Condeco Connect: Built for the Cloud

Description of Cloud Offering & Security Features

January 2018 | Document v1.1

Condeco Connect:
Built for the Cloud. Built to Scale

- Condeco Connect is based around a cloud-connected Condeco Touch meeting room screen that seamlessly handles room booking in MS Exchange

- The screens connect to the Connect Cloud environment for easy setup and control, requiring no on-premises software or complicated installation

- Connect is positioned as a premium solution for managing room bookings, with features that help drive meeting room efficiency and an improved user experience

- Without a server application, other room screen solutions on the market are unlikely to be able to provide these features: User authentication, RFID card reading, central configuration of screens and reporting

Fully Multi-Tenanted and Self Service

Based on Microsoft Azure’s industry-leading secure cloud platform

NEVER hold any passwords or sensitive info in Connect cloud

Secure by Design

Condeco Connect is:

- Built around Microsoft's Azure platform, with the most comprehensive compliance coverage of any cloud provider
- Fully utilises Azure secure scalability using latest Azure components such as:
  1. "Azure Service Fabric" - Scalable clusters of Virtual Machines, used to underpin key Microsoft products such as Bing & Skype

Connect is secure by design:

1. NO unencrypted endpoints: SSL throughout (HTTPS / Port 443)
2. NO unauthenticated endpoints: Valid credentials always required
3. External authentication using MS Azure "B2C AD" (for Connect Cloud Portal & Connect mobile app)

For more details on Azure's security credentials, please visit:
https://azure.microsoft.com/en-gb/support/trust-center/

Connect Data in the Cloud

We understand concerns about what data is stored in the cloud.
Remember: The Connect Cloud environment does NOT store any of the following:

- MS Exchange room mailbox passwords
- User’s or Admin’s MS Exchange passwords
- Wi-Fi network information or passwords
- Appointment titles
- Attendee information

What gets reported to the Cloud

Triggers for the screen sending data to the Connect Cloud for reporting are:

1. Meeting ends at normal time (original end or extended end)
2. Meeting ends early
3. The meeting is automatically cancelled (no-show)

Items sent to cloud for each meeting:

- Start time / End time
- Actual start time / Actual end time
- Auto cancelled (Y/N)
- Booked at screen (Y/N)
- Booker email address
- Room identifier
- Account/customer identifier

Meeting Room A
08:30
Available until 12:30 today
Next meeting
PC Consulting Catchup 13:00 - 13:45
08:30
08:45
09:00
09:15
09:30
09:45
10:00
10:15
10:30
10:45
11:00
Tuesday 18 June
CONDECO

SECURITY FEATURES

Information Security Layers

Condeco strive to provide our customers with the most secure solutions and services. For this reason we continuously improve our already outstanding levels on Information Security.

Condeco Connect security is organised into three different layers, as follows

1. Connect software platform
2. Connect IT infrastructure
3. Condeco Information Security

All three layers contribute to deliver a secure service and protect customer's data.

Connect Software Platform

The security of the Connect platform is addressed from the very beginning. From the design phase, to the integration and then the deployment. The following three controls are in place:

a) Security by design
Connect is developed adopting an Agile methodology which adheres to the OWASP guidelines. In particular, Vulnerability Assessments are performed through industrial tools in the following phases

i. at module level, during the development of every storyboard

ii. at build level, after the integration of the different modules

b) Quality Assurance
A team of more than 20 testers (and growing) validate and perform penetration testing on the different releases, in separate staging environments

c) Vulnerability Assessment and Penetration Tests
Every major release* of Connect is penetration tested by an external independent organisation. Vulnerability assessments are performed as well.

**Current release is expected to be tested in September/October 2017*

Connect Scalability

Connect has been designed form the ground up to be scalable. Many of the architectural choices, designs and components were chosen in relation to providing a truly scalable service.

