Technical Document

E-Signature Application Guide

September 30, 2022

niagara4

E-Signature Application Guide

Tridium, Inc.
3951 Westerre Parkway, Suite 350
Richmond, Virginia 23233
U.S.A.

Confidentiality

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

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

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

Trademark notice

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

Copyright and patent notice

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

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

Contents

About this guide

This 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 the steps to configure the E-Signature service by securing the writable points for single and dual level authentication. It details how to install the module, set up the service. customer details can be modified and points can be secured in different zones for single as well as dual signature. The Alarm and History database maintenance views, and Protected Alarm Console allow for maintenance/acknowledgement only after authentication.

Document change log

Changes to this document are listed in this topic.

September 30, 2022

Initial release document.

Related documentation

Additional information on Niagara system, devices and protocols is available in the following documents.

- *Getting Started with Niagara*
- *Niagara Station Security Guide*
- *Niagara Graphics Guide*
- *Installation Qualification and Operational Qualification documents for Electronic Signature*
- *Electronic Signature API documentation*

Chapter 1 Overview

Topics covered in this chapter

♦ Supported architectures
♦ Software Modules
♦ Licensing

E-Signature is an add-on feature for the existing Niagara 4 Framework™. It provides a graphical environment for configuring and validating Niagara 4 applications in compliance with regulation 21 CFR Part 11. This Code of Federal Regulation is required by the US Food and Drug Administration to protect Electronic Records and E-Signatures.

This feature ensures that requested changes to writable secured data points (E-Signature or ESign Secured Points) require single or dual-level authentication and provides the following features:

- User and User Role configurations for authenticating and documenting change control.
- Customer information and Zone configuration of an E-Signature enabled project.
- Modeling the E-Signature secured points in a zone.
- Remote authentication at the second level of authentication for control point changes.
- A web API for executing authenticated changes to writable secured data points.
- Provides authentication for history and alarm database maintenance and alarm acknowledgement.
- Supports LDAP Authentication scheme along with Digest Authentication scheme.

Supported architectures

E-Signature supports any configuration where the Niagara 4 Framework is being used, because it is implemented by the Framework and has no outside dependencies.

In a stand-alone Supervisor, this service provides secured point protection and logging for local control points.

In an embedded controller (standalone JACE), the service protects and logs changes for local control points, excluding Edge10.

In a network of Supervisors and embedded controllers the service supports securing **NiagaraNetwork** proxied control points originating in a JACE and proxied to a Supervisor. This allows for scaling of the secured control point environment across an enterprise installation or multi-JACE local integration via the **NiagaraNetwork** protocol (FoxS). This architecture requires implementing network users in the Supervisor and JACE.

Software Modules

This topic explains the modules that need to be installed to run and execute the E-Signature application.

E-Signature depends on Java class files contained in four modules.

- electronicsignature-rt contains runtime class files and components.
- electronicsignature-ux contains PX binding for graphics.
- electronicsignature-wb contains Workbench client class files.
- electronicsignatureremote-rt supports securing the **NiagaraNetwork** proxy points.

Licensing

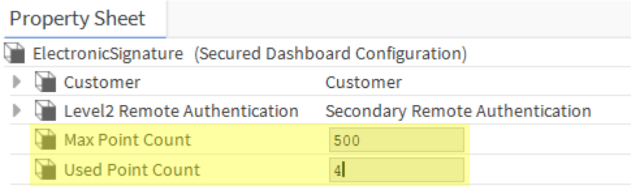
E-Signature is available for purchase as an add-on feature for Niagara Supervisors and JACE s through your Niagara 4 distributors.

The service checks for the presence of the E-Signature license feature in the host's license.

Only a host (Supervisor or JACE) where the original control points that are secured by an E-Signature, require the E-Signature license. A Supervisor station that has **NiagaraNetwork** proxied points from a JACE does not require an E-Signature license.

E-Signature is licensed with an associated Secured Point Limit. Actions executed on any secured control points beyond the host's licensed Secured Point Limit fail. The E-Signature in the station has a **Used Point Count** property that indicates how many Secured Points exist in the host.

The software updates the **Used Point Count** on station start.



Property Sheet

ElectronicSignature (Secured Dashboard Configuration)

Customer	Customer
Level2 Remote Authentication	Secondary Remote Authentication
Max Point Count	500
Used Point Count	4

Chapter 2 Deployment and setup

Topics covered in this chapter

♦ Module installation
♦ Workbench
♦ Opening a Platform Connection
♦ Creating a station
♦ Starting a Station
♦ Installing the service
♦ Modifying a Customer Details
♦ Setting up reasons and reason sets
♦ Creating a zone and adding points to it
♦ Setting up history Log
♦ User security
♦ Protected Alarm Console Recipient configuration
♦ PX graphic bindings

This chapter documents the details to install the module, set up a service, establish a secure connection, and add protected points for authentication.

Module installation

The standard Niagara workflow or procedure for installing other modules applies to the E-Signature modules.

- You can manually install them in a Supervisor station by copying the module files into the Niagara System home’s /modules folder followed by restarting the station.
- You can use the Platform connection’s Software Manager to install the modules into an embedded controller.
- You can use the Niagara Provisioning Service to install the modules into one or many remote JACE s at once, making it easy to deploy the software in a large installation.

Workbench

Workbench is the name for the framework’s graphical user interface. It allows users to connect and run a supervisor stations to perform physical operations and to create logical data in the visual form.

There are several ways to start Workbench.

You can start it from the Windows Start Menu:

- To start from the Start menu click All **Programs→Niagara 4.x.x.x→Workbench**.
- You can start it directly by running the Windows executable, or from the command line. The default path for the executable depends on your specific installation or software brand. For example: `C:\Niagara\Niagara-4.x.x.x\bin\wb.exe`.

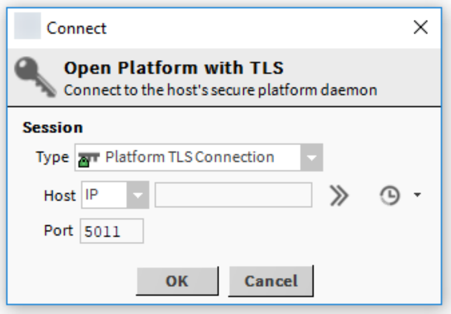
Opening a Platform Connection

A platform refers to a host that is running the Niagara deamon. It can be a Windows PC or a JACE. The platform connection interacts with the host to configure and manipulate station application(s).

Prerequisites: Workbench is installed on your PC and running.

Step 1 To open a platform connection, click **File→Open→Open Platform**.

The **Open Platfrom** window opens.



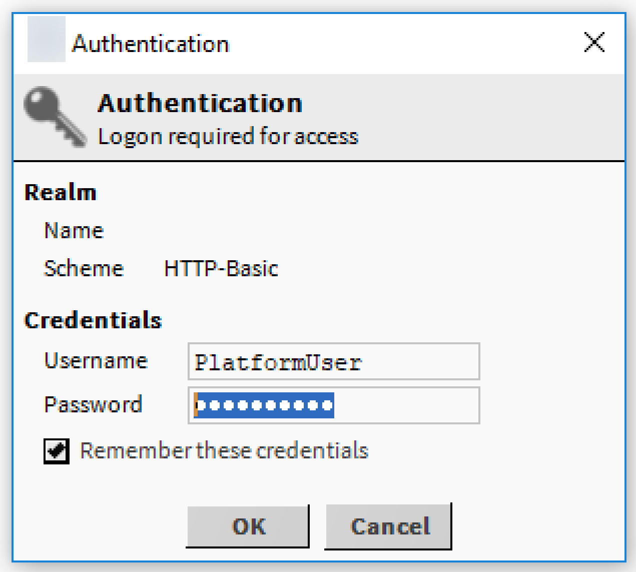
Type: Platform TLS Connection
Host: IP
Port: 5011

As shown above, the connection defaults to a secure **Type** `Platform TLS Connection`.

Step 2 Enter the host's `IP Address` and `Port` type, then click **OK**.

The default port is 5011 for secure platform connection.

The **Authentication** window opens and prompts for platform credentials.



Name
Scheme: HTTP-Basic
Username: PlatformUser
Password: ●●●●●●●●●●
☑ Remember these credentials

Step 3 Enter the platform credentials, select the **Remember these credentials**, and click **OK**.

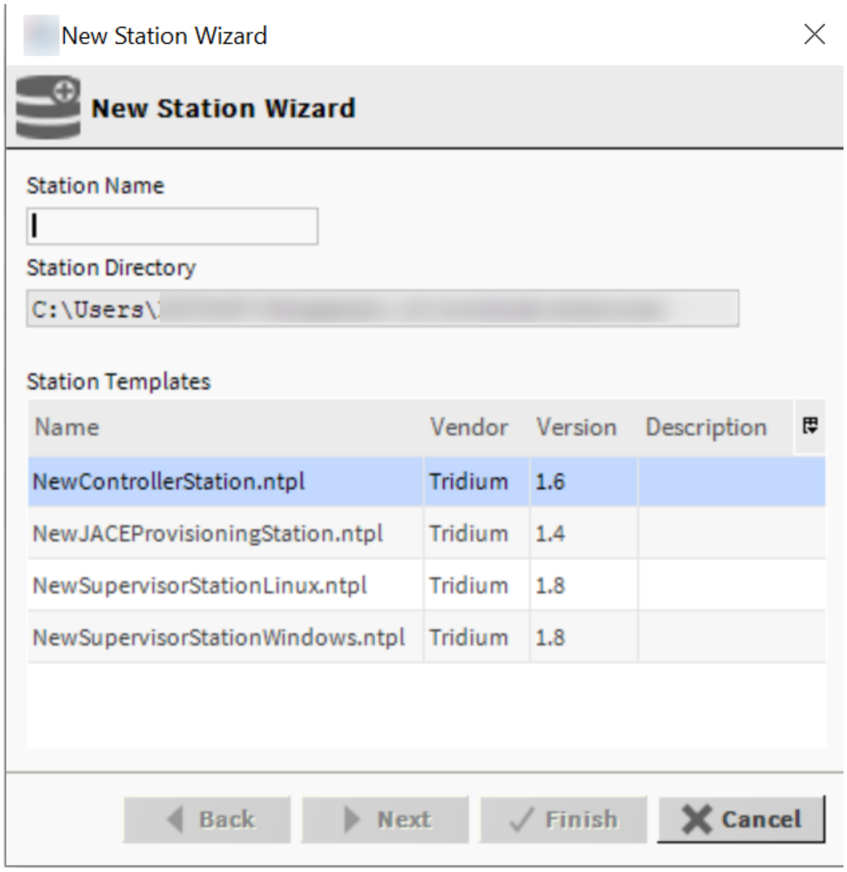
Creating a station

Use the **New Station** tool from the **Tools** menu to create a new Supervisor station. The new station is automatically configured with appropriate services.

Prerequisites: You are working inWorkbench running on a PC

Step 1 In Workbench, select **Tools→New Station**.

The **New Station Wizard** opens.



Station Name

Station Directory

C:\Users\[redacted]

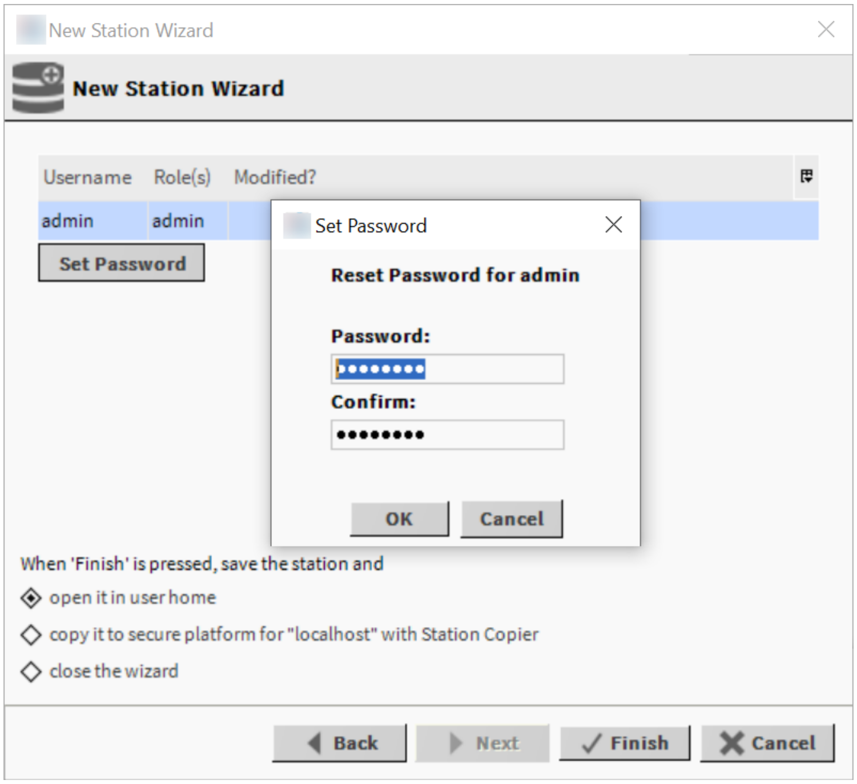
Station Templates

Name	Vendor	Version	Description
NewControllerStation.ntpl	Tridium	1.6	
NewJACEProvisioningStation.ntpl	Tridium	1.4	
NewSupervisorStationLinux.ntpl	Tridium	1.8	
NewSupervisorStationWindows.ntpl	Tridium	1.8	

Step 2 Enter the `Station Name`, select a `Station Template` and click **Next**.

