



Niagara 4.8

Features Overview

Release Summary

From large enterprises to single site installations, Niagara 4.8 offers features for everyone with new functionality that enhances the Supervisor, JACE, Edge 10 and partner platforms.

New features include:

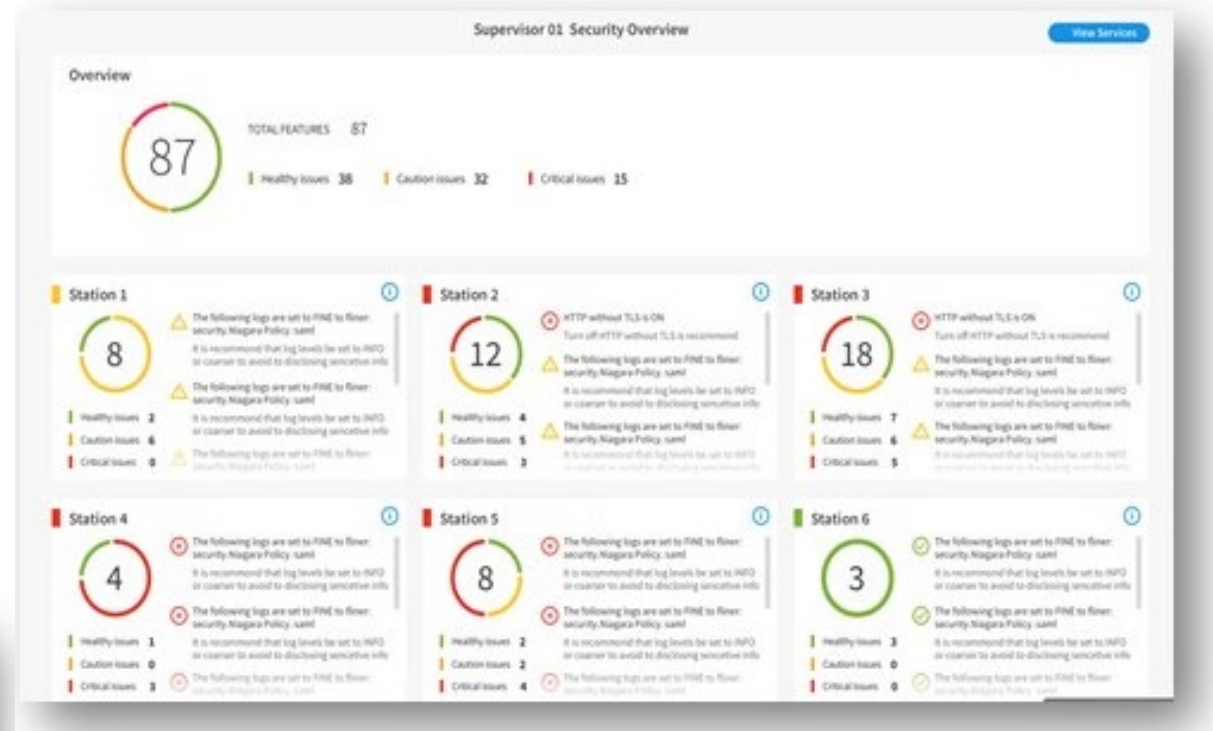
- A new dashboard that allows you to quickly assess the security posture of your Niagara Network.
- 802.1x support for network access authentication.
- ACE, the new deterministic engine for Edge 10.
- The use of client certificate authentication to enable kiosk mode and station to station connectivity.
- New third party module signing and verification support.
- Improved Edge Tools and Export functionality.

Security Dashboard

Quickly assess the security posture of your Niagara Network

Supervisor view shows all JACEs on your network

- Quickly identify issues with roll up view
- Triage Outliers
- Useful for large sites with multiple contractors



