Cloud Security

URL: https://www.mendix.com/evaluation-guide/enterprise-capabilities/cloud-security

1 What Kind of Security Controls Are Available in the Mendix Cloud?

Security controls for the Mendix Cloud include various levels of encryption, transport layer security (TLS), access restrictions, and node settings and permissions. The sections below describe these security controls in detail.

1.1 How Is Data in Transit Secured?

The Mendix Runtime that is running in a container is accessed via a load-balanced routing layer of clustered Nginx web servers that routes traffic to the relevant app environment, whereby the web server is responsible for the TLS connections. In addition, all common access and security services from the IaaS provider are used for the traffic that goes to their infrastructure. The TLS connection starting from the browser terminates at the web server service on the load-balanced routing layer. This ensures that data is encrypted end to end, so other app environments cannot intercept any data from the target app environment.

1.2 How Is Access Restricted for Incoming Requests?

Within the Mendix Cloud, it is possible to restrict access for incoming requests using multiple controls, by configuring access restrictions, you have fine-grained control over the external access to your application.

Restricting access within the Mendix Cloud is configured by access restriction profiles. An access restriction profile can contain any number of IPv4 and IPv6 address ranges, or a client certificate authority, or both.

This is an example of uploading a client certificate:

VIDEO

1.3 How Is Access Restricted for Outgoing Connections?

All inbound connections to applications in the Mendix Cloud are secured with TLS. And because your apps can also connect to other services on the internet, Mendix advises securing outgoing connections via TLS or TLS with client certificate validation.

TLS is the most common scenario, in which the client verifies the server certificate and sets up an encrypted connection. Trust is verified by verifying the chain of trust to a certificate authority in the client's trust store. Using encryption, data sent and received over the connection cannot be intercepted by other parties, so to authenticate the client, a username/password or token can be used with HTTP headers, for example. This can be used for services that natively support TLS.

To connect to your service from the Mendix Cloud, the service can be exposed on an external IP address and port. This can be firewalled to only allow the Mendix Cloud to connect to it.

TLS with client certificate validation adds the requirement that services being used validate the identity of your Mendix application, including encryption in transit using TLS.

1.4 Does Mendix Support Custom Domains?

For connections from the internet to your Mendix Cloud applications, we provide a *.mendixcloud.com* or *.mxapps.io* domain with a certificate managed by Mendix. For situations where pinning is required, you can set up a custom domain where you are in full control of updating the certificate.

1.5 How Is Access Management Handled for My Mendix Cloud Environments?

Fine-grained access management for your Mendix Cloud environments is handled for each of your applications in the Developer Portal. Each team member can subscribe or unsubscribe to alerts, and the **Technical Contact** of an application can manage the various permissions of each team member per environment.

The sections below describe the various development team roles used in node settings.

1.5.1 What Team Role Manages Mendix Cloud Environment Access?

Users with the Technical Contact role can manage all the settings in the cloud node and can edit the privileges of regular development team members with the view, deploy, and monitor permissions. Other team members are restricted in what they can manage.

A cloud node always has only one Technical Contact (while any number of team members can have view, deploy, and monitor permissions).

Only the Technical Contact can give their user role to another team member (after this, the new user has the Technical Contact role, and the old user does not).

The Technical Contact receives the following alerts from the cloud node:

- **Notifications for maintenance** from Mendix Support
- **Alerts** from the node when problems arise

- For example, CPU load is high, running out of disk space
- The Technical Contact cannot turn these alerts off

1.5.2 Who Is the First Point of Contact for Incidents & Changes to the App?

The Technical Contact is the first point of contact from Mendix Support about the application. The Technical Contact can submit requests for the cloud node with the following request types:

- **Incidents** – for example, when the app is down
- **Standard changes** – requests to add cloud resources, change the Mendix app URL, create a new app, obtain or renew a license, reset Google authenticator

1.6 Which Types of Access Control Are Available for My Mendix Cloud Environment?

Node permissions provide fine-grained access control to the management of your application. The node permissions that can be configured are described below.

1.6.1 Transport Rights

With transport rights, you can deploy new versions of the application to the node. You can create new deployment packages, stop and start the environment, and change configuration settings such as constants and scheduled events.

1.6.2 Access to Backups

This permission grants access to the backups of the environment. You can view, create, download, and restore a backup.

1.6.3 Receive Alerts

When the option to receive alerts is turned on in the Developer Portal, the user will receive an email when an alert is triggered. Alerts are triggered when the application goes offline unexpectedly, the app logs a critical-level message, a health check fails, or various infrastructure problems occur.

1.6.4 API Rights

With the API rights, you can use the Deploy API to get programmatic access to the environment. Naturally, the API does not require two-factor authentication, so API access is disabled for the production environment by default. The Technical Contact can assign API access for each user. Note that the API rights are needed in addition to the other permissions, so in order to access backups via the API, you will need both the access to backups permission as well as API rights.

1.6.5 Access to Monitoring

With this permission, you can view the application metrics, logs, and alerts in the Developer Portal. This allows you to successfully operate your Mendix Cloud environments.

2 What Backup Functionality Is Provided by Mendix?

A backup of all data (model, database, and file storage) is made on a daily basis for the acceptance, test, and production environments. Backups are stored in secured locations that are geographically dispersed.

Backups are available for restore as follows:

- **Nightly backups** – maximum 2 weeks history (counted from the day before the request)
- **Sunday backups** – maximum 3 months history (counted from the day before the request)
- **Monthly backups** (1st Sunday of each month) – maximum 1 year history (counted from the day before the request)

Both production data and backup data utilize cloud storage and are subject to the storage limit associated with the Mendix Platform subscription purchased. Companies are advised to set up an internal protocol for the usage and testing of backups. Administrators can download backups from the Developer Portal or develop automated downloads of backups using the Mendix Platform REST API. Mendix also offers the option to use live data replication in order to enable a fallback environment.

