

Miradore connector for Microsoft Exchange ActiveSync

Version information

Last update in Miradore version: 3.5.2
 Release date: 15.4.2013

Description

Miradore connector for Exchange ActiveSync enables the management of Exchange ActiveSync devices with Miradore. Connector is used to read Microsoft Exchange server information (including ActiveSync devices, mailbox policies, and user mailboxes) and report the information to Miradore at configurable intervals. Utilizing this information administrators can assign Exchange ActiveSync mailbox policies to an Exchange user or group of users and perform remote wipe to clear an Exchange-connected Windows Phone device. Miradore connector for Exchange also allows administrators to manage ActiveSync devices' access to Exchange server using the access rules configurable in Miradore. Default access level is defined with organisation access level setting and on top of that administrators can define more accurate access rules for different scenarios (e.g. different rules for different device platforms).

Miradore's Microsoft Exchange ActiveSync connector is built-in to Miradore Windows client. Therefore, it is not necessary to install the connector separately. Instead, the connector can be enabled/disabled from the system settings of Miradore Configuration Management where the connector configurations can be managed as well.

Supported target systems

Microsoft Exchange Server 2010
 Microsoft Office 365 / Exchange Online

Software prerequisites

Exchange ActiveSync connector can only be ran by a Windows-device (Windows XP or later) which has a Miradore client (client version 3.1.0 or newer) and either PowerShell 2.0 (or later) or Exchange Management Tools installed.
 Miradore Configuration Management 3.3.0 or later.

Connector host computer

The connector host computer must be a Windows-computer (Windows XP or newer) which has Miradore client installed and asset configuration item in Miradore. In addition, the host must have a remote connection to Microsoft Exchange server. Alternatively, it is possible to use the Microsoft Exchange server computer as a host for running the connector.

There are two alternative methods for the connector to remotely connect to the Exchange server:

1. Exchange server Management Tools (requires that the Exchange server Management Tools have been installed to the host computer)
2. Implicit remoting with PowerShell (requires that PowerShell has been installed to the host computer)

The connector host computer can be selected from the system settings of Miradore Configuration Management (see Configuration).

Configuration changes made by the connector

Files

Creates log files into following directories on the computer that is selected to run the connector:

C:\Program Files\Miradore\Client\Tasks\Inv\EASConnectorManage
 C:\Program Files\Miradore\Client\Tasks\Inv\EASConnectorSecurity

Configuration

Connector can be configured from "Administration > System settings > Connectors" in the management console of Miradore.

Configuration settings include:

- Selection of host computer: A computer with Miradore client installed and asset configuration item in Miradore.
- Microsoft Exchange server configuration and remote connection parameters.
- Filtering of Exchange users by Operational Unit.
- Polling intervals.
- Exchange ActiveSync access rules
- Organization access level

Network connections

Between connector host and Miradore server

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

Between connector host and Exchange Server

Exchange server (inhouse)

Connector can be run either locally on the Exchange server or connect remotely with PowerShell or Exchange Management Tools

(utilizes WinRM protocols).

If connector is run remotely:

Exchange server must allow Windows Remote Management (WinRM) connections.

Connector communicates with Exchange server through HTTP(S) (default ports 80/443). Additional ports might be used depending on the WinRM configurations on connector host and Exchange server.

Microsoft Office 365 / Exchange Online
Internet connection

Authentication

Between connector host and Miradore server

Standard Miradore client authentication.

Between connector host and Exchange Server

Credentials that are used to read data from Exchange server can be defined in the system settings of Miradore Configuration Management (see Configuration)

The credentials used for reading the Exchange information must have the following permissions on the Exchange server:

Organization Management, Server Management, and Recipient Management

Scheduling

Method

Scheduled by Miradore client scheduler

Interval

Inventory polling (EASConnectorManage task), by default, once a day.

Task that gathers Exchange ActiveSync inventory.

Security actions (EASConnectorSecurity task), by default, every 5 minutes.

Task that executes remote wipe, assigns mailbox policies and follows status of Windows Phone devices.

Principle of operation

Miradore client requests new settings from Miradore server according to configurable polling interval (default 24 hours).

The settings define if Miradore client should act as an Exchange ActiveSync connector.

Alternatively, the client can be woken by selecting Run now from connector settings.

Miradore client scheduler wakes up after defined interval and requests settings for running the connector from Miradore server.

Miradore client scheduler runs Inventory polling or Security actions task for connector using the settings received from Miradore server.

Connector runs itself using the received settings in a PowerShell instance.

Connector returns data to Miradore client.

Miradore client sends data to Miradore server.

Data transferred to Miradore

List of Exchange Server mailboxes, mailbox policies and Exchange ActiveSync device statistics, ActiveSync Organization access setting.

Data transferred from Miradore to the target system

List of Exchange ActiveSync devices queued for remote wipe, assigned Exchange mailbox policies, list of devices whose status is checked (for online status and remote wipe status), list of devices that will be blocked from or allowed to access the Exchange server.

Debugging

Check the connector log files under the following directories on the computer that is selected to run the connector:

<Miradore client install dir>\Client\Tasks\Inv\EASConnectorManage (Inventory polling)

<Miradore client install dir>\Client\Tasks\Inv\EASConnectorSecurity (Security actions)

Miradore client scheduler log:

<Miradore client install dir>\Client\Logs\scheduler.log

Version history

Miradore 3.5.2

Inventory filtering support

Small fixes and improvements

Miradore 3.5.1

Windows Phone 8 support

Miradore 3.4.0

Support for Microsoft Office 365 / Exchange Online

Support for Microsoft Exchange access management

Miradore 3.3.0

Initial release