Self-Service-Password-Reset

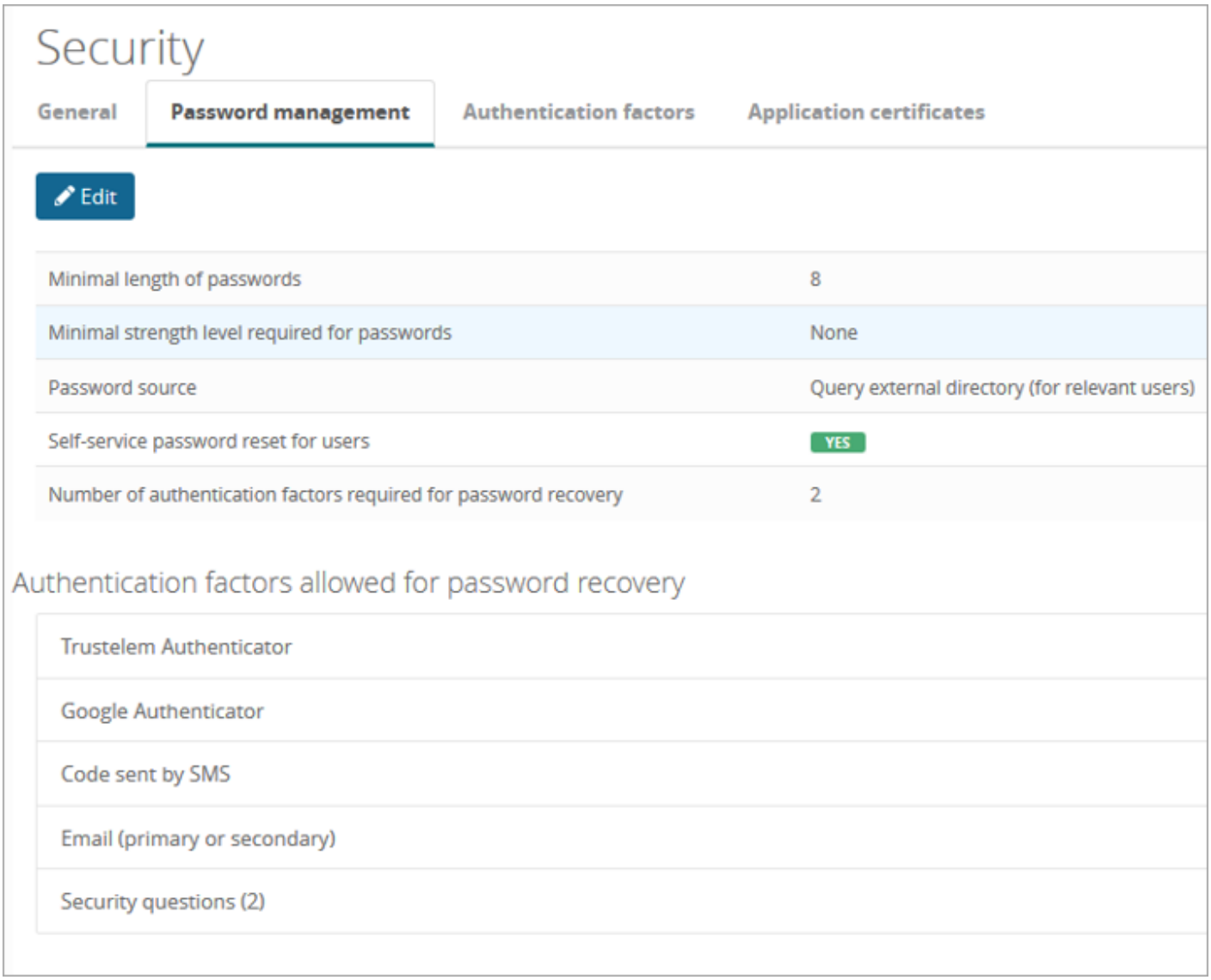
The feature **Self-Service-Password-Reset** (or SSPR) allows Trustelem users to reset a lost password, even if they are from Active Directory.
The goal is to reduce the administrative workload by giving users autonomy.



