white paper

Cloud Security Principles for Niagara Framework® Products

SECURITY CERTIFICATIONS & COMPLIANCE

Niagara Cloud Suite™ is built on a foundation of industry-recognized security standards and independently validated assurance frameworks. These certifications demonstrate a strong commitment to protecting customer data, supporting operational resilience, and embedding security throughout the product lifecycle.

Tridium delivers enterprise-grade security for modern Building Automation Systems (BAS). Recognizing that security is a critical priority for cloud deployments, this document outlines the core protocols, safeguards, and standards built into Niagara Cloud Suite™ to protect customer data and operations.

ISO/IEC 27001:2022

Niagara Cloud Suite is certified to ISO/IEC 27001:2022, the global standard for Information Security Management Systems (ISMS).

This certification validates that the platform operates under a structured, risk-based security framework that is designed to support:

- Protection of data confidentiality, integrity, and availability
- Formal governance, risk management, and compliance processes
- Continuous monitoring and improvement of security controls

IEC 62443-4-1

Niagara Cloud Suite aligns with IEC 62443-4-1, an internationally recognized standard for secure product development in industrial environments. This enables:

- Security-by-design principles across development lifecycle
- Robust threat modeling and security testing practices
- Ongoing vulnerability management and timely remediation.

SOC 2 TYPE 2

Niagara Cloud Suite has undergone SOC-2 assessment, evaluating controls aligned to the Trust Services Criteria, including:

- Security
- Availability
- Confidentiality
- Processing Integrity
- Privacy

Sensiba™ SOC 2® Type 2

Achievement of SOC 2 Type II demonstrates that Niagara Cloud Suite's controls are not only appropriately designed but are consistently operating effectively over time, reinforcing the platform's commitment to robust security, reliability, and data protection. This attestation enhances customer trust by providing assurance of mature operational practices and strong governance across cloud service delivery.

TRIDIUM

niagara remote™

niagara recover™

niagara data service™

SECURITY OVERVIEW

The Niagara Cloud Suite offering provides new integration, connection, and deployment capabilities, building on Tridium's current model of open and extensible integration with devices, services and applications.

Niagara Cloud Suite™ is a scalable cloud-based solution that enables secure, remote building management services.

Built for the Niagara Framework®, Niagara Cloud Suite provides a secure and reliable source of building data that integrates seamlessly with the analytics platforms selected by the customer. It enables secure remote access (Niagara Remote™), cloud-based data storage (Niagara Data Service™), and automated backups (Niagara Recover™), all while improving cybersecurity, operational efficiency, and reducing onsite maintenance.

HOSTING & COMPLIANCE

Niagara Cloud Suite™ is hosted in Azure East US regions and is operated in accordance with industry best practices and compliance standards. Azure services are configured following the Center for Internet Security (CIS) benchmarks, which provide prescriptive security hardening guidelines. This includes secure configurations for storage accounts, networking to reduce attack surfaces. The underlying Azure infrastructure is certified against globally recognized standards such as ISO 27001, SOC 1/2/3. For details on Microsoft certifications and compliance, visit:

- Microsoft Service Trust
- Microsoft Compliance

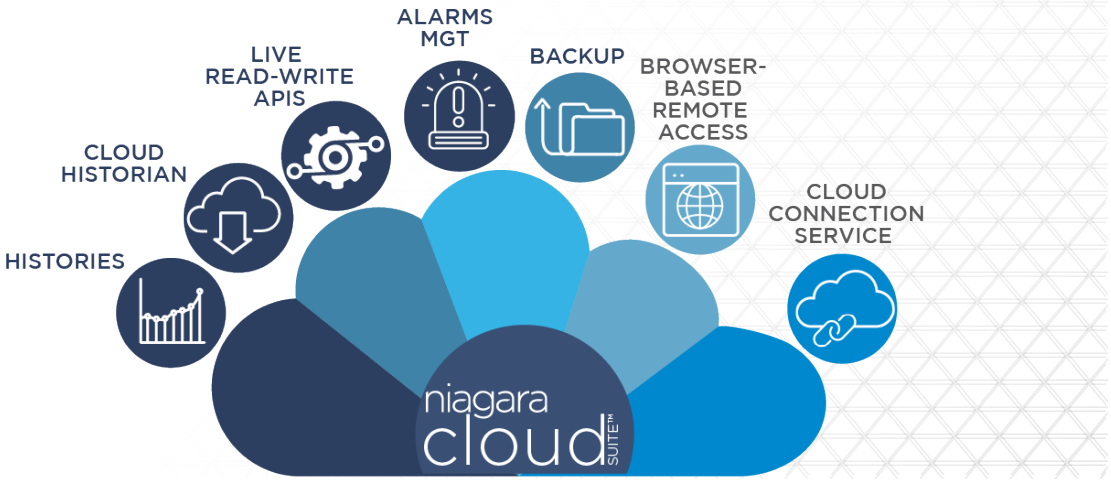
As one of the premier cloud infrastructure providers, Azure employs redundant systems designed to support network availability, power availability, cooling, and physical security controls, including biometric security access controls.

