

SIEMENS



Desigo Optic nHaystack Integration User Guide

Edition notice

Technical specifications and availability subject to change without notice.

This document may not be reproduced, disseminated to third parties or processed and its contents may not be used or disclosed without express permission. Non-compliance shall result in compensation for damages. All rights, including those resulting from a successful patent application and registration of a utility model or design patent, are reserved.

Edition: 2022-02-24

Document ID: A6V13129406_en--_a

© Siemens 2019-2022



Copyright

This document may be duplicated and distributed only with the express permission of Siemens, and may be passed only to authorized persons or companies with the required technical knowledge.

Table of Contents

1	Signing Siemens Modules	8
2	nHaystack	16
2.1	Install latest nHaystack module	16
2.2	Connect to your haystack connector	18
2.2.1	Crypto	19
2.3	Importing your database	20
2.3.1	Tag and clone template option	21
2.3.2	Clone and then tag option	21
2.3.3	Clone Points to Equip tool	23
2.3.4	Using the Clone Tool	24
2.4	Pull property tags	25
2.5	Remove broken refs	25
2.6	Rebuild cache	26
2.6.1	Rebuild cache through FIN	26
2.6.2	Rebuild cache through Niagara	27
3	nHaystack Troubleshooting	28
3.1	(Issue 1) 500: Internal Server Error (N3.8)	28
3.2	(Issue 2) 410: Gone (N4)	28
3.3	(Issue 3) "No suitable auth scheme for: 302 null" when attempting to connect to haystack (FIN v3.0.9 and N4)	29
3.4	(Issue 4) haystack::AuthErr: No suitable auth algorithm for: 302 (FIN v2.1.15 and AX)	29
3.5	Issue 5:	29
3.6	(Issue 6) sys::ParseErr: Unexpected token: eof [line 1]	29
3.7	(Issue 7) sys::IOErr: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed	30
3.8	(Issue 8) sys::IOErr: HTTP error code: 403" with N4.3 and patch 4.3.58.22.7	30
3.9	(Issue 9) sys::ParseErr: Invalid unit name 'in/wc' ["in/wc"] [line 41]	30
3.10	(Issue 10) "sys::Err: Authentication failed: 302" with AX or N4 with FIN v2.1.15	30
3.11	(Issue 11) "auth::AuthErr: Basic auth failed: 401 Authentication failed" with N4.2 or older with FIN v3.0+	31
3.12	(Issue 12) "haystack::AuthErr: Basic authentication failed [401]" with AX and FIN v2.1.15	31
3.13	(Issue 13) "auth::AuthErr: Basic auth failed: 401 Access denied" with AX and FIN v3.0+	31
3.14	(Issue 14) "auth::AuthErr: Basic auth failed: 302 Moved Temporarily" with AX and FIN v3.0+	31
3.15	(Issue 15) "sys::IOErr: Bad HTTP response 302 Found" with N4.2 HTTPS and FIN v2.1.15	32

3.16	(Issue 16) "haystack::AuthErr: Basic authentication failed [302]" with AX and FIN v2.1.15.....	32
3.17	Issue 17: "haystack::AuthErr: Basic auth failed: 401 Authentication failed" with custom haystack pod, N4.3, and FIN v2.1.15	32
3.18	Issue 18: "sys::IOErr: HTTP error code: 500" with custom haystack pod, AX, and FIN v2.1.15.....	32
3.19	Issue 19: "haystack::AuthErr: Basic authentication failed [500]" with AX and FIN v2.1.15.....	32
3.20	Issue 20: "haystack::AuthErr: 404 Not Found"	32
3.21	(Issue 21) "haystack::AuthErr: 403 Authentication failed." with N4 and FIN v2.1.15.....	33
3.22	Issue 22: "auth::AuthErr: 403 Authentication failed." sporadically with N4 and FIN.....	33
3.23	Issue 23: CPU usage is high, which sometimes causes points to go into fault for a few seconds	33



Cybersecurity disclaimer

Siemens provides a portfolio of products, solutions, systems and services that includes security functions that support the secure operation of plants, systems, machines and networks. In the field of Building Technologies, this includes building automation and control, fire safety, security management as well as physical security systems.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art security concept. Siemens' portfolio only forms one element of such a concept.

You are responsible for preventing unauthorized access to your plants, systems, machines and networks which should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. Additionally, Siemens' guidance on appropriate security measures should be taken into account. For additional information, please contact your Siemens sales representative or visit <https://www.siemens.com/global/en/home/company/topic-areas/future-of-manufacturing/industrial-security.html>.

Siemens' portfolio undergoes continuous development to make it more secure. Siemens strongly recommends that updates are applied as soon as they are available and that the latest versions are used. Use of versions that are no longer supported, and failure to apply the latest updates may increase your exposure to cyber threats. Siemens strongly recommends to comply with security advisories on the latest security threats, patches and other related measures, published, among others, under <https://www.siemens.com/cert/en/cert-security-advisories.htm>.

1 Signing Siemens Modules

Use this procedure for Niagara revisions 4.9 and above. For later versions up to 4.8 and Legacy AX 3.6 to 3.8u1, you are not required to use this procedure.

Creating a Self-Signed Code Signing Certificate

▷ In the Niagara Workbench:

1. Open **Tools** and click on **Certificate Management**.

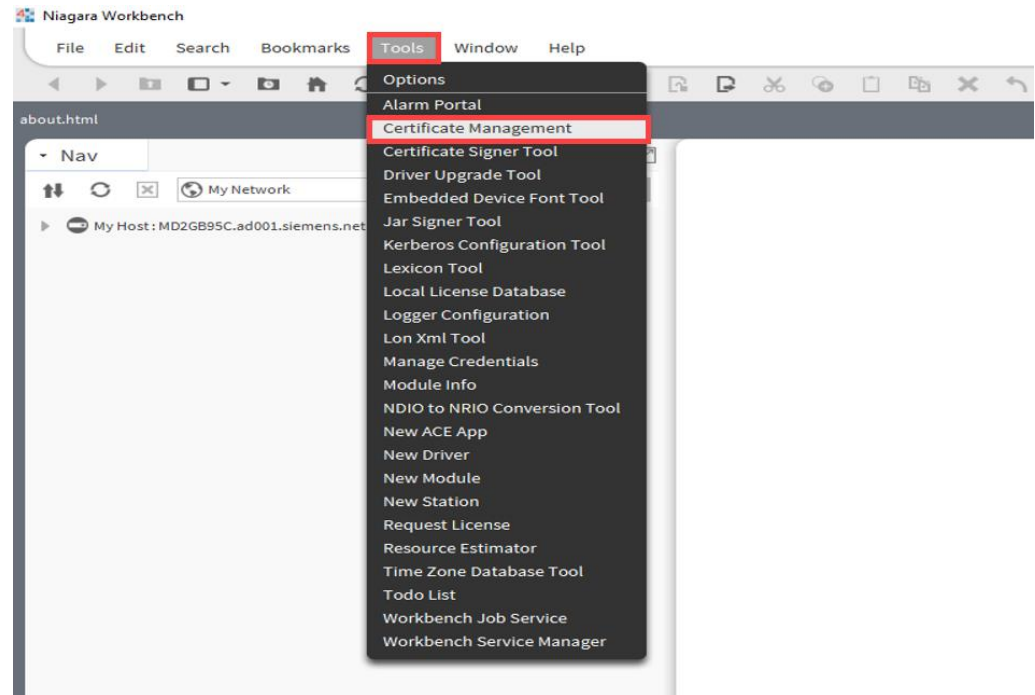


Fig. 1: Certificate Management in Tools



Certificate Management can also be found under **Platform**. Either Certificate Management can be used, but the public key must be imported into the Certificate Management's User Trust Store.

