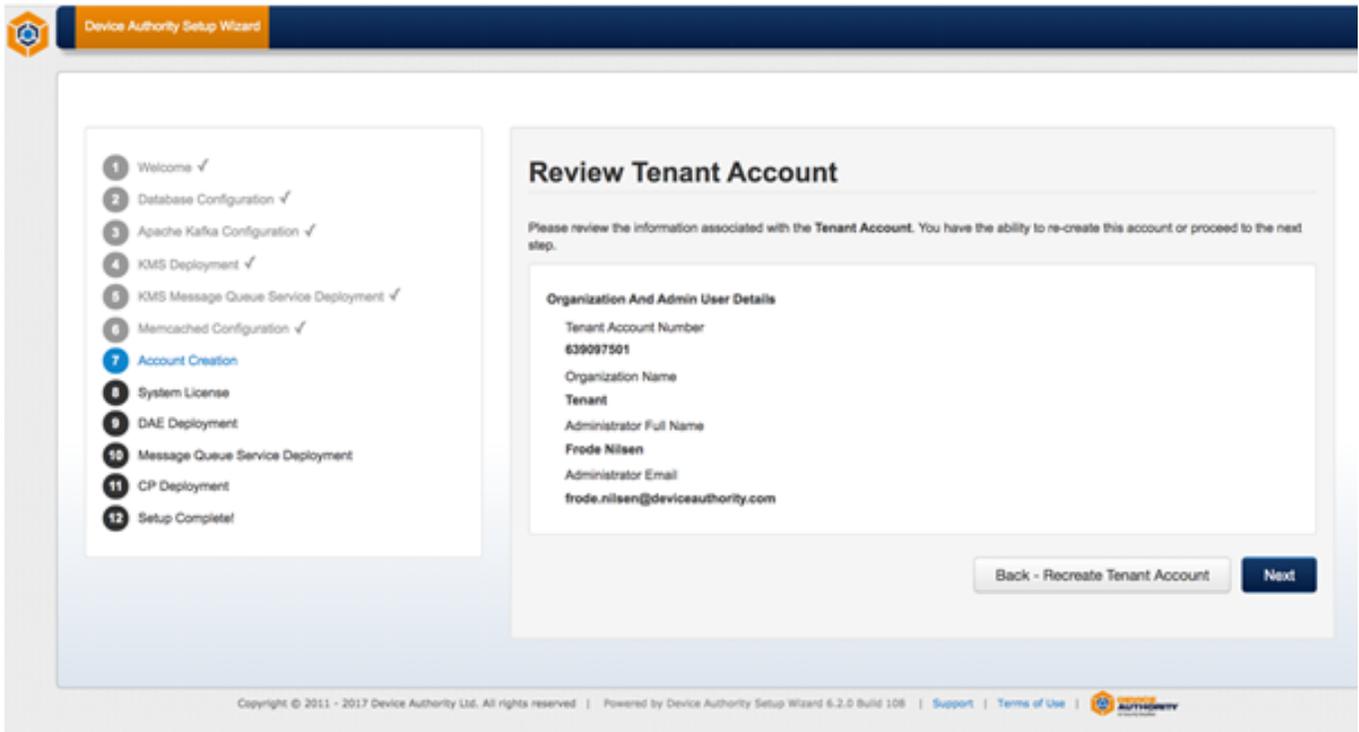
Administrator Full Name:

Administrator Email:

Administrator Password:

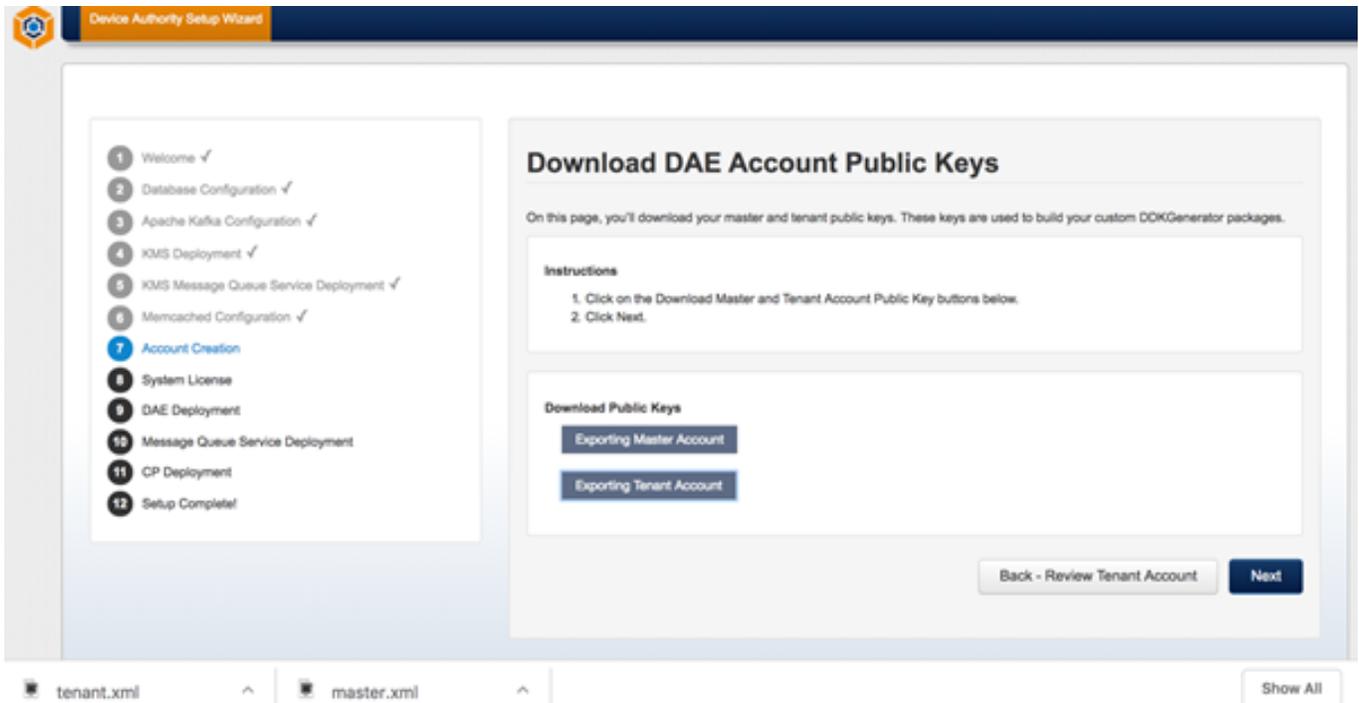
Show Characters

Take note of the email and password entered.
You'll use these credentials when you link your device for accessing the Control Panel (CP).



2.2.8.3 Download DAE Account Public Keys

In this step, you download your master and tenant public keys. These files (or ones created again in the future) will be used to build your custom DDKG generator packages. Click on the buttons to download the Public Key files. These xml files are not needed at this time. Then click Next to continue.



2.2.9 System License

2.2.9.1 Import System License

If you haven't already downloaded your system license, go to the Device Authority Customer Portal, Product License page and click the Download License button. Transfer the license file to your server.

1. Locate and open the license file using an editor. Copy the contents of the file.
2. Navigate back to the Wizard and paste it into the window provided. Then click Import System License.

If the import is successful, you will automatically proceed to the next step. If the import is unsuccessful, retry the copy/paste and make sure there are no missing nor extra characters copied.

WELCOME TO DEVICE AUTHORITY'S CUSTOMER PORTAL

Welcome, Frode Nilsen. We've provided the links below for easy access to the most common Customer Portal features.

- [Product License](#) – view license details or download your license file for use during installation.
- [Download Software](#) – download server-side software bits for your on-premise KeyScaler™ installation.
- [Request DDK Generators](#) – request customer-specific device key generators for your KeyScaler system. These device key generators are built to include the public PKI keys generated by your system. You must upload those keys to your customer portal account.



KeyScaler™ Customer Portal Manage Devices - Reports & Notification - Help -

PRODUCT LICENSE

Product License

On this page, you can view product license information.

[View License](#)

The following table shows your current account licensing information.

Organization	LAGOP54
Account Number	XXXXXXXXXX
Product Type	DAE
Tenancy	SINGLE
License Type	TRIAL
Last Renewed	11/07/2017 17:09:30
License Expires	03/29/2023 17:09:30

In CP Host field enter dae.keyscaler-672-001.com

- 1 Welcome ✓
- 2 Database Configuration ✓
- 3 Apache Kafka Configuration ✓
- 4 KMS Deployment ✓
- 5 KMS Message Queue Service Deployment ✓
- 6 Memcached Configuration ✓
- 7 Account Creation ✓
- 8 System License ✓
- 9 **DAE Deployment**
- 10 Message Queue Service Deployment
- 11 CP Deployment
- 12 Setup Complete!

DAE Configuration

In this step, we'll configure the database settings for the **Device Authority Engine (DAE)**.

Host Details

The hostname entered in the earlier Wizard step is shown below. Once deployed, the address will be used by CP instance via RESTful APIs. In the next step, we'll verify that the DAE is accessible from this address.

DAE Host

Database Details

For convenience, we have re-entered the database configuration settings in use by the Setup Wizard.

Host

Port

Leave blank to use default port 3306

Database Name

Username

Password

Show Characters

CP Host Details for SNMP

Please enter the hostname that you will be using for CP deployment. In most cases, this is the same hostname as your DAE hostname. Please enter the hostname without https:// prefix.

CP Host

2.2.10.3 Deployment

Copy the DAE ([service.war](#) file) to the tomcat webapps directory. Once deployed, click the [Check Status](#) button to verify the DAE has deployed successfully, and toggling the log viewer.

```
[root@ip-172-31-42-166 software]# cd /home/ec2-user/installer/software
```

```
[root@ip-172-31-42-166 software]# cp service.war /var/www/tomcat/webapps
```

Item 42 – Copy *service.war* file for deployment

The screenshot shows the 'Device Authority Setup Wizard' interface. On the left, a progress bar lists 12 steps, with '9 DAE Deployment' highlighted in blue. The main content area is titled 'DAE Deployment' and contains the following instructions:

Follow these instructions to deploy the DAE (*service.war*) and to verify that it's running properly:

Publish the DAE web application

- Using a session to your server, copy the service war file to the tomcat webserver:
`cp [path-to-download-location]/installer/software/service.war /var/www/tomcat/webapps`
- Verify the DAE is operational by toggling the Log Viewer and clicking the Check Status button.

