

Technical Document

Niagara Cloud Backup as a Service



About this guide

This topic contains important information about the purpose, content, context, and intended audience for this document.

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

This document describes how to connect to Niagara Cloud to manage device/station backups for station and enterprise systems. Sections in this guide include chapters about cloud-based backup tasks, concepts, and reference information. Also included are images and descriptions of the primary software user interface windows involved when working with cloud backups.

- [Document change log](#)
Updates (changes and additions) to this document are listed below.
- [Related documentation](#)
Additional information is available in the following documents.

Document change log

Updates (changes and additions) to this document are listed below.

June 21, 2023

Edited component topics to include JACE-9000.

November 13, 2019

Minor changes to facilitate online help content, plus updated image in the “CloudConnector” component topic.

August 12, 2019

Edited the “Requirements” topic to include mention of the transparent proxy server requirement.

May 23, 2019

Added valid SMA to the “Requirements” topic.

November 1, 2018

- Edited the topics, “Requirements” and “cloudBackup_CloudBackupService”, to include Supervisor platforms in statements on platform requirements.
- Edited prerequisites section in the procedure, “Restoring an unencrypted backup”.

April 2, 2018

Minor changes throughout for branding purposes only.

December 7, 2017

- In the Components section edited the topic, “cloudConnector-CloudConnector”, to revise content throughout.
- Added the topic, “cloudIotHubDep-MessageClientUpgrader” and related procedure, “Upgrading the CloudConnector to use nCloudDriver”.

September 20, 2017

- In the following topics, added content indicating that manually initiated backups can be flagged for data retention: “Backup as a Service”, “Making a manual backup”, “cloud-CloudBackupService”, and “Cloud Backup Manager view”.
- Added the procedure, “Making a cloud master backup”.

August 30, 2017

- In the topic, “Backup as a Service,” added a note regarding management of user access to controllers configured with the CloudBackupService.
- In the topics, “Backup as a Service” and “Frequently asked questions,” added the statement that there is no backup storage limit.

July 18, 2017

- Revised the following topics to include the recommendation to remove the local BackupService when installing the CloudBackupService: “Installing cloud components in the station” and “Best practices for cloud backups”.
- In the “Frequently asked questions” topic, added information about having both the local Backup Service and the Cloud Backup Service in a station.
- Added alarm alerts information to the topics describing the CloudConnector and CloudBackupService components.

July 11, 2017

Initial publication.

Parent topic: [About this guide](#)

Related documentation

Additional information is available in the following documents.

- *Niagara 4 Hardening Guide*, available on <https://www.tridium.com/us/en/services-support/library>
- *Niagara Asset Manager Guide*

Parent topic: [About this guide](#)

Overview

The emergence of “the cloud” and related technologies has enabled new delivery models for connected systems. In Niagara 4.3, expanding Niagara platform services into the cloud enables OEMs to provide traditional and new application services through modern “Internet of Things” (IoT) delivery models.

What is “cloud computing”

The term “cloud computing,” often referred to as “the cloud,” indicates the use of computing resources that are located somewhere else and accessed in the “cloud” of remote networks via Internet connectivity. These computing resources include applications, data storage centers, and other IT resources, which are accessed via self-service, on-demand, 24 x 7.

The main features of cloud computing are:

- **Flexibility** — You can scale services to meet your needs, customize applications, and access cloud services from anywhere via an Internet connection.
- **Efficiency** — Enterprise users can get applications to market quickly without developing or supporting the underlying infrastructure.
- **Strategic value** — Cloud services give enterprises a competitive advantage by providing the most innovative technology available.

What are cloud services

“Cloud services” refers to a broad category of cloud-based IT resources that a service provider delivers to customers via the Internet. Several types of services are offered via the cloud.

Infrastructure as a service offers basic computing blocks (compute, block storage, and network resources) from the cloud provider. These services provide the hardware capabilities on-demand to users to run their own software and services.

Platform as a service provides services (load balancers, identity services, message queues, managed databases, billing services, etc.) that allow a third party to build and run applications without having to develop or maintain the software or invest in hardware.

Software as a service is basically any type of application (content, analytic, communication, or backup) which runs in the cloud. This allows the user to use a web application without installing and maintaining software or storing data on a local computer or other type of device.

- **[Niagara Cloud Services](#)**
Prior to the development of cloud technology, Niagara systems typically fit one of a few architectures, with a Supervisor serving as the hub of the architecture, if present at all. In a Niagara system that includes a Supervisor, the Supervisor centralizes many system level functions (user access, system navigation, alarm management, historical data, etc.).
- **[Secure controller-to-internet communications](#)**
For the current implementation of Niagara Cloud Services running on the Sentience cloud platform, the JACE embedded controller makes a secure one-way TLS Internet connection to Niagara Cloud Services. Note that the controller is never exposed to Internet-initiated communications.
- **[About the Asset Manager tool](#)**
The Asset Manager manages users, organizations, and devices in preparation for interacting with any of the Niagara Cloud Services. Additionally, Asset Manager provides automated Niagara Service Maintenance Agreement (SMA) management and notifications.
- **[Backup as a Service](#)**

Niagara Cloud Backup as a Service (BaaS) provides easy, secure, and scalable backups of a device from the JACE station to Niagara Cloud.

Niagara Cloud Services

Prior to the development of cloud technology, Niagara systems typically fit one of a few architectures, with a Supervisor serving as the hub of the architecture, if present at all. In a Niagara system that includes a Supervisor, the Supervisor centralizes many system level functions (user access, system navigation, alarm management, historical data, etc.).

Niagara Cloud Services extend the capabilities of the Niagara application platform into “the cloud” by leveraging the capabilities of existing third party cloud platforms (for example Microsoft Azure) and adding new services to those platforms. This enables the creation of new applications that leverage the unique capabilities of any cloud platform. Additionally, the availability of Niagara Cloud Services in multiple clouds allows developers to choose the best cloud platform and combination of services to meet their application needs.

The goal of Niagara Cloud Services is to provide a new software distribution model for supervisory and application services to new and existing Niagara systems.

Parent topic: [Overview](#)

Secure controller-to-internet communications

For the current implementation of Niagara Cloud Services running on the Sentience cloud platform, the JACE embedded controller makes a secure one-way TLS Internet connection to Niagara Cloud Services. Note that the controller is never exposed to Internet-initiated communications.

The device authentication and authorization workflow occurs in this way:

- The device connects to the Sentience Identity Service, and conducts an RPK negotiation over TLS to establish device identity
- The identity service signs a short-lived JavaScript Object Notation Web Token (JWT) for the device to use to take to the provisioning service
- The provisioning service validates the token and returns a longer-lived JWT and Shared Access Signature (SAS) token for the device to use in communication with subsequent services

Additionally, the Cloud Backup Service ensures encryption of all communications, as well as integrity in transit via TLS 1.2. The encrypted backups in the cloud require the source station's system passphrase (the one in use at the time the backup was created) from Niagara 4 in order to restore the backup. Finally, the system ensures storage of sensitive data at rest (via RPK private key) by utilizing the Java KeyStore (JKS).

Security features summarized

Niagara Cloud Services protects your data via the following methods:

- User authentication provides fine grained permissions for each backup operation: view, create, download, delete
- Device authentication uses raw public key (RPK) key exchange over a one-way TLS transport
- Device authorization utilizes short-lived tokens for service-based authorizations
- Encryption of all communications and integrity in transit with TLS 1.2

- Backups in the cloud are encrypted with the source station's system passphrase
- Storage of sensitive data at rest (RPK private key) utilizes Java KeyStore

Parent topic: [Overview](#)

About the Asset Manager tool

The Asset Manager manages users, organizations, and devices in preparation for interacting with any of the Niagara Cloud Services. Additionally, Asset Manager provides automated Niagara Service Maintenance Agreement (SMA) management and notifications.

It is accessed via either of these methods:

- In a web browser connection to Niagara Community (www.niagara-community.com), click the Asset Manager link
- In a browser/Workbench connection to a station configured for cloud connectivity, click on the CloudConnector service. Note that a station connection to Asset Manager is solely for purposes of device registration and authenticating with Niagara Cloud Services.

The tool is organized by groups of related activities used to set up and maintain users, organizations, and devices. They are logically grouped by functionality.

- Organization Management - manage aspects of an organization's account. For example, the company name and address, and primary/secondary contact information.
- User Management - manage users within the organization. For example, add new users and assign roles.
- Device Management - manage device licensing maintenance and notifications, as well as user access to device backups via assigned role.

Services

Following are a few of the device-related services:

- Device Registration

Registering a device in the Asset Manager generates a System GUID (globally unique identifier) for the device. Both the device's host ID and System GUID are in the asset manager and associated with a particular organization.

- Maintenance management

Monitors device licensing and asset details.

- Notifications

Notifies Organization Managers of imminent license expirations, pending user requests, pending organization affiliation requests, as well as tagged devices

Tagged devices

Tags are metadata markers which are associated with a device in order to facilitate grouping and searching.

Roles

Roles determine which activities are authorized for a user within the Asset Manager, as shown in the following table. By default, a new user is assigned the User role which has the lowest permission level. Note that a user may be assigned multiple roles.