- A user provides his login and additional secrets on `https://mydomain.trustelem.com/forgot`.
- Then he can define a new password.
- This new password is saved on Trustelem or sent to Active Directory.

The setup is done in the **Security settings** tab, then **Password management**:
`https://admin-mydomain.trustelem.com/app#/security/passwords/edit` --> Self-service password reset for users

When the feature is activated the administrator can select the number of required factors then select which factors will be required.



Notes:

- In order to use a second factor for SSPR, it has to be activated and enrolled first.

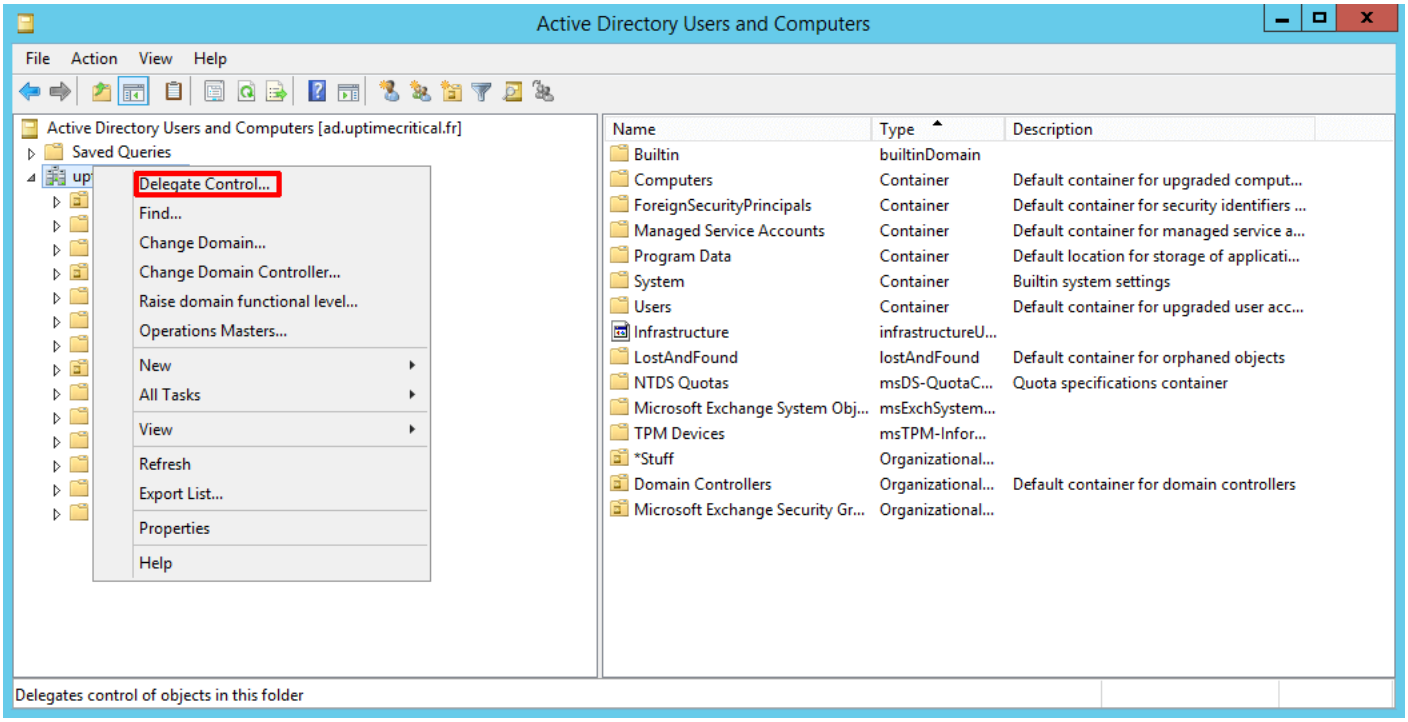
  See: https://doc-trustelem.wallix.com/administration/mfa/
- If users have a password stored by Trustelem there is no need for more configuration.
- When the password used is not stored by Trustelem (users from AD or Azure AD), a special configuration has to be done in order to give Trustelem the needed rights.

