# Keysight N8844A Data Analytics Web Service Software

Installation Guide

# Notices

## Manual Part Number

N8844-97008

## Edition

Fifth edition, April 2018

Available in electronic format only

Published by:
Keysight Technologies, Inc.
1900 Garden of the Gods Road
Colorado Springs, CO 80907 USA

## Print History

N8844-97003, May 2017

N8844-97005, May 2017

N8844-97006, July 2017

N8844-97007, January 2018

N8844-97008, April 2018

## Warranty

**The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Keysight disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Keysight shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Keysight and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.**

## Technology License

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

## U.S. Government Rights

The Software is "commercial computer software," as defined by Federal Acquisition Regulation ("FAR") 2.101. Pursuant to FAR 12.212 and 27.405-3 and Department of Defense FAR Supplement ("DFARS") 227.7202, the U.S. government acquires commercial computer software under the same terms by which the software is customarily provided to the public. Accordingly, Keysight provides the Software to U.S. government customers under its standard commercial license, which is embodied in its End User License Agreement (EULA), a copy of which can be found at www.keysight.com/find/sweula. The license set forth in the EULA represents the exclusive authority by which the U.S. government may use, modify, distribute, or disclose the Software. The EULA and the license set forth therein, does not require or permit, among other things, that Keysight: (1) Furnish technical information related to commercial computer software or commercial computer software documentation that is not customarily provided to the public; or (2) Relinquish to, or otherwise provide, the government rights in excess of these rights customarily provided to the public to use, modify, reproduce, release, perform, display, or disclose commercial computer software or commercial computer software documentation. No additional government requirements beyond those set forth in the EULA shall apply, except to the extent that those terms, rights, or licenses are explicitly required from all providers of commercial computer software pursuant to the FAR and the DFARS and are set forth specifically in writing elsewhere in the EULA. Keysight shall be under no obligation to update, revise or otherwise modify the Software. With respect to any technical data as defined by FAR 2.101, pursuant to FAR 12.211 and 27.404.2 and DFARS 227.7102, the U.S. government acquires no greater than Limited Rights as defined in FAR 27.401 or DFAR 227.7103-5 (c), as applicable in any technical data.

## Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

**A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.**

# Contents

1 Installation

Installing the N8844A Data Analytics Web Service Software / 6

Accessing the N8844A Web Service locally / 15

Accessing the N8844A Web Service remotely / 16

2 Using Keysight Cloud Services (KCS)

Accessing the Administrator Console / 18

Configuring the Cloud System / 20
- Authentication provider / 20
- Adding an OIDC provider / 20
- Adding an LDAP provider / 21
- Email server / 22

Working with Applications / 24

Setting Up Users / 25
- How it works / 25
- Creating a user account / 25
- Managing CoreAdmin rights / 26
- Resetting a password / 26
- Creating a service account / 27
- Managing service accounts / 27

Manage Roles / 28
- Role definitions / 28
- Assigning Roles / 29

Monitoring the System / 31

Index

# 1 Installation

Installing the N8844A Data Analytics Web Service Software / 6
Accessing the N8844A Web Service locally / 15
Accessing the N8844A Web Service remotely / 16

This guide describes installing the N8844A Data Analytics Web Service Software on a PC.

The software requires a PC with these characteristics:

- OS: Windows Desktop 64-bit (Windows 7 or Windows 10)
- Memory: 8G minimum
- Performance: Quad core minimum
- HDD Size: 500 GB minimum
- One of these browsers:
    - Internet Explorer 11
    - Chrome
    - Firefox

When you install the N8844A Data Analytics Web Service Software on your PC, it works as a self-hosted server, and you can access the Database locally on your web browser using localhost in the URL.

When you install the N8844A Data Analytics Web Service Software on a PC that you may be accessing remotely, you can access the Database remotely on your web browser using the IP address of the remote PC in the URL.

After you purchase the N8844A Data Analytics Web Service Software from Keysight, you shall be provided the web link to download the installer file.

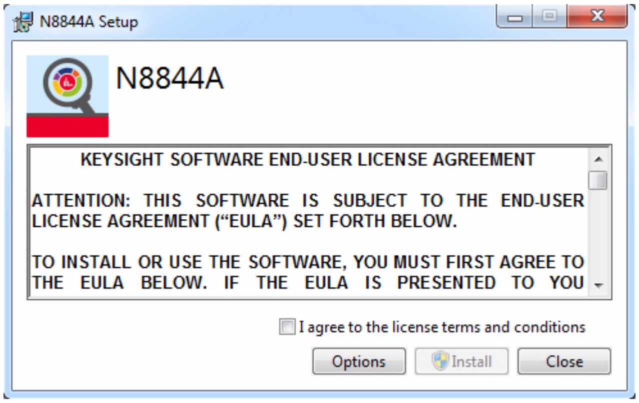
## Installing the N8844A Data Analytics Web Service Software

Perform the following steps to install the N8844A Software on a PC.

1 Download the installer file from the provided Keysight web URL to the PC.

2 Double-click the installer icon for N8844A to begin installing the software.

The KEYSIGHT SOFTWARE END-USER LICENSE AGREEMENT window is displayed.



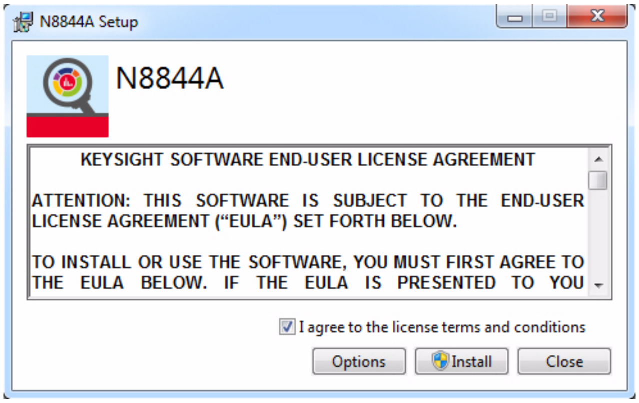
KEYSIGHT SOFTWARE END-USER LICENSE AGREEMENT

ATTENTION: THIS SOFTWARE IS SUBJECT TO THE END-USER LICENSE AGREEMENT (“EULA”) SET FORTH BELOW.

TO INSTALL OR USE THE SOFTWARE, YOU MUST FIRST AGREE TO THE EULA BELOW. IF THE EULA IS PRESENTED TO YOU

□ I agree to the license terms and conditions

3 Select the check-box for **I agree to the license terms and conditions**. The **Install** button gets enabled.



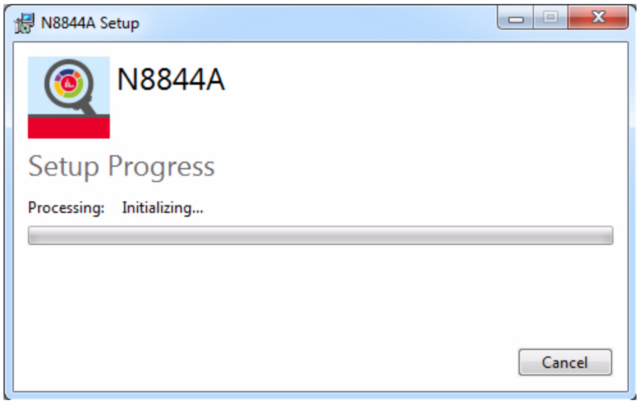
KEYSIGHT SOFTWARE END-USER LICENSE AGREEMENT

ATTENTION: THIS SOFTWARE IS SUBJECT TO THE END-USER LICENSE AGREEMENT (“EULA”) SET FORTH BELOW.

TO INSTALL OR USE THE SOFTWARE, YOU MUST FIRST AGREE TO THE EULA BELOW. IF THE EULA IS PRESENTED TO YOU

☑ I agree to the license terms and conditions

4 Click **Install** to begin installing the N8844A Software. The progress window is displayed.



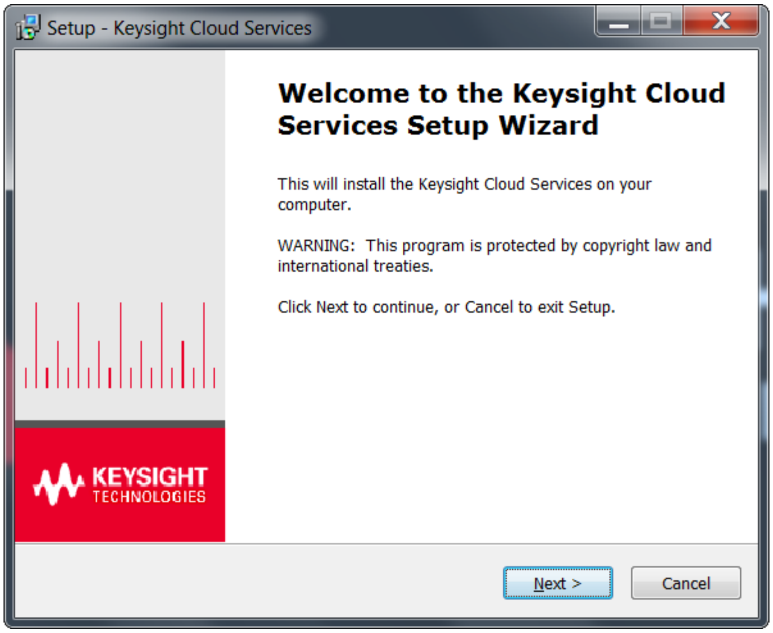
Setup Progress

Processing: Initializing...

