Technical Document

Niagara Cloud Suite (NCS) Partner Guide

February 7, 2025

niagara4

Legal Notice

Tridium, Incorporated

3951 Western Parkway, Suite 350
Richmond, Virginia 23233
U.S.A.

Confidentiality

The information contained in this document is confidential information of Tridium, Inc., a Delaware corporation (Tridium). Such information and the software described herein, is furnished under a license agreement and may be used only in accordance with that agreement.

The information contained in this document is provided solely for use by Tridium employees, licensees, and system owners; and, except as permitted under the below copyright notice, is not to be released to, or reproduced for, anyone else.

While every effort has been made to assure the accuracy of this document, Tridium is not responsible for damages of any kind, including without limitation consequential damages, arising from the application of the information contained herein. Information and specifications published here are current as of the date of this publication and are subject to change without notice. The latest product specifications can be found by contacting our corporate headquarters, Richmond, Virginia.

Trademark notice

BACnet and ASHRAE are registered trademarks of American Society of Heating, Refrigerating and Air-Conditioning Engineers. Microsoft, Excel, Internet Explorer, Windows, Windows Vista, Windows Server, and SQL Server are registered trademarks of Microsoft Corporation. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Mozilla and Firefox are trademarks of the Mozilla Foundation. Echelon, LON, LonMark, LonTalk, and LonWorks are registered trademarks of Echelon Corporation. Tridium, JACE, Niagara Framework, and Sedona Framework are registered trademarks, and Workbench are trademarks of Tridium Inc. All other product names and services mentioned in this publication that are known to be trademarks, registered trademarks, or service marks are the property of their respective owners.

Copyright and patent notice

This document may be copied by parties who are authorized to distribute Tridium products in connection with distribution of those products, subject to the contracts that authorize such distribution. It may not otherwise, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written consent from Tridium, Inc.

The product(s) described herein may be covered by one or more U.S. or foreign patents of Tridium.

Contents

About this guide

This guide documents the Niagara Cloud Suite and the services that are in the suite. It is intended for the systems integrator who is responsible for installing and configuring the Niagara Framework® at customer sites.

Product Documentation

This document is part of the Niagara technical documentation library. Released versions of Niagara software include a complete collection of technical information that is provided in both online help and PDF format. The information in this document is written primarily for Systems Integrators. To make the most of the information in this book, readers should have some training or previous experience with Niagara software, as well as experience working with JACE network controllers.

Document Content

The topics and procedures in this guide describe how to configure the Niagara Cloud Suite software-as-a-service products associated with the Niagara Framework. Most procedures apply equally to single (stand-alone) controller systems and company-wide systems where controllers are joined and subordinate to a Supervisor station.

Document change log

Changes to this document are listed in this topic.

February 7, 2025

- Included the Operator Role requirement in the "Live reading and writing of data points" topic.
- Added "Sending user invitation to customer" topic to "Customer organization configuration (NCS)" chapter.
- Added "Live reading and writing of point data" topic to "Niagara Data Service" chapter.
- Added "Exporting device data" topic to "Niagara Data Service" chapter.

November 18, 2024

- Added "Viewing device details" topic.
- Added "Niagara Cloud audit logging" topic.

September 16, 2024

- Added "Re-registering a device" topic.
- Updated "Viewing usage metrics" topic
- Added "Viewing alarms" topic.

July 1, 2024

- Updated “Assigning Partner user access” in the “Customer organization configuration” chapter to include “Nds Operator” role.
- Updated “Ncs role-based access control” in the “Overview” chapter to include the Nds Operator role.

February 2, 2024

- Updated “Registering a device” in “Preparation to connect to the cloud” chapter.
- Added “CloudLink version requirements for NCS” section to “Requirements” chapter.
- Added “Deleting a device” topic to the “Customer organization configuration” chapter.

October 26, 2023

- Added “Niagara Remote” chapter.
- Added “Signing up for NCS Salesforce MFA” topic.

- Added “NCS role-based access control”.
- Added “Assigning partner user access” and “Assigning customer user access” topics to the “Customer organization configuration” chapter.
- Added “Binding license to Host Id” to the “Niagara Data Service” chapter.
- Updated “Viewing usage metrics” topic.
- Changed document title to use the full product name: Niagara Cloud Suite (NCS).

April 7, 2023

- Added Niagara Recover topics.
- Added “Searching for histories” to NDS
- Added “Viewing and exporting saved reports” and “Exporting on-demand reports” to NDS.
- Added “Niagara Recover” chapter.
- Added “Saved Backups view” to the “Reference” chapter.

January 19, 2023

- Updated terminology, several graphics and procedures.
- Added customer and project edit topics.
- Added usage metrics topic.

October 3, 2022

- Moved “Customer organization configuration” chapter ahead of “Niagara Data Service” chapter.
- Qualified the presence of the okhttp-rt module in the “Requirements” chapter.
- Added Step 7 to “Installing software,” which tells the user to use Platform Administration Commissioning or Software Manager to install the software on any remote platform.
- Moved all information about Internet access using a proxy server to this topic. Identical information was in two separate places.
- Added step 4 to “Adding cloud endpoints to the Workbench browser allowlist,” which tells the user to restart Workbench for the updated allowlist to take effect.
- Expanded the step result following step 1 in “Running the model upload job” regarding other data sources that receive a **`cloudId`**.
- In “Bulk upload and activating the channel” rewrote what **`Onboarding`** = `true` means.,
- In “Creating a report” added a sentence to Prerequisites. changed references to “points” and “point values” to “source” and “source values” since a data source may not always be a point.
- Expanded the problem and solution sections in the “Proxy server preventing connection” topic.

September 13, 2022

- Added info about pre-configured properties to “Authenticators, transports and channels.”
- Created a table to document the channels.
- Improved the steps for opening the palette in “Adding the CloudConnectionService.”
- Removed UUID from “Registration and Certificates.”
- Rewrote “Configuring histories to export data.”
- Added to “Bulk upload and activating the channel.”
- Added options to “Creating a report.
- Edited “Viewing reports” and a sentence about SI Admin users as the only ones who can save reports.
- Updated CloudLink logs.
- Added advice regarding creating backups to “What files to collect.”
- Added more to the Solution for what to do when “Connector keys are lost.”

- Added topics: “Cloud History, table of histories to export” and “CloudHistoryExportConfig.”

September 6, 2022

- Added `azure-devices.net` to the list of domains that must be accessible via a **proxyService**, if used with CloudLink.
- Added `force.com` as a required URL to include in the browser allowlist.
- Updated graphics to remove NCS following component name and Forge.
- Removed Egress API topics from the *Partner Guide* to a new *NDS API Guide*.
- Edited a number of topics to improve the read, correct inaccuracies and expand information.
- Added location to “Registering a Device.”

Related Documentation

Additional information is available in these documents.

Niagara Cloud Suite (NCS) Customer Guide

Niagara Cloud Service Guide

JACE-8000 Install and Startup Guide

Chapter 1. Overview

The Niagara Cloud Management Portal, located at *https://www.niagara-cloud.com*, provides a suite of services to support and augment local controller and Supervisor stations running the Niagara Framework. These services represent the next step to expand the functionality of Niagara.

The services include common Niagara functionality in the Niagara Cloud. Among other features, this release provides the Niagara Data Service, which stores history records from Niagara stations in the cloud and provides access to them for charting, reporting, and analysis.

A Niagara Community login (https://www.niagara-community.com/Comm_Login) authorizes system integrators and customer users to access *niagara-cloud.com*, otherwise referred to as the Niagara Cloud Management Portal.

Niagara Cloud Service

The cloudLink module sends and receives data to and from the cloud. Its main purpose is to provide a mechanism to push data from a collection of network capable devices (Thermostats, HVAC Units, NiagaraStations, and others.) such that they can be securely managed and controlled from the cloud.

This module acts as an adapter, bridging Niagara's internal data to a cloud-specific format. The service contains a set of configurable authenticators, transports, and communication channels, which can be implemented for the desired cloud platform. For a specific cloud platform with known capabilities and requirements, some parts of the service are fixed and configured by the choice of the palette.

The station running Niagara Cloud Service maintains a connection to the Niagara Cloud Platform. The station sends history and semantic model data to the cloud platform and receives commands from the cloud platform. Separately, the Niagara Cloud Platform provides RESTful API access to this data for programmatic access as well as viewing in its browser-based UI.

Requirements

This topic describes the platform, licensing, and software requirements for using Niagara Cloud Service and the Niagara Cloud Management Portal.

Platform and application requirements

- The **NiagaraCloudService** requires a compatible Niagara version.
- A Workbench connection is required to install the cloudLink modules and configure the **NiagaraCloudService**.
- A browser is required to access the Niagara Cloud Management Portal.

License requirements

- A cloudLink license must be enabled on the host.
- You must have an active SMA (Software Maintenance Agreement).
- An active subscription to one or more Niagara Cloud services.

Niagara Community credentials

To register a device using the Niagara Cloud Management Portal, you must be a registered user of the Niagara Community and your Partner Admin must have given you access to a particular customer. A user without access will be redirected to Niagara Community.

Software modules

NCS requires a core set of modules. Some modules are optional. The following table shows the required and optional modules that are needed for each version of Niagara.

NOTE: In the Software Manager, carefully select the correct modules based on the table below, especially if you wish to perform a Niagara upgrade because some module names have changed.

Selecting the "select first" modules, cloudLinkNcs-rt.jar also automatically selects some of the other modules in the table, but not all of them. As a result, you will need to install some manually.

NOTE: When upgrading, ensure that you delete the unused modules so that these unnecessary modules will not be included in the station backups. This would makes a restore from backup difficult as the old unnecessary modules must be obtained for a restore to work.

Table 1. Niagara versions 4.10.6, 4.12.2, 4.13.0

Module	Required	Software Installation	Upgrade to: 4.10.7+, 4.13.2+, 4.14+	Notes
cloudLink-rt.jar	yes	automatic		
cloudLink-ux.jar	yes	manually select		
cloudLinkForge-ux.jar	yes	manually select		
okhttp-rt.jar	yes	automatic		Niagara version 4.10.6+ only

Table 2. Niagara versions 4.10.7+, 4.13.2+, 4.14+

Module	Required	Software Installation	Upgrade from: 4.10.6, 4.12.2, 4.13.0	Notes
cloudLink-rt.jar	yes	automatic		
cloudLink-ux.jar	yes	manual		
cloudLinkAzure-rt.jar	yes	automatic		
cloudLinkForge-ux.jar	yes	manual		
cloudLinkNcs-rt.jar	yes	select first	When upgrading from Niagara 4.10.6, 4.12.2, 4.13.0, this module replaces cloudLinkNds-rt.jar, which should be manually deleted.	Use the palette in this module to install the **NiagaraCloudService**.
clUtils-rt.jar	yes	automatic	When upgrading from Niagara 4.10.6, 4.12.2, 4.13.0, this module replaces modelDiscovery-rt.jar, which should be manually deleted.	
clUtilsBacnet-rt.jar		manual	When upgrading from Niagara 4.10.6, 4.12.2, 4.13.0, this module replaces modelDiscoveryBacnet-rt.jar, which should be manually deleted.	Install this module for Cloud support of Bacnet network devices.
clUtilsNiagara-rt.jar		manual	When upgrading from Niagara 4.10.6, 4.12.2, 4.13.0, this module replaces modelDiscoveryNiagara-rt.jar which should be manually deleted.	Install this module for Cloud support of Niagara network devices.

Module	Required	Software Installation	Upgrade from: 4.10.6, 4.12.2, 4.13.0	Notes
okhttp-rt.jar	yes	automatic		Niagara version 4.10.7+ only

Internet access

Internet access is required for all stations and clients. For more information, refer to Setting up device Internet access.

Security precautions

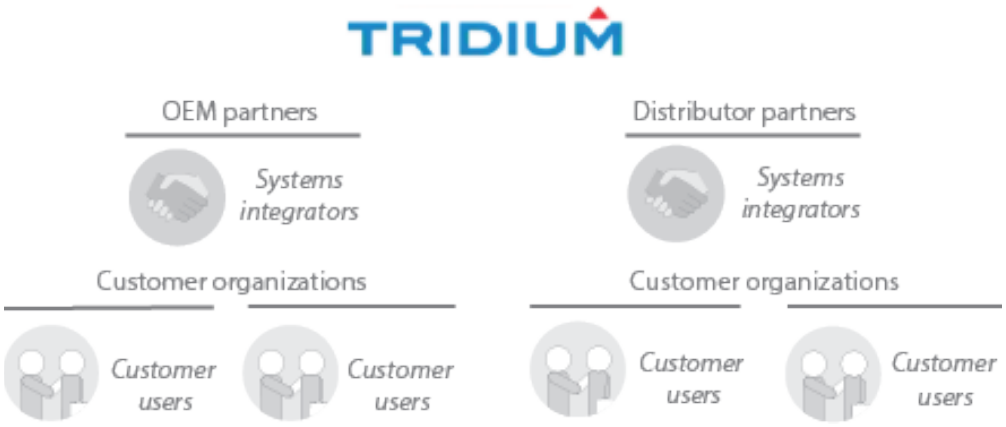
Station security is a must-have for all Niagara applications. Adequate security involves these best practices:

- Restricted physical access to each device (controller) and computer: do not make it easy for unauthorized individuals to access your devices. Users should be trained not to walk away from the PC while a sensitive view is open for others to see. Any user who has access to a dashboard should be configured for auto-logoff.
- User authentication with strong passwords: a minimum of 10 characters that include numbers, upper and lower-case letters and special characters (! @ # $ %); do not reuse passwords; establish a password policy that includes periodic password changes.
- Limited role assignments that configure access permissions: giving any user broad permissions on the **RoleService** is risky. A user with admin write permissions can create, edit, rename or delete any role. Such permission should be limited to only appropriately-authorized users.
- Client/server authenticated TLS communication at all levels: internal Foxs communication, HTTPS network communication, and external links to the Internet using VPN. TLS certificates must be signed by a third-party Certificate Authority. Self-signed certificates do not provide communication authentication.
- Components that support strong passwords, encryption, and authentication: replace older components, such as cameras, that do not support secure communication with components that support TLS.
- Encrypted data transmission over all communication channels.
- Signed program code (all Niagara modules are signed). Third-party modules should also be signed. Do not sign a module on behalf of a third party except as a last option, and then only if you trust the module authors.
- Separate locations for the Daemon User Home and Workbench User Home.

Users

A wide variety of people use the Niagara Cloud Management Portal to configure the cloud system, manage the uploading of data, create reports, and use reports.

Figure 1. Types of users



A Tridium *partner* is an original equipment manufacturer or distributor that resells the Niagara Framework to its *customer organizations*.

The members of a partner's staff who install and configure the Niagara Framework at customer organization sites are *systems integrators* (SIs).

Six *roles* determine the functions an individual can perform:

- The *Partner Admin* role provides complete functionality for the systems integrator who functions as the administrator on a partner's staff.
- The *Partner User* role provides limited functionality for other people who are members of a partner's staff.
- The *Customer Admin* role provides access to other customer users.
- The *Customer User* role lets the customer's facility manager or building owner view reports.
- The *Nds Operator* role provides a moderate level of access to Niagara Data Service components.
- The *Niagara Remote* role provides remote access to the station's web interface.

NCS role-based access control

The following tables give you an overview of the permitted actions that a specific role has within Niagara Cloud Suite.

Niagara Cloud Management Portal

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
View customer	✓	✓	✗	✗	✓	✓
View project	✓	✓	✓	✓	✓	✓
Create project	✓	✗	✗	✗	✗	✗
Edit project	✓	✗	✗	✗	✗	✗

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Delete project	✓	✗	✗	✗	✗	✗
View device	✓	✓	✓	✓	✓	✓
Register device	✓	✗	✗	✗	✗	✗
Edit device	✓	✗	✗	✗	✗	✗
Delete device	✓	✗	✗	✗	✗	✗
View user	✓	✗	✓	✗	✗	✗
Modify user role	✓	✗	✓	✗	✗	✗
View service account	✓	✗	✗	✗	✗	✗
Create service account	✓	✗	✗	✗	✗	✗
Edit service account	✓	✗	✗	✗	✗	✗
Delete service account	✓	✗	✗	✗	✗	✗
Regenerate service account secret	✓	✗	✗	✗	✗	✗
Modify service account role	✓	✗	✗	✗	✗	✗

Niagara Data Service

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Query model API	✓	✓	✓	✓	✗	✓
Query egress API	✓	✓	✓	✓	✗	✓

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Create report	✓	✗	✓	✗	✗	✗
Delete report	✓	✗	✓	✗	✗	✗
View report	✓	✓	✓	✓	✗	✓
Export history	✓	✓	✓	✓	✗	✓

Niagara Recover

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
View backups	✓	✓	✓	✓	✗	✗
Edit backup details	✓	✗	✗	✗	✗	✗
Download backup	✓	✓	✓	✗	✗	✗
Delete backup	✓	✗	✗	✗	✗	✗

Niagara Remote

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Connect to station	✓	✗	✓	✗	✓	✗

Live Read/Write

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Read point	✓	✓	✓	✓	✗	✓
Write point	✓	✗	✓	✗	✗	✓

Niagara Alarms

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Viewing alarms	✓	✓	✓	✓	✗	✓

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Managing alarms	✓	✗	✓	✗	✗	✓

Niagara cloud audit logging

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Viewing audit logs	✓	✓	✓	✓	✓	✓
Exporting audit logs	✓	✓	✓	✓	✓	✓

Bulk export

Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Viewing bulk export	✓	✓	✓	✓	✗	✗
Downloading bulk export	✓	✓	✓	✓	✗	✗
Initiate bulk export	✓	✓	✓	✗	✗	✗

User invitations

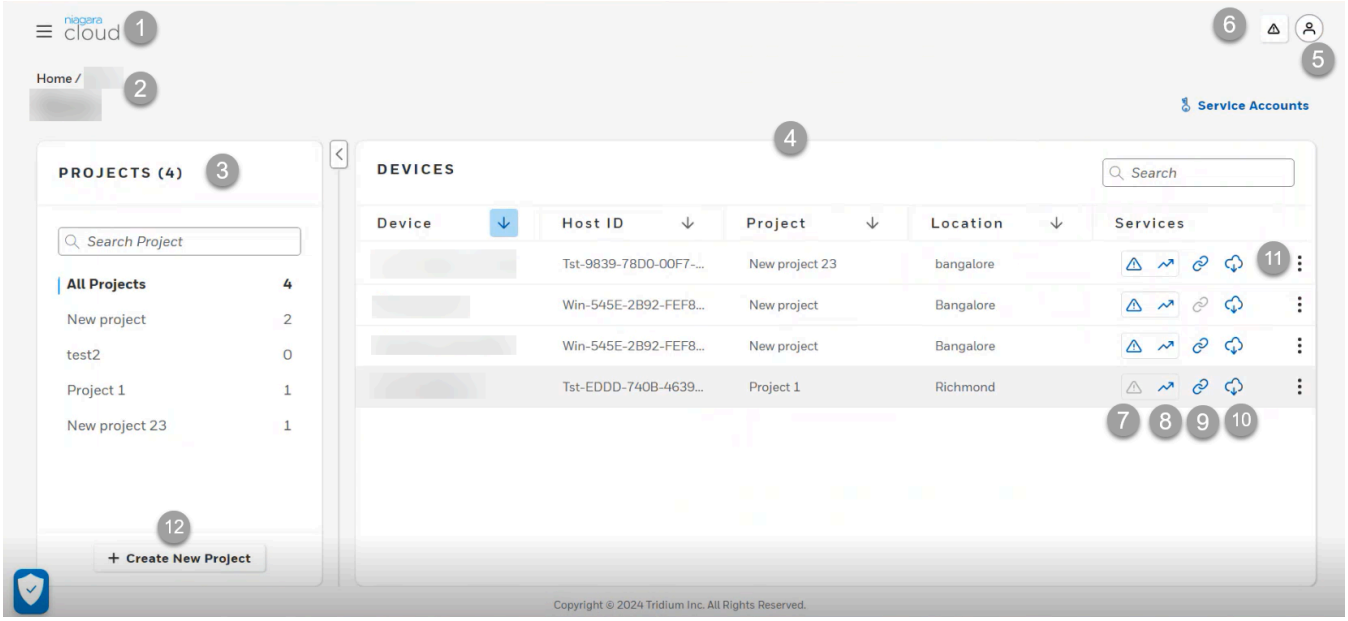
Action	Partner Admin	Partner User	Customer Admin	Customer User	Niagara Remote	NDS Operator
Viewing invitation	✓	✗	✗	✗	✗	✗
Inviting users	✓	✗	✗	✗	✗	✗
Resending invitation	✓	✗	✗	✗	✗	✗
Viewing pending invitations	✓	✗	✗	✗	✗	✗

Interface

Niagara Cloud Suite (NCS) runs in a browser at *https://www.niagara-cloud.com*.

The following is an example of a home page for a specific customer.

Figure 2. Home page



1. Menu opens a side panel with additional options
2. Customer name
3. Projects
4. Device-specific data for the selected customer and project
5. Log-out icon
6. View alarms icon
7. View device-specific alarm icon
8. Niagara Data Services icon
9. Niagara Recover icon
10. Niagara Remote icon
11. Row features provide functions that apply to each row of data.
12. Create new project button

When you open a customer, each customer has a list of projects that appear in the left pane. When you select one of the projects or click on **All Projects**, the right pane displays the list of devices associated with the project or the list of devices for all of the customer's projects.

Chapter 2. Connection preparation

Connecting to NCS requires that you sign up and authenticate with Salesforce MFA.

The following topic describes how to get started with connecting to NCS .

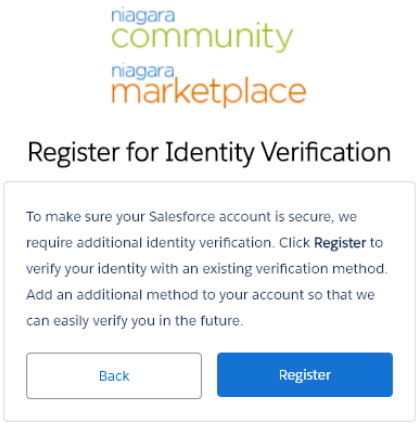
Signing up for NCS Salesforce MFA

For all Niagara Cloud Management Portal users, multi-factor authentication (MFA) is needed to meet high security standards. The following section describes how you can sign up for the Salesforce MFA for Niagara Cloud Management Portal.

Prerequisites:

- You have credentials to sign in to Niagara Community for NCS associated with an email address whose account you can access.
- The Salesforce Authenticator app or a generic authenticator app is installed on your mobile device.

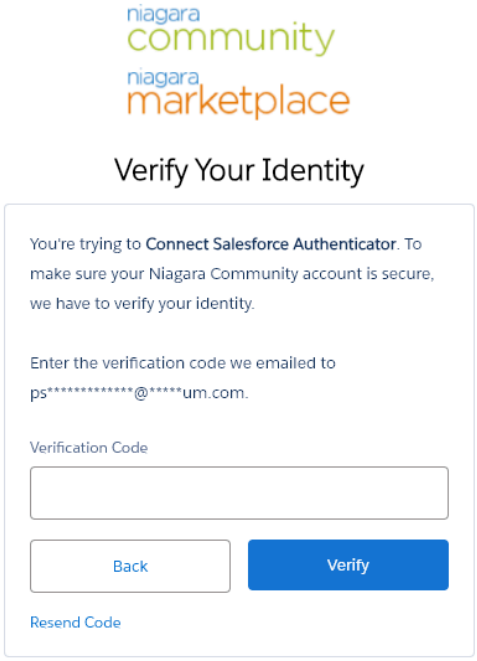
Step 1. Sign in to the Niagara Cloud Management Portal (https://www.niagara-cloud.com) using your Niagara Community credentials.



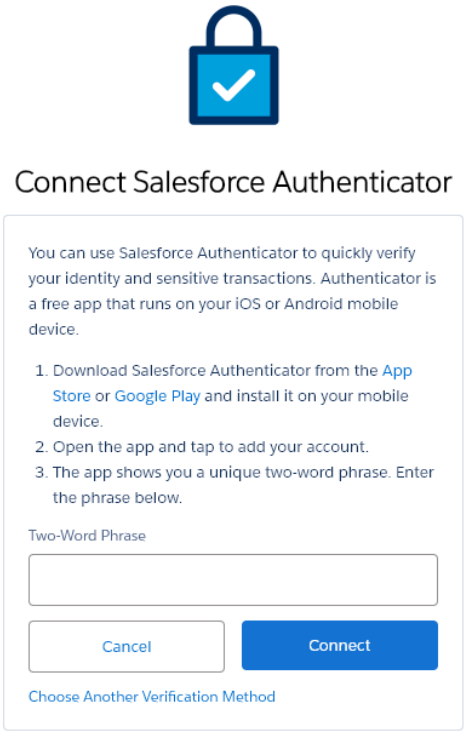
The **Register for Identity Verification** window opens.

Step 2. Click **Register**.

The **Verify Your Identity** window opens.



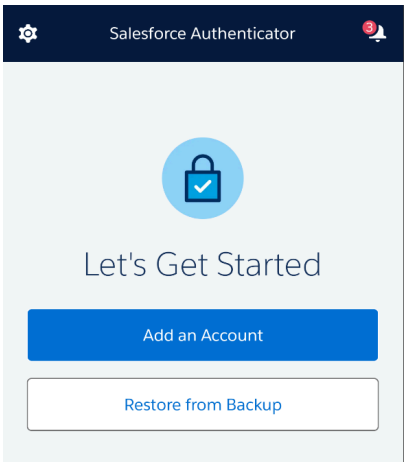
Step 3. Get the verification code from the associated email account, enter it in the **`Verification Code`** field, and click **Verify**.
The **Connect Salesforce Authenticator** window opens.



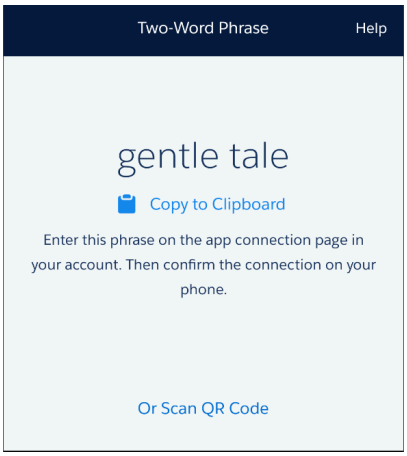
Step 4. Continue with the setup of the Salesforce Authenticator, or click **Choose Another Verification Method** to use a generic authenticator app.

Continuing with Salesforce Authenticator

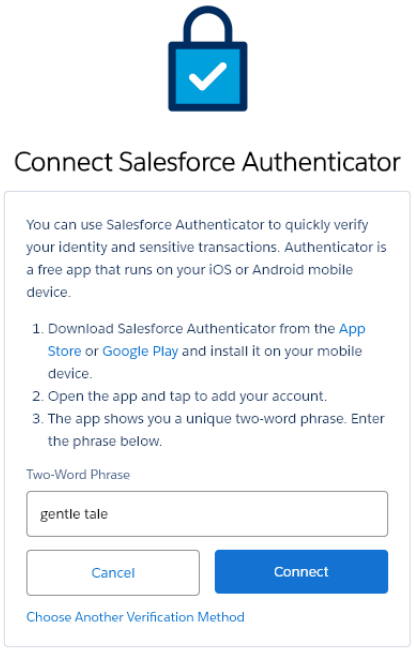
Step 5. From the Apple App Store or Google Play Store, download the Salesforce Authenticator app, open the app, and click **Add an Account**.



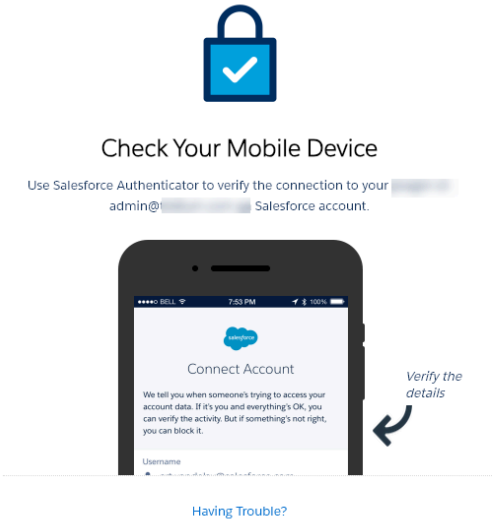
The **Salesforce Authenticator** window displays a two-word phrase.



Step 6. Navigate back to your browser and enter the phrase in the **`Two-Word Phrase`** field.



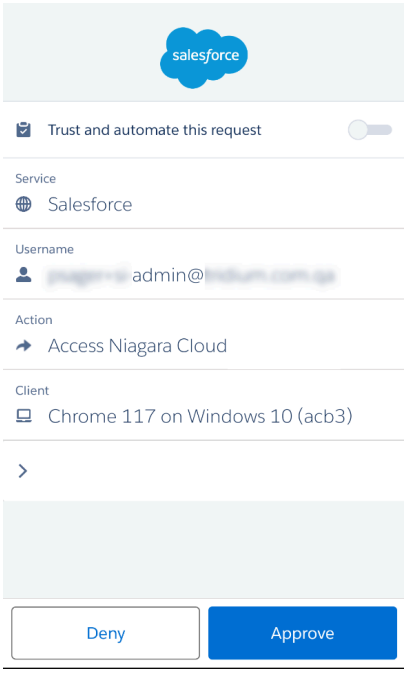
The browser displays a message to check your mobile device.



The app updates with the account information of the sign-up account.

Step 7. On the **Connect Account** window, click **Connect**.
The **Account Added** message confirms that the procedure was performed successfully.

Step 8. On the push notification that you receive, click **Approve** to approve the sign-up.



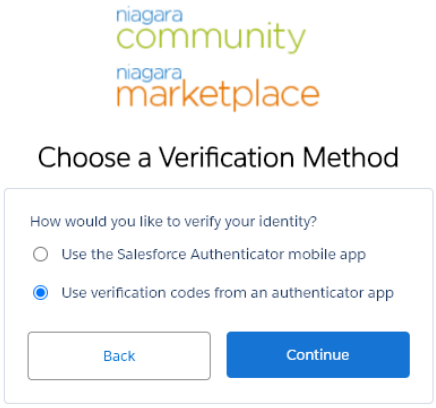
At this point, the enrollment process is complete and your browser continues to the NCS user interface.

NOTE: The authenticator app will prompt you to enable the location, which is an optional step that you can complete if you want the Salesforce Authenticator to auto-approve logins based on source device and mobile location.

Each time you log in to NCS, you will receive a push notification from Salesforce Authenticator. You can approve the logins from your mobile device.

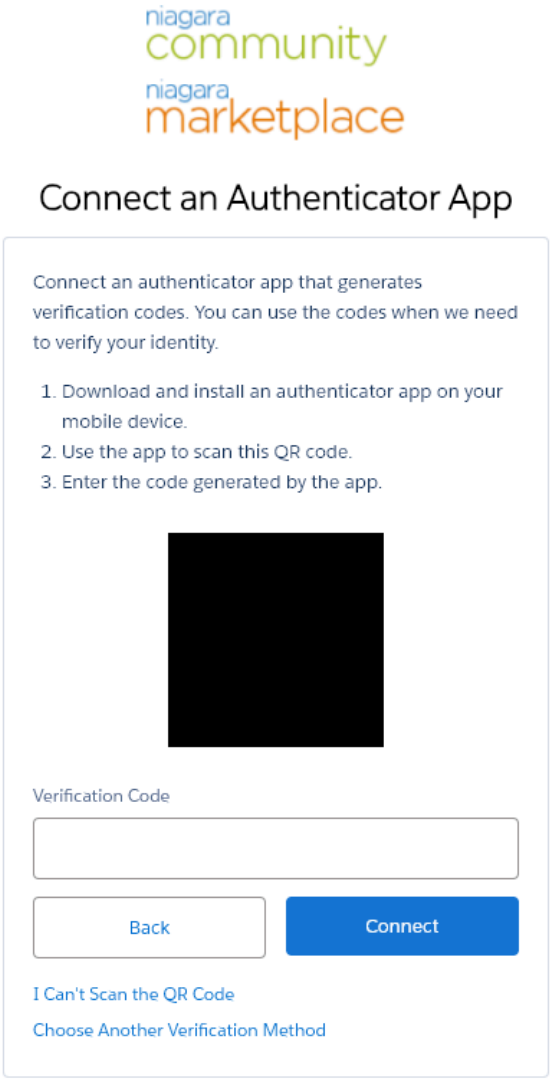
Continuing with a generic authenticator

Step 9. On the **Choose a Verification Code** window, select **Use verification codes from an authenticator app** option and click **Continue**.



You will be prompted to scan a QR code with your authenticator app.

Step10. Open your authenticator app and scan the code.



Your authenticator app displays a six-digit token for the newly added account.

Step11. Enter the six-digit token in the **Verification Code** field and click **Connect**.
You are asked to enter the verification code again to verify the login.

Step12. Enter the code from your authenticator app and click **Verify**.
The enrollment is complete. You will be asked for the verification code at each login.

Preparation to connect to the cloud

Each station must be configured to send data to the Niagara Cloud. Niagara Cloud Service provides the components you need to configure this connection. Niagara Cloud Service contains a set of configurable authenticators, transports, and communication channels which can be implemented for other desired cloud platforms.

