Technical Reference

See your IT more clearly

Miradore Security Information

Table of Contents

1 Executive summary 3
1.1 Fast Facts 3
1.2 About Us 3
1.3 References 3
2 Security aspects of Miradore 3
2.1 Interfaces 3
2.2 Stored passwords 5
2.3 Database access 5
2.4 Code signing 6
2.5 Distribution 6
3 Further questions 6
4 Contact 6

1 EXECUTIVE SUMMARY

This section provides a brief introduction to the history and references of Miradore Ltd.

1.1 Fast Facts

- Established in 2006
- Offices in Helsinki, Stockholm and Lappeenranta

1.2 About Us

Miradore was born when the global paper giant UPM needed a better way to manage their own IT infrastructure. Since existing options did not address the challenges they faced in a company with 20,000 workstations in over 30 countries, a custom solution was created. The pilot project and full-scale roll out was a success, and Miradore Ltd was founded in 2006 with UPM as the first customer. Because Miradore was built by IT professionals for IT professionals, we know the challenges faced on a daily basis:

- Fast growing workforce mobility and device diversity
- The demand for agile services instead of cumbersome infrastructure
- Composition of data from diverse systems to provide a big picture
- Abstraction of various device technologies into a simple, unified workflow
- Safeguarding the integrity and access to company data

And of course, for managed service providers, these IT infrastructure challenges are multiplied by the number of customers served.

Miradore provides a solution for overcoming these challenges. It helps to efficiently manage devices across their entire lifecycle. Miradore also provides tracking of overall network quality from one console - it aggregates data from existing systems including user directories, patching and security solutions to provide a unified big picture of the entire environment.

1.3 References

At present, Miradore is used to manage hundreds of thousands of assets all over the world. It is trusted by both public and private sector customers in industries ranging from retail to IT services to government and defense. Miradore is also the device management solution for dozens of international Managed Service Providers.

2 SECURITY ASPECTS OF MIRADORE

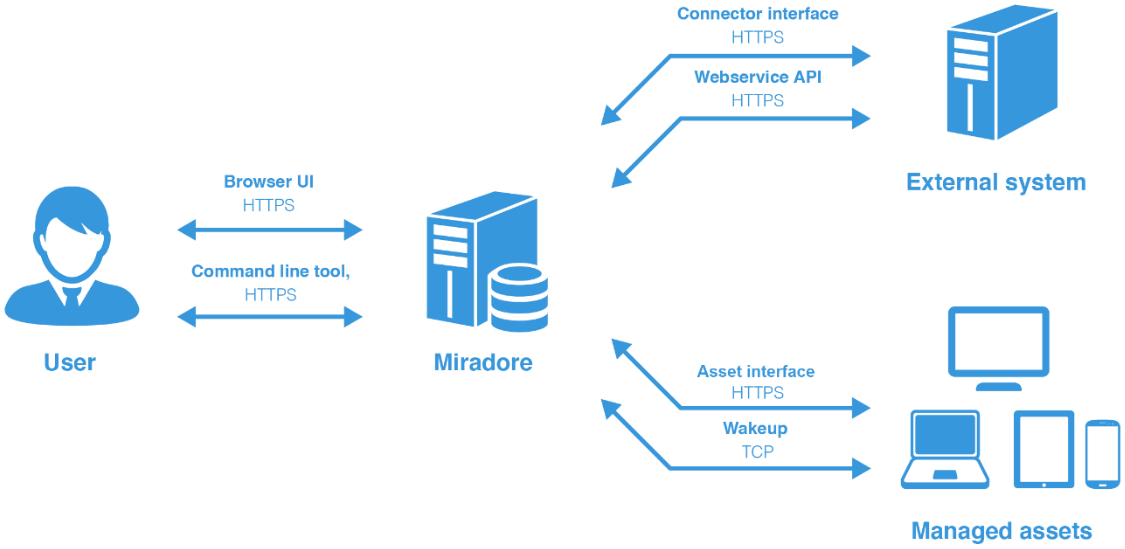
Miradore utilizes the industry standard HTTPS and TLS protocols to secure network traffic. All communications between the end user and the user interface as well as the servers and the clients are encrypted. Additionally, all system passwords are stored in an encrypted form and access management is employed to control user privileges. This section discusses the security aspects of Miradore.

2.1 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, antivirus systems and secure erasure systems. The web service API can be used by third parties to query data in order to interface with the Miradore server.