Verify the DAE is operational

Common Check Status failure reasons:

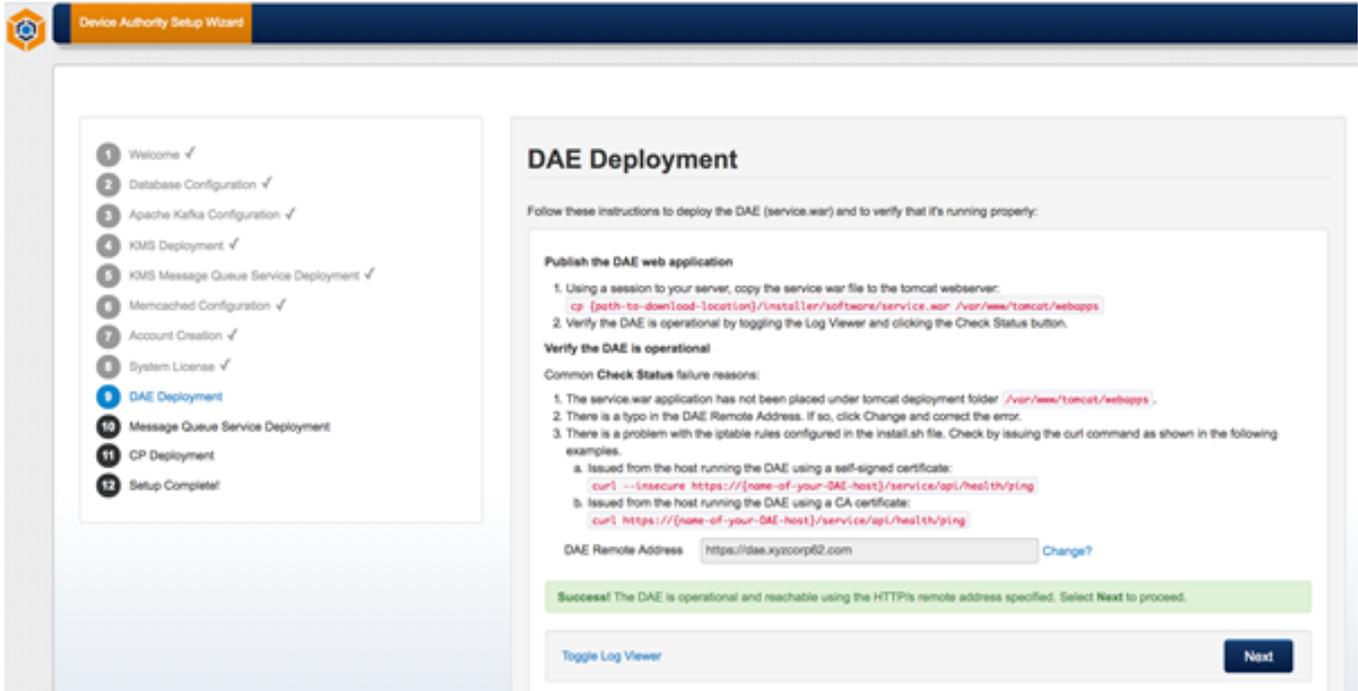
- The service.war application has not been placed under tomcat deployment folder `/var/www/tomcat/webapps`.
- There is a typo in the DAE Remote Address. If so, click Change and correct the error.
- There is a problem with the table rules configured in the install.sh file. Check by issuing the curl command as shown in the following examples.
 - Issued from the host running the DAE using a self-signed certificate:
`curl --insecure https://[name-of-your-DAE-host]/service/api/health/ping`
 - Issued from the host running the DAE using a CA certificate:
`curl https://[name-of-your-DAE-host]/service/api/health/ping`

DAE Remote Address [Change?](#)

[Toggle Log Viewer](#) [Check Status](#)

The following message indicates success:

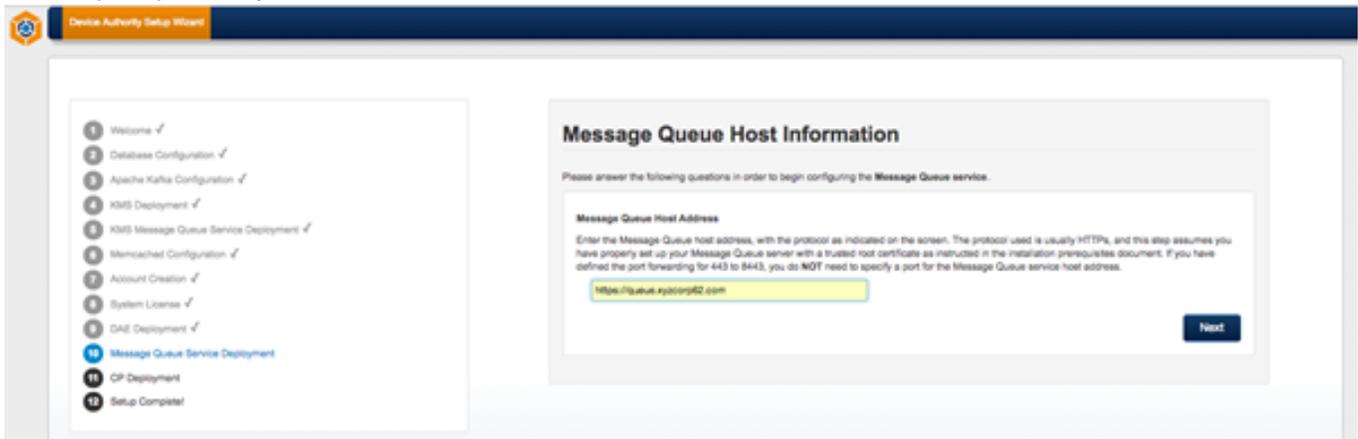
✔ Success! The DAE is operational and reachable using the HTTP/s remote address specified. Click **Next** to Proceed.



2.2.11 Message Queue Service Deployment

2.2.11.1 Message Queue Host Info

Enter <https://queue.keyscaler-672-001.com> and click **Next**



2.2.11.2 Deployment

```
[root@ip-172-31-42-166 software]# cd /home/ec2-user/installer/software
```

```
[root@ip-172-31-42-166 software]# cp keyscaler-services.war /var/www/tomcat/webapps
```

Item 46 – KeyScaler Server – Copy keyscaler-services.war for deployment

Click [Check Status](#)

The screenshot shows the 'Device Authority Setup Wizard' interface. On the left, a progress list shows steps 1 through 12, with step 10, 'Message Queue Service Deployment', highlighted in blue. The main content area is titled 'Message Queue Deployment' and contains instructions for deploying the message queue service. It includes a 'Publish the Messaging web application' section with two steps, a 'Verify the message queue is operational' section with common failure reasons, and a 'Message Queue Remote Address' input field containing 'https://queue.yzcorp62.com'. A 'Check Status' button is visible at the bottom right.

The following message indicates success:

✔ Success! The message queue is operational and reachable using the HTTP/s remote address specified. Click **Next** to Proceed.

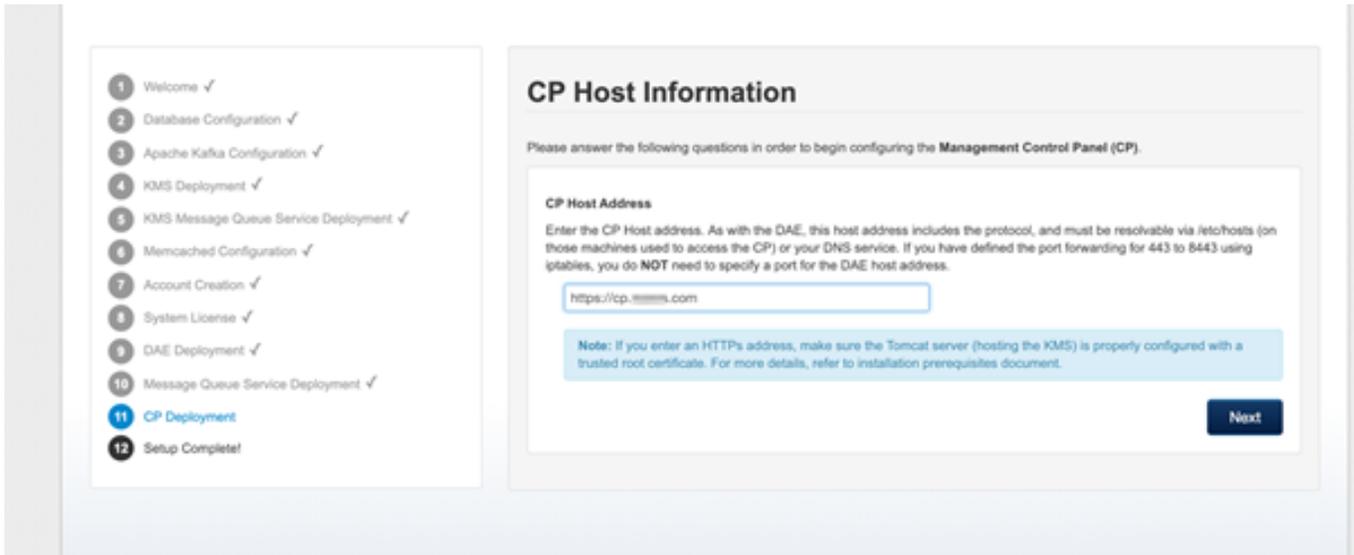
This screenshot shows the same 'Device Authority Setup Wizard' interface as the previous one, but with a green success message displayed in the main content area. The message reads: 'Success! The message queue is operational and reachable using the HTTP/s remote address specified. Select Next to proceed.' The 'Check Status' button has been replaced by a 'Next' button.

2.2.12 CP Deployment

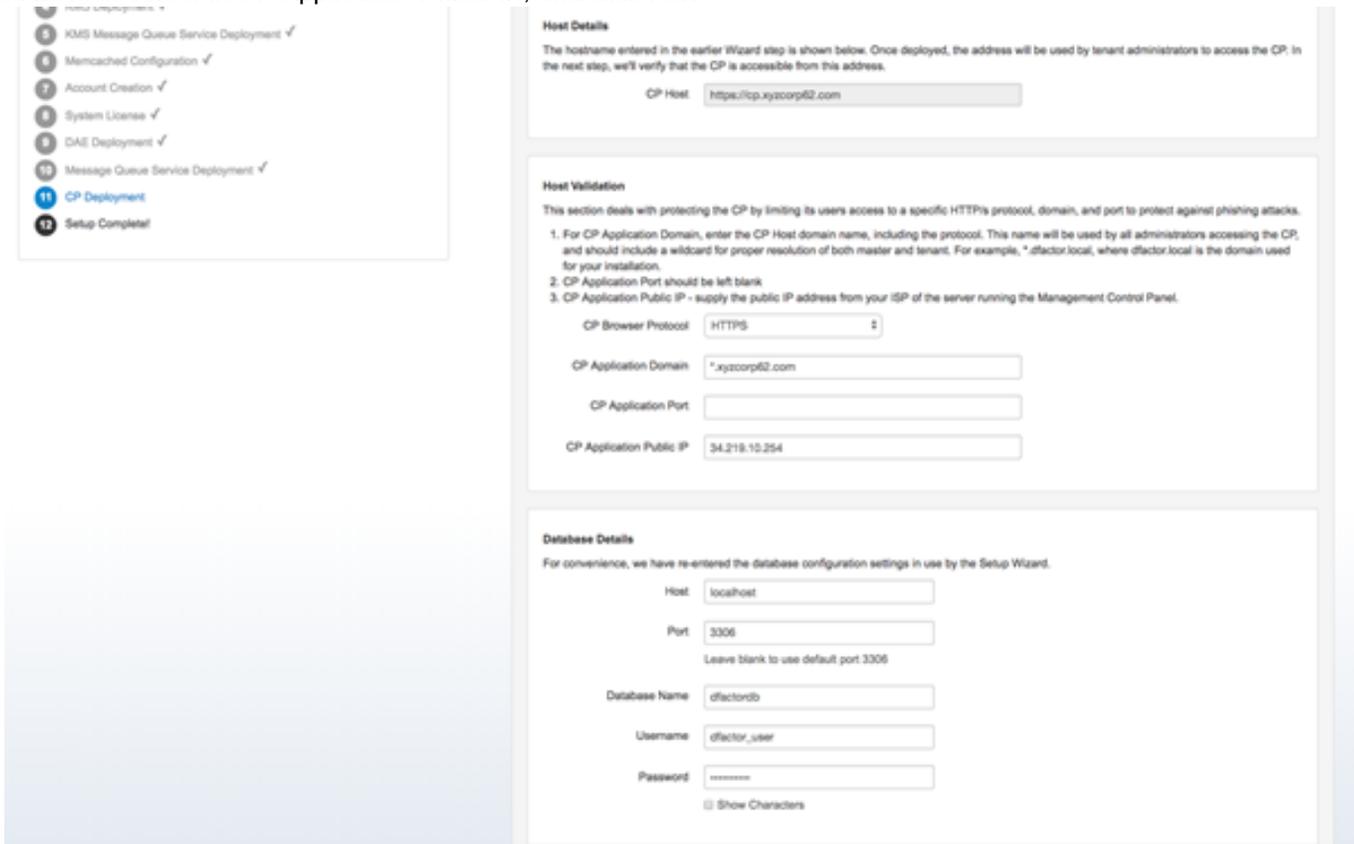
2.2.12.1 Configuration

Enter <https://cp.keyscalear-672-001.com> and click **Next**

The screenshot shows the top portion of the 'Device Authority Setup Wizard' interface, including the progress list on the left and the 'Device Authority Setup Wizard' header.