Role	Description
Organization Manager	Performs both user and organization management activities. Adds users, assigns user role(s), adds organization affiliations, adds devices (single or multiple), provides approvals (affiliation and user) via notifications
Device Manager	Performs device management activities including device registration and device backup. May submit business affiliation requests.
User	The default user role, the user can view basic organization and device information but cannot perform other organization- or device-related actions. Also, allows the user to manage his or her own contact information.

Parent topic: [Overview](#)

Backup as a Service

Niagara Cloud Backup as a Service (BaaS) provides easy, secure, and scalable backups of a device from the JACE station to Niagara Cloud.

Using either Workbench or a browser connection to the JACE station, you can configure automated backups by time or event triggers, or initiate a backup manually, as well as flag backups for data retention. You are able to view, download or delete your cloud backups, as well as add notes to new manually initiated backups.

Backup transmissions are streamed, so there are no block space requirements on the device. The streaming approach means that each segment of a backup is sent immediately and not saved anywhere on the device. The platform only needs to have enough space to hold that one segment, usually much smaller in size than an entire backup.

By default, backups includes all of the same elements that are included in a local backup (config.bog file, station files, graphics, licenses, and certificates). Note that the alarm and history databases are excluded by default (as in the legacy local Backup Service) mainly because these files can be very large. Cloud backups can be configured for additional exclusions if desired.

Note: It is possible to remove the default exclusions of history and alarm databases should you wish to include them in your backups. For example, if preparing to migrate a station, you may wish to make a more complete backup that includes the history and alarm databases for that station. For details on how to do this, see [cloudBackup_CloudBackupService](#).

In Niagara Cloud, a backup file is chunked, encrypted (in transit and at rest) and posted to the cloud. Once a backup is committed, it must be decrypted using the source station's system passphrase (the one in use at the time the backup was created). All backup files are encrypted so that the data is secure, and stored in Windows Azure in Microsoft's Data Centers. The encryption means that your data is safe.

Note: The management of users with admin privileges and access to JACE embedded controllers configured with the CloudBackupService is the sole responsibility of the customer.

The backup service is geo-located which means that the CloudBackupService will connect to a "traffic manager"

that will automatically route the station's backup service to a cloud service that is closest to the site, to minimize the latency (i.e. delays) in the communication while uploading the backup. Storage servers are synced in the background.

The current storage limit for cloud backups is 1GB for JACE controllers, and 5GB for Supervisors, regardless of the number of backups.

Should a hardware failure or corruption occur, any cloud backup (the last known good or historic) can be downloaded at any time (24x7x365) by authorized individuals from a secure cloud login. The backup can be downloaded in encrypted format (EDIST). Or, using the source station's system passphrase (in use at the time the backup was created), it can be downloaded in decrypted format (DIST).

If a backup is downloaded in encrypted format (EDIST), the Workbench File System provides a utility to decrypt the file using the source station's system passphrase (requires the passphrase in use at the time the backup was created).

Once decrypted the backup DIST file can then be installed on a new embedded controller, thereby minimizing disruption of operations.

Parent topic: [Overview](#)

Getting Started

Niagara Cloud Backup as a Service (BaaS) provides easy, secure, and scalable backups of a device from the JACEstation to Niagara Cloud.

Using Workbench to connect to the JACE station, you can store and delete the backups from the cloud.

- [Requirements](#)
Requirements include hardware, software and licensing.
- [Basic workflow for getting started](#)
Use this checklist as a guide to help you get started using Niagara Cloud Services.
- [Registering your organization](#)
Signing up to join the Asset Manager [on the Niagara Community portal](#) also registers your organization.

Requirements

Requirements include hardware, software and licensing.

Platform requirements

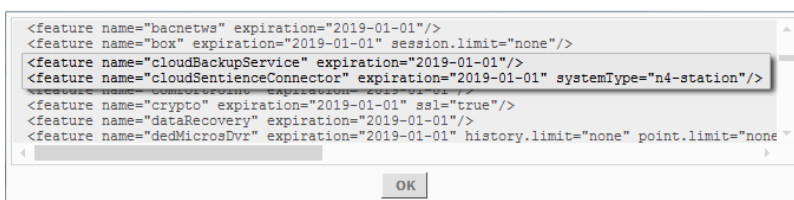
The Cloud Backup Service functions on any JACE or Supervisor platform capable of running Niagara 4.3 or later.

License requirements

For a station to connect to Niagara Cloud Services and use the Cloud Backup Service, the following features must be licensed for your platform, as shown.

- cloudBackupService
- cloudSentienceConnector

Figure 1. Cloud licensing features



Note: The cloudSentienceConnector license feature includes a “systemType” attribute with the value: “n4-station”. This specifies the system type that is registered by the connector.

Additional software requirements

- A valid Software Maintenance Agreement (SMA) is required to use BaaS.
- The following modules must be installed on your system:
 - cloudBackup (-rt, -ux, -wb)
 - cloudConnector (-rt)

- cloudSentienceConnector (-rt -ux)
- Internet access for all stations and clients.

Note: If your local network uses a proxy server to provide Internet access, work with your on-site IT department to configure the proxy server to allow access to the Niagara Cloud platform. The Cloud Connector requires that any intermediate proxy server be a fully transparent proxy; named proxy servers, also known as explicit proxy servers, are not supported at this time. The station requires unauthenticated proxy access to the following domains, which are part of the Niagara Cloud ecosystem:

- *.scm.azurewebsites.net
- *.azurewebsites.net
- *.cloud.tridium.com
- *.tridium.com
- *.dsentience.net
- *.honeywell.com
- *.force.com
- *.niagara-community.com
- *.trafficmanager.net
- *.azure-devices.net
- *.honeywellcloud.com
- *.windows.net

-
- Web browser that supports HTML5

Parent topic: [Getting Started](#)

Basic workflow for getting started

Use this checklist as a guide to help you get started using Niagara Cloud Services.

In the Niagara Community web portal...

1. Sign up to join Asset Manager. On the sign-up form:
 - Enter your organization's information
 - Accept the Electronic Users License Agreement
 - Enter your user account information
2. Access **Niagara Licensing** and add the cloud features to your JACE license.

In your Workbench PC...

1. Install the cloud software modules

In a platform connection to the JACE...

1. Set up the device for internet access
2. Install cloud connectivity software, updated license, and updated core software dist files

In a connection to the JACE station...

1. Copy the cloud services components to the station's Services node
2. Connect to Niagara Cloud and register the device (if not already preregistered).

Parent topic: [Getting Started](#)

Registering your organization

Signing up to join the Asset Manager on the Niagara Community portal also registers your organization.

- Existing user account on Niagara Community
1. Log in to Niagara Community (www.niagara-community.com) and click on **Get Started** (located lower right corner).
 2. Review the Niagara Cloud Services license agreement and click **Accept** to proceed.
 3. On the **Organization** view, click **My Organization**.
 4. Review your organization data and if necessary click **Edit** (located right side) to make changes:

The screenshot shows the 'My Organization' page with the following sections:

- My Organization** (header) with an **Edit** link on the right.
- Users & Roles** (left sidebar menu).
- Company Name**: Niagara Asset Manager Inc.
- Primary Contact**: Jane Test
- Primary Email**: niagaraassettesting@gmail.co...
- Address**: 1 Test Street, Richmond, VA 23233
- Affiliated Organizations** (table):

Affiliated Organizations		Add Affiliation	Edit List
Tridium USA Tridium, Inc. Ste 350 Richmond23233 US	Pending		
Mid-Atlantic Controls Corp 8511 Oakview Avenue Richmond23228 US	Approved		

5. If desired, click **Add Affiliation** to search for additional applicable organizations.
6. Click **Register** to complete the process.

Parent topic: [Getting Started](#)

Setting up for cloud connectivity

The following procedures describe how to set up a device and station for interaction with Niagara Cloud Services. This includes configuring DNS settings on the device, installing core and cloud software on the device, copying the necessary components to the station, and registering the device in the Asset Manager.

Additionally, where the device is on an internal (closed) network an essential prerequisite of setting up for cloud connectivity is coordinating with the on-site IT department in configuring the proxy server to allow access to Niagara Cloud servers.

- [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. Additionally, you must enter the proper DNS Server and DNS Host configuration for your network on the device.
- [Installing cloud software on the device](#)
This procedure describes using the **Commissioning Wizard** to install upgraded core software .dists and cloud connectivity software on the remote device.
- [Installing cloud components in the station](#)
This procedure describes the steps to remove the local backup service, and copy the cloud components to the station.
- [Registering the device](#)
Registering the device is required in order to make the device known to the Niagara Cloud application, as well as successfully authenticating the device. Even if the device was previously added in the Asset Manager (via the "Add Single Device" procedure), that merely tells the asset manager tool about the existence of this device. You must still complete this Device Registration procedure, initiating it from the station/device, in order to provide the secure connection information so that the device can connect to the cloud securely. This procedure describes the steps to register a device using Workbench.

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. Additionally, you must enter the proper DNS Server and DNS Host configuration for your network on the device.

A platform connection has been opened to the remote device. For a device behind a network firewall, the appropriate DNS Host Name and DNS Server IP address(es) for your network are defined.