The **`station name`** is case sensitive and starts with a letter. The station should be installed, based on the type of the host the template should be selected.

It creates a station name and password wizard opens.



Username	Role(s)	Modified?
admin	admin	

Set Password

Reset Password for admin

Password: ••••••••

Confirm: ••••••••

When 'Finish' is pressed, save the station and

◈ open it in user home

◇ copy it to secure platform for "localhost" with Station Copier

◇ close the wizard

Step 3 To set the password, click **Set Password** and click **OK**.

Your password must contain at least 10 characters, one digit, one uppercase character and one lowercase character.

Step 4 Select the **Copy it to secure platform for localhost with station copier** or by default the station option is `open it in user home` and click **Finish.**

The **Transferring Station** window opens.

Step 5 To continue transfer, click **Next**, followed by clicking **Finish**.

The wizard asks if you want to open the **Application Director**.

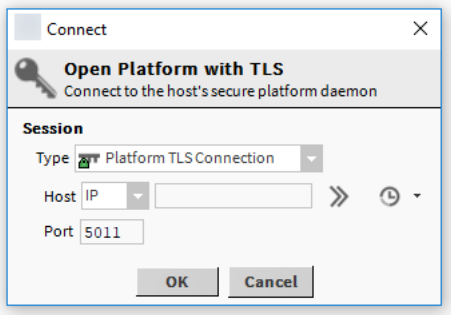
Step 6 Click **Yes** to continue.

Starting a Station

A station must be running before it can be opened and accessed.

Step 1 To start a station, click **File→Open→Open Platform**

The **Connect** window opens.



Open Platform with TLS

Connect to the host's secure platform daemon

Session

Type: Platform TLS Connection

Host: IP

Port: 5011

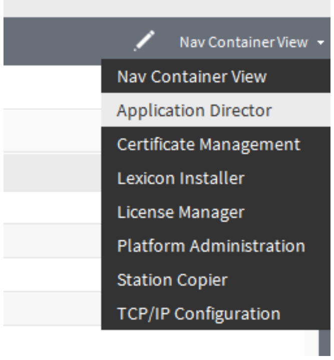
Step 2 Enter the host **IP Address**. and click **OK**.

For local machine platform the host is `localhost`.

The **Nav Container View** opens.

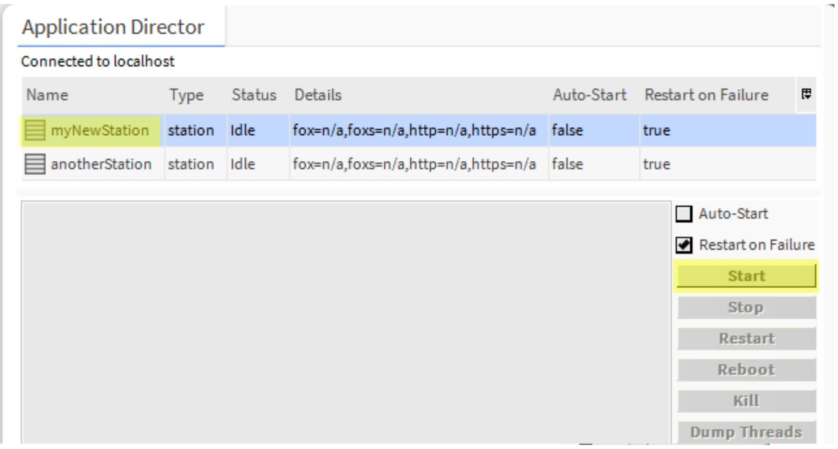
Step 3 To open the **Application Director** do the following.

- In the **Nav Container View**, double-click the **Application Director**.
- In the top upper left corner, click drop-down menu and click **Application Director**.



The **ApplicationDirector** view opens.

Step 4 In the **ApplicationDirector** view, select the station and click **Start** to run the station.



Connected to localhost

Name	Type	Status	Details	Auto-Start	Restart on Failure
myNewStation	station	Idle	fox=n/a,foxs=n/a,http=n/a,https=n/a	false	true
anotherStation	station	Idle	fox=n/a,foxs=n/a,http=n/a,https=n/a	false	true

☐ Auto-Start

☑ Restart on Failure

Installing the service

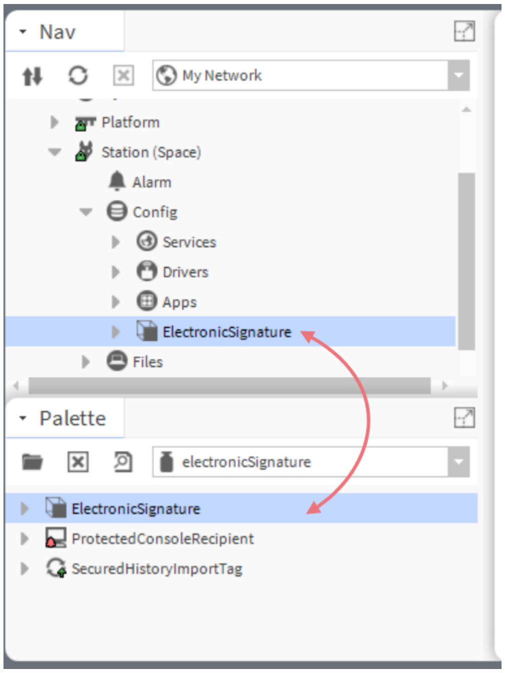
This topic explains how to open the palette and add the **`ElectronicSignature`** component to the **Config** space of the connected station.

Step 1 To open palette, click **Windows→SideBars** and click **Palette.**

The palette side bar appears in the side bar pane.

Step 2 Click 📁 icon to open the palette and select the **`ElectronicSignature`** module in the filter and click **OK**.

The **ElectronicSignature** modules are appears in the palette.



Step 3 Drag the **ElectronicSignature** component directly onto the **Config** space of a Niagara station.

Adding the **ElectronicSignature** component to the station is required in stations that have locally secured points, but also required in a Supervisor station that will proxy those points through the **Niagara Network**. The component is required so that Users who are logged in to the Supervisor can modify the proxied signed points.

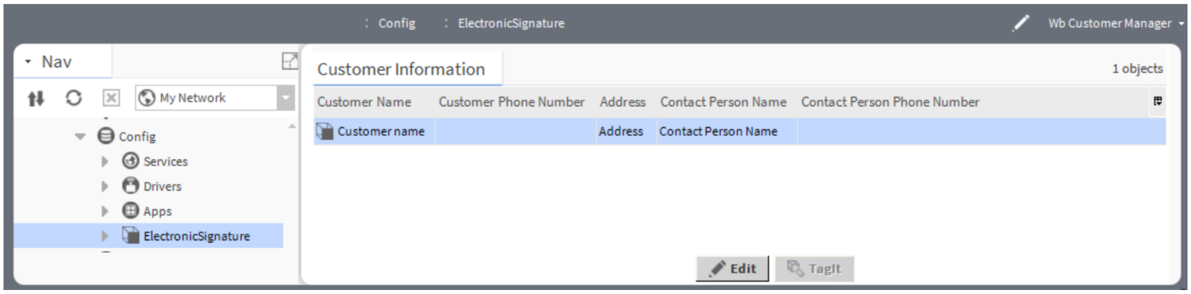
If the Niagara Supervisor station has local (non-Niagara Network proxy) points that need to be signed points, it requires the application to be installed and configured locally. The **Electronic-Signature** component is installed directly under the **Config** container of the station.

Modifying a Customer Details

This topic explains how to modify customer information using the **Wb Customer Manager** view.

Step 1 To modify a customer, right click the **ElectronicSignature** component and select **Wb Customer Manager**.

The **Wb Customer Manager** window opens.

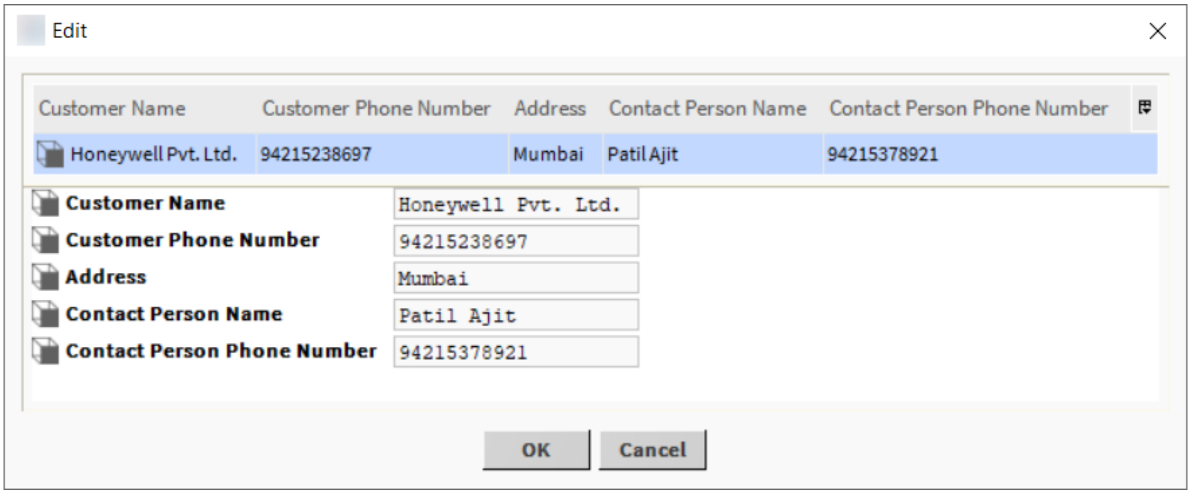


Customer Information

1 objects

Customer Name	Customer Phone Number	Address	Contact Person Name	Contact Person Phone Number
Customer name		Address	Contact Person Name	

Step 2 Select the customer and click **Edit**.



Customer Name	Customer Phone Number	Address	Contact Person Name	Contact Person Phone Number
Honeywell Pvt. Ltd.	94215238697	Mumbai	Patil Ajit	94215378921

Customer Name	Honeywell Pvt. Ltd.
Customer Phone Number	94215238697
Address	Mumbai
Contact Person Name	Patil Ajit
Contact Person Phone Number	94215378921

Step 3 In the window, enter the customer information:

- **Customer Name**
- **Customer Phone Number**
- **Address**
- **Contact Person Name**
- **Contact Person Phone Number**

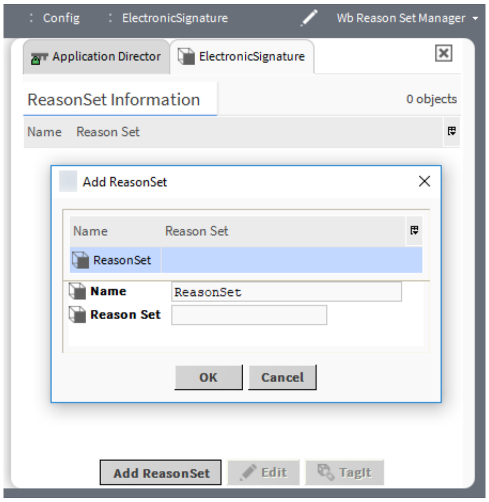
Step 4 Enter the customer information and click **OK** to save the changes.

Setting up reasons and reason sets

This topic describes configuring the reasons and reason sets for changing control points protected by the electronic signature service. You must indicate a reason for the change and why it is necessary, and the reasons are most repetitive. The service provides a feature that allows users to provide predefined reasons and organize them into sets called ReasonSets.

Step 1 To configure the reason, expand **Config→ElectronicSignature** and navigate to **Wb Reason Set Manager**.

The **Wb Reason Set Manager** view opens. You can add reasons sets in the **ReasonSet information**.



Name	Reason Set
ReasonSet	

Name	ReasonSet
Reason Set	

Step 2 To add the reason sets, click **Add ReasonSet**.

