



**TRIDIUM**

niagara  
remote™

Features Overview

# niagara remote™

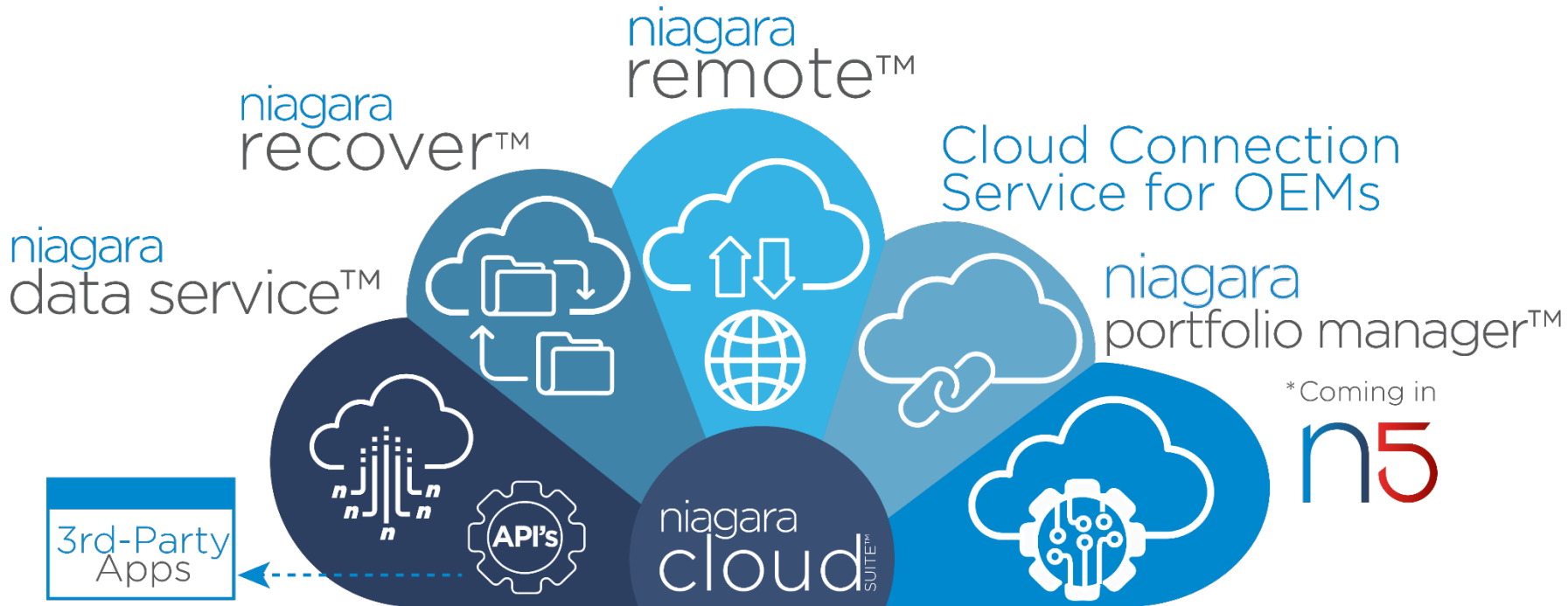
***Any Tech,  
Any Station,  
Anywhere...***



Tridium Confidential - ©2026 by Tridium Inc. All rights reserved.  
All items and schedules are subject to change at Tridium's sole discretion. Tridium  
has no obligation to deliver any future product outlined in this document.