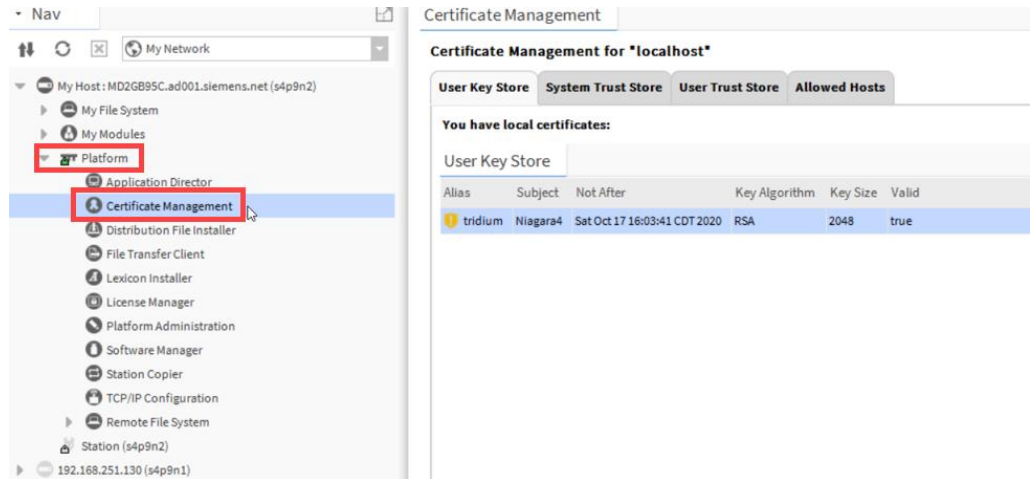
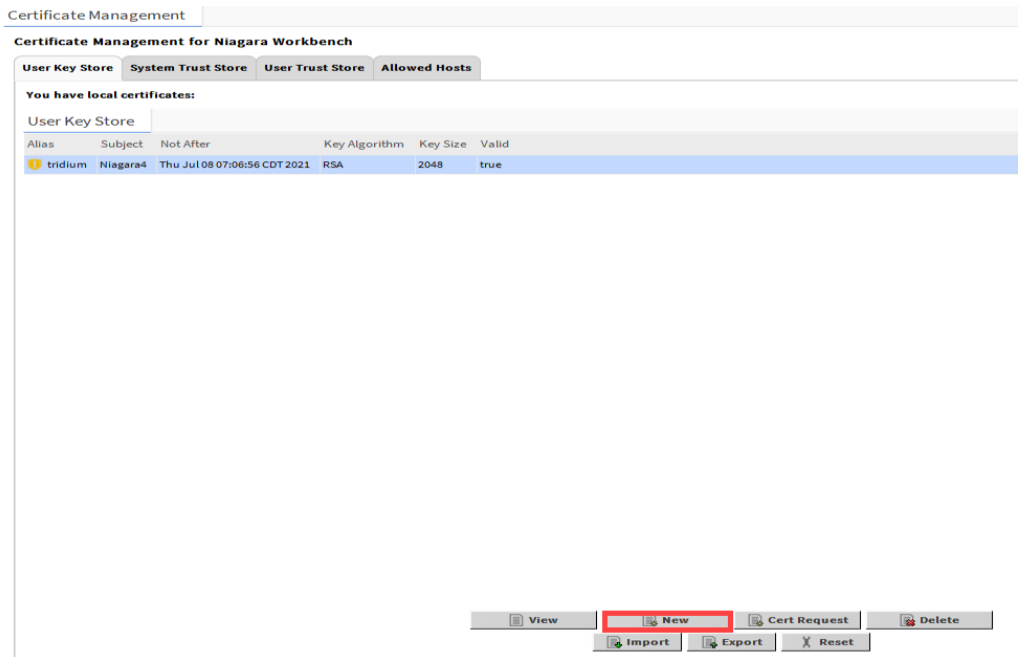


Fig. 2: Certificate Management in Platform

2. Click **New** to create a certificate.



3. In the dialog box, fill in **all** appropriate fields before proceeding. Click **OK**.

Generate Self Signed Certificate

Generate Self Signed Certificate
Generates a self signed certificate and inserts it into the keystore

Alias: MyCert (required)

Common Name (CN): MyCertificate (required)
* this may contain the host name or address of the server

Organizational Unit (OU): Your Organization Unit

Organization (O): Your Company (required)

Locality (L): Your Address

State/Province (ST): Your state

Country Code (C): us (required)

Not Before: 09-Jul-2020 03:52 PM CDT

Not After: 09-Jul-2021 03:52 PM CDT

Key Size: 1024 bits 2048 bits 3072 bits 4096 bits

Certificate Usage: Server Client CA Code Signing

Alternate Server Name:

Email Address: your@email

OK Cancel

4. In the next dialog box, create a password for the certificate. Click **OK**.

Generate Self Signed Certificate

Generate Self Signed Certificate
Generates a self signed certificate and inserts it into the keystore

Alias: MyCert (required)

Common Name (CN): MyCertificate (required)
* this may contain the host name or address of the server

Organizational Unit (OU):

Organization (O): (required)

Locality (L):

State/Province (ST):

Country Code (C):

Not Before:

Not After:

Key Size: 1024 bits 2048 bits 3072 bits 4096 bits

Certificate Usage: Server Client CA Code Signing

Alternate Server Name:

Email Address: your@email

OK Cancel

Private Key Password
Private Key Password

Private Key Password (required):

Password:

Confirm:

OK Cancel

5. Once created successfully, the certificate will be added in the **User Key Store**.

Certificate Management

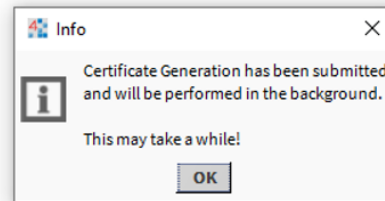
Certificate Management for Niagara Workbench

User Key Store System Trust Store User Trust Store Allowed Hosts

You have local certificates:

User Key Store

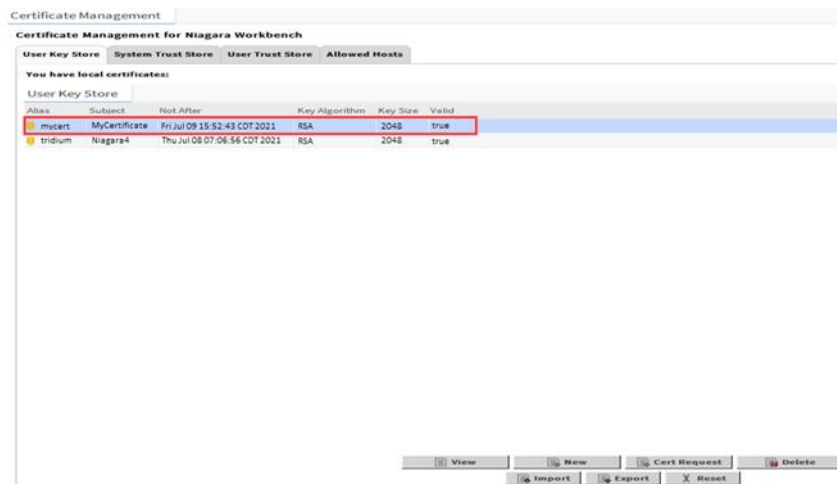
Alias	Subject	Not After	Key Algorithm	Key Size	Valid
mycert	MyCertificate	Fri Jul 09 15:52:43 CDT 2021	RSA	2048	true
tridium	Niagara4	Thu Jul 08 07:06:56 CDT 2021	RSA	2048	true