5 The first part of the N8844A software installation is the installation of Keysight Cloud Services (KCS) for Windows.

Keysight Cloud Services (KCS) is a framework that provides core services for cloud-based applications, such as authentication, authorization, and licensing (although the N8844A Data Analytics Web Service Software does not use the KCS licensing).

On the Keysight Cloud Services Setup Wizard screen, click **Next** to read the user License Agreement.



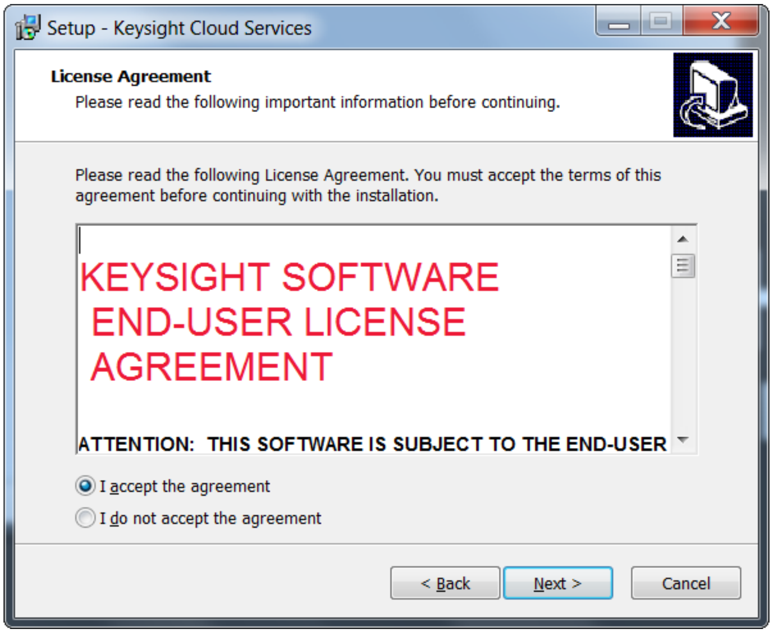
Welcome to the Keysight Cloud Services Setup Wizard

This will install the Keysight Cloud Services on your computer.

WARNING: This program is protected by copyright law and international treaties.

Click Next to continue, or Cancel to exit Setup.

6 On the License Agreement screen, accept the agreement and click **Next** to specify the installation location.



**License Agreement**

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

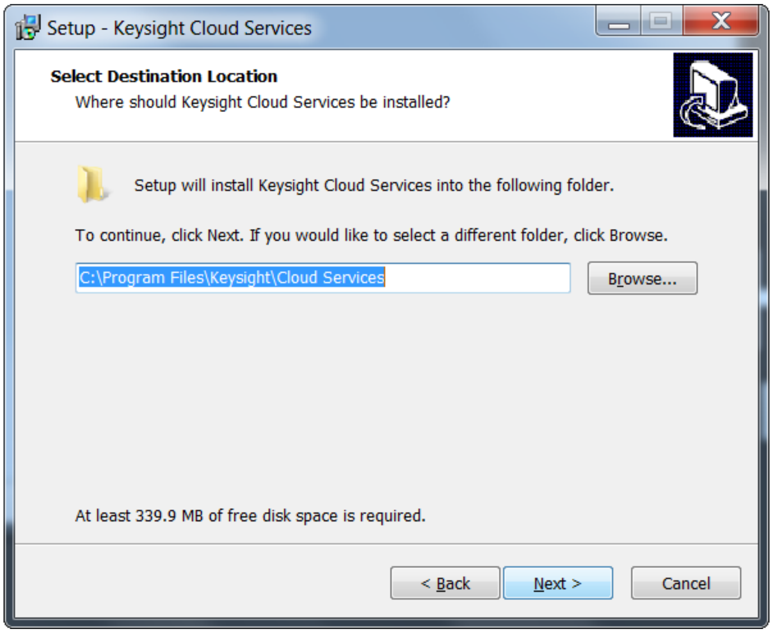
KEYSIGHT SOFTWARE END-USER LICENSE AGREEMENT

ATTENTION: THIS SOFTWARE IS SUBJECT TO THE END-USER

● I accept the agreement

○ I do not accept the agreement

7 On the Select Destination Location screen, you can either click **Browse** to change the installation location or click **Next** to install KCS at *C:\Program Files\Keysight\Cloud Services*, which is the default location.



**Select Destination Location**

Where should Keysight Cloud Services be installed?

Setup will install Keysight Cloud Services into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\Keysight\Cloud Services

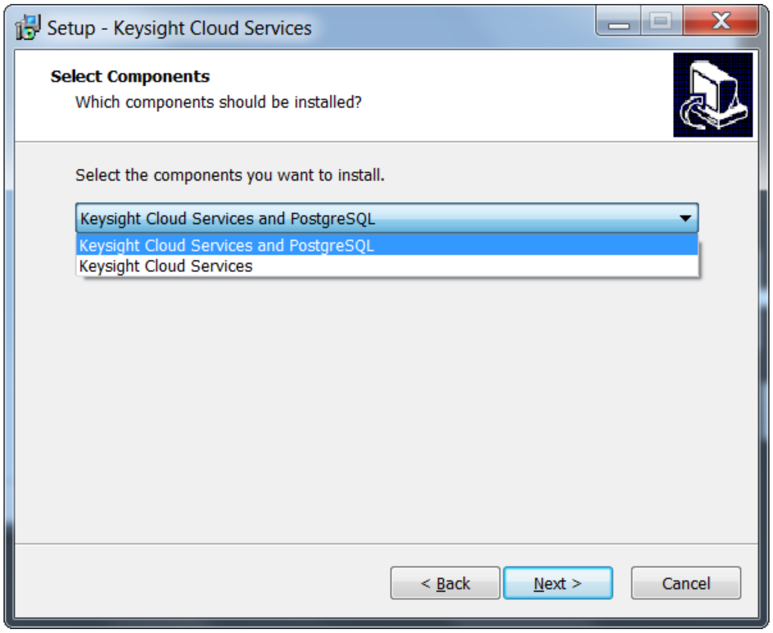
At least 339.9 MB of free disk space is required.

8 On the Select Components screen, select either of the following and click **Next**:

- **Keysight Cloud Services and PostgreSQL** when PostgreSQL is not installed on your machine.

- **Keysight Cloud Services** when PostgreSQL is already installed on your machine.

NOTE The PostgreSQL database is used to store session information, registered applications, and access credentials for the local database.



Setup - Keysight Cloud Services

**Select Components**

Which components should be installed?

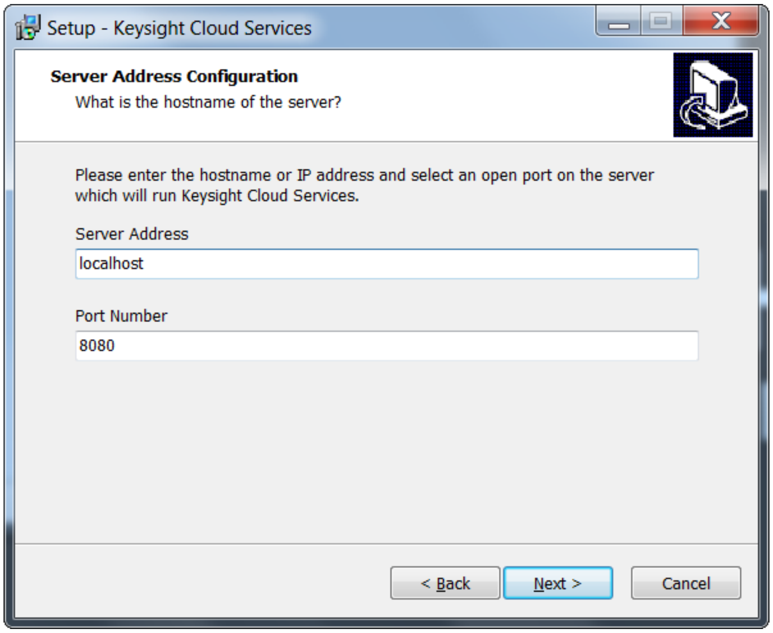
Select the components you want to install.

Keysight Cloud Services and PostgreSQL

Keysight Cloud Services and PostgreSQL
Keysight Cloud Services

9 On the Server Address Configuration screen, specify the **Server Address** (hostname/IP address) and **Port Number** to run Keysight Cloud Services, and click **Next**.