Note: If your local network uses a proxy server to provide Internet access, work with your on-site IT department to configure the proxy server to allow access to the Niagara Cloud platform. The station requires access to the following domains, which are part of the Niagara Cloud ecosystem:

- *.scm.azurewebsites.net
 - *.azurewebsites.net
 - *.cloud.tridium.com
 - *.tridium.com
 - *.dsentience.net
 - *.honeywell.com
-

- *.force.com
 - *.niagara-community.com
 - *.trafficmanager.net
 - *.azure-devices.net
 - *.honeywellcloud.com
 - *.windows.net
-

1. In the platform **TCP/IP Configuration** view, enter the appropriate values for the following properties:
 - DNS Domain (ex: [company.net](#))
 - DNSv4Servers (add a field for one or more DNS Servers, enter the appropriate IP address for each)
2. Click **Save**.
Upon saving your changes you are prompted to reboot the device.

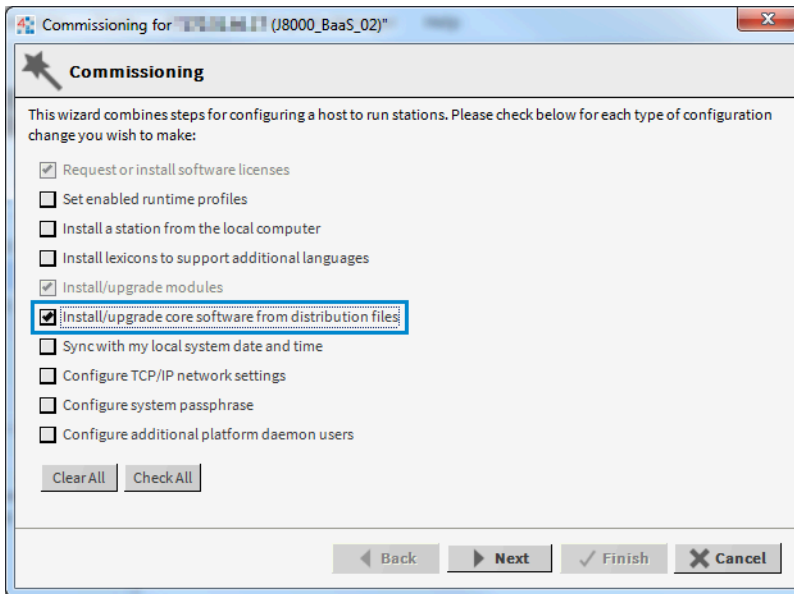
CAUTION: From a cyber security perspective, it is crucial that your station is not exposed to the Internet. The CloudConnector component requires an outbound connection from your station to the Internet, but does not allow incoming connections to your stations from the Internet. For this reason, we strongly recommend following the best practices and steps in the *Niagara 4 Hardening Guide*, which is available on: <https://www.tridium.com/us/en/services-support/library>.

Parent topic: [Setting up for cloud connectivity](#)

Installing cloud software on the device

This procedure describes using the **Commissioning Wizard** to install upgraded core software .dists and cloud connectivity software on the remote device.

- Appropriate administrative access to the Workbench PC
 - A platform user account for the JACE
1. In Workbench, open a platform connection to the remote device.
 2. In the Nav tree, right-click the Platform node and then click on the **Commissioning Wizard** option.
 3. In the **Commissioning** dialog, click **Clear All** and then (if not already selected) click the option to **Install/upgrade core software from distribution files**, as shown here:



The wizard steps you through the process and on completion, reboots the device.

Note: The "Request or install software licenses" option must also be checked (if not selected by default). This is necessary if the license has been updated to include the new cloud features and the license is not yet installed on the JACE. However, if the cloud-enabled license is already installed, then it is not necessary to update the license at this time. Additionally, the "Install/upgrade modules" option must also be checked (if not selected by default).

Parent topic: [Setting up for cloud connectivity](#)

Installing cloud components in the station

This procedure describes the steps to remove the local backup service, and copy the cloud components to the station.

- Platform connection to the device which is already commissioned with cloud-related software
 - The cloudBackup and cloudSentienceConnector palettes
1. In a platform connection to the device, open the **Application Director** and start the station.
 2. Connect to the station and in the Nav tree, expand the station Services node and delete the local BackupService (which is included in the installation by default).

Note: Always remove the local Backup Service when installing the Cloud Backup Service. The reason for this is that station operation depends upon interacting with a single backup service. The Cloud Backup Service provides all of the behavior of the local Backup Service, including local and provisioned backups, in addition to backing up to the Niagara Cloud. Leaving the local Backup Service in place when installing the Cloud Backup Service may cause confusion for users and yield unintended results when accessing and performing backups.

3. Open each of the cloud-related palettes and drag the following components to the station's Services container.
 - CloudConnector (from the cloudSentienceConnector palette)
 - CloudBackupService (from the cloudBackup palette)

The station is set up to connect to Niagara Cloud Services. You can proceed to register the device or if the device is already registered you can proceed to make cloud backups.

Parent topic: [Setting up for cloud connectivity](#)

Registering the device

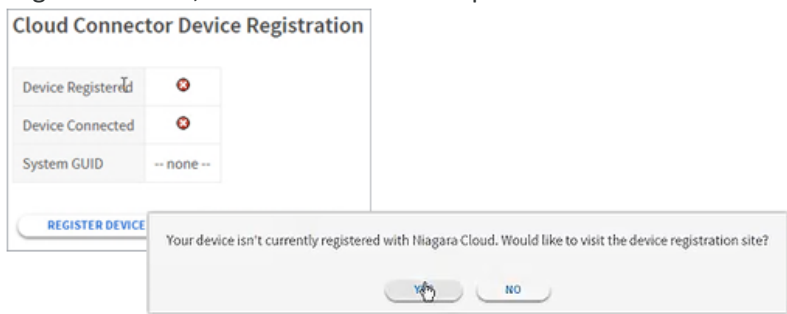
Registering the device is required in order to make the device known to the Niagara Cloud application, as well as successfully authenticating the device. Even if the device was previously added in the Asset Manager (via the "Add Single Device" procedure), that merely tells the asset manager tool about the existence of this device. You must still complete this Device Registration procedure, initiating it from the station/device, in order to provide the secure connection information so that the device can connect to the cloud securely. This procedure describes the steps to register a device using Workbench.

- An existing user account for Niagara Community
- An existing user on the Asset Manager tool with Device Manager permissions
- Connected to a running station, already configured for cloud connectivity
- The client interface (Workbench/browser) requires internet connectivity

Note: Even if the JACE/device has internet connectivity, a client Workbench/browser only connected to the private side (without internet access through the proxy) for example, will not be able to complete device registration.

Device registration may be initiated using either a browser or Workbench JACE station connection to Niagara Cloud via the Cloud Connector Service.

1. In the Nav tree, expand the station's Services container and double-click the CloudConnector component to connect to Niagara Cloud. This invokes the **Device Registration** view. The view shows that the device is not registered.
2. A popup appears confirming that the device is not registered and prompts you to go to the Device Registration site, as shown. Click **Yes** to proceed.



3. In the **Sign In** view, enter your user credentials for the Asset Manager tool and click **Sign In**.

Community Marketplace Software Licensing University Tridium

- The **Niagara Cloud Device Registration** view appears displaying your Registration Details (as shown), click **Register** to proceed.

niagara
community

Community Marketplace Software Licensing University Tridium

Niagara Cloud Device Registration

Registration Details

Registering User

Claire Newman

System Id

N4:J8000-BaaS-02:Tst-CC8F-1893-6FC4-E526

System Type

n4-station

Register

- In the certificate **Identity Verification** window, click **Accept** to accept the site certificate and proceed.
- The **Add Single Device** view appears displaying the Host ID for your JACE, click **Continue** to proceed.

Community Marketplace Software Licensing University Tridium



Asset Manager

Organization



Search



Add Single
Device

Enter Host ID*

Tst-CC8F-1893-6FC4-E526

Bulk Add
Devices

Cancel

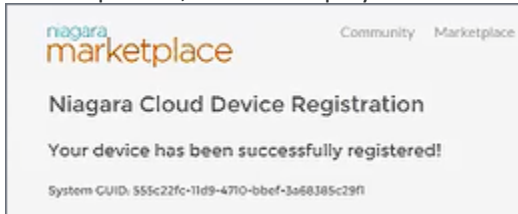
Continue

- A message appears confirming that the device has been successfully added to Asset Manager.
- The **Niagara Cloud Device Registration** view reappears displaying your Registration Details, click **Register** to proceed.

Note: Taking longer than 15 minutes to complete the **Add Single Device** workflow causes an added security measure to prevent cross-site request forgery (CSRF) attacks to be invoked. When the application focus returns to the **Device Registration** window it will not proceed automatically. If this happens, simply click the **Register** button a second time.

8. Click **Done**.

On completion, the site displays a confirmation message, as shown here.



The station is registered as a device which can use the Niagara Cloud application. You can proceed to make cloud backups.

Parent topic: [Setting up for cloud connectivity](#)

Using BaaS

This section describes how to use the Cloud Backup Service to make cloud backups manually, make master backups, configure time triggered interval backups and schedule triggered backups, download and restore cloud backups as well as delete cloud backups.