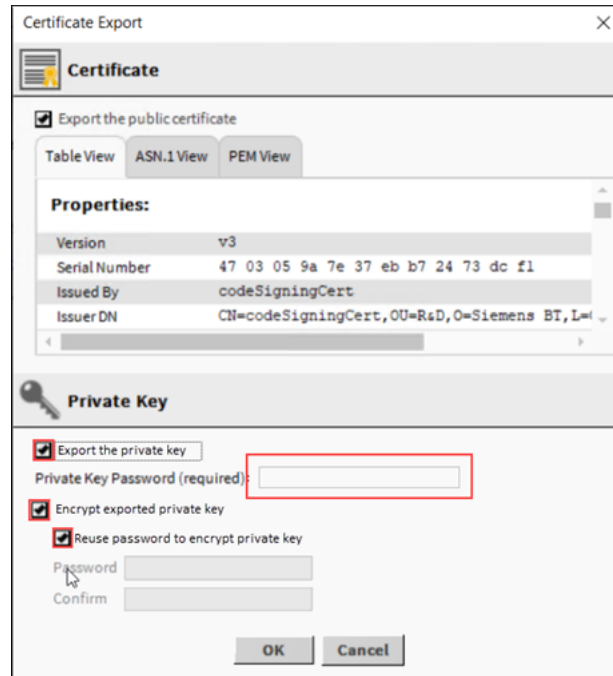
Exporting the Public Key and Importing into the User Trust Store

▷ You have created a self-signed code signing certificate. In the Niagara Workbench:

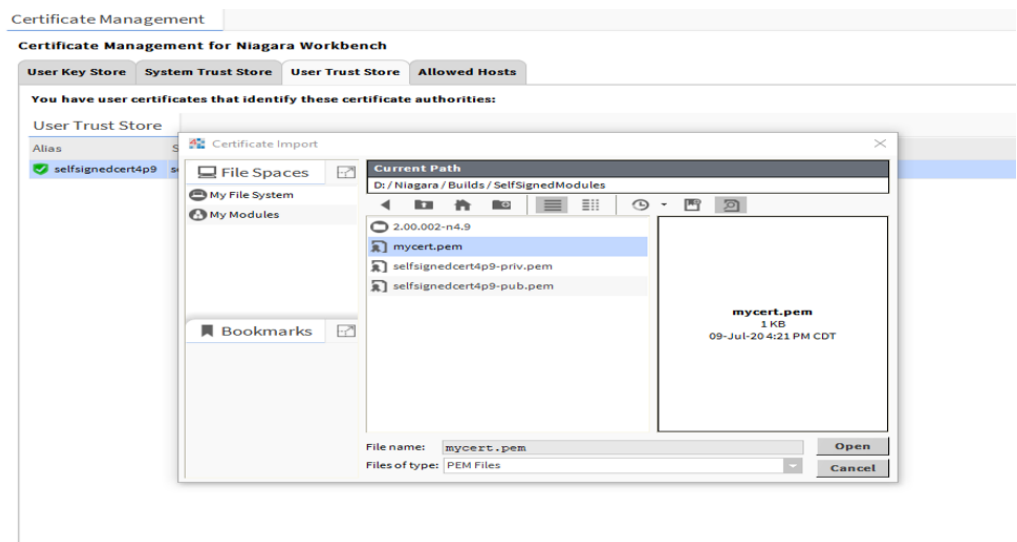
1. Click on the certificate in the **User Key Store** tab and click **Export**.



2. Check the box **Export the private key**. This will export the certificate.



3. Click **OK** and save the export. The N4.9 workbench will generate a .pem file.
4. Once the file is generated, import the .pem file into the **User Trust Store** using the Platform Certificate Management tool (Certificate Management under Platform).
5. In the **User Trust Store** tab, click **Import**.
6. Choose the .pem file created and click **Open**.



7. Click **OK**.
8. You should now see the public key added in the **User Trust Store**.

Certificate Management

Certificate Management for Niagara Workbench

User Key Store System Trust Store **User Trust Store** Allowed Hosts

You have user certificates that identify these certificate authorities:

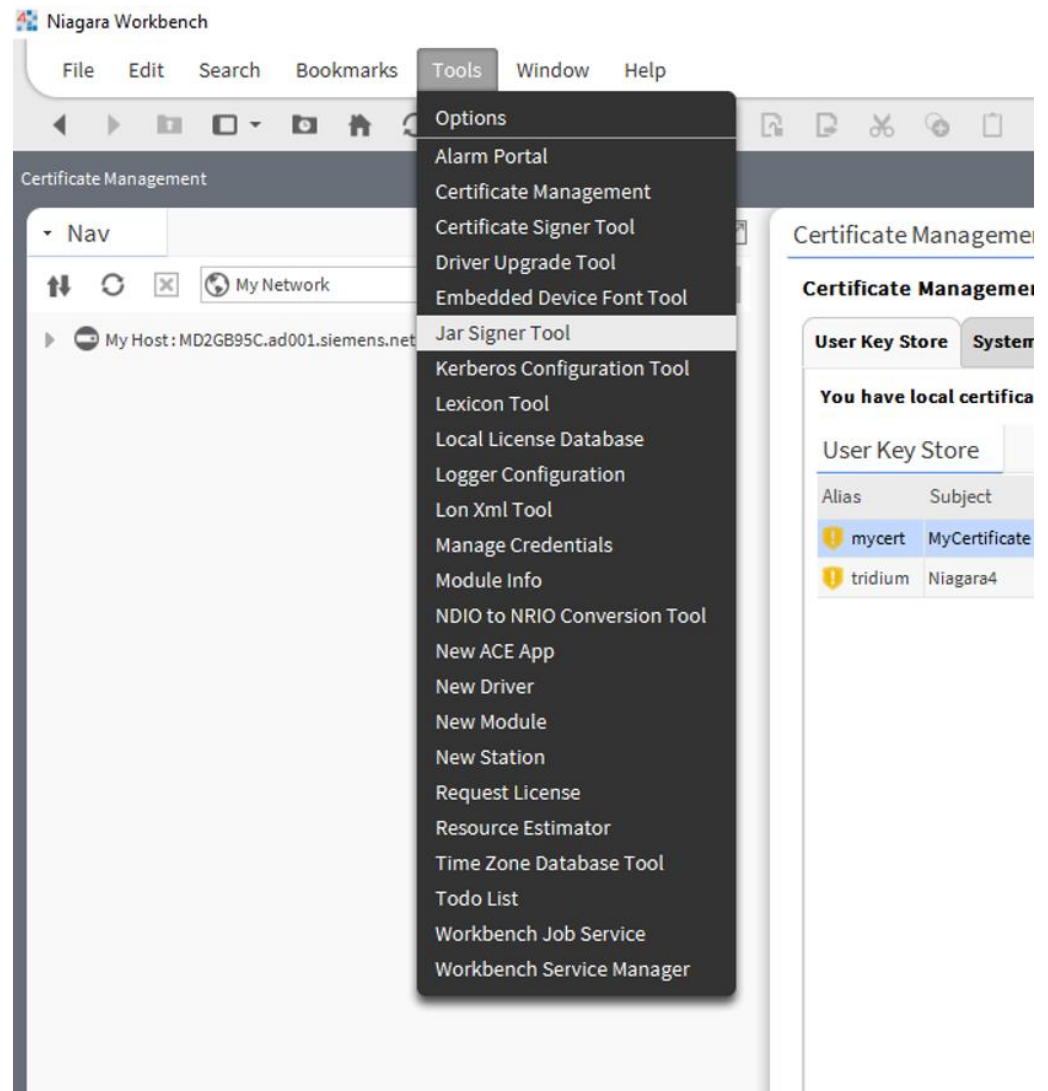
User Trust Store

Alias	Subject	Not After	Key Algorithm	Key Size	Valid
✓ mycertificate	MyCertificate	Fri Jul 09 15:53:43 CDT 2021			true
✓ selfsignedcert4p9	selfsignedcert4p9	Fri Jul 09 11:12:07 CDT 2021			true