# PART OF NIAGARA CLOUD SUITE™

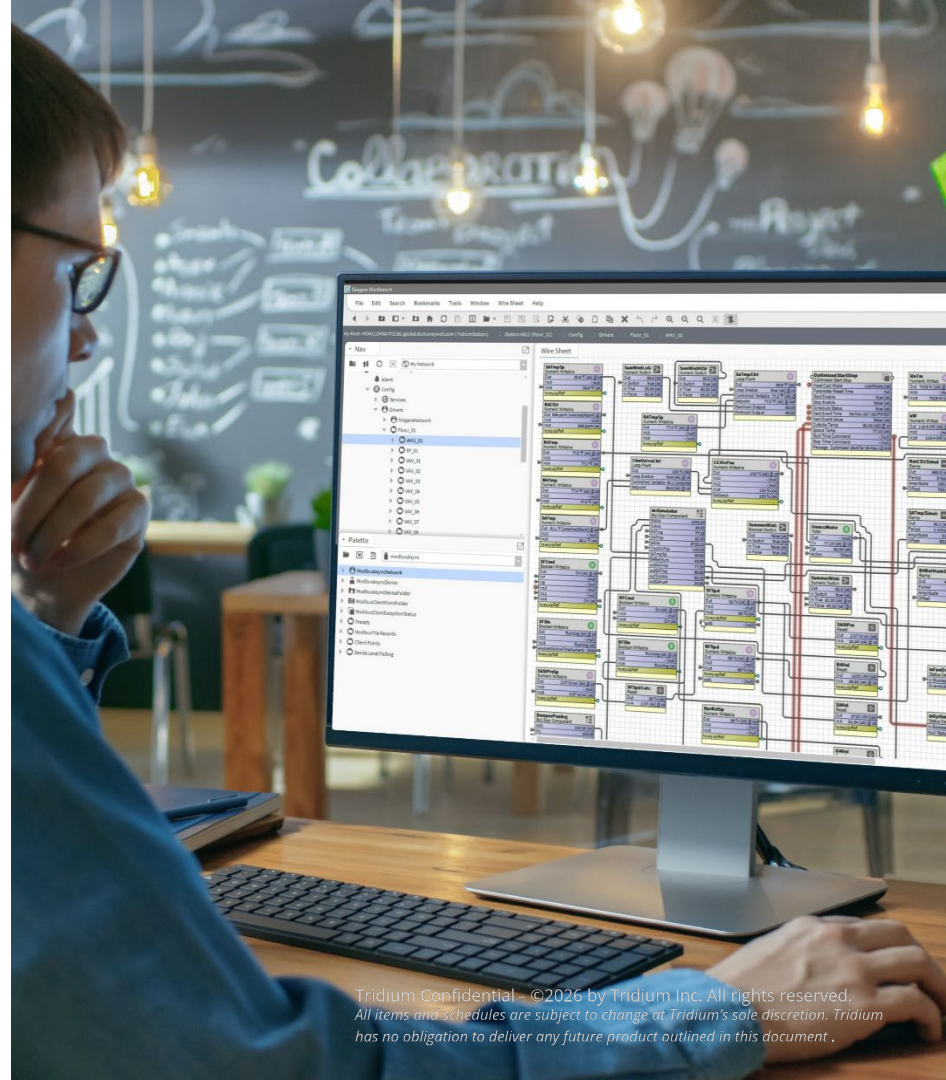
Tridium supports hybrid cloud-on-premises strategies. Add cloud capabilities to your Niagara Framework® deployment when and where you are ready.



# WHY NIAGARA REMOTE?

**A productivity-enhancing and cost-saving option for the busy Niagara Framework user that needs to:**

- Troubleshoot a Niagara deployment
- Do regular engineering and maintenance work
- Access the Niagara UI to check the status of Niagara stations across a Niagara-based network
- Create and edit Px graphics to continuously improve user experience
- Remotely connect to a Niagara station, without a VPN, static IP connection or additional firewall rules.



# BENEFITS OF REMOTE ACCESS FOR SERVICE MAINTENANCE BUSINESS

## Niagara Partners have realized gains in each of these categories:

- **Improved Efficiency:** Remote monitoring of customer deployments enables faster response times
- **Cost Savings:** Fuel and mileage-related expenses are curtailed
- **Less Disruption:** Issues can be detected and resolved with minimal interruption of customer operations
- **Increased Access:** Service support can be extended to customer properties located at a wider geographical distance



# CURRENT RELEASE

*Users have web browser-based access to a Niagara-Remote-enabled station from any Internet-connected device.*