If you are configuring this station to send data to the Niagara Cloud for the first time (a new station), it is a good idea to import additional points and add history extensions into your station before you configure and register the device.

If you are configuring a station with a lot of history records, the software exports the data to files and passes them through the IoT Hub. The default number of records that triggers a bulk export is 500,000. You can change this value.

Authenticators, transports and channels

The CloudLinkNcs module contains the **NiagaraCloudService**, which provides the functionality to send and receive data to and from the cloud. The main purpose of the service is to push data from a station to secure storage in the cloud.

To accomplish this, the **NiagaraCloudService** has three basic partitions:

- Authenticators
- Transports
- Channels

Channels and transports come pre-configured with default settings, which are sufficient for most installations but can be changed as needed. Some channels also include default export policies, which control the data and frequency at which the data are sent to the cloud.

Authenticators

This partition contains the mechanisms for authenticating to a specific cloud platform. For example, the FederatedIdentityAuthenticator authenticates to the Niagara Cloud Suite. This specific authenticator provides the means of authentication. For example, the authenticator provides a valid token when uploading a file via an HTTP request to the cloud.

Transports

This partition contains the mechanisms for transporting data. Such transports can include:

- HTTP transport is the mechanism for sending data via HTTP.
- AMQP (Advanced Message Queuing Protocol) transport is the mechanism for sending data via AMQP.

Channels

This partition contains the independent features that enable the **NiagaraCloudService** to function once provisioning is completed. Each channel handles communication for one application layer, such as messaging or history data. To communicate with the outside world the channel has pointers to the specific transport and authenticator it needs.

Channel	Description
Alarms	Installs a **CloudLinkAlarmRecipient** in the **AlarmService**, which should be connected to an Alarm Class to route alarms to the cloud.
Backup	Uploads station backups to the cloud according to the backup policy configuration. These backups are similar to those made by Niagara's **BackupService**, however, they are encrypted with the system passphrase or a configured password, and sent to the cloud.
Heartbeat	Maintains an active link with the IoT Hub service in the cloud to which it periodically sends short messages (“heartbeats”) via AMQP according to its frequency setting. The configuration for the Heartbeat channel in the Niagara Cloud Suite has entries for a transport type of AMQP and an authenticator ID of RpkAuthenticator. This means that when the Heartbeat channel needs to send a heartbeat message it does the following: 1. Query the specific authenticator for the needed credentials. 2. Create an AMQP message. 3. Send the message to the AMQP transport along with the associated details to ensure the message can be sent.
Histories	Sends history records to the cloud according to a station’s history export policy. This channel comes with an export folder and a pre-configured automatic export policy, which is disabled by default. This policy sends all histories to the cloud but allows for the exclusion of individual histories. To enable history exports, either enable the automatic export policy and configure its execution time or add additional history export policies.

Channel	Description
	Large stations should use the automatic export policy. Customizing the policy by, for example, by selecting individual histories for exclusion, can result in slow response times on history export policy pages.
Messaging	Sends messages to the cloud from components that are not channels, such as authenticators. This channel is installed and enabled by default. The Messaging channel provides a direct messaging capability to the transports. The authenticators use it to authenticate to the cloud platform.
Model	This channel sends detailed component information to the cloud including points, histories and log histories. The information sent includes type, facets, properties, tags and relations. The channel comes with one export policy, which the Cloud Id Manager will execute after it has assigned new cloud Ids.
Points	Sends data to the cloud based on its default export policy, which is disabled. Use the Histories channel instead to send telemetry data to the cloud. If you enable this channel, both the Points and Histories channels send data to the cloud. This potential duplication of data can produce unexpected results.

Installing software modules

If the cloudLink modules are not part of your Niagara image, use this procedure to install them. You can skip this procedure in cases where Niagara Cloud Service is packaged inside a docker image. In that scenario, the act of creating the docker image handles downloading and installing Niagara Cloud Service.

Prerequisites:
You are working in Workbench and are connected to a station. The station is connected to the Internet. You have a user account on the Niagara Community Software portal.

Only the system being registered with the cloud needs the cloudLink modules. Subordinate stations do not need the modules. If a subordinate station itself needs to communicate directly to the cloud, you will need to install the modules and register that station separately.

NOTE: If the Workbench platform is used to install the Niagara Cloud Service to a JACE, you need to also install the modules on the JACE using the platform's **Software Manager** view. For more information about the **Software Manager** view, see the *Niagara Platform Guide.*

Step 1. Open a web browser and log in to the Niagara Community Software portal.
The address is `https://www.niagara-community.com`.

Step 2. Click **Software** in the upper right of the home page.

Step 3. Scroll down to locate CloudLink and click the appropriate zip file link.
The choice depends on your Niagara version. You should choose the same major/minor/update version as the Niagara version that you currently use. For example, if you use Niagara 4.10.9, the filename of the zip file would contain "4.10.9" in it. The build version may be different for Niagara Cloud Service and Core Niagara).
The zip file downloads to your system.

Step 4. Navigate to your Windows downloads folder (`c:\Users\<UserName>\Downloads`) where < `UserName` > is unique for your computer.

Step 5. Right-click the zip file in the downloads folder and extract its contents to your SysHome installation folder (for example, `Niagara/Niagara-4.10.x`).

NOTE: If the system prompts you to `Overwrite any existing previous versions?`, click **OK**.

This installs the modules. The palettes are included in the modules.

Step 6. Restart the station and restart Workbench.

Step 7. To install the software on any remote platform (JACE), use the Platform Administration Commissioning tool or the Software Manager tool.

Result
Once the station restart is complete, you can proceed to install and configure Niagara Cloud Service.

Synchronizing clocks

Any platform (device) where the **NiagaraCloudService** is installed must have NTP (Network Time Protocol) of some type configured. This procedure sets up a one-time provisioning job to synchronize the clocks in all stations.

Prerequisites:
You are working in Workbench and are connected to a station.

If a platform clock is out of synchronization with the cloud platform, you may not be able to get the certificate to register the federated identity. Especially if your clock is behind, the system may think the certificate is not yet valid, which prevents the station from storing the certificate.

For a PC you configure the clock through Windows.

Step 1. Open the **provisioningNiagara** palette and drag a **ProvisioningNwExt** component to the **NiagaraNetwork**.

Step 2. From the **provisioningNiagara** palette, drag the **BatchJobService** component to the station's **Services**.

Step 3. To open the **Niagara Network Job Builder**, double-click **ProvisioningNwExt**.

Step 4. Under the **Steps to run for each station** pane (middle), click the plus (+).
The **New Job Step** window opens.

Step 5. Select the **Set Time** step.
The **Set Time** window opens.

Step 6. Select **`Use NTP time`** and click **OK**.

Step 7. Under the lower **Stations to include in the job** pane, click the plus (+).
The **Add Device** window opens.

Step 8. Select the stations to synchronize and click **OK**.

Step 9. Review your choices and click **Run Now**.
The view changes to the Niagara Network Job View where steps and results appear as the station executes them.

If you do not use a Provisioning Supervisor or Provisioning JACE, which are required for Niagara Provisioning, you do not need to set up the clock synchronization. If you use a standalone JACE-8000, refer to the "*Ntp Platform Service Editor Qnx view (platform-NtpPlatformServiceEditorQnx)" section* in the *Niagara Platform Guide* for more information.

Setting up device Internet access

Internet access is required for all stations and clients. If your device is on an internal (closed) network, this is done by setting up proxy server settings typically handled by the on-site IT department. Your proxy server must allow access to the Niagara Cloud Suite. Explicit (named) proxy support is provided through the **net-HttpProxyServer** from the net-rt module and configure it to your proxy server settings. For information on how to set up the **proxyService**, refer to the *Getting Started with Niagara*.

Prerequisites:
You are working in Workbench with a platform connection to the controller. For each device behind a network firewall, appropriate DNS Host name and DNS Server IP address(es) are available for your network. Your platform's clock is synchronized with the cloud platform.

If the **proxyService** is available and configured, Niagara Cloud Service automatically uses it. If you are using a proxy server with the **net-HttpProxyServer**, the **proxyService** must be able to access the following domains, which are part of the Niagara Cloud Suite:

- *.azure-devices.net
- *.force.com
- *.honeywell.com
- *.honeywellcloud.com
- *.niagara-cloud.com
- *.niagara-community.com
- *.pingone.com
- *.tridium.com
- *.windows.net

Step 1. In the platform **TCP/IP Configuration** view, enter the appropriate values for the following properties:
   - **`DNS Domain`** (for example: company.net)
   - **`DNSv4Servers`** (add a field for one or more DNS Servers; enter the appropriate IP address for each)

Step 2. Click **Save**.
On saving your changes you are prompted to reboot the device.

Next steps

CAUTION: From a cyber security perspective, it is crucial that your station is not exposed on the Internet. Communications via Niagara Cloud Service require only an outbound connection from your station to the Internet. Follow the best practices in the *Niagara 4 Hardening Guide* which is available on: https://www.tridium.com/us/en/services-support/library.

Adding cloud endpoints to the Workbench browser allowlist

Before registering devices, the browser allowlist (whitelist) in the Workbench System Home must allow the cloud endpoints to communicate with Workbench.

Prerequisites:
You are connected to a controller station and working in Workbench. You are aware of the security implications and organizational policies involved in editing an allowlist.

Step 1. To navigate to the allowlist configuration properties, expand **My Host** > **My File System** > **Sys Home** > **defaults** and double-click **system.properties**.
The text editor view opens.

Step 2. Use the search (**Ctrl** + **F**) to locate the `niagara.webbrowser.urlWhitelist` property in the `system.properties` file.

Step 3. Add these URLs to the allowed list: `auth.pingone.com`, `niagara-cloud.com`, `force.com` and click the save icon ().

Step 4. For the updated allowlist to take effect, close and restart Workbench.

Adding the NiagaraCloudService

The **NiagaraCloudService** component under the **Services** container connects the station to the Niagara cloud.

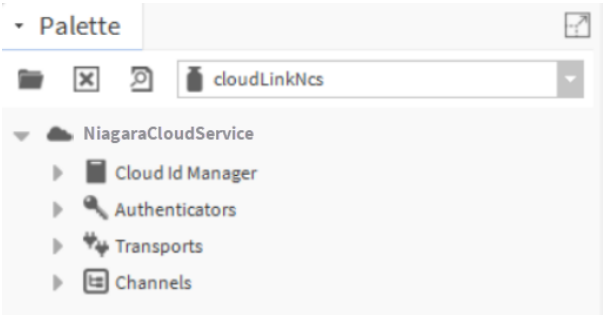
Prerequisites:
You are working in Workbench and are connected to a station. The cloudLinkNcs module is installed.

Step 1. To open the **Palette** side bar from the **Menu** bar, click **Window** > **Side Bars** > **Palette**.

The **Palette** side bar opens on the lower left of the page.

Step 2. Click on the Open Palette (folder) icon ( ).
The **Open Palette** window opens.

Step 3. Enter `cloud` in the filter box, select the cloudLinkNcs palette and click **OK**.



The palette opens in the side bar.

Step 4. Expand your station and drag **NiagaraCloudService** to the **Services** container in the Nav tree.
The **Name** window opens.

Step 5. Accept the default name or enter the different name and click **OK**.

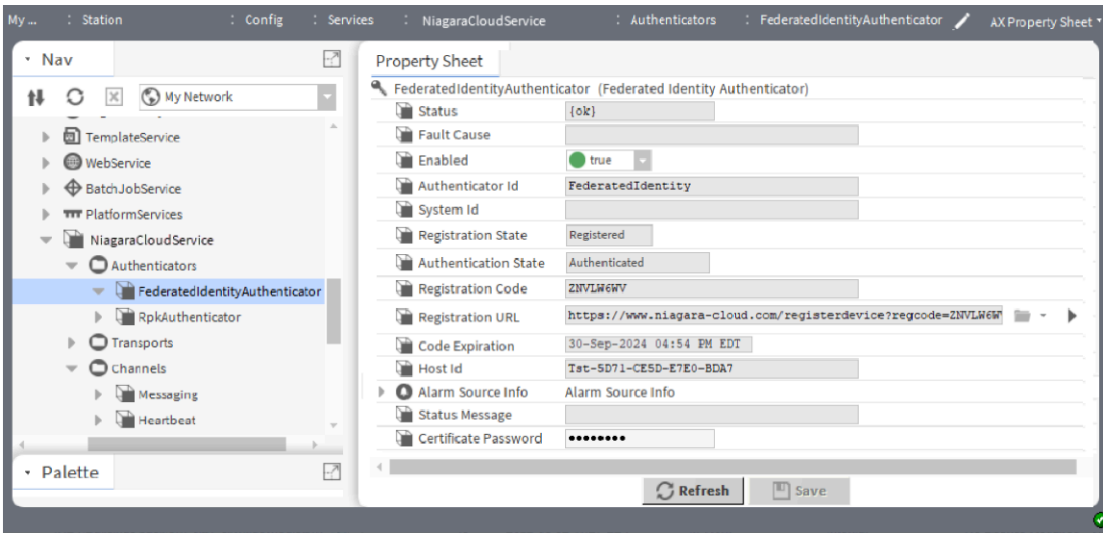
Registering a device

This procedure registers devices (stations) with specific customer projects. It is required for the use of Niagara Data Service, Niagara Recover, and Niagara Remote.

Prerequisites:

- You are using Workbench and are connected to a station to which you added the NiagaraCloudService.
- You have a Niagara Community account.
- You have set up projects in the Niagara Cloud Management Portal.

Step 1. Expand **NiagaraCloudService** > **Authenticators** and double-click **FederatedIdentityAuthenticator**.
The **FederatedIdentityAuthenticator Property Sheet** opens.



Step 2. Right-click the authenticator name and click **Actions** > **Start Registration**.

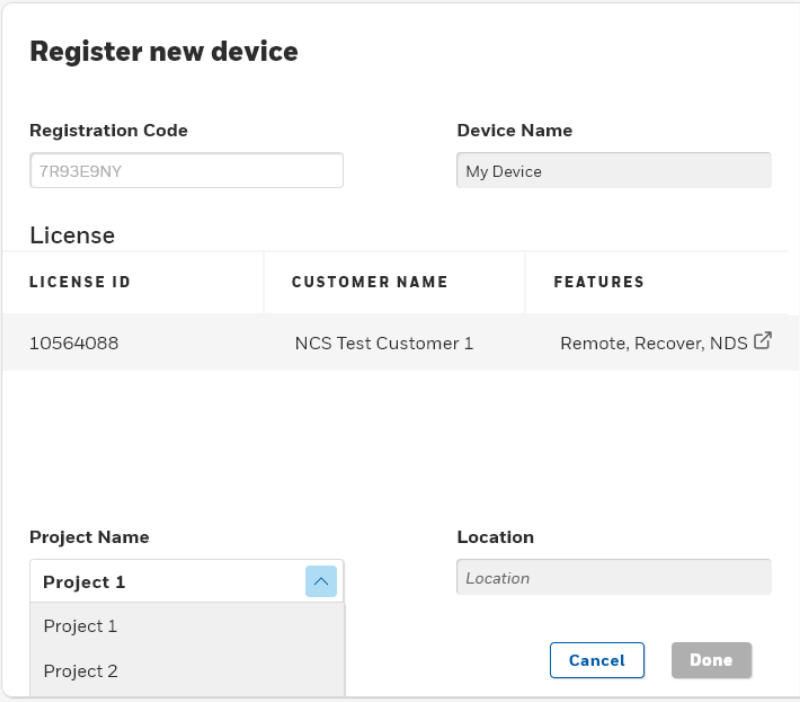
This action announces the station to the cloud registration service from which it receives the **User Code**, and populates the **User Code**, **User Registration Url** and **Code Expiration** properties.

NOTE: The **Registration Code** is good for 15 minutes. If you take longer than that to complete registration, an error occurs and you must start again.

The expiration time displays as **Code Expiration**. You need to complete the next step in the portal before the time is up or you will have to start again.

Step 3. Click the link arrow to the right of the **User Registration Url** property or copy the URL and paste it into a browser.
For more information about how to configure the web-browser whitelist (allowlist), see "Configuring the web-browser whitelist (allowlist)" in the *Getting Started with Niagara* guide and "Adding cloud endpoints to the Workbench browser allowlist." in the *Niagara Cloud Suite (NCS) Partner Guide*.
The Niagara Community log-in window opens.

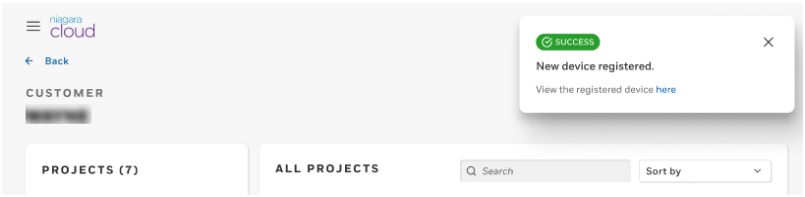
Step 4. Log in to the Niagara Cloud Management Portal using your Niagara Community account.
The **Register new device** window opens showing the **Registration Code**.



Step 5. Enter a **Device Name**, select a license from the available licenses if there are more than one licenses, select a project for the customer from the **Project Name** list, enter the **Location** and click **Done**.

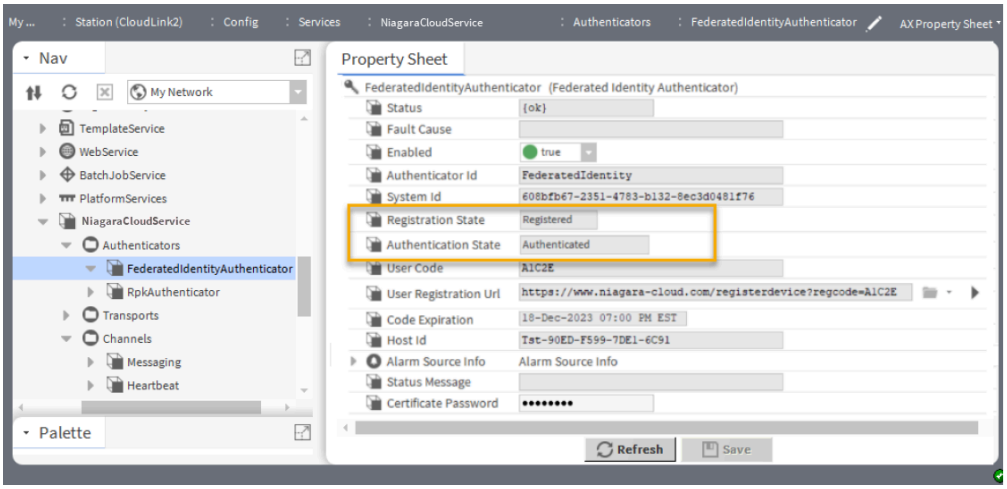
- **Device Name** can be the station name. However, you can change it to make it more descriptive of the project or location.
- **Licenses** selects the desired license from all available licenses to determine what features and functionality, which will be based on ordered subscriptions, are authorized to use.
- **Project Name** is the name of the Niagara Cloud Suite project to which this device belongs. It is selected from a dropdown of all the projects to which the user has access.
- **Location** identifies the building's geographic location.

The success pop-up confirms the device registration.



The system registers the device with the Niagara Cloud.

Step 6. To confirm the federated registration and connection, go back to the station's **FederatedIdentityAuthenticator Property Sheet**.
The property sheet opens.



The device is registered and, after a moment authenticated, which means that it has its station certificate, and that the software has provisioned Niagara Cloud Service.

NOTE: The provisioning process sometimes can take a few minutes before everything is set up in the station and fully registered. For example, the RPK Authenticator takes time to become authenticated. Until then, it may be present but it is disabled. It will not work if you try to enable it.

The provisioning of the components takes place based on the device subscriptions you ordered in Niagara Licensing. As an example, if you order Recover, under **Channels**, the **Backup** channel will be automatically added.

Result

The platform and station are now fully registered with the Niagara Cloud Suite. They have a certificate for the federated identity and are connected to the IoT Hub (the cloud). However, no data have been sent to the cloud.

Re-registering a device

You need a station's cloud identity to connect to Niagara Cloud Service and it's related data stored in the cloud. If the cloud identity is lost or the station is moved to a new device (device replacement), you need to re-register the device to restore the station's cloud identity.
Examples of scenarios in which a re-registration is needed:

- Restoring a JACE station from a backup (DIST tool) or just a station copy to a new JACE .
- Restoring a Supervisor from a backup with a station copy (DIST tool is not supported on a Supervisor) to a new computer.
- If the cloud identity of a station is lost, for example, because the NiagaraCloudService was deleted, or

authenticators or certificates expired.

NOTE: If the station is restored from a backup or copied to the same device, you do not need to re-register the device or change the license.

Device restore (same device): If the station is restored from a backup or copied to the same device, you may not need to re-register the device. Device re-registration is needed only if the station is not connecting to the cloud, for example, because certificates expired. Since the station is running on the same host, you do not need to change the license.

Device replacement (new device): This is the case where a previously registered station is copied or restored from a backup to a new device. In this case, the prerequisite is that you move the subscription from the old license bound to the old Host ID to a new license that is bound to the new Host ID. Otherwise, the re-registration process will not find a subscription for the new Host ID and the re-registration process cannot be completed.

NOTE: It is possible in some cases that a device replacement that was restored from a cloud backup will still retain its cloud identity. However, you should only consider this as temporary and re-register the device to avoid future subscription issues with the new Host ID.

Re-registering from a station

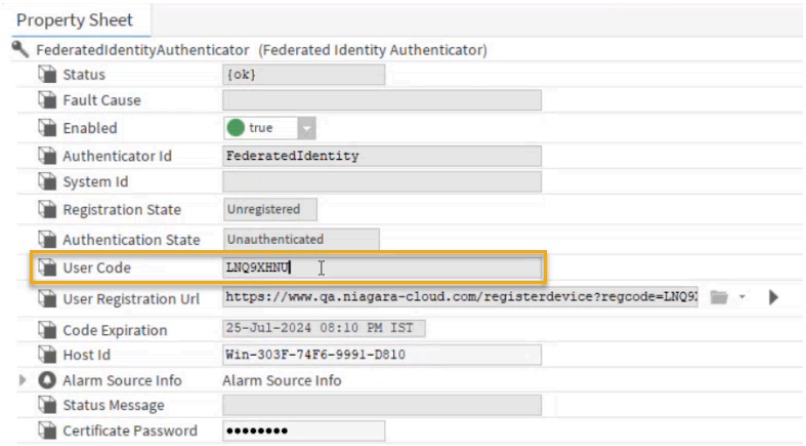
Step 1. In the station:

a. Expand **Config** > **Services** > **NiagaraCloudService** > **Authenticators**, and delete **FederatedIdentityAuthenticator** and **RpkAuthenticator**.

b. In the cloudLinkNcs palette, expand the **NiagaraCloudService** component, and expand the **Authenticators** folder.

c. Drag a new FederatedIdentityAuthenticator into the station under **Config** > **Services** > **NiagaraCloudService** > **Authenticators**.

d. To start the re-registration process, right-click on FederatedIdentityAuthenticator and select **Actions** > **Start Registration**.

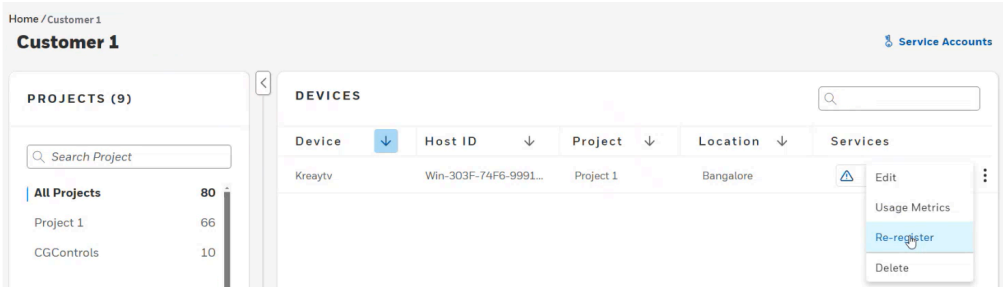


The user code automatically populates the **`User Code`** field.

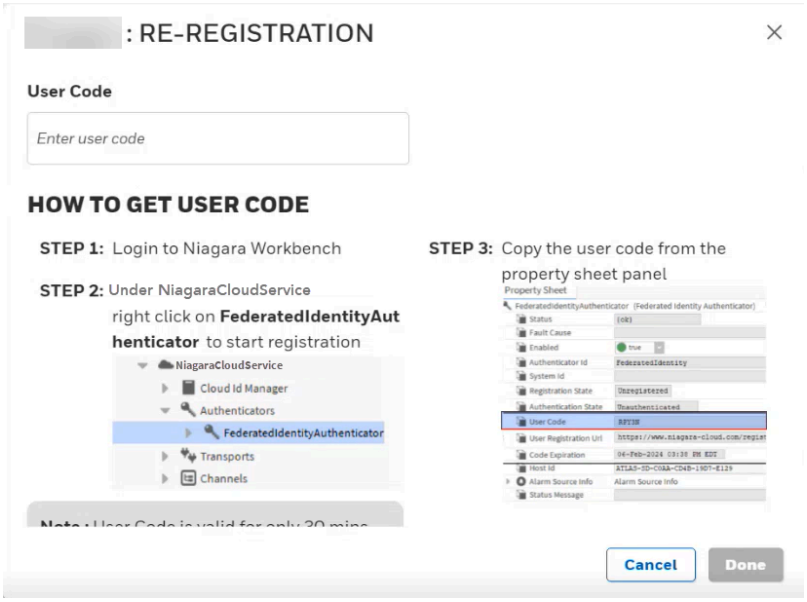
e. Copy the code from the **`User Code`** field as you will paste it in the **`User Code`** field in the Niagara Cloud Management Portal **Re-Registration** window.

Step 2. In the Niagara Cloud Management Portal:

a. Navigate to the device you wish to re-register and click the vertical ellipsis (three vertical dots).



b. From the drop-down menu, select **Re-register**.



The **Re-Registration** window opens containing the **`User Code`** field in which you enter the user code and the step-by-step instructions on how to obtain the user code.

c. Paste the user code that you copied earlier from the station's **`User Code`** field in the **`User Code`** field of the **Re-Registration** window, and click **Done**.

Step 3. In the station, check the status of the **FederatedIdentityAuthenticator** and the **RpkAuthenticator** as shown below.

FederatedIdentityAuthenticator: In **Config** > **Services** > **NiagaraCloudService** > **Authenticators**, the **FederatedIdentityAuthenticator** should show the **`Registration State`** as `Registered` and **`Authentication state`** as `Authenticated`. The **`Host Id`** property should shows the current Host Id.

RpkAuthenticator: In **Config** > **Services** > **NiagaraCloudService** > **Authenticator**, the RpkAuthenticator screen should have a green check next to **`Device Registered`**, **`Authenticator Enabled`**, and **`Device Connected`**. The RpkAuthenticator should have values for **`System Type`** and **`System Guid`**.

Step 4. Restart the station.

Chapter 3. Customer organization configuration

Niagara Cloud Suite (NCS) stores histories in the Niagara Cloud from where they are available to Niagara partners who configure reports for the partner's customer organizations.

NCS supports these functions:

- A station can access the data from the cloud.
- Systems integrators can use APIs with business intelligence and analytics software, such as Tableau and Microsoft's Power BI platform, to analyze the data.
- If a customer organization has its own cloud, the systems integrator may use APIs to add an additional layer of storage or use any other third-party tools.
- Customer users (members of a customer organization) can view reports containing charts.

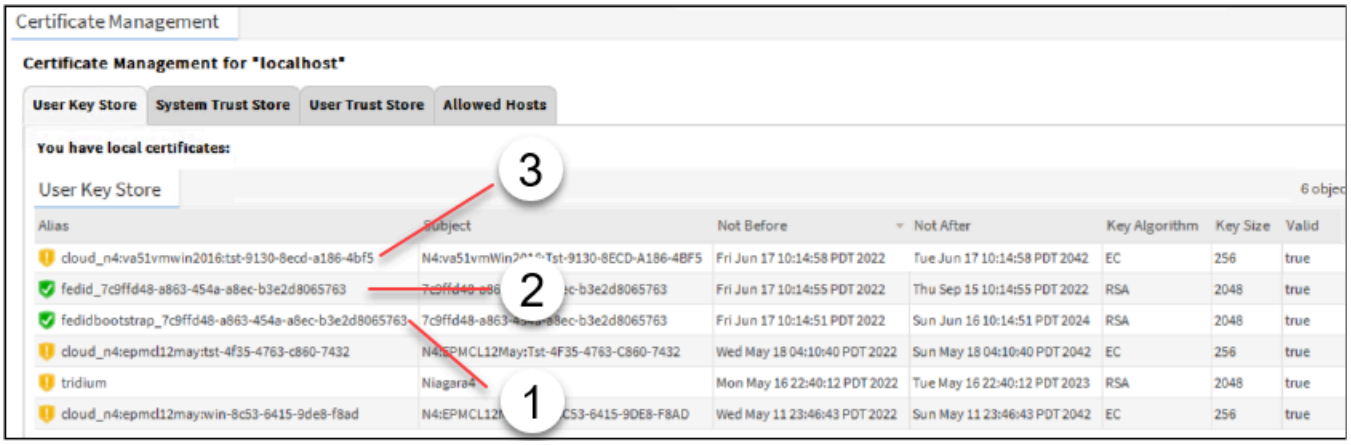
Registration and certificates

All communication between each controller station and the Niagara Cloud as well as between the Niagara Cloud Management Portal and Niagara Cloud is secured by certificates.

Certificate management (signing and renewing) is automated for the Niagara Cloud Suite using these certificates.

- Bootstrap certificate, which the software automatically updates based on an automatic expiration date.
- Rolling certificate, which the software automatically renews one month before it expires, currently set for every 90 days. You may configure the expiration days on the cloud side. This means that the system rolls the certificate approximately every 60 days give or take a day or two.
- Root certificate in the **User Trust Store** used to sign the rolling certificates.
- Key pair, which the RPK authenticator uses to link to the Niagara Cloud.

To view these certificates, navigate to the **CertManagerService**.



During registration, after the **FederatedIdentityAuthenticator** receives the device's global/universal identifier, the station generates a certificate signing request (CSR), which it sends to the certificate management web service.

If the device code is valid and matches the device's identifier, the certificate management web services signs and returns the signed bootstrap certificate. The station joins the bootstrap certificate with the private key that

was retained on the station and saved (not visible). The root certificate of the signing chain goes into the **User Trust Store** and the bootstrap and rolling certificates plus any intermediate certificates go into the **User Key Store**.

1. Once the authenticator has a bootstrap certificate the station repeats the process, this time authenticating with the bootstrap certificate instead of the device code.
2. This produces the rolling certificate. The station authenticates all subsequent requests with this rolling certificate.
3. After the **FederatedIdentityAuthenticator** has a rolling certificate, NiagaraCloudService uses it to authenticate to the device provisioning service.If the device is enrolled in Niagara Data Service, the device provisioning service will instruct Niagara Cloud Service to add the RPKAuthenticator to the station and creates the RPK authenticator's certificate in the **User Key Store**. This certificate is visible only in non-JACE platforms.

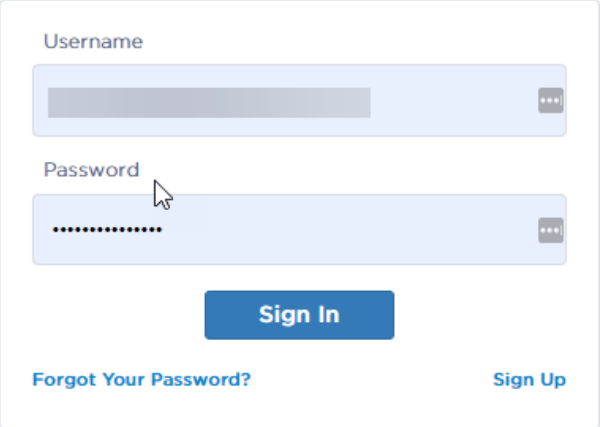
CAUTION: Since certificate management is automated for the Niagara Cloud Suite, **DO NOT delete these certificates without instruction from support**.

Signing in and out

Niagara-cloud.com requires you to sign in using your Niagara Community credentials. This procedure is for all users.