Station view shows individual services

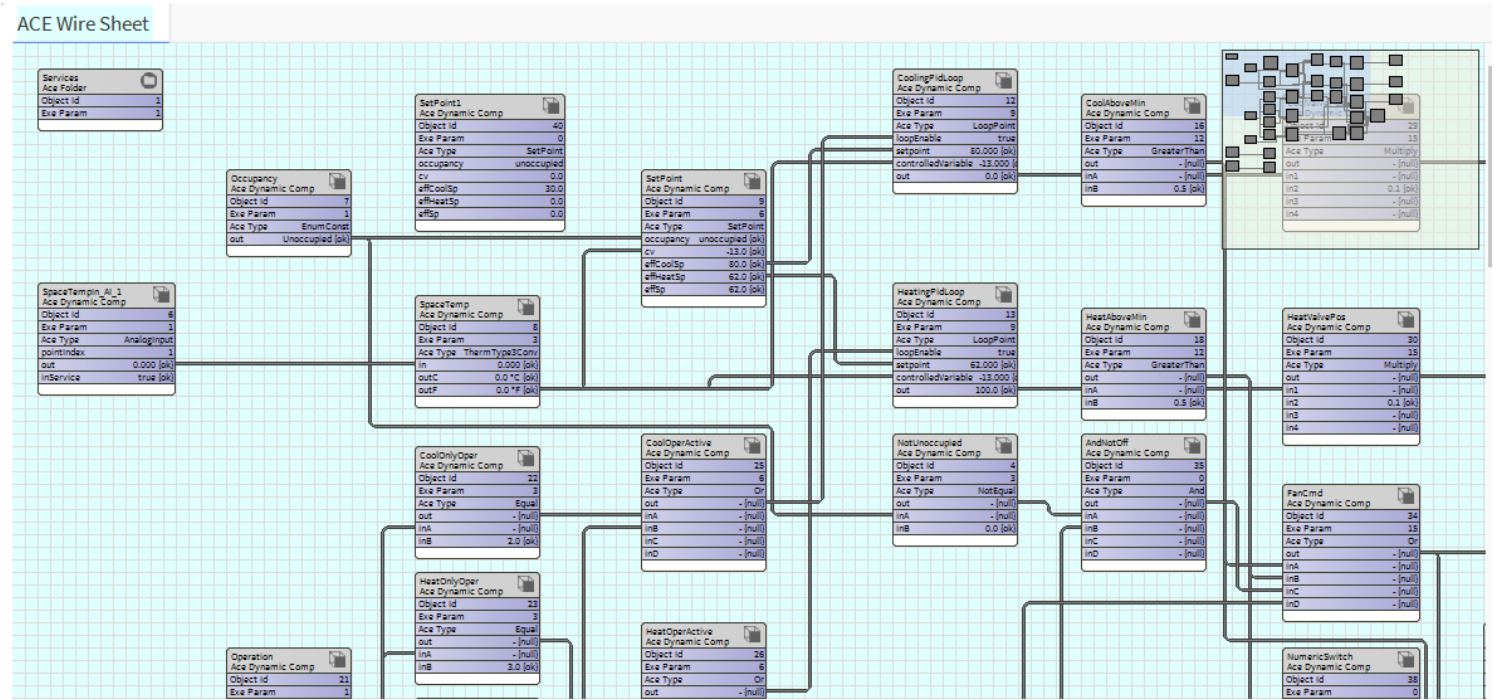
- User Service
- Fox Service
- Web Service
- Login Service
- Authentication Service
- Module Permissions

Client Certificate Authentication



Utilizing client certificate authentication, pre-configured browsers can be used to facilitate Kiosk Mode functionality providing public users a dedicated view of a Niagara system.

ACE - Deterministic Runtime Engine



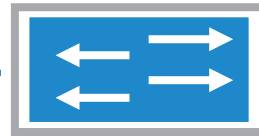
ACE for Edge 10 enables fast startup to control time and deterministic timing when servicing the IO. Create deterministic applications in Wire Sheet as you would in normal Niagara applications.

IEEE 802.1x Support

802.1x Supplicants



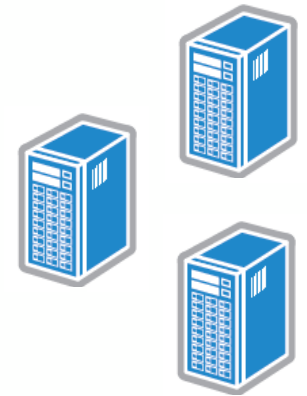
Wired Switch
(Authenticator)



RADIUS Server
(Authentication Server)



Identity Sources



802.1x, an IEEE standard for network access authentication, is typically used in enterprises and campuses with large scale networks to provide security, scalability and ease of management. The JACE 8000 and Edge 10 are now compliant with this standard and can be used as wired clients (supplicants) in a 802.1x based network.

Third Party Module Signing

Commissioning for "172.31.66.50 (jace)"

Software Installation

Please check each additional item you wish to have installed to the remote host. Any software known to be required for stations to run is already checked.