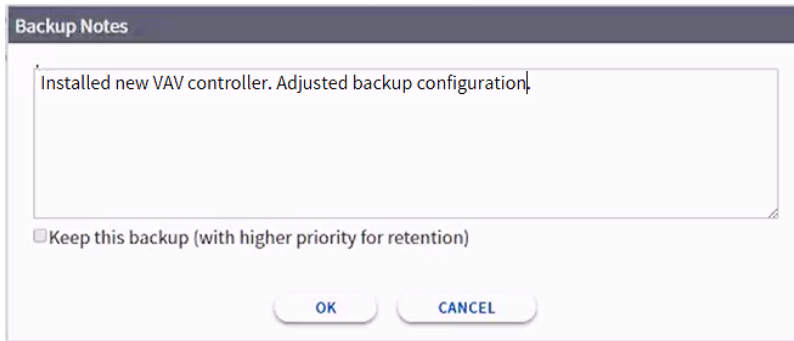
Refer to the following procedures.

- **[Making a manual cloud backup](#)**
By default, the Cloud Backup Service is configured for manually triggered backups. Using either Workbench or a browser connection to the remote station, you can easily initiate a manual backup on a registered device. This procedure describes the steps to create a manual cloud backup using a Workbench connection to the station.
- **[Making a cloud master backup](#)**
There are two types of cloud backups, Regular and Master. Master backups have a higher priority for retention than regular backups. The differentiated retention policy means that if an older backup must be replaced (deleted) due to space constraints, a regular backup will be replaced before any master backup is. A master backup will be replaced only when no regular backup exists. This procedure describes steps to make a master backup.
- **[Setting up a time triggered backup](#)**
You can automate station backups via the randomized Time Triggered interval backups to the cloud. The randomizer selects a random time for the first interval of the backup to occur. After the first backup invoked by the Trigger Mode, the subsequent backups will be triggered exactly at the set interval (7, 30 or 90) days later, at the same randomized time. Although not recommended, you can set a specific time for the Next Trigger to occur. Afterwards, the cloud backups will occur according to the set interval.
- **[Setting up a schedule triggered backup](#)**
If you require a more specific time trigger than the standard 90-, 30-, and 7-day options, you can configure the Cloud Backup Service to initiate a backup via trigger schedule. This procedure describes using Workbench to set up a trigger schedule that causes the Cloud Backup Service to run a backup at midnight each night.
- **[Downloading a cloud backup](#)**
- **[Restoring a cloud backup](#)**
As shown here, a cloud backup file can be downloaded in two different forms. The downloaded backup is either an encrypted (EDIST) file which must be decrypted (using Workbench) prior to installing it, or a decrypted (DIST) file which has been decrypted during the download process.
- **[Deleting a backup](#)**
You can easily delete one or more existing backups listed in the **Cloud Backup Manager** view.

Making a manual cloud backup

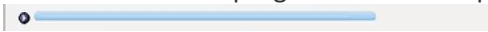
By default, the Cloud Backup Service is configured for manually triggered backups. Using either Workbench or a browser connection to the remote station, you can easily initiate a manual backup on a registered device. This procedure describes the steps to create a manual cloud backup using a Workbench connection to the station.

- Workbench connection to the JACE station
 - The station is already set up for cloud connectivity and is registered in the asset manager
1. In the Nav tree, expand station Services and double-click on Cloud Backup Service.
 2. In the **Cloud Backup Manager** view, click **Backup Now** (located at the bottom of the view).
 3. Optionally, in the **Backup Notes** dialog. Enter a descriptive backup note (max. limit is 1024 characters) and click **OK**.



Note: Adding Backup Notes is not required to complete a manual backup.

This invokes a blue progress bar that displays at the top of the view:

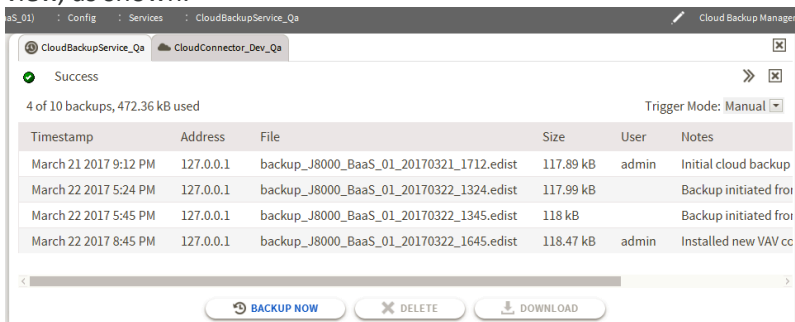


Additionally, you can click the chevron icon » (located at right) to open the backup Job bar dialog to view status messages as the backup runs. You can also double-click on items in the job log to get additional information about an entry which can be useful when diagnosing a problem.

✓ Success	22-Mar-17 4:45 PM	Writing : niagara_user_home/security/keystore.jceks
✓ Success	22-Mar-17 4:45 PM	Writing : niagara_user_home/security/untrusted.jceks
✓ Success	22-Mar-17 4:45 PM	Writing : niagara_user_home/stations/J8000_BaaS_01/config.bog
✓ Success	22-Mar-17 4:45 PM	Adding distribution manifest
ⓘ Message	22-Mar-17 4:45 PM	Written block id: c280f0b9-2e66-4f66-9fdd-27db4aa86fe9
✓ Success	22-Mar-17 4:45 PM	Backup successful
ⓘ Message	22-Mar-17 4:45 PM	Blocks written
ⓘ Message	22-Mar-17 4:45 PM	Committed backup
ⓘ Message	22-Mar-17 4:45 PM	Encrypted backup using system passphrase
ⓘ Message	22-Mar-17 4:45 PM	Backup successfully created
✓ Success	22-Mar-17 4:45 PM	Job Success

Note that this backup Job bar dialog displays only a limited number of rows (2048). The complete job log is available through the Job Service. Also note that you can click **OK** in the Job log to close the window.

On backup completion, a “Success” notification replaces the progress bar and the backup details are listed in the view, as shown.



Parent topic: [Using BaaS](#)

Making a cloud master backup

There are two types of cloud backups, Regular and Master. Master backups have a higher priority for retention than regular backups. The differentiated retention policy means that if an older backup must be replaced (deleted) due to space constraints, a regular backup will be replaced before any master backup is. A master backup will be replaced only when no regular backup exists. This procedure describes steps to make a master backup.

- Workbench connection to the JACE station
- The station is already set up for cloud connectivity and is registered in the asset manager

Note: Only a manually initiated backup can be set as a master backup. Also once the master designation is applied to a backup, it cannot be changed.

1. In the **Cloud Backup Manager** view, click **Backup Now** (located at the bottom of the view).
2. In the **Backup Notes** dialog. Enter a descriptive backup note if desired, click the checkbox to **Keep this backup (with higher priority for retention)**, and click **OK**.

A progress bar displays at the top of the view while the backup is being created. On completion, a “Success” notification replaces the progress bar and the backup details are listed in the view, as shown.

CloudBackupService_QA						
Success						
5 backups out of 5 allowed, 725.02 kB used						
Timestamp	File	Size	Retain	User	Notes	
Sep 12 2017 3:34 PM EDT	backup_emanqapation_20170912_1534.edist	62.48 kB	yes	admin	Master of backups.	
Sep 12 2017 3:42 PM EDT	backup_emanqapation_20170912_1542.edist	62.53 kB	no	admin	Regular #2	
Sep 13 2017 8:31 AM EDT	backup_emanqapation_20170913_0832.edist	199.99 kB	no	admin	Unleaded	
Sep 13 2017 8:33 AM EDT	backup_emanqapation_20170913_0833.edist	200 kB	yes	admin	Full of lead.	
Sep 13 2017 8:55 AM EDT	backup_emanqapation_20170913_0855.edist	200 kB	no	Automatic trigger	Cloud backup initiated from service trigger schedule	

Note that the “yes” value in the **Retain** column indicates a Master backup. The “no” value indicates a Regular backup.

Parent topic: [Using BaaS](#)

Setting up a time triggered backup

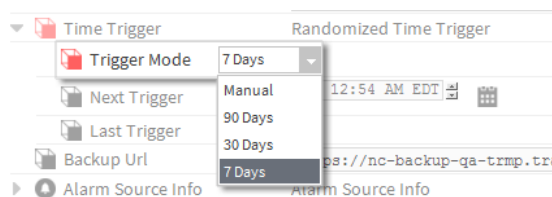
You can automate station backups via the randomized Time Triggered interval backups to the cloud. The randomizer selects a random time for the first interval of the backup to occur. After the first backup invoked by the Trigger Mode, the subsequent backups will be triggered exactly at the set interval (7, 30 or 90) days later, at the same randomized time. Although not recommended, you can set a specific time for the Next Trigger to occur. Afterwards, the cloud backups will occur according to the set interval.

- User role(s) already assigned to you in the asset manager
- Connected to a running station, already configured for cloud connectivity
- The device is already registered in the asset manager

Note: You can use either Workbench or a browser connection to the remote station to configure the randomized time triggered interval backups. Also, configuring the time trigger can be accomplished either in the **Cloud Backup Manager** view or in the **Property Sheet** view for the Cloud Backup Service.