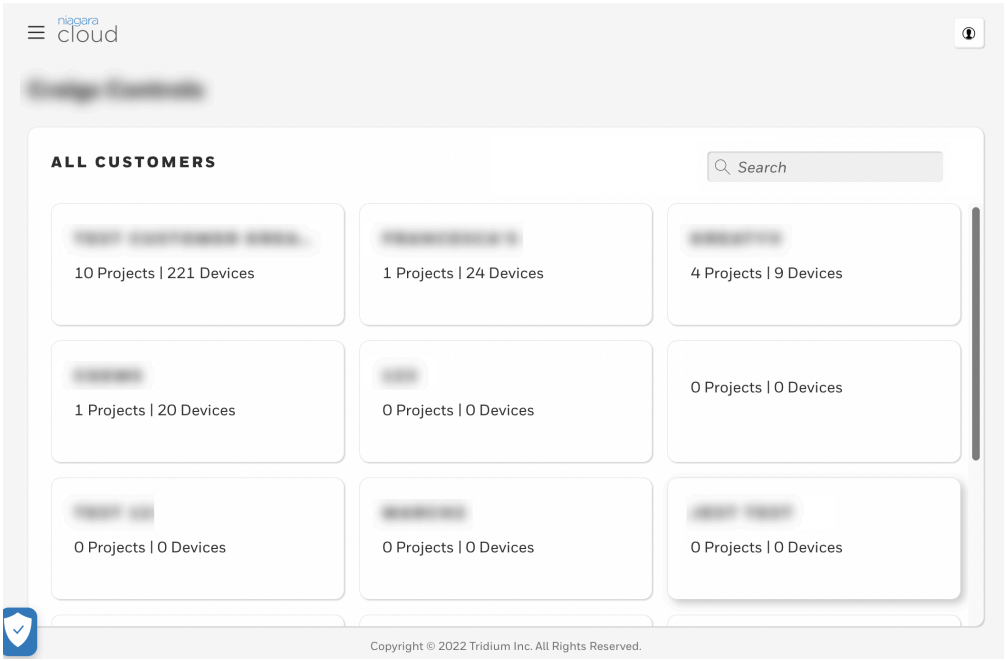
Prerequisites:
You have a Niagara Community account.

Step 1. Launch the Niagara Cloud (https://www.niagara-cloud.com).
The Niagara Community sign-in window opens.



Step 2. Enter your credentials and click **Sign In**.

The **Partner** view opens.



Step 3. To sign out, click the user actions button ( ) in the upper right corner of the view and click **Sign Out**.

Assigning partner user access

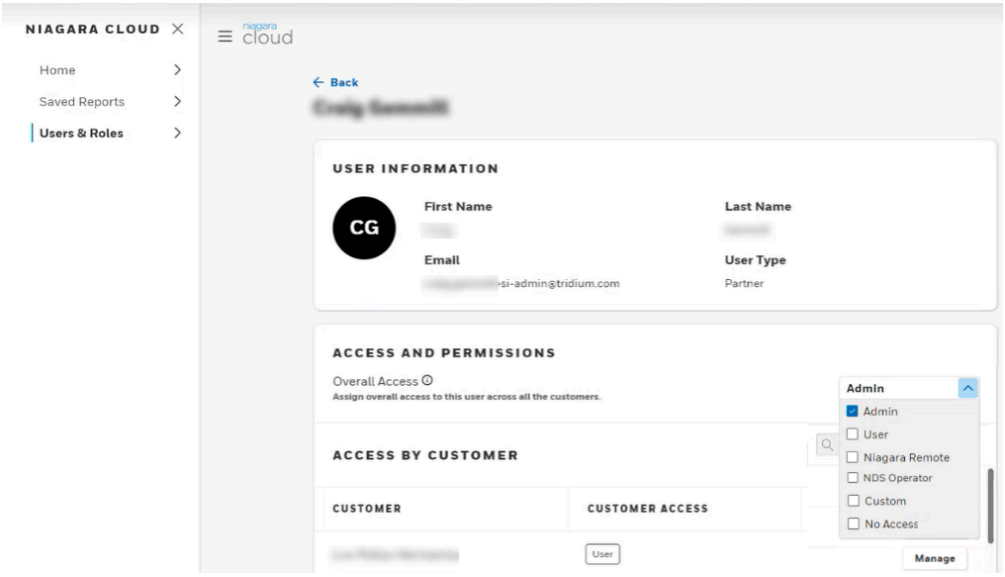
As a Partner admin modifying a Partner user, you can assign overall access or access at customer level.

Prerequisites:
You are a Partner admin. You have credentials to sign in to the Niagara Community.

Step 1. Sign in to the Niagara Cloud Management Portal (`https://www.niagara-cloud.com`) using your Niagara Community credentials.

Step 2. Navigate to **Users & Roles**, and from the list of ALL USERS, click the name of the desired **Partner** user.
The USER INFORMATION of the respective Partner opens.

Step 3. To assign access to a Partner at the organizational level, select the appropriate role from the **Overall Access** drop-down menu.

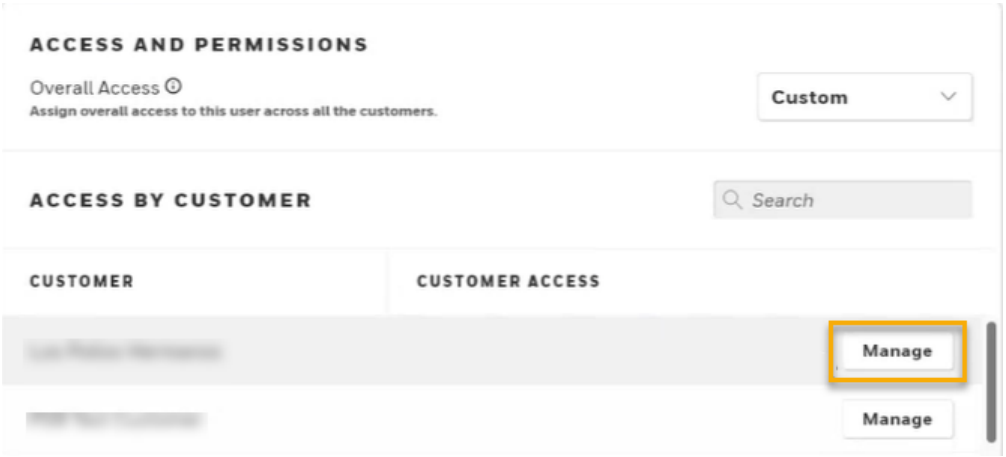


If you select `No Access`, all customer, project, and device-level permission changes will be lost.

All available roles briefly explained:

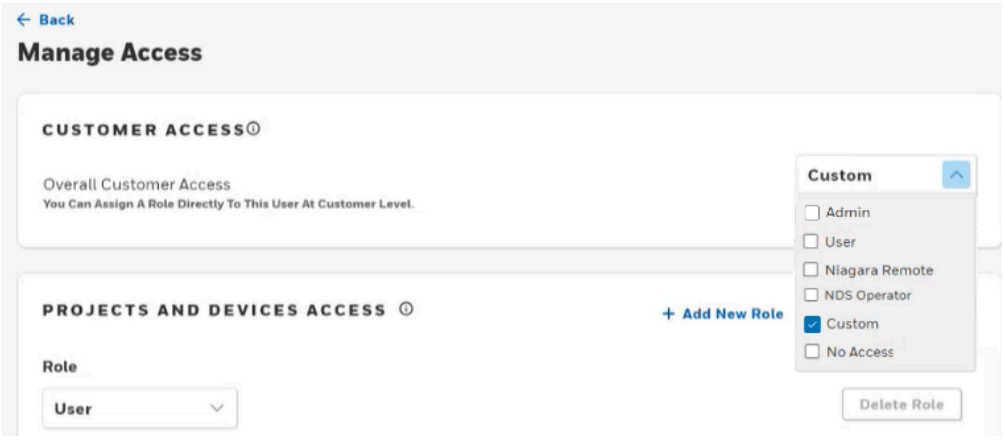
- *Admin*: Users with this permission have access to all customers, projects, and devices.
- *User*: Users with this permission have limited access to all customers, projects, and devices.
- Niagara Remote: Users with this permission have access to connect to customers, projects, and devices through Niagara Remote.
- *Nds Operator*: Users with this role have basic Niagara Data Service permissions in addition to permission to write point values.
- *Custom*: Individually provide the user access to customers, projects, and devices.
- *No Access*: This role revokes the user's access to customers, projects, and devices.

Step 4. If I want the user to have only limited access within this SI, select `Custom` and grant access at the individual customer level or project level. To manage access on the customer or project level, click **Manage** next to the customer name.



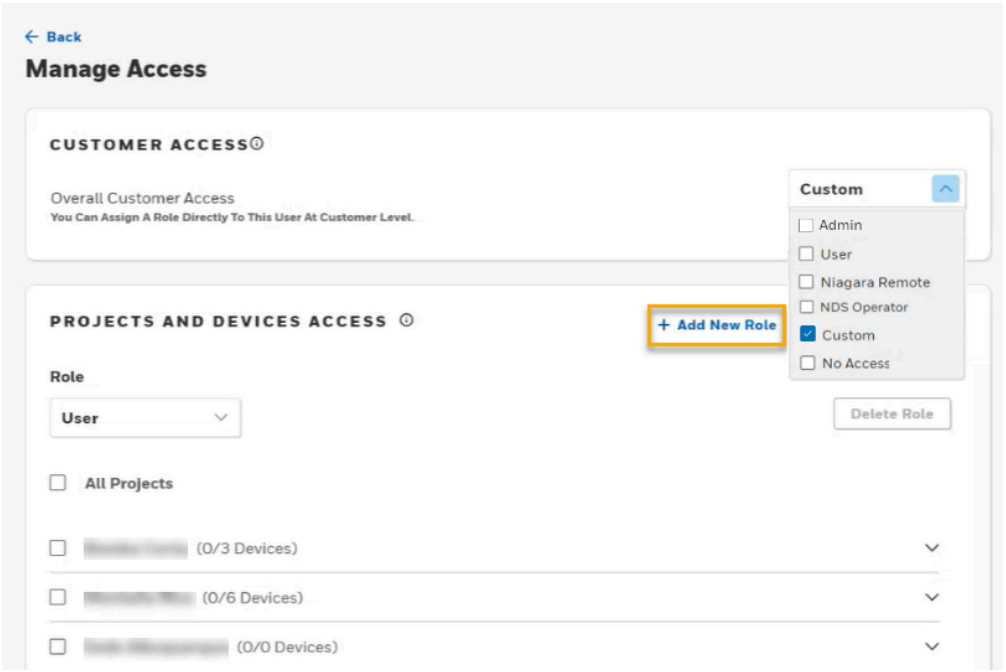
The **Manage Access** page opens.

Step 5. On the **Manage Access** page, select the desired access role.



Step 6. To grant a user the right to read and view all devices at the customer level, but at the same time, to allow the user to manage the registration and editing of certain devices for particular projects, do the following:

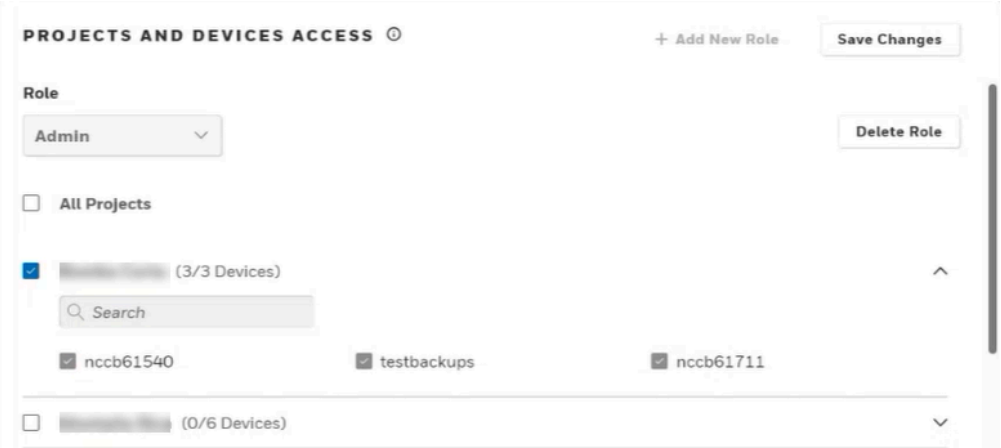
- Assign overall `User` access at the customer level. The **Change Customer Access?** window opens to confirm that by changing the user role, all project and device level permission changes will be lost.
- Click **+Add New Role** to assign `Admin` access to specific projects or devices.



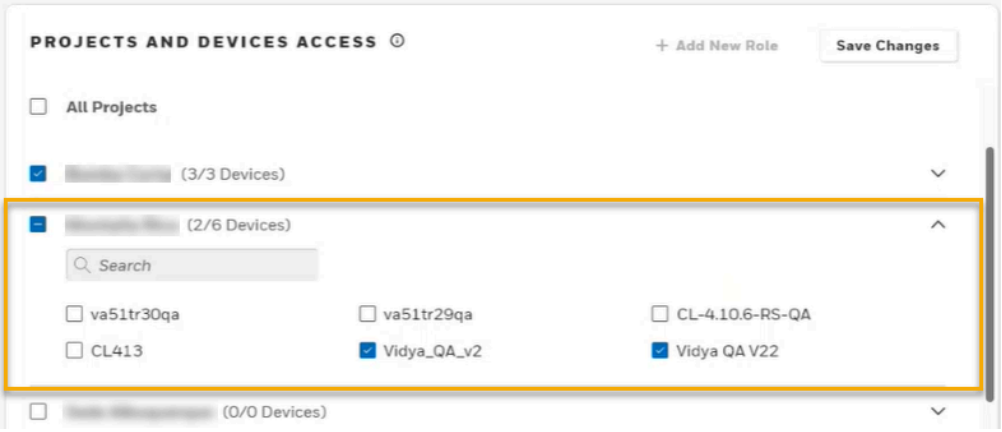
For the newly created role, the **Role** assignment automatically switches to `Admin` in the PROJECTS AND DEVICES ACCESS section.

Step 7. On the project level, you can now assign `Admin` access in two ways:

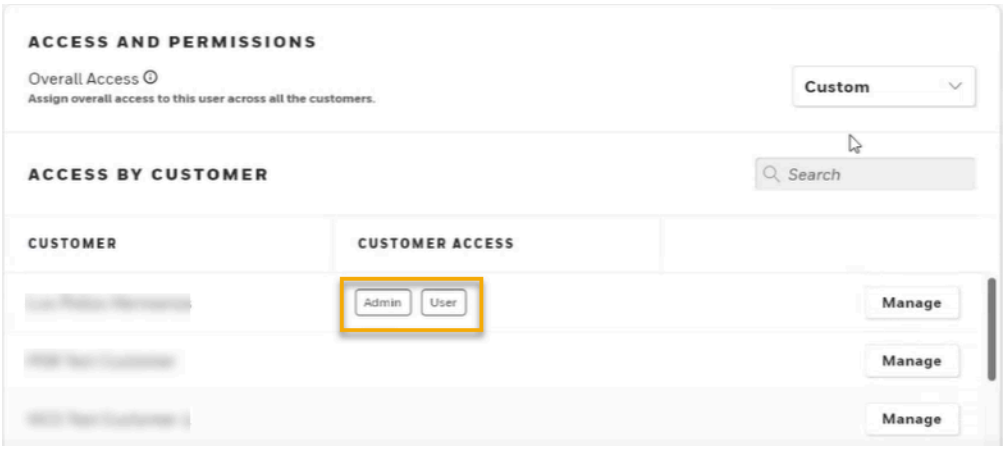
- Select the check box of a particular project to enable the user to edit and register new devices, and click **Save Changes**.



- Expand a particular project to view its registered devices, select the check boxes of those devices you want the user to manage, and click **Save Changes**.



On the USER INFORMATION page of this particular user, in the CUSTOMER ACCESS column, you can see the assigned access rights within a particular customer.



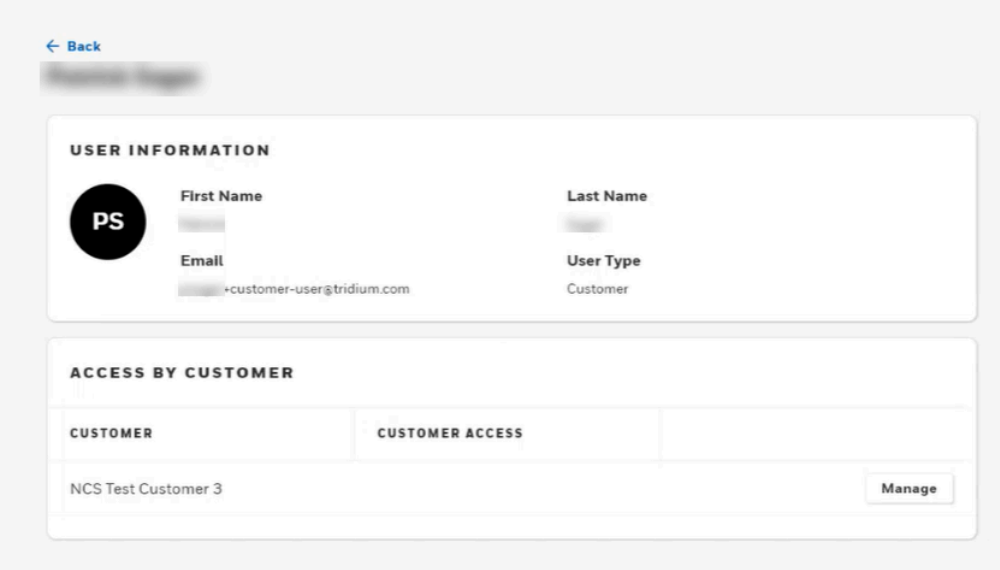
Assigning customer user access

As a Partner admin modifying a Customer user, you can only grant access to projects and devices within the customer with which the customer user is associated.

Prerequisites:
You are a Partner admin. You have credentials to sign in to the Niagara Community.

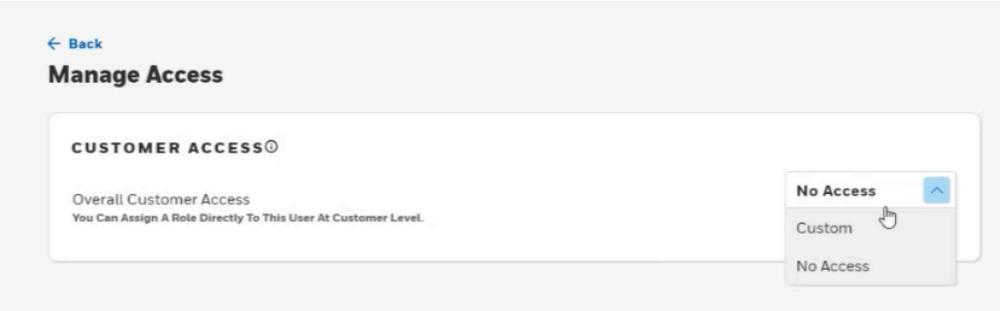
Step 1. Sign in to the Niagara Cloud Management Portal (`https://www.niagara-cloud.com`) using your Niagara Community credentials.

Step 2. Navigate to **Users & Roles**, and from the list of ALL USERS, click the name of the desired **Customer** user.
The USER INFORMATION of the respective Customer opens.



Step 3. Navigate to the customer of interest in the ACCESS BY CUSTOMER section, and click **Manage**.
The **Manage Access** page opens.

Step 4. Select from the drop-down menu if you want to grant **Custom** access or **No Access**.

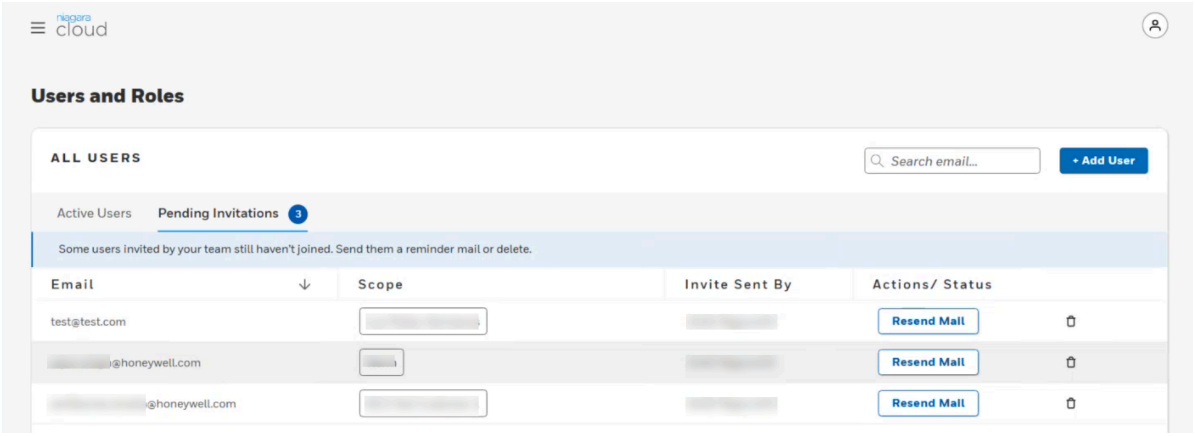


Sending user invitation to customer

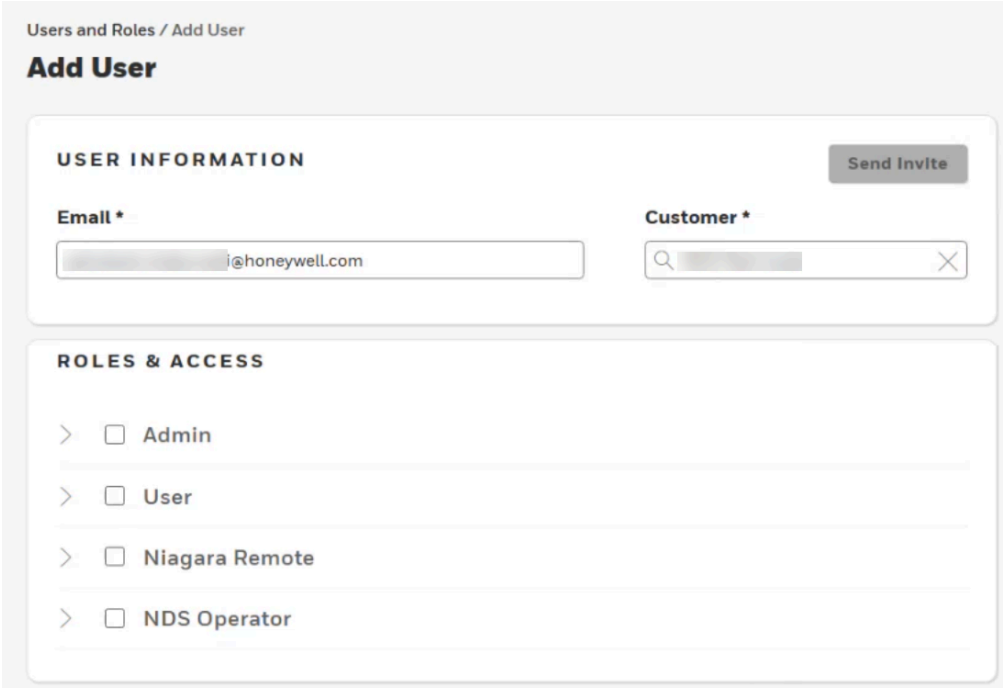
As a Partner admin, you can send user invitations to customers to allow them to join a particular customer organization.

Prerequisites:
You are logged in the Niagara Cloud Management Portal as a system integrator (SI).

Step 1. In the Niagara Cloud Management Portal, navigate to **Users & Roles**.



Step 2. In the upper right corner, click **Add User**.



Step 3. Enter a valid customer email and select the corresponding customer name (organization). After you selected the customer name, the **Roles & Access** options appear.

Step 4. From the **Roles & Access** options, select the role(s), project(s) and device(s) that you want the invited user to have, and click **Send Invite**.
A confirmation window appears in the upper right corner of the screen to inform you that the invitation has been sent successfully.

NOTE:

The invited user will receive an email, which contains information as to how to create a Niagara Community account needed to log in and access the newly assigned NCS customer organization. After the invited user logs into the Niagara Community account, a **User Invitation** window appears to prompt the user to accept or decline the invitation. Accepting the invitation will remove the user from the currently assigned organization. Declining it will direct the user to the currently assigned organization.

Once users activate their accounts in the Niagara Community, they may need to wait up to 30 minutes before they can log back into the NCS application. This waiting period ensures that the account is properly synced with Salesforce.

Step 5. To resend the same invitation to the customer, click **Resend Mail** in the **Actions/Status** column of

the appropriate customer.

Step 6. To delete a user invite, click the **Delete** icon next to the **Resend Mail** of the appropriate customer. Deleting the user invite will result in the loss of all added permissions at project and device level.

Editing project names

You may edit project names.

Prerequisites:
You have signed in to niagara-cloud.com.

The procedure to edit the customer and project names is the same.

Step 1. To edit either name, hover the cursor over the customer name or project row.
An edit icon ( ) appears to the right of the name.

Step 2. Click the edit icon.
A blue background for customer name and gray background for project opens behind the name.

Step 3. Edit the name and click outside the name property.
A success message in the upper right of the page indicates that the name changed.

Deleting projects

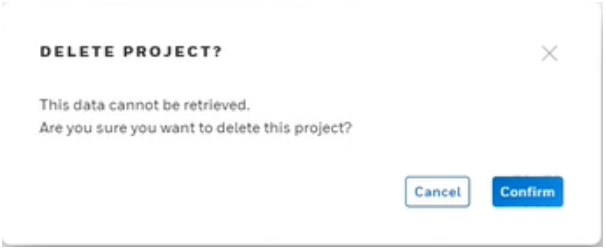
You may delete a project only if no devices are assigned to it.

Prerequisites:
The project is empty (contains no device assignments).

Step 1. Open the list of projects and select a project.

Step 2. Confirm that the project is empty (no devices are assigned to it).
The delete icon activates.

Step 3. Click the delete icon ( ).
A confirmation message opens.



Step 4. To delete the empty project, click **Confirm**.

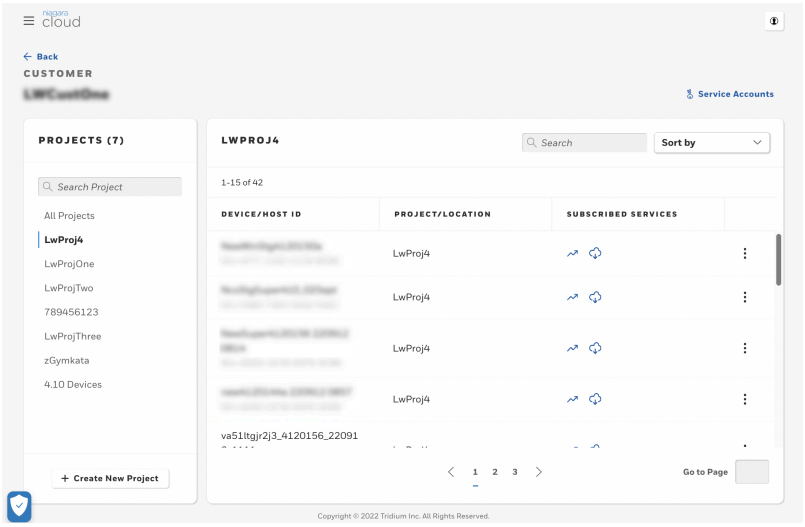
Setting up a project

A customer project can be any entity used by the customer to organize controller stations within the customer's company. This organization can be by location (city, floor, building), function, department, etc. This procedure is for Partner Admin users.

Prerequisites:
All devices have been registered. You are logged in to the Niagara Cloud Management Portal at the Integrator home page.

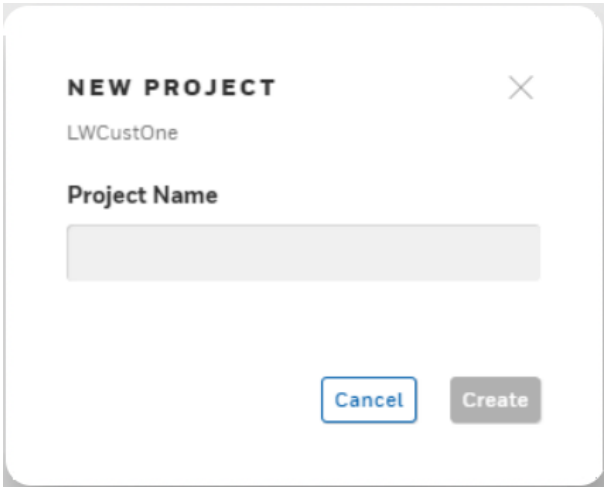
Step 1. Click a customer tile.

The **PROJECTS** view opens.



The left pane, **PROJECTS**, lists the projects.

Step 2. To create a new project, click **+ Create New Project**.
The **+ Create New Project** button is at the bottom of the Projects pane.
The **New Project** window opens.



Step 3. Enter a **`Project Name`** and **`Location`**, then click **Create**.
A message confirms the creation and the project appears in the left pane.

You can click to select this project, but no devices show in the table until you register each device with the project. Once device registration is complete, the service automatically adds the device to the project and it appears on the customer's project view.

Editing device information

You may change a device name, associate it with a different project or change its location.

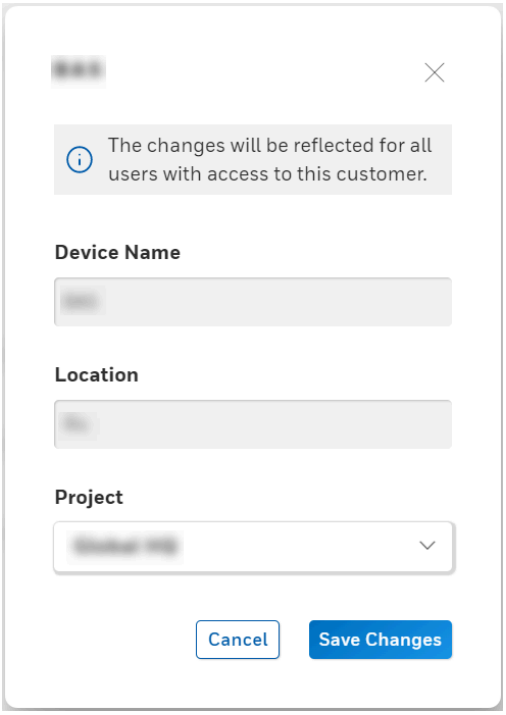
Prerequisites:
The device is registered and associated with the project.

Step 1. Open the customer page where the project and devices are currently associated.

Step 2. Find the device.
You may need to scroll or search on another page.

Step 3. Click the three vertical dots to the right of the device row.
An options list opens.

Step 4. Click **Edit**.
A window with two properties and a drop-down list opens.



The projects that appear in the **Project** drop-down list are for the current customer.

Step 5. Use the **Device Name** property to change the name of the device, the **Location** property to enter a different location, and **Project** drop-down list to associate this device with a different project, then click **Save Changes**.
The page activates the **Save Changes** button as soon as you make a change.
After saving changes, the interface reflects the change(s). For example, if you change the project, in future the device appears under the changed project within the customer.

Deleting a device

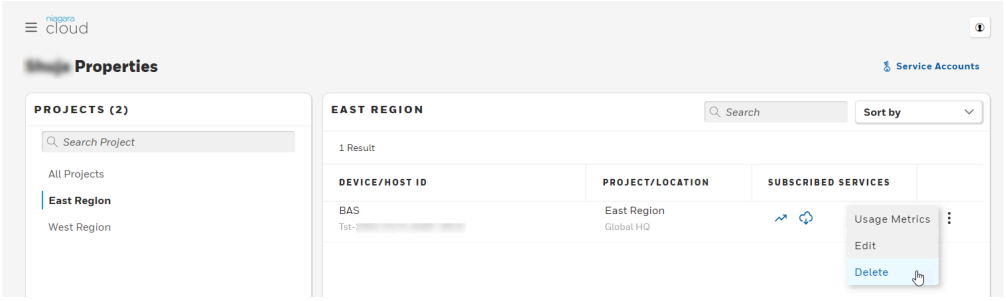
You can disassociate and delete a device from a project.

Prerequisites:
The device is registered and associated with a project.

Step 1. Open the customer page where the project and the device(s) are currently associated.

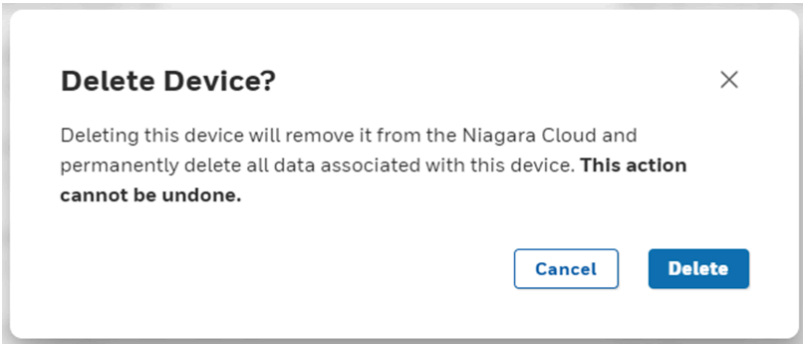
Step 2. Locate the device you want to delete.
You may need to search on another page.

Step 3. Click the three vertical dots to the right of the device row, and click **Delete**.



The **Delete Device?** window opens.

NOTE: Deleting the device permanently and irrevocably deletes all data associated with this device.