Enter the values as shown in example below (e.g. CP Application Domain: *.keyscaler-672-001.com) the IP address of server in CP Application Public IP, and click Next



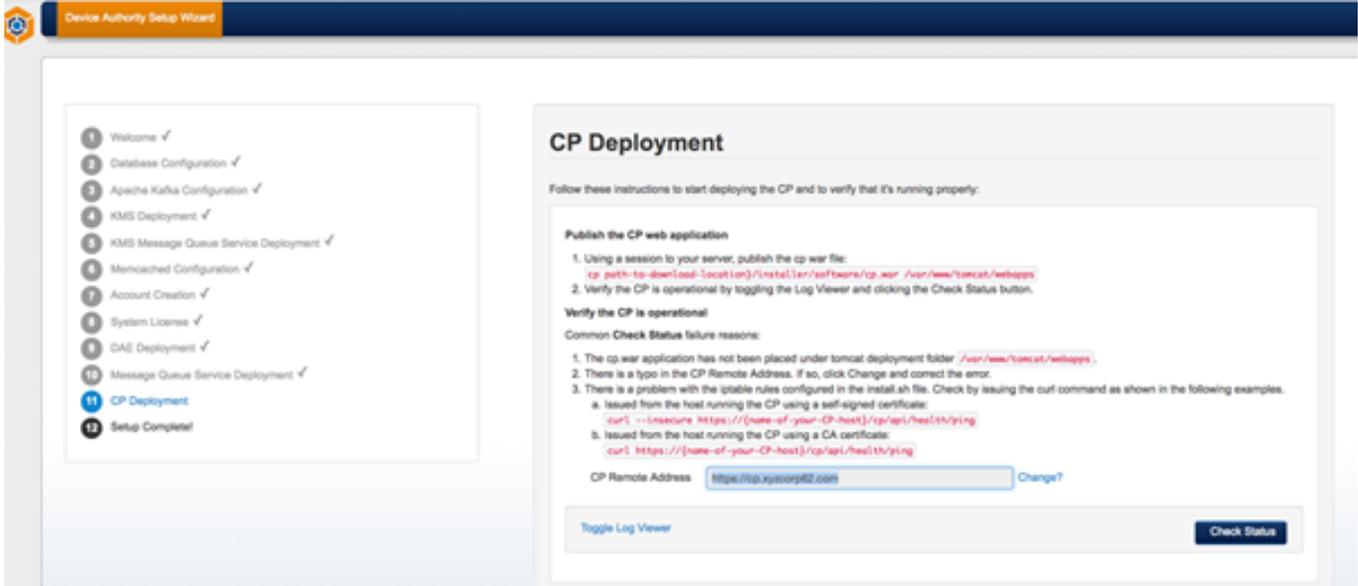
2.2.12.2 Deployment

Publish the cp.war by following the instructions in the Wizard. You'll be copying the file to your web application directory

```
[root@ip-172-31-42-166 software]# cd /home/ec2-user/installer/software
[root@ip-172-31-42-166 software]# cp cp.war /var/www/tomcat/webapps
```

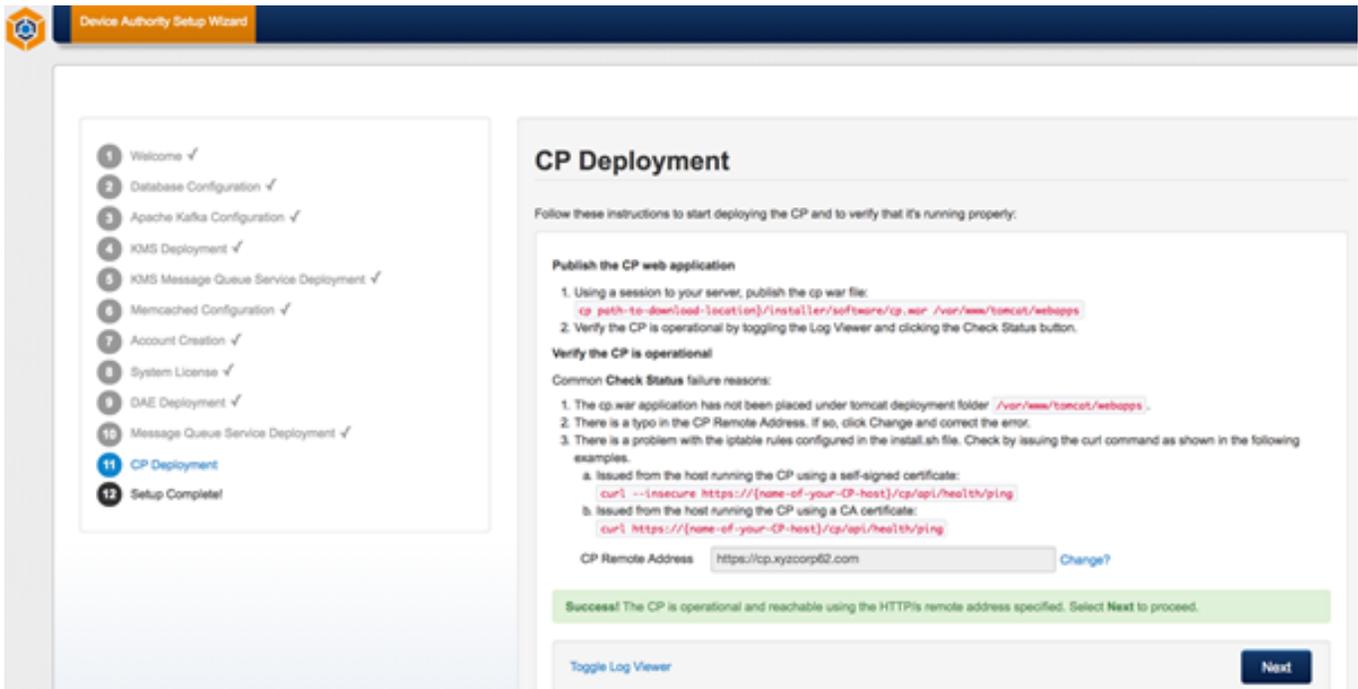
Item 51 KeyScaler Server – Copy cp.war for deployment

Once published, use the Wizard to verify the `cp.war` file has deployed properly by clicking **Toggle Log Viewer** and then **Check Status**.



The following message indicates success:

✓ Success! The CP is operational and reachable using the HTTP/s remote address specified. Click **Next** to Proceed.

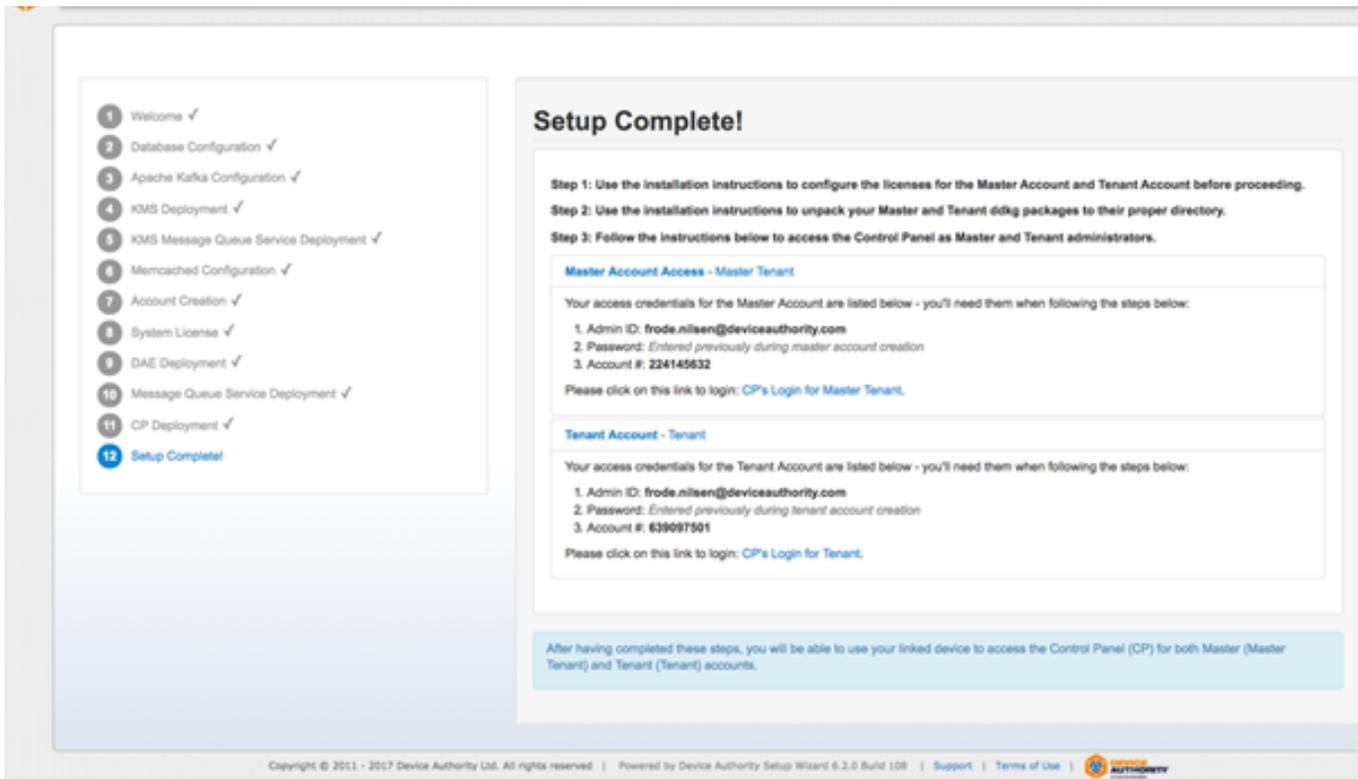


2.2.13 Setup Complete

⚠ Make sure you note down the Master Account and Tenant Account Numbers or leave the wizard page open as you will need this info in subsequent sections.

Next, please proceed with section 4.3 to configure license.





2.3 Configure Licenses

Licenses must be configured for the Master and Tenant Accounts that were created during installation. Licenses are configured using a menu-driven command-line license management tool (`na-tool.sh`) that is bundled with the DAE. Use the following steps to configure your licenses. Note: The steps outlined in this document must be executed on the server where DAE (`service.war`) was deployed and must be run as the `dfactor_user` user.

Below shows an example where there are 15 licenses available, where 5 are allocated for master account and the remaining 10 are allocated for tenant account. Your system will most likely have more than 15 licenses available for use, in which case the numbers you enter below is likely to differ from this example.

```
[root@ip-172-31-2-31 ec2-user]# su - dfactor_user
```

```
Last login: Mon Apr 23 10:13:30 UTC 2018 on pts/1
```

```
[dfactor_user@ip-172-31-2-31 ~]$
```

```
[dfactor_user@ip-172-31-42-166 conf]$ sh /var/www/tomcat/webapps/service/WEB-INF/classes/tools/bin/na-tool.sh
```

Running in DAE mode!

