Miradore Online connector

Version information

Connector version: 1.2.0

Released in Miradore Management Suite version: 5.6.0

Released: 11/2021

Description

This connector is used for importing mobile device data from Miradore MDM to Miradore Management Suite.

Supported target systems

Miradore Online

Software prerequisites

Windows 7 or newer

.NET Framework 4.7.2 or later

Correct SSL certificate must be available in the connector host computer's Windows certificate store if HTTPS connection method is enabled.

The following cipher suites must be configured for the connector host computer (you can use for example IISCrypto for the configuration):

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

Connector host computer

Miradore Online connector can be installed on any computer, which meets the software prerequisites and is able to connect Miradore Managent Suite server and Miradore MDM.

Configuration changes made by the connector

Installation

Files

During the connector installation, user must extract a zip archive (*MiradoreOnlineConnector.zip*) which includes all the files that the connector needs to run. The user may freely select the file path for the extracted files.

Scheduled tasks

When the connector is being installed, connector configurator adds a Windows Scheduled Task (*MiradoreOnlineConnector-<KEY>*) to the host computer's Windows Scheduler. With the configurator, user can define suitable running interval and appropriate user account for the Scheduled Task running the connector.

Changes made by the program itself

Files

The program creates a log file into the connector's installation folder.

The program writes connector configurations to *OnlineConnector.exe.config* file in the connector's installation directory.

Configuration

Common configuration

It is required to configure MMS instance name, MMS server address, port, and SSL information during the connector installation. All those parameters can be configured with the Connector Configurator (OnlineConnector.exe). The Configurator will also ask you to grant "LOCAL SERVICE" account permissions to access to the connector's directory. Make sure to grant the access.

Connector-specific configuration

Connector-specific configuration can be performed in the management console of Miradore at: "*Administration > System settings > Connectors > Miradore Online > host computer* "

Following values must be configured:

Online site: Miradore MDM site's unique name (first part of site's URL). This information is displayed at the Infrastructure diagram within the Miradore MDM product.

API key: The key for Miradore MDM API. You can create the API key through the Infrastructure Diagram on your Miradore MDM site.

Network connections

Between the connector and MMS server

HTTP(S) connection (port depends on Miradore server configuration, default is 80/443).

Between the connector and Miradore's MDM product

HTTPS connection to port 443.

© 2021 Miradore Ltd. All rigths reserved.

Authentication

Between the connector and MMS server

Standard Miradore connector authentication (the connector must be authorized from the management console of Miradore).

Between the connector and Miradore MDM

Miradore MDM API authentication key.

Scheduling

Method

By default, the connector scheduling is based on a Windows scheduled task.

Interval

By default, the connector runs once in a day.

Principle of operation

Connector connects to the given Miradore server, and checks if it is authorized to run.

Terminate connection if not authorized.

Send start event to Miradore server if allowed to run.

Connector connects to the Miradore server and reads the connector configuration.

Connector connects to Miradore MDM API to read mobile device data. Only Android, iOS and iPadOS devices will be imported to MMS.

Connector repeats the following loop per each device that was found

Convert inventory data to a format which can be imported to MMS.

Update asset attributes (location, responsible person) into MMS.

Activate imported Asset configuration items in MMS.

If a device has been retired from Miradore MDM, it will be also retired in MMS.

Connector sends a stop event to MMS server.

Data transferred to MMS

Device data from Miradore MDM

Hardware inventory

Software inventory (software inventory is transferred with a separate query)

User (The user must exists in Miradore. However, if the user doesn't exist, the asset is left in *AutoGenerated* status.)

Location (The location must exists in Miradore. However, if the location doesn't exist, the asset is left in *AutoGenerated* status.)

Debugging

Set Log severity setting's value to Debug by using connector configurator.

Version history

Miradore Management Suite 5.6.0 / Connector 1.2.0

Performance improvements to the connector's data queries that sometimes were slow and even timed out with the old connector versions.

This new connector version no more imports data about Windows Phone devices, because the support for them is ending in Miradore MDM.

Miradore Management Suite 5.2.0 / Connector 1.1.8

- The connector was recompiled using .Net Framework 4.7.2 to ensure compatibility with TLS 1.2 and TLS 1.3 protocols.

- Connector error logging was enhanced.

Miradore 4.6.0 / Connector 1.1.6

The connector was modified to ignore Windows 10 computers when importing device data from Miradore Online to Miradore Management Suite, because with the previous connector version Windows 10 devices caused a lot of warning entries to the connector's log.

Miradore 4.3.0 / Connector 1.1.0

The connector was modified to support the changed identification logic of Android devices. Earlier, Miradore Management Suite used MAC address to identify devices which didn't have telephony hardware (SIM slot or IMEI code) as a basis for the identification. Unfortunately, Android 6.0 removed the programmatic access to Android devices' MAC address, and therefore a new method for device identification was needed. Starting from Miradore Management Suite 4.3.0 and Connector version 1.1.0 Android devices will be identified using the serial number that is retrieved from the managed device by Miradore Online client for Android.

Miradore Management Suite 4.3.0 doesn't allow any connections from earlier connector versions than 1.1.0.

Miradore 4.1.1 / Connector 1.0.2

There was a bug, which crashed the connector if device's application list contained an application without a version information.

© 2021 Miradore Ltd. All rigths reserved.

Miradore 3.8.0 / Connector 1.0.0

© 2021 Miradore Ltd. All rigths reserved.