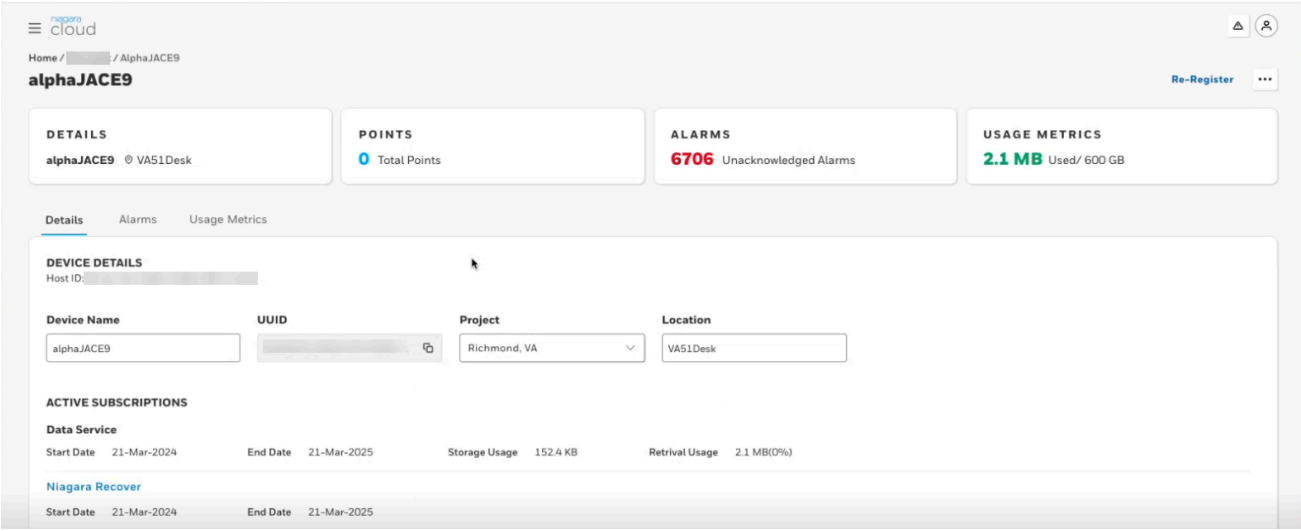


Step 4. Click **Delete** to delete the device.
In the upper right corner of the customer page, a message appears confirming that the device has been successfully deleted. The data associated with the deleted device cannot be retrieved.

NOTE: Deleting a device does not remove any of the station-side components. It is recommended to delete the **Niagara Cloud Service** manually from the station.

Viewing device details

The device details page allows you to view details such as device name, UUID, Host Id, project, and the location of a particular device, and you can see the data that the device has sent to the cloud.



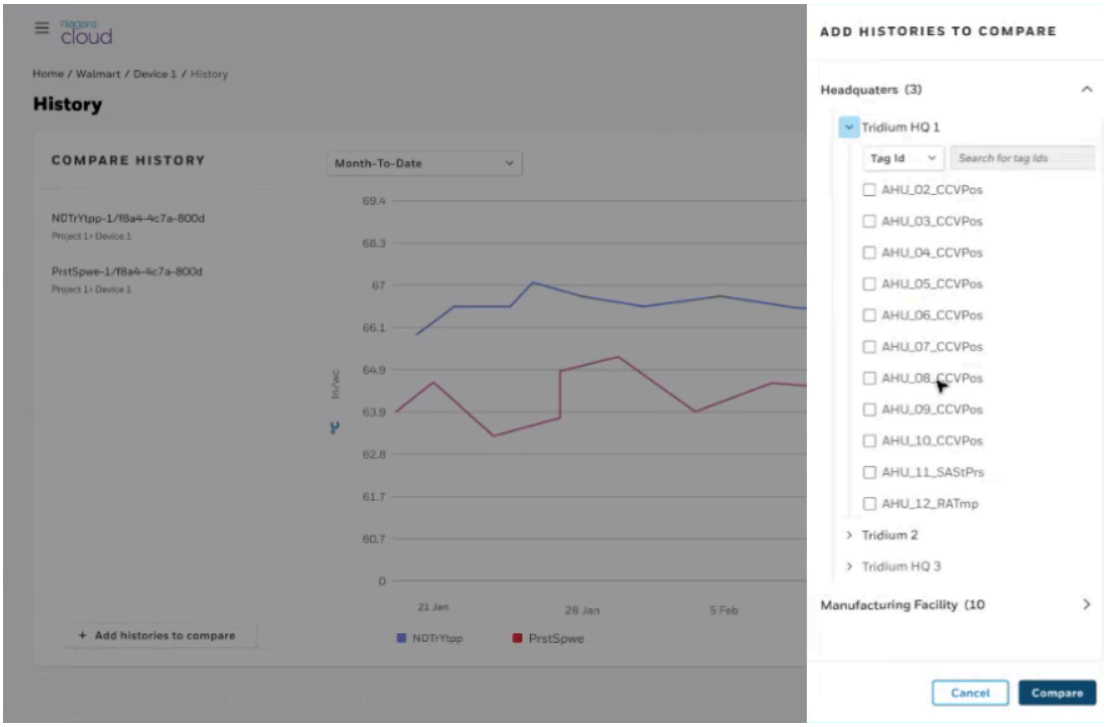
The **Device Details** page also provides the following functions:

- Edit the device name.
- Assign the device to a different project.

- Change the device's location.
- Delete a device.
- Re-register a device.
- On the **Alarms** tab, you can view all the alarms of the device and filter them by various categories such as duration, source, acknowledgement. You also have the option to show and hide columns, for example, the UUID or user column.
- On the **History** tab, you can view the history name and their corresponding telemetry Id. When you click on a history name, you will navigate to the **History** page where you can click the **Add histories to compare** option. From the right pane, you can select up to 10 points, which will populate the histories charts accordingly.

  NOTE: Charting features are not supported for history items that are of enum, boolean, or string types.

  You can save the report by clicking **Save Report** in the upper right corner of the **Compare History** screen. In the left pane that displays the selected histories, you can clear the histories from the **Compare Histories** list.



I

- On the **Usage Metrics** tab, you can view the retrieval usage of the Niagara Data Service with the options to select by month or total usage, and it displays the usage start date and end date.

Viewing usage metrics

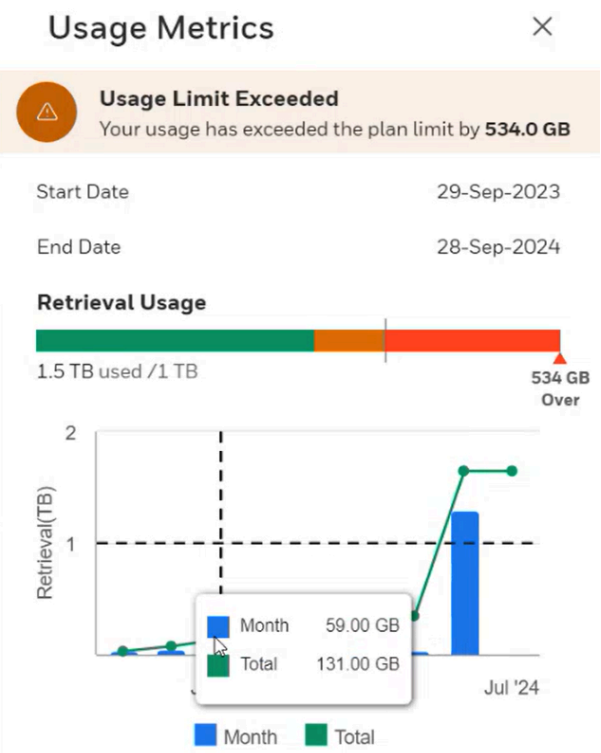
The Niagara Data Service keeps track of the number of records stored in the cloud and data retrieved for each device associated with each project.

Step 1. Open the customer page where the project and devices are currently associated.

Step 2. Select a project in the left pane.

Step 3. Locate the device, click on the vertical ellipsis on the right end of the device row and select **Usage Metrics**.

The **Usage Metrics** window opens.



The **Usage Metrics** window shows the subscription start and end dates. The **Retrieval Usage** bar displays up to 80% of usage in green, over 80% in orange, and over the limit (100%) in red. The chart shows usage bars per year or month, depending on your subscription terms (5 years, 3 years, 1 year). The usage limit is indicated by the dashed horizontal line. If you used more than 80% of your limit, a warning will be displayed.

Chapter 4. Niagara Data Service

This service is used by an SI to generate charts (reports). The charts are available at *niagara-cloud.com*.

The Niagara Data Service provides:

- Report creation implemented by an SI.
- Report viewing, which is available to all users.

The procedures in this chapter are designed to be performed in sequence.

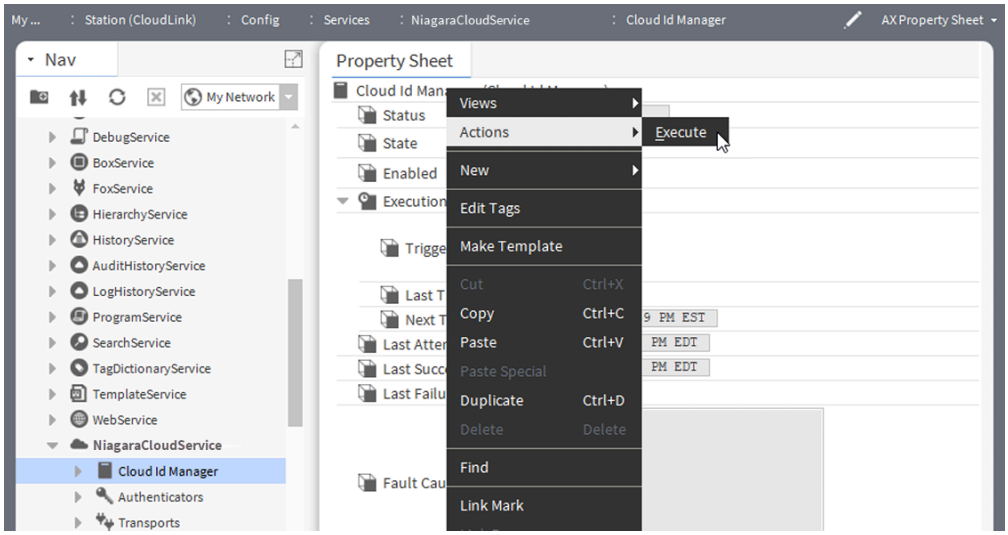
Exporting Model data to the cloud

Before the station can upload data to the cloud, it must run the Cloud Id Manager, which triggers a model upload after it has assigned cloud Ids. The following steps describe how to export model data to the cloud by executing the Cloud Id Manager, which adds cloud Ids and telemetry Ids. This also triggers a model export if there are new components, otherwise the model will not be sent. This process ensures that a station's model is kept up-to-date in the cloud.

Prerequisites:

- Your station is registered.
- You have configured your networks:
  1. Add networks.
  2. Add drivers.
  3. Add proxy points (optional for model data).
  4. Add history imports (required for model and telemetry data).
- You have configured local components.
  1. Add control points.
  2. Add history extensions (required for telemetry data).
- You have configured other histories as needed.
  1. Audit Service history
  2. Log Service history
  3. System Monitor Service history
- If needed, you have tagged with nc:excluded any components or folders that you do not wish to send to the cloud.

Step 1. To run the **Cloud Id Manager** component, expand **Config** > **Services** > **NiagaraCloudService**.



Step 2. Right-click Cloud Id Manager and select **Actions** > **Execute**.

Result
The amount of time the export takes depends on the number of components in your station. You can monitor the status of the model export job in the Job Service.

After every configuration update of your network, local components, and histories, export the Model again.

NOTE: The recommended execution sequence is that you first configure the History exports, and then enable them.

Configuring histories to export data to the portal

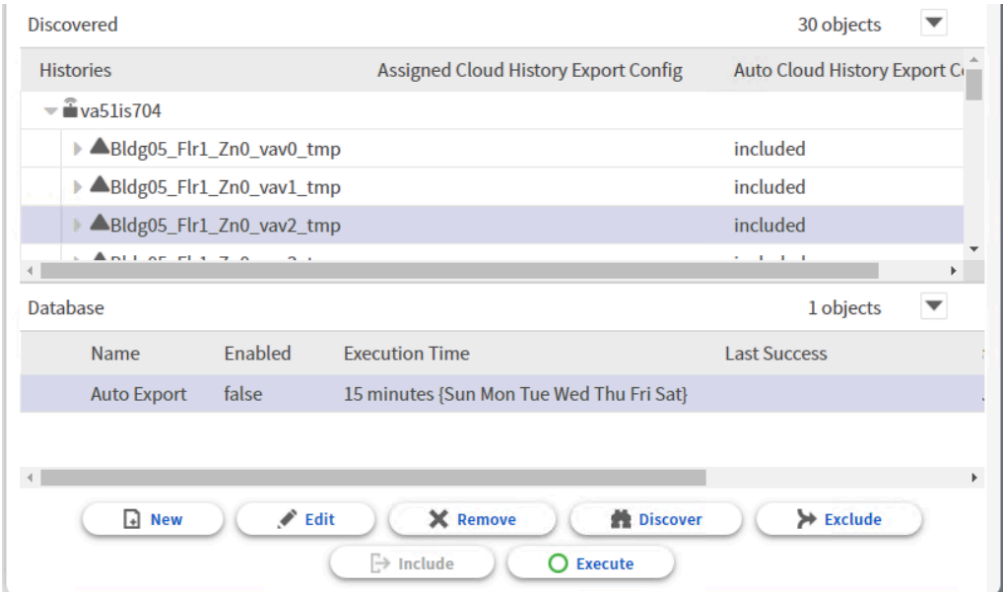
Automatic export of histories to the cloud must be enabled. By default, all histories are included for Auto Export. The default auto export Interval is 15 minutes.

Prerequisites:
You are connected to the station from which you uploaded the data model to the cloud.

Step 1. Double-click on the **Exports** container under **Channels/Histories**.
The configuration page opens.

Step 2. To view the available histories, click **Discover**.

The discovery job identifies the available histories.



Step 3. Select one or more histories to export and click **Include**.
Selecting a history causes the **Assign** and **Unassign** buttons to automatically change to **Include** and **Exclude** buttons.

For large stations, you should use only **`Auto Export`** without selecting individual histories for inclusion/exclusion.

Step 4. Configure **`Auto Export`**, **`Trigger Mode Interval`** and click **Save**.

Next steps
As an alternative, you may create a new, custom history export configuration. This is recommended only for stations with few history records that need to be exported on a different interval.

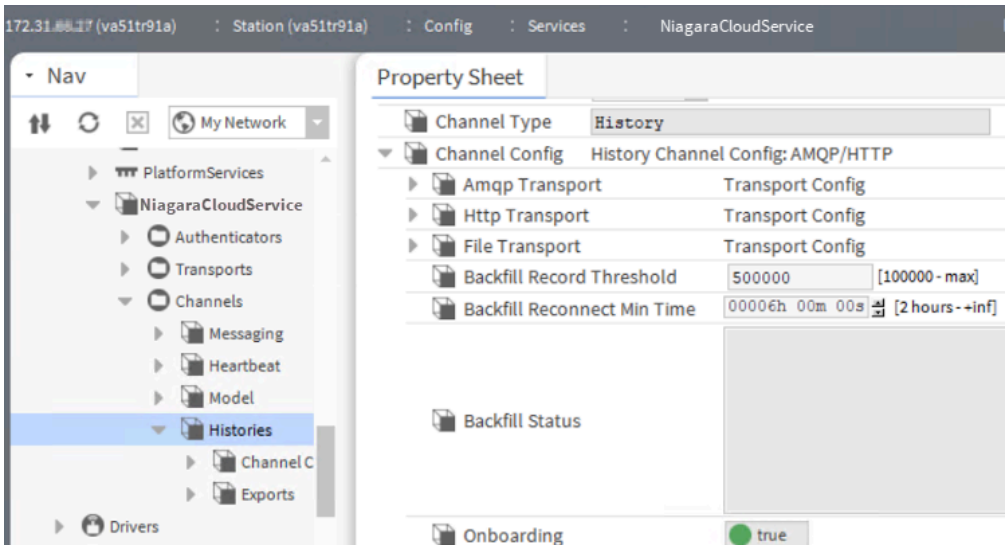
Bulk upload and activating the channel

If your station has a large number of records, uploading them to the cloud one by one could take a long time. When the number of records in an existing station exceeds a specified number, which defaults to 500,000, the system automatically collects the records into files and uploads the files through the IoT Hub to the cloud. Even so, depending on the amount of data, bulk upload can take additional time.

Prerequisites:
You are working in Workbench and are connected to the station from which you uploaded the data model to the cloud.

Step 1. Expand **NiagaraCloudService** > **Channels** > **Histories** and double-click **Channel Config**.

The **Channel Config AX Property Sheet** opens.



The Backfill properties configure a bulk upload. **`Backfill Record Threshold`** defaults to 500,000 records. This means that across all histories in the station, if there are 500,000 or more records waiting to be sent to the cloud, the backfill function packages the records into files, which it sends to the cloud through the IoT Hub instead of passing the records individually through the IoT Hub.

A change to the **`Backfill Record Threshold`** applies whenever you onboard additional records even if the station has been disconnected from the cloud for a long period of time.

NOTE: The auto export defaults to disabled so enabling the auto export or creating a new export policy serves as channel activation.

Step 2. To immediately upload data to the cloud, right-click **Auto Export** and click **Actions** > **Execute**.

Step 3. To confirm the execution check the **`Last Success`** property.

Result
Bulk upload uses the HTTP Transport component to upload the files to the cloud. In the cloud, a database stores all the uploaded records. There may be some additional delay between when a bulk upload leaves the station and arrives in the database. The quantity of records and the load in the cloud determine when the records will be available.

To view the data records in the cloud you would use the Niagara Data Service function at niagara-cloud.com.

Searching for histories

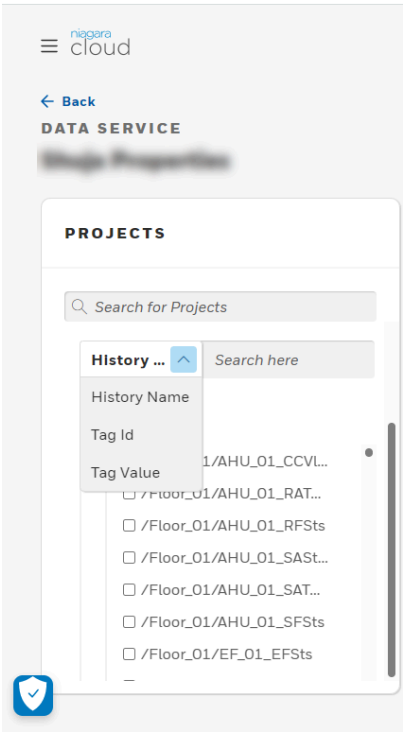
Once your histories are in the cloud, you can search for a specific history using its name, an associated tag or tag value.

Prerequisites:
Your points have history extensions. You are a system administrator with admin rights to the Niagara Cloud portal. Your history extensions are tagged or you know the specific history name you are looking for. History data are available in the cloud.

Step 1. Sign in to the Niagara Cloud (https://www.niagara-cloud.com) using your Niagara Community credentials.
The **ALL CUSTOMERS** view opens.

Step 2. Click the customer tile, select a project from the **PROJECTS** column and, along a project row, click the Data Service ( ) for a specific station.

Under the **PROJECTS** column, the system opens the specific station you selected and displays the search fields.



Step 3. From the **Tag Id** drop-down list, select the type of search.
Tag Id searches for a history by tag name, for example, `n:geoCity`.

Tag Value searches for a history by the tag name and value associated with the tag name, for example, `n:geoCity=New York`.

History Name searches for a specific history by its full name, for example, `/Station101/NumericWritable`.

Step 4. Enter the search value in the *Search here* field and press **enter**.
When searching for a specific history, you must type the whole string, for example `/Station101/NumericWritable`.
The system searches for the history within the currently-open station and displays the search results under the station name in the left column. It does not search all stations in the database.

If you searched for a **Tag Id**, the display includes all histories that are tagged with the name you entered.

If you searched for a **Tag Value**, the display includes all histories with the name and value you entered.

If you searched for a specific **History Name**, the display shows the single history name you entered.

For **Tag Id** and **Tag Value** searches you may enter multiple names separated by commas. For example: `n:name,n:type,n:geoState` (no space after each comma)

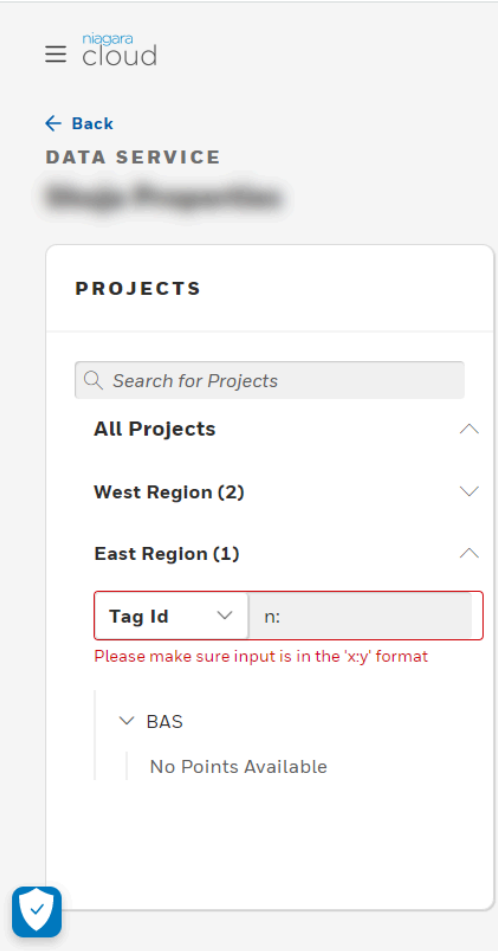
In this example, the only histories displayed would be those that have all the Tag Ids.

Search errors

Searching requires you to supply exact syntax for each search argument. Several error messages identify what is required.

Tag Id search error

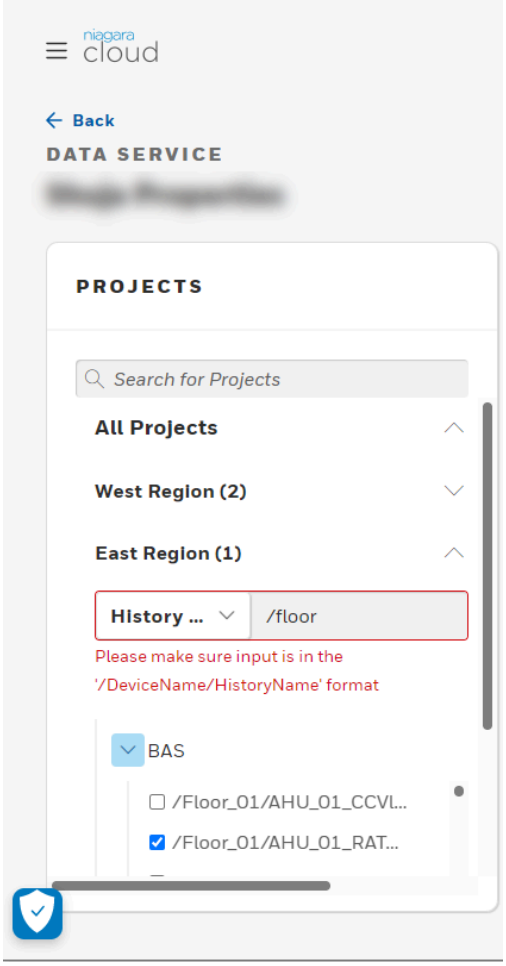
When searching using a tag, you must supply the full tag.



In the screen capture, the user provided only part of the tag ID. The message, “Please make sure input is in the ‘x:y’ format,” reminds you of the required format.

History search error

When searching using a history, you must supply the full name.



In the screen capture, the user provided only the beginning of the file name. The message, "Please make sure input is in the '/DeviceName/HistoryName' format," reminds you of the required complete format.

Creating and saving reports (charts)

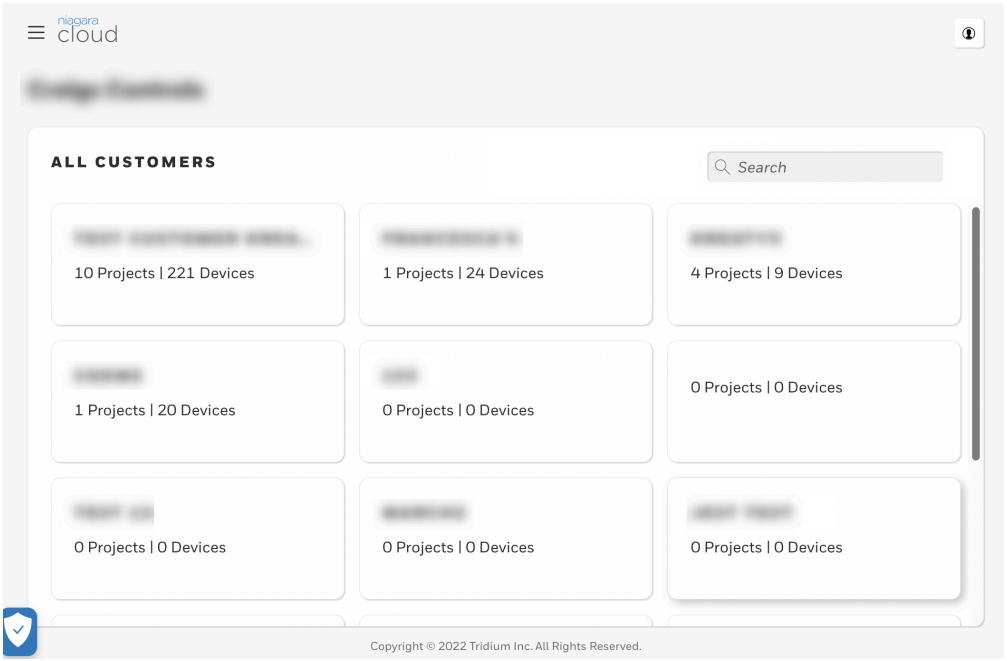
On-demand reports display data but are not saved for future use. Saved reports are available for customers to view. You may export an on-demand or a saved report either as a PDF or CSV file. This procedure is for Partner Admin users.

Prerequisites:
The partner and customer accounts and projects exist in the portal. The associated devices (stations) have been registered with the Niagara cloud, the model exported and histories successfully exported from the stations to the cloud.

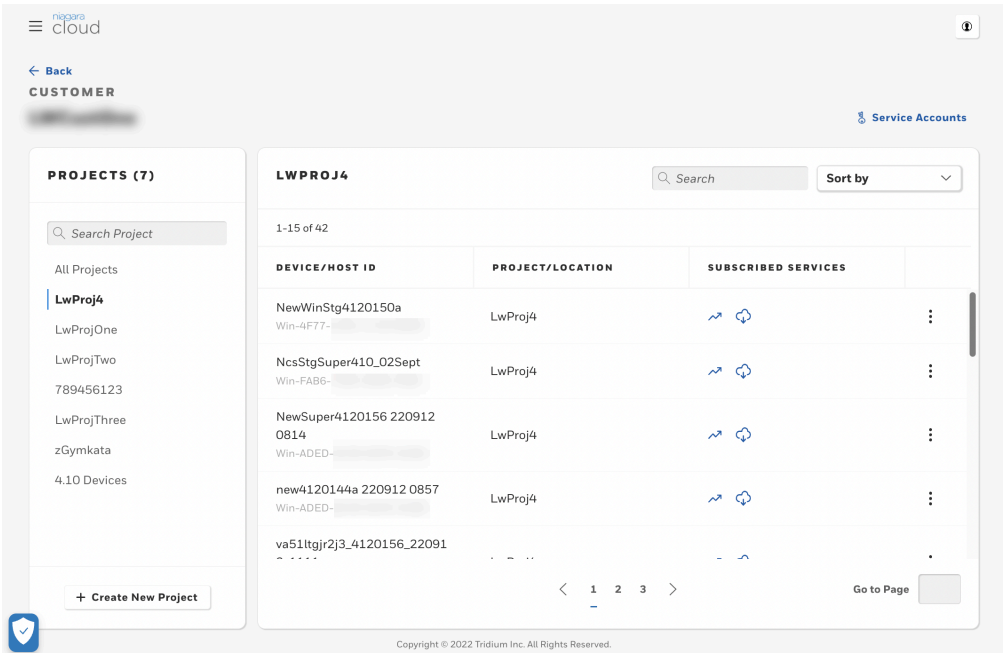
NOTE: The system creates charts from numeric, Boolean and enum history data. Exporting string data to CSV is not supported.

Step 1. Sign in to the Niagara Cloud (https://www.niagara-cloud.com) using your Niagara Community credentials.

The **ALL CUSTOMERS** view opens.



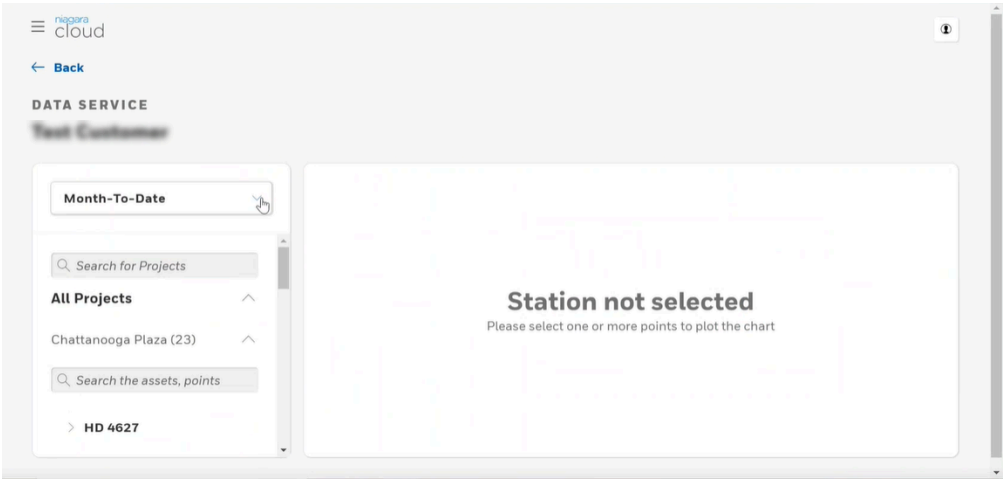
Step 2. Click a customer tile.
The **PROJECTS** view opens with all customer projects listed in the left column.



Step 3. Select a project and locate the device (station) in the center of the view.
The selected project is highlighted on the Nav tree. On the project view, you may need to scroll to find the device or you can search for the device name using the search box at the top right of the view.

Step 4. Click the **Data Service** link ( ) under the device's **Subscribed Services** column.

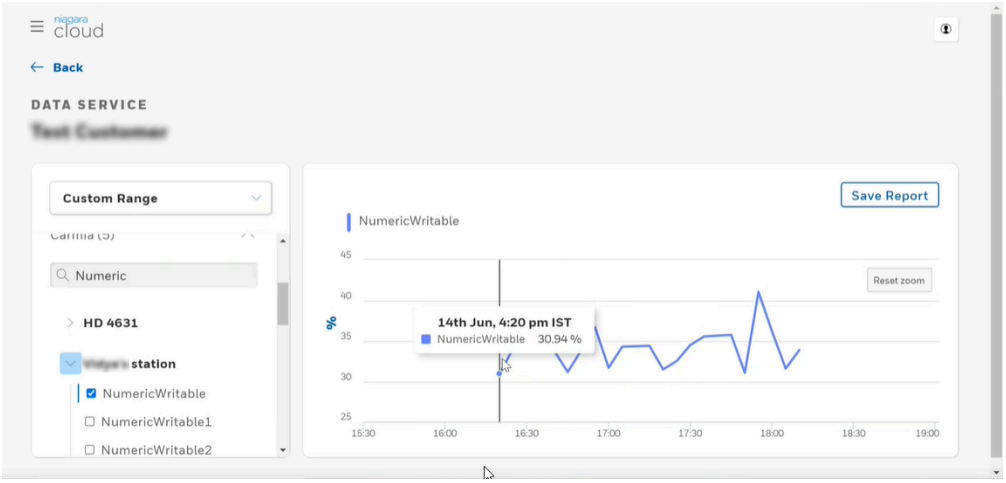
The **DATA SERVICE** view opens.



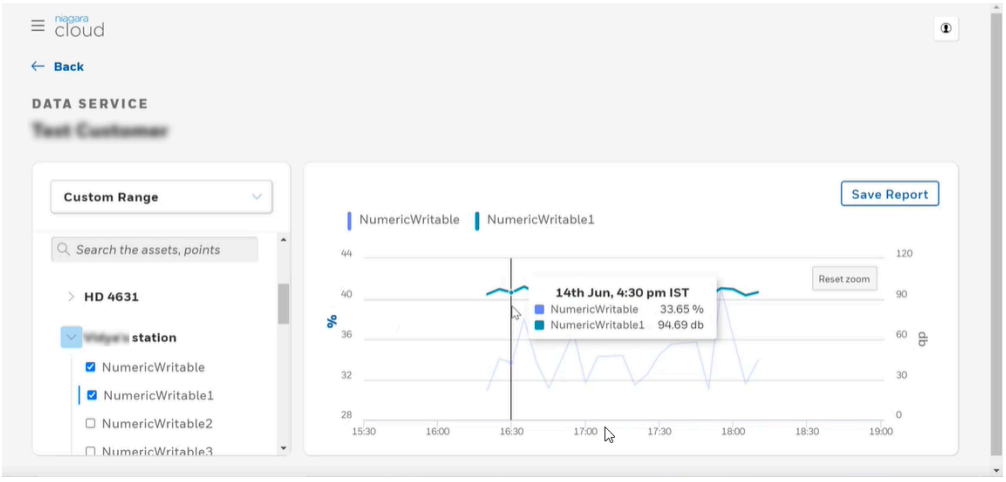
Step 5. Configure the date range for the report.
This range defaults to `Month-to-Date`. In addition, options include `Last 7 days`, `Today`, `Last 3 months`, `Last 6 Months`, `Year To Date` and `Custom Range`, which pops up a calendar for easy selection.