The data moving between a managed asset and the server consists of the client polling the server for commands and the server returning them if any or the client posting scheduled task results. The commands can include e.g. password resets and software installations, and scheduled task results, e.g. hardware and software inventories. Additionally, the server can contact a client with a custom wakeup TCP message causing it to poll immediately.

While some of the interfaces can be configured to transmit data unencrypted, this is discouraged and this document assumes all security features are enabled. The possibility is mentioned where available, however.



2.1.1 The Main User Interface

The main user interface is web browser based and configurable to allow users to connect using either HTTP, HTTPS or both protocols. Allowing the insecure HTTP is strongly discouraged.

Users are authenticated using ASP.Net forms authentication with a username and a password. The user passwords are salted and stored in the database as SHA-512 hashes and are thus not recoverable for anyone but a user’s password can be reset by an administrator. In the case of imported user accounts, such as those from AD, the password changes are not propagated to the external system in question and will be overwritten if the import is run again. The password of the built-in administrator account can only be reset through a special database procedure by a user with write access to the database. Each customer is able to individually define the password requirements to match their own policy.

Integrated support for user groups allows configuring users to only have access to necessary parts of the system respective to their role. To ensure further accountability, user actions are logged in event logs providing an audit trail.

2.1.2 Web Service API and the Command line tool

The web service API is a rest based web service which can be used to read information stored in the Miradore server. The command line tool is a custom tool which can be run from a windows command prompt and can be used to both read from and write to the server.

The web service API is authenticated with http basic authentication and the command line tool is authenticated with asp.net forms authentication using the same accounts as with the main user interface. Any user belonging to the integrated web service readers group can access the service. Depending on the actions the user wants to perform with the command line tool, the user account used will need to have the proper privileges configured. While the server and the tools can be configured to communicate over the http protocol, it is strongly discouraged in favor of https.

2.1.3 Connectors

Importing data from external systems, e.g. Active Directory, is handled by connectors. A connector authenticates itself with a unique randomly generated key code, its device name and the connector type. Each connector must be manually authorized from the user interface of Miradore by a user with administrator privileges. The key codes are stored in the database of the Miradore server. On a connector host, the key code is stored either in a text file or in the system registry, in most cases AES encrypted but in some cases as plaintext. While the unencrypted HTTP communications protocol is supported, its use is strongly discouraged in favor of HTTPS.

2.1.4 Managed Services

Managed assets communicate with the Miradore server either through a custom program called the Miradore client in case of desktop operating systems (Windows, Linux, macOS). The Miradore client can connect to the server using either a custom TCP protocol, HTTP or HTTPS. The use of the TCP and HTTP options are discouraged in favor of the secure HTTPS. With the exception of a wakeup message causing the client to poll the server immediately, the communications paradigm is one where all tasks are requested by the client from the server, always ensuring its authenticity. Furthermore, anytime an asset moves between networks, the client assesses whether it can still contact the server, and if not, also stops listening for the wakeups messages.

Mobile devices use the platforms’ integrated mobile device management features provided respectively by Microsoft, Google and Apple. The devices communicate with the server exclusively through HTTPS.

2.2 Stored passwords

As a configuration management system needs to store many administrative passwords, the security of these passwords is paramount. For this, Miradore relies heavily on database access security. Additionally, some passwords are stored only in an encrypted form even in the database. Most passwords are managed centrally in the System settings view of the user interface and can only be entered or changed but not read by any user with the notable exception of local administrator passwords of assets which are managed on the asset form and can be both read and written.

2.3 Database access

Miradore utilizes Microsoft’s SQL Server for data storage. Databases should be set up on dedicated secure network segment to which only the Miradore instance has access.

The database access credentials are stored on the instance computer system registry using the Microsoft Data Protection API ensuring they cannot be deciphered even if the registry was to fall into the wrong hands.

Additionally, different processes access the database with either reader, writer, or admin privileges depending on their function in order to ensure no procedure is running with excessive rights.

2.4 Code signing

All Miradore installation packages for client and server components are signed with certificates provided by GlobalSign, ensuring the software cannot be modified by a third party. This guarantees the customer can trust any Miradore program with authentic signature to be safe.

2.5 Distribution

Miradore software is distributed exclusively through the Miradore support website, hosted on Miradore premises, ensuring both the physical security of the files as well as enabling total control over the distribution channel.

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@miradore.com or through our website at http://www.miradore.com.

4 CONTACT

Miradore Oy
Laserkatu 6
53850 Lappeenranta
Finland

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