- Azure data centers implement barriers, badge readers, cameras, and environmental controls such as fire detection and temperature monitoring.
- 24-hour, 365-day year-round security including video surveillance, foot patrols, and perimeter inspections.
- Computing equipment housed in access-controlled state of the art steel containers.
- Facilities engineered for local seismic, storm, and flood risks.

ARCHITECTURE

Niagara Cloud Suite is designed for secure edge-to-cloud movement of building operational data. Niagara Framework® use cases vary in terms of where processing and storage activities should take place *on-premises* or *in-cloud.* Thus, Niagara Cloud Suite supports hybrid on-premises/cloud architectures, providing robust, enterprise-grade cyber security protections at exchange points in all its current service offerings.

CUSTOMER SERVICE DEMANDS



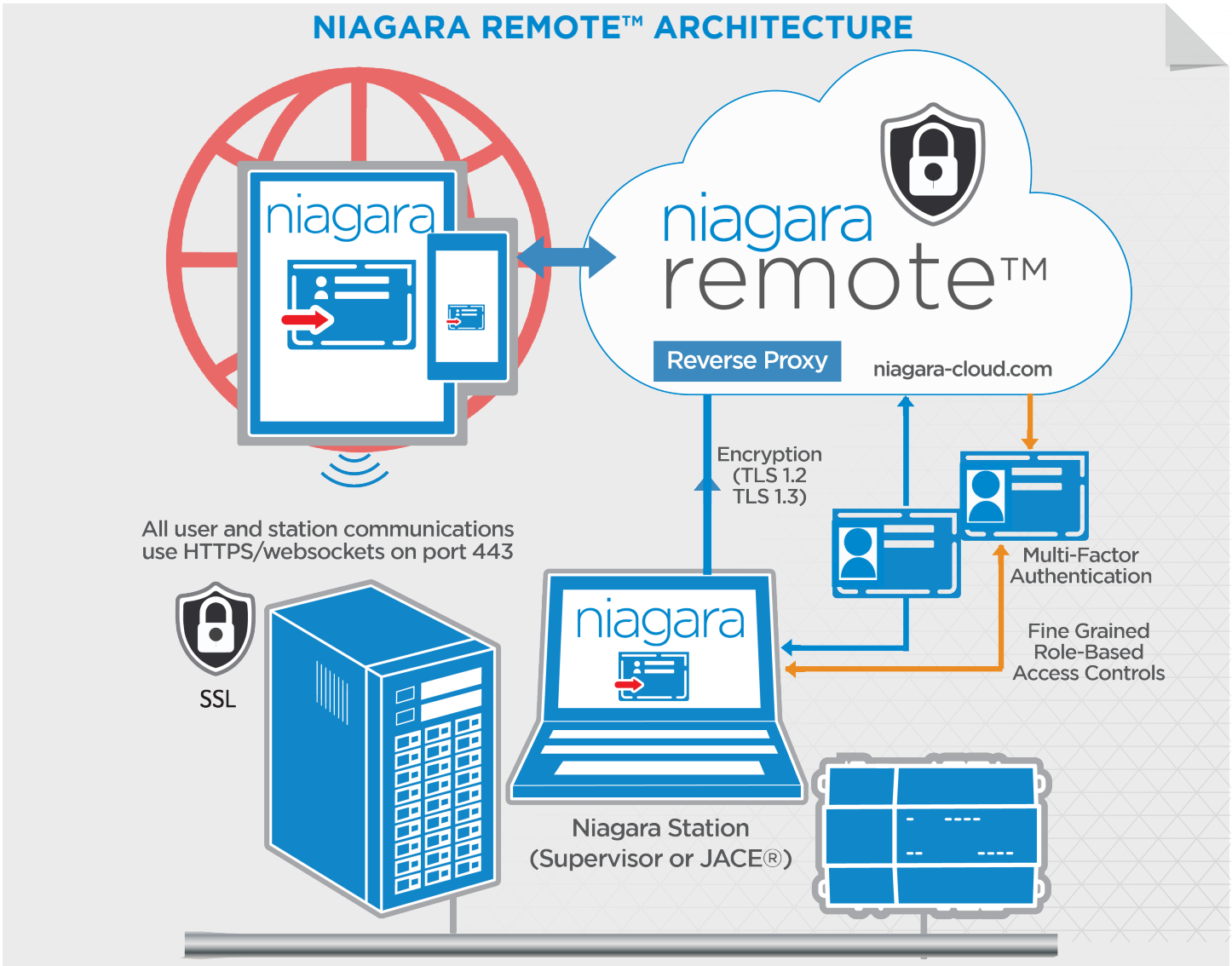
TRIDIUM

niagara remote™

Niagara Remote™

- Works with standard IT-network firewall technology.
- All user and station communications use HTTPS / web sockets on port 443.
- Enables one Niagara system to initiate outbound, remote access connection to another without inbound Firewall rules.
- The station uses a single endpoint api.niagara-cloud.com for all communication with NCS.
- MFA required for remote access to station.
- Fine-grained, role-based access controls allow user access to be managed at the station level.
- TLS1.2+ (TLS1.3 recommended) for all communications.

NIAGARA REMOTE™ ARCHITECTURE

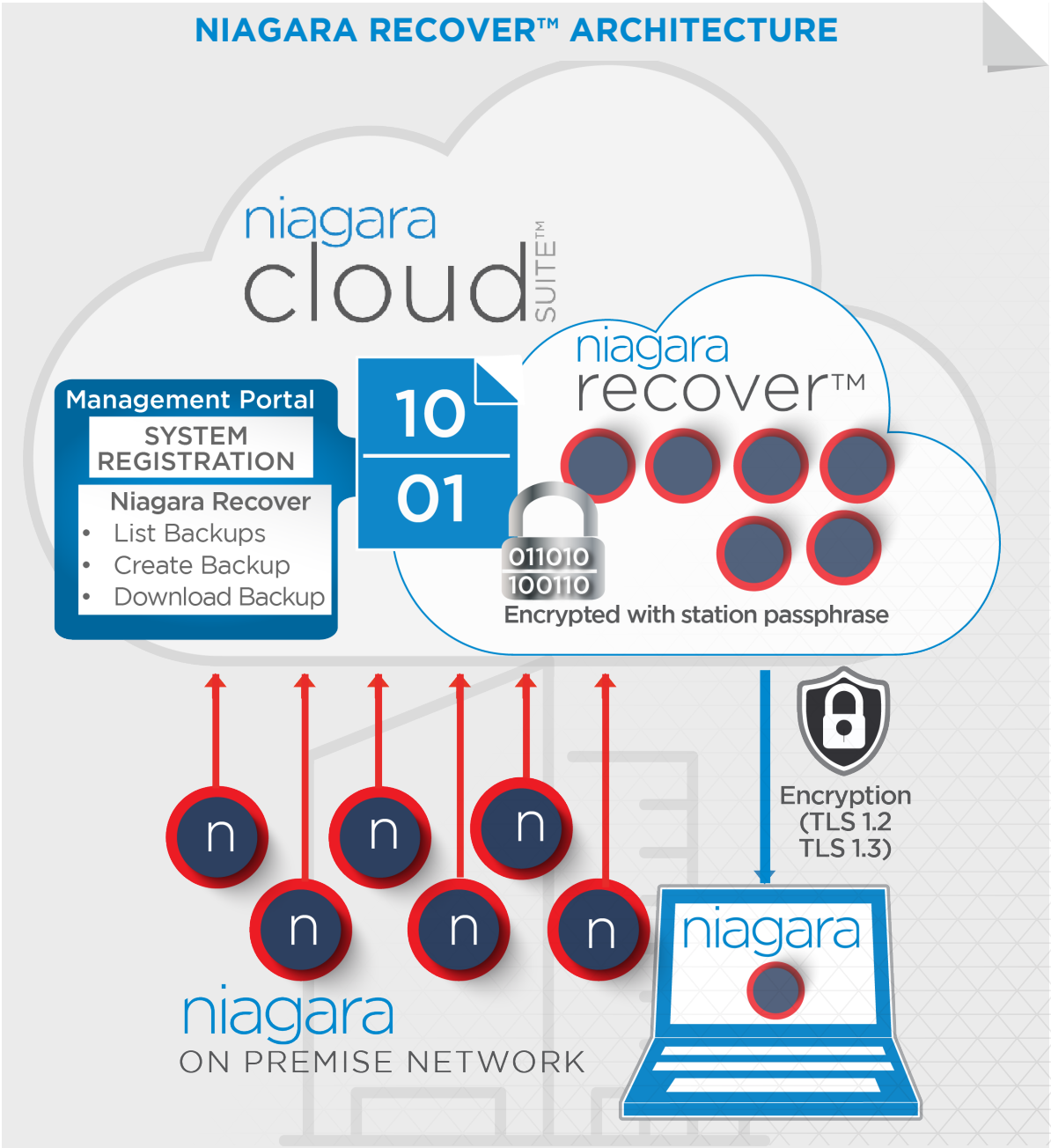


niagara recover™

Niagara Recover™

- Automated and on-demand backups.
- Secure data encryption in motion and at rest.
- Backup is encrypted using the station passphrase or a configured password.