Step 6. To select the source values (for example, point values) to chart, scroll down, expand the station name and click the selection check box to the left of the source name.
You may search for specific source values. You can select up to 10 sources together on the same chart.

The software plots the source data.



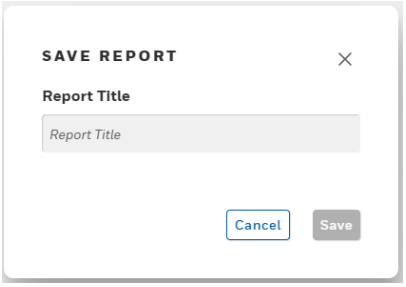
If you selected more than one source, the software plots them all on the same chart.



Step 7. To view the value for an individual source, move the cursor along the displayed line in the center of the chart.

Passing the cursor over a time instance causes the tool tip to display the source's value at that time. When you select multiple sources, the tool tip displays the values for all the sources at the selected time.

Step 8. When you get the report the way you want it, click **Save Report**.
The **SAVE REPORT** window opens.



Step 9. Enter a report name and click **Save**.

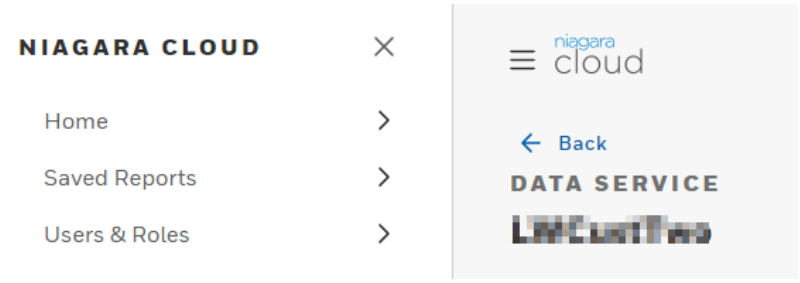
The report is now available for a customer user to view.

Viewing and exporting saved reports

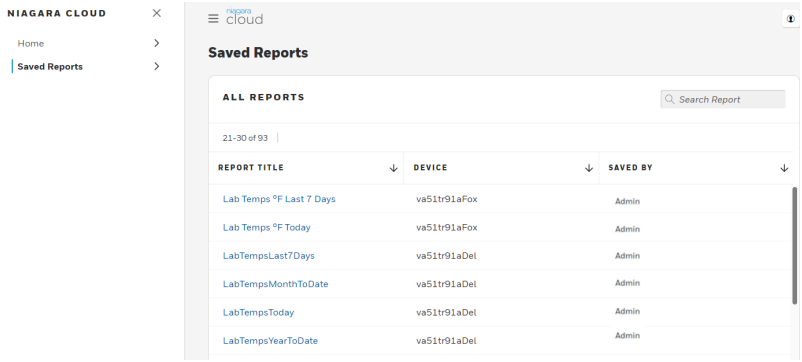
Saved reports differ from on-demand reports in that they have names and can be viewed by admin and customer users at any time.

Prerequisites:
You are a Partner Admin user and have signed in to `https://www.niagara-cloud.com`.

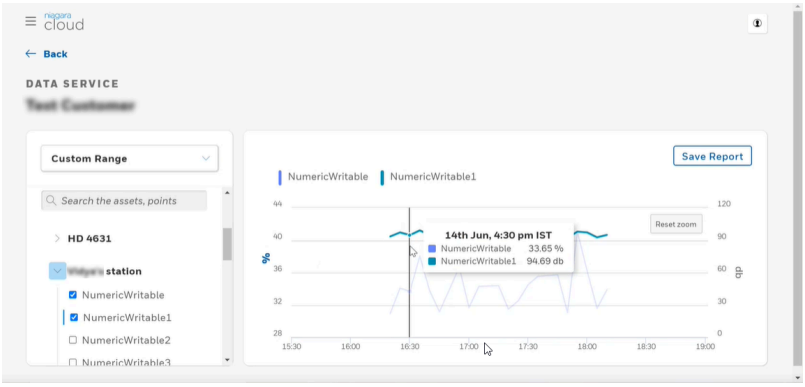
Step 1. Select a customer, select a project and click the **Data Service** link ( ).
The **DATA SERVICE** view opens.



Step 2. Click the menu button ( ) and choose **Saved Reports**.
The list of reports opens.



Step 3. Select the **REPORT TITLE**, **DEVICE** (station) and report creator (**SAVED BY**).
The report opens.

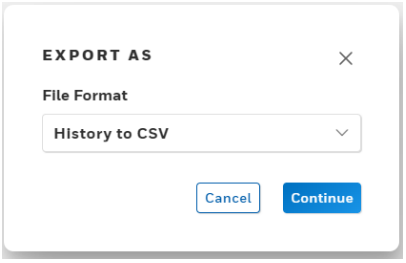


Each report can include data from more than one device.

Step 4. To view the value for an individual point, move the cursor along the displayed line in the center of the chart.

Passing the cursor over a time instance causes the tooltip to display the point's value at that time. When you select multiple points, the tooltip displays the values for all the points at the selected time.

Step 5. To export this saved report, click the export button ( ) in the upper right of the view (to the left of the **Save Report** button).
The **EXPORT AS** window opens.



Your choices are **History to Chart PDF** and **History to CSV**.

Step 6. Select the type of export from the drop-down list and click **Continue**.
The system saves the PDF or CSV file in your computer's **Downloads** folder.

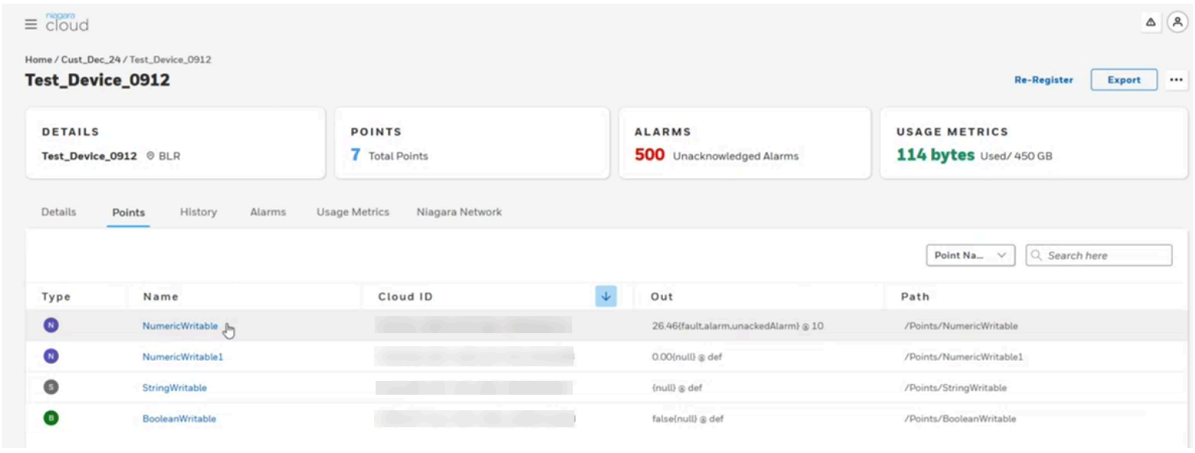
Live reading and writing of point data

The live read and write functionality allows you to read and write numerical, string, Boolean, and enum point data. This enables you to make better control decisions for cloud-based building systems.

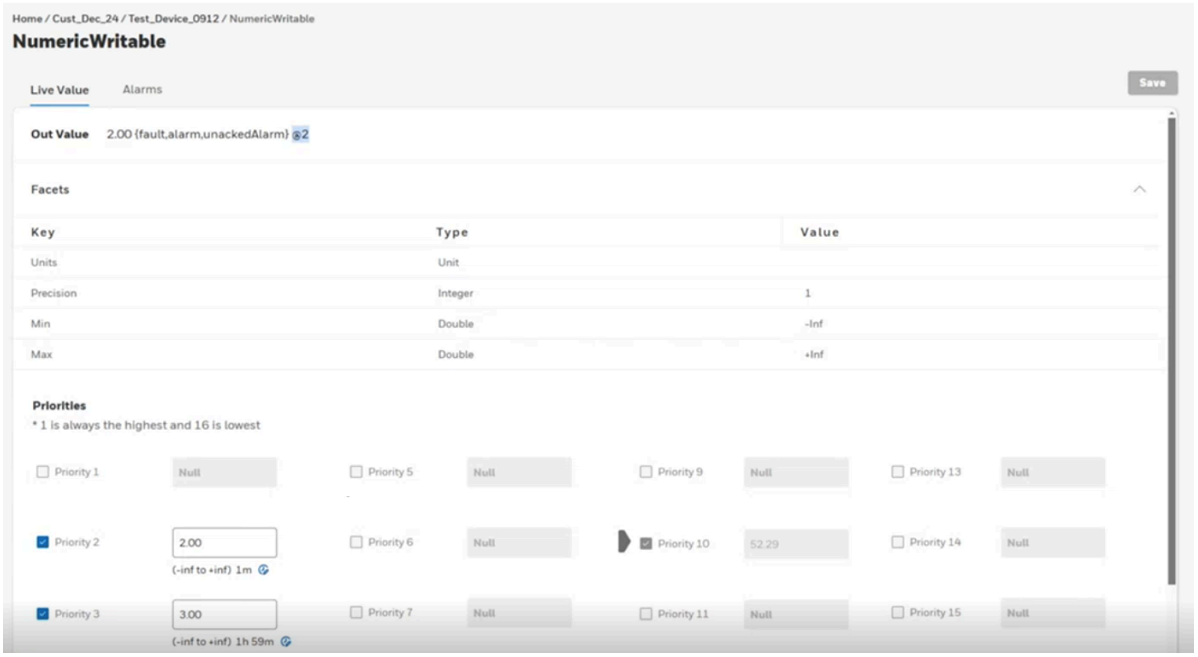
Prerequisites:
When commanding points from the cloud, it is important to have the **Operator Role** assigned to your user account. This role is necessary to ensure that you have the proper permissions and to enable seamless interaction with points through the cloud interface.

Security considerations: The service account user executes write commands to a station. It is essential to configure the station with specific roles that define what actions this account is authorized to perform. This setup allows you to manage which Niagara Cloud users can write and modify data.

Step 1. In the Niagara Cloud Management Portal, navigate to the Device Details page of the respective customer and select the **Points** tab.



Step 2. On the **Points** tab, click on the desired point to navigate to the **Live Value** tab.

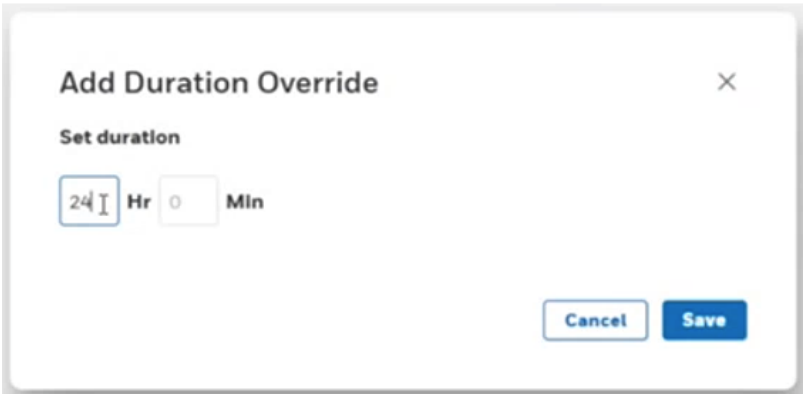


You can view the current **`Out Value`** and the **`Facets`** values of this particular point. The **`Min`** and **`Max`** value range determines the range within which you set the priorities.

Step 3. Based on the facets values and the point type, set the priorities as needed in the **Priorities** section. There are 16 priorities in total with Priority 1 being the highest priority and Priority 16 the lowest priority.

NOTE: You cannot edit Priority 1 because in Niagara Cloud it is highly recommended to create safety level commands to the station manually and on premise.

Step 4. To specify the duration override of a priority, click the clock icon located underneath the priority value field.
The **Add Duration Override** window opens.



Step 5. Enter the desired duration and click **Save**.
The default time is 15 minutes. Maximum duration is 24 hours.

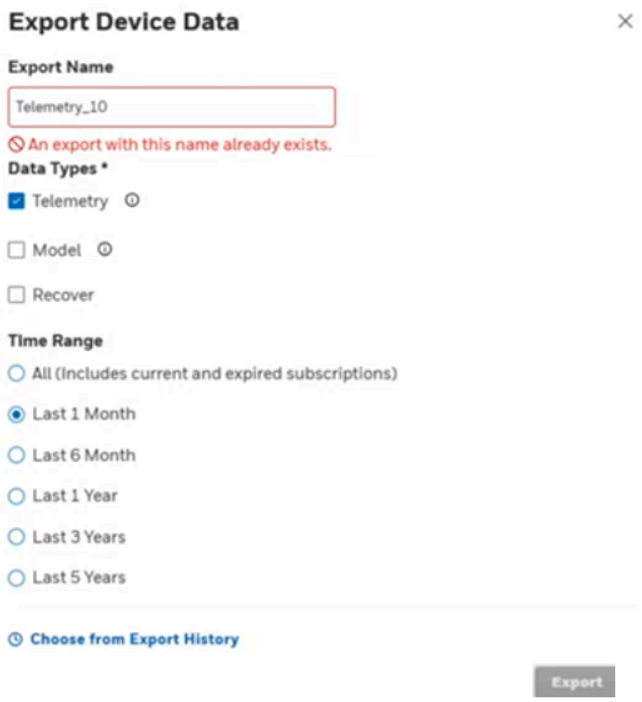
Step 6. Repeat the same step for additional priorities if needed and click **Save** in the upper-right corner of the **Live Value** page of the point.
To be able to see the current **`Out Value`** based on the defined priorities and durations, refresh the **Live Value** tab.

Step 7. To cancel the action, deselect the **Priority** checkbox or adjust the time duration accordingly.

Exporting device data

On the **Device Details** page, you can perform bulk exports of device data. The types you can export are Telemetry, Model, and Recover data.

Step 1. On the **Device Details** page, click **Export** in the upper right corner of the screen.
The **Export Device Data** window opens.



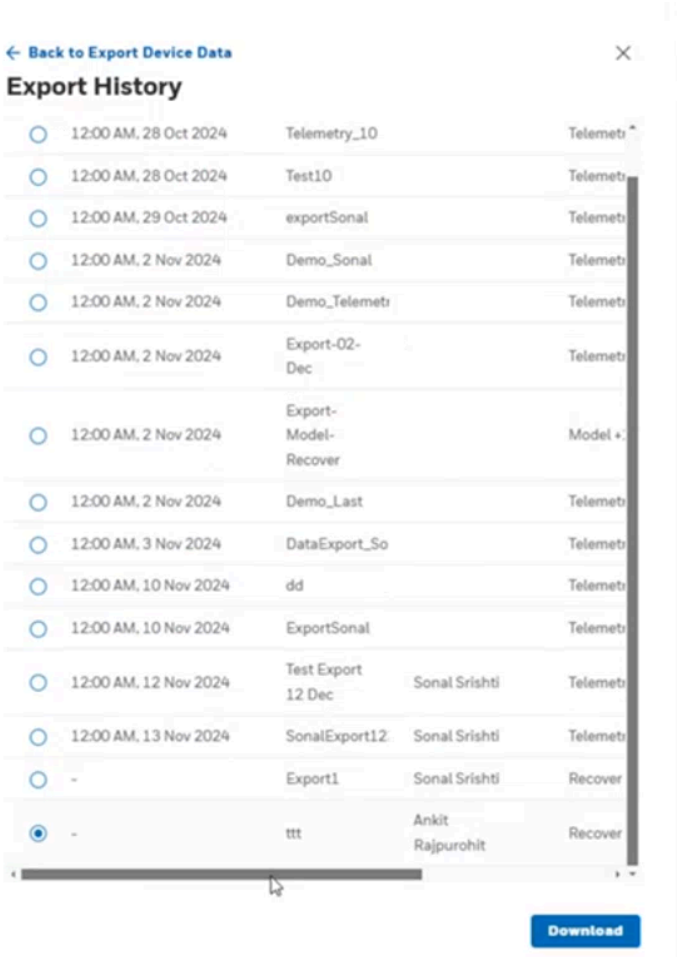
Step 2. Enter an export name that does not exist yet, select the desired data type(s) and time range, and click **Export**.

- Telemetry: Histories/telemetries that are sent from the Niagara station to the cloud.
- Model: The semantic model information about point values that are sent from the Niagara station to the cloud.
- Recover: Uploads station backup distribution files to the cloud.

You can close the browser without stopping the export action. It will continue to export the data.

Step 3. To cancel the export action, click X in the export status window.

Step 4. To view the exported data, navigate to **Export** > **Choose from Export History** > **Export History** from where you can download the exported data.



Step 5. In addition, on the Niagara Cloud Management Portal homepage under **Saved Exports**, you can view, retry the export action, download and delete all completed exports from all devices.

Exporting on-demand reports (charts)

The export feature provided by NDS creates a PDF of an on-demand chart.

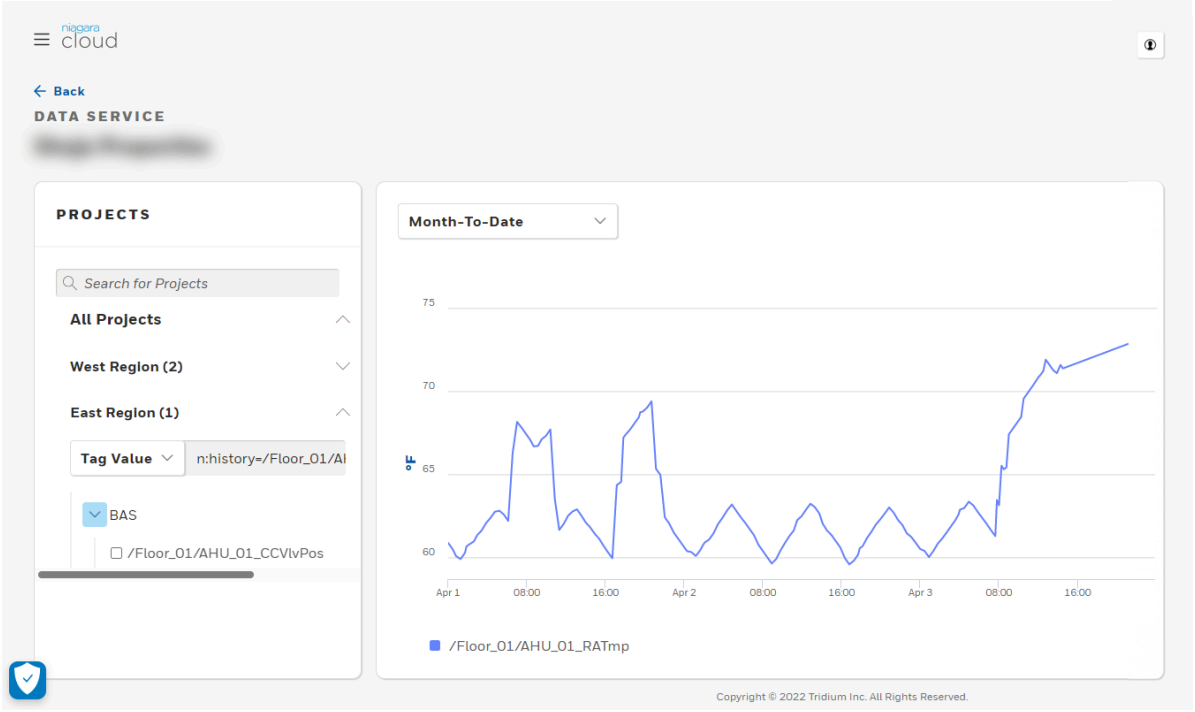
Prerequisites:
You are a system administrator with admin rights to the Niagara Cloud portal. You are already signed in to `https://www.niagara-cloud.com`.

On-demand charts do not have titles. Saved charts, which customers can view, have titles. This procedure demonstrates how to export an on-demand report.

Step 1. Click the customer tile, select a project from the **PROJECTS** column and, along a project row, click the **Data Service** link ( ) for a specific station.
Under the **PROJECTS** column, the system opens the specific station you selected and displays the search drop-down list.

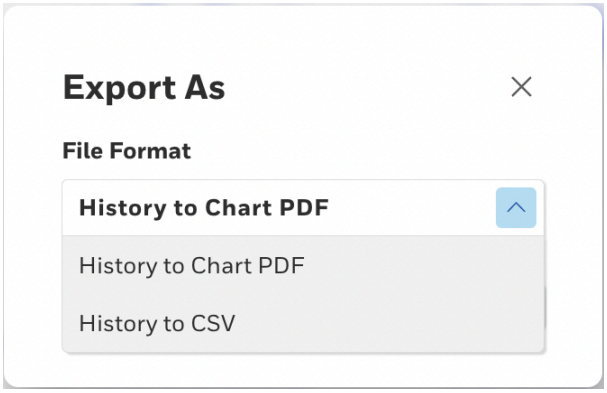
Step 2. Search for a history by **Tag Id**, **Tag Value** or **History Name**.

The available histories display under the station name in the **PROJECTS** column.



Step 3. Configure the date range for the report.
The system retrieves the history data and constructs the line chart.

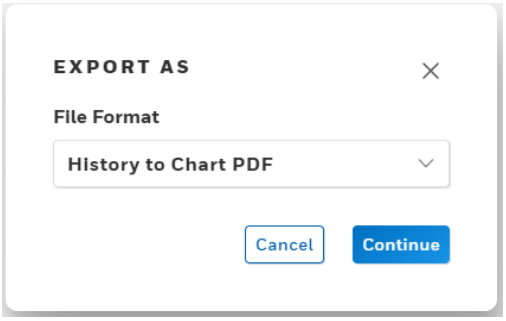
Step 4. To export this on-demand chart, click the export button ( ) in the upper right of the view (to the left of the **Save Report** button).
The **EXPORT AS** window opens.



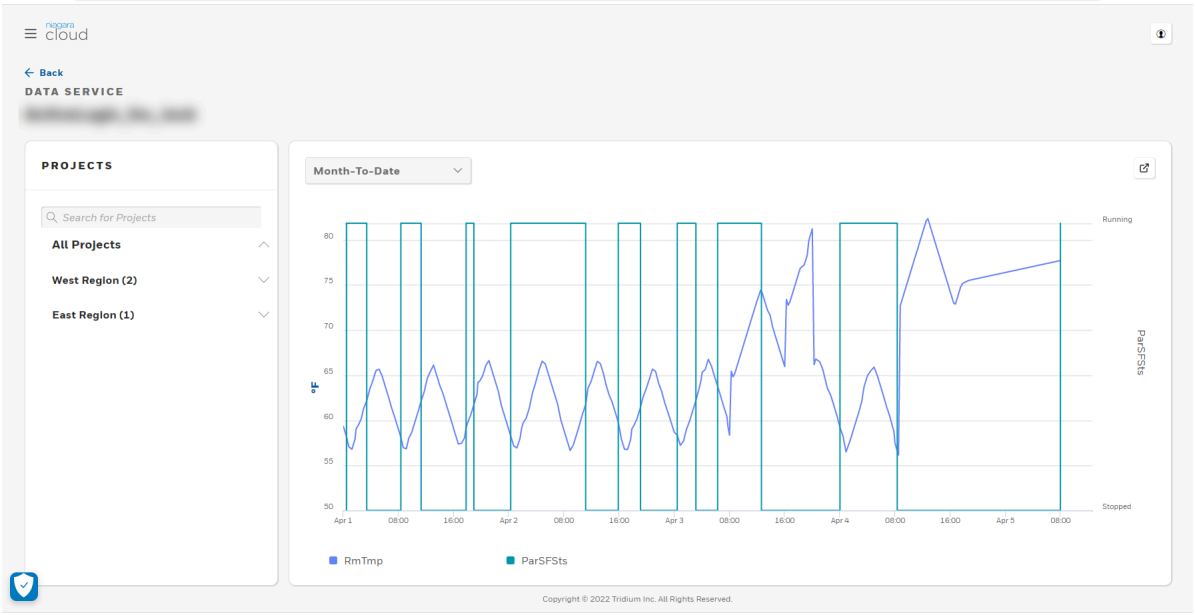
Your choices are **Export Chart as PDF** and **Export Histories as CSV**.

Step 5. Select a PDF or CSV file.

The EXPORT AS window displays your choice.



Step 6. To continue, click **Continue**.
The system saves the PDF in your computer's **Downloads** folder.



The screen capture is an example of a PDF.

Exporting Model data to the cloud

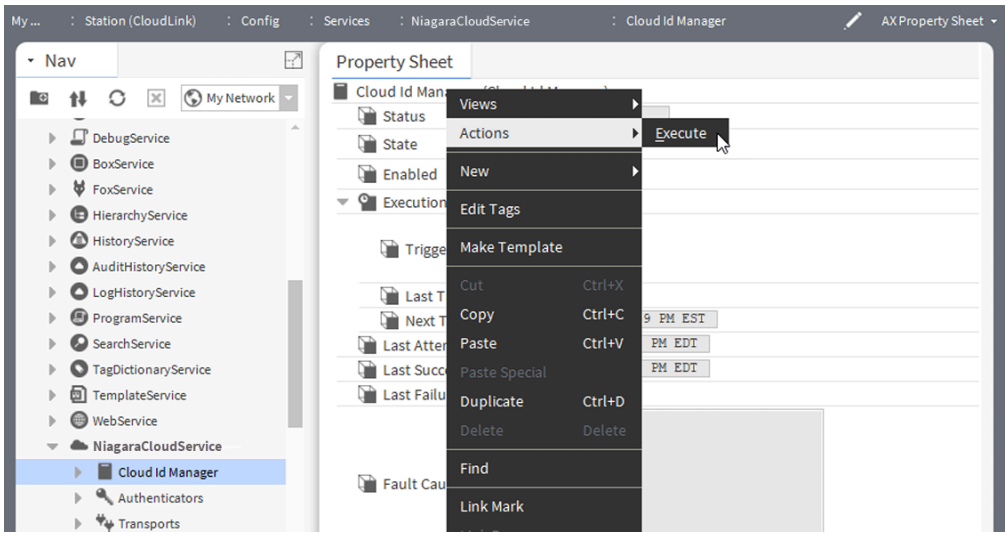
Before the station can upload data to the cloud, it must run the Cloud Id Manager, which triggers a model upload after it has assigned cloud Ids. The following steps describe how to export model data to the cloud by executing the Cloud Id Manager, which adds cloud Ids and telemetry Ids. This also triggers a model export if there are new components, otherwise the model will not be sent. This process ensures that a station's model is kept up-to-date in the cloud.

Prerequisites:

- Your station is registered.
- You have configured your networks:
  1. Add networks.
  2. Add drivers.
  3. Add proxy points (optional for model data).
  4. Add history imports (required for model and telemetry data).
- You have configured local components.
  1. Add control points.
  2. Add history extensions (required for telemetry data).

- You have configured other histories as needed.
  1. Audit Service history
  2. Log Service history
  3. System Monitor Service history
- If needed, you have tagged with nc:excluded any components or folders that you do not wish to send to the cloud.

Step 1. To run the **Cloud Id Manager** component, expand **Config** > **Services** > **NiagaraCloudService**.



Step 2. Right-click Cloud Id Manager and select **Actions** > **Execute**.

Result
The amount of time the export takes depends on the number of components in your station. You can monitor the status of the model export job in the Job Service.

After every configuration update of your network, local components, and histories, export the Model again.

NOTE: The recommended execution sequence is that you first configure the History exports, and then enable them.

Chapter 5. Niagara Recover

This service manages the storage and retrieval of station distribution file backups that have been stored in the Niagara Cloud Management Portal.

A Partner Admin may need to restore a station into a host as a replacement for a failed device or to revert an existing device to an earlier configuration. Working with station backups stored in the cloud involves these system functions:

- Workbench configures backup frequency.
- Niagara Cloud Service creates and uploads station backup distribution files to the cloud.
- Niagara Recover can associate notes with cloud backups, designate one backup as preferred, and download a selected backup to a device.
- Workbench decrypts and restores a downloaded backup to a station.

To back up and restore a station to and from your local drive instead of the cloud, use the Workbench **BackupService**.

Cloud backup and restore strategy

Each backup is a full backup that includes the history and alarm databases by default. The backup file made from a controller is relatively small, whereas, the file from a Supervisor station may be substantially larger. Storage in the cloud imposes no file size limits.

The NiagaraCloudService Backup Channel's **Default Backup Policy** defines when backups occur. This policy defaults to once a week at 2 am on Sunday mornings. Although you are free to change this policy, be aware of the important implications of any changes you make.

- Niagara Recover manages a maximum of five backup files for each station.
- If the newest backup would cause the backup file count to exceed five files, Niagara Recover saves the current backup and deletes the oldest backup that is not designated as preferred (this is called a rolling update).
- A backup includes multiple TLS certificates each with its private and public keys. These include a certificate for: Federated Identity, FoxService, WebService, and others. All certificates periodically expire and must be replaced. For example, the Federated Identity certificate expires every 90 days. Niagara Cloud Service replaces it automatically every 60 days. Other certificates may not be automatically replaced. Depending on the frequency of station backups, the oldest stored backup may not be appropriate to restore if any one of its certificates has expired.
- Although not required, you may designate one of the five files as the preferred backup. This can establish a known point of proper station configuration should an operator inappropriately change a station's configuration. If you designate a preferred backup, your backup strategy should define how frequently to change the preferred backup to a more recent file.

Using CloudLink to back up a station

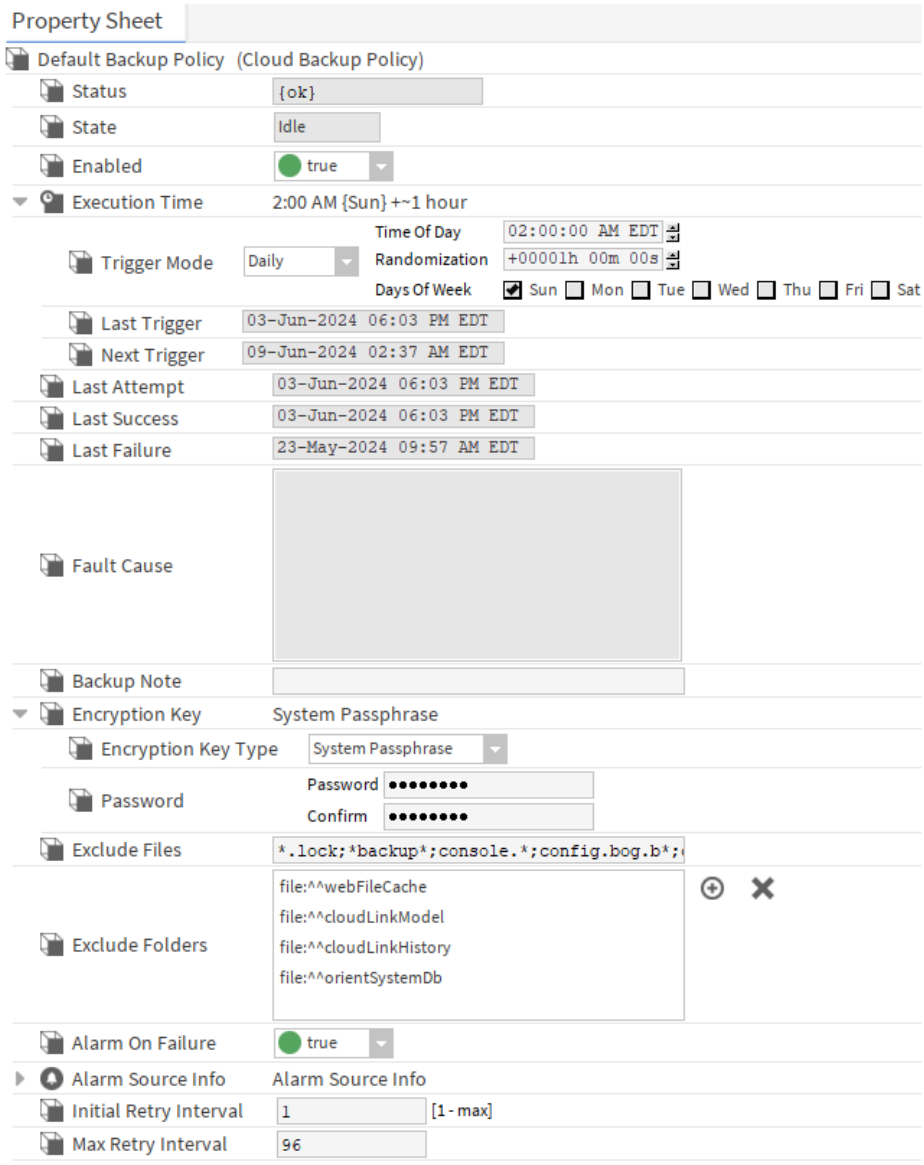
A station backup provides a snapshot of device configuration at a moment in time. CloudLink creates the backups for individual devices (stations) and uploads them to the cloud.