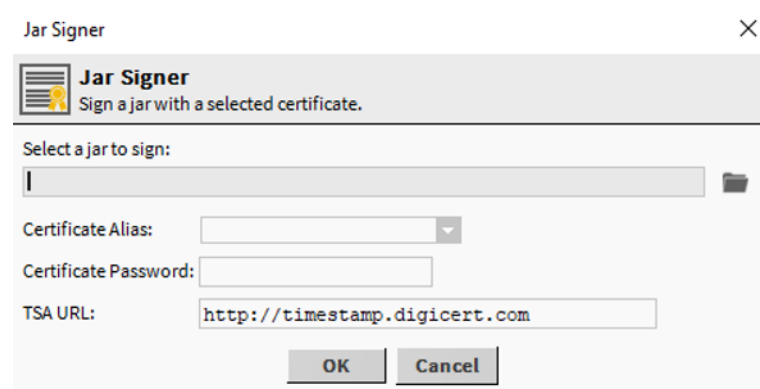
Using Jar Signer Tool to Sign Siemens Modules

- ▷ You have created a self-signed code signing certificate and exported the public key. In the Niagara Workbench

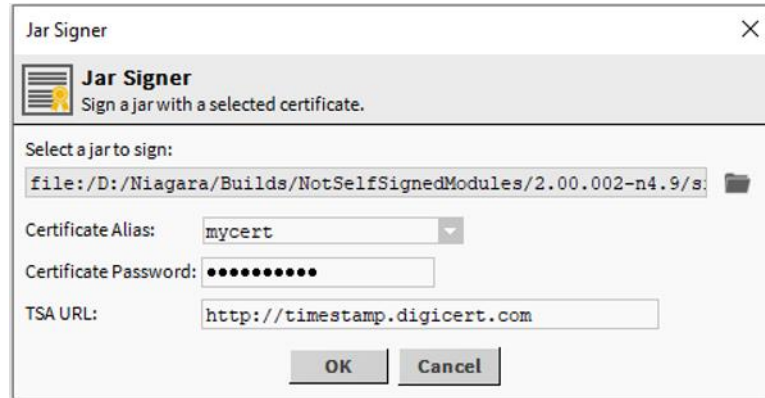
1. Open **Tools** and click on **Jar Signer Tool**.



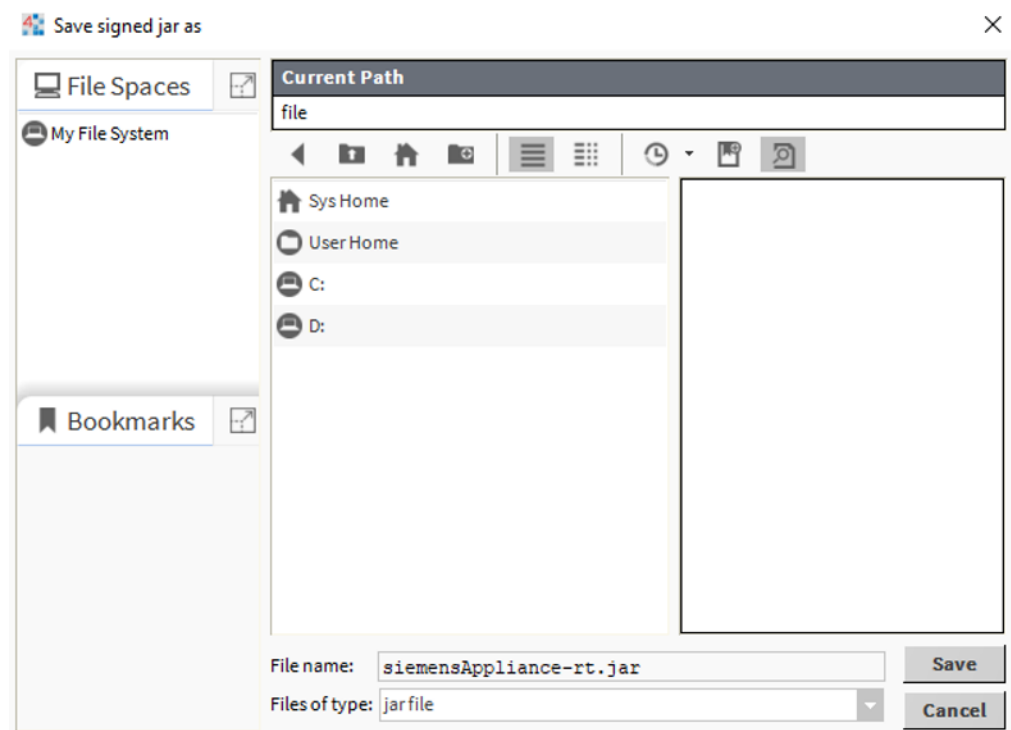
2. In the pop-up, select a Siemens module and the certificate that you created.



3. Enter the password and click **OK**.



4. Choose the desired location of your file and click **Save**.



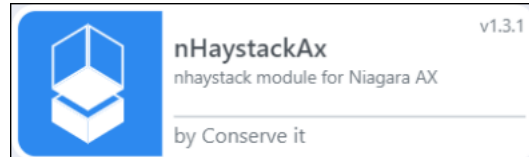
5. Repeat steps 1-4 to sign the rest of the Siemens Modules and the BACnet module.
6. Once module signing is completed, copy and paste the signed modules to the **modules** folder in the Niagara Workbench.

2 nHaystack

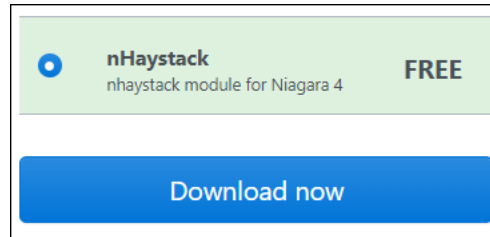
2.1 Install latest nHaystack module

Install the latest nHaystack jar modules to enable communication between FIN Stack and Niagara.

