Nureva® Console security
Introduction to Nureva Console

Nureva Console is a cloud-based device management platform (also available as a desktop application) with broad capabilities that make it simpler for IT to keep Nureva audio and other room systems on track while ensuring optimal performance.

Anyone with a user account (owner or admin) can manage and monitor the devices. A quick scan of the platform's dashboard lets these users know the status of each room — and available email alerts can inform them right away if attention is required. There's no need to go room to room to access systems. With remote management, firmware can be updated, devices and cameras monitored, assets managed and settings fine-tuned from anywhere.

Nureva Console provides powerful analytics and insights on room acoustics and usage. And alongside Nureva Console is the Nureva Developer Toolkit, a collection of easy-to-use APIs that enable the creation of seamless integrations for device control and management, third-party camera tracking, room acoustic and usage data and more. Pre-built integrations are also available.

Nureva Console is part of a family of audio conferencing products and services that deliver the simplicity IT and users have come to expect from their technology products. This can only be achieved with the advanced technology that we also apply to security for all our systems.

Nureva Console security

Nureva Console is designed and built with security and privacy at its core. Our strict security governance ensures security and privacy are built into every feature. To provide state-of-the-art security, we leverage industry leaders Microsoft and Okta. Furthermore, Nureva Console limits data exposure by not collecting and storing sensitive and personal meeting and classroom data. And since our platform is cloud based, there is no need for additional servers and the management, maintenance and security issues they may entail.

Secure data

Microsoft® Azure: Nureva Console is hosted on the Microsoft Azure platform. The service is segregated so that each customer has access only to their own devices, services and data. The data collected is stored in an encrypted Azure SQL Database within the Microsoft Azure platform.

Secure encrypted data: Data within the Nureva Console service is encrypted using 256-bit AES encryption while at rest and Transport Layer Security (TLS) 1.2 while in transit. We maintain an A ranking from Qualys® SSL Labs (ssllabs.com) for our certificate, protocol support, key exchange and cipher strength.

Secure access

Auth0 by Okta identity platform: Nureva Console leverages Auth0 by Okta for all identity and access management (IAM) services.

User authentication and access: Nureva Console employs an authentication/authorization service that uses standard OAuth 2.0 protocols to identify and authorize users accessing resources within Nureva Console.

Secure process

Security governance: Nureva implements an information security management system (ISMS) that complies with the ISO/IEC 27001 standard.

Secure by design: Nureva follows a secure software development process that ensures security and privacy are integrated throughout every phase of the development life cycle. All new features are tested, and the system is regression tested by a dedicated quality assurance team prior to release.

Service availability and disaster recovery: Nureva takes proactive steps by planning and testing our business continuity and disaster recovery capabilities to reduce the time and effort of recovering from a potential disruptive incident. If a security event is suspected to have occurred, our security incident process guides us through threat evaluation, containment of the event and notifying customers.

Security testing: We regularly engage an independent, accredited company to conduct vulnerability assessments and penetration tests of Nureva Console and other associated services based on STIRT, OSSTMM and OWASP methodology. Any high-severity vulnerabilities detected are immediately remedied and then retested.

Secure devices

Device authentication: A device is enrolled into Nureva Console using industry-standard OpenID Connect and OAuth 2.0 to authenticate it and to allow the device to be accessed by the user account.

Azure IoT Hub: All user interaction with enrolled devices in Nureva Console is done via encrypted communications using industry-leading TLS 1.2 communications.

Automatic software updates: Device software updates are sent out automatically to ensure they have the latest security updates.

Nureva security practices can be found at nureva.com/security-practices.

Privacy

DATA COLLECTION

Privacy standards: The Nureva Privacy Policy is modeled on accepted Canadian, American and European standards for the protection of personal information.

No capturing or storing of sensitive audio or video data: The Nureva devices do not store or record calls or any sensitive or personal meeting or classroom data.

Data residency: The Nureva Console service stores and retrieves data from an Azure SQL Database. Data stored in the Azure SQL Database is encrypted.

DATA RETENTION AND DELETION

Data retention: Nureva account data is encrypted and stored for 90 days within Nureva Console.

Data deletion: As stated in our privacy policy: "An Account Administrator may also contact us and request the deletion of all Personal Information related to a User from our system. Such requests should be sent to PrivacyOfficer@nureva.com."

Data privacy

WE COLLECT	WHY WE COLLECT IT
Nureva Console owner and admin names and email addresses	• Support the Nureva Console service account • Administer the account and for billing purposes • Authenticate and authorize users of the Nureva Console service • Communicate with account users
Actions performed in account	• Administer the Nureva Console service and improve its features and usability • Address bugs, errors and faults
Geographic area	• Administer the Nureva Console service and improve its features and usability • Address bugs, errors and faults
Device identifiers	• Administer the Nureva Console service and improve its features and usability • Address bugs, errors and faults
Log information	• Administer the Nureva Console service and improve its features and usability • Address bugs, errors and faults

CONFIGURING A NETWORK FOR NUREVA CONSOLE

You can find additional information regarding configuring a network for Nureva Console here.

For more information

Nureva Console Privacy Policy
nureva.com/nureva-console-privacy-policy

Nureva Console Security Practices
nureva.com/nureva-console-security-practices

Nureva Privacy Policy
nureva.com/privacy-policy

nureva®

We are Nureva

We believe that amazing things happen when people come together. They imagine greater possibilities, create better solutions and find greater joy in how they work and learn. It's why we create and support truly original solutions that make it astonishingly easy for our customers to connect and collaborate no matter where they are.

Connect

Nureva Inc.
sales@nureva.com
1.403.699.9781

Book a live demo   **Contact sales**