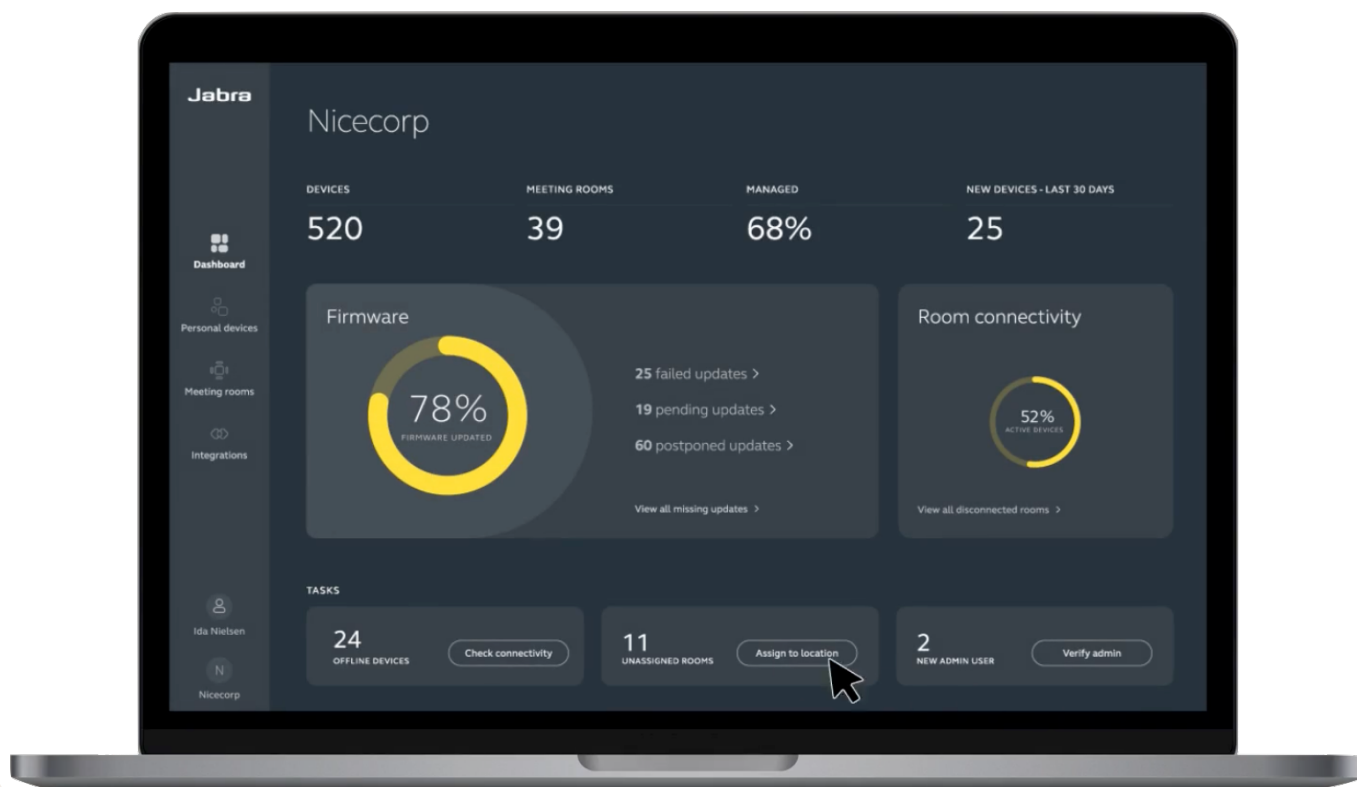




SECURITY WHITEPAPER

Protect personal privacy and sensitive data with Jabra+

Jabra+

Jabra+ is a multi-tenant, cloud-based, software-as-a-service (SaaS) solution for remotely managing, supporting, and integrating Jabra devices in enterprise environments, providing you with advanced data insights and data collection.

This whitepaper outlines Jabra's approach to security and compliance in the context of Jabra+. It addresses security-related aspects in the Jabra+ architecture, including data encryption, access security, content security, and other considerations.

Specifically, Jabra+ uses an industry-standard infrastructure and services for a secure, reliable, scalable solution that protects sensitive data and secures communication channels.