Microservice Architecture

- Connect is built as a series of microservices. This allows the product, or moreover, particular parts of the product to be scaled independently, allowing services bearing the heaviest load to be increased.
- The architecture also allows us to scale service instances dynamically to meet demand.
- Micro-services run on Microsoft's Azure Service Fabric which can be scaled vertically, for example bigger/more capable virtual machines and horizontally, for example more virtual machines.
- Azure Service Fabric underpins many of Azure's biggest services – for example CosmosDB and Bing

IOTHub

- IOTHub is an Azure service for management and control of devices.
- At the basic tier, IOTHub, supports millions of devices and a throughput of 6 million messages a day.
- IOTHub can be scaled vertically, increasing the throughput limit of a single hub, and horizontally, increasing the number of hub's used, to meet capacity requirements.

Connect IT Infrastructure

Connect is deployed through the Microsoft Azure platform, the most secure Cloud platform on the market. Why Microsoft Azure? …Their Cloud infrastructure is far superior to on-premises data centres for hosting applications, data and services.

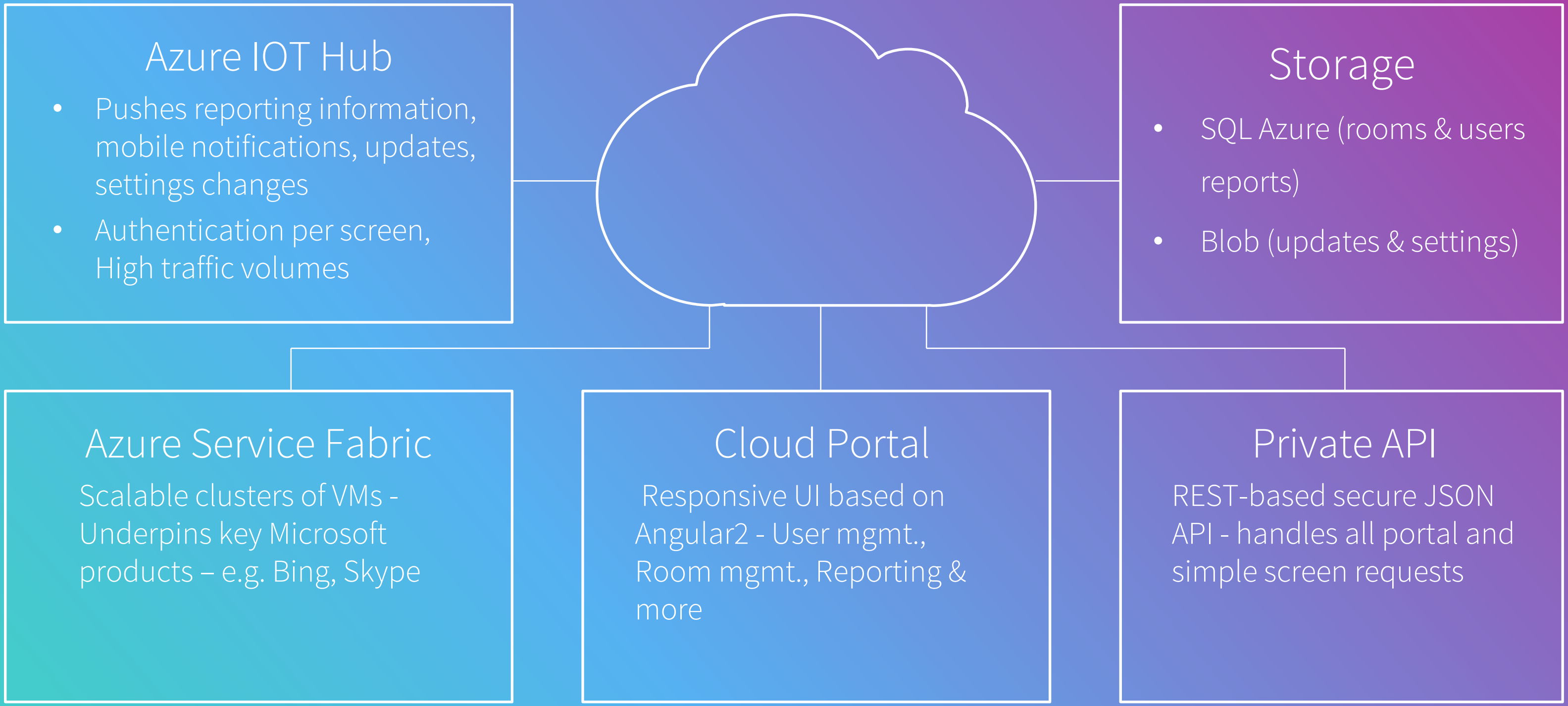
a) Security
Built-in security features, encryption, industry standard and best practices for physical security measures, industry accepted security certifications, biometrics access controls of physical assets, servers, buildings and overall data centres