The **Add ReasonSet** window opens.

Step 3 In the **Add ReasonSet**, enter the following information and click **OK**.

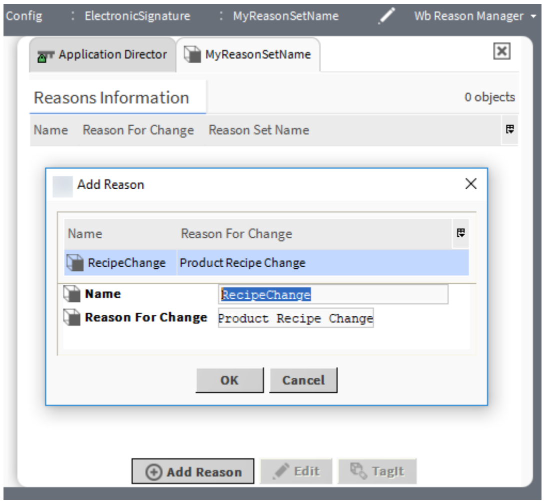
a. **Name**

b. **ReasonSet**

It adds a new **ReasonSets** in the **ReasonSet information**.

Step 4 Double-click on a **ReasonSet**.

The **Wb Reason Manager** view opens. You can add reasons to the reason sets.



Name	Reason For Change
RecipeChange	Product Recipe Change

Name: RecipeChange

Reason For Change: Product Recipe Change

Step 5 To add reasons, click **Add Reason**.

The **Add Reason** window opens.

Step 6 In the **Add Reason** window, enter the following information and click **OK**.

a. **Name**

b. **Reason For Change**

It adds a new reason for the selected reason set.

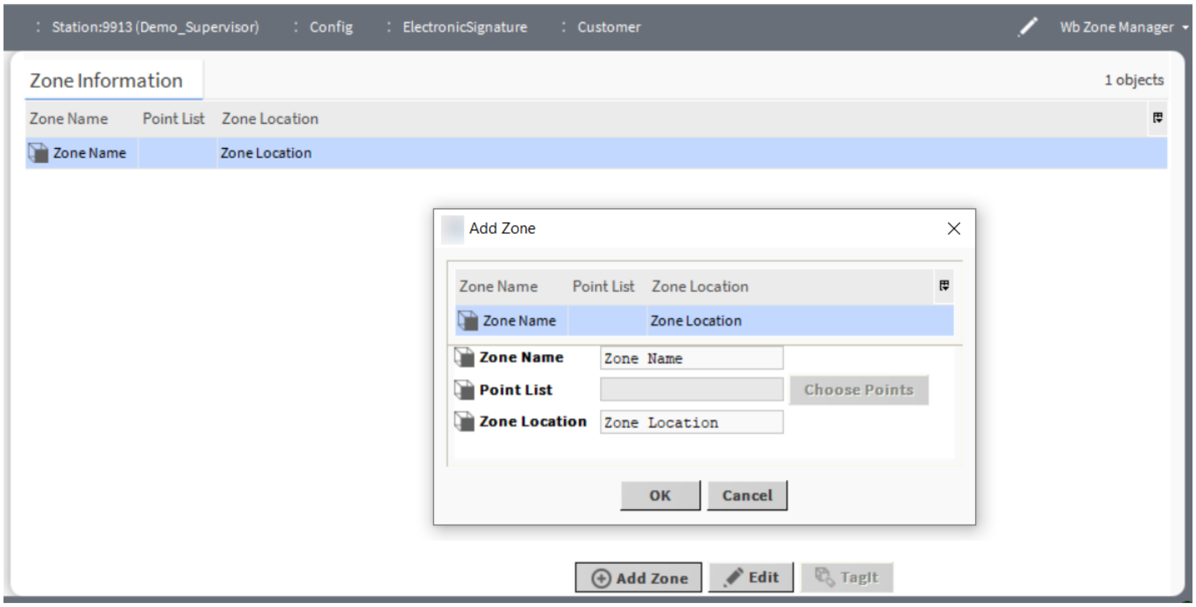
Creating a zone and adding points to it

This topic explains how to create a zone information for a customer and how to secure the points using **Point Chooser** dialog box.

Step 1 To create a zone, expand **Config→ElectronicSignature** and double-click on **Customer**.

The **Wb Zone Manager** view opens. The view displays the zone for the customer.

Step 2 To edit the zone information, double-click the **Zone** or select the zone and click **Edit**.



Zone Name	Point List	Zone Location
Zone Name		Zone Location

Zone Name: Zone Name
Point List:
Zone Location: Zone Location

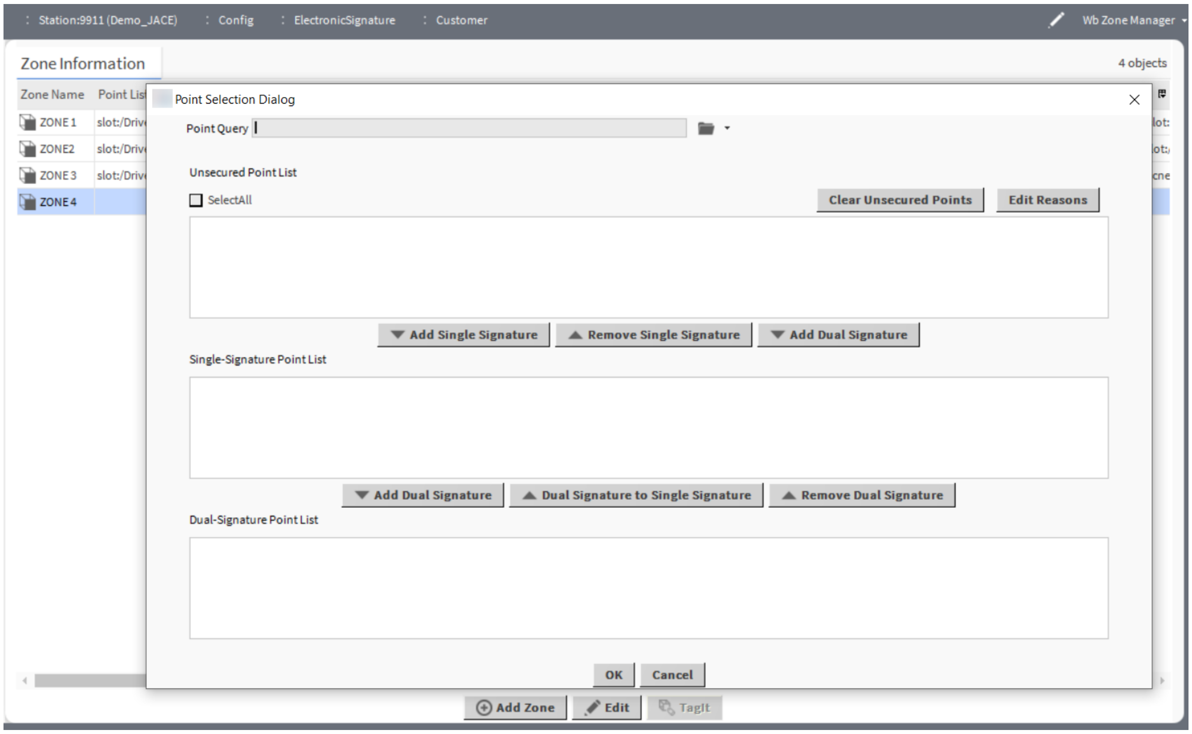
Step 3 In the **Edit** window, enter the following information.

a. **Zone Name**

b. **Zone Location**

Step 4 To secure the control points in the **Point List** , click **Choose points** in the zone.

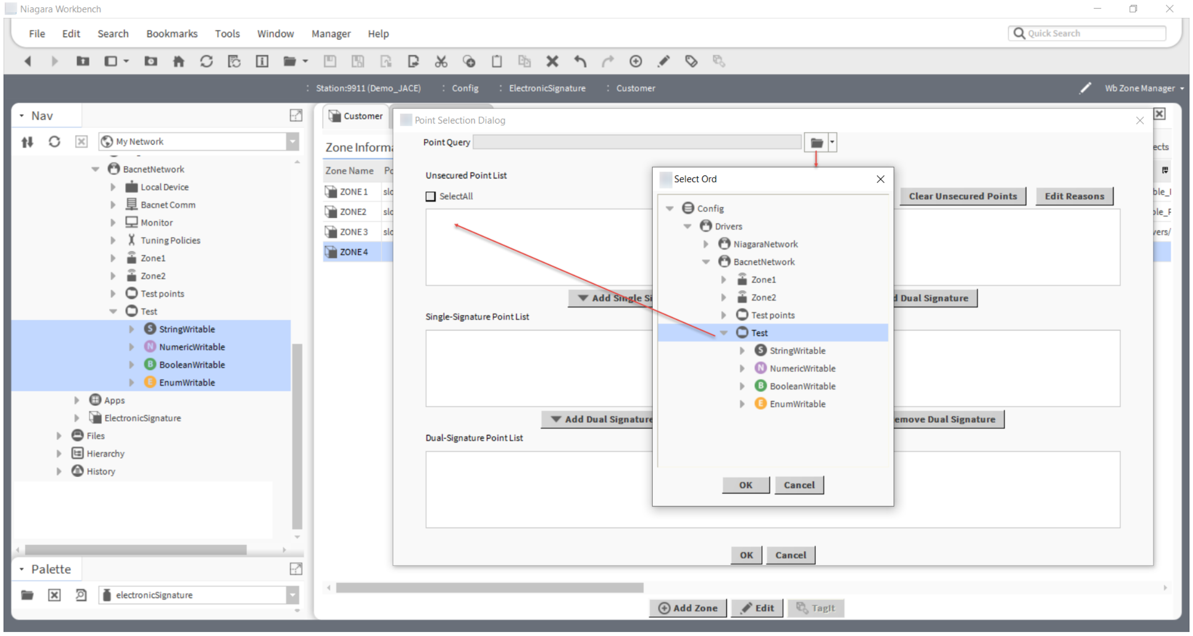
The **Point Selection Dialog** window opens. The **Point query** allows the user to select an object from the Niagara Station that contains the control points to be secured.



Zone Name	Point Lis
ZONE 1	slot:/Driv
ZONE2	slot:/Driv
ZONE 3	slot:/Driv
ZONE 4	

Step 5 To open the points chooser, click the down arrow next to the folder icon in the **Point Query** type.

The **Select ord** window opens.



Step 6 Select the query from the **Select Ord** window and click **OK**.

NOTE: Navigate to the component to be searched for unsecured points. The secured points chooser will only return unsecured control points as part of its query. It will also not return any **Niagara Network** proxy points, as those points should be secured in the originating Niagara Station.

The query is added in the **Point Query**. Once the query is added, the unsecured points are displayed in the **Unsecured Point list** and can be added to the **Single-Signature Point List**.

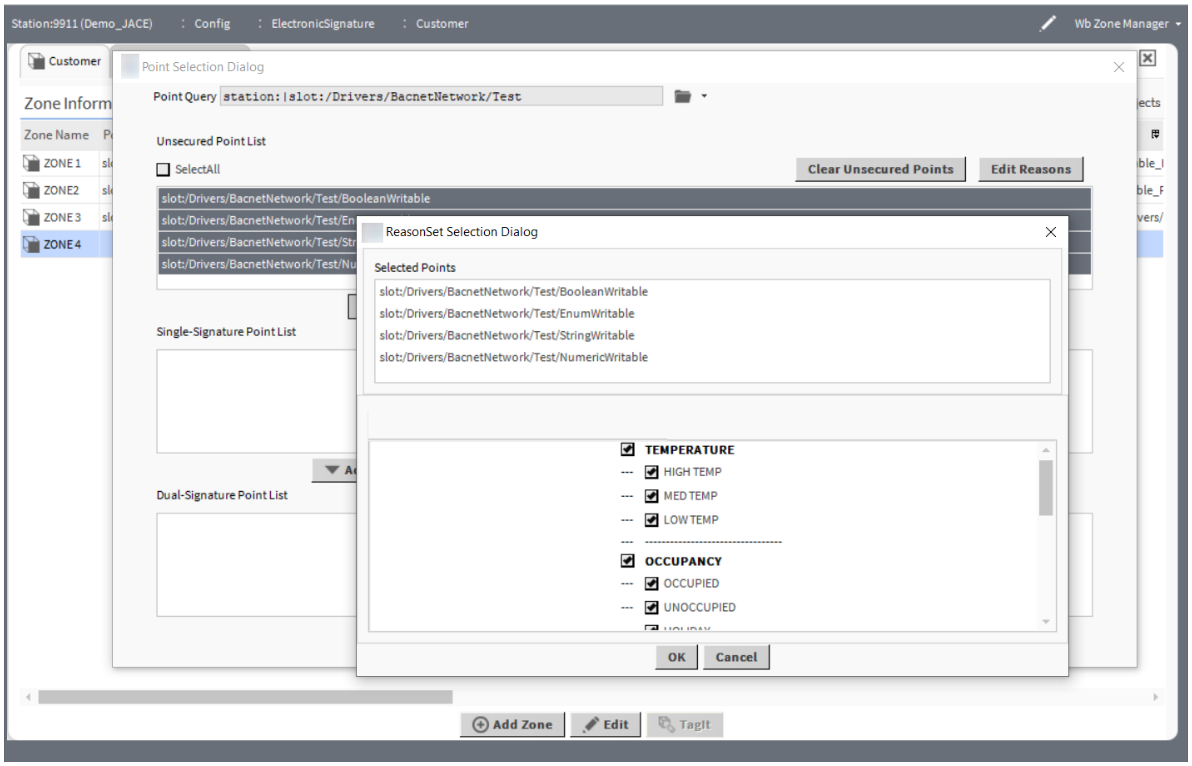
Step 7 To add the unsecured points in the **Single-Signature Point List**, click **Select All→Add Single Signature**.