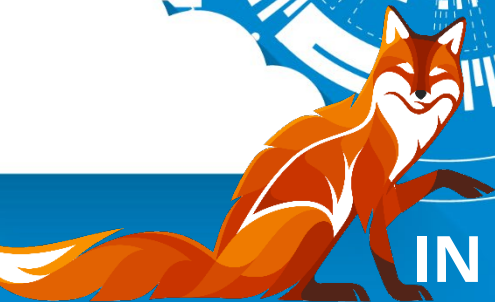
*Designed for enterprise-IT-grade secure-socket connectivity.*

*Plus, all Niagara Defense-in-Depth features at Supervisory and JACE Levels*



*Coming soon...*

niagara  
remote™  
**FoxC**



**IN BETA RELEASE**

- ❖ To participate in FoxC Beta program you need to be running 4.15u4

## Niagara Remote™ With Fox C Is Now Available For Evaluation

- Seamlessly enable cloud-mediated, secure station-to-station communication between all Niagara Remote™ enabled devices.
- No VPN or static IP connection required.
- Enable one Niagara station to initiate outbound connections to another without inbound firewall rules.

\* Beta features are provided for evaluation and may be modified, suspended, or discontinued. Beta features should be used only as permitted under applicable Beta terms.

# NOW IN BETA



## FoXC

Niagara Network connectivity via Niagara Remote, which allows points, schedules, histories, alarms, etc between stations.

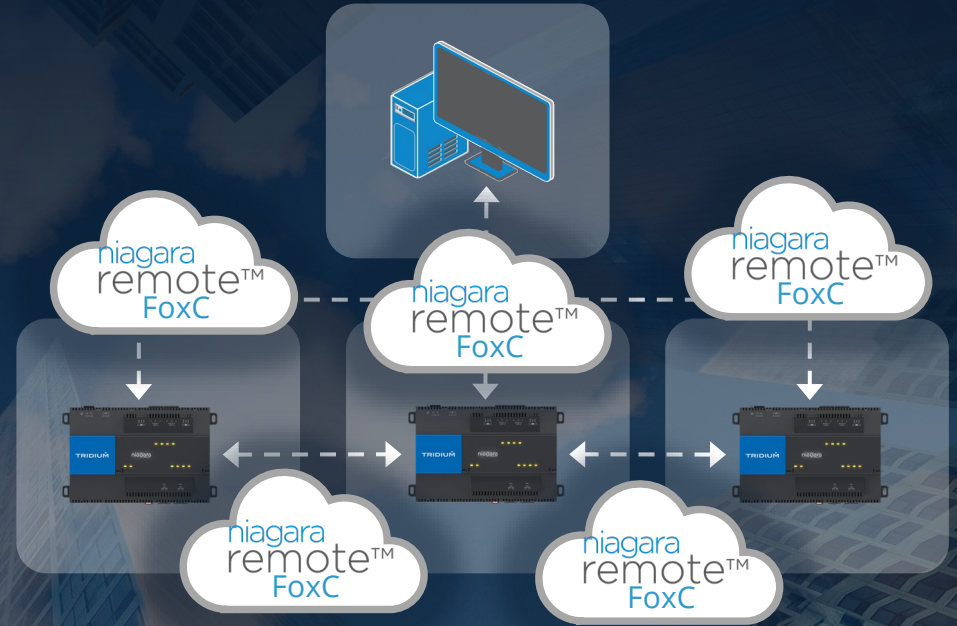
*No VPN, static IP connection or firewall penetration required*



# FoxC

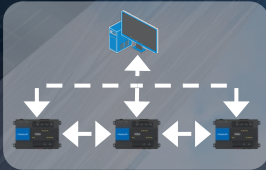
## STATION-TO-STATION

communication for Niagara devices located on **DIFFERENT** networks through **OUTBOUND PORT 443 WITHOUT** requiring a **VPN SOLUTION**



