Technical Reference

# Miradore Online

# Security Information

# Technical Reference

## Table of Contents

# 1 SECURITY ASPECTS OF MIRADORE ONLINE

This section discusses the security aspects of Miradore Online.

## 1.1 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 Online, and how we will treat your account while you are our customer:

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

## 1.2 Privacy Policy

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

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

## 1.3 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/

## 1.4 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 Online 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.

### 1.5 Interfaces

This section discusses the encryption and security of the interfaces and the communications between entities as presented in Figure 1. Connectors are used to interface with external systems such as Microsoft Active Directory. Miradore Online API (Application Programming Interface) can be used by Miradore Online users to query data in order to interface with their own site in the Miradore Online service.

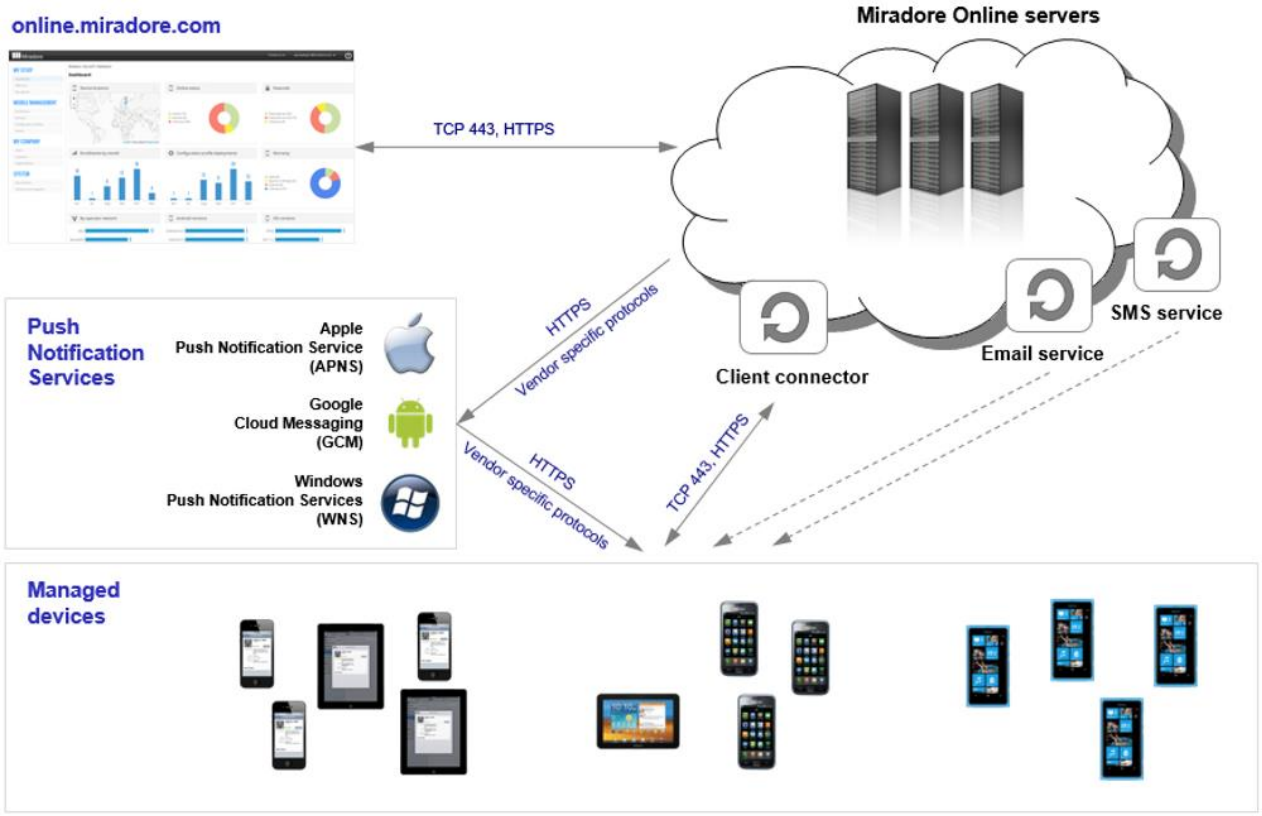


Figure 1: Communication Infrastructure and Interfaces

#### 1.5.1 The Main User Interface

The main user interface i.e. the management console of Miradore Online 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.

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

### 1.5.2 Web Service API

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

### 1.5.3 Connectors to Third-Party Systems

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

The connector authenticates with Miradore Online with an authentication key, which is generated automatically for each connector component. These authentication keys can be deleted from the management console of Miradore Online (*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.

### 1.5.4 Miradore Online in the Managed Devices

Mobile devices i.e. *assets*, that are managed with Miradore Online, communicate with the Miradore Online service server either through a custom program called the Miradore client (Android platform), or through the platform's integrated mobile device management framework provided by Apple (iOS), Google (Android), or Microsoft (Windows Phone and windows 10).

All devices are introduced to the Miradore Online mobile device management solution 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 Online 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 Online 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 Online.

The vendor push notification services (Apple Push Notification Service, Google Cloud Messaging Service, and Windows Push Notification Service) are connected to the managed devices and to the Miradore Online service with HTTPS and vendor-specific protocols (Figure 1). Additionally, Miradore Online client for Android platform uses cryptographic keys to authenticate connections with the Miradore Online service.

Regardless of the device platform, device users are always able to see whether their device is managed with Miradore Online. On Android devices, Miradore Online shows as a client application, whereas on Windows devices it is visible as a Company app or Workplace account, and Apple iOS devices are managed with a management profile or profiles. In addition, the Android users are able to open the client application and change the connection settings between the client application and the service. They can, for example, define the interval how often the application should connect to the service.

### 1.6 Service Hosting

The Miradore Online service is hosted in the Microsoft's privacy focused Azure cloud in Germany.

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.

### 1.7 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 Online service updates are performed following a change management process, and manufacturer's recommendations.

### 1.8 Backups

Database servers and front-end web servers hosting Miradore Online 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.

### 1.9 Service Breaks

Server hardware, operating systems, and Miradore Online 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 Online about the break and its duration.

Target uptime for the service is 99,7%.

### 1.10 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 Online is a PCI compliant merchant:
https://articles.braintreepayments.com/reference/security/pci-compliance

## 2 FURTHER QUESTIONS

Further information can be requested by contacting Miradore Online 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 in the Miradore Online service.

## 3 CONTACT

Miradore Oy
Laserkatu 6
53850 Lappeenranta
Finland

Visit http://www.miradore.com/miradore-online/ for more information.