When points are added to the **Single-Signature Point List**, a popup window is displayed that allows the user to select Reasons or entire Reason Sets. These reasons will be available to the operator when making a change to a secured point to indicate why the change is necessary. Then the points are added to **single-signature point list**.

Step 8 To edit the reasons, select the points, and click **Edit Reasons**.

The new window **ReasonSet Selection Dialog** opens.

Step 9 To change the reason, select the reason and click **OK**.



Point Query station:|slot:/Drivers/BacnetNetwork/Test

slot:/Drivers/BacnetNetwork/Test/BooleanWritable
slot:/Drivers/BacnetNetwork/Test/En
slot:/Drivers/BacnetNetwork/Test/Str
slot:/Drivers/BacnetNetwork/Test/Nu

Selected Points

slot:/Drivers/BacnetNetwork/Test/BooleanWritable
slot:/Drivers/BacnetNetwork/Test/EnumWritable
slot:/Drivers/BacnetNetwork/Test/StringWritable
slot:/Drivers/BacnetNetwork/Test/NumericWritable

☑ TEMPERATURE
--- ☑ HIGH TEMP
--- ☑ MED TEMP
--- ☑ LOW TEMP
--- ------------------------------
☑ OCCUPANCY
--- ☑ OCCUPIED
--- ☑ UNOCCUPIED

Step 10 To change the secured points from the **Single-Signature Point List** to **Dual-Signature Point List**, select the points from the **Single-Signature Point List** and click add **Add Dual-Signature Point List**.

The points are added to **Dual-Signature Point List**. You can directly secure the unsecured points by selecting them from Unsecured list and clicking the Add Dual Signature. Downgrading secured points works in the same way using the Dual Signature to Single Signature, Remove Dual Signature, and Remove Single Signature buttons.

Setting up history Log

The Electronic Signature Service provides a record of changes requested or changes completed on secured points. The records include information required by 21 CFR Part 11.

Step 1 Expand **Config→ElectronicSignature** and double-click **Secured History Config**.

The **Property Sheet** opens. You can change the properties of **`Capacity`** and **`Full Policy`**.

Step 2 To change the properties for the **`Capacity`** and **`Full Policy`**, click drop-down list, select the property and click **Save**.

The two editable properties are:

- **`Capacity`** : Represents the number of trend log records (histories) to store in the histories database. When capacity is reached, newer records overwrite the oldest records.
- **`Full Policy`** : The property has two options `Stop` and `Roll`. `Stop` indicates the log will no longer include any new records and `Roll` indicates that when a new record is added to the log, the oldest record will be deleted.

The updates to the **`capacity`** and **`Full Policy`** are effective from the next time.

User security

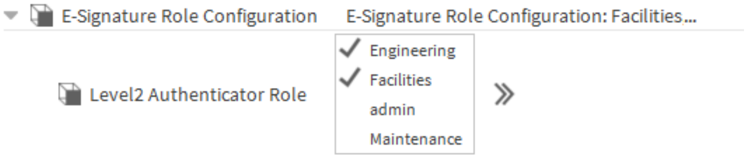
It is important to use Niagara Categories and Roles to prevent users from accessing some Admin level views and capabilities.

Please refer to the Installation Qualification and Operational Qualification documents for E-Signature for information about how to configure user security.

The *Niagara Station Security Guide* in Workbench help provides information and instructions for configuring secure network communication: module://docStationSecurity/doc/index.html

With the E-Signature added to a station, all the station's users require a property called **`E-Signature Role Configuration`**. This property allows you to select and assign Niagara roles from the **RoleService** to station users. Each role authorizes users to act as the secondary authenticator for changes to secured points requested by the user.

Figure 1 E-signature Role Configuration



E-Signature Role Configuration E-Signature Role Configuration: Facilities...

Level2 Authenticator Role

✓ Engineering
✓ Facilities
admin
Maintenance

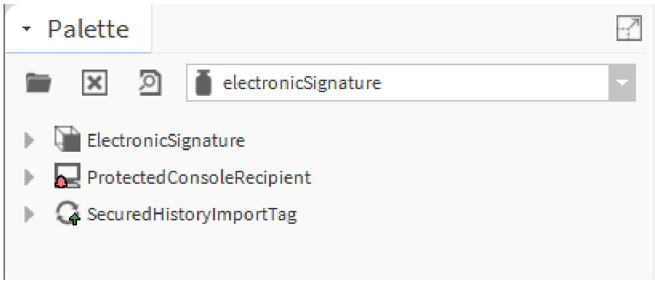
Users in large installations (that is installations with a Supervisor station and subordinate JACEs) that need to modify signed points in a remote station, must be network users. Niagara 4 checks the permissions and roles of users requesting changes on signed points. For this reason, such users must be assigned with the same role both in the Supervisor station and in the JACE station where the signed points are located.

NOTE: If a Supervisor user requests to change a secured point's value, and the secured point is a **Niagara-Network** proxy point, the Supervisor user's role and the secondary authenticator's role must exist in the JACE where the secured point originates.

Protected Alarm Console Recipient configuration

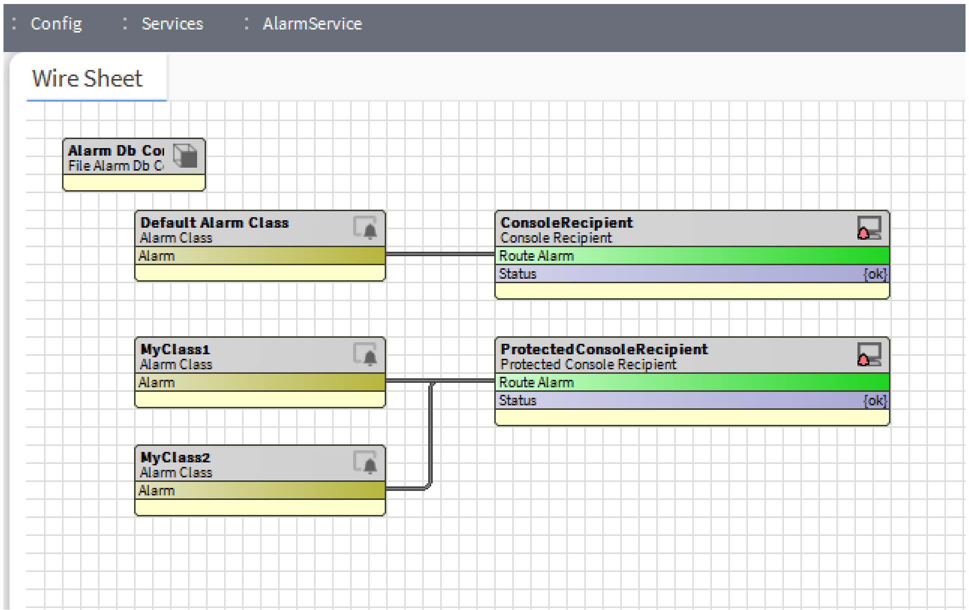
The Protected Alarm Console Recipient provides the ability to require an E-Signature when an alarm is acknowledged or cleared. The object is available in the **`electronicSignature`** module's palette.

Figure 2 ElectronicSignature Palette



To use the Protected Alarm Console Recipient, drag and drop the object from the palette onto the **AlarmService**. Create Wiresheet links between the alarm classes you would like to route alarms from and the **Route Alarm** slot on the Protected Alarm Console Recipient object.

Figure 3 Wiresheet view for console Recipient



The object includes a Protected Alarm Console View in both Workbench and the browser. The view looks and operates the same way the normal Alarm Console views work, but it requires authentication for acknowledging alarms.

By default, Protected alarm console view asks for single authentication while acknowledging the alarm or force clearing the alarm. But from eSign 2.3 version, system integrator can require dual authentication by disabling **`Use Single Authentication For Alarm Property`** on eSign AX Property sheet.

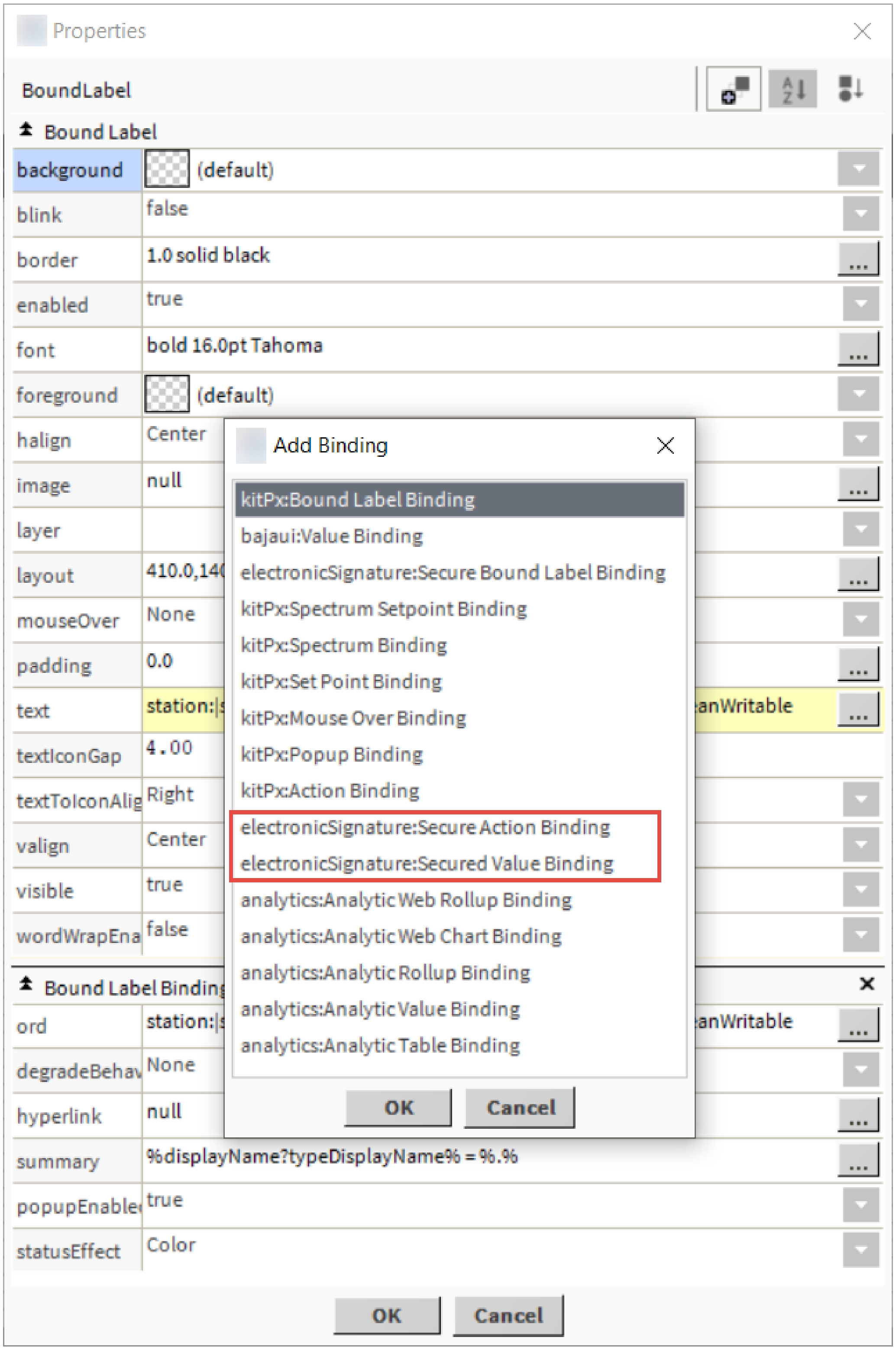
PX graphic bindings

A secured point that is made available to view or set via a PX graphic in the Niagara Station must use special bindings so that the authentication requirement for setting the point will be met.