Self-Service password Reset for Active Directory

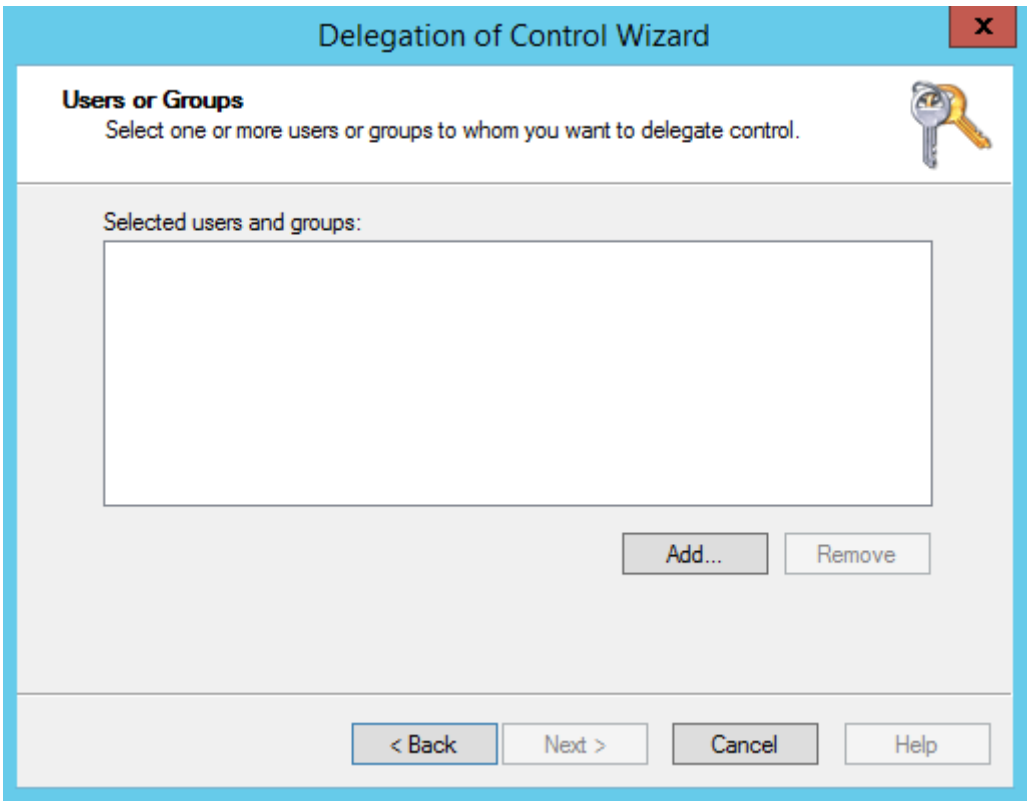
If you want to activate the SSPR service for Active Directory, you should already have a directory setup with an AD Connect installed.

See: Active Directory synchronization First, you have to go on your Trustelem directory setting page and activate the feature **Password recovery**.
Then SSPR service requires the Trustelem connector service account to be granted with privilege **delegation for user's password reset**.