Prerequisites:
You are using Workbench and have installed the **NiagaraCloudService**.

The **NiagaraCloudService** provides a **Backup** channel.

Step 1. Expand **Config** > **Services** > **NiagaraCloudService** and double-click the **Backup** channel.

The **Channel Config** (Backup Channel Config:HTTP) **AX Property Sheet** opens.



The example screen capture shows the default **`Execution Time`** with **`Randomization`** set for one (1) hour. This causes the system to randomly choose the specific backup time within one hour of 2 am. The **`Next Trigger`** property identifies this random time, in this case 2:52 am on Sunday morning.

Step 2. To create an immediate backup, right-click the **Backup** policy and click **Actions** > **Execute**.

CloudLink generates, encrypts and uploads the backup file to Niagara Recover's backup storage in the cloud. It reports the outcome of the action in the lower right corner of the view. This job also appears in the job log.

The backup filename provides information about the station and when the encrypted backup was made.

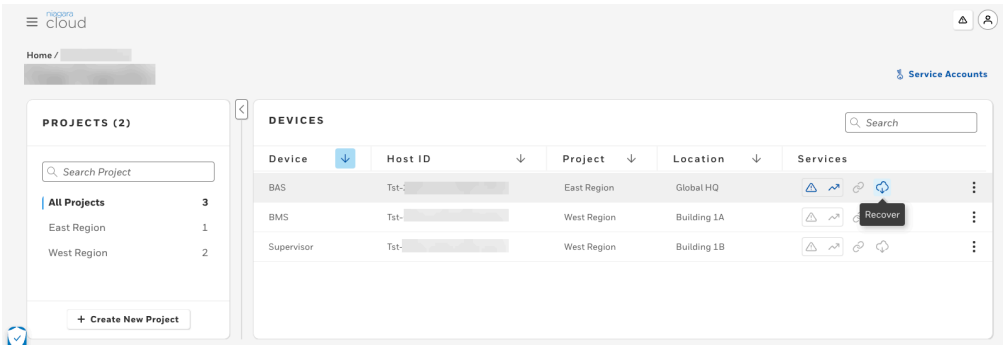
Number	Description
1	Device (station) name
2	Date the backup was made using the UTC timezone.
3	Time the backup was made using the UTC timezone.
4	Unique ID from the CloudConnectionService—Federated Identity Authenticator—System Id. CloudLink generates this ID when a device is registered.
5	File extension

Managing saved backups

After Niagara Cloud Service creates a backup distribution file, you use Niagara Recover to add a note and identify the file as the preferred backup.

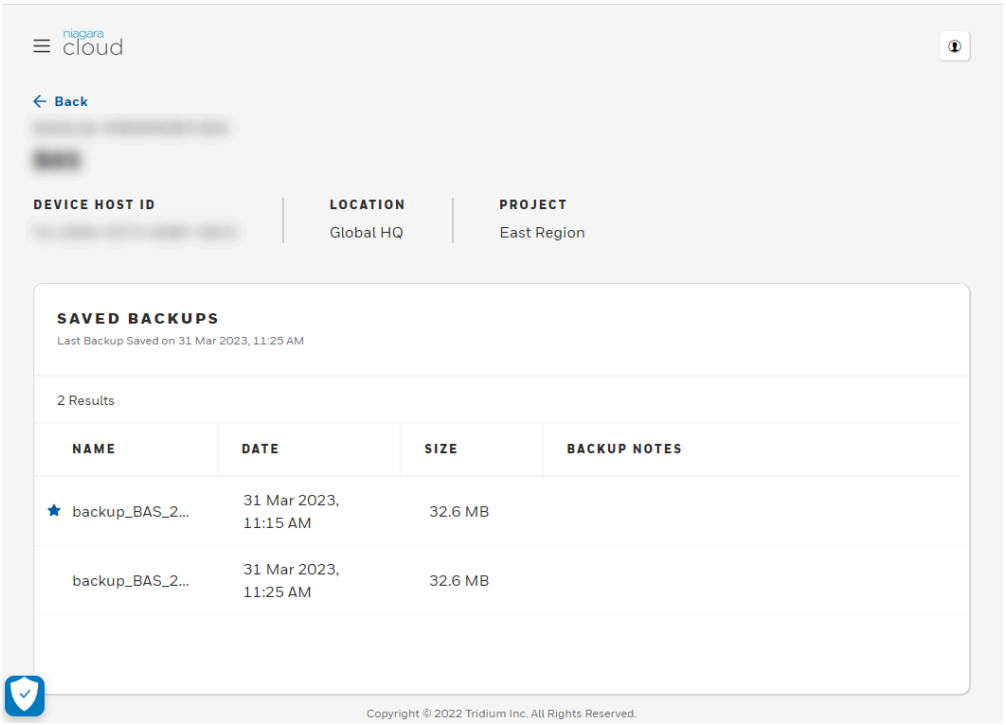
Prerequisites:
You are a Partner Admin user and have signed in to `https://www.niagara-cloud.com`. The backup is available in the cloud.

Step 1. Select a customer, select a project and search for a device.
The device row displays in the **CUSTOMER** view.



Step 2. Click the Recover icon ( ).

The **SAVED BACKUPS** view opens.

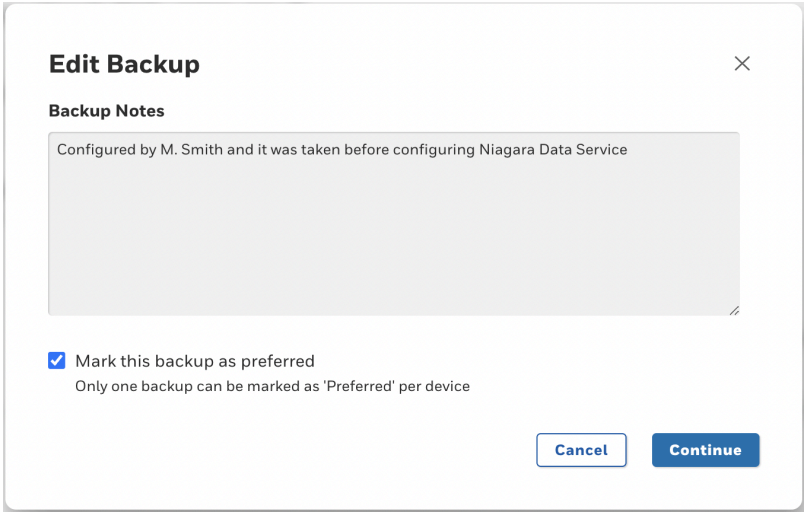


The screen capture shows two backup files. One is preferred as indicated by the star to the left of the file name.

The date and time you see under the **DATE** column are the browser's equivalent date and time, which may not be the same as that recorded in the filename.

Backup file names can be long. To see the entire name, move the cursor over the name.

Step 3. To add a note or designate a backup as preferred, click the Edit icon ( ) under the **ACTIONS** column.
The **EDIT BACKUP** window opens.



Step 4. To add a note for this backup, click into the **`Backup Notes`** property and type your text.
A note can be 1024 characters in length, which should be enough to fully document the backup.
The **SAVED BACKUPS** view displays the first two lines of the note and provides a **More** link to display the rest of the note.

Step 5. To designate this backup as preferred, enable the **`Mark this backup as preferred`** check box.

Only one backup file may by designated as preferred. If another backup is already preferred, the check box is grayed out.

Step 6. To prefer this backup instead of another, first click **Cancel**, disable the **`Mark this backup as preferred`** check box for the other backup, then come back and enable this one.

Step 7. When you finish editing the note and preferred status, click **Save**.
If this is the preferred backup the star icon displays to the left of the file name. If you added a note, it displays under the **BACKUP NOTES** column.

When you mark a backup as preferred, you cannot delete it. The Delete icon under the **ACTIONS** column is grayed out.

Restoring a station

You restore an individual station from a backup distribution (dist) file using Workbench.

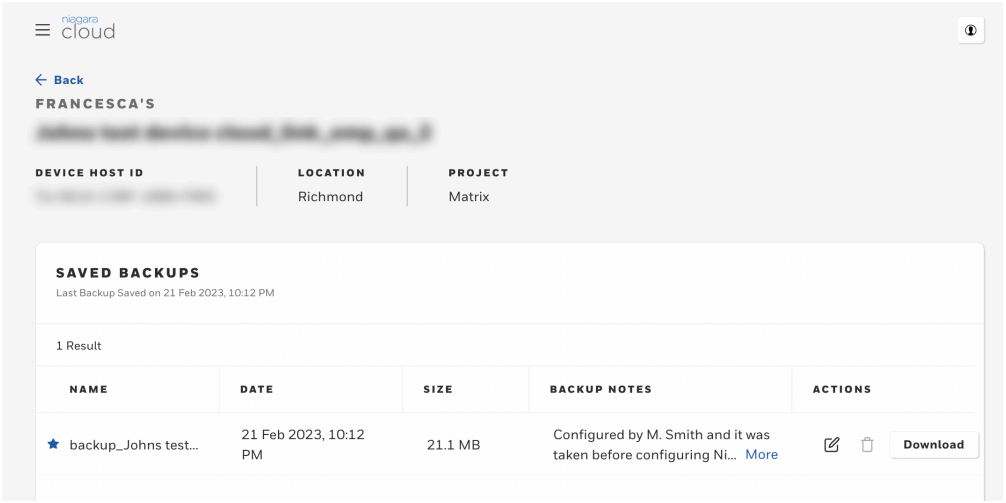
Prerequisites:

- You are a Partner Admin user and have signed in to `https://www.niagara-cloud.com`.
- You know the station's passphrase or user-created password.

CAUTION: Do not forget the station's passphrase. You will be asked to enter it when you perform a station backup.

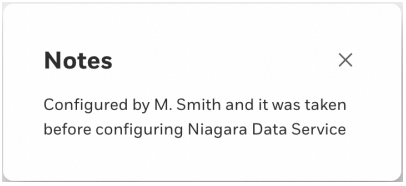
Step 1. Select a customer, select a project and search for the device to restore.
The device row displays in the **CUSTOMER** view.

Step 2. Click the Recover icon ( ).
The **SAVED BACKUPS** view opens.



Step 3. To confirm that the file to restore is the one you expect, pass the cursor over the file name.
The whole name displays. The file extension is `.edist2`. This extension indicates that the file is encrypted.

Step 4. To view the full note, click **More**.
The **Notes** window opens.



Step 5. Click the **Download** button at the right end of the row.
The system downloads the file to the local computer that is connected to Niagara Recover. This is usually your laptop or Supervisor PC. The **Download** button indicates the progress of the download.

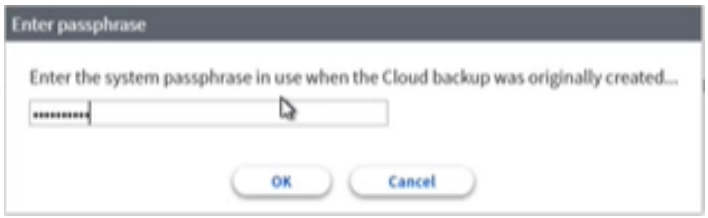
When the download finishes, the browser prompts you to select what to do with the backup.

Step 6. Select a location on your computer's hard drive.
An appropriate location to store the download is the Niagara user home's backups folder: **C:** > **Users** > **[user name]** > **[**Niagara **version]** > **tridium** > **backups**.

Step 7. If it's not already open, open Workbench and make a connection to the station.

Step 8. Expand the station and navigate to where you stored the downloaded backup file under **My Host** > **My File System**.
The screen capture shows the Niagara User Home's backups folder.
When you expand the folder, Workbench displays a table with a row for each backup file.

Step 9. Double-click the file name and click the **Decrypt DIST file** button.
The **Enter passphrase** window opens.



Step10. Enter the station's unique passphrase and click **OK**.
Workbench decrypts the `.edist2` file, which results in a `.dist` file.

Step11. Use the platform tool, **Dist File Installer**, to restore the station.

Deleting a backup

At any time you can remove backup files that are stored in the cloud.

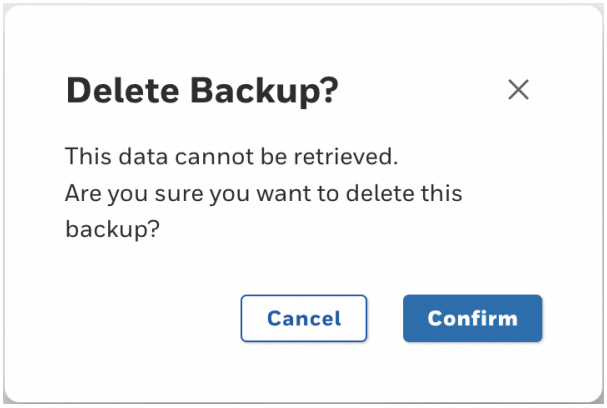
Prerequisites:
You are a Partner Admin user and have signed in to `https://www.niagara-cloud.com`.

Step 1. Select a customer, select a project and search for a device.
The device row displays in the **CUSTOMER** view.

Step 2. Click the Recover icon ( ).
The **SAVED BACKUPS** view opens.

Step 3. Confirm that you found the correct distribution file to delete and click the Delete icon ( ) under **ACTIONS**.

The **DELETE BACKUP?** window opens.



Step 4. To continue, click **Confirm**.
Niagara Recover deletes the backup file and displays a SUCCESS message in the upper right corner of the view.

Chapter 6. Niagara Remote

Niagara Remote enables you to securely access the built-in web interface on your Niagara stations directly from the Niagara Cloud Management Portal without using a VPN. You can connect to multiple stations at once and switch between them if needed.

Without Niagara Remote, if a device is installed on a remote network, the only way for you to access the web interface is by exposing the device's web interface on a publicly accessible web address, or over a separate VPN solution, which is complex, expensive to administer, and complicates access.

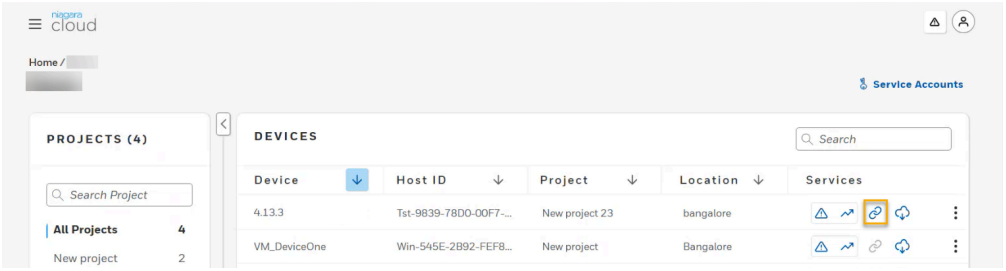
Connecting remotely to the station

Niagara Remote allows you to securely access the web interface of a Niagara device from where and when you need to connect. Here are the steps to follow.

Prerequisites:

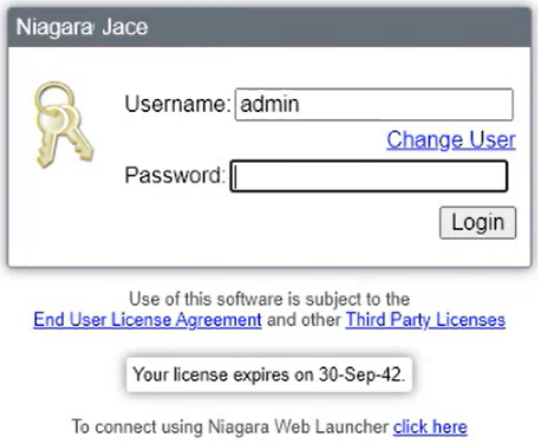
- You have installed all required Niagara Cloud Service modules on the station to be registered.
- The station to which you want to connect remotely is registered with Niagara Cloud Suite.
- The station has a Niagara license with an active subscription for the Niagara Remote product.
- You have the Niagara Remote or Admin role. You were able to multi-select Niagara Remote role and, for example, User role.

Step 1. Log in to Niagara Cloud Management Portal and select the desired device.



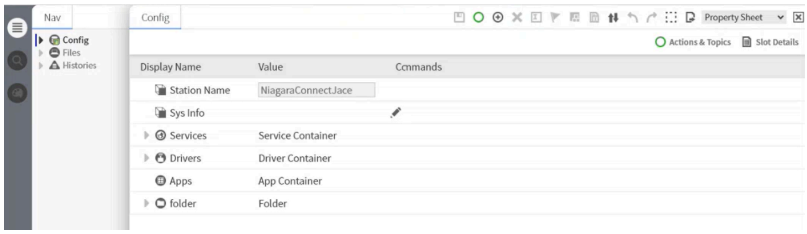
The device, which has the Niagara Remote subscription, displays the **Remote** link.

Step 2. Click on the **Remote** link.



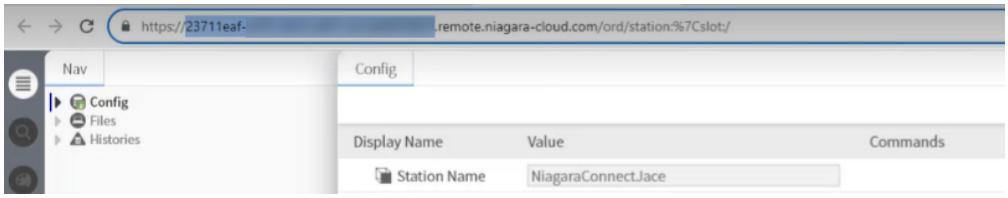
The web login window for the station opens.

Step 3. To log on remotely to the station, enter username and password.



You have accessed the station via browser. From here you can see all web views just like you would when connecting to the station directly.

NOTE: Notice: In the URL, notice the device UUID (Universally Unique Identifier). This URL will always be the same for this particular device.



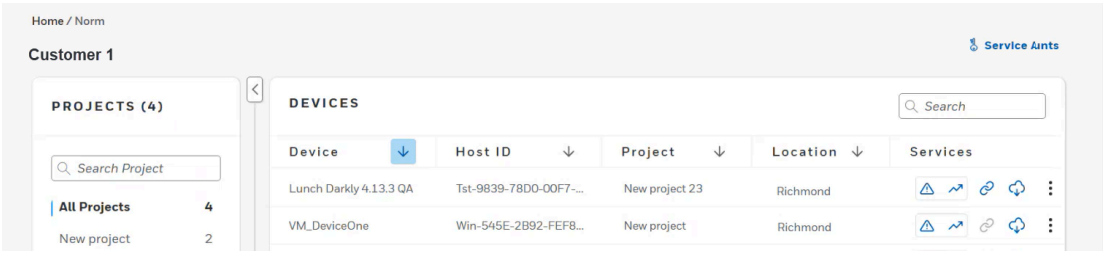
- You can share the URL with another user who is permitted through Niagara Cloud to remotely connect to this device.
- Another practical aspect is that you can bookmark the URL and later use it to connect to the station without first logging in directly to the Niagara Cloud Management Portal. First, you are directed to the Niagara Community login from where you are asked to enter your credentials. This will prompt a multi-factor authentication (MFA) request. From there, you will be redirected back to the station login.

Chapter 7. Niagara Alarms

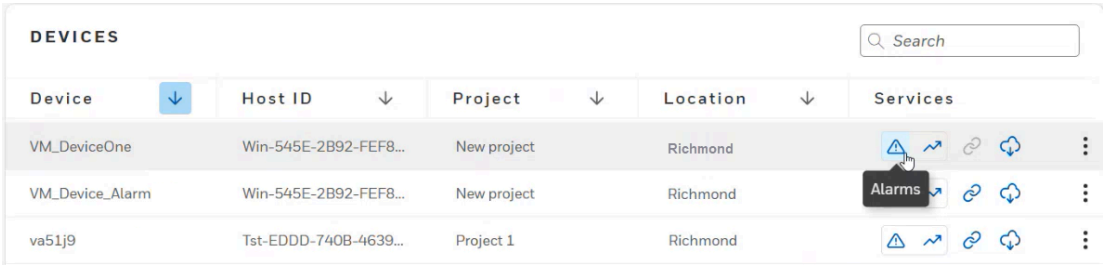
The Niagara Cloud Management Portal allows you to view detailed information about alarms for each individual device or all existing devices. You can also view all alarms on a project-specific basis

Viewing alarms

Step 1. In Niagara Cloud Management Portal, navigate to the customer and the associated devices whose alarms you wish to view.

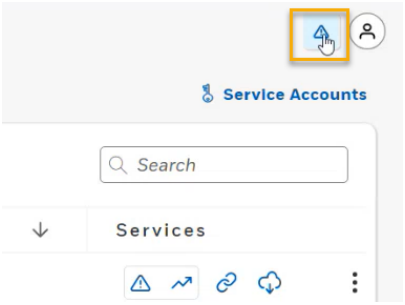


Step 2. To view the alarms for a specific device, click the **Alarms** icon in the **Services** column of the respective device.

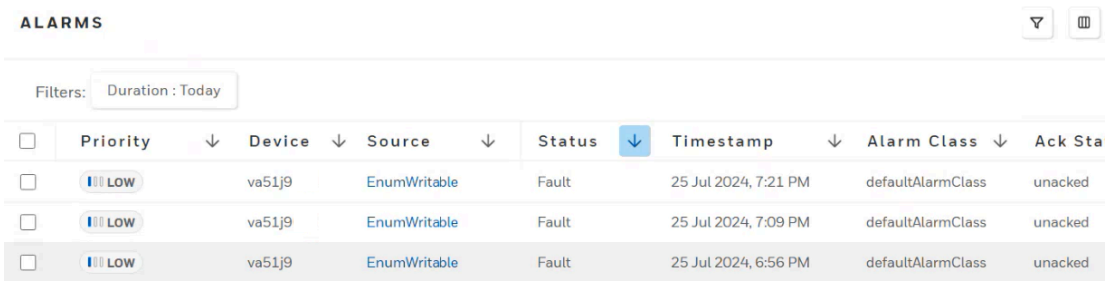


The Alarms page opens. By default, you see today's alarms for this particular device.

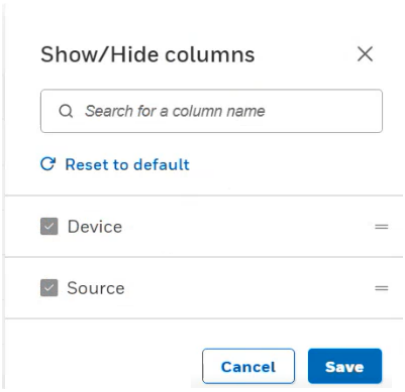
Step 3. To view all existing alarms from all devices, click the **Alarms** icon in the upper right corner of the screen.



By default, you see today's alarms of all devices of a specific customer.

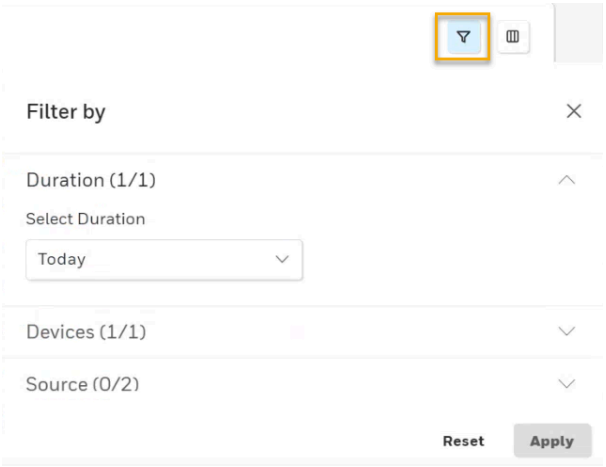


Step 4. To add or hide alarm columns, click **Show/Hide columns** icon in the upper right corner of the screen, and select or deselect the desired columns.



You can also change the order of the columns by dragging the column name to the desired position in the **Show/Hide columns** window. Click **Reset to default** if you want to go back to the original column setting.

Step 5. To set filters, click the filter icon in the upper right corner of the screen.

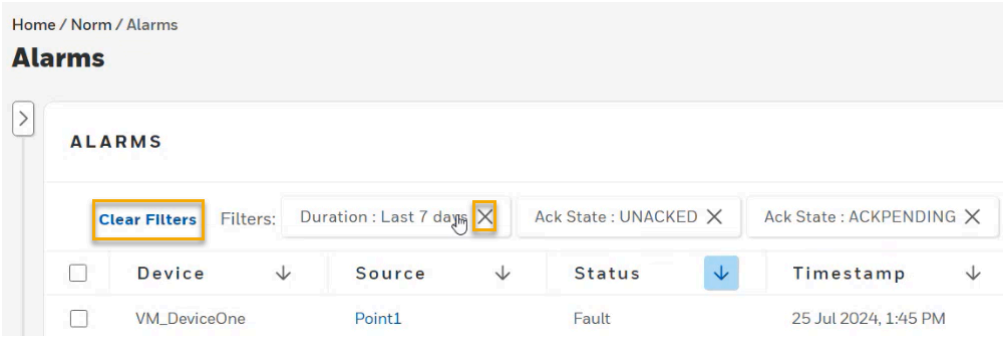


The following alarm filters are available:

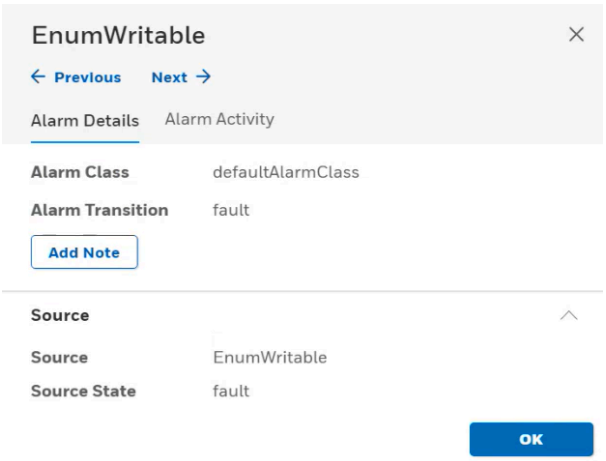
- Devices
- Source (for example, EnumWritable) and state of source
- Acknowledgment (Ack State, Ack Required, Ack Time)
- Alarm Information (Alarm Class, Alarm Transition)
- Priority (High, Medium, Low)
- Time (Normal Time)
- User

All applied filters will be shown on the **Alarms** result page.

Step 6. To clear a filter, click the **x** of the desired filter, and to clear all filters, click **Clear Filters**.

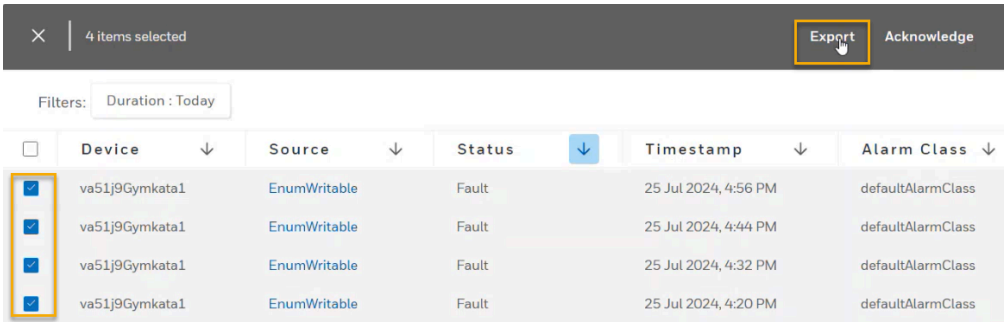


Step 7. To create a note for the alarm, click the link in the **Source** column of the particular device to open the alarm details window, and click **Add Note**.



The alarm note will be added to the station's alarm database.

Step 8. To export the information about device alarms, select the devices and click **Export** in the upper right corner.



A `.csv` file will be created containing all alarm information.

Step 9. To acknowledge a device alarm, click **Acknowledge** in the top right corner of the screen.

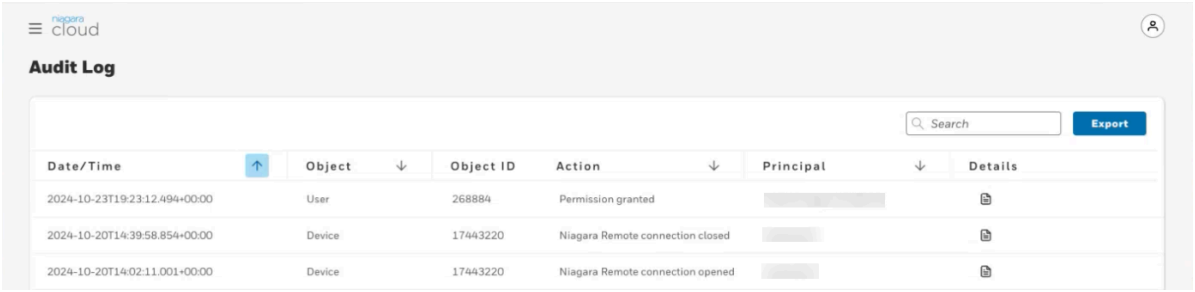
Chapter 8. Niagara Cloud audit logging

Audit logging helps monitor specific actions taken in the Niagara Cloud. This means you can track activities related to various entity types, such as reports, device projects, service control assignments, and backups.

Viewing audit logs

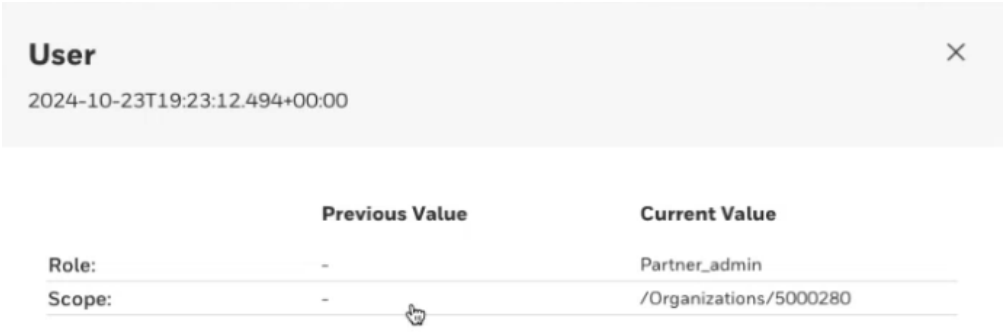
The following steps describe how to view audit logs.

Step 1. To access the audit log, click the navigation menu in the upper left corner of your screen in the Niagara Cloud Management Portal and select **Audit Log**.
The Audit Log screen opens. It displays information about date/time, object, object Id, action, principal, and details.



Step 2. To sort the information by date, time, object, actions, or principal, click the arrow icon located next to each column.

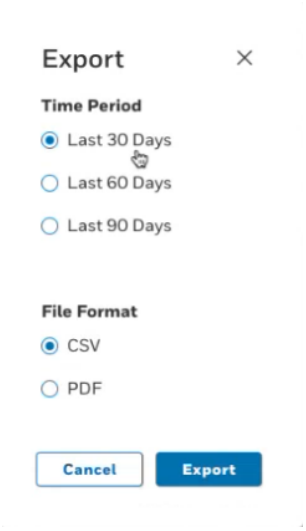
Step 3. To view additional user context such as previous values (if applicable) and current values, click the icon in the **Details** column.



Step 4. To look up specific audit log entries, you can use the **Search** field in the upper right corner of the screen.

Step 5. To export data, click **Export** in the upper right corner of the screen.

The Export window opens. You can export data using the CSV or PDF format and select if you want to export the data of the last 30, 60, or 90 days.



Chapter 9. Troubleshooting

This information is provided to make the troubleshooting and diagnosis of the **NiagaraCloudService** as straightforward as possible.

This troubleshooting information is intended for anyone who may be using the **NiagaraCloudService**, or supporting those who are using it.

Most of the pieces of the **NiagaraCloudService** have individual enable flags, so they can be separately enabled or disabled. In most cases, you should not disable any parts of the service, as most cloud applications depend upon all data streams being in place. However, it may be easier to diagnose a problem with an individual component if you disable the other components that are in parallel with the component under investigation. Do not disable the component(s) used by the aspect of the **NiagaraCloudService** you are investigating.

When an incident occurs

Collecting the following recommended information helps the technical support team get to the root cause of the problem quickly, characterize defects fully, and address the problem for immediate and future users.

Information to collect

- Date and time of incident; be as accurate as you can with the time
- Customer or user in question, including brand
- Hardware platform (for example, OS, version)
- Core Niagara software version (and any additional patches beyond base).
- Niagara Cloud modules versions, not just the release but the specific version of each module
- Any third party modules in use
- Any relevant log output or stack traces; see “What Logs to Collect”. More is better; extraneous information can be discarded if it is not important, but lost information cannot be recovered.
- Any relevant files; see “What Files to Collect”.
- Authenticator information (for example, system ID, system type); see “Collecting Authenticator Information”.

Questions to answer

- What steps were taken before and after the problem? Be as specific and complete as possible.
- Information about the network environment is critical in many cases. Is the host experiencing network disconnections (either intentional or not)? Is a proxy server in use? If yes, is it transparent or explicit (named). Is the Niagara **HttpProxyServer** service used?
- What steps were taken to resolve the problem?
- Was the **NiagaraCloudService** or authenticator `disabled`/`enabled`, did you do a **forceReconnect**, was the station restarted, did you attempt to reregister the authenticator? Ideally, if the station state can be left unchanged, the support team may suggest steps to correct the problem, or to learn more about it.