This is the browser URL to access the server interface and the value needed by other components to access the KCS server.



**Server Address Configuration**

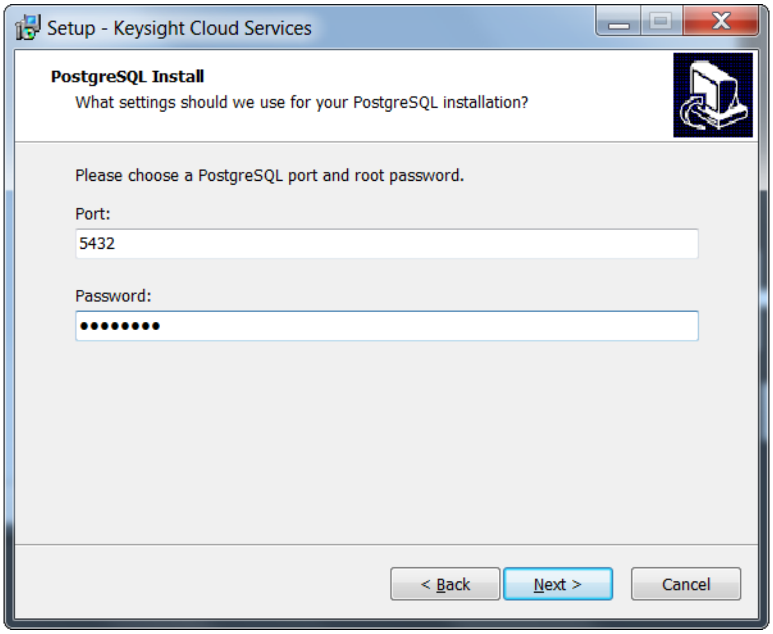
What is the hostname of the server?

Please enter the hostname or IP address and select an open port on the server which will run Keysight Cloud Services.

Server Address: localhost

Port Number: 8080

10 If PostgreSQL is not installed, specify the PostgreSQL **Password** on the PostgreSQL Install screen and click **Next**.



**PostgreSQL Install**

What settings should we use for your PostgreSQL installation?

Please choose a PostgreSQL port and root password.

Port: 5432

Password: ••••••••

11 If PostgreSQL is already installed, do the following:

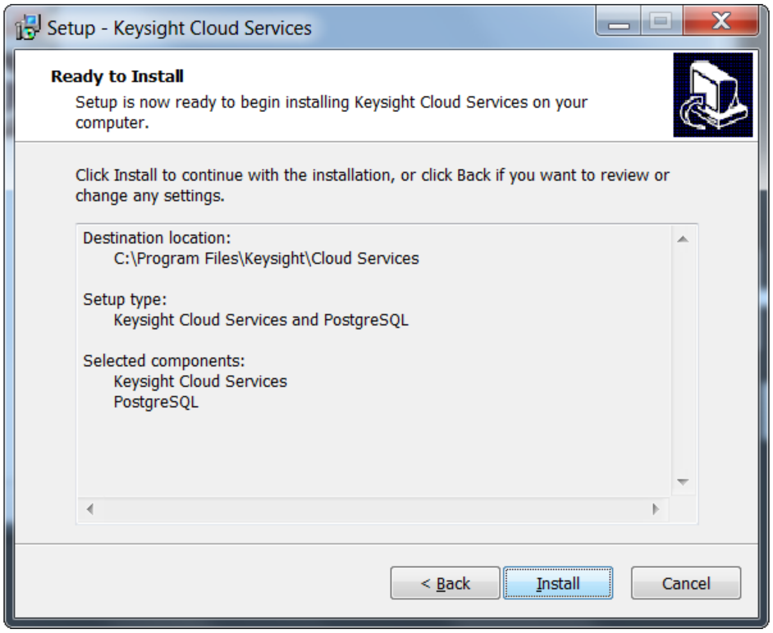
a On the Select PostgreSQL Directory screen, click **Browse** to specify the installation directory and click **Next**.

b On the PostgreSQL Configuration screen, specify the PostgreSQL **Port** and **Password**, and click **Next**.

NOTE

If PostgreSQL is already installed, be sure to specify its existing port and password. Changing these here will not take effect and will cause errors.

12 On the **Ready to Install** screen, click **Install**.



Setup - Keysight Cloud Services

**Ready to Install**

Setup is now ready to begin installing Keysight Cloud Services on your computer.

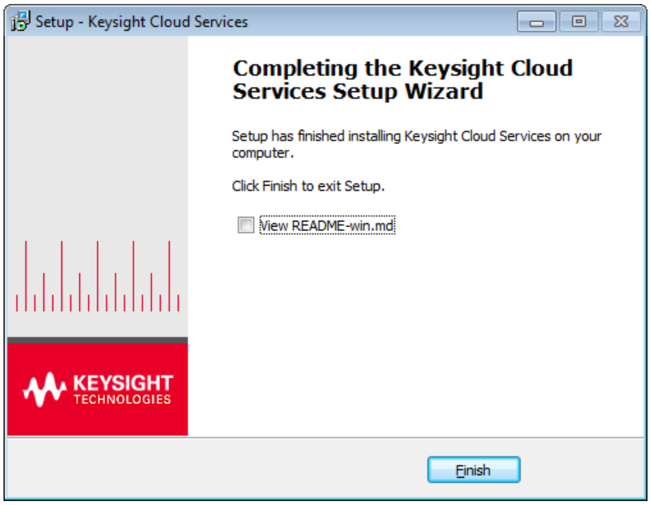
Click Install to continue with the installation, or click Back if you want to review or change any settings.

```
Destination location:
      C:\Program Files\Keysight\Cloud Services

Setup type:
      Keysight Cloud Services and PostgreSQL

Selected components:
      Keysight Cloud Services
      PostgreSQL
```

13 After KCS installation, click **Finish**.



Setup - Keysight Cloud Services

**Completing the Keysight Cloud Services Setup Wizard**

Setup has finished installing Keysight Cloud Services on your computer.

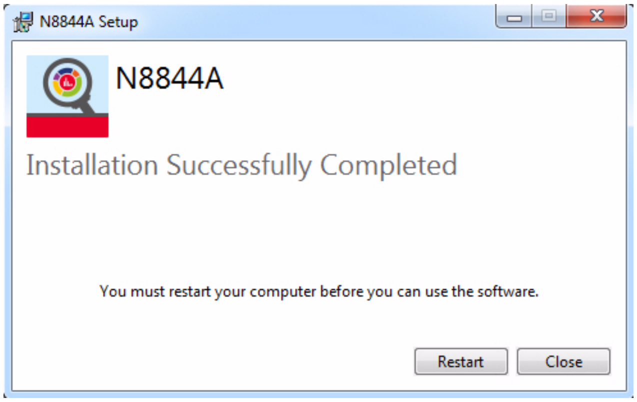
Click Finish to exit Setup.

□ View README-win.md

NOTE

The Keysight Cloud Services installer will write the user selected installation directory to the registry. The value is written to the InstallPath property located at *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Keysight\Cloud Services*.

**14** When the following window that marks the end of a successful installation appears, click **Restart** to restart your PC.



N8844A Setup

N8844A

Installation Successfully Completed

You must restart your computer before you can use the software.

**15** After restarting your computer, use the browser URL to access the KCS server interface (specified in step 9).

When you access the URL (hostname/IP address and port) for the first time, it will launch the KCS Startup Wizard.

a On the Welcome to the Keysight Cloud Services Startup Wizard page, click **Next** to set up the authentication provider and CoreAdmin.

b On the Configure the Authentication service page, you may either set up the authentication provider now or do it later. For information on setting up authentication providers, see "Configuring the Cloud System" on page 20.

c Click **Next** to set up the CoreAdmin user.

d Specify the **User Name**, **Email**, **Password**, and **Confirm Password** of the CoreAdmin user, and click **Next**.

e On the Welcome to the Keysight Cloud Services Startup Wizard (Finish) page, click **Finish** to complete the set up of the CoreAdmin user.