NIAGARA RECOVER™ ARCHITECTURE

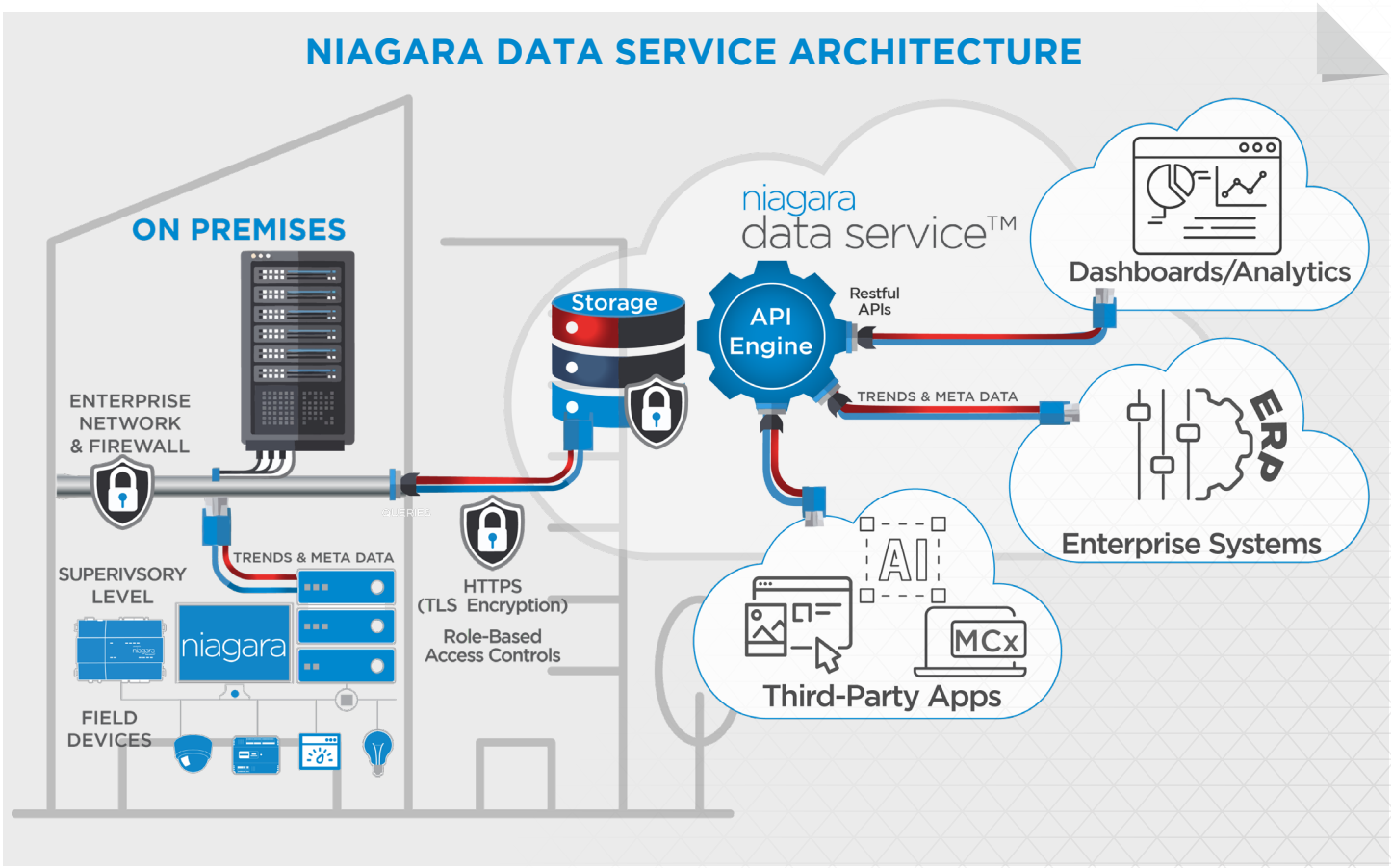


niagara data service™

Niagara Data Service™

- In-Transit Encryption: Data is primarily sent via AMQP with TLS encryption, protecting it against interception.
- Data Encryption & Access Controls: Stored data is encrypted at rest and can only be accessed via token-based authorization.
- API Gateway Protection: Restful APIs securely manage read-write queries, allowing third-party tools to interact with normalized data without exposing the local network.