DAE Tool/

```
=====
```

1. Exit
2. Manage - DAE Master Account
3. Manage - DAE Tenant Account
4. Manage - DAE Account Licenses
5. Manage - DAE System License

- 6. Troubleshooting
- 7. DAE Update 6.1

Enter choice: [0 - 6]

3

DAE Tool/Manage - DAE Account Licenses/

=====

- 1. Exit
- 2. Configure - Master Account License
- 3. Configure - Tenant Account License
- 4. Display - Master Account License
- 5. Display - Tenant Account License

Enter choice: [0 - 4]

1

Enter number of registration seats for Master Account [Available 20]:

1

<PRESS ENTER>

Will attempt to create license with following information:

Account Number : 442338917
Licensed Product : DAE
Licensed Crypto Module : Yes
Licensed Credential Module : Yes
License Type : TRIAL
License Seat Type : TENANT_DEVICES
License Seat Limits : 1
Transaction Verification : Yes
Expiration (in days) : 51
Grace Period (in days) : 12

Please review the above information. If the information is correct then confirm to proceed [y/N]:

y

<PRESS ENTER>

DAE Tool/Manage - DAE Account Licenses/

- =====
1. Exit
 2. Configure - Master Account License
 3. Configure - Tenant Account License
 4. Display - Master Account License
 5. Display - Tenant Account License

Enter choice: [0 - 4]

2

Enter Tenant Account Number: *Plesase see Item 53 for where to find*

624842953

Enter number of registration seats for Tenant Account [Available 19]:

19

<PRESS ENTER>

Will attempt to create license with following information:

Account Number : 624842953

Licensed Product : DAE

Licensed Crypto Module : Yes

Licensed Credential Module : Yes

License Type : TRIAL

License Seat Type : TENANT_DEVICES

License Seat Limits : 19

Transaction Verification : Yes

Expiration (in days) : 51

Grace Period (in days) : 12

Please review the above information. If the information is correct then confirm to proceed [y/N]:

y

<PRESS ENTER>

DAE Tool/Manage - DAE Account Licenses/

- =====
1. Exit

2. Configure - Master Account License
3. Configure - Tenant Account License
4. Display - Master Account License
5. Display - Tenant Account License

Enter choice: [0 - 4]

0

DAE Tool/

=====

1. Exit
2. Manage - DAE Master Account
3. Manage - DAE Tenant Account
4. Manage - DAE Account Licenses
5. Manage - DAE System License
6. Troubleshooting
7. DAE Update 6.1

Enter choice: [0 - 6]

0

[dfactor_user@ip-172-31-19-187 ~]\$

Item 55 - Configure License

2.4 Deploy DDKGs

Ensure you have unzip installed

```
[root@ip]# yum install unzip -y
```

Item 56 - Install unzip utility

On the server running the Management Control Panel (CP), create a new directory as shown

```
[root@ ~]# mkdir /var/dfactor/data/cp-hosted-downloads
```

Item 57 - Create new directory

```
[root@ip-172-31-19-187 software]# cd /home/ec2-user/  
[root@ip-172-31-22-127 ec2-user]# chmod +x ddkg_setup.sh  
[root@ip-172-31-22-127 ec2-user]# ./ddkg_setup.sh  
<content omitted>  
Please enter Master Account Id: 454526887  
Please enter Tenant Account Id: 145293661  
[root@ip-172-31-22-127 ec2-user]#
```

Item 58 – Please find the account numbers in Item 53

2.5 CP Access

Note: Master and tenant host name must be resolvable by your DNS. The preferred method is to create DNS entries for each; however, you can also provide access by creating /etc/host entries on the desktop or laptop you'll use to access the CP.

Please note: You will need to replace the below domain name (keyscaler-672-001.com) to match your own domain name.

localhost name resolution is handled within DNS itself.

127.0.0.1 localhost

::1 localhost

54.186.32.181 master.keyscaler-672-001.com

54.186.32.181 tenant.keyscaler-672-001.com

Item 59 – Example of /etc/hosts file on your **local computer** that you will use to access the KeyScaler Control Panel.

2.5.1 Tenant Control Panel

Now you should be able to access CP via <https://tenant.keyscaler-672-001.com:8443/cp>

The screenshot shows the KeyScaler Control Panel interface. At the top, there is a navigation bar with the KeyScaler logo and the text "KeyScaler™ Control Panel Login". Below this is a large white box containing a "LOGIN" form. The form has two input fields: "Admin ID" with the placeholder text "Your email address" and "Password". Below the fields is a link that says "Can't access your account?" and a blue "Login" button. At the bottom of the page, there is a footer with copyright information: "Copyright © 2011 - 2018 Device Authority, Ltd. All rights reserved. | Powered by Device Authority 6.4.0 Build 336 | Support | Terms of Use | AUTHORITY".

Below the login form is the main dashboard area. It features a dark blue navigation bar with the KeyScaler logo and the text "KeyScaler™ Dashboard". The dashboard is divided into two main sections: "SYSTEM STATISTICS" and "RECENT SYSTEM EVENTS".

The "SYSTEM STATISTICS" section is titled "Provision A Device" and contains a table with the following data:

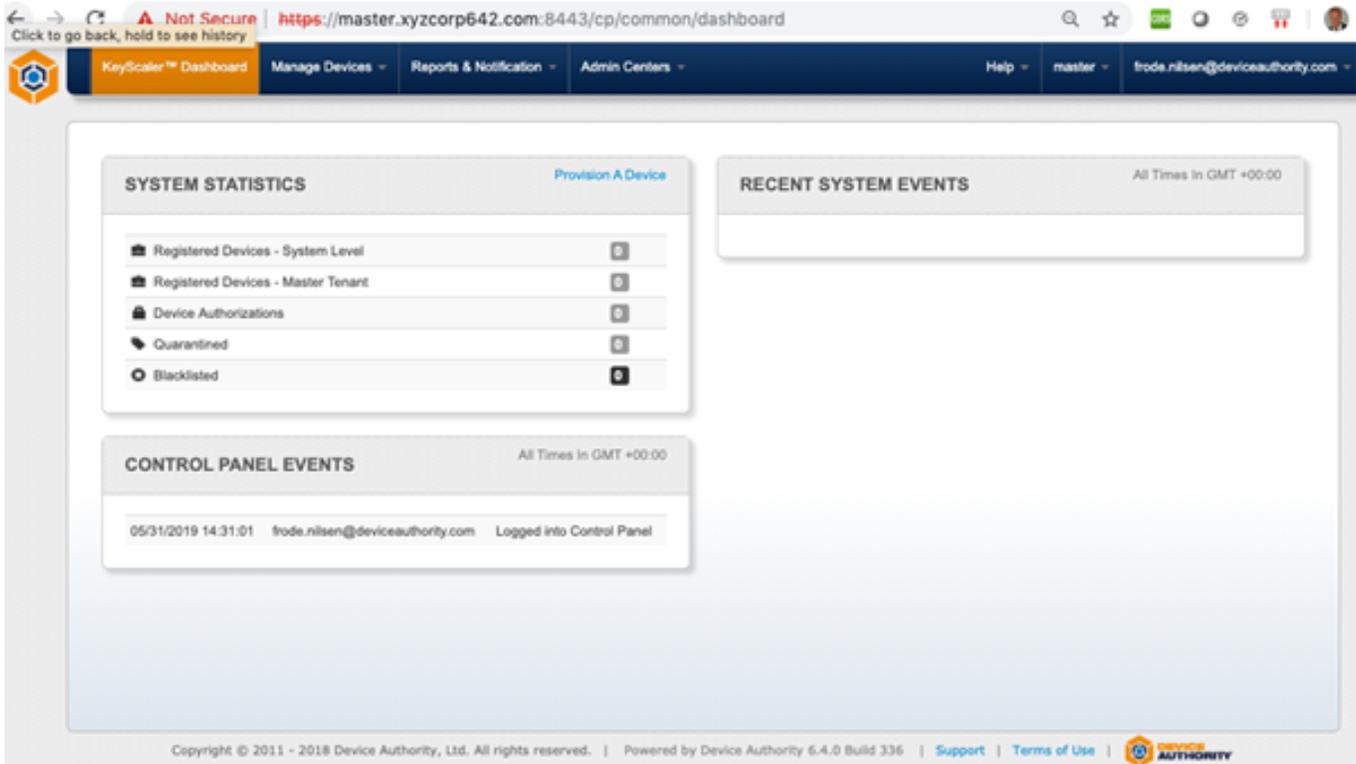
Category	Count
Registered Devices	0
Device Authorizations	0
Quarantined	0
Blacklisted	0

The "RECENT SYSTEM EVENTS" section is titled "All Times In GMT +00:00" and currently shows no events.



2.5.2 Master Control Panel

Login as with the tenant in previous section. <https://master.keyscaler-672-001.com:8443/cp/>



2.5.3 Post-installation activities

Next, there are some post-installation activities in section 6.2, which are necessary if you want to fully configure your system to handle notifications and configure outgoing emails etc. This can also be done at a later stage.

Next, we will proceed with the installation of the Service Access Controller in section 5, which is required to successfully register devices the KeyScaler System. E.g. a device will never communicate directly to the KeyScaler System, but only the Service Access Controller (SAC), which will take care of relaying the messages to KeyScaler.

3 Service Access Controller Installation

3.1 Overview

The Device Authority Service Access Controller (SAC) is a web application that provides an out-of-the-box management service for managed Device Authority Gateway Agents. It has been designed to keep external TCP/IP

traffic from ever connecting directly to internal infrastructure, such as the core Device Authority Engine API, or database instances. On a production environment the SAC should be installed on its own server, but it is possible to have the SAC running on the same server as that of the KeyScaler system (See 0)

3.2 Install on Same Server

Install the Service Access Controller on the same server on which the KeyScaler system was installed. Please use the instructions below to install the SAC on the same server used to run KeyScaler. On your KeyScaler server, change the directory to the installer directory in Item 62

3.2.1 Unpack the SAC Zip file

```
[root@ ~]# cd /home/ec2-user/installer/software
```

Item 63 - Change Directory

Unpack the sac.tar.gz file

```
[root@ ~]# tar -xvzf sac.tar.gz
```

Item 64 - Unpack the sac software package

3.2.2 Configure the SAC

Create sac.properties and copy the configuration shown in Item 65Item 90

```
[root@ip-172-31-22-20 ec2-user]# vi /var/dfactor/conf/sac.properties
```

Item 65 – Create sac.properties file with the content shown in Item 64

Add the following content shown in Item 65 the [sac.properties](#) file and update the the following values:

- [participantId](#) to be swapped with the **Tenant** value found in Control Panel Item 66
- [participant.secret](#) to be swapped with the **Tenant** value found in Control Panel Item 66
- [hostVerificationDomainPublicIP](#) to be swapped with the IP address of your server

```
deviceAuthenticationService=https://dae.keyscaler-672-001.com
multiTenancy=false
participantId=4132c7d2-6f21-4c74-ad93-8d5c4a7fcabe
participantSecret=65a24097-c97d-42b7-a45c-d09f092e5926
hostVerificationProtocol=https
hostVerificationDomain=sac.keyscaler-672-001.com
hostVerificationWildcardDomain =
hostVerificationDomainPublicIP=18.236.164.27
hostVerificationPort =
schedule.orders.new=800000000
schedule.orders.pending=800000000
schedule.orders.revoked=800000000
schedule.orders.renewal=1240000000
```

```
schedule.awsiot.new=864000000
schedule.awsiot.status=864000000
schedule.mpowers.new=864000000
```

Item 66 - sac.properties

The screenshot shows the KeyScaler™ Dashboard interface. The top navigation bar includes 'KeyScaler™ Dashboard', 'Manage Devices', 'Manage Policies', 'Reports & Notification', 'Help', and 'tenant'. A red arrow points to the 'Account Settings' menu item, which is expanded to show a list of options: 'Customize Account Logo', 'Manage Message Queue', 'Manage KeyScaler Cert Authorities', 'Manage Service Connectors', 'Manage Notifications', 'Manage Administrators', 'Manage Customer Accounts', 'Manage Authorization IDs', 'Manage Key Rotation', 'Product License', 'Manage DAE API Settings', 'Manage Device Attribute Feed', 'Manage IDP', 'Manage SP', and 'Download Software'. The main content area displays 'SYSTEM STATISTICS' with a 'Provision A Device' link, a table of device statuses (Registered, Device Authorizations, Quarantined, Blacklisted), and 'CONTROL PANEL EVENTS' showing a recent login event.