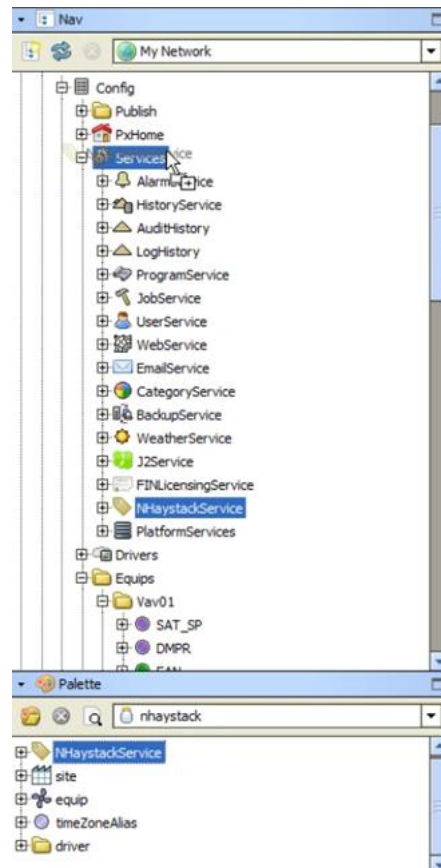
1. Download the latest nHaystack.jar module(s). Depending on what version of Niagara you have, you may need to download one or two modules.
 - **AX** - AX has one module nHaystack ([Download](#))



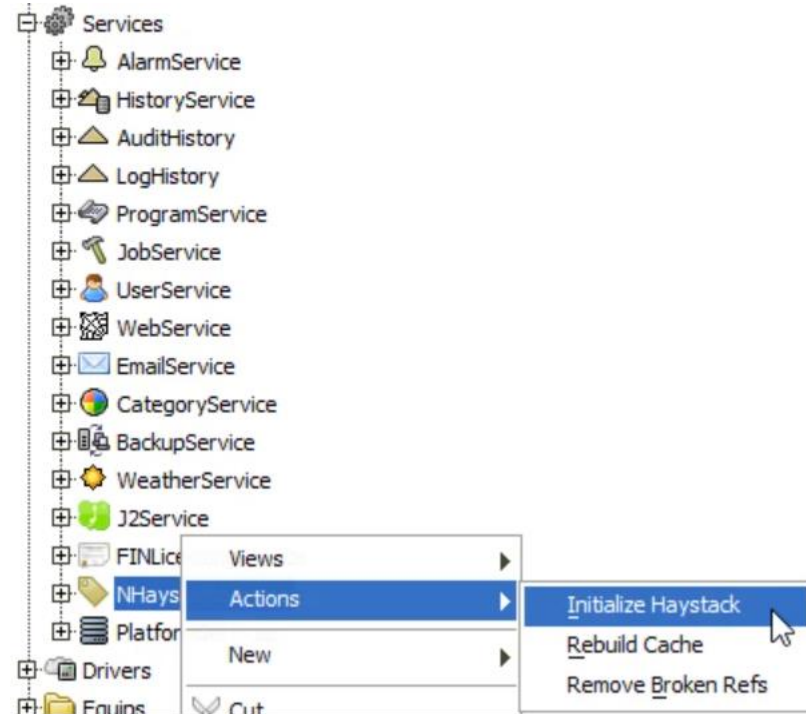
- **N4** - N4 has two modules nHaystack-rt and nHaystack-wb ([Download](#))



2. Drag the nHaystack.jar into your modules folder.
 - To add them, you may need to close your station.
3. In Niagara, drag the nHaystackService from the Palette to **Nav > Config > Service**



4. Restart your station.
5. After the restart is completed, reopen Niagara.
6. Right-click on the **nHaystackService > Actions**
7. Run each action individually:
 - **nHaystackService > Actions > Initialize Haystack**
 - **nHaystackService > Actions > Rebuild Cache**
 - **nHaystackService > Actions > Remove Broken Refs**



NOTICE



You can test the connection by typing `<niagaraStationIP>/haystack/about` into your browser.

Your browser should display the following message if your connection is successful.

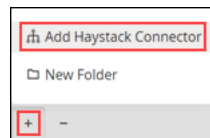


If you do not receive this message, see our page on how to troubleshoot Haystack.

2.2 Connect to your haystack connector

After installing the latest nHaystack module, use this procedure to connect to your haystack connector.

1. In the DB Builder, expand **Connectors > Haystack**.
2. Select or **+ > Add Haystack Connector** to add a new Haystack connection.



3. Enter your credentials:



URI	Enter the IP address that connects to the station. The URI scheme must be in the following format: http://host/haystack (Note: If you configured your station to use HTTPS, your URI must use HTTPS. You will get an error about a certificate if your host is not trusted. To trust your host, reference the Crypto page.)
Display Name	Name the connector.
(Optional) Haystack Slot	Default is set to No . Only select Yes if you will import points into your DB Builder. This is only applicable if dragging in data through the "Site" folder under haystack connector.
(Optional) Equip Filter	If haystack slot = Yes , filter equipment that is allowed to be imported.
(Optional) Point Filter	If haystack slot = Yes , filter points that are allowed to be imported.
Username and Password	Enter the same credentials used to log into the station.

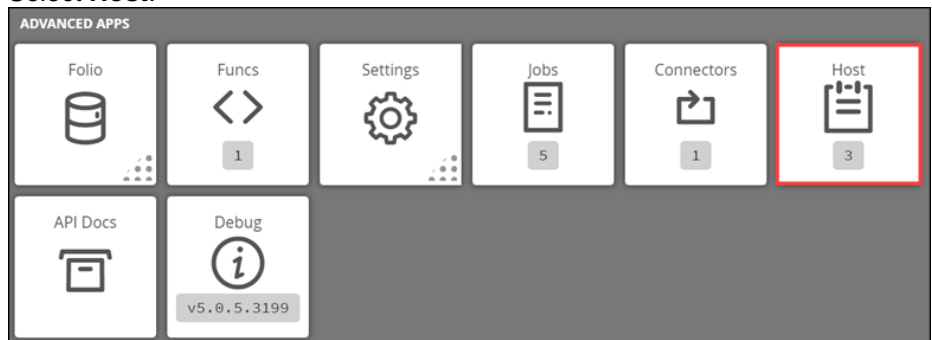
You will see the same structure that appears in Niagara through the Component Space.

If you have trouble connecting to the station, visit our nHaystack Troubleshooting guide for help.

2.2.1 Crypto

Use **Crypto** to view information about your trusted certificates. You can Trust, Rename, or Delete certificates. You can access **Crypto** in two ways.


1. Access **Crypto** from the home page.
 - Select  on the left-hand side of the screen.
2. Alternatively, you can access **Crypto** from within the host application.
 - Click .
 - Navigate to **Advanced Apps**.
 - Select **Host**.



- Select  on the left-hand side of the screen.

2.2.1.1 Trust


Use the following procedure to trust a certificate.

1. Click on the certificate you want to trust.
2. In the lower left corner of the work area, click .

3. The **Trust URI** window will appear.
 - **URI:** Type the **URI** into the text box. It should be in the following format:
https://host/
 - **Alias:** Name the trusted certificate.
 4. Press **Apply**.
- ⇒ After you press **Apply**, you will trigger an HTTPS handshake with the trusted device and capture the X.509 certificate information so you can trust the device in the future.


2.2.1.2 Rename

Use the following procedure to rename your certificate. You can also use this to decide if you want to keep or force the certificate.

1. Click on the certificate you want to trust.
2. In the lower left corner of the work area, click .
3. The **Rename Key** window will appear.
 - **New Name:** Enter a new name for the certificate.
 - **Keep:** Toggle no or yes
 - **Force:** Toggle no or yes.
4. Click **Apply**.

2.2.1.3 Delete

Use this procedure to delete a certificate.

1. Click on the certificate you want to delete.
2. In the bottom-right corner of the work area, click .
3. You will be asked to confirm that you want to delete the selected certificate.
 - Click **Yes** to delete the certificate.
 - Click **Cancel** to keep the certificate.

2.3 Importing your database


When you have successfully connected to your Haystack connector, you can import your data from Haystack to the software. After you import the data, you must decide when you want to tag your points.

