Nureva® Console security

Introduction to Nureva Console

Nureva Console is the cloud-based device management platform (also available as a desktop application) with broad capabilities that make it simpler for IT to keep its systems on track while ensuring optimal performance in each of your rooms. A quick scan of the platform's dashboard lets you know the status of each one of your devices – and available email alerts can let you know right away if your attention is required. There's no need to go room to room to access your systems. With remote management, you can perform firmware updates, monitor your cameras, manage your assets and fine-tune settings for any of your devices from anywhere.

You get powerful analytics and insights that let you know how your rooms perform acoustically. You'll also see how they are being used so you can identify opportunities for optimization. Nureva Console also includes the Nureva Developer Toolkit, a collection of easy-to-use APIs that let you create 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 delivers 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 is built into every feature. To provide state of the art security, we leverage industry leaders Microsoft® and Okta. Furthermore, Nureva Console limits your 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 (www.ssllabs.com) for our certificate, protocol support, key exchange and cipher strength.

Secure access

Okta Identity Cloud: Nureva Console leverages Okta Identity Cloud for all identity and access management (IAM) services

User authentication and access: Nureva Console employs an authentication/authorization service that uses standard OAuth2 protocols to identify and authorize users accessing resources within Nureva Console

Secure process

Security governance: Nureva implemented an information security management system (ISMS) that complies with the ISO27001 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 OAuth2 to authenticate it and to allow the device to be accessed by the user account

Microsoft 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 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
Your name and email address	• Support your Nureva Console Service account • Administer the account and for billing purposes • Authenticate and authorize Users of the Nureva Console service • Communicate with you
Actions you perform in your account	• Administer the Nureva Console service and improve the features and usability of it • Address bugs, errors and faults
Geographic area	• Administer the Nureva Console service and improve the features and usability of it • Address bugs, errors and faults
Device identifiers	• Administer the Nureva Console service and improve the features and usability of it • Address bugs, errors and faults
Log information	• Administer the Nureva Console service and improve the features and usability of it • Address bugs, errors and faults

CONFIGURING YOUR NETWORK FOR NUREVA CONSOLE

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

For more information

Nureva privacy policies can be found at nureva.com/privacy-policy.

Frequently asked questions

WHAT DATA IS COLLECTED WITH NUREVA CONSOLE?
We collect your name, email address, actions you perform in your account, device and location identifiers and log information. Please refer to the Information We Collect and Use section of the Nureva Console Privacy Policy for more information on what data we collect and why we collect it.

WHERE IS DATA STORED WITH NUREVA CONSOLE?
Nureva Console is hosted on the Microsoft Azure platform. The data collected is stored in an encrypted Azure SQL database within the Microsoft Azure platform.

HOW IS DATA STORED WITH NUREVA CONSOLE?
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. Please refer to the Nureva Console Security Practices for more information related to security.

WHAT PRIVACY ACCREDITATIONS DOES MICROSOFT AZURE INCLUDE?
Microsoft Azure cloud services have extensive built-in security controls that Microsoft advises conform to the following security and privacy accreditations: ISO/IEC 27001, 27018, GDPR, SOC1, SOC2, SOC3, FedRAMP, PCI, NIST, EU/US Privacy Shield.

More information about Microsoft Azure cloud services can be found at microsoft.com/en-us/trustcenter.

HOW LONG IS DATA STORED WITH NUREVA CONSOLE?
Account data is stored for 90 days within Nureva Console. Furthermore, 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."

WHAT SECURITY DOCUMENTATION IS AVAILABLE FOR NUREVA CONSOLE?
Information relating to security and general practices for Nureva Console is available at nureva.com/nureva-console-security-practices.

DO WE RECORD VIDEO AND AUDIO FROM MEETINGS?
No. The information about the data we collect and why it is collected is documented within the privacy policy for Nureva Console and the security practices for Nureva Console.

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**