3.2.3 Deploy service-access-controller.war

```
[root@ip-172-31-22-20 ~]# cp service-access-controller.war /var/www/tomcat/webapps/
```

Item 69 – Deploy the service access controller to Tomcat

3.2.4 Restart the KeyScaler DFactor Service

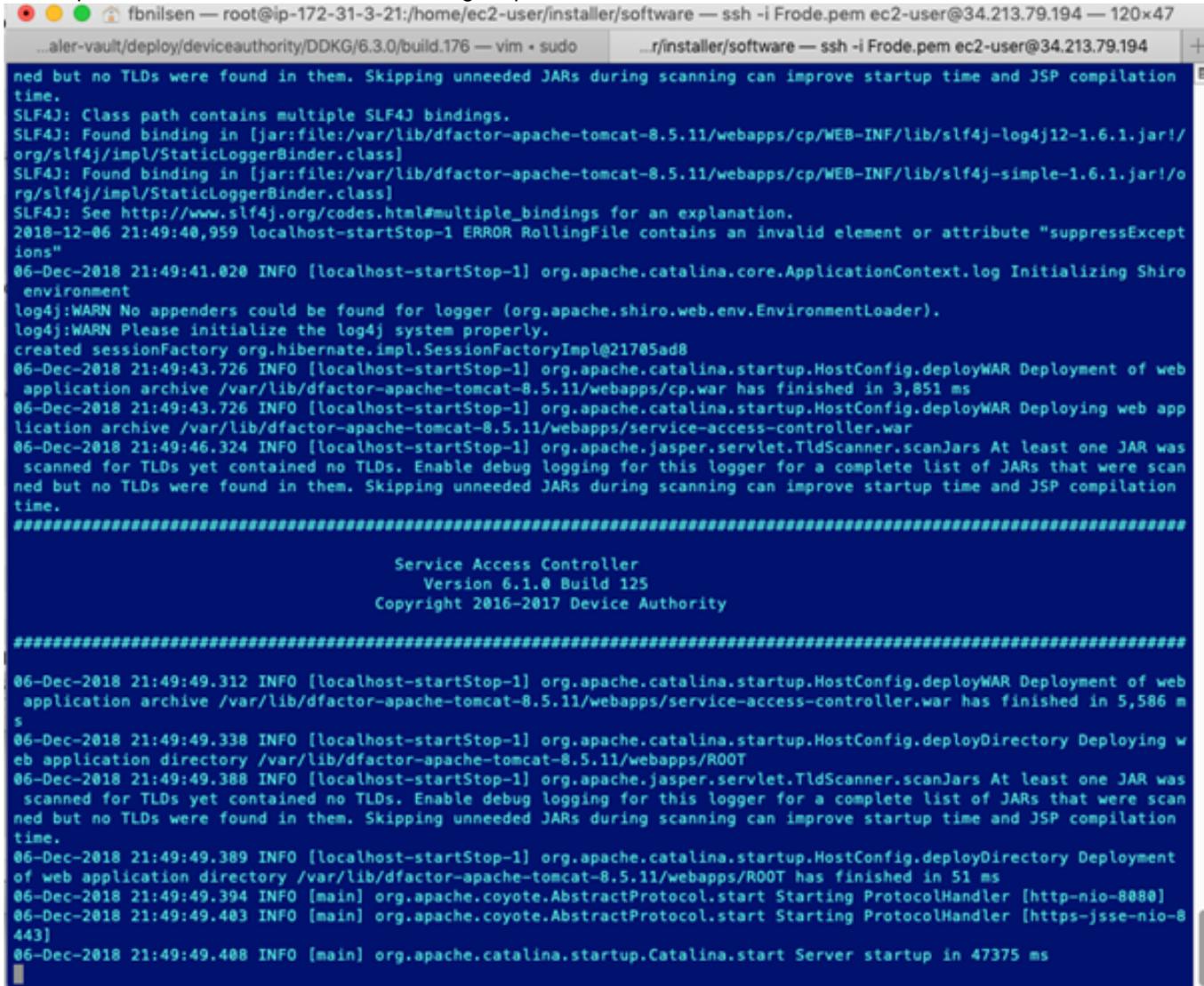
```
[root@ip-172-31-22-20 ~]# service dfactor restart
```

Item 70 - If the service is not running, start the service

```
[root@ip-172-31-22-20 ~]$ tail -f /var/www/tomcat/logs/catalina.out
```

Item 71 - Tail the catalina.out log file to make sure the service has started successfully. You should see output similar to the following:

The output should look similar to the following output:



```
ned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation
time.
SLF4J: Class path contains multiple SLF4J bindings.
SLF4J: Found binding in [jar:file:/var/lib/dfactor-apache-tomcat-8.5.11/webapps/cp/WEB-INF/lib/slf4j-log4j12-1.6.1.jar!/
org/slf4j/impl/StaticLoggerBinder.class]
SLF4J: Found binding in [jar:file:/var/lib/dfactor-apache-tomcat-8.5.11/webapps/cp/WEB-INF/lib/slf4j-simple-1.6.1.jar!/o
rg/slf4j/impl/StaticLoggerBinder.class]
SLF4J: See http://www.slf4j.org/codes.html#multiple_bindings for an explanation.
2018-12-06 21:49:40,959 localhost-startStop-1 ERROR RollingFile contains an invalid element or attribute "suppressExcept
ions"
06-Dec-2018 21:49:41,020 INFO [localhost-startStop-1] org.apache.catalina.core.ApplicationContext.log Initializing Shiro
environment
log4j:WARN No appenders could be found for logger (org.apache.shiro.web.env.EnvironmentLoader).
log4j:WARN Please initialize the log4j system properly.
created sessionFactory org.hibernate.impl.SessionFactoryImpl@21705ad8
06-Dec-2018 21:49:43,726 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web
application archive /var/lib/dfactor-apache-tomcat-8.5.11/webapps/cp.war has finished in 3,851 ms
06-Dec-2018 21:49:43,726 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deploying web app
lication archive /var/lib/dfactor-apache-tomcat-8.5.11/webapps/service-access-controller.war
06-Dec-2018 21:49:46,324 INFO [localhost-startStop-1] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was
scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scan
ned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation
time.
=====
Service Access Controller
Version 6.1.0 Build 125
Copyright 2016-2017 Device Authority
=====
06-Dec-2018 21:49:49,312 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deployment of web
application archive /var/lib/dfactor-apache-tomcat-8.5.11/webapps/service-access-controller.war has finished in 5,586 m
s
06-Dec-2018 21:49:49,338 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDirectory Deploying w
eb application directory /var/lib/dfactor-apache-tomcat-8.5.11/webapps/ROOT
06-Dec-2018 21:49:49,388 INFO [localhost-startStop-1] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was
scanned for TLDs yet contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scan
ned but no TLDs were found in them. Skipping unneeded JARs during scanning can improve startup time and JSP compilation
time.
06-Dec-2018 21:49:49,389 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployDirectory Deployment
of web application directory /var/lib/dfactor-apache-tomcat-8.5.11/webapps/ROOT has finished in 51 ms
06-Dec-2018 21:49:49,394 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler [http-nio-8080]
06-Dec-2018 21:49:49,403 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler [https-jsse-nio-8
443]
06-Dec-2018 21:49:49,408 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in 47375 ms
```

Item 72 - Tail the catalina.out log file to make sure the service has started successfully. You should see output similar to the above

3.2.5 Connectivity Test

Test connectivity from your laptop to the SAC by running following curl command from your laptop. A successful connection should return an HTTP 200 Status Code.

```
frodes-MBP-9:~ fbnilsen$ curl -k https://sac.keyscaler-672-001.com:8443/service-access-controller/health/ping
```

```
{"requestId":"72be70bc-2d1b-4b43-b77d-aed938816e80","responseTimestamp":1524687633452,"
httpCode":200,"statusCode":0,"message":null,"assets":[]}
```

frodes-MBP-9:~ fbnilsen\$

Item 73 – curl command connectivity test

Note: At this point you are done with the KeyScaler Installation and ready to register a device to sanity test the system.

3.3 Install SAC on Standalone Server

3.3.1 Pre-requisites

For a production environment it is recommended that the SAC is installed on a separate server. Please review the following documents to ensure you have met all the necessary hardware and software requirements for the Service Access Controller.

- <https://deviceauthority.zendesk.com/hc/en-us/articles/217078538-KeyScaler-Hardware-Requirements>
- <https://deviceauthority.zendesk.com/hc/en-us/articles/217078568>

Create a single dedicated Linux server instance and install and/or complete the following prerequisites.

3.3.1.1 Java Runtime Environment (JRE) 1.8

From oracle pages, download Java 8 as follows:

<http://www.oracle.com/technetwork/java/javase/downloads/jdk8-downloads-2133151.html>

Java SE Development Kit 8u172

You must accept the [Oracle Binary Code License Agreement for Java SE](#) to download this software.
Thank you for accepting the Oracle Binary Code License Agreement for Java SE; you may now download this software.

Product / File Description	File Size	Download
Linux ARM 32 Hard Float ABI	77.99 MB	jdk-8u172-linux-arm32-vfp-hflt.tar.gz
Linux ARM 64 Hard Float ABI	74.9 MB	jdk-8u172-linux-arm64-vfp-hflt.tar.gz
Linux x86	170.07 MB	jdk-8u172-linux-i586.rpm
Linux x86	184.91 MB	jdk-8u172-linux-i586.tar.gz
Linux x64	167.15 MB	jdk-8u172-linux-x64.rpm 
Linux x64	182.08 MB	jdk-8u172-linux-x64.tar.gz
Mac OS X x64	247.87 MB	jdk-8u172-macosx-x64.dmg
Solaris SPARC 64-bit (SVR4 package)	140.05 MB	jdk-8u172-solaris-sparcv9.tar.Z
Solaris SPARC 64-bit	99.35 MB	jdk-8u172-solaris-sparcv9.tar.gz
Solaris x64 (SVR4 package)	140.63 MB	jdk-8u172-solaris-x64.tar.Z
Solaris x64	97.06 MB	jdk-8u172-solaris-x64.tar.gz
Windows x86	199.11 MB	jdk-8u172-windows-i586.exe
Windows x64	207.3 MB	jdk-8u172-windows-x64.exe

Item 74 – Java Download

Right click on link in Item 73 and Copy Link Address to clipboard.

<http://download.oracle.com/otn-pub/java/jdk/8u191-b12/2787e4a523244c269598db4e85c51e0c/jdk-8u191-linux-x64.rpm>

```
[ec2-user@ip-172-31-40-78 ~]$ sudo yum install wget -y
```

Item 75 – Install package installer wget

Download Java using the URL copied above.

```
[ec2-user@ip-172-31-40-78 ~]$ sudo wget --header "Cookie: oraclelicense=accept-securebackup-cookie" http://download.oracle.com/otn-pub/java/jdk/8u191-b12/2787e4a523244c269598db4e85c51e0c/jdk-8u191-linux-x64.rpm
```

Item 76 - Get Java license

Install Java:

```
[ec2-user@ip-172-31-40-78 ~]$ sudo yum localinstall jdk-8u191-linux-x64.rpm
```

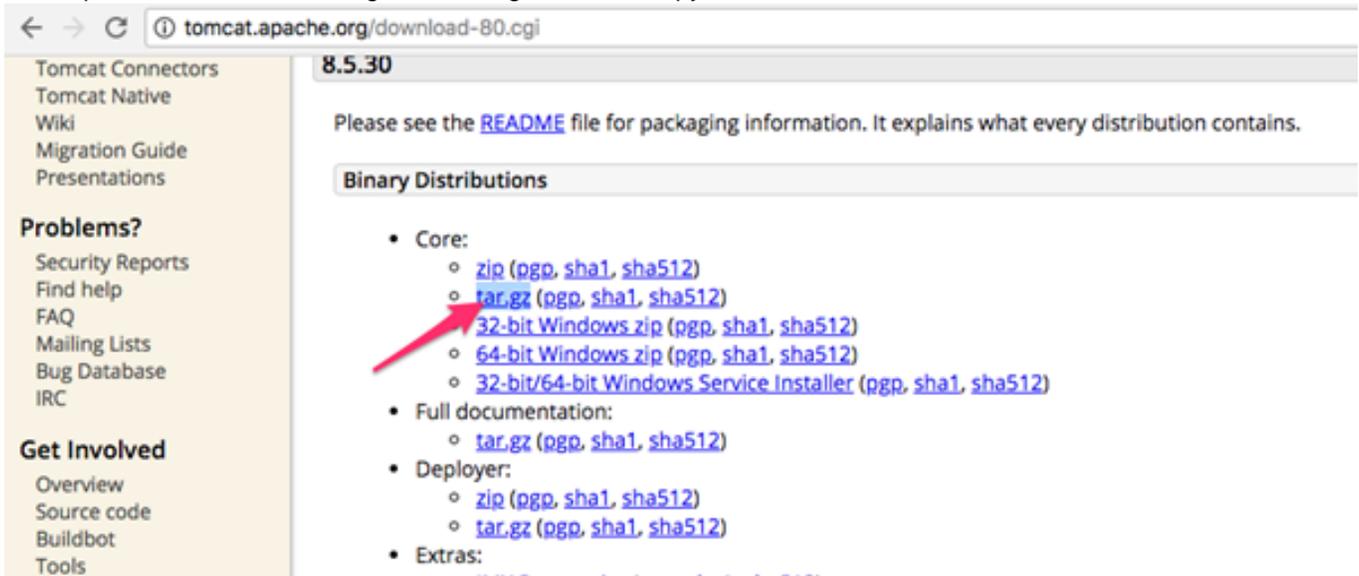
Item 77 - Install Java

```
[ec2-user@ip-172-31-26-184 ~]$ java -version
java version "1.8.0_191"
Java(TM) SE Runtime Environment (build 1.8.0_191-b12)
Java HotSpot(TM) 64-Bit Server VM (build 25.191-b12, mixed mode)
[ec2-user@ip-172-31-26-184 ~]$
```

Item 78 - Check Java version

3.3.1.2 Apache Tomcat 7

Go to apache tomcat site and right click tar.gz link and Copy Link Address.