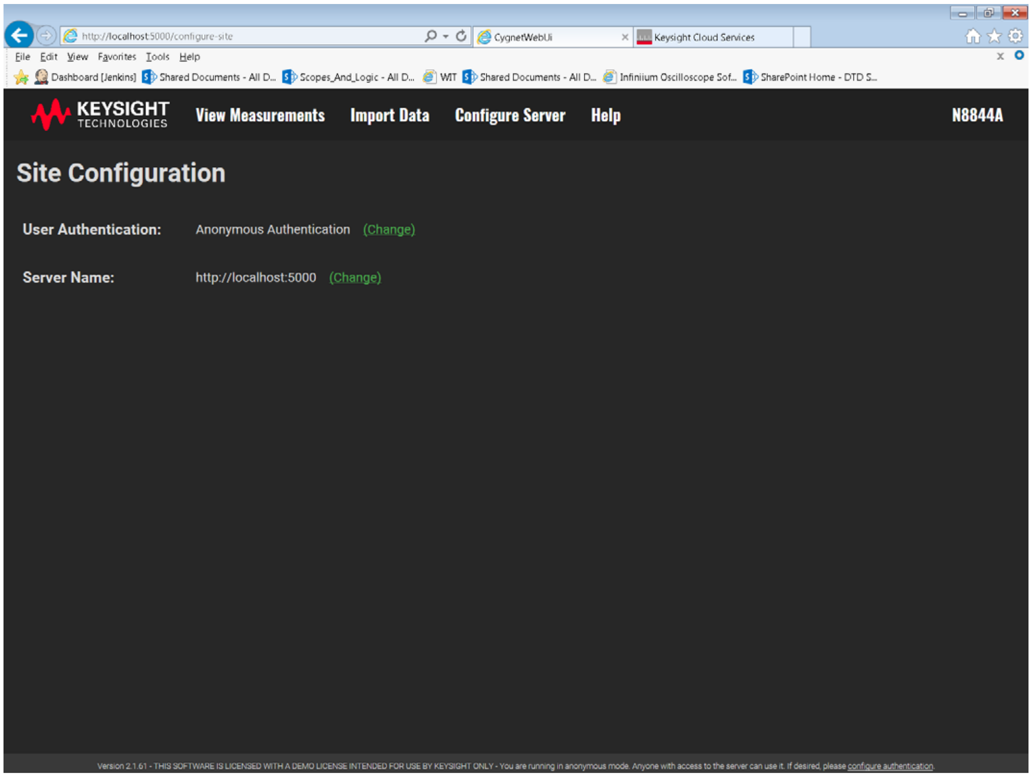
The Keysight Cloud Services login page is displayed.

For more information on using Keysight Cloud Services, see Chapter 2, “Using Keysight Cloud Services (KCS),” starting on page 17.

16 Log in to the N8844A web server using port 5000.

17 Click **Configure Server**.

For **User Authentication**, click **Change**.


http://localhost:5000/configure-site
CygnetWebUi
Keysight Cloud Services
File Edit View Favorites Tools Help
Dashboard [Jenkins]
Shared Documents - All D...
Scopes_And_Logic - All D...
WIT
Shared Documents - All D...
Infiniium Oscilloscope Sof...
SharePoint Home - DTD S...
KEYSIGHT TECHNOLOGIES
View Measurements
Import Data
Configure Server
Help
N8844A

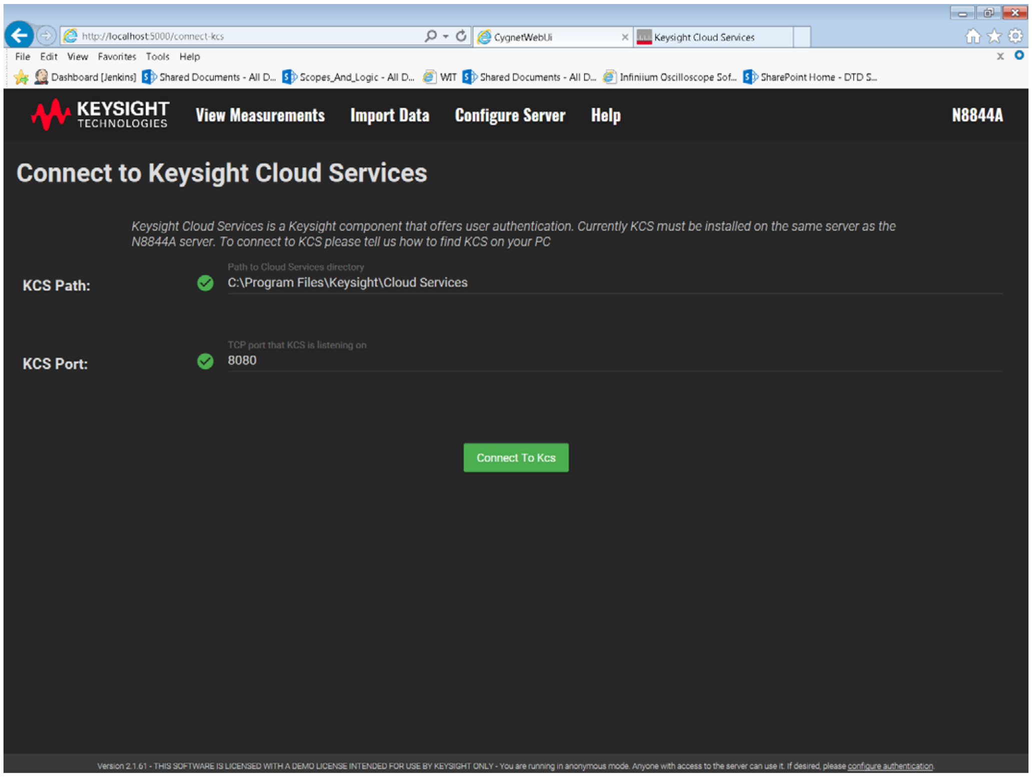
Site Configuration

User Authentication: Anonymous Authentication (Change)

Server Name: http://localhost:5000 (Change)

Version 2.1.61 - THIS SOFTWARE IS LICENSED WITH A DEMO LICENSE INTENDED FOR USE BY KEYSIGHT ONLY - You are running in anonymous mode. Anyone with access to the server can use it. If desired, please configure authentication.

18 Verify the **Path to Cloud Services directory** and the **TCP port that KCS is listening on**; then, click **Connect to Kcs**.


http://localhost:5000/connect-kcs
CygnetWebUi
Keysight Cloud Services
File Edit View Favorites Tools Help
Dashboard [Jenkins]
Shared Documents - All D...
Scopes_And_Logic - All D...
WIT
Shared Documents - All D...
Infiniium Oscilloscope Sof...
SharePoint Home - DTD S...
KEYSIGHT TECHNOLOGIES
View Measurements
Import Data
Configure Server
Help
N8844A

Connect to Keysight Cloud Services

*Keysight Cloud Services is a Keysight component that offers user authentication. Currently KCS must be installed on the same server as the N8844A server. To connect to KCS please tell us how to find KCS on your PC*

KCS Path: ✓ Path to Cloud Services directory C:\Program Files\Keysight\Cloud Services

KCS Port: ✓ TCP port that KCS is listening on 8080

Version 2.1.61 - THIS SOFTWARE IS LICENSED WITH A DEMO LICENSE INTENDED FOR USE BY KEYSIGHT ONLY - You are running in anonymous mode. Anyone with access to the server can use it. If desired, please configure authentication.

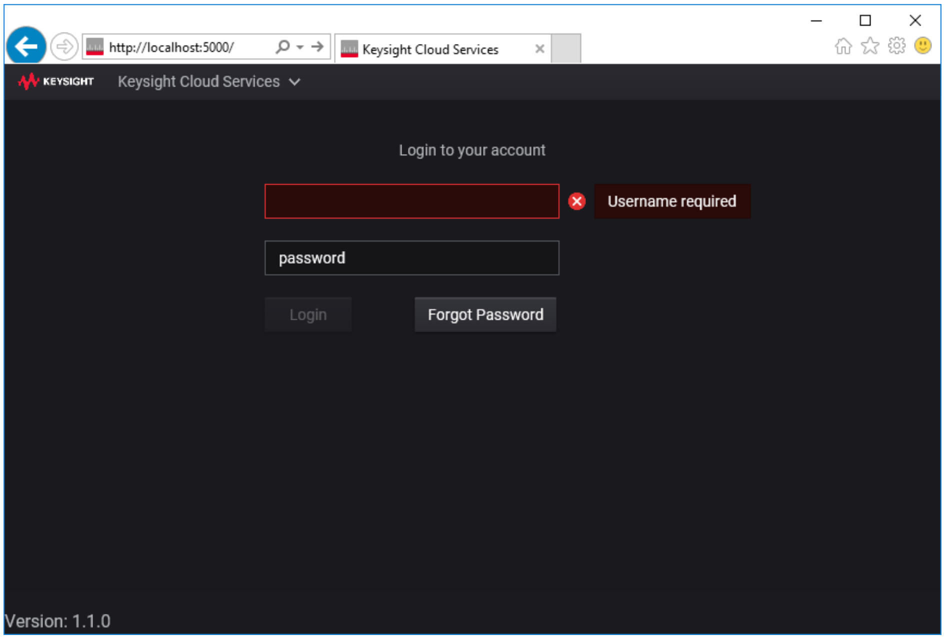
At this point, the software installation and setup is complete. Now, you are able to access the N8844A Web Service normally, either from the local server or from a remote computer. See:

- "Accessing the N8844A Web Service locally" on page 15
- "Accessing the N8844A Web Service remotely" on page 16

## Accessing the N8844A Web Service locally

1 To access the N8844A Dataset repository locally, launch any internet browser on your PC.

2 On the address bar, type `localhost:5000` to launch the N8844A Data Analytics Web Service Software. The following sign-in page is displayed.



