iviva Platform
Security Overview

Introduction

Eutech knows that the confidentiality, integrity and availability of our customers' data are vital to their business operations and consequently, to our success. Our platform uses multiple techniques and processes to ensure the that we meet our customers' growing demands.

iviva Product Overview

iviva provides enterprise-class smart workplace solutions to businesses of all sizes. The iviva platform consists of a whole suite of applications and technologies spanning Asset Management, Facility Management, Unified Communications and Real-Time Building Management.

Each class of applications has their own unique security concerns.
The iviva platform addresses this in a unique way by building all data access on an underlying framework while applications are built on a higher level specification that sit on on top of the framework.

So, as the framework is strengthened, the whole suite of applications automatically inherits it as well.

Data Center Access Control

iviva can be and is hosted on multiple cloud platforms such as Amazon Web Services.
It is also hosted through partnerships with large hosting providers. All hosting providers are vetted to make sure they comply with industry standards such as SASS 16 and ISO 27001.

System Entry Points

The only entry points for users to the iviva system is through the web interface and mobile applications. Web based authentication is used to authenticate the user and perform authorization on actions. Mobile applications are authenticated by a one-time code generated from the website.

Subsystems and 3rd party applications that integrate with iviva access the system only through an http based API.

Web access goes through IIS with a load balancer or reverse proxy in front of it. All entry points are as secure as the IIS server cluster being used.

User Sessions and Authentication

Users are authenticated at login and issued a security token which is re-authenticated with each request. Requests without a valid user session attached are rejected. Sessions auto-expire after a specific time.
For convenience, users are individually given the option of letting the browser remember their security token. However, on major events like password change and password reset, all security tokens are reset.

API Access

iviva provides an http based API for 3rd parties to integrate with. Use of the API requires an api key to be issued from the application and the key must be sent with each request. Each api key is associated with a set of privileges and API usage is controlled according to the api key.

Authorization

User authorization is managed by a three-tiered system:

Application Roles, User Roles, User Groups

Application Roles

Each application in iviva publishes a list of fine-grained application roles that control access to access to data and resources. There are hundreds of application roles available.

User Roles

User Roles are configurable and are defined in each application.
They typically map to the various use cases for accessing an application (an Operator, a Normal User, a Power User, an Admin User etc...)
Each user role is a collection of application roles.

User Groups

User Groups are a high-level, system-wide definition of the various personas in the organization. User Groups are configurable and define what applications and what user roles within each application are enabled.
Users in iviva are assigned to user groups.

Secure Transmission over a network

All communication between the client and server goes via SSL/TLS ensuring safe encrypted passage of data. Optionally, public key pinning and HTTP Strict Transport Protocol can be enabled for additional security.

Data Control

As a single iviva installation can potentially host many customers, it is paramount that data is isolated to prevent data leakage where one customer accidentally sees data from another.

The platform is architected to prevent this scenario from ever occurring. Each customer's data resides in a separate database (and possibly a separate database server). All data access goes via the underlying framework. Applications running on the iviva platform do not directly manipulate connections to the underlying database. All application code is sandboxed and runs in the context of a customer account, making cross-account data leakage improbable.

Even within a given account, applications have the ability to control data access using a novel technique called scoping. This allows applications to define data scopes for different user roles which are then applied at the database level, preventing data from ever being shown to a user who isn't authorized to view it.

Audit Logs

All major events in iviva are logged and recorded for auditing purposes. This includes user logins, failed logins attempts, issuing and deleting of api keys as well as all major application functionality.

Application-level audit logs are available through iviva’s user interfaces. Login activity logs can be provided as custom reports.

Backups and Disaster Recovery

Eutech works with our hosting partner and customer to provide the level of backup and disaster recovery your business needs. We support Sql Server Mirroring, Clustering and HighAvailability features.

We also do incremental and full backups according to customer requirements.

Customer data or backups will be used only during a disaster recovery situation or if approved by the customer for replicating data on to a non-production environment for testing the disaster recovery mechanism.

However if the customer approves a replication for any other testing purpose, customer details like contact numbers and email addresses will not be replicated on to the testing environment.

Disaster recovery mechanisms should be tested every 6 months with client approval, using the latest available backup on a non-production environment. Once the testing is completed, all replicated files and data will be deleted from the non-production environment.

Password Security

All passwords are hashed using bcrypt - a cryptographically secure hashing algorithm - before storing in the database. bcrypt has the novel property that its work factor can be cranked at up at any time, thus increasing the amount of computation required to calculate a hash and thus making brute force attacks unfeasible even with better hardware performance. Password hashes are salted, preventing rainbow table attacks

Individual user passwords are never revealed. However system administrators have the ability to reset user passwords. A 'forgot my password' option is available allowing users to reset their own password (this feature can be disabled on a per-customer basis).

SCADA Security

Real-Time monitoring and control is an integral part of iviva and special considerations are taken due to the sensitive and historically weak nature of SCADA security.

Typically, SCADA solutions in iViva are architected using a gateway system residing within the client building which talks to the central iviva server over http.
The gateway opens and maintains a persistent outbound connection to the server thus negating the need for client sites to open up the network to the outside.

The gateway system also acts as a bridge between the SCADA subsystem and the rest of the application suite. With this architecture, the SCADA subsystem can operate on an independent IP stack from the rest of the applications, relying on the gateway alone to manually and safely pass messages across. This allows the SCADA system to operate locally without having to lower its perimeter security.

Guarding against Application Vulnerabilities

iviva guards against common and lethal vulnerability patterns.
The following are examples.

Buffer Overflows

As iviva is built on higher level managed memory technology, buffer overflows are limited to those found in underlying components like IIS, the .NET Runtime Engine and Windows itself.

Cross Site Scripting

The html user interfaces generated by applications are done via a high level specification provided by the underlying framework. Applications do not directly generate raw unescaped html. The underlying framework ensures that all user data is safely encoded and escaped before being generated in the user interface.

Sql Injections

The iviva platform performs data access through pre-defined data models that auto-generate the required data access sql. No variable interpolation is done at any level and sql is carefully built using named parameters only.

Directory Traversal

Like most modern web frameworks, urls are internally mapped to specific actions in application code and never directly to physical files on disk.

Cross Site Request Forgery

All web based requests are verified against a randomly generated token, preventing malicious websites from forging requests on behalf of the logged-in user.

User Customizability

Customers can control their security to a certain degree. They can

- Host iviva on a private server with their own SSL certificates (and custom tcp ports if they choose)
- Manage their users' individual authorization levels through user roles and application roles
- Request hosting on a specific subdomain or top level domain
- Request custom password strength requirements for users
- Grant and revoke API keys for 3rd party software