1. You can tag and clone your data at the same time.
 - Tag and clone your data at the same time to create a perfected template to apply to other similar pieces of equipment. Use this option if you already know how you want to tag your equipment and points. You do not have to tag each point or equipment individually, but can add additional points later.
2. You can clone your data first and tag it later.
 - Clone your data first if you want to import your data right away but are not sure what tags you want to use. You might also use this option if you do not have time to create a perfected equipment to use as a template. With this option,

you can use the Advanced Tag Editor to create batches of tags to apply to your equipment when you are ready.


2.3.1 Tag and clone template option

Use this option to create a template with tags that can be applied to all similar types of equipment. For example, all VAV equipment will be tagged using the template you create in the DB Builder.

1. Create your **Site**, **Floor**, and **Equips** in the **DB Builder**.
2. In **Connectors**, expand **Haystack connector > Component Space > BacnetNetwork**.
3. Expand the equipment you want to tag and clone.
4. Expand **Points**.
5. Drag the points in the connector to the equipment you want to tag and clone in the **Equip Tree**.
6. Name the equipment in **DB Builder**.
7. Tag the points.
 - This will be your template to clone to the rest of the pieces of similar equipment.
 - Rename the points if necessary.
8. Select **Clone**  to apply this template to other similar pieces of equipment. (See **Clone** tool.)
9. Repeat this process for other types of equipment.





2.3.2 Clone and then tag option

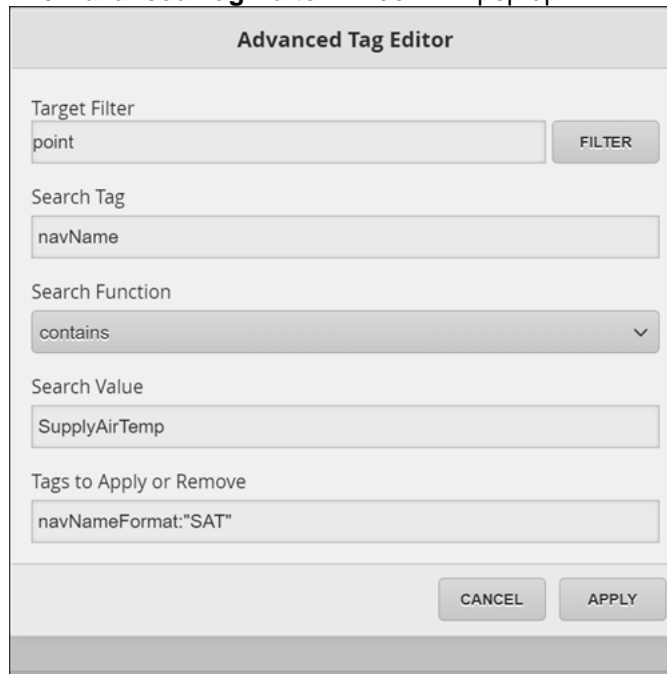
Use this option to clone equipment without adding tags. This option allows you to add your points into the database without creating tags. You can tag your equipment and add extra points later.

1. Create your **Site**, **Floor**, and **Equips** in the **DB Builder**.
2. In **Connectors**, expand **Haystack connector > Component Space > BacnetNetwork**.
3. Expand the equipment you want to clone.
4. Expand **Points**.
5. Drag the points in the connector to the equipment you want to clone in the **Equip Tree**.
6. Name the equipment in the **DB Builder**.
7. Rename points if necessary, but do not tag them.
8. Select the **Clone**  to clone the rest of your equipment. (See **Clone** tool.)
9. Repeat this process for other types of equipment.
10. When you are ready, use the **Advanced Tag Editor** to batch tag points.
11. If necessary, you can add extra points later.

2.3.2.1 Advanced Tag Editor

This tool allows you to add or remove custom tags such as markers and properties for database points. The points can be filtered by name, tag, and string value.




1. Select  > **Folio**  >  **Launch**
2. Select **Tools** 
3. In the **Tools** list, select **Advanced** > **Batch Tagging** > **Advanced Tag Editor**
4. The **Advanced Tag Editor** window will pop up.



- **Target Filter:** Filter tags to edit. "Point" will automatically populate in this box.
 - **Search Tag:** Search for specific tags. "navName" will automatically populate in this box.
 - **Search Function:** Choose one of three options to filter the search based on String Value: **contains**, **startsWith**, and **endsWith**.
 - **Search String Value:** Search for multiple values at the same time by separating main key words with **or**. You can also search for a single key word.
 - **Tags to Apply or Remove:** Enter tags that you want to add or remove. To remove tags, add - before the tag (e.g. "-vav"). Tags must start with a lower case letter. Separate tags with commas.
5. After you enter your desired values, click **Apply**.
 6. Click **OK** on the confirmation window will appear.
 - If you want the initial form to reopen to continue tagging, then select **Continue Tagging** before clicking **OK**.

2.3.3 Clone Points to Equip tool

The Clone Points to Equip tool allows the user to filter what points and tags are cloned to other Equips. You can use this to customize the points and tags that are applied to certain Equips.

1. Select  > **DB Builder** 
2. Expand the **Equip Tree**.
3. Select a site, floor, or equipment.
4. Click **Tools** 
5. Select **Batch Edit and Clone > Clone Points to Equip**.
6. The **Clone Points to Equip** window will appear. You must select the points and tags you want to clone and the equipment you want to clone them to.
 - **Select Points:** Allows the user to select or unselect all points found on the selected equipment.
 - **Select Points to Clone:** Displays all points. You can select points to clone or unselect points that you do not want to clone. Selections are highlighted in dark grey.
 - **Apply to All Markers:** Applies point selections to all **Marker Tags**. Uncheck this box if you do not want to clone the selected points to all **Marker Tags**.
 - **Marker Tags to Clone:** Displays all possible **Marker Tags** for the user to clone after points have been chosen.
 - **Apply to All Property Tags:** Applies point selections to all **Property Tags**. Uncheck this box if you do not want to clone the selected points to all **Property Tags**.
 - **Property Tags to Clone:** Displays all possible **Property Tags** for the user to clone after points have been chosen.
 - **Also Copy Points:** Allows the user to copy points that don't exist on the **Clone Points to Equip** tool.
 - **Filter for Equips to Modify:** Filter equipment types that you want to apply the above modifications to.

The image shows two sequential screenshots of the 'Clone Points To Equip' dialog box in a software application.

Top Screenshot:

- Title: Clone Points To Equip
- Section: Select Points (check this first)
 - Dropdown menu: none
- Section: Select Points to Clone (click to refresh)
 - List: OccCool, OccHeat, ReHeat Valve, Rm Humidity, Room Setpoint, Room Temp, SAT, UnOccCool, UnOccHeat
- Checkbox: Apply To All Markers
- Section: Marker Tags to Clone
 - List: air, cooling, heating, sp, temp, unocc, writable, zone
- Buttons: CANCEL, APPLY

Bottom Screenshot:



- Title: Clone Points To Equip
- Section: Marker Tags to Clone
 - List: air, cooling, heating, sp, temp, unocc, writable, zone
- Checkbox: Apply To All Property Tags
- Section: Property Tags to Clone
 - List: actions, disMacro, kind, maxVal, minVal, navName, precision, tz, unit
- Checkbox: Also Copy Points
- Section: Filter for Equipments to modify
 - Text input: equip and vav and heating
 - Button: FILTER
- Buttons: CANCEL, APPLY

- When the fields have been filled out, hit the **Apply** button for the changes to take effect.

2.3.4 Using the Clone Tool

Use the Clone tool to apply points and tags from one perfected piece of equipment to other types of similar equipment. You can use this template as many times as you want for that type of equipment.