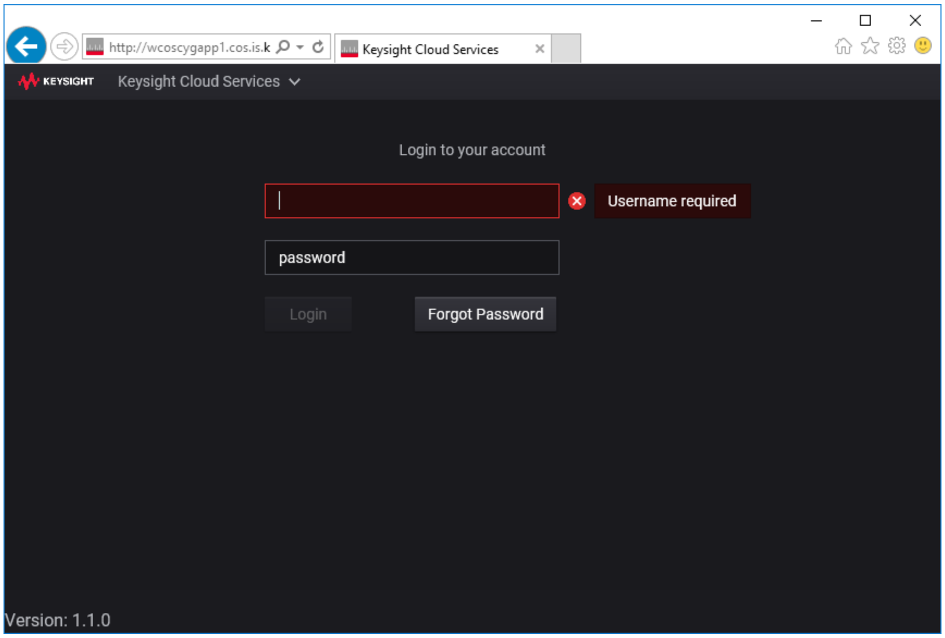
3 Proceed to sign-in with the credentials provided by the N8844A Web Service Administrator.

**NOTE** The initial login email is "admin@localhost" and the initial passowd is "admin". For security purposes, you should change the password.

## Accessing the N8844A Web Service remotely

1 To access the N8844A Dataset repository remotely, launch any internet browser on your PC.

2 On the address bar, type the IP address of the remote PC along with port 5000 to launch the N8844A N8844A Data Analytics Web Service Software. The following sign-in page is displayed.



3 Proceed to sign-in with the credentials provided by the Administrator for the N8844A Web Service.

**NOTE** The initial login email is "admin@localhost" and the initial password is "admin". For security purposes, you should change the password.

# 2 Using Keysight Cloud Services (KCS)

Accessing the Administrator Console / 18
Configuring the Cloud System / 20
Working with Applications / 24
Setting Up Users / 25
Manage Roles / 28
Monitoring the System / 31

Keysight Cloud Services (KCS) is a framework that provides core services for cloud-based applications, such as authentication, authorization, and licensing (although the N8844A Data Analytics Web Service Software does not use the KCS licensing).

Keysight Cloud Services (KCS) can be used by multiple applications, giving you a common Navigation Bar and Application Monitor across standard desktop and web-based applications.

Once the Keysight Cloud Services (KCS) are installed, you can perform administration tasks, based on your user role.

CoreAdmin user

As a CoreAdmin user, do the following:

- Log into the interface. See "Accessing the Administrator Console" on page 18.
- Configure the system (for example, user authentication and system emails). See "Configuring the Cloud System" on page 20.
- Add applications. See "Working with Applications" on page 24.
- Create user accounts. See "Setting Up Users" on page 25.
- Assign roles. See "Manage Roles" on page 28.
- Monitor the system. See "Monitoring the System" on page 31.

AppAdmin user

As an AppAdmin user, do the following:

- Log into the interface. See "Accessing the Administrator Console" on page 18.
- Assign roles. See "Manage Roles" on page 28.

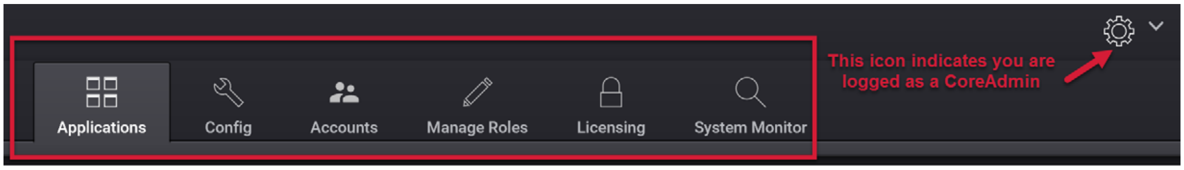
## Accessing the Administrator Console

This section describes how to access the system and your initial view upon login.

**CoreAdmin user**

1. Launch your browser application and enter the KCS server's URL.
2. Enter your login profile's user name and password.
3. Click **Login**.

   The administrator console is displayed. Because you are a CoreAdmin, all tabs are visible.

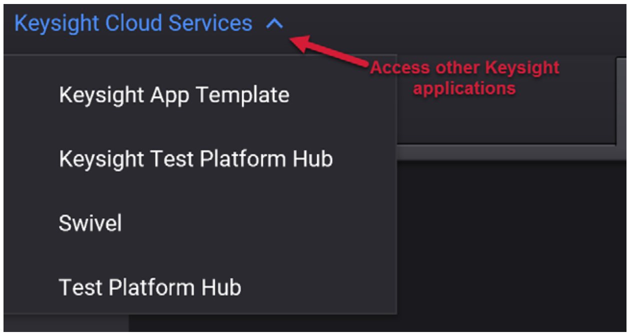


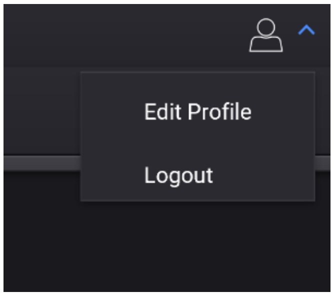
**AppAdmin user**

1. Launch your browser application and enter the KCS server's URL.
2. Enter your login profile's user name and password.
3. Click **Login**.

   Because you are an AppAdmin user, only the Manage Roles tab is available.

**Navigation** The console provides navigation options to both application and core administrators.





Edit Profile
Logout

# Configuring the Cloud System

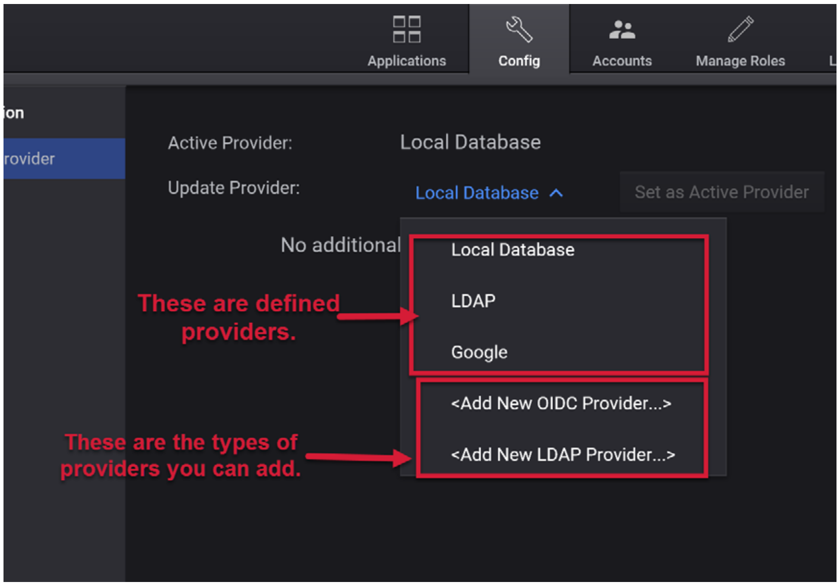
System configuration includes integrating with your authentication provider and email server.

- "Authentication provider" on page 20
- "Adding an OIDC provider" on page 20
- "Adding an LDAP provider" on page 21
- "Email server" on page 22

## Authentication provider

Click **Config** in the navigation bar. On the left is a second navigation pane called General Configuration. By default, the Authentication Provider area is the start page.

To set up a provider, click the dropdown by the Update Provider field.