This procedure describes how to set up a time triggered backup using a Workbench connection to the remote station.

1. In the Nav tree, expand station Services and double-click on the Cloud Backup Service to invoke the **Cloud Backup Manager** view.
2. Click on the Trigger Mode dropdown list and select one of the following preset periods: 90 Days, 30 Days, or 7 Days.



- For example, if you choose 7 Days, the station will initiate a cloud backup every 7 days.
3. In the Next Trigger field, enter the desired date and time for the next backup to occur, and click **Save**.

Note: Entering a specific time for the Next Trigger somewhat negates the purpose of the randomizer, which is to balance demand.

Automated cloud backups will occur at the set interval starting on the specified date and time. Note that automated backups have a lower priority for retention, preventing the inadvertent replacement of manually created master backups.

Parent topic: [Using BaaS](#)

Setting up a schedule triggered backup

If you require a more specific time trigger than the standard 90-, 30-, and 7-day options, you can configure the Cloud Backup Service to initiate a backup via trigger schedule. This procedure describes using Workbench to set up a trigger schedule that causes the Cloud Backup Service to run a backup at midnight each night.

- User role(s) already assigned to you in asset manager
- Connected to a running station, already configured for cloud connectivity
- The device is already registered in the asset manager
- Schedule palette

1. Open a **Property Sheet** view on the Cloud Backup Service.
2. From the schedule palette, drag a Trigger Schedule to the top of the property sheet.
3. In the **Name** dialog, enter a name for this event trigger, for example: Midnight_Backup.
4. In the property sheet, click on the new trigger property to open the **Trigger Scheduler** view.
5. Click to **Add** a new event trigger, configure the event name, date, and time as needed and click **Save**. For this example, the new MidnightBackupTrigger is set to occur every day at 12:00 AM.

6. In the Nav tree, expand the Cloud Backup Service, and link the new event trigger (ex: Midnight_Backup) to the Cloud Backup Service. To do this:
 - a. Right-click on the new event trigger (ex: Midnight_Backup) and click **Link Mark**.
 - b. Right click on the Cloud Backup Service and click **Link From (ex: Midnight_Backup)** .
 - c. In the **Link** dialog, click on the source slot Trigger and the target slot Backup, and click **OK**.

The added event trigger will trigger the service to run a cloud backup each night at midnight. Note that although useful as an example, this degree of frequency may not be preferable in an actual production environment.

Parent topic: [Using BaaS](#)

Downloading a cloud backup

- Niagara 4 user role that permits access to the Cloud Backup Service's category
 - Device is already registered in the asset manager
 - Connected to a running station, already configured for cloud connectivity
 - Existing cloud backups
1. In the **Cloud Backup Manager** view, select the desired backup and click **Download**.
 2. In the **Choose Backups Directory** dialog, browse to select a directory on the local PC to store the downloaded backup, as shown.
 3. In the **Download** dialog, select the desired download option:
 - [Download encrypted \(secure\) EDIST file](#)
 - [Download decrypted \(non secure\) DIST file](#)

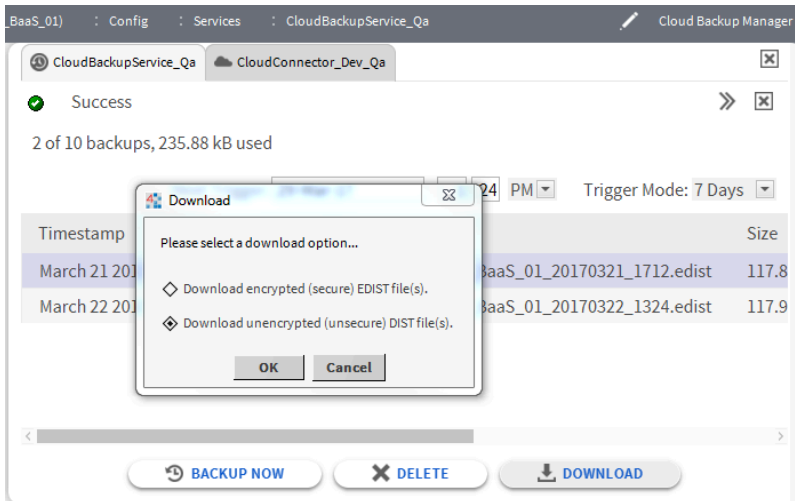
Note: In order to restore and decrypt a downloaded encrypted EDIST backup file you are prompted to provide the source station's system passphrase. That would be the passphrase in use at the time the backup was created, which may not be the current passphrase. The same is true when downloading an unencrypted DIST file (download and decrypt "on the fly") you are prompted to provide the source station's system passphrase in order for the download to complete.

On completion a **Success** dialog appears letting you know the file(s) were successfully downloaded.

Parent topic: [Using BaaS](#)

Restoring a cloud backup

As shown here, a cloud backup file can be downloaded in two different forms. The downloaded backup is either an encrypted (EDIST) file which must be decrypted (using Workbench) prior to installing it, or a decrypted (DIST) file which has been decrypted during the download process.



- [Restoring an encrypted backup](#)
This procedure describes the steps to restore a downloaded encrypted cloud backup (EDIST) file on a remote controller using Workbench.
- [Restoring an unencrypted backup](#)
This procedure describes the steps to install an unencrypted cloud backup (DIST) file on a remote controller using Workbench.

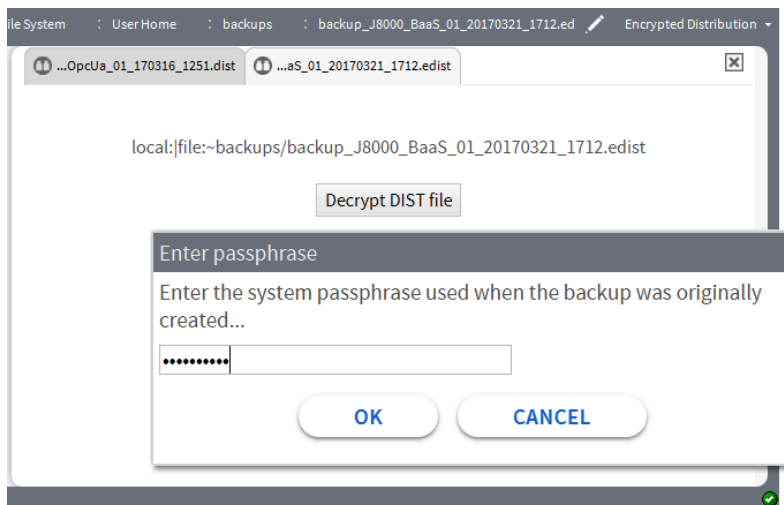
Parent topic: [Using BaaS](#)

Restoring an encrypted backup

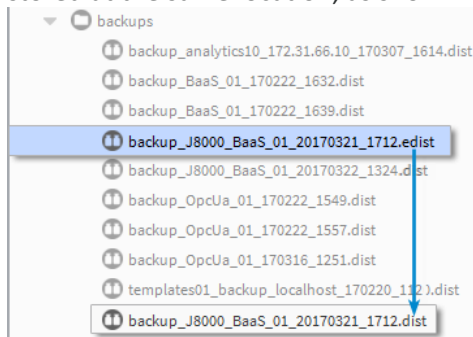
This procedure describes the steps to restore a downloaded encrypted cloud backup (EDIST) file on a remote controller using Workbench.

- Connected to a running station, already configured for cloud connectivity
 - Appropriate administrative access to the Workbench PC
 - A platform user account for the JACE
 - One or more encrypted cloud backups already downloaded
 - The source station's system passphrase.
1. In the Nav tree, navigate to your stored cloud backups.
 2. Double-click on an encrypted (*.edist) backup file to invoke the **Encrypted Distribution** view, and click **Decrypt DIST file**.
 3. In the **Enter Passphrase** dialog, enter the source station's system passphrase and click **OK**.

Note: You must enter the system passphrase that was in use at the time the backup was created, which may not be the current passphrase.



During decryption the EDIST file is converted to an unencrypted DIST file of the same name, and is stored at the same location, as shown.



4. A confirmation dialog appears, notifying you of the successful decryption and prompts whether you want to go to the DIST file. Click **Yes** to continue. The dist file appears in the **Distribution View**, listing the file details as well as software dependencies and exclusions.

Note: If you click **No** in the confirmation dialog, the view remains focused on the EDIST file (selected in Step 2) in the **Encrypted Distribution** view.

You can proceed to install the newly decrypted DIST file using the platform **Distribution File Installer**. Refer to the procedure, [Restoring an unencrypted backup](#).

Parent topic: [Restoring a cloud backup](#)

Restoring an unencrypted backup

This procedure describes the steps to install an unencrypted cloud backup (DIST) file on a remote controller using Workbench.

- Connected to a properly licensed platform commissioned with the same version of Niagara as that of the downloaded backup
- One or more decrypted cloud backups already downloaded and stored in your User Home Backups folder.

Note: If your controller has suffered a hardware failure, you can download the cloud backup via the asset manager tool in the Niagara Community portal, and save it to the Workbench PC that is commissioning the

replacement JACE.