- ▷ Create a piece of equipment that will be used as a template for your other pieces of equipment.

1. Select  > **DB Builder** 
 2. Navigate to the piece of equipment you want to clone. You can do this via the **Navigation Tree** or the **Equip Tree** and selecting the arrow to make it context.
 - All Equips and points must be tagged.
 - All points must be connected from the connector.
 3. Once the equipment has been selected, select **Connectors > Haystack**.
 4. Navigate to the Haystack connector.
 5. Select the parent folder that contains the equipment you want to clone.
 6. In the large pane on the right, select the equipments that the template will be applied to.
 7. Select **Clone**.
 8. The **Clone Options** window will appear.
 - **Equip to Use as a Template:** The equipment you set as context will automatically populate in this menu.
 - **Base URL:** Displays the location of the equipment that you want to clone. (This should be the same as the Equip to Use as Template.)
 9. Select **Create**.
- ⇒ You have successfully cloned your perfected Equip to other pieces of equipment. Repeat this process for other equipment that you want to clone.

2.4 Pull property tags

Use the Pull Property Tags function to update properties from Niagara to FIN. You can pull the following tags:

- Actions
- minVal
- maxVal
- Precision
- Unit
- Enum

Use this process to update FIN with property tags from your haystack connector.

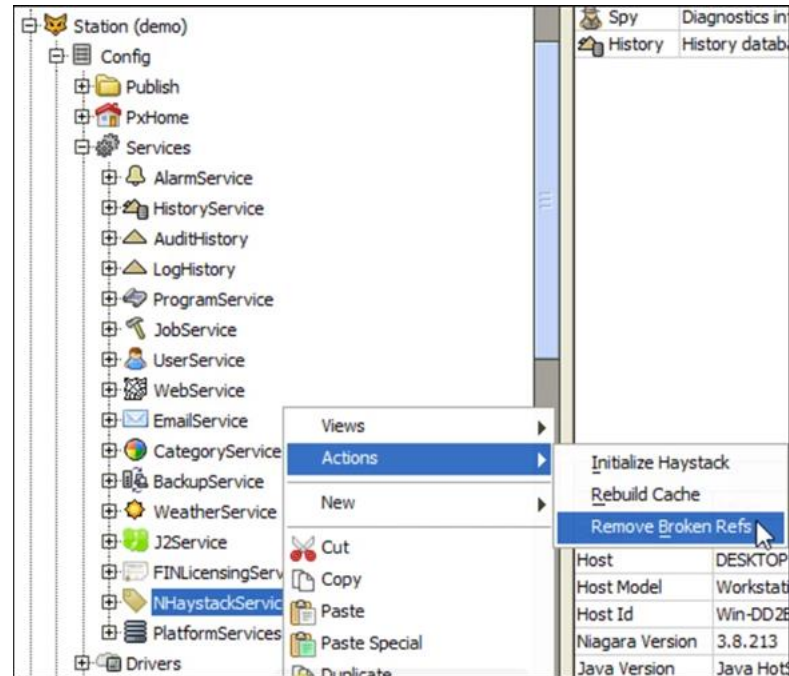
1. Select your connector and click on the Pull Property Tags tool.
2. Check the property tags you want to update.
3. Enter a filter to update your chosen property tags.
4. Click **Apply**.


2.5 Remove broken refs

When you are setting up relationships between references in a station, you might delete a component that references other components. As a result, you will receive an invalid **equipRef** error. To delete all invalid references, you can use the **removeBrokenRefs** action on **nHaystackService**. Every time you delete an invalid

reference, the log station will generate a message telling you what component was fixed. This can be executed in Niagara.

1. Open the Niagara workbench.
2. Open the Station.
3. Navigate to **Config > Services > nHaystackService**
4. Right-click on **nHaystackService > Actions > Remove Broken Refs**





5. Refresh  your connector in the **DB Builder**.

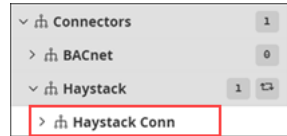
⇒ The log will generate a message about which component was fixed.


2.6 Rebuild cache

Adding or removing a Component or History causes a structural change to a station. Structural changes will invoke an action on the nHaystackService called rebuildCache. When this action is executed, the nHaystack Server traverses through the entire station and rebuilds all of its internal data structures so it can monitor interrelated components in the station. You can execute this action in FIN or Niagara.

2.6.1 Rebuild cache through FIN

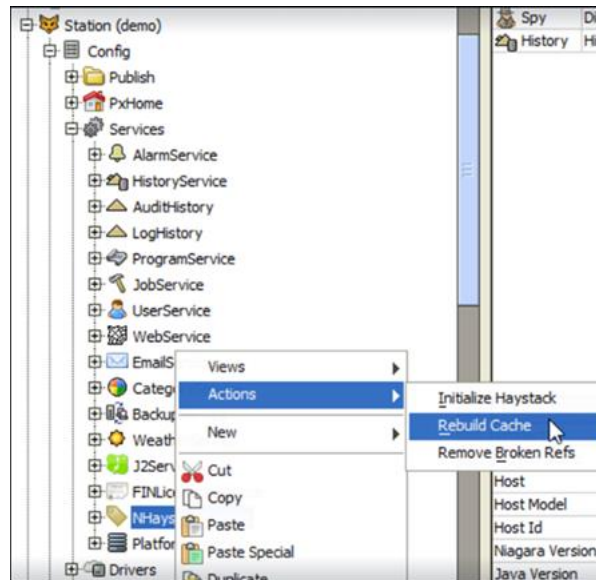
1. Click  > **DB Builder** 
2. In the **DB Builder**, expand **Connectors**.
3. Expand **Haystack**.
4. Select a Haystack Connector.




5. Click **Tools** 
6. In the **Tools** window, select **nHaystack > Rebuild cache > Apply**
7. Refresh  the connector.

2.6.2 Rebuild cache through Niagara

1. Open the Niagara workbench.
2. Open the Station.
3. Navigate to **Config > Services**
4. Select **nHaystackServices > Actions > Rebuild Cache**



5. In the **DB Builder**, refresh  the connector.

3 nHaystack Troubleshooting

3.1 (Issue 1) 500: Internal Server Error (N3.8)

You are connecting to your station through a web browser and get the following **500: Internal Server Error**.

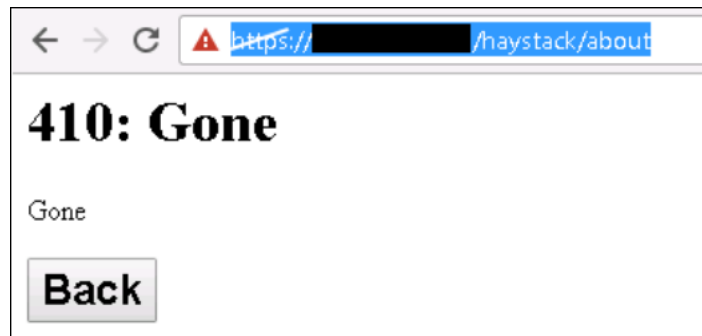


Use this procedure to resolve this error:

1. In JACE, go to your station and navigate to **Platform > Platform Administration > Set Module Filter to UI + Runtime**.
2. Restart your station.
3. Connect to your station through the web browser.

3.2 (Issue 2) 410: Gone (N4)

You are connecting to your station, haystack, or About and get the following **410: Gone** error.



Use this procedure to resolve the error.

1. In Niagara, navigate to **nHaystackService**.
2. Right-click on **nHaystackService** and execute the following actions:
 - **Initialize Haystack**
 - **Remove Broken Refs**
 - **Rebuild Cache**
3. Connect to your station through the web browser.