2.1 How Does Mendix Mitigate Disasters?

The Mendix Cloud has multiple mitigations for disasters, including high availability with deployment to multiple availability zones, scaling, and auto-recovery.

Disaster recovery tests are performed quarterly on the Mendix Platform. These tests are reported in our ISAE 3000 Type II report, ISAE 3402 Type II report, SOC 1 Type II report, SOC 2 Type II report, SOC 3 Type II report, and ISO/IEC 27001:2013 certification.

2.2 Does the Mendix Cloud Offers High Availability & Auto-Recovery?

The Mendix Cloud offers high availability for all app environments, ensuring zero downtime in the case of a Mendix Runtime outage. Users are able to scale Mendix app environments using the Developer Portal. Furthermore, the Mendix Cloud enables auto-recovery and failover within the same availability zone.

For more details, see the sections How Does Mendix Cloud Offer High Availability?, How Does Mendix Provide Disaster Recovery?, and How Does Mendix Cloud Provide Auto-Recovery & Auto-Healing? in *Cloud Architecture*.

3 What Kind of Encryption Is Provided in the Mendix Cloud?

Mendix offers encryption for data at rest and in transit for app environments out of the box. For more encryption control, Mendix supports the encryption of specific columns within application databases and makes it possible to encrypt uploaded files.

For details on routing and network encryption, refer to the section How Is Data in Transit Secured? above.

4 What Kind of Logging & Audit Trails Are Provided in the Mendix Cloud?

Mendix applies extensive logging of the whole application lifecycle. Logging is done not only on actions performed by the Mendix Runtime, but also on activities during the design, development, and deployment of an application. Accordingly, there is a full audit trail of all the relevant activities in an app, as well as who executed them and when they were executed.

The following sections go into more detail about the various levels of logging.

4.1 Can I Identify Who Defined Which Requirements?

The Mendix Platform supports the definition of requirements in the form of user stories (via the Projects module of an app project). Mendix logs actions related to the user stories in order to trace who defined which requirements.

4.2 How Is the Integrity of My Application Development Monitored?

The integrity of the application being developed is monitored by the Team Server, which allows you to link all change commits within a Mendix app to specific user stories and users. This enables you to trace who developed which part of your application and for what reason.

4.3 Which Deployment Activities Are Logged?

The Developer Portal is the component of the Mendix Platform that, among other functions, handles the deployment of application packages (called deployment archives in Mendix). Activities pertaining to deployment in the Developer Portal include the deployment and staging of apps across environments. In addition, backup and restore actions are logged, so there is full traceability of the administrative tasks performed.

4.4 Which Runtime Activities Are Logged?

The Mendix Runtime offers the option to log user behavior and object manipulations, enabling audit trails to the lowest level. Aside from standard log details (for example, active users), Mendix Studio and Mendix Studio Pro allow you to add custom logging. You can even add active alerts based on bespoke integrity triggers.

Logs are persistently stored in log files, and Mendix provides an API for subscribing to log events. Mendix also integrates with third-party tools like RSA for the encrypted storage of log files in environments where secure logging and auditing is required.

5 How Does the Mendix Cloud Support DTAP Environments?

The Mendix Platform deployment architecture is based on Cloud Foundry, which is the industry-standard cloud application platform used by SAP, IBM, Pivotal, and GE, among others. Cloud Foundry logically separates Mendix applications using containers. This includes an (optional) test, acceptance, and production environment, each running in their own app environment.

6 How Does Mendix Provide Containment Within the Mendix Cloud?

A Mendix Cloud node is a grouping of virtual and autonomous instances of the Mendix Runtime that is dedicated to your company. A Mendix Cloud node includes an (optional) test, acceptance, and production environment, each running in their own app environment. This app environment also includes firewall, web server, and database services. Mendix Cloud nodes run on Cloud Foundry containers. The purpose of an app container is to contain the behavior and consumption of an environment while shielding other environments (and apps) from each other.

Cloud Foundry uses **Garden containers** that have been designed to run applications and dependencies based on a buildpack. Garden containers consists of two layers: a read-only layer with an operating system root file system, and a non-persistent read/write layer for Mendix applications and dependencies.

Databases and files are also logically contained within the Mendix Cloud and Cloud Foundry. A database for a Mendix application is hosted on a separate instance of PostgreSQL, and this specific instance only allows traffic from this specific Mendix application.

As each app environment has its own dedicated web server and firewall services, Mendix supports customization at an app environment-level through the Developer Portal without affecting other app environments. For example, the customization of request handlers for a specific app environment is not compromised by the demands and desires of other Mendix customers.

The app environment setup allows test, acceptance, and production instances of the same application to operate identically but independently. Because the app environments are fully standardized, Mendix optimizes the combination of OS, integration software, and virtualization software while implementing the highest possible degree of security and performance. Furthermore, Mendix offers encryption for data at rest for app environments out of the box.

7 Does Mendix Establish and Maintain Baseline Configurations for Hardening?

The Mendix Security team has an established hardening security baseline based on international standards like SANS and CIS. This is audited by our independent third-party auditors and results in our annual published ISAE 3402 Type II report, SOC 1 Type II report, SOC 2 Type II report, SOC 3 Type II report, and ISO/IEC 27001:2013 certification.

8 Which Physical Security Controls Are in Place for the Mendix Cloud?

Mendix Cloud is hosted in industry-leading data centers, which are reviewed bi-annually for compliance by the certified Information Security Officers of Mendix. All the data centers possess third-party certifications and/or third-party assurance reports like ISO/IEC 27001:2013, SOC 2, and PCI-DSS.