Miradore

Security Information

Table of Contents

1 Our approach to information security

At Miradore, we have an Information Security Management System (ISMS) that consists of a comprehensive set of policies and procedures governing information security.

The goal of our ISMS is to ensure business continuity, prevent data breaches and protect the integrity, confidentiality and availability of information processed, stored or transmitted by Miradore.

Our internal Security Team is continuously working on improving our ISMS towards ISO 27001 certification. As part of the process, we collaborate annually with external auditors to test and validate the security of our products and services.

2 Security aspects of Miradore

This section discusses the security aspects of Miradore device management software.

2.1 TERMS OF SERVICE

These Terms of Service, including our Privacy Policy and Cookie Policy, define the terms and conditions under which you are allowed to use Miradore, and how we will treat your account while you are our customer:

https://www.miradore.com/terms-of-service/

2.2 PRIVACY POLICY

Miradore privacy policy describes the information collected on the users of Miradore service, and how the information is used and disclosed. The privacy policy is incorporated as a reference into the Miradore Terms of Service, and it is available at:

https://www.miradore.com/privacy-policy/

2.3 COOKIE POLICY

This Cookie Policy explains how Miradore uses cookies and similar technologies to recognize you when you visit our website, or any website or mobile application owned, operated or controlled by us. The Cookie Policy describes what these technologies are and why we use them.

Our Cookie Policy is available at:

https://www.miradore.com/cookie-policy/

2.4 COMMUNICATION MODEL

The data moving between a managed device and the service consists of the client polling the service for commands, the service returning the commands, and the client posting back the task results. The commands can include enforcement of configuration policy settings, software installations, and scheduled task results, e.g. hardware and software inventories. Additionally, the service can request a managed device to poll the service immediately through an applicable push notification service, if an instant synchronization is needed.

Miradore utilizes the industry standard HTTPS (TLS) protocols to secure network traffic. All communications between the end user and the user interface as well as the servers and the clients are encrypted. Additionally, all system passwords are stored in an encrypted form.

2.5 INTERFACES

This section discusses security of the different Miradore interfaces.

Connectors are used to interface with external systems such as Microsoft Active Directory. Miradore API (Application Programming Interface) can be used by Miradore users to query data in order to interface with their own site in the Miradore service.

2.5.1 THE MAIN USER INTERFACE

The main user interface i.e. the management console of Miradore is browser-based and it always employs the secure HTTPS protocol between the user and the service.

Users are authenticated with a username and a password, which must be at least eight characters long. The user passwords are salted and stored in the database as SHA-512 hashes and are thus not accessible for anyone. If a user forgets his password, he or she is able to reset his/her password by using the password recovery workflow that has been built-in to the service, and is available through the service login screen. The password recovery workflow sends an email to the user, containing a hyperlink for resetting the user's password. In addition, the users' identity can be verified using two-factor authentication upon every login.

All user connections to the service are logged. In addition, the service logs the user actions within the service, and displays them in the Action log, providing an audit trail.

2.5.2 WEB SERVICE API

Miradore API is a REST based web service which is intended for integrating Miradore with external information systems. It is used over HTTPS with GET method to export data directly from the database of Miradore in XML or JSON format. All API requests are authenticated with authentication keys, and the authentication keys are managed in the management console of each Miradore site. For more information about the API, see About Miradore API.

2.5.3 CONNECTORS TO THIRD-PARTY SYSTEMS

Importing data from external systems, e.g. Microsoft Active Directory, is handled by connectors. The network traffic between Miradore, and the connector is secured with HTTPS (TLS).

The connector authenticates with Miradore with an authentication key, which is generated automatically for each connector component. These authentication keys can be deleted from the management console of Miradore (*System > Infrastructure Diagram > Miradore Connector for Microsoft Active Directory*) in a similar way as the API keys are deleted.

In the target system, the connector is run by the logged in user account, but it is possible to configure the connector to be run by some other account as well.

2.5.4 MIRADORE IN THE MANAGED DEVICES

Devices communicate with the Miradore service server either through a custom program called the Miradore Client, or through the platform's integrated mobile device management framework provided by Apple (iOS), Google (Android) or Microsoft (Windows).

All devices are introduced to Miradore through an enrollment process, which is initiated either by the device user or site administrator. Either way, the enrollment is always authenticated with one-time enrollment credentials, which are created for that specific enrollment only. If the enrollment process is started by the site administrator, then the enrollment credentials are included in the enrollment invitation

message that is sent to the user either by email or SMS. But, if the device user is enrolling his or her device to Miradore as a self-service, then he/she will be asked to enter a specific company PIN code when enrolling the device via the enrollment portal (online.miradore.com/enroll). The self-service enrollment is only possible for users who are listed in the specific Miradore site as device users. After a successful enrollment, the user who got the enrollment invitation or performed the self-service enrollment, will be assigned as the user of the device in Miradore.

The vendor push notification services (Apple Push Notification Service, Firebase Cloud Messaging, Azure SignalR and Windows Push Notification Service) are connected to the managed devices and Miradore with HTTPS and vendor-specific protocols. Additionally, Miradore Client for Android platform uses cryptographic keys to authenticate connections with the Miradore service.

Regardless of the device platform, device users are always able to see whether their device is managed with Miradore. Usually there is a Client application or MDM profile visible to the device users.

2.6 SERVICE HOSTING

The Miradore service is hosted in the Microsoft's privacy focused Azure cloud in Germany. The service undergoes regular independent third-party audits for ISO/IEC 27001 compliance.

Network connections from Internet to the datacenter network are limited with firewalls to allow only connections over HTTPS (port 443) to designated web servers, and there is also a load balancer in between, which distributes the requests evenly amongst the web servers.

2.7 SERVICE MAINTENANCE

Only a limited group of people have access to the datacenter premises, and their visits are logged, and access is only permitted for maintenance or upgrade operations. Also administrative access to the servers through network is always logged.

All the server hardware, server software, operating system, and Miradore service updates are performed following a change management process, and manufacturer's recommendations.

2.8 BACKUPS

Database servers and front-end web servers hosting Miradore are backed up on a daily basis, and the backups are stored for 3 months.

We have a recovery procedure that has been practiced and tested. The recovery procedure is always carried out by Miradore support technicians. In the case customer has accidentally deleted some data, the recovery service is chargeable with an hourly rate.

2.9 SERVICE BREAKS

Server hardware, operating systems, and Miradore service are continuously being monitored and server responsible persons will be alerted if there happen any deviations in the service operability. If any deviations or service breaks take place, Miradore will inform the users of Miradore about the break and its duration.

Target uptime for the service is 99,7%.

2.10 CREDIT CARD INFORMATION

Miradore does not store any credit card information. Customer credit card details will be securely stored in encrypted form by Braintree https://www.braintreepayments.com/, a company owned by PayPal, and they will never be given to any third party. Miradore is a PCI compliant merchant: https://articles.braintreepayments.com/reference/security/pci-compliance.

3 Further questions

Further information can be requested by contacting Miradore support via telephone at +358 45 1207 056, by sending an e-mail to support.online@miradore.com, or by sending feedback using the Contact us form that is provided our website at www.miradore.com.