1. Open a platform connection to the controller.
2. Double-click on the **Distribution File Installer** option.
3. In the **Distribution File Installer** view, click **Backups**.
4. Select the desired unencrypted DIST file and click **Install**.

Parent topic: [Restoring a cloud backup](#)

Deleting a backup

You can easily delete one or more existing backups listed in the **Cloud Backup Manager** view.

- Device is already registered in asset manager
 - Connected to a running station, already configured for cloud connectivity
 - Existing cloud backups
1. In the Nav tree, click to expand the station **Config > Services** nodes and double-click on the CloudBackupService.
 2. In the **Cloud Backup Manager** view, select the backup to be removed and click **Delete** (located at the bottom of the view).
 3. In the confirmation dialog, click **Yes** to proceed.

On completion, the view refreshes with the deleted backups removed.

Parent topic: [Using BaaS](#)

BaaS reference

This section provides information on frequently asked questions, best practices for cloud backups, components and plugins, as well as troubleshooting tips.

Refer to the following topics.

- [Frequently asked questions](#)
- [Best practices for cloud backups](#)
Following is a list of recommended best practices for cloud backup usage.
- [Components](#)
Components include services, folders and other model building blocks associated with a module. You may drag them to a property or wire sheet from a palette.
- [Plugins](#)
There are many ways to view plugins (views). One way is directly in the tree. In addition, you can right-click on an item and select one of its views. Plugins provide views of components.
- [Troubleshooting](#)
This topic covers general issues that may occur during a backup to the cloud.

Frequently asked questions

- **What are the version compatibilities of BaaS?**

Backup as a Service is compatible with Niagara 4.3 and later.

- **Can I have both the local Backup Service and the Cloud Backup Service in a station?**

Always remove the local Backup Service when installing the Cloud Backup Service. The reason for this is that station operation depends upon interacting with a single backup service. The Cloud Backup Service provides all of the behavior of the local Backup Service, including local and provisioned backups, in addition to backing up to the Niagara Cloud. Leaving the local Backup Service in place when installing the Cloud Backup Service may cause confusion for users and yield unintended results when accessing and performing backups.

- **Where is my data actually stored? Are the data centers in the U.S.?**

Your cloud backups are stored in the Microsoft Azure cloud platform, geo-located in the nearest Microsoft data center (either US east coast or US west coast). The data is encrypted at all times and only your authenticated users can see the data.

- **How secure is BaaS? Is my data safe?**

The data is encrypted end-to-end, which means in transit and at rest. This makes it impossible for anyone other than your authenticated users to view your data. The JACE is connected to the Internet but makes only outgoing connections. The controller will not accept incoming messages from the Internet.

- **What cloud backup actions can I perform while logged in to the Asset Manager tool in Niagara Community?**

In the Asset Manager tool, while viewing the **Asset Details** for a particular Host Id, you can click the link to **View All Backups** for that device. While viewing the list of backups you can download encrypted backup EDIST files, or view the full text of a backup note, as well as delete selected backups. Note that you cannot initiate a backup from the Asset Manager.

- **How can I automate cloud backups?**

Set up time triggered cloud backups. Using the Trigger Mode dropdown list in the **Cloud Backup Manager** view you can schedule backups to occur periodically.

- **What if my JACE doesn't have connectivity?**

The unit must have internet connectivity in order to connect to Niagara Cloud.

- **What are the space requirements for the cloud modules?**

The cloud-related modules listed here require an additional 150k disk space on the controller:

- cloudBackup (-rt, -ux, -wb)
- cloudConnector (-rt)
- cloudSentienceConnector (-rt -ux)

- **What is the backup storage capacity?**

The current storage limit for cloud backups is 1GB for JACE controllers, and 5GB for Supervisors, regardless of the number of backups.

Using the FIFO (First In First Out) file rotation method, when the storage limit is reached the first backup made is the first backup to be deleted. This automatically makes space for your most recent backups.

Parent topic: [BaaS reference](#)

Best practices for cloud backups

Following is a list of recommended best practices for cloud backup usage.

- For Systems Integrators, it can be difficult to keep track of the last known good backup for a particular customer. A best practice is to always use the Cloud Backup Service to safely store the latest backups to the cloud. This practice makes the same set of backups, including the last known good backup, available to the SIs.
- For an established fully configured JACE station, a 30 or 90 day backup is sufficient to retain configuration data.
- Always remove the local Backup Service when installing the Cloud Backup Service. The reason for this is that station operation depends upon interacting with a single backup service. The Cloud Backup Service provides all of the behavior of the local Backup Service, including local and provisioned backups, in addition to backing up to the Niagara Cloud. Leaving the local Backup Service in place when installing the Cloud Backup Service may cause confusion for users and yield unintended results when accessing and performing backups.
- Using the randomized Trigger Mode is recommended. The randomizer selects a random time for the first interval of the backup to occur. After the first backup invoked by the Trigger Mode, the subsequent backups will be triggered exactly at the set interval (7, 30 or 90) days later, at the same randomized time.

Parent topic: [BaaS reference](#)

Components

Components include services, folders and other model building blocks associated with a module. You may drag them to a property or wire sheet from a palette.

Descriptions included in the following topics appear as context-sensitive help topics when accessed by:

- Right-clicking on the object and selecting **Views > Guide Help**
- Clicking **Help > Guide On Target**
- [Cloud Connector \(cloudConnector-CloudConnector\)](#)
This component enables a **NiagaraStation** running in a localhost or on an embedded controller to securely connect to a specific cloud platform.
- [MessageClientUpgrader \(cloudIoTHubDep-MessageClientUpgrader\)](#)
This component facilitates the upgrading of messages from the cloudBackup driver to the nCloudDriver. It has no properties.
- [cloudBackup_CloudBackupService](#)
This component provides the functionality for a registered device to initiate cloud backups. **Cloud Backup Manager** is the default view for this component. The Cloud Backup Service component is found in the cloudBackup palette.

Parent topic: [BaaS reference](#)

Cloud Connector (cloudConnector-CloudConnector)

This component enables a **NiagaraStation** running in a localhost or on an embedded controller to securely connect to a specific cloud platform.

For example, the **CloudConnector_Sentience nCloudDriver** component provides device registration and a secure connection to the Honeywell Sentience cloud platform for use with the Niagara CloudNiagara Cloud and other cloud services.

In addition to enabling cloud connectivity, the cloud connector authenticates the device to Niagara Cloud; maintains a message queue for sending messages to and from the cloud; raises an alarm if a connectivity problem occurs; and provides a bearer token to other services to identify those as coming from a properly registered device.

The cloud connector service generates alerts for the fault state, that is `Cannot connect to Cloud` and routes them to the alarm class specified in the service's Alarm Source Info property.

Device Registration is the default view that enables a user to register a device.

This component is found in the cloudSentienceConnector palette.

In the Niagara Cloud release 2018_4 and later, the connectors in the cloudSentienceConnector palette are renamed for clarity. The intended use for each one is as follows:

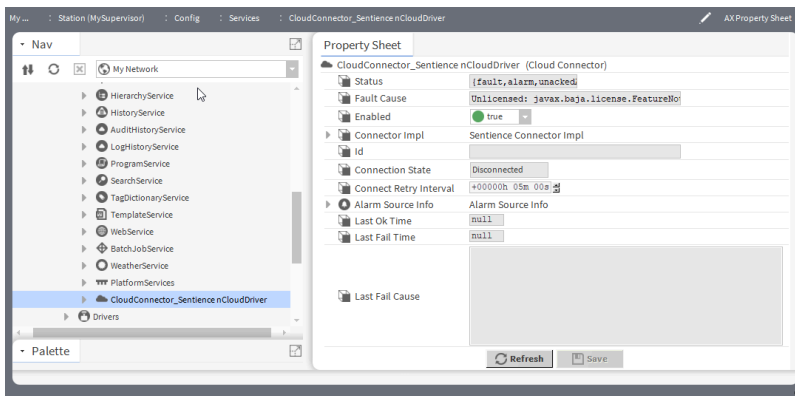
- **CloudConnector_Sentience nCloudDriver** supports the Niagara Cloud and .
- **CloudBackupService** supports the JACE-8000 and JACE-9000 controllers.
- Use “CloudConnector_Sentience cloudBackup Only” for CloudBackupService when nCloudDriver is not supported (JACE-7 and older).
- Upgrade From cloudBackup Only to nCloudDriver supports installations that initially provided a

connector that was for cloud backups only, or if you had an older connector that pre-dates the release of Niagara Cloud.

Place **Upgrade From cloudBackup Only to nCloudDriver** under **CloudConnector/Connector Impl** and select the action **Switch To lot Hub Message Client**. A JACE-8000 and JACE-9000, as well as the CloudlotHubDep-rt.jar module are required for this upgrade.

For legacy platforms (JACE-3, JACE-6, JACE-7 and JACE-8000), and JACE-9000 platforms that are only used for cloud backups, only use the CloudConnector_Sentience cloudBackup Only component. This component does not support the Niagara Cloud, so this driver should not be used with legacy JACE platforms or with JACE-8000 platforms that are only used for cloud backups.

Figure 1. CloudConnector_Sentience nCloudDriver properties



To access these properties, expand **Config > Services**, scroll to **CloudConnector_Sentience nCloudDriver**, right-click the driver and click **Views > AX Property Sheet**.

