WINDOWS LOCAL USERS AND COMPUTERS OUT OF DOMAIN

Windows Local Users and Computers Out Of Domain

Windows Local Users Local Accounts

1. Overview

This tutorial will explain to you how to configure WebADM/OpenOTP servers and OpenOTP Credential Provider for Windows to authenticate local users using 2-factor authentication. We will also explain how to authenticate your users with OpenOTP and OpenOTP Credential Provider for Windows on a computer out of the domain.

Both scenarios require an LDAP server to store user metadata (Token metadata needs to be stored on a user account in WebADM even for local account authentication).

Each scenario require OpenOTP Credential Provider for Windows. The OpenOTP Credential Provider for Windows is a component that integrates the RCDevs OpenOTP one-time password authentication into the Windows login process. RCDevs OpenOTP Authentication Server is a WebApp that is tightly coupled to the RCDevs WebADM application server.

2. General Prerequisites

For this recipe, you will need to have WebADM/OpenOTP installed and configured. Please, refer to WebADM Installation Guide and WebADM Manual to do it.

2.1 Prerequisites for Local Users Authentication

Note

In this scenario, users credentials (Username and password) will be checked locally on the Windows machine according to the `Remote LDAP password Check option` and the second factor authentication will be checked remotely on the OpenOTP server. To check the 2FA, OpenOTP has to know which user is trying to authenticate to be able to check Token metadata on the user account. That's why a concordance between the local user and the LDAP user should be present. This concordance is done by the username information.

To have a WebADM instance working properly, an LDAP datastore configured with WebADM is mandatory. In this scenario, we will show you how to authenticate Windows local users with a WebADM/OpenOTP instance already configured with an LDAP server.

We can identify 3 scenarios :

- **User account exist on the Windows machines (local account) and in WebADM**. You can configure the `Remote LDAP password check` setting to `No` to keep password validation and policies on Windows only. If `Remote LDAP password check` is set to `Yes`, then the local password will be sent to OpenOTP and according to the configured policies on WebADM, the password can be verified as LDAP password for the corresponding WebADM account.
- **Users account exist on the Windows machines but not on WebADM**. In this case, you will have to create a WebADM account. From an organizational point of view, you can create a fresh Organizational Unit, and create your "local users" in this OU to be able to identify "local and LDAP" users easily.

- **The user account exist in WebADM but not on Windows**. In that case, you can enable the setting `Auto Create Local Account` during the Credential Provider installation. When OpenOTP server will respond with a success response for an authentication, if the account doesn't exist on Windows, the Credential Provider will auto-create it with the username and password provided during the authentication process. The user password validated by OpenOTP will override the local user password on the Windows at each login. That way, you don't have to maintain password on Windows. It can also auto-populate selected local groups.

> **Note**
>
> For local user accounts, the password is not inevitably the same on both side because the user password will not be checked by OpenOTP but locally by the Windows machine.

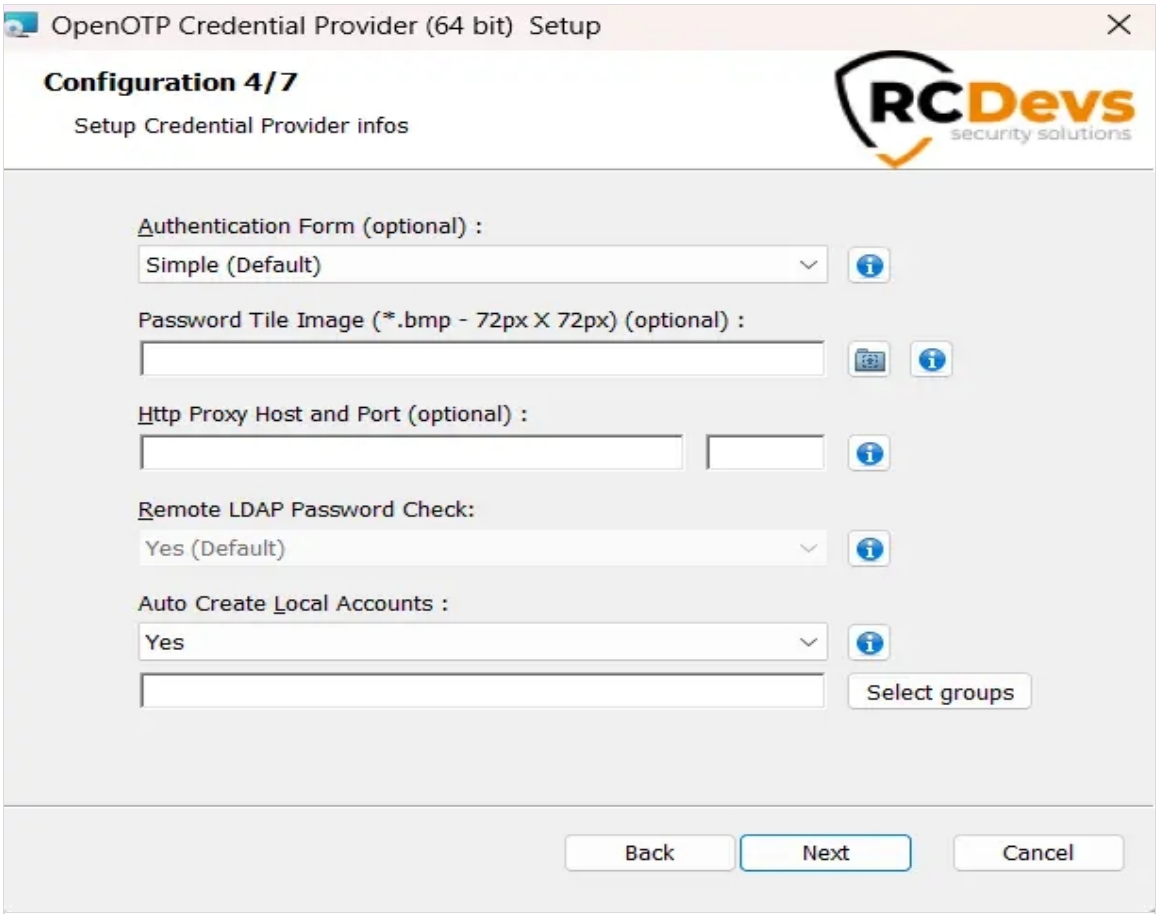
In some circumstance, the authentication can be a success on one side and a failure on the other side. This will prevent you to login so, be careful on how you configure Credential Provider and policies.