There are three PX Bindings available:

- Secured Bound Label Binding
- Secured Action Binding
- Secured Value Binding

Figure 4 PX graphic bindings



Properties
BoundLabel
Bound Label
Add Binding
kitPx:Bound Label Binding
bajaui:Value Binding
electronicSignature:Secure Bound Label Binding
kitPx:Spectrum Setpoint Binding
kitPx:Spectrum Binding
kitPx:Set Point Binding
kitPx:Mouse Over Binding
kitPx:Popup Binding
kitPx:Action Binding
electronicSignature:Secure Action Binding
electronicSignature:Secured Value Binding
analytics:Analytic Web Rollup Binding
analytics:Analytic Web Chart Binding
analytics:Analytic Rollup Binding
analytics:Analytic Value Binding
analytics:Analytic Table Binding
OK
Cancel
Bound Label Bindin
OK
Cancel

background	(default)
blink	false
border	1.0 solid black
enabled	true
font	bold 16.0pt Tahoma
foreground	(default)
halign	Center
image	null
layer	
layout	410.0,14(
mouseOver	None
padding	0.0
text	station:|s … anWritable
textIconGap	4.00
textToIconAlig	Right
valign	Center
visible	true
wordWrapEna	false
ord	station:|s … anWritable
degradeBehav	None
hyperlink	null
summary	%displayName?typeDisplayName% = %.%
popupEnable	true
statusEffect	Color

All three bindings can be configured in the same way the regular Bound Label and Action Bindings are configured. The new bindings contain support for the authentication requirement that is required for interacting with secured control points.

Chapter 3 Secured actions

Topics covered in this chapter

♦ Changing a point value
♦ Remote authentication

New actions are added to the control points when adding control points to an Electronic Signature Zone. These actions allow for interaction with the control points in a secure way, requiring authentication for changes to be made.

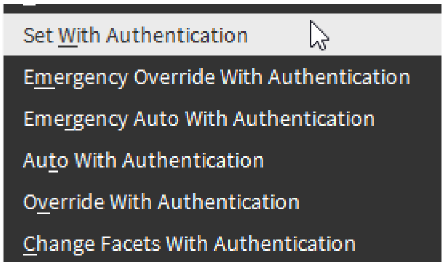
There are six actions:

- Set With Authentication
- Override With Authentication
- Emergency Override With Authentication
- Auto With Authentication
- Emergency Auto With Authentication
- Change Facets With Authentication

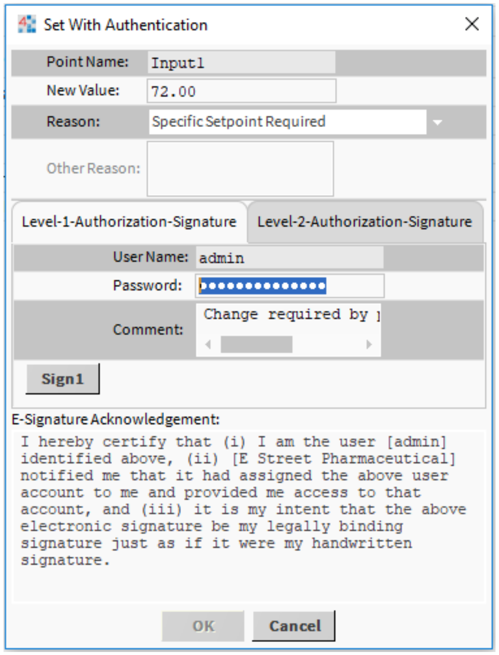
Changing a point value

Changing a point value must include the reason for the change.

Step 1 To change the point value, expand **Config**, right-click on the point and click **Actions→SetWithAuthentication**.


Set With Authentication
Emergency Override With Authentication
Emergency Auto With Authentication
Auto With Authentication
Override With Authentication
Change Facets With Authentication

The **Set With Authentication** window opens. You can enter the information to add new value.


Set With Authentication
Level-1-Authorization-Signature
Level-2-Authorization-Signature
Sign1
OK
Cancel

Point Name: Input1
New Value: 72.00
Reason: Specific Setpoint Required
Other Reason:
User Name: admin
Password: ●●●●●●●●●●●●●●
Comment: Change required by

E-Signature Acknowledgement:

```
I hereby certify that (i) I am the user [admin]
identified above, (ii) [E Street Pharmaceutical]
notified me that it had assigned the above user
account to me and provided me access to that
account, and (iii) it is my intent that the above
electronic signature be my legally binding
signature just as if it were my handwritten
signature.
```

Step 2 In the **Set With Authentication** window, enter the following information

a. **New Value** and **Reason**

b. To select the predefine reasons, click the drop-down arrow next to the **Reason** field and select the required reason.

c. To enter the other custom reasons in the **Reason** field, select `Other` and enter the reason in the **OtherReason** field.

Step 3 To authenticate primary user, click **Level-1–Authorization-Signature**, enter the following information, read the acknowledgment and click **Sign1**.

a. **UserName**

b. **Passowrd**

c. **Comment**

The details are added for single authentication.

Step 4 To authenticate secondary user, click **Level-2–Authorization-Signature**, enter the following information, read the acknowledgment and click **Sign2**.

a. **UserName**

b. **Passowrd**

c. **Comment**

The details are added for dual authentication.

Step 5 For single and dual authentication, click **OK** to update a new value for a point.

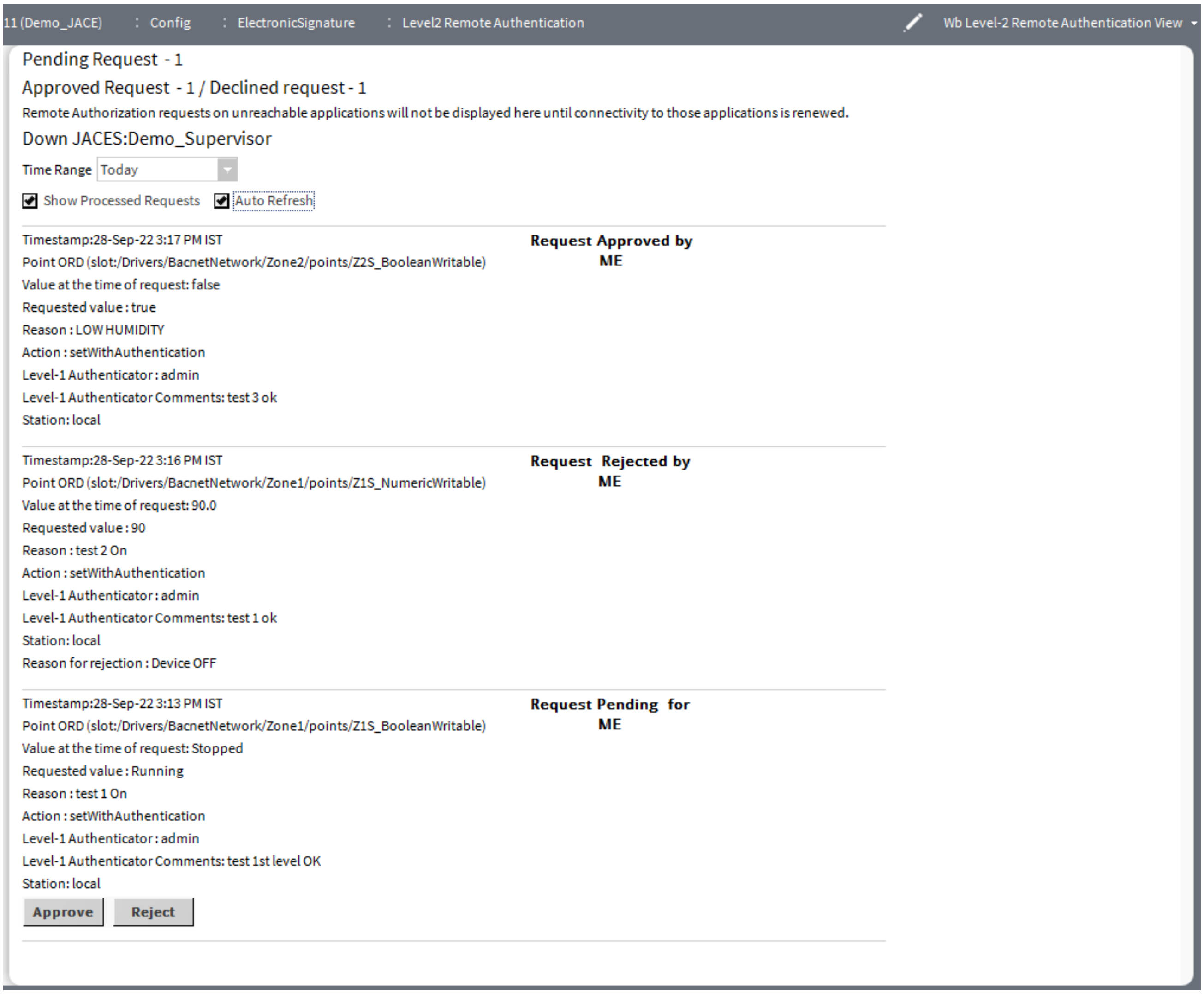
Remote authentication

With remote authentication feature, a user can submit a request for a change that necessitates dual factor authentication without having their second-level authenticator. The request for remote authentication is cached in the server until the second level authenticator logs in and accepts the change.

The remote requests are persisted in the memory and will not be available after station restart. Use the property **Should Store Station Remote Requests In BOG File** to persist the remote requests even after station restart.

The view provides to accept or reject the pending requests for the second level authenticator.

Figure 5 Level2 Remote Authentication


11 (Demo_JACE) : Config : ElectronicSignature : Level2 Remote Authentication
Wb Level-2 Remote Authentication View

Pending Request - 1

Approved Request - 1 / Declined request - 1

Remote Authorization requests on unreachable applications will not be displayed here until connectivity to those applications is renewed.

Down JACES:Demo_Supervisor

Time Range Today

☑ Show Processed Requests ☑ Auto Refresh

Timestamp:28-Sep-22 3:17 PM IST
Point ORD (slot:/Drivers/BacnetNetwork/Zone2/points/Z2S_BooleanWritable)
Value at the time of request: false
Requested value : true
Reason : LOW HUMIDITY
Action : setWithAuthentication
Level-1 Authenticator : admin
Level-1 Authenticator Comments: test 3 ok
Station: local

Request Approved by
ME

Timestamp:28-Sep-22 3:16 PM IST
Point ORD (slot:/Drivers/BacnetNetwork/Zone1/points/Z1S_NumericWritable)
Value at the time of request: 90.0
Requested value : 90
Reason : test 2 On
Action : setWithAuthentication
Level-1 Authenticator : admin
Level-1 Authenticator Comments: test 1 ok
Station: local
Reason for rejection : Device OFF

Request Rejected by
ME

Timestamp:28-Sep-22 3:13 PM IST
Point ORD (slot:/Drivers/BacnetNetwork/Zone1/points/Z1S_BooleanWritable)
Value at the time of request: Stopped
Requested value : Running
Reason : test 1 On
Action : setWithAuthentication
Level-1 Authenticator : admin
Level-1 Authenticator Comments: test 1st level OK
Station: local

Request Pending for
ME

Two types of Checkboxes:

- **Show Proceed Requests** : Deselect the option to show only pending requests waiting for either approval/rejection.
- **AutoRefresh**: When the Auto-Refresh is on, the system will fetch fresh remote request if any automatically every 30 seconds. The Refresh-interval of 30 seconds can be configured from **AX property sheet** of Secondary Authentication component.

The above image shows three type of requests for remote authentication:

- Pending Request : The requests that are pending in the queue are sent by the primary user for second-level approval.
- Approved Request : Once the secondary user has accepted the request, the request is shown as approved request.

- Reject Request : Once the secondary user has rejected the request, the request is shown as reject request

The Level 2 Remote Authentication view shows information about any request made by primary level authenticators for which the viewing user is a secondary level authenticator. It displays the information related to the change request including the time of the request, the primary user name, the requested change value, the Reason, etc. The view includes an Accept and Reject button for each request. Both the Accept and Reject options require the secondary level authenticator to authenticate before accepting or rejecting the request.

If a change was requested for a secured point that is not a local point, but a **NiagaraNetwork** proxy, the **NiagaraNetwork** connection to the control point's originating station must be usable to view, accept, or reject the change. If the Niagara station (JACE) is not reachable, it's pending changes will not be displayed and appropriate message indicating the down JACE s will be displayed.