Current free space 3,288,233 KB To be installed 0 KB Estimated free space after install 3,288,233 KB

Software	Installed Version	Avail. Version	
<input type="checkbox"/> invalidSig-rt	-	Acme 1.0	Not Installed
<input type="checkbox"/> caSigned-rt	Acme 1.0	Acme 1.0	Up to Date
<input type="checkbox"/> selfSigned-rt	Acme 1.0	Acme 1.0	Up to Date
<input type="checkbox"/> selfSignedTimestamped-rt	Acme 1.0	Acme 1.0	Up to Date
<input type="checkbox"/> unsigned-rt	Acme 1.0	Acme 1.0	Up to Date
<input type="checkbox"/> caSignedTimestamped-rt	Acme 1.0	Acme 1.0	Up to Date
<input type="checkbox"/> aaphp-rt	-	Tridium 4.8.0.16	Not Installed
<input type="checkbox"/> aaphp-wb	-	Tridium 4.8.0.16	Not Installed

Software Details

Module selfSignedTimestamped-rt

Description A self signed, timestamped module

	Installed	Available
Version	Acme 1.0	Acme 1.0
Release Date	-	-
Status	Signature Warning	Signature Warning
Processed for Jace	Not Processed	Not Processed

Installable File Details

Path C:\Niagara\Niagara-4.8.0.16\sw\1.0\selfSignedTimestamped-rt.jar

Size 5.9 KB

Installed Signature Details

Status Self-signed signing certificate
Certificate path validation failure

Signers

[self_signed](#)

- This signer is using a self-signed certificate. Self-signed certificates will not be allowed by default in a future version.
- This signer's certificate path could not be validated. Modules must be signed with a valid trusted certificate in a future version.

Available Signature Details

Status Self-signed signing certificate
Certificate path validation failure

Signers

[self_signed](#)

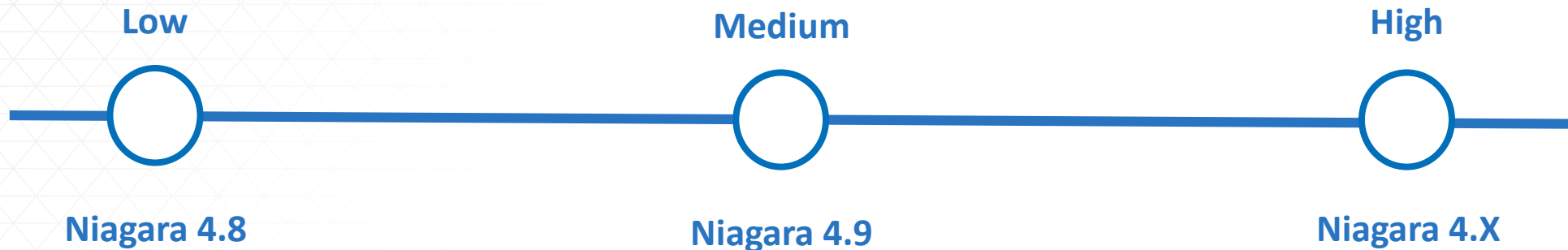
- This signer is using a self-signed certificate. Self-signed certificates will not be allowed by default in a future version.
- This signer's certificate path could not be validated. Modules must be signed with a valid trusted certificate in a future version.

OK

Requiring all third party modules to be signed increases security posture of a Niagara installation by making administrators aware of modules that may have been tampered with or come from an untrustworthy source. This feature will be rolled out over a number of Niagara releases to ensure that developers are able to transition to signing their code.