Active Provider: Local Database

Update Provider: Local Database

No additional

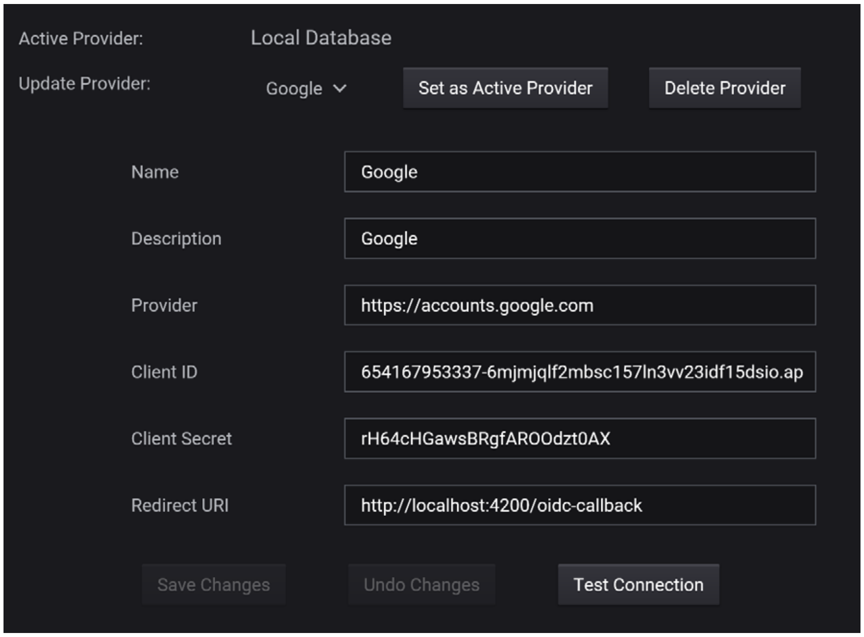
These are defined providers.

These are the types of providers you can add.

## Adding an OIDC provider

Select **<Add New OIDC Provider...>**.

Enter the **Name** and **Description** data. The other fields will need to be provided by your IT department. The **Provider** field is the provider's URL. The **Client ID** and **Client Secret**, which are specified by the provider, are needed so that the cloud service can talk to the provider. The screen below is an example of Google authentication, which uses OIDC.



Active Provider: Local Database

Update Provider: Google

Name: Google

Description: Google

Provider: https://accounts.google.com

Client ID: 654167953337-6mjmjqlf2mbsc157ln3vv23idf15dsio.ap

Client Secret: rH64cHGawsBRgfAROOdzt0AX

Redirect URI: http://localhost:4200/oidc-callback

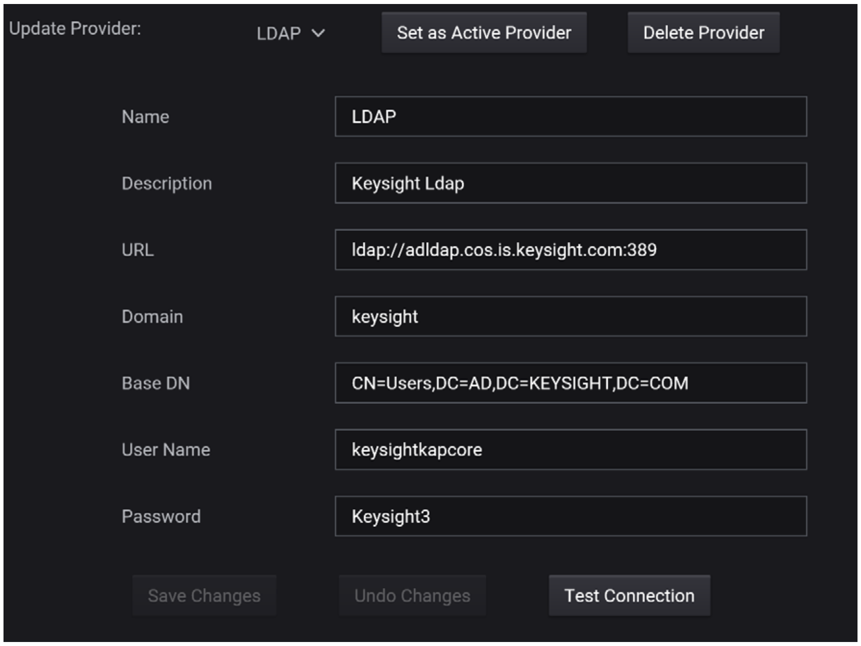
Once a provider has been created, it can be set as the active provider (where the cloud will go to authenticate), deleted, and the connection tested. When **Test Connection** is chosen, the service will reach out to the provider. The test's results are then displayed.

If changes are made, the **Save Changes** and **Undo Changes** are enabled.

## Adding an LDAP provider

Select **<Add New LDAP Provider...>** from the dropdown list.

Again, with the exception of the **Name** and **Description**, the customer's IT department will provide the information. LDAP requires that queries include a user and group **Base DN**. When the user is found, the full DN (for example cn=admin, dc=example, dc=com) is used to bind with the supplied password. The server then hashes the password and compares that result with the stored hash value.

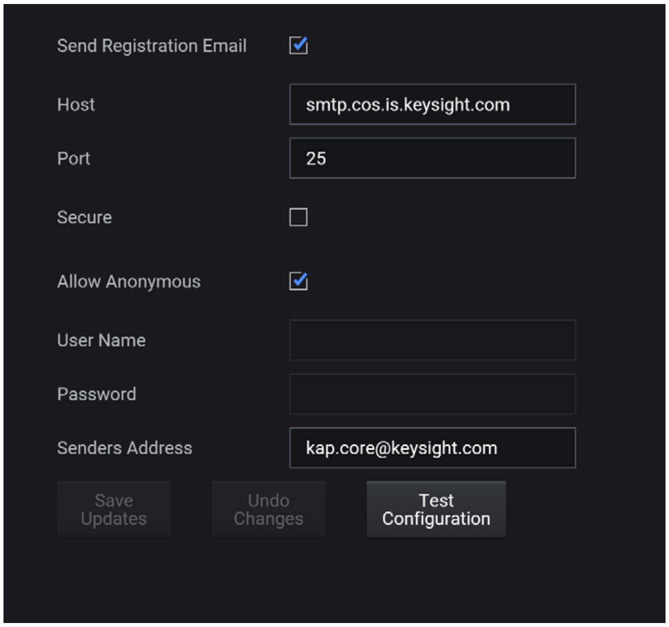


Update Provider: LDAP

| | |
|---|---|
| Name | LDAP |
| Description | Keysight Ldap |
| URL | ldap://adldap.cos.is.keysight.com:389 |
| Domain | keysight |
| Base DN | CN=Users,DC=AD,DC=KEYSIGHT,DC=COM |
| User Name | keysightkapcore |
| Password | Keysight3 |

## Email server

The email server needs to be configured to send the confirmation email and to reset passwords. Under General Configuration, click **Email Server**.

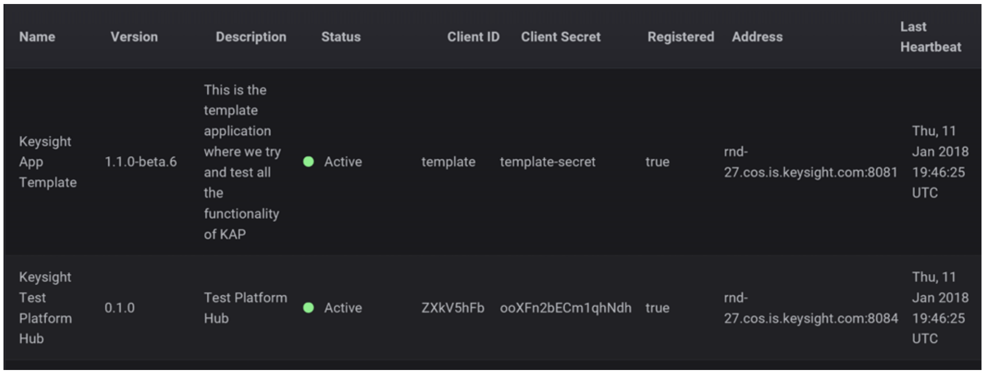


| | |
|---|---|
| Send Registration Email | ☑ |
| Host | smtp.cos.is.keysight.com |
| Port | 25 |
| Secure | ☐ |
| Allow Anonymous | ☑ |
| User Name | |
| Password | |
| Senders Address | kap.core@keysight.com |

Note that the registration email is optional and you can choose to allow anonymous access to the server. If this is checked, the **User Name** and **Password** are not necessary. Testing the configuration simply checks whether the connection is successfully made and does not trigger a sample email.

## Working with Applications

KCS provides a snapshot view of all the Keysight applications in your system and their status. Click **Applications** in the navigation bar.

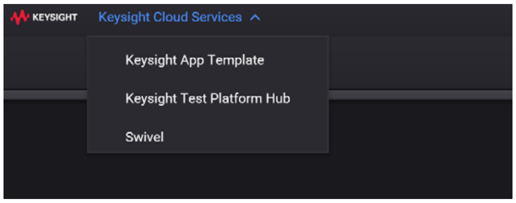


| Name | Version | Description | Status | Client ID | Client Secret | Registered | Address | Last Heartbeat |
|---|---|---|---|---|---|---|---|---|
| Keysight App Template | 1.1.0-beta.6 | This is the template application where we try and test all the functionality of KAP | ● Active | template | template-secret | true | rnd-27.cos.is.keysight.com:8081 | Thu, 11 Jan 2018 19:46:25 UTC |
| Keysight Test Platform Hub | 0.1.0 | Test Platform Hub | ● Active | ZXkV5hFb | ooXFn2bECm1qhNdh | true | rnd-27.cos.is.keysight.com:8084 | Thu, 11 Jan 2018 19:46:25 UTC |

This page lists the Keysight applications registered with KCS. The client ID and secret were used by the application to identify itself to KCS during registration. When it registers, the application tells KCS its associated license set, its version, and its address. Once registered and connected, the service polls the application every 5 seconds to verify it still has a heartbeat. If a heartbeat is not detected for a certain period, the application is set to Disconnected.