By default system shows the remote requests from all the subordinate stations. List of subordinate stations for which the remote requests needs to be shown can be configured from **station list** property using **AX Property sheet** of **Level2Remote Authentication** component.

Chapter 4 Components

Topics covered in this chapter

- ♦ Customers and Zones
- ♦ Reasons and reason sets
- ♦ Secure History Config
- ♦ Secure Alarm History Config
- ♦ Email Configuration
- ♦ ElectronicSignature

Components include services, folders and other model building blocks associated with a module.

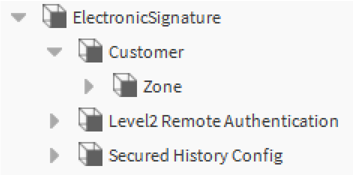
This chapter describes the details of the components that are present under **`ElectronicSignature`** component service.

Customers and Zones

A customer is the parent object of a zone, where we can edit customer information, and the customer can add multiple zones, which allows for better organization of signed points.

The E-Signature includes the concept of a customer and a zone. A customer is an organization a client or plant with a validated and regulated process or plant operation.

A zone is a collection of E-Signature secured points (for instance within a meaningful context of a multi-process manufacturing line). A zone is an organized container for references to signed points.



These terms are used to organize signed data points. You can add and remove points from a secure zone.

Customers can use multiple zones for better organization of signed points.

The customer includes properties for **CustomerName** and location information. The operator sees the **CustomerName** property as a part of the legal agreement displayed when making changes to secured points.

Reasons and reason sets

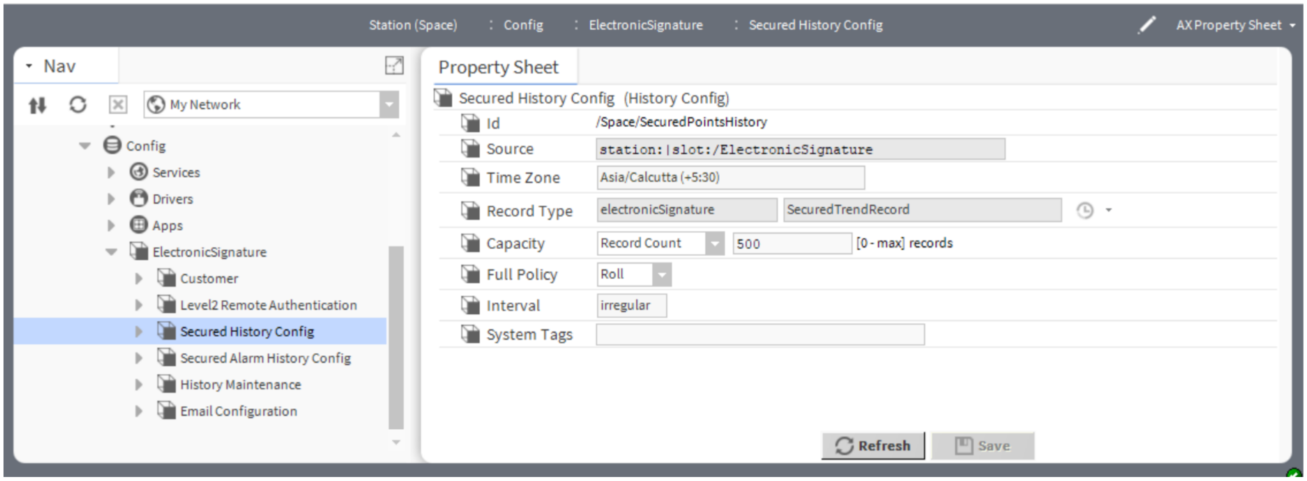
Changes to protected points cannot be made without reason.

The same reason for a change, such as maintenance or shutdown, may be used repeatedly. Using the Electronic Signature Service, you can predefine reasons and organize them into sets so that providing the reason for a change is easy.

Secure History Config

This component configures the history storage for the secured point history.

Figure 6 Secure History Config



Secured History Config (History Config)

Id	/Space/SecuredPointsHistory
Source	station:|slot:/ElectronicSignature
Time Zone	Asia/Calcutta (+5:30)
Record Type	electronicSignature SecuredTrendRecord
Capacity	Record Count 500 [0 - max] records
Full Policy	Roll
Interval	irregular
System Tags	

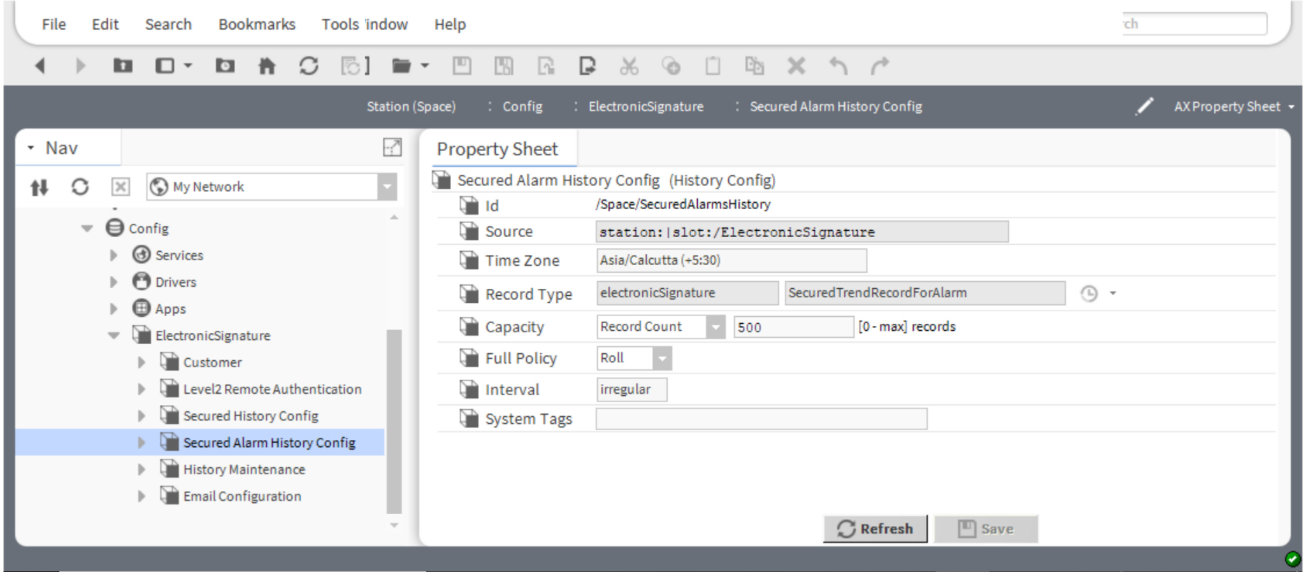
To access this view, expand **Config→ElectronicSignature** and double-click **SecuredHsitoryConfig**

Property	**Value**	**Description**
Id	Text string	Read only value. String results from value configured in history extension's **securedHistoryConfig** property. An error string here indicates the **SceuredHistoryConfig** property is incorrectly configured. The history name can be renamed by going into the **AX Property Sheet** of Esignature and change the property name in the **SecuredHistoryName** and click **Save**. Then the property name is updated in the **SecuredHistoryConfig**.
Source	ORD	Read only value. Displays the ORD of the active history extension.
Time Zone	read-only	Displays the current time zone.
Record Type	read-only	Read only values. Displays the data that the record holds in terms of: extension type (ElectronicSignature) and data type (SecureTrendRecord).
Capacity	drop-down list	Specifies the number of trend log records (histories) to store in the histories database. When capacity is reached, newer records overwrite the oldest records.
Full Policy	drop-down list	Determines what happens when the history table reaches its maximum **Capacity**. Stop restricts the table to the **Capacity**. After reaching this number, the system ignores new records. Roll replaces the oldest records with newer records.
Interval	Text string	Read only value. For Interval-based data collection, the cycle time, or how often the history properties are checked. Any time you change this property, a new history is created (or "split-off") from the original history because histories with different intervals are not compatible.
System Tags	Text	This property allows you to assign additional metadata (the System Tag) to a history extension.

Secure Alarm History Config

This component resides under the **ElectronicSignature** in the Nav tree. The view allows the user to configure the history storage for the acknowledged alarms.

Figure 7 Secure Alarm History Config



Secured Alarm History Config (History Config)

Id	/Space/SecuredAlarmsHistory
Source	station:|slot:/ElectronicSignature
Time Zone	Asia/Calcutta (+5:30)
Record Type	electronicSignature SecuredTrendRecordForAlarm
Capacity	Record Count 500 [0 - max] records
Full Policy	Roll
Interval	irregular
System Tags	

To access this view, expand **Config→ElectronicSignature** and double-click **SecuredAlarmHsitoryConfig**

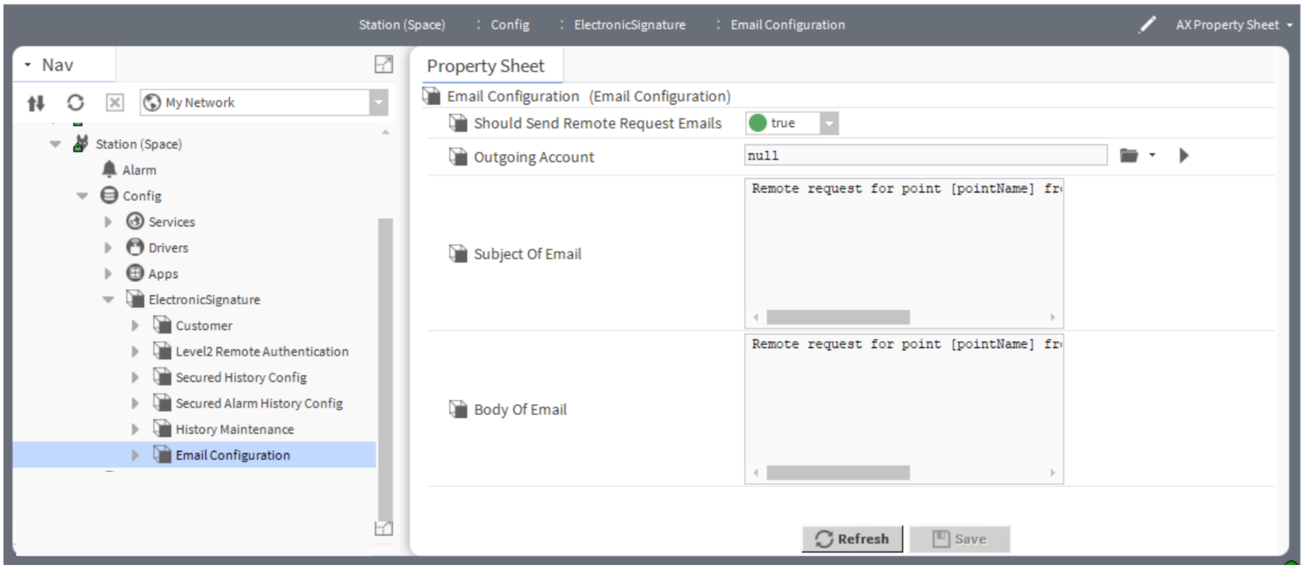
Property	Value	Description
Id	Text string	Read only value. String results from value configured in history extension's **Alarm History** property. An error string here indicates the **Alarm History** property is incorrectly configured. The alarm history name can be renamed by going into the **AX Property Sheet** of E-Signature and change the property name in the **SecuredAlarmHistoryName** and click **Save**. Then the property name is updated in the **SecuredAlarmHistoryConfig**.
Source	ORD	Read only value. Displays the ORD of the active history extension.
Time Zone	read-only	Displays the current time zone.
Record Type	Text	Read only values. Displays the data that the record holds in terms of: extension type (ElectronicSignature) and data type (SecureTrendRecordForAlarm).
Capacity	drop-down list	Specifies the number of trend log records (histories) to store in the histories database. When capacity is reached, newer records overwrite the oldest records.
Full Policy	Roll (default), Stop	Determines what happens when the alarm history table reaches its maximum **Capacity**. Stop restricts the table to the **Capacity**. After reaching this number, the system ignores new records. Roll replaces the oldest records with newer records.

Property	Value	Description
Interval	Text string	Read only value. For Interval-based data collection, the cycle time, or how often the history properties are checked. Any time you change this property, a new history is created (or "split-off") from the original history because histories with different intervals are not compatible.
System Tags	Text	This property allows you to assign additional metadata (the System Tag) to a history extension.

Email Configuration

The feature of email notification for remote requests can be enabled by setting the **Should Send Remote Request Emails** property to true. By default the value for the property is set to false.

