

Cross domains

ad, provisioning, system

What are cross-domains?

By **cross-domains**, we mean a **set of external systems** that are linked and share, for example, the same **permissions**.

A typical example of a cross-domains group might be the linking of multiple domains in **MS Active Directory**. In this case, we can have several **AD domains that share groups with each other**. That is, within one AD domain it is possible to assign users to groups from another AD domain. The groups are thus shared across the entire group of domains (cross-domains). From the end user's perspective, **the systems thus appear to have the same set of groups**.

The goal of cross-domains in **CzechIdM** is to connect systems as described in the example above and to allow to simulate the same property, i.e. that individual group can be assigned to any system in the same cross-domain group.



A user in CzechIdM can assign a role to all or only one system **in the cross-domain group**.

How to use cross-domains in CzechIdM?

To properly use cross-domains in **CzechIdM**, we need three basic things:

1. **Create systems** connecting systems in each domain.
2. Configure the **cross-domain group of systems**.
3. Create and configure **no-login roles**.

Create systems

The first step is to create systems and connect them to individual domains. If we have a group consisting of **three domains**, then we need to create **three systems** that will provision user accounts to each of the domains (each system will connect users from one domain).

Currently, **CzechIdM supports cross-domains only for MS AD**. For proper connection, it is necessary to use the **WIN-RM connector** in the correct version and setup.

The detailed configuration of the connector and its scripts is described here: [WinRM + AD Connector](#)

Groups of systems

After you create a domain system, you must create a **cross-domain group of these systems in IdM**.

You can create a **new group in the system group management agenda**. The group must be of type '**Cross-domain**'.

You can then add the systems you created to this group. For each system, you must select the **attribute that manages the group**. In an **MS AD** environment this will typically be the '**IdapGroups**' attribute.

The screenshot shows the 'MS AD Cross-domain Edit system group definition' form with the 'Basic information' tab selected. The form contains the following fields:

- Code:** A text input field containing 'MS AD Cross-domain'.
- Group type:** A dropdown menu with 'Cross domain' selected.
- Description:** A large text area.
- Inactive:** A checkbox that is currently unchecked.

At the bottom right, there are 'Back' and 'Save' buttons.

The screenshot shows the 'MS AD Cross-domain Edit system group definition' form with the 'Connected systems' tab selected. The form displays a list of connected systems:

- A header row with a checkbox, a 'System' label, and a search icon.
- A row for 'MS AD - Users - Parking' with a checkbox and a search icon.
- A row for 'MS AD - Users - Zoo' with a checkbox and a search icon.

At the top right of the list, there is a '+ Add' button and a refresh icon. At the bottom right, it says '1 - 2 of 2 records'.

No login roles

The last step in setting up the cross-domain environment in IdM is to **create and set up the appropriate roles**. The goal is to **create roles that represent groups in each domain**.

It is not necessary to create the roles manually, but we can use **group synchronization** to do so. This means that for each domain that we will create a system for role/group synchronization. This synchronisation will create roles corresponding to groups, but it will also directly create a connection to that system in IdM. This connection will assign a group identifier (typically the **group DN**) within

the attribute that manages the groups in the domain (typically 'IdapGroups').

Roles created in this way will contain a link to the domain from which the group originates. However, to function properly within a cross-domain, we need to create links to other domains as well. So the goal is for each role to link to all domains while assigning an **identifier (DN)** to the group's managing attribute (**IdapGroups**). The value of the group identifier (DN) **will be the same in all connections to that role!**

If you make the settings described above, the role should switch to **no-login mode**. No-login mode means that assigning such a role to a user will **not create an account** on the system. An account will only be created if the user has another role assigning an account. Such a role is then called a **login-role**, which is a common system-assigning role from the IdM perspective.

The prerequisite for a role to become a no-login role is that the connected system must be part of some **active group of systems with a cross-domain type**, and also that this role **overloads the same merge attribute** as is used in the group.

If the role is in **no-login mode** for cross-domains, then the **information box is displayed on that system connection**:

Basic information

More information

Role attributes

Business role

Incompatible roles

Role authorizers

Role catalogue

Permissions

Automatic roles

Users with role

Systems

Accounts

Connected system

Role

domainGroupOne

System

AD user parking

Mapping

Mapping (Identity - Provisioning)

☐ Forward account management

If checked, then an account on this system is created even though the assignment of this role to the user will be valid in the future.

☐ Automatically create accounts

Assigning this role will automatically create an account on the system. If this option is not selected, then the account will only be created if another role is assigned for this system and creates the account automatically.

This connection is part of a Cross-domain group. Account management will be managed according to the role rules in Cross-domain groups. The automatic account creation setting will be ignored.

Back

Save

Attributes mapped within role

+ Add

<input type="checkbox"/>	Name	IdM key	Identifier	Strategy	Entity attr.	Extended attr.	Disable	Transformation
<input type="checkbox"/>	IdapGroups			Merge (only provisioning)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

1 - 1 of 1 records

Assing no-login role to only one domain

In the previous step, we described what cross-domain **no-login** roles are. We already know that if we assign such a role to a user, then no account will be created on the end system.

Now let's have a situation where we have a no-login role that assigns a group to **three domains**. If

This behavior can be a problem when we want to assign a group to only one account on one of the domains.

This selection will only be displayed for no-login roles in a cross-domain group and if the role contains more than one linked domain.

+ Add roles

Role

x domainlocalgroupkotas2

x ▾

System with an account

domainlocalgroupkotas2 - AD user zoo (IDENTITY)

x ▾

Select the system with the account to which you want to assign this role. If you do not select any system, then the role will be assigned to all systems for this role. If the account does not exist on the system yet, then this role will not create it!

Contracted position

Default

▾

Connection to organization or another tree structure

Valid from

x

Valid till

x

Close

Set

Future improvements



Group synchronization **could create a merge attribute connection not only to the system from which it is synchronized, but also** to all other systems in the cross-domain group.



Group synchronization **could assign roles to users not only according to the state on the system from which**



the group originates, but also from all other systems in the cross-domain group.

Limitations



No-login connections cannot overload the primary mapping attribute (UID)!



Adding or removing too many groups at once is not supported. Length limitation of environment variable on Windows is 8191 characters so if combination of all added and removed group's DNs plus commas, doublequotes and the script itself is longer than that cmd.exe just ignores it. The result is no script is being run and no error or exception occurs. Relatively safe is to add or remove about 50-100 groups at once.

From:

<https://wiki.czechidm.com/> - **CzechIdM Identity Manager**

Permanent link:

<https://wiki.czechidm.com/devel/documentation/adm/cross-domains>

Last update: **2023/11/08 13:43**