Within the page, an application can be deleted if you are either an AppAdmin for that program or you are a CoreAdmin. Hovering the cursor over the instance will evoke the **Delete** (🗑) icon.

To access an application, go to the drop-down in the upper left corner of the user interface and choose the program.



# Setting Up Users

This is the authorization piece of the equation. Once the user has been validated and attempts to access an application, the cloud user management service steps in and lets the application know what role the user has for that application.

- "How it works" on page 25
- "Creating a user account" on page 25
- "Managing CoreAdmin rights" on page 26
- "Resetting a password" on page 26
- "Creating a service account" on page 27
- "Managing service accounts" on page 27

## How it works

In order to access Keysight applications, the user must have a cloud account, a license, and one or more roles assigned. Roles are defined by the application itself; the cloud service does not know what the role definition is or what it means. Within the cloud UI, a cloud administrator will create that user account and assign the role(s) on a per application basis. This Keysight specific information is stored in a token attached to that user's account.

When the user attempts to access a Keysight application, that application will query the cloud service for that user's information using the Cloud provided API (REST endpoints) to query and manage authorization. Any application needing this data will need to work through that API.

## Creating a user account

Click **Accounts** in the navigation bar.

Note there are two account types listed in the left pane:

- Users – represent resources that will manually interact with the application.
- Service Accounts – enables automated users of the ecosystem to authenticate with the service.

To add a user account, type their email into the **<user email>** text box and click **Add User**.

If configured, an email containing a link to confirm the address and update their password is sent to the user. (This is optional. If the email is not sent, the user will click **Forgot Password** on the log in screen to receive the email with the link.)

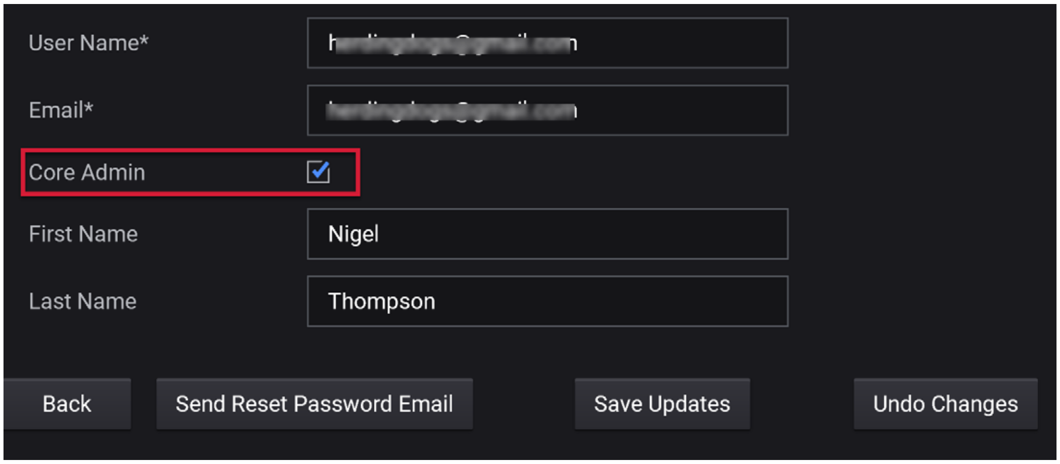
## Managing CoreAdmin rights

**NOTE** Only CoreAdmin users can manage these rights. To learn more about the CoreAdmin role, please visit "Manage Roles" on page 28.

By default, CoreAdmin rights are not enabled and can only be granted by editing the user. In the Accounts page, hover the mouse in the user's row. Two icons appear on the right: edit (✎) and delete (🗑).

Click the **edit** icon.

The CoreAdmin option is a check box. Select it to enable the rights (or de-select to take them away). When changes are made, the **Save Updates** and **Undo Changes** options are enabled.



| | |
|---|---|
| User Name* | [redacted] |
| Email* | [redacted] |
| Core Admin | ☑ |
| First Name | Nigel |
| Last Name | Thompson |

## Resetting a password

There are two ways to reset a password.

**Administrator** An administrator can trigger an account change for a user.

1 On the Accounts page, hover the mouse over the user's entry until the edit and delete icons appear on the right.

2 Select the **edit** icon.

3 Click **Send Reset Password Email**.

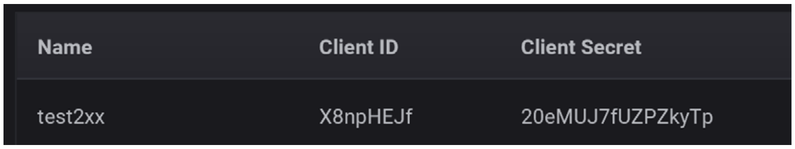
**User** A user can also evoke the email by clicking **Forgot Password** on the login screen and entering their email address.

## Creating a service account

Service accounts allow system resources, such as agents or automated processes, to be authenticated, since that type of user cannot manually log in. Service accounts also enable the assignment of metadata, such as license information, that applications can use when validating the account. For example, an instrument may run an agent to report data to a Keysight application; this agent would use a service account to authenticate itself within the ecosystem.

A service account is often a software tool that will perform a task and is designed by the end user and the service account simply enables that agent to interact with the application. However, instead of being assigned a role, a service account is granted a seat license to that application.

In the Accounts area, click the **Service Accounts** option under Account Types.



| Name | Client ID | Client Secret |
|---|---|---|
| test2xx | X8npHEJf | 20eMUJ7fUZPZkyTp |

Each service account has a client ID and a client secret that is generated upon creation. Applications also have a client ID and secret, but the service account and its application do not need to match each other. They are only used to authenticate with the service and receive an access token.

Enter an account name and click **Add Account**. The entry is added to the list with its ID and secret.

## Managing service accounts

Service accounts are granted licenses for application access. When edited, only the account name can be changed.

CAUTION

**It is strongly recommended *not* to delete a service account as the service will no longer be able to log in to the application.**

# Manage Roles

Within the cloud, roles are defined as access to application features. There is one application role defined by the cloud authorization service, which is the AppAdmin role. This is used to control access to administration functionality. A typical user will not be an AppAdmin but will have other app specific roles assigned to them by the AppAdmin. Application specific roles are defined by the app developer and then registered/injected into the authorization system via API. There is also an API that enables the application to query the service for the user's information. How many roles are available for an application and what those roles represent are managed entirely by the application developer. The knows of the existence of the roles for each application (since they have been provided) but has no insight into their meanings.

In addition, there is the CoreAdmin role. The core admin user is a recognized KSF Cloud user and is authenticated by the authorization service. This user administers cloud functionality that are larger in scope than applications, such as licensing and configuring authentication providers. In order to set up the system for use, there must be at least one CoreAdmin, so one is set up with the startup wizard on first launch.

- "Role definitions" on page 28
- "Assigning Roles" on page 29

## Role definitions

The following table summarizes the general functionality of each role. Description of application specific functionality is limited to what that user can see and a general note that permissions are determined by the application.

| Description | CoreAdmin | AppAdmin (for this app) | Application defined roles |
|---|---|---|---|
| Add users via accounts page | Yes | | |
| Assign users via roles page | Yes | Yes (only for their application(s)) | |
| Delete users via users page | Yes | | |
| Add/remove CoreAdmin authority for others | Yes | | |
| Delete other CoreAdmin users | Yes (not themselves) | | |
| Change authentication provider | Yes | | |

| Description | CoreAdmin | AppAdmin (for this app) | Application defined roles |
|---|---|---|---|
| Add roles (including AppAdmin) to users | For all apps and all users | Only in this app and its users | |
| Remove roles (including AppAdmin) from users | For all apps and all users | Only in this app and its users | |
| Visible tabs | ALL | Manage roles tab for their app only, App tab (their app only is listed) | |
| App Functionality | Only if app defined roles are assigned | Only if app defined roles are defined | Only if app defined roles are assigned |
| Download System Monitor Data | Yes | | |
| Add/Delete Applications | Yes | | |
| Update Email Server Configuration | Yes | | |
| Test Email Server Configuration | Yes | | |

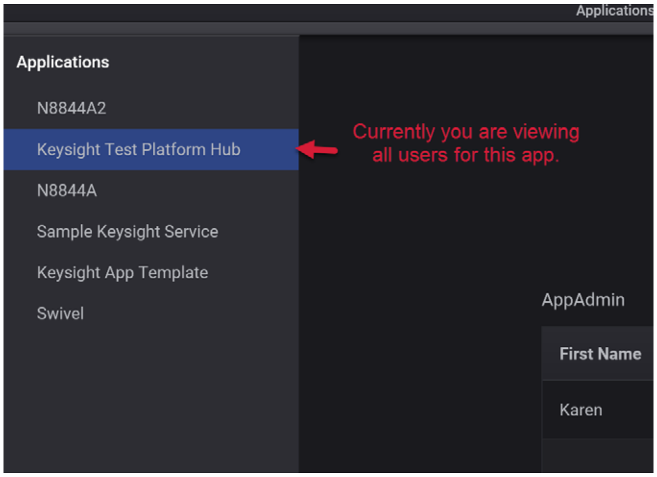
## Assigning Roles

Because roles are created with applications, applications must be registered with the KCS before users can be assigned. Please see "Working with Applications" on page 24.