Name	Value	Description
Status	read-only	<p>Indicates the condition of the connector at the last check.</p> <ul style="list-style-type: none"> {ok} indicates that the cloud connector component is licensed, registered with Sentience and Niagara Cloud, and successfully connected. {down} indicates that the cloud connector is not connected to the Niagara Cloud, perhaps it is not registered, or possibly loss of network connection. {disabled} indicates that the Enable property is set to false. {fault} indicates another problem. Check the Fault Cause property for more information.
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension,

Name	Value	Description
		etc.) is not working (in fault). This property is empty unless a fault exists.
Enabled	true (default) or false	Activates (true) and deactivates (false) use of the object (network, device, point, component, table, schedule, descriptor, etc.).
Connector Impl	additional properties	Contains read only properties that show registration and connection URLs, which determine how the device will be registered and connected. The topic SentienceConnectorImpl documents these properties.
Id	text string	Defines a globally unique identifier for each host, supplied by the Identity Provider with which the connector is registered. For the Honeywell Forge cloud platform, this is a system GUID (Globally Unique Identifier) that uniquely identifies the station within the cloud platform.
Connection State	read-only	Indicates whether or not the cloud connector is currently connected to the specified cloud platform. <i>Disconnected, Connected, Pending Connect</i>
Connect Retry Interval	hours minutes seconds (defaults to 20 seconds)	Configures the amount of time between attempts to establish a connection upon a failure to connect.
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 <i>Niagara Alarms Guide</i>
Last OK Time	read-only	Displays the last date and time the cloud connector was functioning as expected.
Last Fail Time	read-only	Displays the last date and time the cloud connector failed to connect.
Last Fail Cause	read-only	Displays the reason for the last failure of the cloud connector to connect.

Actions

- **Reconnect** — This helps to reconnect the cloud.

Parent topic: [Components](#)

MessageClientUpgrader (cloudIoTHubDep-MessageClientUpgrader)

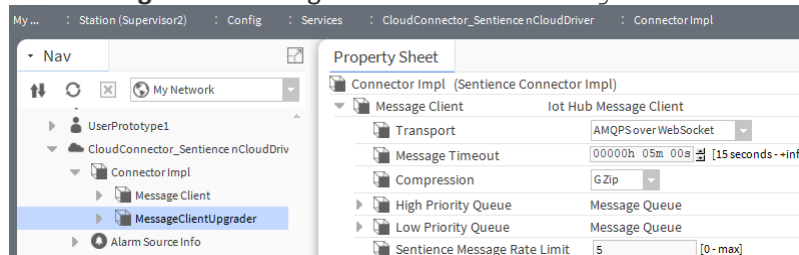
This component facilitates the upgrading of messages from the cloudBackup driver to the nCloudDriver. It has no properties.

This component is available in the cloudSentienceConnector palette.

This component makes a slight change to the installed cloud connector to use the modules for the Niagara Cloud.

To use this component, from the cloudSentienceConnector palette, expand **Upgrade From cloudBackup Only to nCloudDriver**, move **MessageClientUpgrader** to the **Connector Impl** folder, then right-click **MessageClientUpgrader** and select **Actions > Switch to IoT Hub Message Client**.

The **Message Client** changes from Null Message Client to IoT Hub Message Client.



Actions

- **Switch To IoT Hub Message Client** changes to the IoT Hub Message Client.
- [Upgrading the Cloud Connector to use Niagara Cloud](#)
This procedure is only necessary if your Niagara 4.3 installation included the cloudConnector/cloudSentienceConnector modules for BaaS, and you have subsequently upgraded to Niagara 4.4.

Parent topic: [Components](#)

Upgrading the Cloud Connector to use Niagara Cloud

This procedure is only necessary if your Niagara 4.3 installation included the cloudConnector/cloudSentienceConnector modules for BaaS, and you have subsequently upgraded to Niagara 4.4.

- The cloudSentienceConnector palette is required.

Note: If either of the following is true, then you do NOT need to perform this procedure:

- If you installed the cloudConnector/cloudSentienceConnector modules in Niagara 4.4 or greater.
- If you are using a “legacy” JACE (i.e., JACE-3, JACE-6, or JACE-7; basically anything other than a JACE-8000 or JACE-9000 or Supervisor), then you cannot use the Niagara Cloud, so this procedure is not necessary. Also, if you are not configuring the JACE-8000 or JACE-9000 or Supervisor for Niagara Cloud then it is not necessary to perform this procedure.

1. In the **Open Palette** window, click **Browse** to locate and open the cloudSentienceConnector palette.
2. Drag the MessageClientUpgrader onto the ConnectorImpl child of the installed CloudConnector service.
3. Right-click on the MessageClientUpgrader, and select **Actions > Switch To IoT Hub Message Client**

The CloudConnector is upgraded. Typically, this is done only once and afterwards you can delete the MessageClientUpgrader component.

Parent topic: [MessageClientUpgrader \(cloudIoTHubDep-MessageClientUpgrader\)](#)

cloudBackup_CloudBackupService

This component provides the functionality for a registered device to initiate cloud backups. **Cloud Backup Manager** is the default view for this component. The Cloud Backup Service component is found in the cloudBackup palette.

Cloud Backup Service properties

The Cloud Backup Service is licensed for JACE and Supervisor platforms capable of running Niagara 4.3 or greater.

Via the service, you can manage your cloud backups as follows:

- view existing backup details
- download backups (encrypted and decrypted)
- manually initiate backups and if desired, flag them for data retention
- configure randomized time triggered backups
- delete backups

The Cloud Backup Service generates alerts for the fault state, i.e. `Cloud backup failed`. Alerts are routed to the alarm class specified in the service's Alarm Source Info property.

Name	Value	Description
Status	read-only	Reports the condition of the entity or process at last polling. {ok} indicates that the component is licensed and polling successfully. {down} indicates that the last check was unsuccessful, perhaps because of an incorrect property, or possibly loss of network connection. {disabled} indicates that the Enable property is set to false. {fault} indicates another problem. Refer to Fault Cause for more information.
Fault Cause	read-only	Indicates the reason why a system object (network, device, component, extension, etc.) is not working

Name	Value	Description
		(in fault). This property is empty unless a fault exists.
Enabled	true or false	Activates (true) and deactivates (false) use of the object (network, device, point, component, table, schedule, descriptor, etc.).
Exclude Files	*.hdb;*.adb;*.lock;*backup*;console.*;config.bog.b*;config_backup*	Specifies the types of files to omit from backups.
Exclude Directories	file:^^alarm; file:^^history	Specifies the directories to omit from backups.
Offline Exclude Files	*.hdb;*.adb;*.lock;*backup*;console.*;config.bog.b*;config_backup*	Specifies the types of files to omit from backups that are created when performing an offline backup, i.e., the station is not running on the controller.
Offline Exclude Directories	*.lock;*backup*;console.*;config.bog.b*;config_backup*	Specifies the directories to omit from backups that are created when performing an offline backup, i.e., the station is not running on the controller.
Trigger Mode	7–days (default), 30–days, 90-days, Manual	Specifies whether to initiate backups using one of the randomized time trigger intervals or to initiate backups manually.
Next Trigger	date, time, AM/PM, time zone	Specifies the next scheduled trigger firing time.
Last Trigger		Displays the timestamp of the last firing of the trigger firing time.
Backup URL		Specifies the URL used to connect to the BaaS application in Niagara Cloud Services.
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 <i>Niagara Alarms Guide</i>
Block Size	4MB (default)	Defines the block size for backup files being written to the cloud.

Name	Value	Description
		A cloud backup is split into and streamed to the cloud in blocks. For example, a 360MB backup file will comprise 90 4MB blocks. There is no limit on the number of blocks for a backup file (as many as it takes)

Note: It is possible to remove the default exclusions of history and alarm databases, should you wish to include them in your backups. This would require modifying the default configuration on the Cloud Backup Service, removing both of the entries listed in the excludeDirectories property, as well as removing the entries (*.hdb and *.adb) listed in the excludeFiles property.

Actions

When you right-click on the service you can invoke the following action(s):

- Backup — initiates a backup

Parent topic: [Components](#)

Plugins

There are many ways to view plugins (views). One way is directly in the tree. In addition, you can right-click on an item and select one of its views. Plugins provide views of components.

In Workbench, access the following summary descriptions on any plugin by selecting **Help > On View (F1)** from the menu, or pressing **F1** while the view is open.

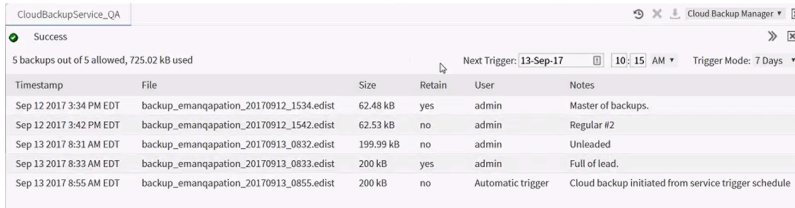
- [Cloud Backup Manager view](#)
The **Cloud Backup Manager** is the default view for the Cloud Backup Service. The view lists the cloud backups for the station and allows you to perform backup-related functions.
- [Device Registration](#)
Device Registration, is the default view for the Cloud Connector Service component. Double-clicking the component invokes this view which queries the device to determine if it is registered to access Niagara Cloud Services.