3.3 (Issue 3) "No suitable auth scheme for: 302 null" when attempting to connect to haystack (FIN v3.0.9 and N4)

You are connecting to N4 on FIN Stack V3.0.9 or later and get the following error: **No suitable auth scheme for: 302 null**. Use the following procedure to resolve this error:

1. In the N4 workbench, create a new user.
2. Set the user authentication to **Basic Authentication**.
3. In the Niagara Web Service, disable the **HTTPS** port.
⇒ You can now connect to N4 on FIN Stack.

3.4 (Issue 4) haystack::AuthErr: No suitable auth algorithm for: 302 (FIN v2.1.15 and AX)

Use the following procedure to resolve this error: **haystack::AuthErr: No suitable auth algorithm for: 302**.

HTTP

1. Ensure **HTTPS Only** is disabled
2. Set the **Authentication Scheme** to **Basic**.
3. Disable and re-enable the connector.

HTTPS

1. Set the **Authentication Scheme** to **Basic**.
2. Trust the HTTPS certificate on the **Crypto** page.

3.5 Issue 5:

3.6 (Issue 6) sys::ParseErr: Unexpected token: eof [line 1]

If you get a **sys::ParseErr: Unexpected token: eof** error, there may be unescaped spaces in the point paths. Use the following procedure to resolve the error:

1. In Niagara, navigate to **nHaystackService**.
2. Right-click on **nHaystackService** and execute the following actions:
 - **Initialize Haystack**
 - **Remove Broken Refs**
 - **Rebuild Cache**
3. Connect to your station through the web browser.

3.7 (Issue 7) sys::IOErr: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed

If you get a **sys::IOErr: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed** error, HTTPS is enabled on your station. Trust your certificate in Crypto to connect with HTTPS. Use this procedure to resolve this error:

1. In Crypto, click on the certificate you want to trust.
2. In the lower left corner of the work area, click .
3. The **Trust URI** window will appear.
 - **URI:** Type the **URI** into the text box. It should be in the following format:
https://host/
⇒ The URI must be configured as HTTPS.
 - **Alias:** Name the trusted certificate.
4. Press **Apply**.

3.8 (Issue 8) sys::IOErr: HTTP error code: 403" with N4.3 and patch 4.3.58.22.7

Change the **Authentication Scheme** on the user from **Basic** to **Digest**.

3.9 (Issue 9) sys::ParseErr: Invalid unit name 'in/wc' ["in/wc"] [line 41]

1. In a text editor, such as Notepad++, save a file as UTF-8.
2. Navigate to your FIN Stack directory.
3. Open the "units.txt" file in your director and add the unit on line 328.
 - The format of the line should be as follows: **inches_of_water, inH₂O; kg1*m-1*sec-2; 248.84.**
 - After applying the unit, the format of the line should be as follows: **inches_of_water, in/wc, inH₂O; kg1*m-1*sec-2; 248.84.**
4. Save the file and restart the FIN Stack service.

3.10 (Issue 10) "sys::Err: Authentication failed: 302" with AX or N4 with FIN v2.1.15

You might get this error with any version of N4.

1. N4.2 or older
 - Set your **Authentication Scheme** to **Digest**.
2. N4.3 or newer
 - Refer to troubleshooting Issue 5, "Can't connect to N4.3.58 using FIN v2.1.15".

NOTE: If you try logging through the browser to connect directly to the station and the **Authentication Scheme** is set to **Basic**, you will get an error that "User does not support logging in through this interface".

3.11 (Issue 11) "auth::AuthErr: Basic auth failed: 401 Authentication failed" with N4.2 or older with FIN v3.0+

There are two fixes for this error:

1. Set the authentication scheme to **Basic**.
2. Re-enter your credentials.
 - Verify your credentials are correct by connecting to the station via the browser.

3.12 (Issue 12) "haystack::AuthErr: Basic authentication failed [401]" with AX and FIN v2.1.15

This error occurs when credentials are entered incorrectly. To resolve the error:

- ◆ Re-enter your credentials.
 - Verify that your credentials are correct by connecting to the station via the browser.

3.13 (Issue 13) "auth::AuthErr: Basic auth failed: 401 Access denied" with AX and FIN v3.0+

This error occurs when credentials are entered incorrectly. To resolve the error:

- ◆ Re-enter your credentials.
 - Verify that your credentials are correct by connecting to the station via the browser.

3.14 (Issue 14) "auth::AuthErr: Basic auth failed: 302 Moved Temporarily" with AX and FIN v3.0+

This error occurs when credentials are entered incorrectly. To resolve the error:

- ◆ Re-enter your credentials.
 - Verify that your credentials are correct by connecting to the station via the browser.

3.15 (Issue 15) "sys::IOErr: Bad HTTP response 302 Found" with N4.2 HTTPS and FIN v2.1.15

This error occurs when credentials are entered incorrectly. To resolve the error:

- ◆ Re-enter your credentials.
 - Verify that your credentials are correct by connecting to the station via the browser.

3.16 (Issue 16) "haystack::AuthErr: Basic authentication failed [302]" with AX and FIN v2.1.15

This error occurs when credentials are entered incorrectly. To resolve the error:

- ◆ Re-enter your credentials.
 - Verify that your credentials are correct by connecting to the station via the browser.

3.17 Issue 17: "haystack::AuthErr: Basic auth failed: 401 Authentication failed" with custom haystack pod, N4.3, and FIN v2.1.15

Change the **Authentication Scheme** on the user to **Basic**.

3.18 Issue 18: "sys::IOErr: HTTP error code: 500" with custom haystack pod, AX, and FIN v2.1.15

This error occurs because Tridium does not let connect with anything older than N4. To resolve this error, contact Tridium.

3.19 Issue 19: "haystack::AuthErr: Basic authentication failed [500]" with AX and FIN v2.1.15

This error occurs when JACE is commissioned to use **runtimeOnly**. Commission JACE to use **runtime+UI**.

3.20 Issue 20: "haystack::AuthErr: 404 Not Found"

You get the following error: **haystack::AuthErr: 404 Not Found**. This happens when the URI scheme is in the wrong format. The URI scheme must have **haystack** appended to the host. For example, **http://10.10.10.100/haystack**.

3.21 (Issue 21) "haystack::AuthErr: 403 Authentication failed." with N4 and FIN v2.1.15

You log in and get the following error: **haystack::AuthErr: 403 Authentication failed**. There are two reasons that this may happen:

1. You did not enter the correct credentials.
2. The user does not exist in Niagara.

To resolve this error, re-enter your credentials or create a new user.

3.22 Issue 22: "auth::AuthErr: 403 Authentication failed." sporadically with N4 and FIN

To resolve this error, disable the user's auto-logout property.

3.23 Issue 23: CPU usage is high, which sometimes causes points to go into fault for a few seconds

Points may go into fault for a few seconds at a time if you are watching or using too many in a program. If you are not using too many points, the polling could be too frequent for the JACE. Use the following procedure to resolve this issue:

1. Add a number tag called **haystackPollFreq**.
2. Set the tag to 10-15 seconds. (The default setting is 1 second.)
3. Include the unit "s" for seconds when you set the value. For example, 10s.
4. Disable and then re-enable the connector.

Issued by
Siemens Industry, Inc.
Smart Infrastructure
1000 Deerfield Pkwy
Buffalo Grove IL 60089
+1 847-215-1000

© Siemens 2019-2022

Technical specifications and availability subject to change without notice.