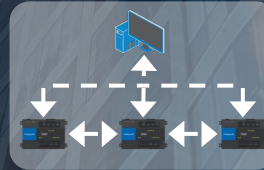
## FOX S

**STATION-TO-STATION** communication for Niagara devices located on the same network through **PORT 4911**



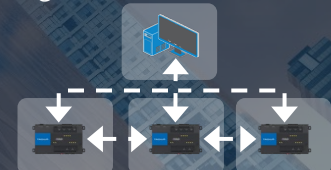
## FOX WSS

**STATION-TO-STATION** communication for Niagara devices located on the same network through **PORT 443**



## FOX WSS + VPN

**STATION-TO-STATION** communication for Niagara devices located on **DIFFERENT** networks through **PORT 443 & VPN**



# FoxC supports NEW USE CASES



EXAMPLE:  
**SECURELY**  
integrate  
multi-site Niagara  
devices to a  
**CENTRALIZED**  
Supervisor  
**WITHOUT a VPN**

**FoxC**  
extends  
the **VALUE**  
proposition of  
NIAGARA for a  
wide range of  
building & project  
types



**RETAIL**



**SCHOOL &  
HEALTHCARE**



**INDUSTRY &  
WAREHOUSING**



**DISTRIBUTED  
EQUIPMENT**

## **BENEFITS IN MULTI-SITE PORTFOLIO SCENARIO**

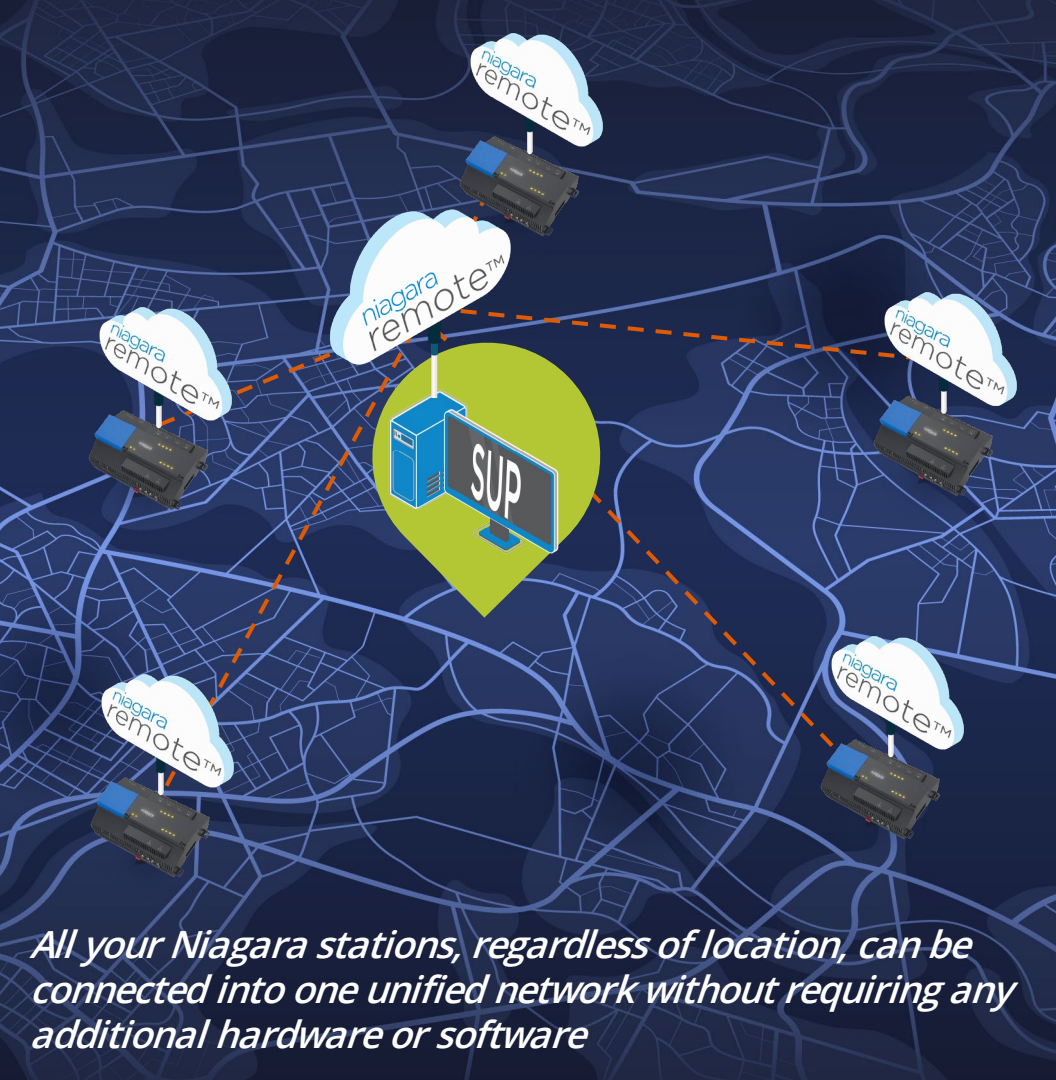
- Niagara network is extended over the Internet with security controls
- Bidirectional communication is enabled
- Users can monitor, control, and manage equipment at any location
- Isolated sites become fully integrated parts of your Niagara ecosystem
- No need for complex networking infrastructure with associated costs and cyber risks