Parent topic: [BaaS reference](#)

Cloud Backup Manager view

The **Cloud Backup Manager** is the default view for the Cloud Backup Service. The view lists the cloud backups for the station and allows you to perform backup-related functions.

Figure 1. Cloud Backup Manager view



Timestamp	File	Size	Retain	User	Notes
Sep 12 2017 3:34 PM EDT	backup_emanqapation_20170912_1534.edist	62.48 kB	yes	admin	Master of backups.
Sep 12 2017 3:42 PM EDT	backup_emanqapation_20170912_1542.edist	62.53 kB	no	admin	Regular #2
Sep 13 2017 8:31 AM EDT	backup_emanqapation_20170913_0832.edist	199.99 kB	no	admin	Unleaded
Sep 13 2017 8:33 AM EDT	backup_emanqapation_20170913_0833.edist	200 kB	yes	admin	Full of lead.
Sep 13 2017 8:55 AM EDT	backup_emanqapation_20170913_0855.edist	200 kB	no	Automatic trigger	Cloud backup initiated from service trigger schedule

The view enables you to do the following:

- Initiate manual backups
- Configure automated time triggered backups (7-, 30-, or 90-day)
- Download backup files (encrypted EDIST or unencrypted DIST)
- View the date when a backup was made
- View the size of a backup
- View which user created the backup (providing the backup was created manually)
- View backup notes
- View retention priority on backups (the “yes” value in the **Retain** column indicates a master backup which has a higher retention priority. The “no” value indicates a regular backup.)
- Delete a backup

Note: An unsuccessful Cloud backup does not raise an alarm. The job status is marked as failed (indicated in red on the **Cloud Backup Manager** view’s job bar at the top of the page).

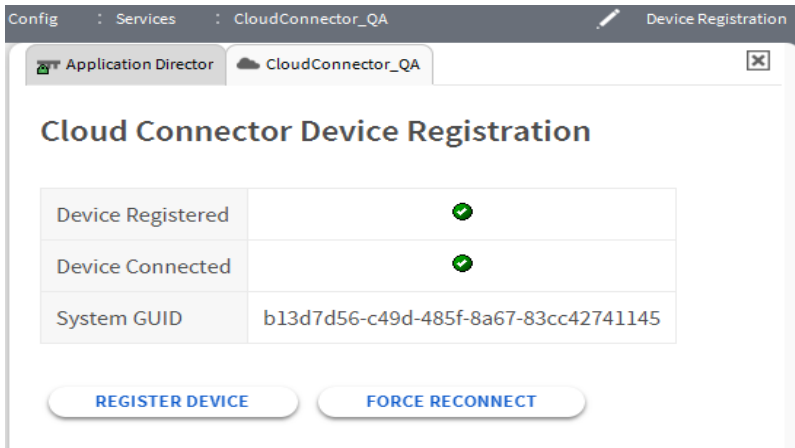
Parent topic: [Plugins](#)

Device Registration

Device Registration, is the default view for the Cloud Connector Service component. Double-clicking the component invokes this view which queries the device to determine if it is registered to access Niagara Cloud Services.

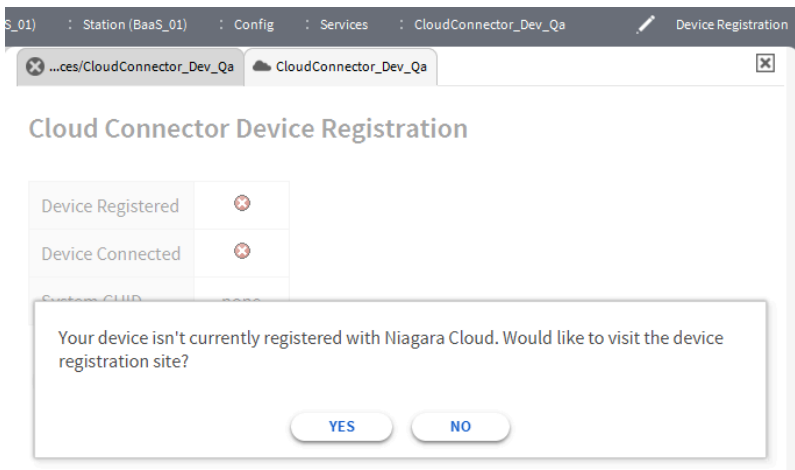
If the device is already registered, the view displays as shown here, indicating the device is both registered and connected to Niagara Cloud. Also listed is the assigned System GUID for the device. The System GUID is a unique identifier assigned during device registration, and is never changed.

Figure 1. View for a registered device



If the device is not registered, a notification message appears with a prompt that redirects you to **Device Registration** view in the Asset Manager tool in Niagara Community, as shown.

Figure 2. Notification that device is not registered



For more details see [Registering the device](#).

Parent topic: [Plugins](#)

Troubleshooting

This topic covers general issues that may occur during a backup to the cloud.

Failed backup

The exception, "Cannot connect to the cloud backup server," is visible in the **Cloud Backup Manager** view (and concurrently in the station output for the backup process) if the Niagara Cloud Backup Service becomes unavailable while a backup is occurring. Additionally, there is a "failed" status in the Job Bar for the backup, upon reconnecting to the cloud service.

Note: This type of failure in a production environment is a rare occurrence. Typically, you are informed ahead of time if the service will not be available.

Parent topic: [BaaS reference](#)

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

- [Asset Manager](#)
- [BaaS](#)
- [CSRF](#)
- [Device Manager](#)
- [GUID](#)
- [Niagara Cloud application](#)
- [Niagara Cloud Suite](#)
- [Niagara Community](#)
- [Organization Manager](#)
- [registered device](#)
- [SaaS](#)
- [the cloud](#)

Asset Manager

The Asset Manager tool is a web-based tool in Niagara Community which provides a means of managing users, organizations, and devices in preparation for interacting with any of the Niagara Cloud Suite. Additionally, the Asset Manager provides automated software maintenance management and notifications.

Parent topic: [Glossary](#)

BaaS

Backup as a Service (BaaS), the first cloud-based service provided by Niagara Cloud Services. provides seamless, secure, and scalable backups of the device from Niagara stations to the Niagara Cloud.

Parent topic: [Glossary](#)

CSRF

Cross-Site Request Forgery (CSRF) is a type of attack that occurs when a malicious web site, email, blog, instant message, or program causes a user's web browser to perform an unwanted action on a trusted site for which the user is currently authenticated.

Parent topic: [Glossary](#)

Device Manager

One of three roles (i.e. permission sets) which may be assigned to users of the Asset Manager tool. A Device Manager performs device management activities including adding devices, device registration, and device backup. May submit business affiliation requests.

Parent topic: [Glossary](#)

GUID

A globally unique identifier (GUID) is a system ID number assigned to a device during the device registration

process in the Asset Manager tool.

Parent topic: [Glossary](#)

Niagara Cloud application

This term refers to a web application that is running within the Tridium-provided Azure cloud space. A few examples are: Niagara Cloud Device Registration, Niagara Cloud Backup Service, and Niagara Cloud Device Details.

Parent topic: [Glossary](#)

Niagara Cloud Suite

Niagara Cloud Suite is a collection of user-facing (and some non-user-facing) web applications, running within the Tridium-provided Azure cloud space, providing a known set of service features.

Parent topic: [Glossary](#)

Niagara Community

Niagara Community is a portal for the cloud-based services and tools available at: *<http://www.niagara-community.com>*.

Parent topic: [Glossary](#)

Organization Manager

One of three roles (i.e. permission sets) which may be assigned to users of the Asset Manager tool. An Organization Manager performs both user and organization management activities. Adds users, assigns user role(s), adds organization affiliations, adds devices (single or multiple), provides approvals (affiliation and user) via notifications.

Parent topic: [Glossary](#)

registered device

This term refers to an embedded JACE controller registered with the Asset Manager tool and assigned a global identifier for purposes of tracking software maintenance management and authenticating with Niagara Cloud Suite.

Parent topic: [Glossary](#)

SaaS

The term "software as a service" (SaaS) is part of the nomenclature of cloud computing. SaaS is a software distribution model in which software is licensed on a subscription basis and is centrally hosted. It is sometimes referred to as "on-demand software". SaaS is typically accessed by users using a thin client via a web browser.

Parent topic: [Glossary](#)

the cloud

Simply put, the term refers to a type of Internet-based computing that provides shared computer processing resources and data to computers and other devices on demand. It is a model for enabling on-demand access to a shared pool of resources (e.g., computer networks, servers, storage, applications and services). Cloud computing and cloud storage solutions provide users and enterprises with capabilities to store and process their data in third-party data centers.

In traditional computing systems, users run software applications installed on a physical computer or corporate server. Cloud computing enables users to access the same kinds of applications through the Internet, paying a subscription fee for individual services, thereby paying only for what they use. If an organization quickly needs access to more resources, it can scale quickly in the cloud. If it needs to scale down resources, it can do so just as easily.

Parent topic: [Glossary](#)