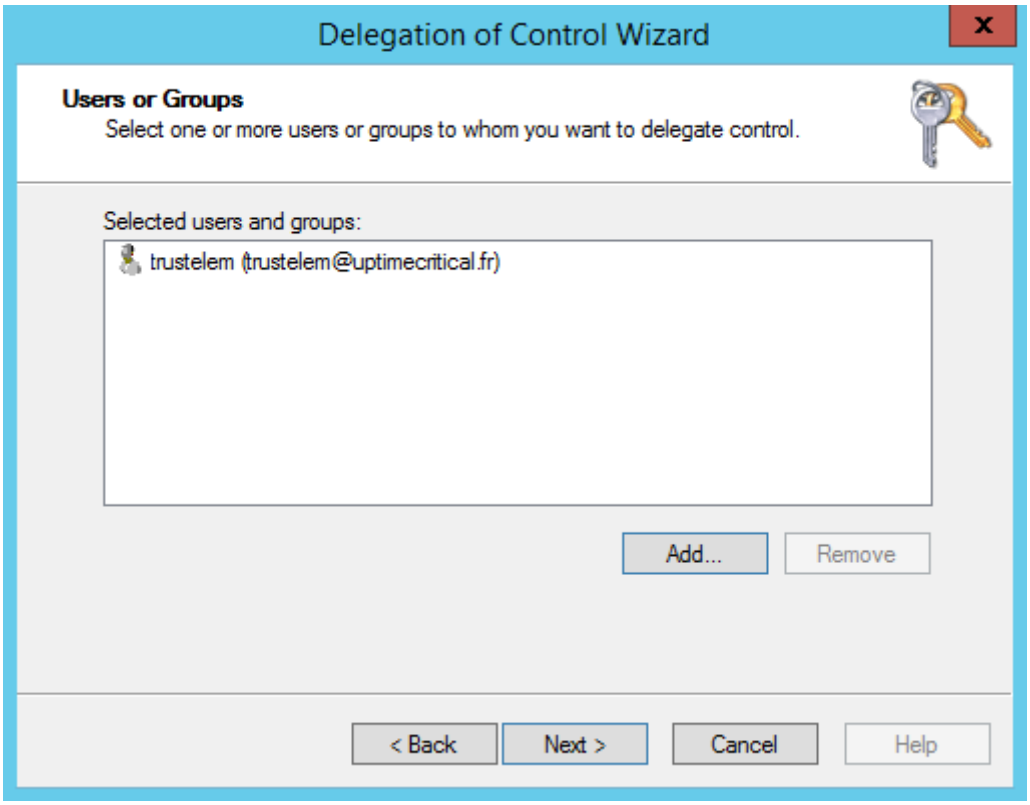
- Open the **Active Directory Users and Groups** panel and right-click on target domain. Then select item **Delegate Control...**



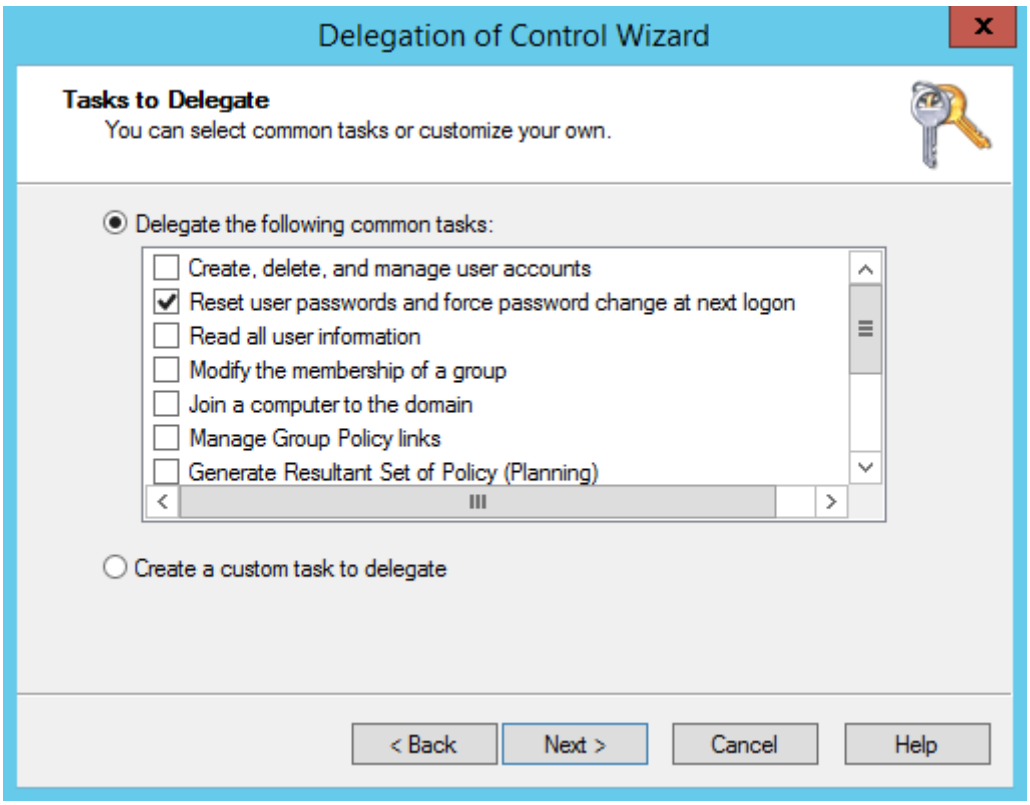
- In the delegation wizard, click on **Next**, then click on **Add**.... Click on **Next**