Figure 8 Email Configuration



Email Configuration (Email Configuration)

Should Send Remote Request Emails: ● true

Outgoing Account: null

Subject Of Email: Remote request for point [pointName] fr

Body Of Email: Remote request for point [pointName] fr

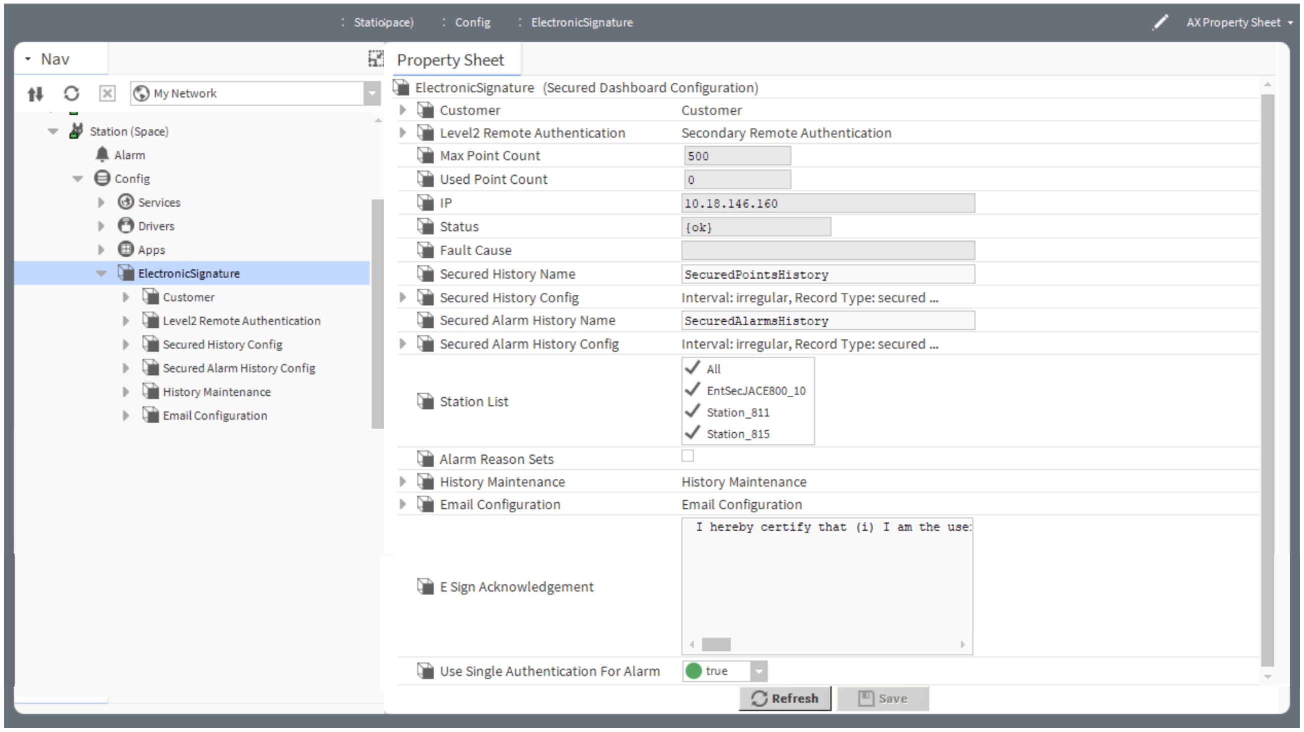
Should Send Remote Request Emails

Type	Value	Description
Should Send Remote Request Emails	true or false	It sends a notification of the remote request to secondary users whenever a remote request is raised . By enabling this property to `true`, user can send email notifications, and to disable this property to `false`, if you don't want to send email notifications.
Outgoing Account	Ord chooser	Select the 📁 ord chooser for email services outgoing account which will be used to send the remote request notifications.
Subject of Email	Text	It displays the information about the email, and you can modify the subject of the email.
Body of Email	Text	It displays the body of the email to convey the message.

ElectronicSignature

This is a core component of an ElectronicSignature module. It contains a full complement of Customer information, Remote Authentication, History database, Email Configuration, and so on. This component is used to configure E-Signature related information.

Figure 9 Ax Property Sheet



ElectronicSignature (Secured Dashboard Configuration)

Customer	Customer
Level2 Remote Authentication	Secondary Remote Authentication
Max Point Count	500
Used Point Count	0
IP	10.18.146.160
Status	{ok}
Fault Cause	
Secured History Name	SecuredPointsHistory
Secured History Config	Interval: irregular, Record Type: secured ...
Secured Alarm History Name	SecuredAlarmsHistory
Secured Alarm History Config	Interval: irregular, Record Type: secured ...
Station List	✓ All ✓ EntSecJACE800_10 ✓ Station_811 ✓ Station_815
Alarm Reason Sets	□
History Maintenance	History Maintenance
Email Configuration	Email Configuration
E Sign Acknowledgement	I hereby certify that (i) I am the use:
Use Single Authentication For Alarm	● true

To access these properties, expand **Config** and right-click **ElectronicSignature** and click **Views→Ax Property Sheet**.

Type	Value	Description
Customer	additional properties	Contains the information about the customer, Zones, and associated secured points.
Level2 Remote Authentication	additional properties	Contains the information about the remote authentication request.
Max Point Count	Number	Displays the max number of points that can be secured in the host station.
Used Point Count	Number	Displays the number of secured points in the host station.
IP	Number	It displays the IP address of the host.
Status	read-only	Indicates the condition of the component at the last check. `{ok}` indicates that the component is licensed. `{fault}` indicates another problem. Following could be the list of reasons for fault. • E-Signature License feature is expired • E-Signature License feature is missing.

Type	Value	Description
		• Secured point history name is missing. • Please specify different history name to rename existing history. • Error while renaming the history. • Secured alarm history name is missing. • Please specify different alarm history name. • Error while renaming the alarm history.
Fault Cause	read-only	Indicates the reason why a E-Signature component is not working properly (in fault). This property is empty unless a fault exists.
Secured History Name	Text	Display the history name for the secured point history database and user can modify the property to rename the history.
Secured History Config	additional properties	It allows user to configure the history storage for the secured point history.
Secured Alarm History Name	Text	Display the history name for the secured alarm history database and user can modify the property to rename the alarm history.
Secured Alarm History Config	additional properties	It allows the user to configure the history storage for the secured alarm history.
Station List		It displays the list of **NiagaraNetwork** station that will be queried for remote request.
Alarm Reason Sets		Allows users to choose the reasons for acknowledging the alarm.
Email Configuration	additional properties	It sends the email notifications for the secondary level authenticator when remote requests are raised.
Esign Acknowledgement	Text	It allows user to configure legal statement that gets displayed while authorizing the change the secured points. There are two keywords, which will be replaced with actual user who will be authenticating the change and customer name for which the project is configured. • [username] • [customername]
Use Single Authentication For Alarm	true or false(default to true)	Allows user to configure the authentication level for alarm acknowledgement.

Chapter 5 Plugins (views)

Topics covered in this chapter

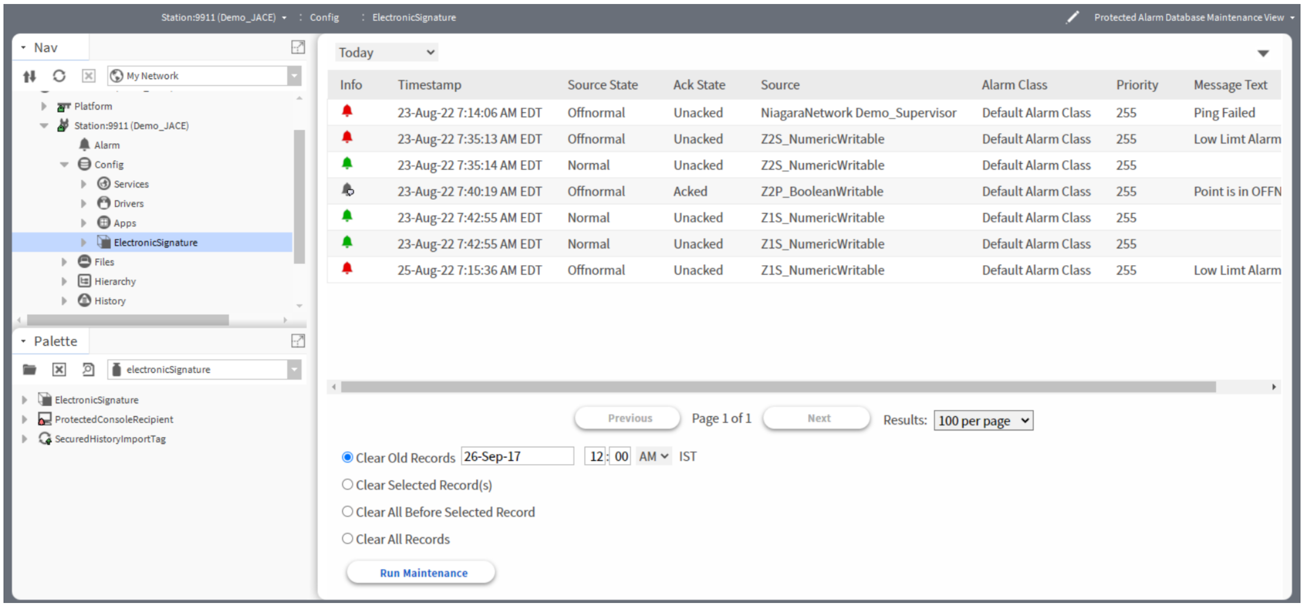
- ♦ Protected Alarm Database Maintenance View
- ♦ Protected History Database Maintenance View
- ♦ Level2 Remote Authentication

Plugins provide views of components and can be accessed in many ways. For example, double-click a component in the Nav tree to see its default view. In addition, you can right-click on a component and select from its **Views** menu.

Protected Alarm Database Maintenance View

This is a maintenance view allows user to remove the old alarm records after authentication.

The alarm database resides in a station file system under the station's alarm folder.



Info	Timestamp	Source State	Ack State	Source	Alarm Class	Priority	Message Text
🔔	23-Aug-22 7:14:06 AM EDT	Offnormal	Unacked	NiagaraNetwork Demo_Supervisor	Default Alarm Class	255	Ping Failed
🔔	23-Aug-22 7:35:13 AM EDT	Offnormal	Unacked	Z2S_NumericWritable	Default Alarm Class	255	Low Limt Alarm
🔔	23-Aug-22 7:35:14 AM EDT	Normal	Unacked	Z2S_NumericWritable	Default Alarm Class	255	
🔔	23-Aug-22 7:40:19 AM EDT	Offnormal	Acked	Z2P_BooleanWritable	Default Alarm Class	255	Point is in OFFN
🔔	23-Aug-22 7:42:55 AM EDT	Normal	Unacked	Z1S_NumericWritable	Default Alarm Class	255	
🔔	23-Aug-22 7:42:55 AM EDT	Normal	Unacked	Z1S_NumericWritable	Default Alarm Class	255	
🔔	25-Aug-22 7:15:36 AM EDT	Offnormal	Unacked	Z1S_NumericWritable	Default Alarm Class	255	Low Limt Alarm

Results: 100 per page

● Clear Old Records 26-Sep-17 12 : 00 AM IST

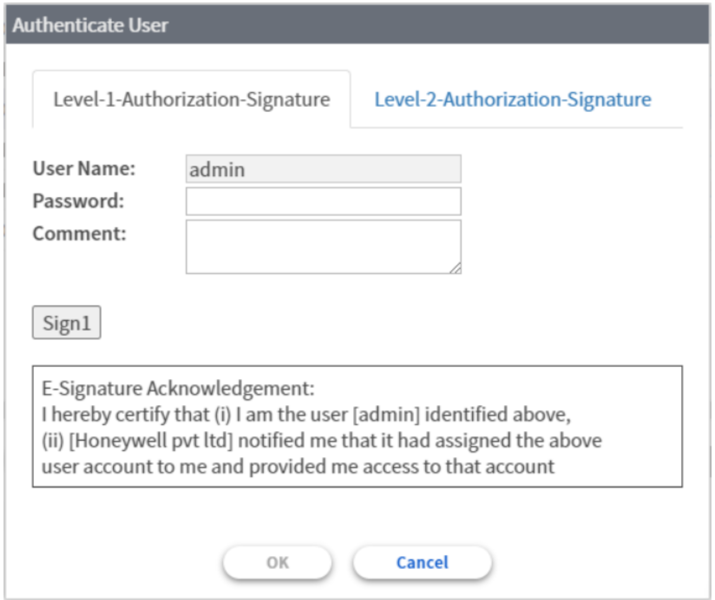
○ Clear Selected Record(s)

○ Clear All Before Selected Record

○ Clear All Records

To access this view, expand **Config** and right-click **Electronic Signature** and click **Views→Protected Alarm Database Maintenance View**.