NIAGARA DATA SERVICE ARCHITECTURE



TRIDIUM

AUTHENTICATION

User Authentication & Portal Access

- Community Login: The user logs in to the NCS Portal using their Niagara Community credentials.
- User Authentication: The portal validates and authenticates the user's identity based on their access permissions.

Service Account Setup & NDS API Access

- Create Service Account: Once logged in, the user creates a service account for their customer project.
- Generate Client Secret: The system generates a unique Client ID and Client Secret using the OAuth client credentials flow.
- Access NDS APIs: This Client Secret is then used as a bearer token to programmatically query and access the Niagara Data Service (NDS).

DEVICE REGISTRATION

- **Initiate Registration:** On the station side, the Niagara Cloud Service initiates device onboarding by making an outbound HTTPS request to the Niagara Cloud.
- Validate Entitlement (Subscription/Active SMA): The cloud checks if the station has a valid license and an active Software Maintenance Agreement (SMA) via a cloud connection service.
- Certificate-Based Registration: Upon confirming the active subscription or SMA, the cloud validates a Certificate Signing Request (CSR) and responds by signing and installing the Client Certificate on the device to complete secure registration.

NETWORK & SYSTEM SECURITY

Network follows segmented, zero-trust aligned architecture with isolated environments, NSG-based tiering, private endpoints, centralized inspection, and threat-intel-driven firewalling.

- Environment separation with unique VNets.
- Public/App/Data tiers with strict network security groups (NSGs).
- ExpressRoute + private endpoints for secure traffic.
- Enterprise API gateway with rate limiting and payload inspection.

APPLICATION SECURITY

All user/service authentication uses federated identity, MFA enforcement, token-based authorization, and strict role separation. Customer and device level authorization is enforced for every API call.

RBAC, least privilege, and Managed Identities are provisioned for service authorization. External access uses Azure Service Principals with rotated secrets. The Niagara Cloud Management Portal uses PingOne/Salesforce via federated OAuth2 with MFA.

DATA SECURITY

Data at Rest

- Storage-level encryption: All persistent and transient data (time series, logs, queue data, processor states) is encrypted at rest using Azure's platform encryption.
- Niagara backup: All the backups generated by Niagara Recover are stored in Azure blob storage and are encrypted using Station passphrase or configured password.

Data in Transit:

- NCS recommends using TLS 1.2 or above (TLS 1.3 recommended). Requests attempting to use TLS 1.1 or lower will be rejected.

ON-BOARDING WITH ENTERPRISE-IT-GRADE SECURITY FEATURES

PRIVACY & GOVERNANCE

Tridium, Inc., a wholly owned subsidiary of Honeywell International Inc., recognizes the importance of privacy to our business and customer trust. We are committed to handling all customer data responsibly. The Tridium privacy policy explains our approach to privacy and how individuals may exercise their rights:

As an organization focused on earning our customers' trust and handling their information assets with care, Tridium, Inc. strives to develop a strong compliance culture and robust security safeguards. You can find more information about our security practice by visiting Trust Security and Trust Compliance.

ABOUT TRIDIUM

Tridium is a global leader in business application frameworks that facilitate open environments for automation and control. Founded in 1996, Tridium revolutionized the industry with the introduction of the Niagara Framework®, a universal software platform that integrates diverse systems and devices, regardless of manufacturer or communication protocol.

The Niagara Framework enables seamless interoperability among various building systems, including HVAC, lighting, energy management, and security. Its open architecture allows for scalable and customizable solutions, empowering organizations to optimize operations, enhance efficiency, and achieve greater control over their facilities.

Tridium's commitment to innovation and excellence has established it as a trusted partner for system integrators, OEMs, and end-users worldwide. With a robust global community and a network of certified professionals, Tridium continues to drive advancements in building automation, IoT integration, and smart infrastructure solutions.

DISCLAIMER: This document is provided for informational purposes only and does not create any contractual commitment, warranty, or representation. The security controls described herein are subject to change without notice at Tridium's sole discretion and may vary based on product version, configuration, deployment model, and applicable customer agreement.

tridium.com

Support
North America & Latin America
support@tridium.com

Europe, Middle East & Africa
ordersEMEA@tridium.com

Asia Pacific
tsupportAP@tridium.com

2026 - 0011