What logs to collect

There are several logs that can be enabled for diagnosing connection problems. The following tables list the logs.

Niagara Cloud Service logs

When you enable moderately or highly verbose logs, it is best practice to stream the station output to a file. For more information, see “What files to collect”. This allows you to capture what may be a larger amount of data than can be saved from the regular station output window and is the recommended way to capture output data. Also, saving the log to a file gives you something to refer to later and to share with technical

support, if needed.

Deciding which logs to enable requires a bit of judgment. You could set every log to: ALL, but this would yield so much data it would be difficult to dig through it all to isolate a specific problem. You need to decide what might be the likely source. Each of the basic Niagara Cloud Service functions, such as histories, has a log level beginning with "cloudLink". These do not generate a giant amount of data, so they can usually be set to ALL for whatever the specific function calls for.

- For issues with message security and authentication, set cloudLink.security and authentication to ALL. The output level is usually low enough to be manageable.
- For Niagara Cloud Suite registration , set cloudLink.auth.federated to ALL; for NDS/RPK registration, use registration, use cloudLink.auth.forge.
- For IoT Hub concerns, set cloudLink.transport.amqp.client. This can be extremely verbose, especially for a large system with many points and histories.

CAUTION: Do not forget to return logger settings to their default INFO levels once your problem is corrected. Leaving the loggers at higher levels of debug can impact system performance, and hide any new problems under a wave of noisy station output. This is especially true for the cloudLink.transport.amqp.client logger.

Log Name	Description	Verbosity	Notes
authentication	Inbound command authentication logging	Low	User authentication; non-cloud, but may be useful in identifying failed command reason
cloudLink.alarm	Alarm recipient logging	Low	alarm message delivery
cloudLink.auth.federated	Federated Device Identity authenticator logging	Low	set to CONFIG for NCS registration trace
cloudLink.auth.key	Logging related to key retrieval	Low	set to CONFIG for information about key retrieval/generation
cloudLink.channel	Common channel logging	Low	
cloudLink.channel.alarm	Alarm channel configuration information	Low	
cloudLink.channel.command	Command Channel information	Moderate	Set to FINER for command tracing
cloudLink.channel.event	Event channel configuration information	Low	
cloudLink.channel.heartbeat	Heartbeat Channel information	Low	
cloudLink.channel.history	History Channel information	Low	
cloudLink.channel.messaging	Message Channel information	Low	
cloudLink.channel.model	Model Channel information	Low	
cloudLink.channel.Point	Point Channel information	Low	
cloudLink.channelConfigFactory		Low	
cloudLink.connectionService	NiagaraCloudService logging	Low	set to ALL for factory management logging
cloudLink.event	Event recipient logging	Low	event message delivery
cloudLink.licenseLimit	License check logging	Low	
cloudLink.model.batch		Low	
cloudLink.model.exportPolicy		Low	
cloudLink.point	Point export policy logging	Low	
cloudLink.queue.inMemory	Outbound message queue logging	Moderate	set to FINER for message queue tracing
cloudLink.security	Trust mapping logger	Low	
cloudLink.smaMonitor	SMA monitor logging	Low	
cloudLink.tag	CloudId tagger logging	Low	
cloudLink.transport	Common transport logging	High	set to FINER form message throttling and tracing information
cloudLink.transport.amqp	AMQP transport Logging	Moderate	set to FINE for inbound message tracing

Log Name	Description	Verbosity	Notes
cloudLink.transport.amqp.client	AMQP client Logging	High	set to ALL for AMQP event tracing
cloudLink.transport.file	Local file system transport logging	Low	Set to ALL for file lock events
cloudLink.transport.http	HTTP transport Logging	Low	
cloudLink.util	Utility Logging	Low	

CloudLinkForge

Log Name	Description	Verbosity	Notes
cloudLink.auth.forge	Forge Authenticator logging	Low	set to CONFIG for RPK trace
cloudLink.forge	Utility logging	Low	
cloudLink.forge.msg	Message serialization logging	High	

What files to collect

After setting logs, collecting the station output is critical to diagnosing the problem. To do this, it is best to stream the station output to a file on your Workbench PC. This can be done from the **Application Director** window.

If the incident has already happened, it can be useful to go into the host's file system and get the older console output. This will be in the User Home with the filename "`console.txt`". Previous console logs from earlier station executions may also be useful. They will be listed under "`console_backup_YYMMDD_HHMM.txt`".

The station database is always helpful, and may allow technical support to determine configuration problems that lead to the behavior being investigated. The station database is in the `config.bog` file. It may also be helpful to include the full station using the station copier.

As a diagnostic tool, it is a good idea to create a backup distribution file, which also contains the cloud certificates. You may use the Workbench BackupService to create this file or Niagara Cloud Service to archive backups in the cloud from where Niagara Recover can retrieve them.

NOTE: If you are providing technical support with the bog file or full station copy, be sure to provide the username and password for the station.

Authenticator information

This information is particularly important if support personnel need to make any modifications to the device registration.

The FederatedIdentityAuthenticator is the authenticator for the Niagara Cloud Suite. It handles the station-side registration with the Federated Identity Service and provides a secure connection to the NCS identity provider.

The RPK Authenticator is only relevant if Niagara Data Service is installed. The authenticator's **`System Id`** property is important if it has been populated. Knowing that the **`System Id`** is empty is also useful, so note if it is empty. The text field size often prevents full display of the values, so the best approach is to right-click on the **RPK Authenticator** and select **Views** > **Spy Remote**. Copy the entire text of that page and paste it into a text file.

Network sanity checks

If you are unable to register a controller with the Niagara Cloud, these sanity checks are intended to help you identify the source of the problem.

Unfortunately, a controller may not provide the full spectrum of tools available to probe the network environment; however, you can run all the basic checks below from the controller. If you can connect a laptop to the controller network you will be able to run the tests in the additional checks section.

Checking network port health

This basic check uses ifconfig to determine if the port is functioning as expected.

Step 1. Log in to the controller through the USB port (see the *JACE-8000 Install and Startup Guide* and enter sh to launch the system shell.

Step 2. To see if the controller has an IP address, run ifconfig.
Output should be similar to that shown.

```
1  $ ifconfig
2  lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 33192
3          inet 127.0.0.1 netmask 0xff000000
4          inet6 ::1 prefixlen 128
5          inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
6  dm0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
7          address: 50:72:24:af:f7:e3
8          media: Ethernet autoselect (100baseTX full-duplex,flowcontrol)
9          status: active
10         inet 172.31.65.202 netmask 0xfffffc00 broadcast 172.31.67.255
11         inet6 fe80::5272:24ff:feaf:f7e3%dm0 prefixlen 64 scopeid 0x2
12 dm1: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
13         address: 50:72:24:af:f7:e5
14         media: Ethernet none
15         inet 192.168.1.1 netmask 0xffffff00 broadcast 192.168.1.255
16         inet6 fe80::5272:24ff:feaf:f7e5%dm1 prefixlen 64 scopeid 0x3
17 pflog0: flags=0 mtu 33192
```

- Line 6 starts the display of information about the primary network port, and line 12 starts the display of the secondary network interface.
- Line 8 indicates that the primary interface is currently connected, where as line 14 indicates that the secondary interface is not connected.
- Lines 10 and 11 show the v4 and v6 IP addresses of the primary interface.

Checking DNS health

This basic test confirms that DNS is working by pinging your favorite web site.

Ping your favorite web site.
Most web sites do not respond to ping requests but for DNS testing you should get a response. DNS is working if you are able to get an IP address for the web site.

```
1  $ ping www.google.com
2  PING www.google.com (216.58.216.4): 56 data bytes
```

In the above example we know DNS is working since www.google.com resolves to an IP address, in this case `216.58.216.4`.

Below is an example where DNS lookup failed.

```
1  $ ping www.google.com
2  ping: Cannot resolve "www.google.com" (Host name lookup failure)
```

It usually takes a short time for the test to fail as the controller times out waiting for the DNS server to respond.

Checking external communication

This basic test confirms that the controller can establish a secure connection to the outside world. This test uses the serial shell (ssh) to attempt a connection to `www.niagara-cloud.com`.

Step 1. For this test, enter the host name of the Device Registration URL in your **RpkAuthenticator**. This is a hidden slot, which you can view from the spy page of the component. Use the fully qualified path to the `ssh` command, and specify the `-v` verbose flag to see what is happening.

```
1  $ /usr/bin/ssh -v -p 443 niagara-cloud.com
2  OpenSSH_5.2 QNX_Secure_Shell-20090621, OpenSSL 1.0.2j  26 Sep 2016
3  debug1: Connecting to niagara-cloud.com [13.82.101.179] port 443.
4  debug1: Connection established.
5  Could not create directory '/.ssh'.
6  debug1: identity file /.ssh/identity type -1
7  debug1: identity file /.ssh/id_rsa type -1
8  debug1: identity file /.ssh/id_dsa type -1
```

Line 4 shows that we were able to successfully connect to the Device Registration Service. Since we are connecting to a web server and not a `sshd` server the connection hangs.

Step 2. To get out of the command, press **Ctrl** + **C**.

Checking endpoint availability

This more advanced test attempts to reach the web endpoints required for device registration with a browser. If you are installing a Supervisor, these checks should provide additional information.

Prerequisites:
You have a Windows or Linux PC connected to the same network as the controller.

Step 1. Open a browser and navigate to `https://api.niagara-cloud.com`.
This should return a JSON formatted response.

Step 2. Navigate to `https://gaprodsystemauthentication.sentience.honeywell.com/api/authentication/rpkchallenge`.
This should return an XML formatted error message stating that the service does not support the GET method.

Step 3. Navigate to `https://gaprodregui.sentience.honeywell.com/api/swagger/public`.
This should return a JSON formatted response.

Step 4. If you cannot reach the endpoints, attempt to see where the problem is using the trace route (`tracert`) Windows command.

This shows the path through the network that packets are taking.

```
>tracert niagara-cloud.com

Tracing route to waws-prod-blu-075.api.niagara-cloud.com[13.82.101.179]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  137.19.60.3
  2     1 ms     1 ms     1 ms  137.19.35.237
  3    15 ms    16 ms    15 ms  10.160.16.2
  4    21 ms    15 ms    15 ms  10.223.255.229
  5    15 ms    15 ms    14 ms  10.223.255.65
  6    16 ms    16 ms    16 ms  10.223.255.58
  7    17 ms    15 ms    16 ms  10.221.192.36
  8    15 ms    15 ms    18 ms  199.64.6.87
  9    15 ms    15 ms    16 ms  199.64.6.52
 10    15 ms    16 ms    16 ms  199.64.6.77
 11    26 ms    58 ms    28 ms  12.249.243.109
 12    22 ms    22 ms    23 ms  cr2.phlpa.ip.att.net [12.123.237.142]
 13    24 ms    22 ms    22 ms  12.122.2.201
 14    22 ms    22 ms    22 ms  gar3.rcmva.ip.att.net [12.122.135.173]
 15    24 ms    20 ms    20 ms  12.122.135.109
 16    23 ms    27 ms    32 ms  12.247.95.62
 17    25 ms    24 ms    25 ms  be-74-0.ibr02.was05.ntwk.msn.net [104.44.9.42]
 18    24 ms    24 ms    24 ms  be-1-0.ibr01.was05.ntwk.msn.net [104.44.4.18]
 19    23 ms    23 ms    22 ms  be-5-0.ibr04.bl20.ntwk.msn.net [104.44.16.183]
 20    23 ms    23 ms    22 ms  ae161-0.icr01.bl7.ntwk.msn.net [104.44.21.230]
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
```

Entries that get an asterisk (*) represent network messages that timed out. If a host gets three asterisks, the endpoint is either down or configured not to respond to ping traffic. Services running in the cloud are usually configured not to respond to ping traffic; however, you can see if our network traffic is making it out of the local network environment.

In the example above, lines 17 and 19 report a response from a server owned by AT&T. Lines 22 through 25 report responses from Microsoft owned machines. This tells us that the station is able to route out of the local environment onto the public Internet.

These traces provide other information. For example, if a host has one or two asterisks on its line, the host or a host leading up to it is dropping packets. This degrades performance and could lead to other problems. A big jump in response times from one line to the next could indicative a potential network problem.

Registration issues

Several problems can prevent the registration of devices with the Niagara Cloud.

Cannot reach device registration web service

This topic provides help when the **RpkAuthenticator** is prevented from reaching the device registration web service.

Cause

This registration problem typically occurs when you are connected to the station using Workbench or a browser on a machine that does not have sufficient access to the Internet. The station host must have Internet access to authenticate directly with the identity provider, which enables cloud communication. Lack of Internet access prevents device registration.

NOTE: Sufficient access means not only that the machine has access to the Internet, but that certain proxy and firewall limitations are not in effect. For details, see the “Requirements” topic in this guide. Your network configuration must satisfy the stated requirements.

Tip

The following error in the Workbench VM, not the station VM, confirms that your client Workbench or browser does not have Internet access, or is blocked by proxy or firewall rules from reaching a necessary destination:

```
>tracert api.niagara-cloud.com

Tracing route to api.forge.connected.honeywell.com [20.120.121.65]
over a maximum of 30 hops:

  1     3 ms     3 ms     3 ms  137.19.60.3
  2     1 ms     1 ms     1 ms  137.19.35.237
  3    15 ms    16 ms    15 ms  10.160.16.2
  4    21 ms    15 ms    15 ms  10.223.255.229
  5    15 ms    15 ms    14 ms  10.223.255.65
  6    16 ms    16 ms    16 ms  10.223.255.58
  7    17 ms    15 ms    16 ms  10.221.192.36
  8    15 ms    15 ms    18 ms  199.64.6.87
  9    15 ms    15 ms    16 ms  199.64.6.52
 10    15 ms    16 ms    16 ms  199.64.6.77
 11    26 ms    58 ms    28 ms  12.249.243.109
 12    22 ms    22 ms    23 ms  cr2.phlpa.ip.att.net [12.123.237.142]
 13    24 ms    22 ms    22 ms  12.122.2.201
 14    22 ms    22 ms    22 ms  gar3.rcmva.ip.att.net [12.122.135.173]
 15    24 ms    20 ms    20 ms  12.122.135.109
 16    23 ms    27 ms    32 ms  12.247.95.62
 17    25 ms    24 ms    25 ms  be-74-0.ibr02.was05.ntwk.msn.net [104.44.9.42]
 18    24 ms    24 ms    24 ms  be-1-0.ibr01.was05.ntwk.msn.net [104.44.4.18]
 19    23 ms    23 ms    22 ms  be-5-0.ibr04.b120.ntwk.msn.net [104.44.16.183]
 20    23 ms    23 ms    22 ms  ae161-0.icr01.b17.ntwk.msn.net [104.44.21.230]
 21     *        *        *     Request timed out.
 22     *        *        *     Request timed out.
```

Solution

Ensure that your client machine running Workbench or the browser has Internet access before attempting device registration. Also, make sure that the URLs specified in the “Requirements” topic of this guide are accessible to the client machine, and are not blocked by a network proxy or firewall configuration.

Connection issues

There are several reasons why a connector might not be able to send data to the Niagara Cloud through the IoT Hub. Many of them relate to issues outside of **NiagaraCloudService**.

Federated identity does a provisioning check every 15 minutes. If it finds an unregistered **RpkAuthenticator** at the end of that check, it tries to register the authenticator. The **RpkAuthenticator** is disabled until the process returns a success registration status response.

Cannot connect to the cloud

A message that indicates a failure to connect to the cloud may require special action.

```
WARNING [14:41:57 02-Oct-18 EDT][cloud.connector] Cannot connect to Cloud
```

Step 1. Set the cloudLink.transport.amqp and cloudLink.transport.amqp.client log levels at least to FINE.

You may set them to an even finer level, such as FINER, FINEST or ALL, although, the finer you set the log level, the more data the log produces.

Step 2. Confirm that your device is enabled.

System Disabled

The Honeywell Forge Operations team tracks and aggressively manages the bandwidth usage of systems participating in the Forge Platform ecosystem. Devices that send too much data are subject to being disabled from the Forge IoTHub. This means that the device is prevented from sending any data to the Forge IoTHub. The device may even be prevented from establishing the IoTHub connection in the first place. This may manifest in several different ways. One example is where the authenticator is able to authenticate to the identity endpoint, but cannot open the connection. You may see the Property Sheet of the RpkAuthenticator show "Connected", or possible "Pending Connect". The following message, or something similar, may show in the station output:

```
1
2  CONFIG [14:33:56 29-Jul-19 BST][cloud.connector.sentience] Starting RPK Challenge
3  CONFIG [14:33:56 29-Jul-19 BST][cloud.connector.sentience] Sending RPK Challenge request to URI https://gaprodsystemauthentication.s
4  FINE [14:33:57 29-Jul-19 BST][cloud.connector.http] HTTP Response Code:200
5  CONFIG [14:33:57 29-Jul-19 BST][cloud.connector.sentience] Checking for existing locally initialized keys
6  CONFIG [14:33:58 29-Jul-19 BST][cloud.connector.sentience] Authenticating using software keys
7  CONFIG [14:33:58 29-Jul-19 BST][cloud.connector.sentience] Sending RPK Challenge Response to URI https://gaprodsystemauthentication.
8  FINE [14:33:59 29-Jul-19 BST][cloud.connector.http] HTTP Response Code:200
9  CONFIG [14:33:59 29-Jul-19 BST][cloud.connector.sentience] Completed RPK Challenge - 2438 ms
10 CONFIG [14:33:59 29-Jul-19 BST][cloud.connector.sentience] Starting System Connections
11 WARNING [14:33:59 29-Jul-19 BST][com.microsoft.azure.sdk.iot.device.transport.amqps.AmqpsDeviceAuthenticationCBSTokenRenewalTask] jav
12 FINE [14:34:02 29-Jul-19 BST][cloud.connector.http] HTTP Response Code:200
13 CONFIG [14:34:02 29-Jul-19 BST][cloud.connector.sentience] Completed System Connections: 3125 ms
14 FINEST [14:34:03 29-Jul-19 BST][cloud.connector] BCloudConnector.pingFail(Could not open the connection), notifying connectCallbacks
15 FINE [14:34:03 29-Jul-19 BST][cloud.connector] Connection fail
16 java.io.IOException: Could not open the connection
17     at com.microsoft.azure.sdk.iot.device.DeviceIO.open(DeviceIO.java:165)
18     at com.microsoft.azure.sdk.iot.device.DeviceClient.open(DeviceClient.java:369)
19     at com.tridium.cloud.client.iotdep.BIotHubMessageClient.lambda$onConnect$4(BIotHubMessageClient.java:441)
20     at java.security.AccessController.doPrivileged(Native Method)
21     at com.tridium.cloud.client.iotdep.BIotHubMessageClient.onConnect(BIotHubMessageClient.java:387)
22     at com.tridium.cloud.client.iothub.BAbstractIotHubConnectorImpl.doConnect(BAbstractIotHubConnectorImpl.java:79)
23     at com.tridium.cloud.client.sentience.BSentienceConnectorImpl.doConnect(BSentienceConnectorImpl.java:734)
24     at com.tridium.cloud.client.BConnectorImpl.connect(BConnectorImpl.java:118)
25     at com.tridium.cloud.client.BCloudConnector.reconnectSync(BCloudConnector.java:527)
26     at java.util.concurrent.FutureTask.run(FutureTask.java:266)
27     at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201(ScheduledThreadPoolExecutor.java:180)
28     at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExecutor.java:293)
29     at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
30     at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
31     at java.lang.Thread.run(Thread.java:748)
32 Caused by: com.microsoft.azure.sdk.iot.device.exceptions.TransportException: Unknown transport exception occurred
33     at com.microsoft.azure.sdk.iot.device.transport.amqps.AmqpsIotHubConnection.onLinkRemoteClose(AmqpsIotHubConnection.java:729)
34     at org.apache.qpid.proton.engine.BaseHandler.handle(BaseHandler.java:176)
35     at org.apache.qpid.proton.engine.impl.EventImpl.dispatch(EventImpl.java:108)
36     at org.apache.qpid.proton.reactor.impl.ReactorImpl.dispatch(ReactorImpl.java:324)
37     at org.apache.qpid.proton.reactor.impl.ReactorImpl.process(ReactorImpl.java:291)
38     at com.microsoft.azure.sdk.iot.device.transport.amqps.IotHubReactor.run(IotHubReactor.java:28)
39     at com.microsoft.azure.sdk.iot.device.transport.amqps.AmqpsIotHubConnection$ReactorRunner.call(AmqpsIotHubConnection.java:824)
40     at java.util.concurrent.FutureTask.run(FutureTask.java:266)
       ... 3 more
```

This log indicates that the IoT Hub has blocked your device due to sending too much traffic.

In the screen capture above, all the authentication steps return an HTTP Response Code of 200 (see lines 3, 7, and 11), indicating success. The exception occurs only when attempting to establish the IoT Hub connection (see lines 32– 40).

If this is happening, your device may be blocked (that is, throttled) by the Niagara Cloud due to sending too much traffic at some point. You should have received an email indicating that the device has been blocked.

Step 3. If you received an email, contact support and request that your device's ability to connect with the cloud platform be re-enabled.

Step 4. If you did not receive an email, and you are connecting for the first time to the cloud, there may be a problem with the email addresses on file for this system. Work with support to set the proper notification configuration and re-enable your device's ability to connect.

Authenticator keys are lost

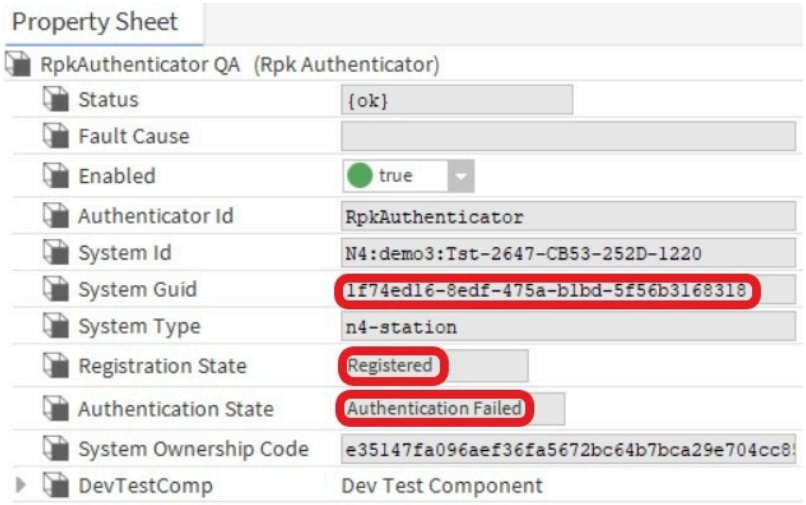
This applies to all non-QNX stations. Controllers should use hardware encryption.

If your station output appears as shown here:

Figure 3. Station output

```
CONFIG [20:58:51 23-Feb-21 EST][cloudLink.auth.forge] Connecting to Forge identity provide
INFO [20:58:51 23-Feb-21 EST][cloudLink.auth.key] Starting to init keys with id of :N4:dem
INFO [20:58:51 23-Feb-21 EST][cloudLink.auth.key] Authenticator found existing local keys
FINEST [20:58:51 23-Feb-21 EST][cloudLink.auth.forge] getConnectionInfo called but no conn
CONFIG [20:58:52 23-Feb-21 EST][cloudLink.auth.forge] Starting RPK Challenge
CONFIG [20:58:52 23-Feb-21 EST][cloudLink.auth.forge] Sending RPK Challenge request to URL
niagara>INFO [20:58:52 23-Feb-21 EST][cloudLink.auth.key] Starting to generate a signed re
INFO [20:58:53 23-Feb-21 EST][cloudLink.auth.key] Generating signature with keyId of N4:de
CONFIG [20:58:53 23-Feb-21 EST][cloudLink.auth.forge] Sending RPK Challenge Response to UR
CONFIG [20:58:53 23-Feb-21 EST][cloudLink.auth.forge] Next RpkAuthenticator token renewal
WARNING [20:58:53 23-Feb-21 EST][cloudLink.auth.forge] Cannot reauthenticate: Could not au
com.tridium.cloudLink.auth.SystemAuthenticationException: Could not authenticate:java.util
        at com.tridium.cloudLink.forge.auth.BRpkAuthenticator.authenticate(BRpkAuthenticat
        at com.tridium.cloudLink.forge.auth.BRpkAuthenticator.reauthSync(BRpkAuthenticator
        at java.util.concurrent.FutureTask.run(FutureTask.java:266)
        at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$201
        at java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(Schedu
        at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
        at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
        at java.lang.Thread.run(Thread.java:748)
Caused by: java.util.concurrent.ExecutionException: com.tridium.cloudLink.transport.HttpSt
        at java.util.concurrent.CompletableFuture.reportGet(CompletableFuture.java:357)
        at java.util.concurrent.CompletableFuture.get(CompletableFuture.java:1908)
        at com.tridium.cloudLink.forge.auth.BRpkAuthenticator.rpkChallenge(BRpkAuthenticat
        at com.tridium.cloudLink.forge.auth.BRpkAuthenticator.authenticate(BRpkAuthenticat
        ... 7 more
Caused by: com.tridium.cloudLink.transport.HttpStatusException:
        at com.tridium.cloudLink.transport.BHttpTransport.lambda$send$1(BHttpTransport.jav
        at java.security.AccessController.doPrivileged(Native Method)
        at com.tridium.cloudLink.transport.BHttpTransport.send(BHttpTransport.java:251)
        at com.tridium.cloudLink.transport.BAbstractTransport.lambda$sendMessages$9(BAbstr
        at java.security.AccessController.doPrivileged(Native Method)
        at com.tridium.cloudLink.transport.BAbstractTransport.sendMessages(BAbstractTransp
        ... 3 more
```

In addition, your **RpkAuthenticator** properties appear as shown here:



your station does not have the required public/private key pair stored in its User Key Store that it needs to authenticate to the Niagara Cloud.

To confirm this, check the **User Key Store** tab of the **Certificate Manager** for a key with an alias matching the station name. This alias will be all lowercase, prefaced with "cloud_" and with hyphens replacing any underscores in the station name. If you do not see the alias for your station, your station cannot register because it does not have the necessary key pair. The station is registered with the cloud, but cannot authenticate.

NOTE: If the key pair is missing when the station starts, the startup process generates a new key pair, however, this key pair is not registered with the cloud so the device cannot authenticate using it.

Solution

If this is a new station, contact support to remove the registration with the Niagara Cloud, and register the device again.

Always keep a current backup distribution file of the station platform that contains the certificates. You may also export the certificates with their private keys so that you them in case of future need. Store any exported keys in a safe place, preferably off campus.

If this is an existing station and, at some point, you exported the keys from the station's **User Key Store**, try importing them back into your **User Key Store** using the **Certificate Manager**. If the file contains the correct keys, the authenticator should reconnect successfully.

Niagara Cloud Service does not attempt connection

If you registered your authenticator and received a success message, but your authenticator does not attempt to connect at all, that is, there is no confirmation message in the station output when your cloudLink.auth.forge log is set to ALL, your device remains disconnected.

Solution

Here is an example of the message that should appear in the log if succeeded: `FINE [11:57:26 26-Apr-24 EDT][cloudLink.auth.forge] Authenticated with the cloud identity provider`. If it does not appear, proceed with the following solution.

Try disabling the **RpkAuthenticator**, then re-enable it.

Proxy server preventing connection

If you are able to register the station with the Niagara Cloud but the station cannot connect (the connector's **`Connection State`** never displays `Connected` and the AMQP Transport's **`Connection State`** never displays `Connected`), there may be a problem with the local IT network's proxy settings, or with the firewall settings imposed upon the station.

Problem

The **NiagaraCloudService** requires Unauthenticated Proxy Access. Without this, the proxy server prompts for credentials, and asks you to approve exemptions for certificates in the Niagara **User Trust Store**. This process repeats itself frequently and does not provide a workable solution.

If network settings prevent the station from connecting properly, the station remains in the unregistered state even if registration reports that it is registered. If you received the "successfully registered!" message, your device is registered. If the device's RPK Authenticator still shows "Unregistered," registration cannot reach the authentication endpoint.

Solution

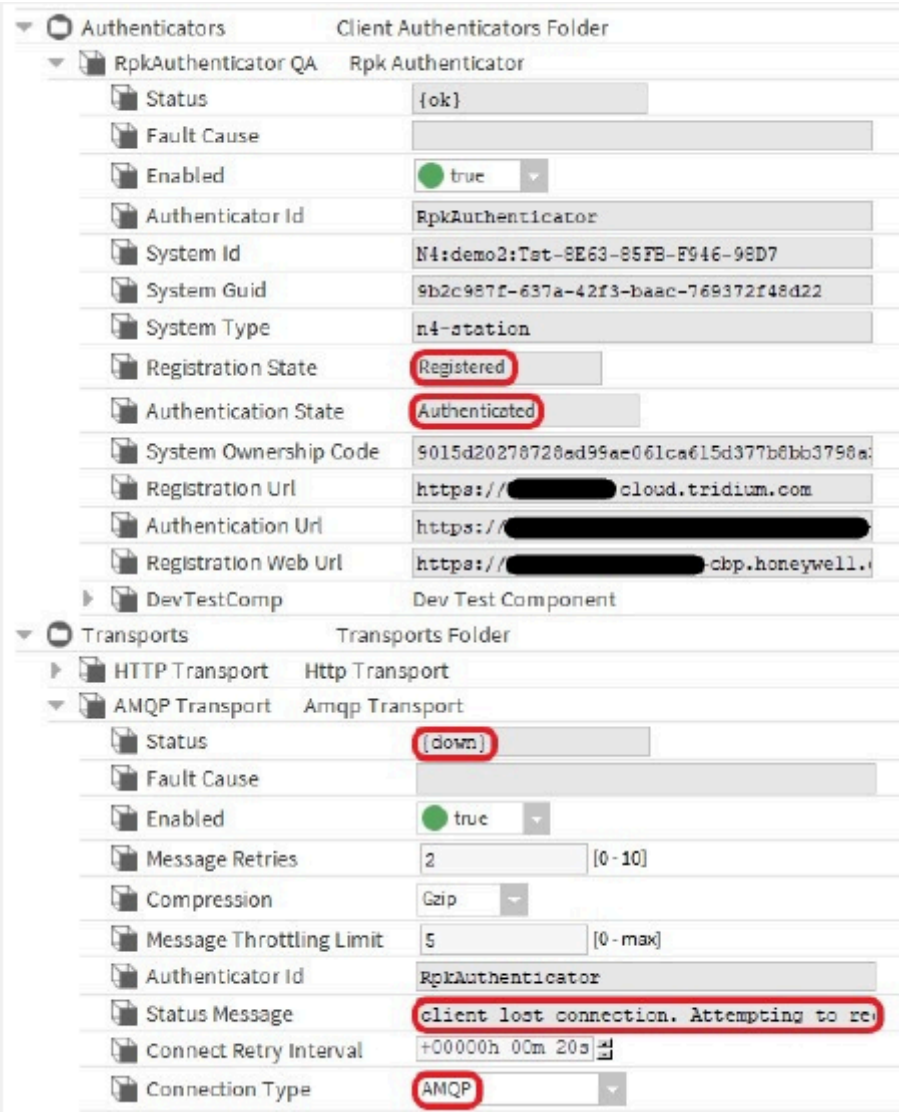
If you are using a proxy server that requires credentials, or an explicit (named) proxy server, install the **HttpProxyServer** service from the net-rt module and configure it with appropriate settings for your proxy server. Use the **HttpProxyServer** to direct traffic.

Review with your IT administrator your Internet connection (refer to "Setting up device internet access" in this guide), specifically regarding firewall access and unauthenticated transparent proxy access. This is a common problem with network setup, especially in a heavily restricted corporate or educational network. Ensure that the requirements in this section are met by the IT network configuration.