While running the maintenance, it asks for the authentication to clear the records from the alarm database.


Authenticate User
Level-1-Authorization-Signature
Level-2-Authorization-Signature
Sign1
OK
Cancel

User Name: admin
Password:
Comment:

E-Signature Acknowledgement:
I hereby certify that (i) I am the user [admin] identified above,
(ii) [Honeywell pvt ltd] notified me that it had assigned the above
user account to me and provided me access to that account

The upper portion of the window contains the alarm history table. As with other tables, you can show or hide columns and use other standard table controls and options that are provided in the Table Options menu. The Table Options menu is located in the top right corner of the table and the export toolbar icon is available on the toolbar.

The lower portion of the screen provides controls for managing the alarm history database.

Alarm History columns

Column	Value	Description
Ack Required	`true` or `false`	Indicates if the alarm must be acknowledged (`true`) or not (`false`).
Ack Time	`hours:minutes:seconds`	Displays the time that the alarm was acknowledged (if applicable).
Ack State	`Acked` or `Unacked`	Indicates if the alarm has been acknowledged.
Alarm Class	List, console column, or field or %alarmClass% on a report.	Specifies or returns the alarm routing option for the component.
Alarm Data	read-only	Presents a detailed list of alarm data, including this information: • Status • toState • msgText • Count • fromState • Timezone
Alarm Transition	text	Shows the initial source state that caused the alarm to be generated. The Alarm Transition may not be the current state of the alarm source. Once an Alarm Transition is created, it does

Column	Value	Description
		not change for a single alarm record. For example, if the source state returned to "Normal" after an "Offnormal" status, this value remains at "Offnormal".
Normal Time or NormalTime	date and time	Displays the date and time (if applicable) that the alarm state returned to normal.
Priority [alarm]	read-only	Ranks the alarm on a pre-defined importance scale. The lower the number, the higher the Priority.
Source	%alarmData.sourceName%	Displays the path to the point that is generating the alarm. **NOTE:** For how to format this information on a report, click on the help icon to the right of the field.
Source State or sourceState	`NormalHigh Limit`	The status of the entity at the time the event, such as an alarm, occurred.
Timestamp	hours:minutes:seconds%timestamp% (on a report)	Specifies the date and time the event occurred.
User [provisioning]	text	The station user that requested the job. This column displays `unknown` if job was triggered by a linked schedule.
Uuid	read-only	Displays the Unique Universal Identifier (UUID) the system uses to uniquely identify the alarm record.
Last Update	read-only	Displays the time the system most recently updated the alarm.

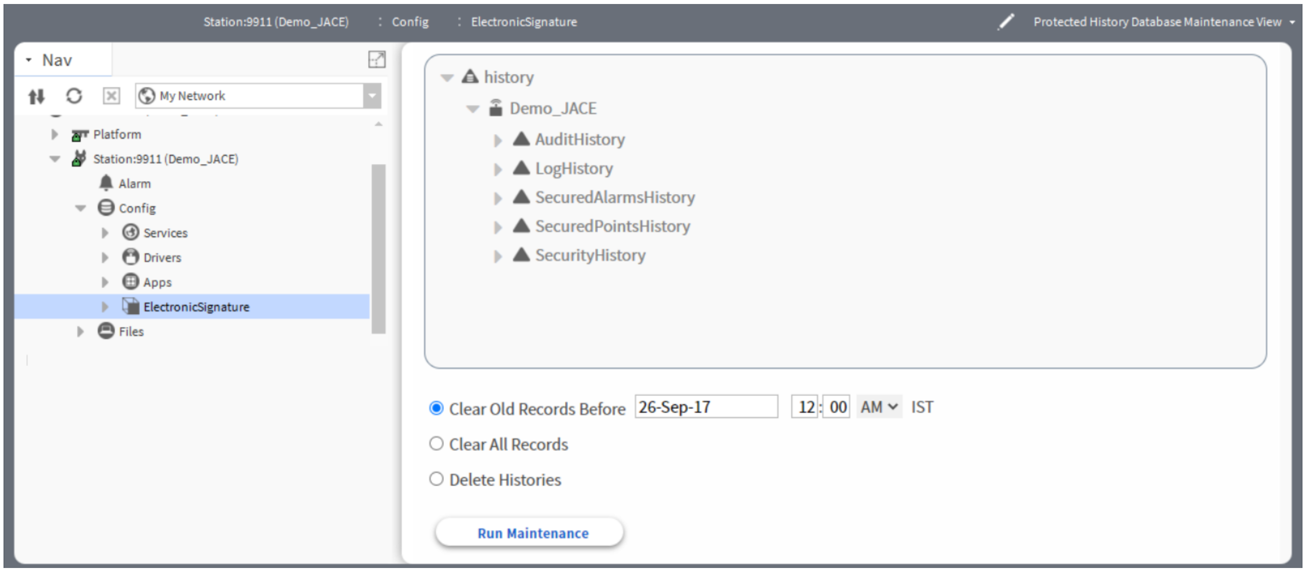
Alarm History maintenance

Option	Value	Description
Clear Old Records and Before property	selection bullet	Deletes alarm records before the date and time you define in the **`Before`** property.
Clear All Before Selected Record	selection bullet	Deletes all records with a timestamp that is earlier than the timestamp of the currently-selected record in the table.
Clear All Records	selection bullet	Deletes all records regardless of the date.
Run Maintenance	button	Executes the maintenance action after authentication.

Protected History Database Maintenance View

This view is a maintenance view allows user to remove the old history records after authentication.

Figure 10 Protected History Database Maintenance View



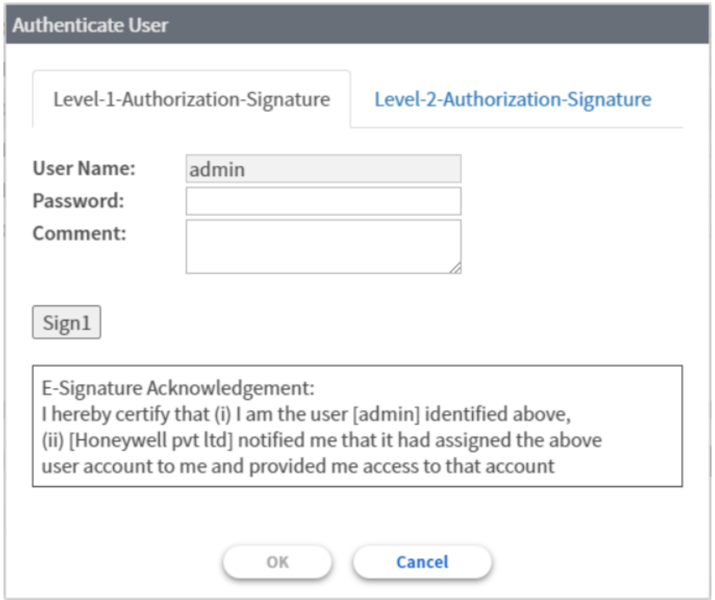
● Clear Old Records Before 26-Sep-17 12 : 00 AM IST

○ Clear All Records

○ Delete Histories

To access this view, expand **Config** and right-click **Electronic Signature** and click **Views→Protected History Database Maintenance View.**

While running the maintenance, it asks for the authentication to clear the records from the history database.


Authenticate User
Level-1-Authorization-Signature
Level-2-Authorization-Signature
Sign1
OK
Cancel

User Name: admin

Password:

Comment:

E-Signature Acknowledgement:
I hereby certify that (i) I am the user [admin] identified above,
(ii) [Honeywell pvt ltd] notified me that it had assigned the above
user account to me and provided me access to that account

The right side of the **histories** area contains the targeted histories window. This window displays the histories that are affected when you click the **Run Maintenance** button. Move the histories that you want manage into this window using the control buttons, as described below:

Controls and options for the database maintenance view are described in the following list:

- Add history button (right arrow)

  Click this button to move histories that are selected in the **available histories** window to the targeted histories window.

- Remove history button (left arrow)

Click this button to move histories that are selected in the **targeted histories** window to the available histories window.

- Clear Old Records option

  Select this option and use the **Before** date selector to remove records, based on date, from the histories that are in the targeted histories window.

- Before date property

  Use this property with the Clear old records option to set the year, month, day, and time properties that you want to use for removing old records.

- Clear all records

  Select this option to delete all records from the selected history database.

- Delete Histories

  Select this option to delete all histories that are in the targeted histories window.

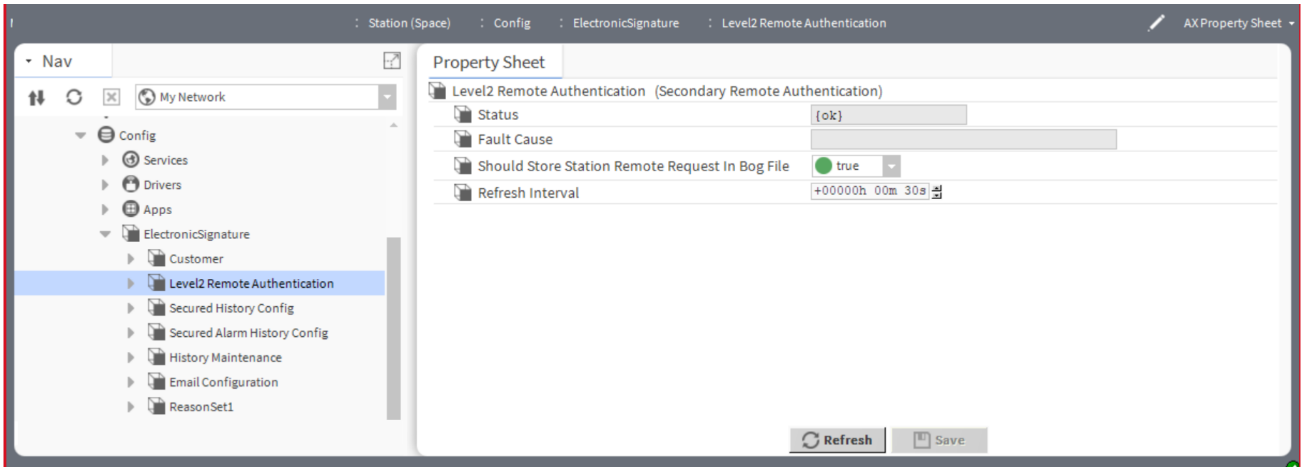
- Run Maintenance button

  Click this button to execute the option that you have selected on the histories in the targeted histories window and it asks for authentication before executing the action.

Level2 Remote Authentication

This page displays properties related to remote authentication configuration.

Figure 11 AX property Sheet



Level2 Remote Authentication (Secondary Remote Authentication)

Status	{ok}
Fault Cause	
Should Store Station Remote Request In Bog File	● true
Refresh Interval	+00000h 00m 30s

To access this view, expand **Config→ElectronicSignature** and right-click **Level2 Remote Authenticatio-nand** click **Views→AX Property Sheet**.

Type	Value	Description
Status	read-only (defaults to ok)	Indicates the condition of the component at the last check. `{ok}` indicates that the component is licensed.
Fault Cause	read-only	

Type	Value	Description
Should Store Station Remote Request in Bog File	true or false (defaults to true)	Allows users to configure the storage type for remote request. When set to `true` the remote requests will be stored in Bog file and be available after station reboot. When set to `False` the remote requests will be stored in RAM and will not be available after station reboot.
Refresh Interval	hours, minutes and seconds (defaults to 30s)	After every 30s the remote request authentication page will be refreshed. Use this property to configure the refresh interval.

Glossary

baja	A term coined from Building Automation Java Architecture. The core framework built by Tridium is designed to be published as an open standard.
Customer (ESignature)	Organization/Client/Plant name that wants to set up a validated and regulated process/plant operation.
CFR	Code of Federal Regulation It is a general and permanent regulation published in the Federal Register by the executive departments and agencies of the federal government.
E-Signature or Esign Secured Point	A point that requires electronic signature to change its properties.
Level 1Authentication	1st level authentication for change in point's value, name, etc.
Level 2 Authentication	2nd level authentication for change in point's value, name, etc. (if/when configured for 2-level authentication).
Reason	The documented purpose for changing the value of a point (E.g. maintenance, shutdown, etc.)
Reason Set	Collection of similar Reasons (Such as environmental requirements, logical control constant changes, recipe changes, etc.).
Zone	A collection of ESignature secured points (for instance within a meaningful context of a multi-process manufacturing line). Points can be added to or removed from a secure zone.

Index