The screenshot shows the Apache Tomcat 8.5.30 download page. The browser address bar shows the URL `tomcat.apache.org/download-80.cgi`. The page content includes a sidebar with navigation links like 'Tomcat Connectors', 'Wiki', and 'Problems?'. The main content area displays the version '8.5.30' and a message: 'Please see the [README](#) file for packaging information. It explains what every distribution contains.' Below this, there is a section titled 'Binary Distributions' with a bulleted list of download options. A red arrow points to the 'tar.gz' link under the 'Core' section.

- Core:
 - [zip \(pgp, sha1, sha512\)](#)
 - [tar.gz \(pgp, sha1, sha512\)](#)
 - [32-bit Windows zip \(pgp, sha1, sha512\)](#)
 - [64-bit Windows zip \(pgp, sha1, sha512\)](#)
 - [32-bit/64-bit Windows Service Installer \(pgp, sha1, sha512\)](#)
- Full documentation:
 - [tar.gz \(pgp, sha1, sha512\)](#)
- Deployer:
 - [zip \(pgp, sha1, sha512\)](#)
 - [tar.gz \(pgp, sha1, sha512\)](#)
- Extras:
 - [...](#)

```
[ec2-user@ip-172-31-40-78 ~]$ sudo wget http://www.mirrorservice.org/sites/ftp.apache.org/tomcat/tomcat-8/v8.5.34/bin/apache-tomcat-8.5.34.tar.gz
```

Item 80 - Get Apache tomcat software

```
[ec2-user@ip-172-31-40-78 ~]$ sudo tar -xvzf apache-tomcat-8.5.34.tar.gz
```

Item 81 - Install Apache tomcat

3.3.1.3 Communicating over HTTPS

Please see Section 3.3.1 in pre-requisites section

3.3.2 Install Instructions

Please use these instructions to install the SAC on a standalone server. These instructions are to be run as root unless otherwise instructed. For AWS instances, you'll need to issue the command `sudo su` to gain root access before beginning.

3.3.2.1 Transfer the Service Access Controller Package to Your Server

On your KeyScaler server, locate the installer, e.g. `/home/ec2-user/installer/software` (see Section - <https://deviceauthority.atlassian.net/wiki/spaces/DFACTORDOC/pages/2049376261#2.3.1--Unpack-downloaded-file>), locate the `sac.tar.gz` file and transfer it to your server. This document will assume `sac.tar.gz` is uploaded to the `/home/ec2-user` directory

3.3.2.2 Unpack the `sac.tar.gz` file

File Name	Date	Size	Type
keyscaler.software-6.2.tar.gz	21 Oct 2018 at 08:10	446.4 MB	gzip co...archive
keyscaler.software-6.2	Today at 10:29	463.9 MB	Folder
service.war	19 Oct 2018 at 00:32	66.7 MB	Java JAR file
sac.tar.gz	19 Oct 2018 at 00:34	76.5 MB	gzip co...archive
prereqs.tar.gz	19 Oct 2018 at 00:34	52.2 MB	gzip co...archive
kms.war	19 Oct 2018 at 00:34	53.6 MB	Java JAR file
kms-user.war	4 Oct 2018 at 22:56	50.6 MB	Java JAR file
keyscaler-services.war	4 Oct 2018 at 22:59	106.3 MB	Java JAR file
dfactor.tools.tar.gz	4 Oct 2018 at 23:09	27.8 MB	gzip co...archive
cp.war	19 Oct 2018 at 00:33	30.1 MB	Java JAR file

Item 82 - KeyScaler Server – Upload the following file to the SAC Server

```
$ scp -i <keyfile>.pem /Users/fbnilsen/Documents/ks6.2_2018-10-21/keyscaler.software-6.2/sac.tar.gz ec2-user@<SAC HOST>:/home/ec2-user
```

Item 83 – Local Computer – Upload the `sac.tar.gz` file to the SAC server

Unpacking this file will result in `service-access-controller.war`, which will be deployed shortly.

```
[root@ip-172-31-40-78 ec2-user]# cd /home/ec2-user
[root@ip-172-31-40-78 ec2-user]# tar -xvzf sac.tar.gz
service-access-controller.war
```

Item 84 - Unpack the SAC software

3.3.2.3 Create Service User

The Service Access Controller runs as an application within the Tomcat web service. To keep configuration consistent, create a service user for running Tomcat.

```
[root@ip-172-31-40-78 ec2-user]# groupadd tomcat
```

Item 85 – Tomcat group

Then create the new service user as a member of that new group:

```
[root@ip-172-31-40-78 ec2-user]# useradd -s /bin/bash -g tomcat dfactor_user
```

Item 86 – add user to tomcat group

3.3.2.4 Create Necessary Directories

There are a few directories that will need to be present to complete the service setup. Note the `/var/dfactor` directory may exist if a self-signed certificate was created in the KeyScaler Pre-requisites document.

```
[root@ip-172-31-40-78 ec2-user]# mkdir /var/www
[root@ip-172-31-40-78 ec2-user]# mkdir /var/dfactor
[root@ip-172-31-40-78 ec2-user]# mkdir /var/dfactor/conf
[root@ip-172-31-40-78 ec2-user]# mkdir /var/dfactor/logs
```

Item 87 – Create new directories

3.3.2.5 Copy Tomcat to /var/lib

```
[root@ip-172-31-40-78 ec2-user]# cp -r apache-tomcat-8.5.34 /var/lib/apache-tomcat-8.5.34
```

Item 88 - Copy tomcat software to /var/lib directory

3.3.2.6 Symbolic link

Create a symbolic link in the newly created `/var/www` directory to the Tomcat folder

```
[root@ip-172-31-40-78 ec2-user]# ln -s /var/lib/apache-tomcat-8.5.34/ /var/www/tomcat
```

Item 89 - Create symbolic link

3.3.2.7 Configure Tomcat and Service Access Controller

Create the configuration file that will be read by the Service Access Controller on service Startup. Note this file does not exist yet, so create it as shown next.

```
[root@ip-172-31-40-78 ec2-user]# vi /var/dfactor/conf/sac.properties
```

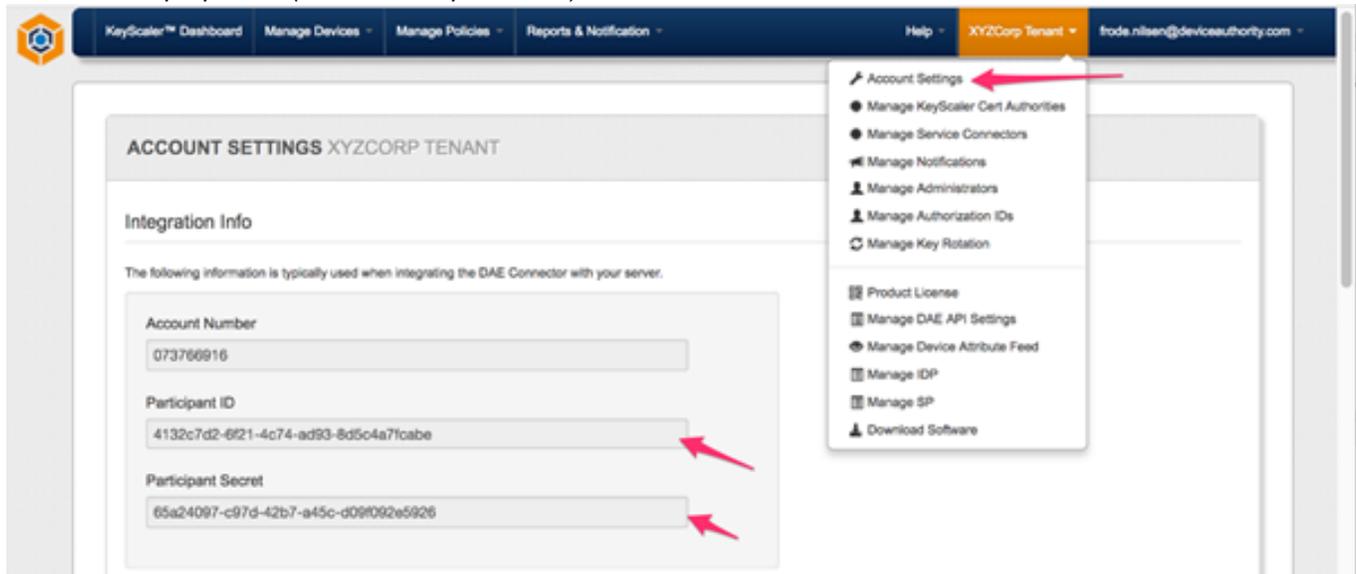
Item 90 – create sac.properties file

Copy/Paste the following example (Item 91) config into the file and fill out the details appropriate to your environment. For a basic provisioning system, the only properties that you would have to change to get up and running with a basic provisioning system are the bold properties. Use as a guideline for each parameter:

```
deviceAuthenticationService=https://dae.keyscaler-672-001.com
multiTenancy=false
participantId=4132c7d2-6f21-4c74-ad93-8d5c4a7fcabe
participantSecret=65a24097-c97d-42b7-a45c-d09f092e5926
hostVerificationProtocol=https
hostVerificationDomain=sac.keyscaler-672-001.com
hostVerificationWildcardDomain =
hostVerificationDomainPublicIP=18.236.164.27
hostVerificationPort =
schedule.orders.new=800000000
schedule.orders.pending=800000000
schedule.orders.revoked=800000000
```

```
schedule.orders.renewal=1240000000
schedule.awsiot.new=8640000000
schedule.awsiot.status=8640000000
schedule.mpowers.new=8640000000
```

Item 91 – *sac.properties* (relates to step: Item 66)



Item 92 – *participantId* and *participantSecret*

3.3.2.8 Install service-access-controller.war into Tomcat

The Service Access Controller application is deployed much like any other Tomcat web application. You can simply copy the .war file into the `$TOMCAT_HOME/webapps` directory, and it will auto-extract on service start.

```
[root@ip-172-31-40-78 ec2-user]# cd /home/ec2-user
[root@ip-172-31-40-78 ec2-user]# cp service-access-controller.war /var/www/tomcat/webapps
```

Item 93 - Copy SAC software to webapps directory

3.3.2.9 Set permissions

Remove write permissions for the core Tomcat directory

```
[root@ip-172-31-40-78 ec2-user]# chmod -R go-w /var/www/tomcat
```

Item 94 - Set Permissions

Change to the Tomcat directory and give ownership of the appropriate sub-directories to the service user that was created in Item 86.

```
[root@ip-172-31-40-78 ec2-user]# cd /var/www/tomcat
[root@ip-172-31-40-78 tomcat]# chown -R dfactor_user:tomcat webapps/ work/ temp/ logs/ conf/ bin/ lib/
[root@ip-172-31-40-78 tomcat]# chown -R dfactor_user:tomcat /var/dfactor
```

Item 95 - Change tomcat ownership

3.3.2.10 Configure Tomcat SSL Connector

At this stage, you have an SSL Certificate, and need to configure Tomcat to use it when sending/receiving traffic over SSL/HTTPS. Update the `server.xml` file to specify the name and location of your `p12` file along with the keystore password you supplied when creating the `p12` file.