1 Click **Manage Roles** in the navigation bar.

2 Select the desired application. The selection turns a darker blue.

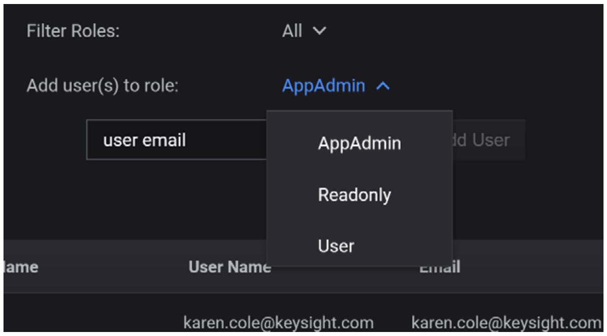
   The default view lists all of the roles defined for the selected application with that role's users.



Currently you are viewing all users for this app.

3 To filter the list to show only a specific role, select the profile from the Filter Roles: drop-down.

4 To see what roles are available, click the drop-down list by **Add User(s) to role:**



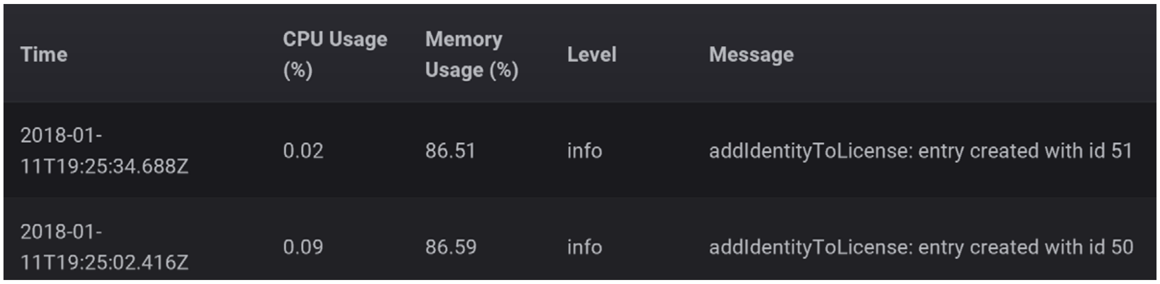
5 Enter the user's email and click **Add User**.

**NOTE** To assign a user to a role, that user account must already be created within KCS.

Note that a user can have more than one role within an application. For example, a user can be an AppAdmin and a User.

## Monitoring the System

The **System Monitor** tab displays the system's logs, rendered in a user-friendly list.

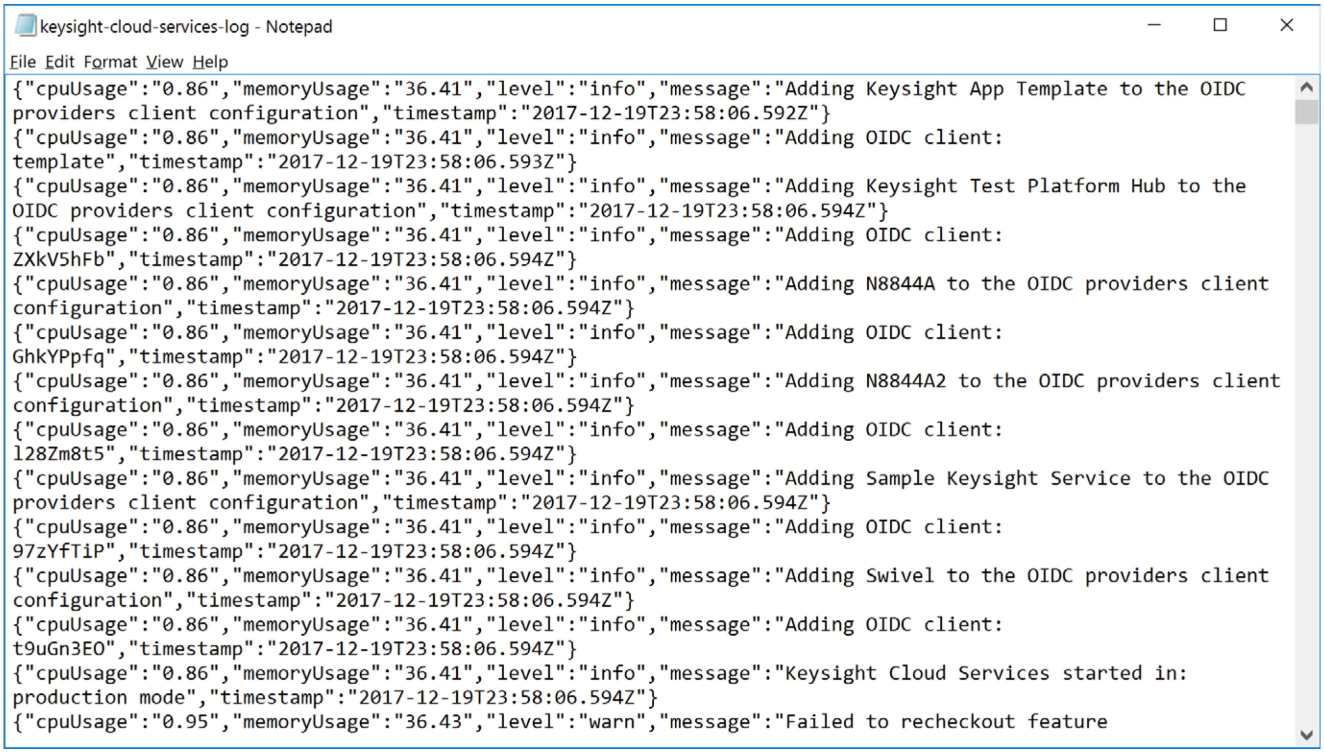


| Time | CPU Usage (%) | Memory Usage (%) | Level | Message |
|---|---|---|---|---|
| 2018-01-11T19:25:34.688Z | 0.02 | 86.51 | info | addIdentityToLicense: entry created with id 51 |
| 2018-01-11T19:25:02.416Z | 0.09 | 86.59 | info | addIdentityToLicense: entry created with id 50 |

Each entry includes the timestamp, CPU and memory usage at the time of event, the log level, and the message.

Because there will be hundreds of lines, the list can be filtered by entering a string parameter in the **Filter** box.

The **Download** option exports the log as a text file.



keysight-cloud-services-log - Notepad
File Edit Format View Help

```
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding Keysight App Template to the OIDC
providers client configuration","timestamp":"2017-12-19T23:58:06.592Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
template","timestamp":"2017-12-19T23:58:06.593Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding Keysight Test Platform Hub to the
OIDC providers client configuration","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
ZXkV5hFb","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding N8844A to the OIDC providers client
configuration","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
GhkYPpfq","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding N8844A2 to the OIDC providers client
configuration","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
l28Zm8t5","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding Sample Keysight Service to the OIDC
providers client configuration","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
97zYfTiP","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding Swivel to the OIDC providers client
configuration","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Adding OIDC client:
t9uGn3EO","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.86","memoryUsage":"36.41","level":"info","message":"Keysight Cloud Services started in:
production mode","timestamp":"2017-12-19T23:58:06.594Z"}
{"cpuUsage":"0.95","memoryUsage":"36.43","level":"warn","message":"Failed to recheckout feature
```

Both the downloaded log and the system monitor GUI only include the most recent events. To access earlier logs, a SysAdmin user will have to go to the log's location and view them.

# Index

## A

administrator console, accessing, 18
administrator console, navigation, 18
Administrator, resetting a password as, 26
AppAdmin user, 17, 18, 28
applications, working with, 24
Authentication provider, 20
authorization, how it works, 25

## C

cloud system, configuring, 20
copyright, 2
CoreAdmin rights, managing, 26
CoreAdmin user, 17, 18, 28

## E

Email server, 22

## I

installation, 5

## K

Keysight Cloud Services (KCS), 17
Keysight Cloud Services (KCS), using, 17

## L

LDAP Provider, 21

## N

notices, 2

## O

OIDC provider, 20

## P

password, resetting, 26

## R

role definitions, 28
roles, assigning, 29
roles, managing, 28

## S

server PC requirements, 5
service account, creating, 27
service accounts, managing, 27
system, moitoring the, 31

## U

user account, creating, 25
User, resetting a password as, 26
users, setting up, 25

## W

warranty, 2