To expand on the following topics, you can request the **Jabra+ Security Framework Guide** from your Jabra representative, which can provide more detailed insights.

COMPONENT SECURITY

Jabra devices are securely connected to Jabra+ through a software client, facilitating remote management of Jabra devices, allowing IT admins to adjust settings, deploy firmware policies, and more via Jabra+ applications and web services.

The Jabra+ architecture considers security measures for the individual technical components, using the Azure Key Vault service to sign and store certificates. This secures data exchanges to/from physical Jabra devices to Jabra+.

When it comes to Jabra devices' firmware, the files are signed to ensure that only Jabra firmware files can be installed on Jabra devices. This prevents unauthorized or malicious firmware from being installed, reducing the risk of security vulnerabilities and ensuring the integrity and security of the devices and their firmware.

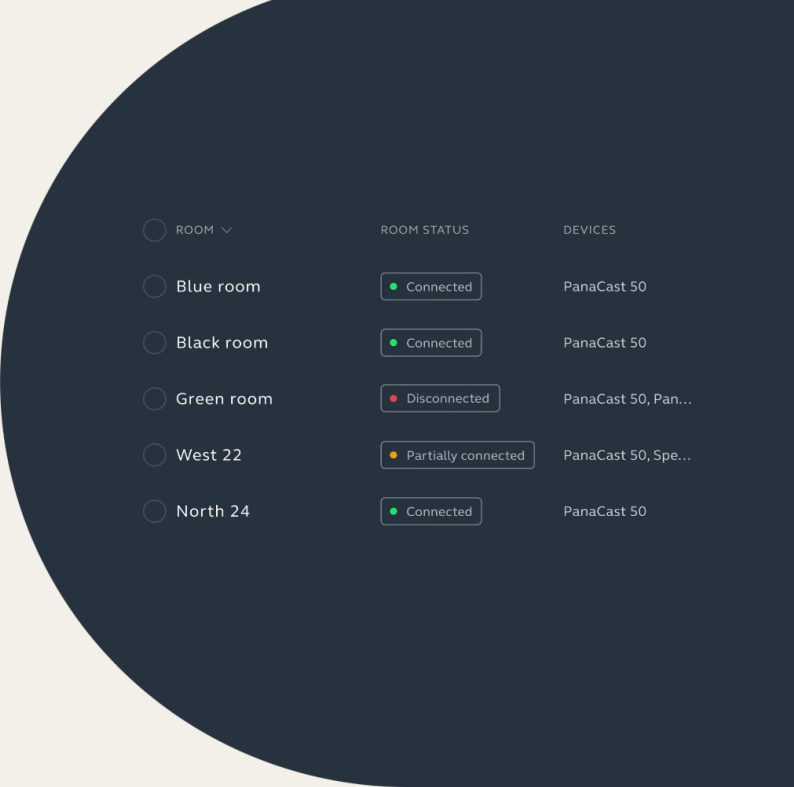
Arrange things to suit you

With Jabra+ for Admins you can clearly categorise information by room, group or individual device to make assessing their status swift and seamless.

The screenshot shows the Nicecorp mobile app interface. On the left, a sidebar lists locations under the 'Nicecorp' header: Delhi (9), Denver (9), Denver Room South (2), Denver Room West (7), North (3), South (4), Prague (6), and London (10). The 'South' location is highlighted in yellow, and a mouse cursor points to it. On the right, the 'South' location details are shown. It has a 'ROOM STATUS' section with four rooms: Red room (Connected), Blue room (Connected), Black room (Connected), and Green room (Empty room). The 'DEVICES' section lists four devices: PanaCast 50, PanaCast 50, PanaCast 50, and PanaCast 50.

Set your own schedule

Thanks to automated firmware updates, you can optimize performance for as many devices and meeting rooms as you want - all at once, at whatever time suits you.



ROOM	ROOM STATUS	DEVICES
Blue room	Connected	PanaCast 50
Black room	Connected	PanaCast 50
Green room	Disconnected	PanaCast 50, Pan...
West 22	Partially connected	PanaCast 50, Spe...
North 24	Connected	PanaCast 50

Jabra+ Security

DATA & COMMUNICATION SECURITY

Data encryption in Jabra+ can occur at various points in the data lifecycle, both at rest and in transit. Data exchange between web services in Jabra+ is encrypted using security protocols such as TLS 1.2.