b) Reliability
Fire suppression, redundant data and power systems, fail over to a co-located data centre

c) Accessibility
All servers hosted within the Cloud are all Virtual Machines (VMs) that are easily managed from the web

d) Uptime
Condeco Connect comes with a 99.5% uptime guarantee. This is underpinned by rigorous service level agreements with Microsoft Azure, many of which are at 99.9% uptime guarantee

Key Cloud Components for Connect



Azure IOT Hub

- Pushes reporting information, mobile notifications, updates, settings changes
- Authentication per screen, High traffic volumes

Storage

- SQL Azure (rooms & users reports)
- Blob (updates & settings)

Azure Service Fabric

Scalable clusters of VMs - Underpins key Microsoft products – e.g. Bing, Skype

Cloud Portal

Responsive UI based on Angular2 - User mgmt., Room mgmt., Reporting & more

Private API

REST-based secure JSON API - handles all portal and simple screen requests

Connect IT Infrastructure

Another feature of the Microsoft Azure platform that cannot be found on an on-premises data centre is its stability. In particular, the architecture of Azure platform provides:

- Redundant copies of data held at all times
- Fail over to backup server to minimize downtime
- Hosting applications on a minimum of two server instances to minimize downtime when hardware failure occurs
- Built-in redundancy, backup and many other features that allow for systems hosted in the Cloud to be far more stable

Connect IT Infrastructure

Microsoft's Azure platform has the following industrial certifications:

- ISO 27001 & ISO 27018
- CSA STAR Attestation (Level 2)
- HIPAA/HITECH
- CJIS
- SOC 1, SOC 2, SOC 3
- FedRAMP
- Singapore MTCS
- Australia CCSL
- UK G-Cloud

For further details, please visit the website:

https://www.microsoft.com/en-us/trustcenter/cloudservices/azure

Condeco Information Security

The security of every surrounding aspect of the Connect experience is critical such as supporting services and compliance. Condeco can prove outstanding levels of Information Security Management thanks to our own processes and corresponding certifications:

1. ISO 27001:2013

   Condeco operates a certified ISMS which includes in its scope: SaaS Global Support, Software Development and Data Protection (BSI certificate no. IS 665819)

2. CSA Star

   Condeco is engaged with BSI to obtain the Cloud Security Alliance Star certification, the most prestigious for Cloud security.

3. GDPR compliance

   Condeco is compliant with the new EU GDPR. Data Protection has been inserted inside the ISO 27001 certificate scope.

4. BCR

   Condeco has in place Binding Corporate Rules for Personal Data Transfer among its subsidiary all over the world. Approval by EU Authorities is expected by the end of 2018

5. IT Governance Steering Committee

   At Condeco, every Information Security issue is ruled by a Committee formed by five Directors and the Information Security Officer

CONNECT

For more information, please contact your Account Manager from Condeco

Or get in touch direct with our **Information Security team** by emailing:
InformationSecurity@condecosoftware.com

www.condecosoftware.com/connect

Our Global Reach | California | New York | London | Frankfurt | France | Stockholm | Zurich | Dubai | Singapore | Gurgaon | Sydney | Hong Kong

CONDECO