Edit the file `/var/www/tomcat/conf/server.xml` and add the following connector definition

```
[root@ip-172-31-4-186 cert]# vi /var/www/tomcat/conf/server.xml
```

Item 96 - Edit server.xml file

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol"
    SSLEnabled="true"
    scheme="https"
    secure="true"
    clientAuth="false"
    sslProtocol="TLS"

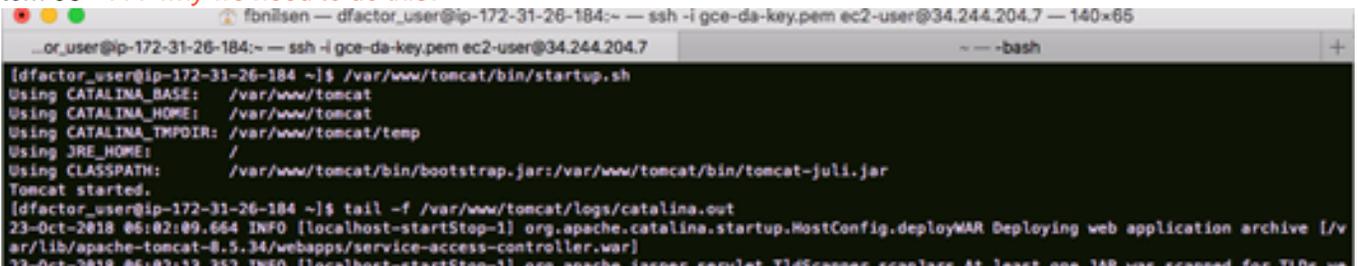
    maxHttpHeaderSize="8192"
    maxThreads="150"
    minSpareThreads="25"
    enableLookups="false"
    disableUploadTimeout="true"
    acceptCount="100"
    useBodyEncodingForURI="true"

    keystoreType="pkcs12"
    keystoreFile="/var/dfactor/cert/self_sign_certificate.p12"
    keystorePass="mypassword" />
```

Item 97 - server.xml

```
[root@ip-172-31-40-78 tomcat]# su - dfactor_user
[dfactor_user@ip-172-31-40-78 ~]$ /var/www/tomcat/bin/startup.sh
[dfactor_user@ip-172-31-40-78 ~]$ /var/www/tomcat/bin/shutdown.sh
[dfactor_user@ip-172-31-40-78 ~]$ tail -f /var/www/tomcat/logs/catalina.out
```

Item 98 - ??? why we need to do this?



```
...or_user@ip-172-31-26-184:~ ssh -i gce-da-key.pem ec2-user@34.244.204.7 - - - -bash
[dfactor_user@ip-172-31-26-184 ~]$ /var/www/tomcat/bin/startup.sh
Using CATALINA_BASE:   /var/www/tomcat
Using CATALINA_HOME:   /var/www/tomcat
Using CATALINA_TMPDIR: /var/www/tomcat/tem
Using JRE_HOME:        /
Using CLASSPATH:       /var/www/tomcat/bin/bootstrap.jar:/var/www/tomcat/bin/tomcat-juli.jar
Tomcat started.
[dfactor_user@ip-172-31-26-184 ~]$ tail -f /var/www/tomcat/logs/catalina.out
23-Oct-2018 06:02:09.664 INFO [localhost-startStop-1] org.apache.catalina.startup.HostConfig.deployWAR Deploying web application archive [/v
ar/lib/apache-tomcat-8.5.34/webapps/service-access-controller.war]
23-Oct-2018 06:02:13.352 INFO [localhost-startStop-1] org.apache.jasper.servlet.TldScanner.scanJars At least one JAR was scanned for TLDs ve
```

```
t contained no TLDs. Enable debug logging for this logger for a complete list of JARs that were scanned but no TLDs were found in them. Skip
ping unneeded JARs during scanning can improve startup time and JSP compilation time.
=====
Service Access Controller
Version 6.1.0 Build 125
Copyright 2016-2017 Device Authority
=====
23-Oct-2018 06:02:31.265 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployWAR Deployment of web application archive
[/var/lib/apache-tomcat-8.5.34/webapps/service-access-controller.war] has finished in [21,601] ms
23-Oct-2018 06:02:31.267 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deploying web application direc
tory [/var/lib/apache-tomcat-8.5.34/webapps/ROOT]
23-Oct-2018 06:02:31.277 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deployment of web application d
irectory [/var/lib/apache-tomcat-8.5.34/webapps/ROOT] has finished in [10] ms
23-Oct-2018 06:02:31.278 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deploying web application direc
tory [/var/lib/apache-tomcat-8.5.34/webapps/docs]
23-Oct-2018 06:02:31.291 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deployment of web application d
irectory [/var/lib/apache-tomcat-8.5.34/webapps/docs] has finished in [13] ms
23-Oct-2018 06:02:31.292 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deploying web application direc
tory [/var/lib/apache-tomcat-8.5.34/webapps/examples]
23-Oct-2018 06:02:31.433 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deployment of web application d
irectory [/var/lib/apache-tomcat-8.5.34/webapps/examples] has finished in [141] ms
23-Oct-2018 06:02:31.434 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deploying web application direc
tory [/var/lib/apache-tomcat-8.5.34/webapps/host-manager]
23-Oct-2018 06:02:31.448 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deployment of web application d
irectory [/var/lib/apache-tomcat-8.5.34/webapps/host-manager] has finished in [14] ms
23-Oct-2018 06:02:31.448 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deploying web application direc
tory [/var/lib/apache-tomcat-8.5.34/webapps/manager]
23-Oct-2018 06:02:31.467 INFO [localhost-startStop-1] org.apache.catalina.startup.MostConfig.deployDirectory Deployment of web application d
irectory [/var/lib/apache-tomcat-8.5.34/webapps/manager] has finished in [19] ms
23-Oct-2018 06:02:31.472 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["http-nio-8080"]
23-Oct-2018 06:02:31.478 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["https-jsse-nio-8443"]
23-Oct-2018 06:02:31.481 INFO [main] org.apache.coyote.AbstractProtocol.start Starting ProtocolHandler ["ajp-nio-8009"]
23-Oct-2018 06:02:31.483 INFO [main] org.apache.catalina.startup.Catalina.start Server startup in 21863 ms
```

Item 99 - Monitor logs catalina.out

3.3.3 DNS Entry

Note: In order for the SAC to communicate to KeyScaler, the following entry [34.212.224.67 dae.keyscaler-672-001.com](#) must be added to the `/etc/hosts` entry on the SAC server, where [34.212.224.67](#) is the IP Address of the KeyScaler system.

```
[ec2-user@ip-172-31-40-78 ~]$ cat /etc/hosts
```

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
34.212.224.67 dae.keyscaler-672-001.com
```

Item 100 - Edit Hosts file

3.3.4 Connectivity Tests

3.3.4.1 Curl from local computer to SAC

Note: The hostname [sac.keyscaler-672-001.com](#) in Item 101 needs to be resolvable by either an `/etc/hosts` entry on your local computer (Item 100) or a public DNS entry. If resolving by `/etc/hosts`, your hosts file will have the following entry, where [18.236.164.27](#) is the IP address of the SAC.

```
18.236.164.27 sac.keyscaler-672-001.com
```

Item 101 - Entry Hosts file

```
frodes-MBP-9:~ fbnilsen$ curl -k https://sac.keyscaler-672-001.com:8443/service-access-controller/health/ping
```

```
{"requestId":"b8f58d85-41cf-471f-9c5c-ab7f846cf59a","responseTimestamp":1524579718653,"httpCode":200,"statusCode":0,"message":null,"assets":[]}
```

```
frodes-MBP-9:~ fbnilsen$
```

Item 102 - curl from local Machine to SAC

3.3.4.2 Curl from SAC to KeyScaler

```
[ec2-user@ip-172-31-40-78 ~]$ curl -k https://dae.keyscaler-672-001.com:8443/service/api/health/ping  
{"req_id":"2d1e638f-4b1e-4260-b85c-019457a24f72","response_ts":1524580057004,"http_code":200,"  
status_code":0,"response_data":null}  
[ec2-user@ip-172-31-40-78 ~]$
```

Item 103 - curl from SAC to KeyScaler System

4 End to End Sanity Tests

End to end sanity test can be performed by installing and registering the [Credential Manager](#) Agent with the KeyScaler System.

4.1 Helpful Information

By default, CP access is allowed without device authentication. Instructions on enforcing CP access by device authentication are provided in the Control Panel User Guide.

Different DDKG plugins are used to access the Device Authority CP, your on-prem CP as a Master administrator and your on-prem CP as Tenant administrator. When each plugin is first used by the browser, you must allow the DDKG plugin to run in order to gain access to the CP. For Chrome users, you also need to install the Chrome DDKG Extension. The link will be provided on screen and is also available here.

4.2 Post-Installation Activities

Following the completion of the installation, there are some activities needed to configure your installation. These can be found here in the next sections.

4.2.1 Account Settings

4.2.1.1 General Settings

Change the time zone used to display alerts and data in the CP if desired.

4.2.1.2 Email URIs for PC Devices

On the Account Settings tab, supply the following URIs so administrators will receive well-formed links in the Administrator invite email to send when creating new administrators. The domain portion of the URI will have to be modified to match your environment. In the examples below, the domain for master CP access is [master.keyscaler-672-001.com](#) This domain was specified during the installation Wizard.

- Login URI: <https://master.xycorp62.com/cp/login>
- Registration URI: <https://master.keyscaler-672-001.com/cp/registerdevice>
- Download URI: <https://master.keyscaler-672-001.com/cp/downloadddkg>

4.2.1.3 Manage Notifications

(Optional) Customize the email templates used when sending out email notifications to CP administrators. In addition, you can control who will receive notifications on this page.

4.2.1.4 Configure Outgoing Mail

The Management Control Panel (CP) sends out emails for various notification purposes (invitations for new administrator access, alerts, etc.), and you'll need to set up the SMTP credentials for successful email delivery for both CP alerts and application alerts. To configure email, select Configure Outgoing Mail, and supply the requested parameters. Values appropriate for your installation can usually be obtained from your IT Operations department.

The following parameters are needed:

- Protocol
- Mail Server Host
- Server Port Number
- From Address
- TLS
- User Name
- Password

4.2.1.2 Manage Administrators

It is a good practice to have at least two administrators authorized to access the CP as Master Admin. Use the Manage Administrators tab to create a new Master CP admin. This feature can also be used to create administrators for your tenant(s) accounts, by selecting the appropriate Organization Name. This step should be done after SMTP has been set up and tested so the new administrators receive an email invitation with their credentials.

4.2.1.3 Tenant Account Setup

Following the installation of your DAE and CP, there are a few housekeeping steps to complete your installation. These functions are all found by accessing your CP tenant and going to the pull-down menu under the tenant name on the CP header.

4.2.1.3.1 Account Settings

URI Setup - for PC Devices

(Optional, and only needed if you are using device authentication for end-user application access.)

4.2.1.3.1.1 URI Setup - for PC Devices

(Optional, and only needed if you are using device authentication for end-user application access.)

On the Account Settings tab, supply the following URIs if email notifications are to be sent out from your application. These settings are needed so end-users will receive well-formed links in the invitations to register their devices. The domain portion of the URI will have to be modified to match your environment. In the examples below, the domain for tenant CP access is <https://mytenant.keyscaler-672-001.com>. This domain was specified during the installation Wizard.