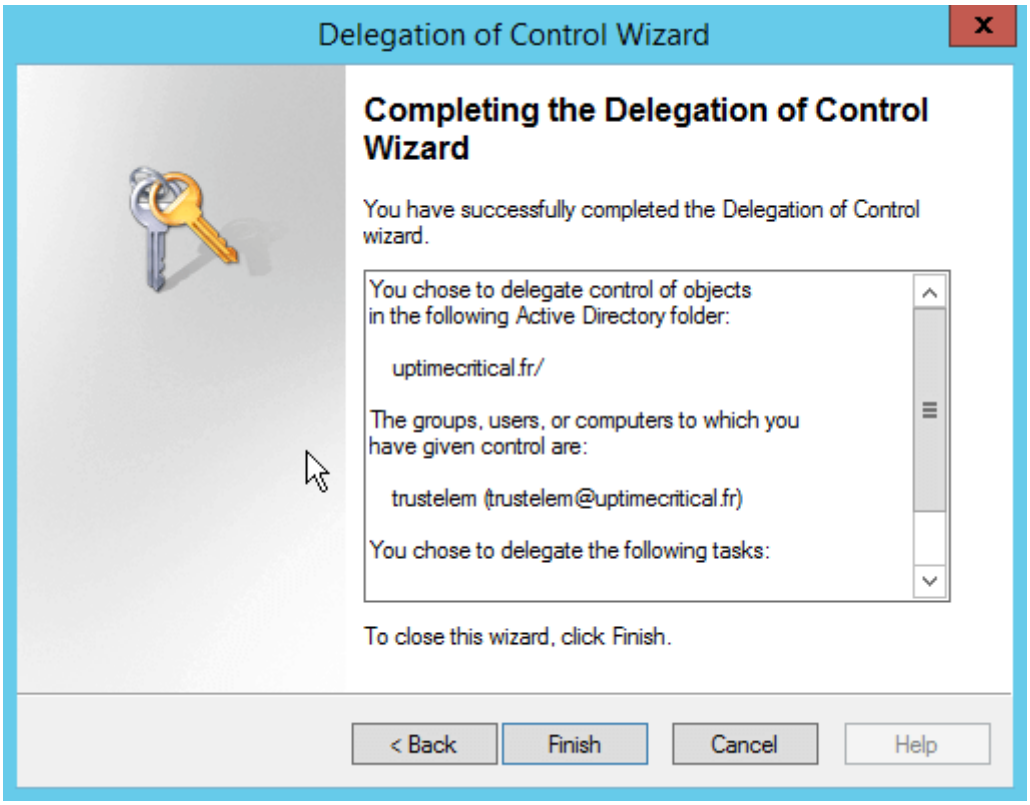
- Choose the service account executing Trustelem AD Connect. Click on **Next**



- Select the following permission to delegate: **Reset user password and force password change at next logon**. Click on **Next**



- Check summary and click on **Finish**



Self-Service password Reset for Azure Active Directory

If you want to activate the SSPR service for Azure Active Directory, you should already have a directory setup with Trustelem.
Note: Azure Active Directory passwords can only be used and reset by Trustelem if Office 365 is not federated.
First, you have to go on your Trustelem directory setting page and activate the feature **Password recovery**.
Then start PowerShell and execute the following script, with the correct value for the **CLIENT ID** of your Trustelem app on Azure AD:

```
Install-Module AzureAD
Connect-AzureAD
$app = Get-AzureADServicePrincipal -filter "AppId eq 'CLIENT ID'"
$role = Get-AzureADDirectoryRole | Where-Object { $_.DisplayName -eq "Helpdesk Administrator"
}
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId $app.ObjectId
$role = Get-AzureADDirectoryRole | Where-Object { $_.DisplayName -eq "Directory Writers" }
Add-AzureADDirectoryRoleMember -ObjectId $role.ObjectId -RefObjectId $app.ObjectId
```

Revision #3
Created 1 July 2022 08:29:55 by WALLIX Admin
Updated 25 March 2025 10:22:34 by WALLIX Admin