## FOR OWNERS OF LARGE, DISTRIBUTED PORTFOLIOS

From a centralized Supervisor hosted in your facility or data center, every Niagara Remote™ enabled site can be part of the same seamless architecture with:

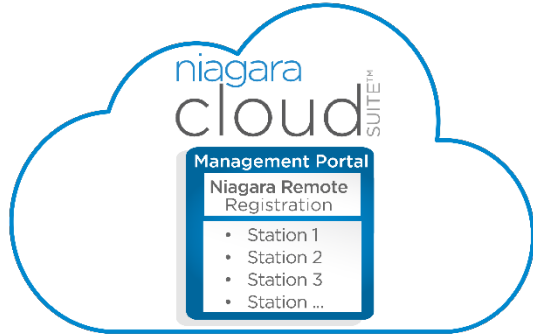
- Consistent management
- Shared data models
- Unified alarms
- Streamlined control strategies

This replaces traditional multi-site integrations and gives you a cleaner, scalable way to operate all your buildings as one system.

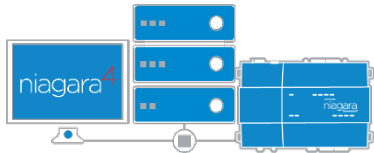
The diagram illustrates a unified network architecture for large, distributed portfolios. It features a central green heart-shaped icon containing a server rack and a monitor displaying the letters 'SUP', representing the centralized Supervisor. Surrounding this central hub are six Niagara Remote™ enabled sites, each consisting of a physical control rack connected to a cloud icon labeled 'niagara remote™'. Dashed orange lines connect the central Supervisor to each of the six remote sites, indicating a seamless network connection. The background is a dark blue map with white lines representing a city street grid.

*All your Niagara stations, regardless of location, can be connected into one unified network without requiring any additional hardware or software*

# HOW NIAGARA REMOTE™ WORKS



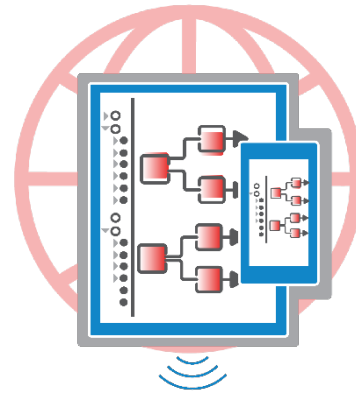
**Registration:** Subscribers register Niagara Supervisors and JACEs on Niagara Cloud Suite™ management portal.



**Connection:** Registered stations create a secure, outbound websocket connection on port 443.



**Log In:** Remote users log into the Management Portal from browser. Upon successful authentication, a remote access session is established over the station's websocket connection.



**Work Remotely:** Remote users can log on to Niagara Stations and do tasks inside Niagara applications, as if they were using an on-premises Niagara station. Web traffic is securely routed over websocket connection.



