# Miradore offline domain join connector

**Version information**

Connector version: 2.0.1

Released in Miradore version: 5.5.0

Released: 5/2021

**Description**

Connector for performing an offline domain join. In the offline domain join process, a computer is configured to join a Microsoft Active Directory domain without contacting a domain controller. This means that also computers without access to corporate network can be joined to a domain.

**Supported target systems**

Microsoft Active Directory on Windows Server 2003 (or newer).

**Software prerequisites for the computer to be joined**

Microsoft Windows 7 (or newer) or Microsoft Windows Server 2008 R2 (or newer).

**Software prerequisites for the connector host**

The connector host computer must run Microsoft Windows 8 (or newer) or Windows Server 2008 R2 (or newer)

The connector host computer must have .NET Framework 4.7.2 or later installed.

The connector host computer must be able to connect to Miradore server (by default, HTTPS connection to port 80/443).

It is not recommended to install the connector to the domain controller, because it will not work reliably.

**About connector host computer**

Miradore offline domain join connector may be installed on any domain-joined computer that is able to connect Miradore server.

Each Microsoft Active Directory domain requires its own connector. Therefore, it's required to install one connector per each domain.

**Configuration changes made by the connector**

Changes made by the installer:

- Files
  - Creates a program folder (user configurable) and adds files
    - C:\Program Files (x86)\Miradore\Connectors\<InstanceName>\ODJ
  - Creates a log folder (user configurable)
    - C:\Program Files (x86)\Miradore\Connectors\<InstanceName>\ODJ\Logs
- Registry
  - Common key for all connectors
    - HKLM\Software\Miradore\Server
  - Connector-specific key
    - HKLM\Software\Miradore\Server\Connectors\ODJ
- Scheduled tasks
  - Adds a Windows scheduled task to run the connector when the host computer starts

Changes made by the program itself

- Files
  - Creates a log file into the log directory.
- Registry
  - Creates value(s) under the connector-specific registry key.

**Connector configuration**

Common configuration

Miradore server, instance name, port, SSL information, and proxy information are entered when installing the connector.

These values are saved in the registry under the common key for connectors.

Connector-specific configuration

Connector-specific configuration is done in the management console of Miradore at:

Administration > System settings > Connectors > Offline Domain Join > Host computer

Following values can be configured:

**Domain:** Domain name (used for display only)

**Default domain**: There can be multiple Offline Domain Join connectors in each Miradore Management Suite instance, one per each domain. This field is used to choose one of the connectors (and one of the domains) as the default option that is used during initial

installations when performing offline domain joins for the computers. The assets are then joined to this domain during their initial installations by default IF the "Offline Domain Join connector" field is left empty at organisation item, that is assigned to the asset(s).

**Use LDAPS:** Do you want the connector to connect to Active Directory through LDAPS? Make sure that LDAPS is also enabled for AD.

**Domain controller:** This field is only required if you want to use LDAPS. Enter in here the fully qualified domain name of the domain controller. The domain controller's name must correspond to the subject name in the certificate used for the LDAPS on the domain controller.

**Username:** Username used to authenticate with Microsoft Active Directory. Use the "DOMAIN\username" format. The user account needs to have admin rights to the connector host, and also permissions to create computer accounts in Active Directory.

**Password:** Password for the authenticating user.

**Target OU:** Target organizational unit in the Active Directory where the computer account gets created or moved if it exists already. If this is empty, the default Microsoft Active Directory container will be used. Target OU is used as /machineou-parameter for djoin.exe.

**DirectAccess policy names:** Policy names (separated by semicolon) to be included in the offline domain join provisioning data created by the djoin.exe. This should include "DirectAccess Client Settings" and any other custom policies you have made for DirectAccess clients. DirectAccess policy names are used as /policynames-parameter for djoin.exe. Policy paths for /policypaths-parameters are determined automatically using the policy names.

**DirectAccess certificate template:** Certificate template name for the DirectAccess clients. DirectAccess certificate template name is used as /certtemplate-parameter for djoin.exe.

**DirectAccess group name:** Name of a security group which is allowed to access company network through DirectAccess. A computer account will be added to this group by the connector.

**Network connections**

- Between connector and Miradore server
  - HTTP(S) connection (port depends on Miradore server configuration, default is 80/443).
- Between connector and Microsoft Active Directory
  - See Microsoft documentation about djoin.exe and LDAP connection.

**Authentication**

- Between connector and Miradore server
  - Standard Miradore connector authentication (must be authorized from the management console of Miradore).
- Between connector and Microsoft Active Directory
  - Authentication is based on account and password that are entered through the connector settings in the management console of Miradore. The account must have administrative access to the computer where the connecor is running (djoin.exe must be run as administrator).

**Scheduling**

- Method
  - By default, scheduled as a Windows scheduled task.
- Interval
  - Connector is started when the host computer starts, and it must be running at all times.

**Principle of operation**

- Connects to Miradore server and checks if it is authorized to run.
  - Terminates if not authorized.
  - Sends a start event to Miradore server if allowed to run.
- Connects to Miradore server and reads connector configuration.
- Waits for Offline Domain Join requests made by the system package.
- Performs Offline Domain Join by executing djoin.exe with the given attributes.
- Adds a computer as a member of the DirectAccess group if the group is configured.
- Sends ODJ data to Miradore server.
- Enters the waiting state again.

**Data transferred from target to Miradore**

- Offline Domain Join provision data produced by djoin.exe.

**Data transferred from Miradore to the target**

- Transferred attributes are configurable through connector settings. See Connector-specific configuration above for a list of attributes

used by the connector. Username and password are passed to the connector as plain text and also the proviosion data is only base64-encrypted, so using SSL encryption with the connection to the Miradore server is strongly recommended.

**Debugging**

Set a registry value FileLogSeverity to Debug or Verbose in HKLM\Software\Miradore\Server\Connectors\ODJ and check the log file.

**Version history**

Miradore 5.5.0 / Connector 2.0.1

- Connector logging improved for making it easier to troubleshoot certain error situations. For example, now the connector better identifies if a computer object already exists in some other OU in Active Directory or if the account configured for the connector does not have enough rights.

Miradore 5.3.0 / Connector 2.0

- Connector version 2.0 connects to Miradore server through WebSockets which improves the reliability of the connection. Miradore server still supports also the older connector versions which use another connection method.
- Offline Domain Join Connector 2.0 can now be configured to use Secure LDAP (LDAPS) connection to Active Directory. There are now "Use LDAPS" and "Domain controller" fields on the Connector page in Miradore, which need to be configured properly if you want to use LDAPS.
- Troubleshooting connector issues is now easier, because Miradore now writes more detailed logs to the ...\Logs\OfflineDomainJoin directory. Miradore's user interface now also shows more detailed output regarding error situations with the offline domain join.
- Bug fix: Earlier connector versions failed to perform the offline domain join if the computer already existed in Active Directory and the target OU was not specified on the connector form. This was problematic when computers were reinstalled, because often in those cases the computer had been in AD already.

Miradore 5.1.0 / Connector 1.0.1

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

Miradore 3.8.0 / Connector 1.0

First version