- **Login URI:** <https://mytenant.keyscaler-672-001.com/cp/login>
- **Registration URI:** <https://mytenant.keyscaler-672-001.com/cp/registerdevic>
- **Download URI:** <https://mytenant.keyscaler-672-001.com/cp/downloadddkg>

4.2.1.4 Manage Notifications

When logged into the CP as a tenant admin, the notification templates are used when sending notifications generated by application (end-user or IoT device) access. These can be customized if desired.

In addition, you can control who will receive notifications on this page.

4.3.1.5 Manage Administrators

It is a good practice to have at least two administrators authorized to access the CP as Tenant Admins. Use the Manage Administrators tab to create a new Tenant CP admin. This step should be done after SMTP has been set up and tested so the new administrators receive an email invitation with their credentials.

4.2.1.6 Manage DAE API Settings

To increase the security of your system, you can limit the Extended API calls that will be accepted by your DAE by disabling those API calls not used. While developing your system, it is often useful to enable all extended APIs in your system, and then selectively disable unused APIs prior to deploying your production application.

4.2.2 Other Configuration Customization's

4.2.2.1 Blocking the Wizard from General Access

Once your system is installed, it is desirable to redirect anyone browsing to your KeyScaler server and make sure the Management Control Panel is loaded instead of the Installation Wizard. To do this, edit the file [/var/www/tomcat/webapps/ROOT/index.html](#) to contain only the following line:

```
<meta http-equiv="refresh" content="0;url=/cp/" />
```

4.2.2.2 Installing DFACTOR Tools

We provide a download package called DFACTOR tools which is available from the Software Section of the Customer Portal. This is a collection of useful scripts and programs. Use the instructions Deploying the D-FACTOR Tools to install the DFACTOR tools.

4.2.3 Master Account Setup

These functions are all found by accessing your master tenant and going to the pull-down menu under the tenant name on the CP header.

4.2.4 DAE And CP Configuration

Following the installation of your DAE and CP, there are a few housekeeping steps to complete your installation. These steps are separated by tasks to be performed as Master Account administrator and those to be performed as Tenant Account administrator.

4.2.5 KeyScaler-Securing Certs and Best Practice

The following are some of the best practices for securing certs in an production / operational environment.

4.2.5.1 Securing SAN Certs

The following commands can be executed as *root* user on the KeyScaler system to:

- Hide the SAN SSL [.pfx](#) cert
- Move the certs in [/var/dfactor/conf](#)

```
[root@ip-172-31-40-78 ~]$ chown dfactor_user:tomcat /var/dfactor/conf/.xxxcompany.crt  
[root@ip-172-31-40-78 ~]$ chmod 644 /var/dfactor/conf/.xxxcompany.crt
```

Item 104 – Hide SAN SSL certs

4.2.5.2 Keeping only the necessary certificates

It is also best practice to keep only the necessary certificates on the KeyScaler system. This can be achieved by moving the [CSR/private.key](#) from the production systems for safe keeping.

```
[root@ip-172-31-40-78 ~]$ chown user:group <path>.xxprivate.key
[root@ip-172-31-40-78 ~]$ chmod 400 <path>.xxprivate.key
```

Item 104 – Hide SAN SSL certs

These will be needed during renewal or conversion to .p12/.pfx format.

Also note: certain configuration (**.properties*) files may have a custom location. Please use the correct ownership.

4.3 Orientation to your KeyScaler System

This section describes key files, directories, users and commands useful for administering your KeyScaler system.

4.3.1 Database

KeyScaler uses a MySQL database. When the DAE or CP accesses the database, both programs use the database user [dfactor_user](#). In the DAE, KMS and CP Installation Prerequisites, it was recommended that you change the database passwords. Should you need to change these database passwords in the future, please contact customer support for instructions on how to change database passwords as they are stored in encrypted form in KeyScaler configuration files.

Default Database Name	Database Users
dfactordb	root, dfactor_use

Item 105 - dfactor Database Users

4.3.2 Linux User

The Linux user [dfactor_user](#) owns the KeyScaler web applications (DAE, KMS and CP). It is occasionally necessary to run certain KeyScaler programs and tools as the [dfactor_user](#). To do so, use the Linux "su" command as illustrated. Please use the - option to properly set environment variables for the [dfactor_user](#).

```
$ su - dfactor_user
```

Item 106 - Switch user to dfactor_user

4.3.1 Log files

The CP, DAE, KMS and Wizard create log files for normal operational and error messages. Depending on system activity, the DAE and CP log files can grow in size and may need to be periodically removed or archived to another server.

Program	Logfile Location and Name	Rotated Logfile Location
CP	/var/dfactor/logs/cp.log	/var/dfactor/logs/older/<yyyy-mm>
DAE	/var/dfactor/logs/dae.log	/var/dfactor/logs/<yyyy-mm>
KMS	/var/dfactor/logs/kms.log	no rotation needed
NA-Tools	/var/dfactor/logs/na-tools.log	no rotation needed
Install Wizard	/var/dfactor/logs/wizard.log	no rotation needed

Item 107 - KeyScaler Logs Files

To unzip log files that have been rotated and compressed use the `gunzip` utility. For example: `gunzip <filename>`

4.3.2 Tomcat

The Tomcat Web application creates its own logs in `/var/www/tomcat/logs`. The information contained in these logs are generally specific to Tomcat, and not the KeyScaler platform. These log files should be monitored periodically and archived if needed.

Tomcat Location	Tomcat Logfile Location
<code>/var/www/tomcat/webapps</code>	<code>/var/www/tomcat/logs/catalina.out</code> , and others

Item 108 - Tomcat Log File

4.3.3 Helpful Commands

4.3.3.1 Start KeyScaler

```
[root]# service dfactor start
```

Item 109 – starting the tomcat service

4.3.3.2 Stop KeyScaler

```
[root]# service dfactor stop
```

Item 110 – stopping the tomcat service

4.3.3.3 Check If KeyScaler is running

```
[root]# service dfactor status
```

Item 111 – check status of tomcat service

4.3.3.4 Run NA Tool - used to configure your KeyScaler license

```
[root]# su - dfactor_user
```

```
[dfactor_user]# sh /var/www/tomcat/webapps/service/WEB-INF/classes/tools/bin/na-tool.sh
```

Item 112 - Run na-tools utility

4.3.3.5 Check to see if KeyScaler is running via Browser

From a browser, issue the following commands from the [URL bar](#). Response will vary but should be similar to what is shown.

```
https://<url_of_your_keyscaler_server>/service/api/health/ping
```

```
{"req_id":"cbf6ffea-dbdd-4c82-a96b-7179a8ac1e21","response_ts":1498847206761,"http_code":200,"status_code":0,"response_data":null}
```

```
https://<url_of_your_keyscaler_server>/kms/api/health/ping
```

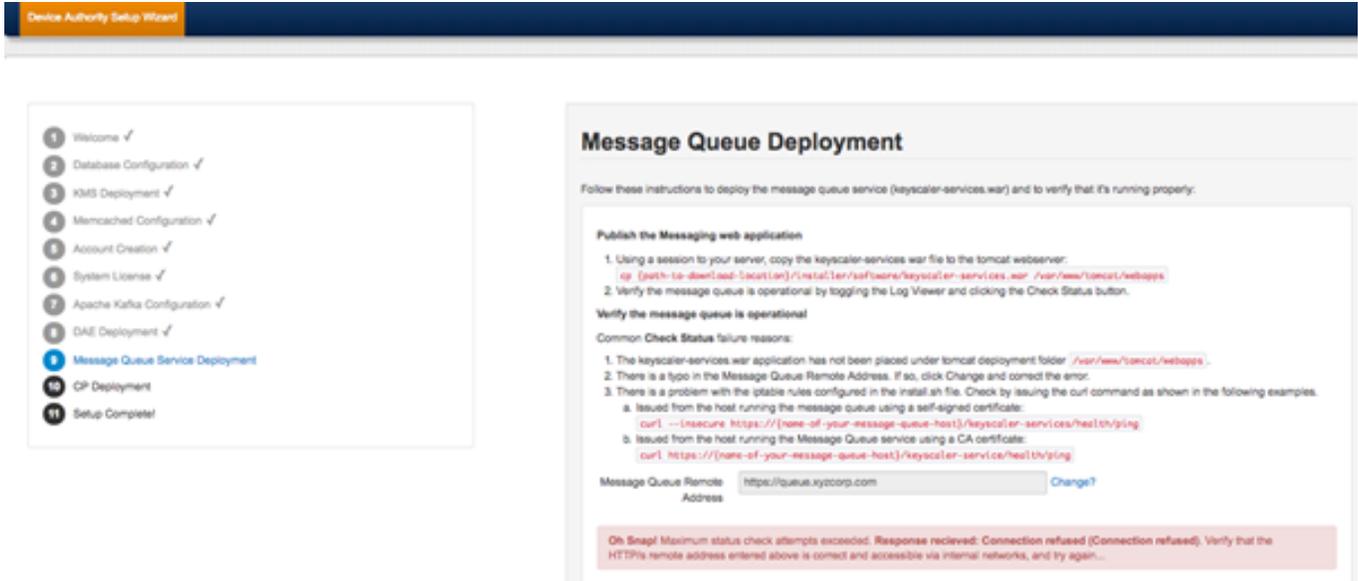
```
{"req_id":"f89dfd67-c444-4dbf-ad84-4fa27bbd3484","response_ts":1498846769391,"http_code":200,"status_code":10000}
```

Item 113 - Ping Connectivity Tests from Browser

4.4 Troubleshooting

4.4.1 Oh Snap! Maximum status check attempts exceeded

Oh Snap! Maximum status check attempts exceeded. Response received: Connection refused (Connection refused). Verify that the HTTP/s remote address entered above is correct and accessible via internal networks, and try again.



Device Authority Setup Wizard

- 1 Welcome ✓
- 2 Database Configuration ✓
- 3 XMS Deployment ✓
- 4 Memcached Configuration ✓
- 5 Account Creation ✓
- 6 System License ✓
- 7 Apache Kafka Configuration ✓
- 8 DAE Deployment ✓
- 9 **Message Queue Service Deployment**
- 10 CP Deployment
- 11 Setup Complete!

Message Queue Deployment

Follow these instructions to deploy the message queue service (keyscaler-services.war) and to verify that it's running properly:

Publish the Messaging web application

- Using a session to your server, copy the keyscaler-services.war file to the tomcat webserver:
`cp (path-to-download-location)/installer/software/keyscaler-services.war /var/www/tomcat/webapps`
- Verify the message queue is operational by logging the Log Viewer and clicking the Check Status button.

Verify the message queue is operational

Common Check Status failure reasons:

- The keyscaler-services.war application has not been placed under tomcat deployment folder `/var/www/tomcat/webapps`.
- There is a typo in the Message Queue Remote Address. If so, click Change and correct the error.
- There is a problem with the iptable rules configured in the install.sh file. Check by issuing the curl command as shown in the following examples.
 - Issued from the host running the message queue using a self-signed certificate:
`curl --insecure https://[name-of-your-message-queue-host]/keyscaler-services/health/ping`
 - Issued from the host running the Message Queue service using a CA certificate:
`curl https://[name-of-your-message-queue-host]/keyscaler-services/health/ping`

Message Queue Remote Address: [Change?](#)

Oh Snap! Maximum status check attempts exceeded. Response received: Connection refused (Connection refused). Verify that the HTTP/s remote address entered above is correct and accessible via internal networks, and try again...

4.3.1.1 Fix – Update hosts file

Ensure the **bold** entry is present in the hosts file.

```
[root@ip-172-31-42-166 software]# cat /etc/hosts
```

```
127.0.0.1 localhost localhost.localdomain localhost4 localhost4.localdomain4
```

```
::1 localhost localhost.localdomain localhost6 localhost6.localdomain6
```

```
127.0.0.1 kms.keyscaler-672-001.com
```

```
127.0.0.1 kafka.keyscaler-672-001.com
```

```
127.0.0.1 dae.keyscaler-672-001.com
```

```
127.0.0.1 queue.keyscaler-672-001.com
```

Item 115 - Hosts File

-----End of Document-----