AMQP blocked

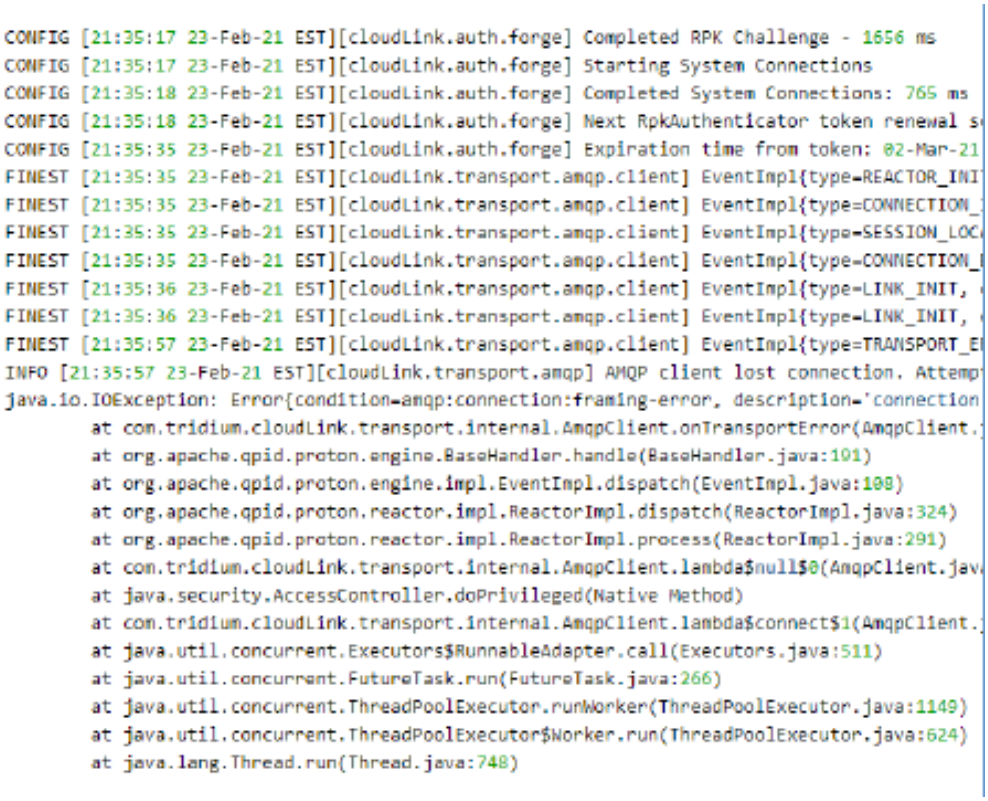
If you are using AMQP as your transport, you have registered your authenticator, and you are seeing the connector status stuck in `Pending Connect`, it may be because AMQP is blocked on your network.

Figure 4. NiagaraCloudService properties for AMQP blocked



To confirm, look at the station output as a connection problem. Set the cloudLink.transport.amqp, cloudLink.transport.http, and cloudLink.auth logs to ALL.

Figure 5. Station output for AMQP blocked



Solution

For a rapid solution, switch to AMQP over WebSocket by changing the setting in the **NiagaraCloudService** > **Transports** > **AMQP Transport**.

If you really want to use AMQP, try working with your IT administration to modify the network settings to allow this protocol.

For most internal networks, AMQP is blocked by default. So, any device on the network needs to use AMQP over WebSocket.

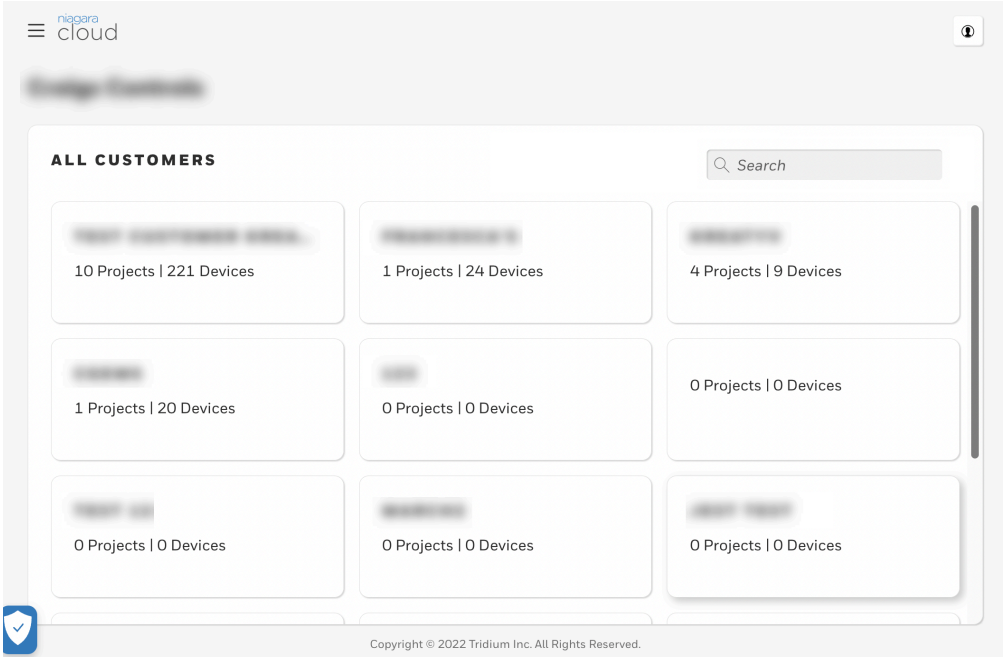
Reference

Each view and window used by the Niagara Cloud Management Portal may contain properties, buttons and tables. This chapter documents views.

All Customers view

This view is for the SI to view all the partner organization's customers, their projects and the associated devices for each project.

The systems integrator can view users and roles. This option is not available on the customer's view.

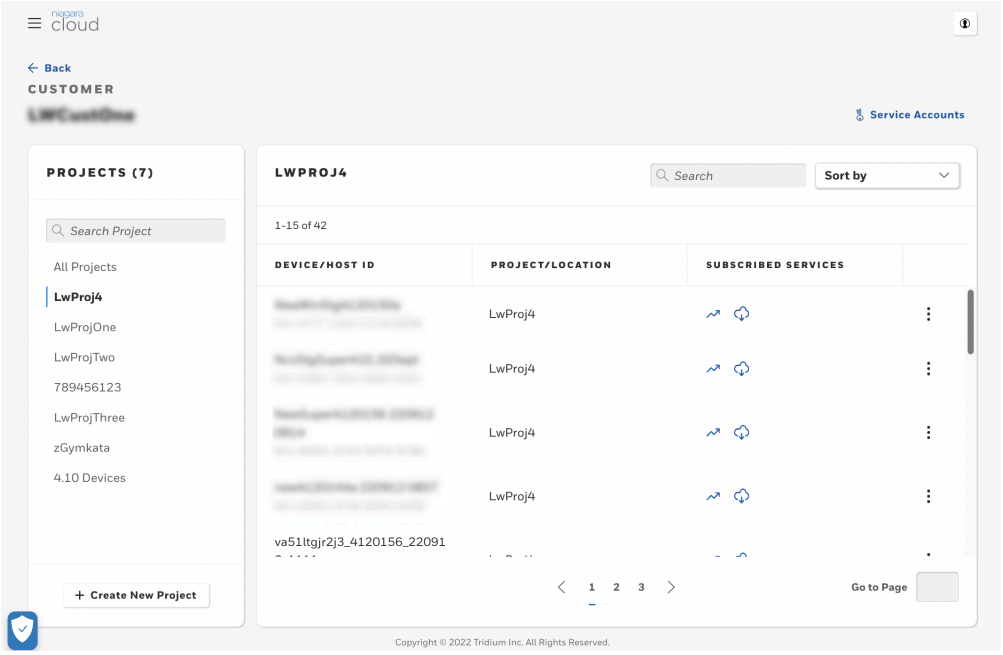


To access this view, log in to the Niagara Cloud Management Portal.

Each tile shows the customer organization name with the number of projects and devices that are associated with the customer.

PROJECTS view

This view is for systems integrators and customer users. It opens to the projects, assigned devices and subscribed services for a customer organization.



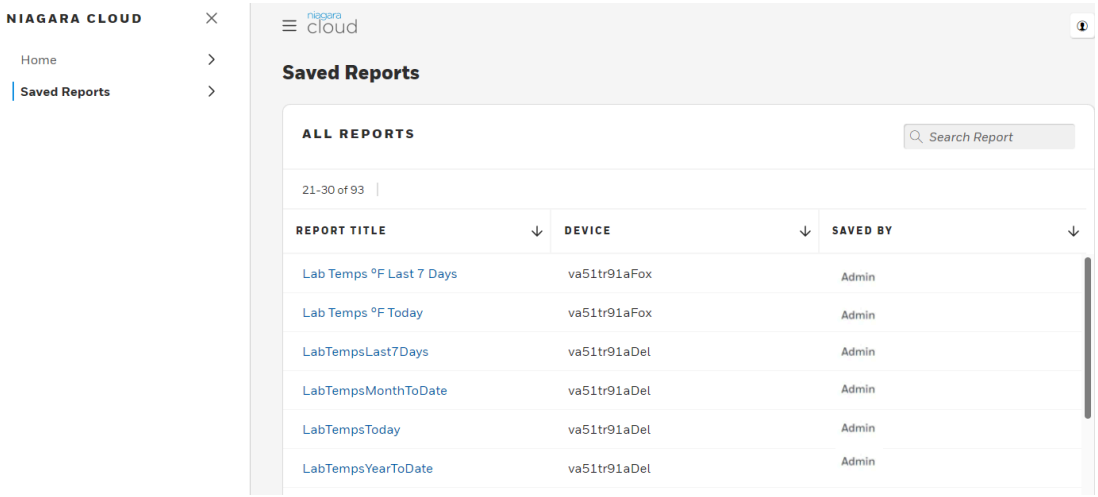
Partners access this view by clicking on a customer in the **Integrator** view. Customer users access this view when they log in to the Niagara Cloud Management Portal.

Column	Description
PROJECTS	The multiple projects under the partner could represent a campus, a building or something else. What it represents depends on how the SI organized the Niagara instance.
DEVICE/HOST ID	Within each project, identifies the devices (Niagara stations) associated with the project.
PROJECT/LOCATION	Identifies the customer site and project associated with the device.
SUBSCRIBED SERVICES	Identifies the service(s) subscribed for this device. Each link opens a service page.

Saved Reports view

This view lists the reports that have been saved and are available to customer users.

Figure 6. Saved Reports view



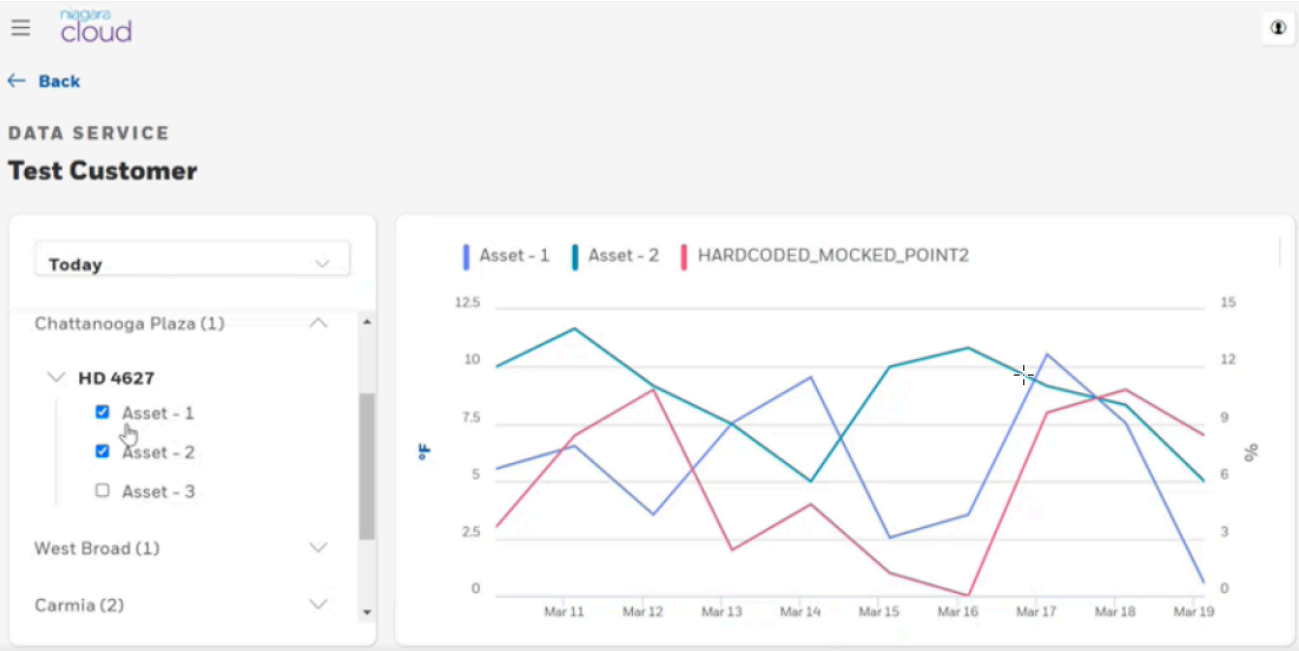
To view this report, sign in to the Niagara Cloud, click the menu button (☰) and select **Saved Reports**.

Column	Description
Report Title	Identifies the report.
Station	Selects the station whose data are plotted on the report.
By	Reports the name of the SI who created the report.

Report view

This view provides a chart of up to 10 data items stored in the Niagara Cloud.

Each line on the chart represents a data item collected from a point in the device.



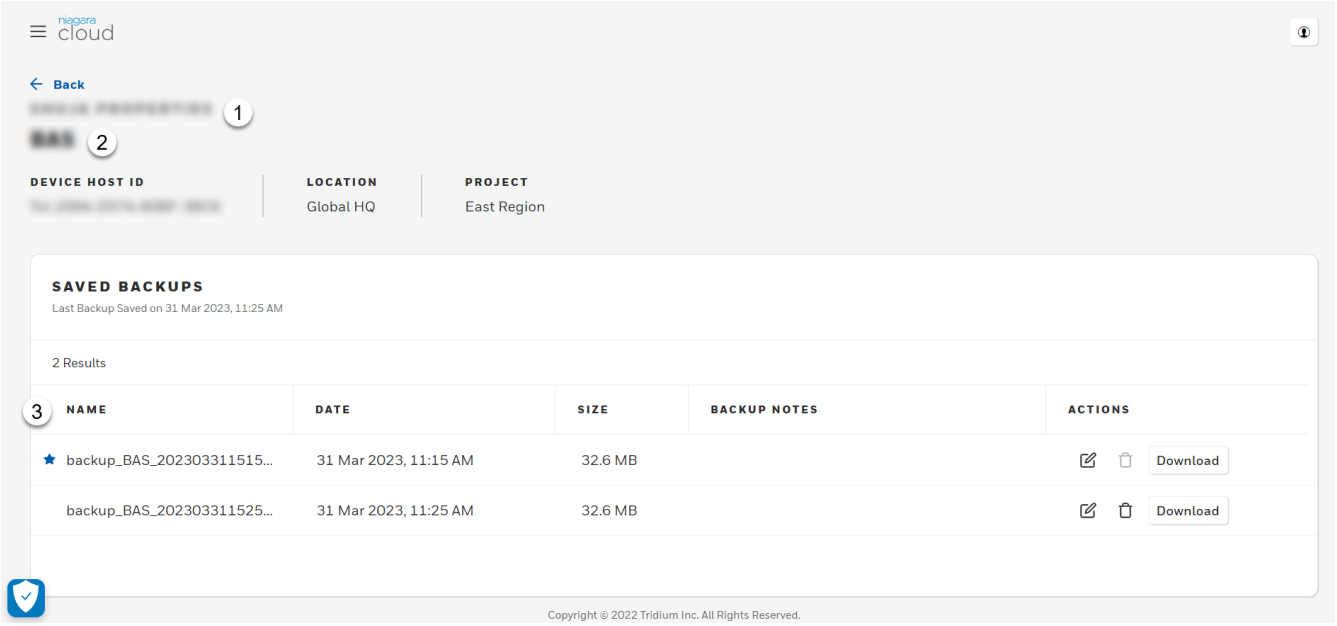
To view a report, sign in to the Niagara Cloud, click the menu button (☰), click the Data Service link for your location and select the report.

Passing the cursor over a time instance causes the tooltip to display the point's value at that time. When you select multiple points, the tooltip displays the values for all the points at the selected time.

Saved Backups view

This view provides access to all saved backup files.

Figure 7. SAVED BACKUPS view



Number	Description
1	Customer name.
2	Device name, which includes the device's host ID, location, and related project.
3	Backup information, which includes information and actions.

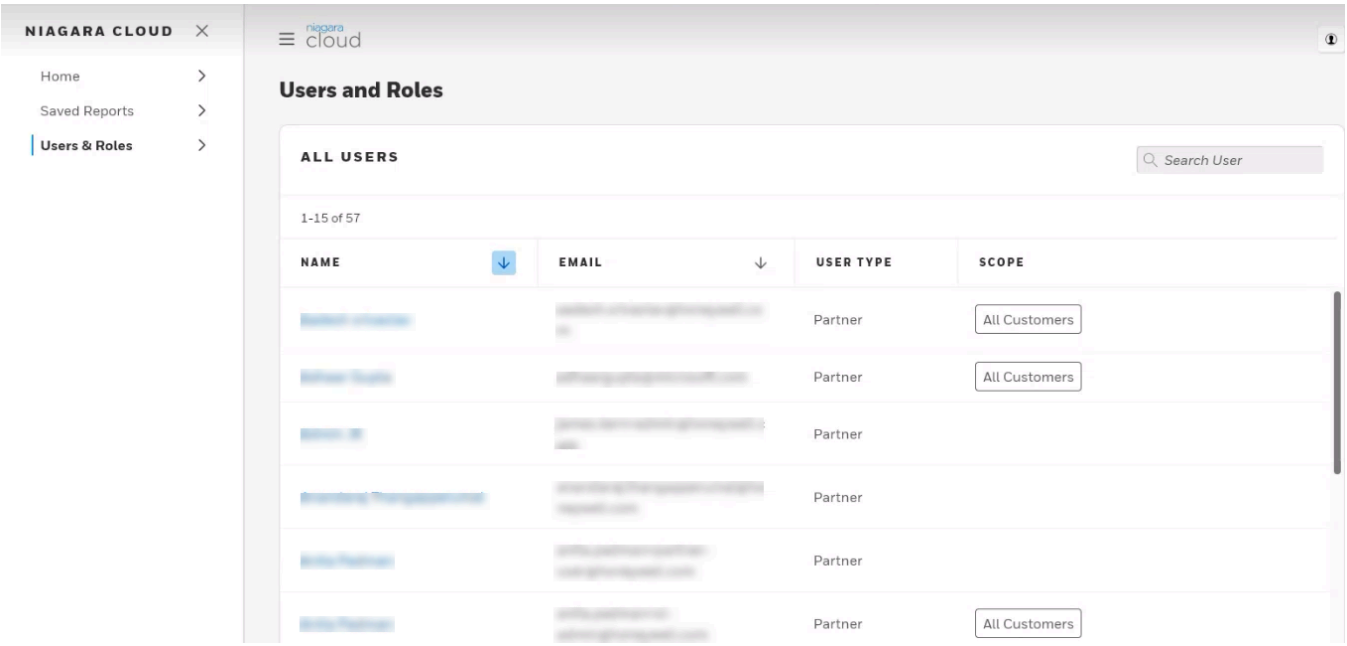
To access this view, log in to `https://www.niagara-cloud.com`, select a customer, select a project and search for a device.

Table 3. Backup file columns

Column name	Description
NAME	Shows the beginning of the backup file's name. To view a tooltip with the full name, pass your cursor over the name. The blue star identifies the preferred backup file.
DATE	Indicates when (date and time) the backup was made based on the UTC timezone.
SIZE	Indicates the size of the file in megabytes.
BACKUP NOTES	Provides up to 1024 characters of additional information. If the note is long, Niagara Recover shows the first two lines and a **More** link. Click this link to view the entire note.
ACTIONS	Provide link to edit, delete and download functions. Edit icon opens the EDIT BACKUP window from which to add a note and configure the backup as preferred. Delete icon removes the selected file from cloud storage. Download button initiates a download of the backup file to your PC.

Users and Roles view

This view, for the SI, creates users (SI users and customer users) including assigning a role to each user.

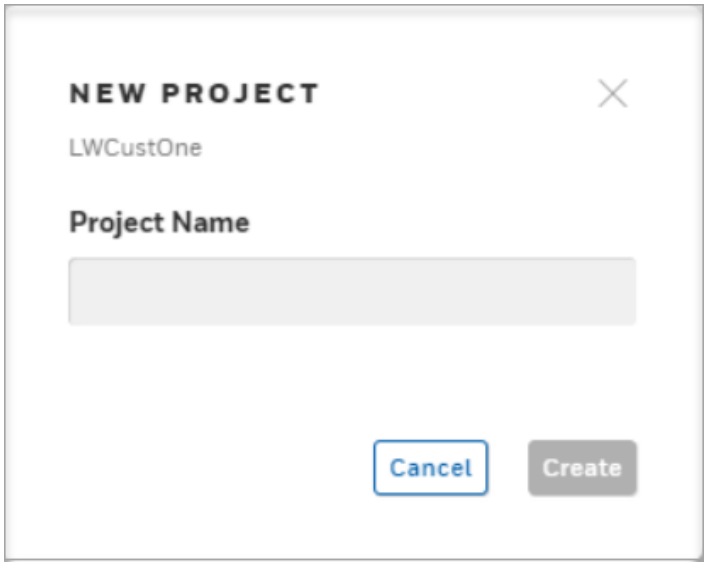


You access this view from the home page by clicking the menu icon (☰) followed by clicking **Users & Roles**.

Column	Description
Name	Defines the name of the user.
Email	Provides the email address of the user.
User Type	Identifies what type of organization the user is associated with: partner organization or customer organization.
Scope	Provides additional information about the SI. For example, Scope could identify where the SI works or some other way to identify the SI's field of influence. This property provides another way to group people within an organization.

New Customer window

This window contains the information needed to set up an account for each customer of a Tridium partner. These customers are companies that have contracted with of one of Tridium's partners for Niagara Framework services. These are not direct customers of Tridium.



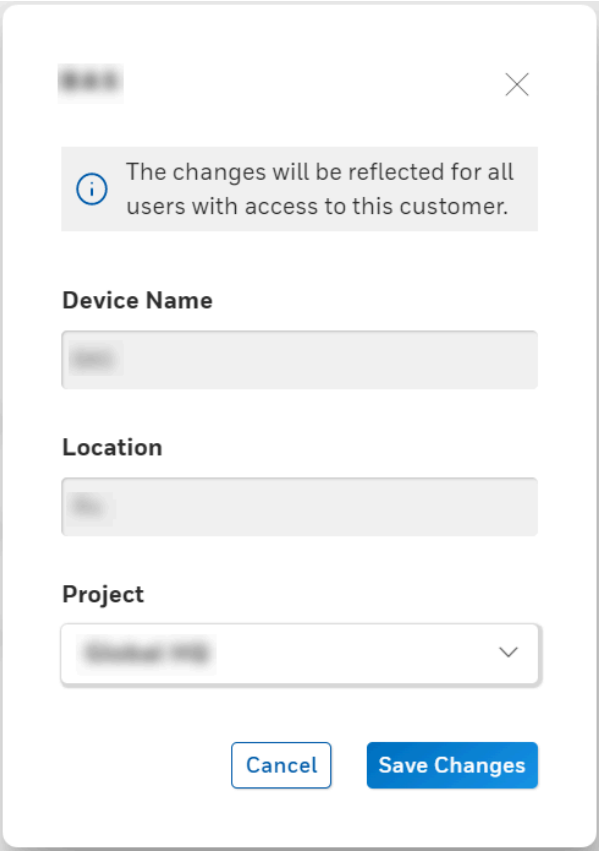
To open this window, log in to the Niagara Cloud Management Portal as an SI with the Partner Admin role and click the + **Create New Customer** button.

Property	Value	Description
Customer Name	text	Name of a company.
Tenant ID	text	Provides a uniqueidentifier for this company who shares a multi-tenant building.

Edit device window

This window contains device information. Devices are children of projects, which are children of customers.

This information is originally entered during device registration.



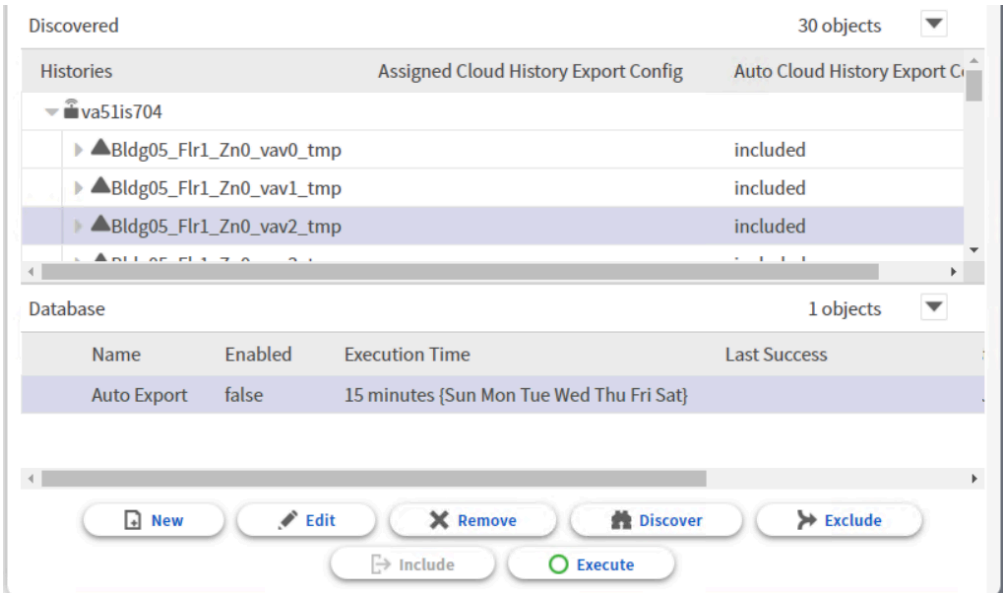
To open this window, locate a device, click the three vertical dots to the right of the device row and click **Edit**.

Property	Value	Description
Device Name	text	Identifies the device.
Location	text	Identifies where the device is located.
Project	drop-down list	Associates the device with a project for the current customer.

Cloud History, table of histories to export

This view discovers and configures export history policy.

Figure 8. Discovered histories to export



Property	Value	Description
Max Concurrent Export Executions	number (defaults to `10`)	Configures the number of export policies that can execute in parallel.
Retry Trigger	minutes (defaults to 15 minutes)	Configures how long the station waits before attempting to export histories again after a failure.
Auto Export	additional properties	Sets up a policy for exporting all histories in the station. This policy is disabled by default.

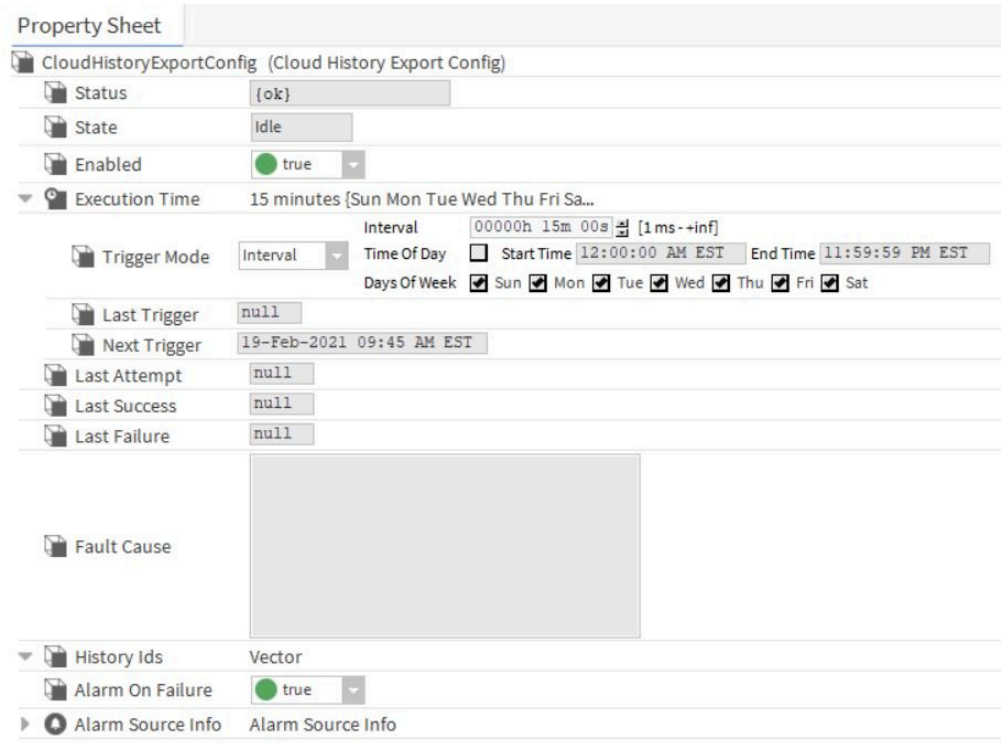
Buttons

- **New** creates a new **CloudHistoryExportConfig** (export policy) in the database.
- **Edit** opens the device's database record for updating.
- **Remove** deletes the selected CloudHistoryExportConfig objects from the database.
- **Discover** runs a discover job to locate histories, which appear in the **Discovered** pane. This view has a standard appearance that is similar to a Manager view.
- **Assign** adds the history to the CloudHistoryExportConfig.
- **Include** adds the selected history to the Auto Export policy. The **Assign** button changes to the **Include** button when you select Auto Export config in the **Database** pane and one or more histories in the **Discovered** pane.
- **Unassign** removes the history from the CloudHistoryExportConfig.
- **Exclude** removes the selected history from the Auto Export policy. The **Unassign** button changes to the **Exclude** button when you select Auto Export config in the **Database** pane and one or more histories in the **Discovered** pane.
- **Execute** triggers the CloudHistoryExportConfig to run if it is enabled.

CloudHistoryExportConfig

This component configures export history properties for individual points.

Figure 9. CloudHistoryExportConfig properties



To access these properties, expand

In addition to the standard properties (Status, Fault Cause and Enabled), these properties configure export properties.

Property	Value	Description
State	read-only	Indicates if the **CloudHistoryExportConfig** is currently executing.
Execution Time	additional properties	Controls the frequency with which the **CloudHistoryExportConfig** should send data to the cloud platform.
Execution Time, Trigger Mode, Interval	drop-down list	Controls when this export should try to send data to the cloud.
Execution Time, Trigger Mode, Time of Day	check boxes (**`Start Time`** defaults to 12:00:00 AM EST, **`End Time`** defaults to 11:29:59 PM EST)	Configures when to start exporting during the day.
Execution Time, Trigger Mode, Days of the Week	check boxes (default to daily)	Configures on which days during the week to export data.
Execution Time, Last Trigger	read-only	Reports the timestamp for the last time the data were exported.
Execution Time, Next Trigger	read-only	Reports the timestamp for the next

Property	Value	Description
		scheduled data export.
Last Attempt	read-only	Reports the date and time of the last attempted execution.
Last Success	read-only	Reports the last time the station successfully performed this function.
Last Failure	read-only	Reports the last time the system failed to perform this function. Refer to **`Fault Cause`** for details.
History Ids	vector	Lists the History Ids to be sent to the cloud platform when this export executes.
Alarm on Failure	`true` (default) or `false`	Controls the recording of ping failure alarms. `true` records an alarm in the station's AlarmHistory for each ping-detected device event (down or subsequent up). `false` ignores device down and up events.
Alarm Source Info	additional properties	Contains a set of properties for configuring and routing alarms when this component is the alarm source. For property descriptions, refer to the *Niagara Alarms Guide*

Chapter 10. Glossary

The following glossary entries relate specifically to the topics that are included as part of this document.

To find more glossary terms and definitions refer to glossaries in other individual documents.

Alphabetical listing

API
Application Programming Interfaces open a company's applications' data and functionality to other in-house developers, external, third-party developers, and business partners. APIs allow services and products to communicate, leveraging the functions provided by each. (IBM)

customer organization
A company that buys the Niagara Framework from an original equipment manufacturer or distributor. This is the organization that hires a systems integrator to set up Niagara Cloud Suite services for their system.

customer user
A person who works for a customer organization. This organization is a customer of one of Tridium's partners. A customer user is authorized to perform limited functions within the Niagara Cloud Suite.

DNS
Domain Name System, translates domain names into IP addresses, which browsers use to load Internet resources, such as web sites.

export policy
Defines when to upload data to the Niagara Cloud.

federated identity
This entity links a person's electronic identity and attributes for use across multiple distinct identity management systems. Single sign-on (SSO) uses an authentication ticket or token to trust a user's identity across multiple IT systems or even organizations. SSO is a subset of federated identity management made possible by some sort of federation. (Wikipedia)

GUID
Globally Unique Identifier also known as a UUID or Universally Unique Identifier, a 128-bit unique reference number that is highly unlikely to repeat.The device UUID is the same as the system ID contained in the **FederatedIdentityAuthenticator** component.

IoT and IoT Hub
Internet of Things, refers to a network of physical devices that connect for the purpose of exchanging data with other devices and services over the Internet. The hub is a managed service hosted in the cloud that provides a central messaging center for communication among IoT applications and attached devices.

Niagara Cloud Suite
A scalable cloud-based solution that provides secure, remote building management services.

partner
An original equipment manufacturer or other Niagara Framework distributor. A partner sells to the customer organizations who use the Niagara Framework to manage their facilities.

SI admin
Systems integrator administrator: a person associated with an original equipment manufacturer or distributor who installs and manages the Niagara Framework at a customer organization's site. This person is authorized to perform Niagara Cloud Suite functions.

SI user

Systems integrator user: a person associated with an original equipment manufacturer or distributor who supports the Niagara Framework at a customer organization's site. This person is authorized to perform limited Niagara Cloud Suite functions.

telemetry

The automatic recording and transmission of data from remote sources to a system in a different location for monitoring and analysis. Niagara's telemetry data come from the databases located in controller stations to be stored in the Niagara Cloud. The word comes from the Greek roots *tele*, which means remote, and *metron*, which means measure.