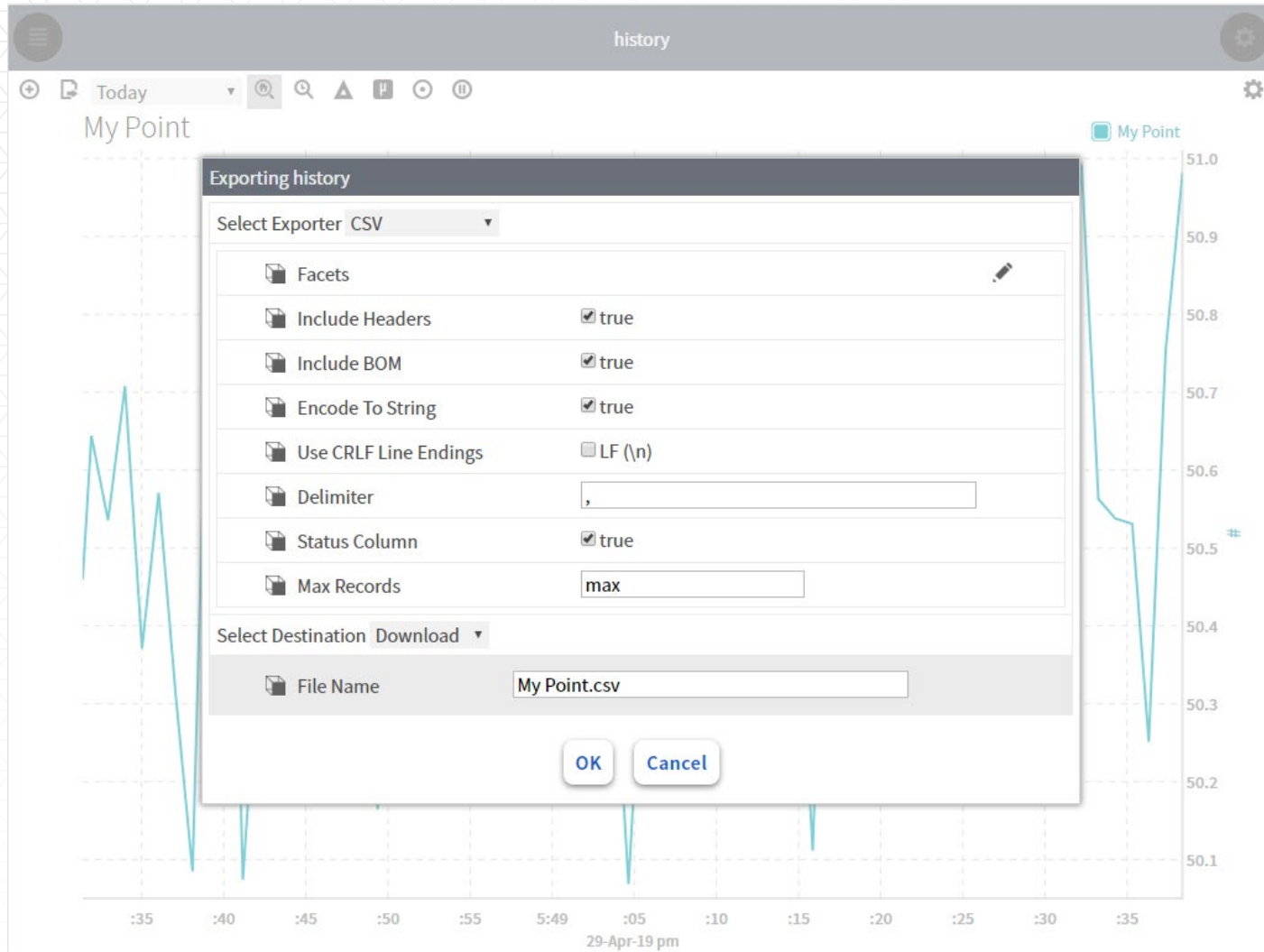
3rd Party Module Signing – Phased Rollout

Default Verification Mode by Version



Verification Mode	Description
Low	Modules that are unsigned, untrusted, or have expired certificates will cause warnings but still function. Error if signed module modified after it was signed. Can be increased to Medium or High.
Medium	All modules must be signed by valid, trusted certificate (may be self-signed). Can be decreased to Low or increased to High
High	All modules must be signed with CA Certificate. Can be decreased to Medium.

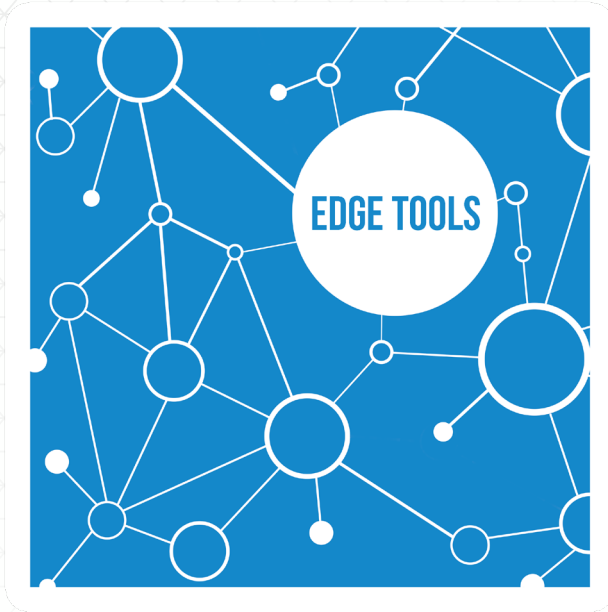
Export Refresh



Updated export capability including:

- Station-side exports from the browser
- Export HTML5 tables directly to CSV or JSON
- Additional customization like Max Records and Page Size

Improved Edge Tools



Continued enhancement of Application Templates to support and streamline the use of peer and supervisory Niagara Network stations in an application.

New Provisioning steps added to enable a low touch mechanism to setup, configure and maintain a Niagara system.

Niagara 4.8 on the JACE



The JACE 8000™ has been upgraded to run the latest QNX release and a new JVM. This will ensure future compatibility with new features and continue ongoing support.