Encrypted data exchange also secures communication between software clients and Jabra+. With Jabra+, data is collected and managed securely using industry best practices.

The software clients also encrypt data when communicating with the Cloud Gateway, which acts as a bridge between the local environment and Jabra+, allowing bi-directional communication with the issuance of digital certificates. This secures data exchange between Jabra devices and Jabra+ cloud services such as storage, computing, and applications, which comprise the Jabra+ architecture.

DATA STORAGE ENCRYPTION

All customer data sent to Jabra+ is encrypted. Data residency is in the West Europe region (Netherlands) and is partitioned based on the organization.

Additionally, Jabra+ uses the AES-256 standard for structured data stored in a multi-model database service (Azure Cosmos DB) and unstructured data in Azure Blob Storage. Any database backups are encrypted and stored in a geo-redundant account.

With regard to data structure, in Jabra+, customer data is segregated through database partitioning, which enhances security by limiting exposure, improving access control, ensuring compliance, and facilitating better incident management, among other benefits. It is a crucial strategy in a comprehensive data security and privacy plan.

It is important to note that users of the Jabra+ platform cannot see each other's data.

Content Security and Governance

ACCESS SECURITY

There are authentication and authorization mechanisms for accessing Jabra+ web applications, including the use of Jabra's unified identity provider (UIP) authentication – which can also be federated with a partner's identity provider (IdP) – as well as predefined roles for authorization.

In this context, software clients use unique organization-specific keys to obtain temporary certificates for secure authentication, enhancing access control. The clients also communicate through an encrypted protocol, ensuring data confidentiality and integrity.

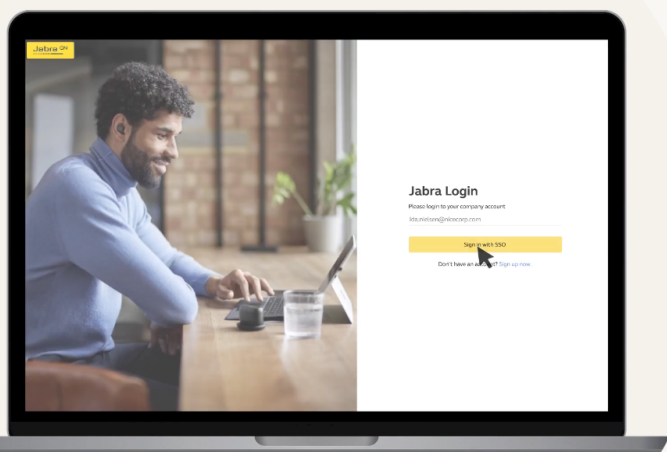
CONTENT SECURITY

With respect to content security, Jabra+ is built on the Azure Platform as a Service (PaaS) resource; data protection relies on native Microsoft Azure security features. Any transit data in Jabra+ uses Transport Layer Security (TLS) to authenticate and encrypt data securely.

DATA GOVERNANCE

Concerning data governance, by default, no one at Jabra has access to any production resources, ensuring that all Jabra+ data is inaccessible to unauthorized parties. Moreover, all of Jabra's web apps that expose front-end files have a security layer (front-door) associated with them, effectively protecting your organization within Jabra+ from Denial of Service (DDoS) attacks, as well as a web application firewall (WAF) to protect from any vulnerability or exploit.

In the context of Room Management, activity logs let an IT admin see user interactions at an individual room level. Events are logged with their respective triggers. For example, a meeting room is assigned a specific configuration, or settings are changed.



Network & device security

Built on Microsoft Azure Suite of Services, Jabra+ for Admins is scalable and secure, with end-to-end encryption and single sign-on integrations to ensure your teams can easily access the platform and collaborate securely from anywhere.



Incident Response

In case of an incident, Jabra has a dedicated Security Center where you can get help and more information about reporting vulnerabilities, security advisories, and other security-related matters.

<https://www.jabra.com/es-es/supportpages/security-center>