**Log Out:** Remote users log out from each Niagara station accessed during the remote session.

The logo for Niagara Cloud Suite, featuring the word "niagara" in a light blue sans-serif font, "cloud" in a larger, dark grey sans-serif font, and "SUITE™" in a smaller, dark grey sans-serif font to the right of "cloud".

niagara  
cloud SUITE™

Annual subscription  
per Niagara Station

## NIAGARA REMOTE

Part Name	Description
NCS-REMOTE-SUP	Supervisor-level subscription
NCS-REMOTE	Controller-Level subscription

1. Requires that the deployment is covered by an active Software Maintenance Agreement (SMA) and is running the current Niagara Framework release or the Long-Term Support (LTS) version [4.10]
2. Niagara Reseller partner must sign the Niagara Cloud Suite reseller addendum before they can purchase this service.

**NOTE:** Availability of cloud services may vary by country or region due to applicable regulatory requirements.

**Niagara Remote™  
subscriptions can  
also be purchased  
as a bundle with  
Niagara Recover™  
when ordered as  
part of a Niagara  
Software  
Maintenance  
Agreement.**



A Niagara Cloud Suite SMA 3- or 5-year subscription bundle includes an active Software Maintenance Agreement, Niagara Recover and Niagara Remote

Part Name	Description
NCS-SMA-8005-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-8005-[3YR, 5YR] Maintenance
NCS-SMA-8010-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-8010-[3YR, 5YR] Maintenance
NCS-SMA-8025-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-8025-[3YR, 5YR] Maintenance
NCS-SMA-8100-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-8100-[3YR, 5YR] Maintenance
NCS-SMA-8200-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-8200-[3YR, 5YR] Maintenance
NCS-SMA-9005-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-9005-[3YR, 5YR] Maintenance
NCS-SMA-9010-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-9010-[3YR, 5YR] Maintenance
NCS-SMA-9025-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-9025-[3YR, 5YR] Maintenance
NCS-SMA-9100-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-9100-[3YR, 5YR] Maintenance
NCS-SMA-9200-[3Y, 5Y]	NCS Recover and Remote [3 year, 5 year] bundle with SMA-9200-[3YR, 5YR] Maintenance



Data Sheet

niagara  
cloud SUITE™

**SMA  
BUNDLES**

# THANK YOU

To learn more about how to purchase and start using Niagara Remote™, please contact your Tridium account manager or Niagara partner.

This document is a non-binding, confidential document that contains valuable proprietary and confidential information of Tridium and must not be disclosed to any third party without our written agreement. It does not create any binding obligations on us to develop or sell any product, service or offering. Content provided herein cannot be altered or modified and must remain in the format as originally presented by Tridium. Any descriptions of future product direction, intended updates, or new or improved features or functions are intended for informational purposes only and are not binding commitments on us and the sale, development, release, or timing of any such products, updates, features or functions is at our sole discretion.

The background is a solid blue color. It features several stylized, light blue clouds of various sizes. Overlaid on these clouds and the background are faint, white line-art icons representing a technical or digital environment. These icons include gears, circuit boards, arrows, and various symbols associated with electronics and data processing. The overall aesthetic is clean and modern, typical of a corporate presentation slide.

# BACKUP SLIDES



# niagara cloud SUITE™

Niagara Cloud Suite is a scalable cloud-based solution that provides secure, remote Building Management Services in accordance with Tridium's model of open and extensible integration with devices, services, and applications.

## PREREQUISITES:

- Niagara Framework® Supported Versions
- Active Software Maintenance Agreement

# MORE ABOUT:

# niagara cloud SUITE™ Management Portal

- *Management by customer, by user and by role*

**niagara cloud**

**Craig's Controls**

**ALL CUSTOMERS**  [+ Create New Customer](#)

<b>VIDYA</b> 2 Projects   20 Devices	<b>VIDYA2</b> 0 Projects   0 Devices	<b>NEERAJ</b> 1 Projects   0 Devices	<b>CGTEST1</b> 1 Projects   5 Devices
<b>LOS POLLOS HERMANOS</b> 4 Projects   2 Devices	<b>TEST_CUSTOMER</b> 1 Projects   0 Devices	<b>TEST JULY</b> 0 Projects   0 Devices	<b>TEST-NEW-CUSTOMER</b> 1 Projects   0 Devices

## NIAGARA CLOUD

- Home >
- Users & Roles >

- *Credentials consistent with Niagara Community profile*

**niagara cloud**

**Users and Roles**

**ALL USERS**

1-15 of 19

NAME	EMAIL	ROLE
Nagendra Setty	nagendra.setty@honeywell.com	Partner Admin
Neeraj Bhawsar	neeraj.bhawsar@honeywell.com	Customer User

- *Customer views also supported*

**niagara cloud**

**Customer View: Vidya**

**PROJECTS (2)**

- All Projects
- Vidya-Project
- Test

**ALL PROJECTS**

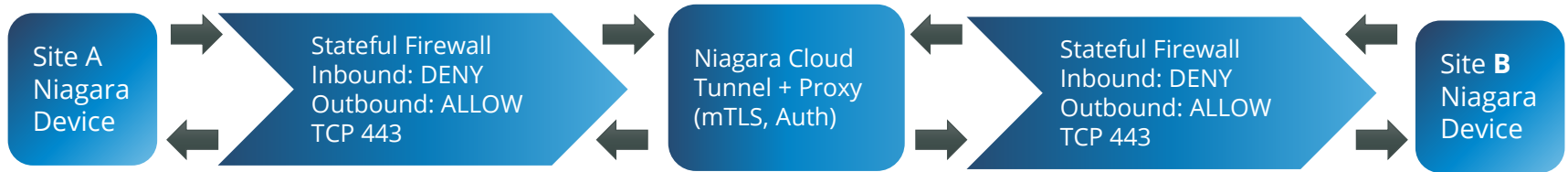
DEVICE/HOST ID	PROJECT/LOCATION	SUBSCRIBED SERVICES
mstagedevice1 N4:msncstage1:Test-C47F-2A5B-44DC-CAB8	Vidya-Project	Data Service
Test_Host_1 N4:NcsStation0A1:Test-4579-7E72-8CE0-985F	Vidya-Project	Data Service
NcsStation3 N4:NcsStation3:Test-41A4-E7E5-F83E-0419	Vidya-Project	Data Service

# ZERO TRUST PRINCIPLES

Niagara Remote applies Zero Trust principles by verifying device identity, authorizing only explicit connections, eliminating implicit network trust, encrypting all communication.

Category	Implementation	Security / IT Benefit
Network Access	Outbound-only connection to api.niagara-cloud.com over TCP 443, HTTP/WebSocket compatible	No inbound firewall rules; aligns with enterprise security policies
Transport Protocol	WebSocket over HTTP-compatible protocol	WebSocket-based Secure Tunnel used to transport Fox protocol traffic. Proxy-friendly and easy to allow in restricted networks
Encryption	End-to-end encryption using TLS 1.2 for all device-to-cloud traffic	Protects confidentiality and integrity of data in transit
Authentication	Mutual TLS (mTLS) and access tokens	Strong device and service identity verification
Inter-Device Communication(FoxC)	Cloud tunnel and proxy-based architecture	Secure cross-network communication without direct exposure

# FoxC NETWORK FLOW



## Example Firewall Rules:

1. ALLOW outbound TCP 443 from Niagara Devices to `api.niagara-cloud.com` (Stateful)
2. DENY all inbound connections to Niagara Devices
3. Allow ESTABLISHED, RELATED return traffic

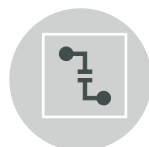
Even though devices communicate bi-directionally, the firewall never sees an inbound connection - only encrypted return traffic on an outbound-initiated, stateful session



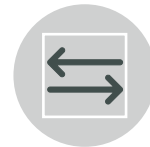
Devices initiate outbound TLS/WebSocket tunnels to the cloud



All inbound communication is delivered as return traffic over established sessions



Firewalls block all unsolicited inbound traffic.



Inbound communication occurs only as encrypted return traffic over outbound-initiated TLS/WebSocket tunnels.

# FoxC NEW USE CASES

Connect to Niagara devices outside your existing BMS network