When this part is done, you can assign a Token to the user account. To do this, please follow this documentation.

3. Authenticate a Windows Local User

3.1 OpenOTP Credential Provider Configuration

You can read the Credential Provider documentation, and follow the installation and configuration part until the Configuration 3/4 screenshot. When you are at the 4/7 configuration step, you can find a setting named `Remote LDAP password Check`. Set this setting to "No":



That means, the LDAP password will not be sent to OpenOTP and will only be checked locally by the Windows machine. In the registry, the key related to this setting is check_ldap. This key is set to 0 to send the -LDAP flag to OpenOTP, which tells it to not check it. When 1 is set, the user password provided during the authentication will be sent by the Credential Provider to OpenOTP and checked there.

Click on the `Next`, `Install` and `Finish` buttons to finish the installation. You can now continue with the WebADM configuration.

3.2 WebADM Configuration

3.2.1 Windows Machine in a Domain

If the Windows machine where the OpenOTP Credential Provider is installed is in a Windows domain, you have nothing to change in WebADM configuration. Your default configuration should be enough. If the authentication failed, please have a look in webadm logs, the most common error is “Domain not found”. If you encounter this error, please read the next part and add the domain found in the WebADM logs in the domain aliases field in your local domain configuration.

3.2.2 Windows Machine out of Domain

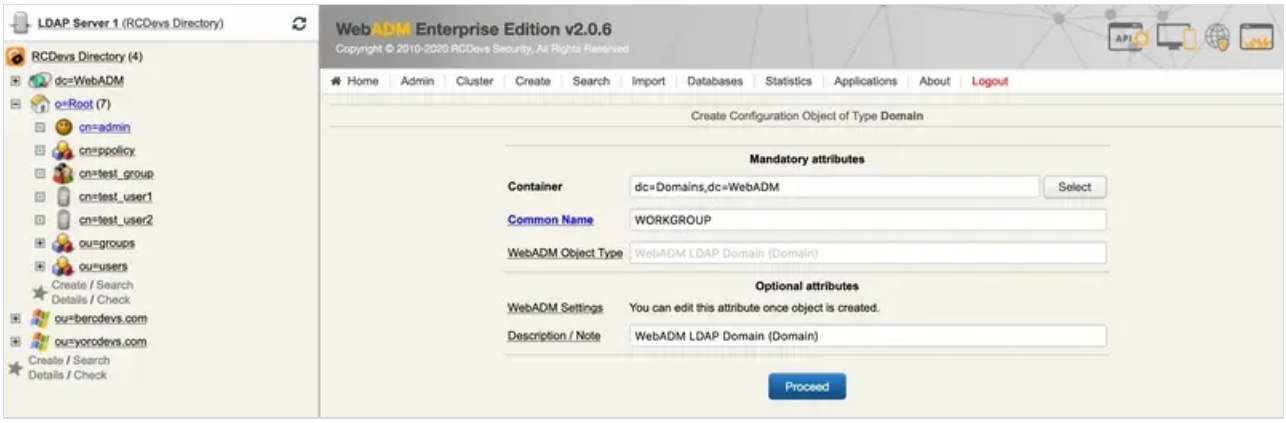
If the Windows machine where the OpenOTP Credential Provider is installed is NOT in a Windows domain, you have to perform some change through the WebADM GUI because, in the authentication request sent to OpenOTP, the domain name (by default) or the Workgroup (when the target machine is not in a domain) is passed. If the machine is not in a workgroup either, the computer name is passed. In this scenario, the Workgroup/computer name will be passed in the authentication request.

To perform these changes, log in on the WebADM GUI as super_admin, click on the `Admin` tab, `Local Domains`. Now you have 2 possibilities:

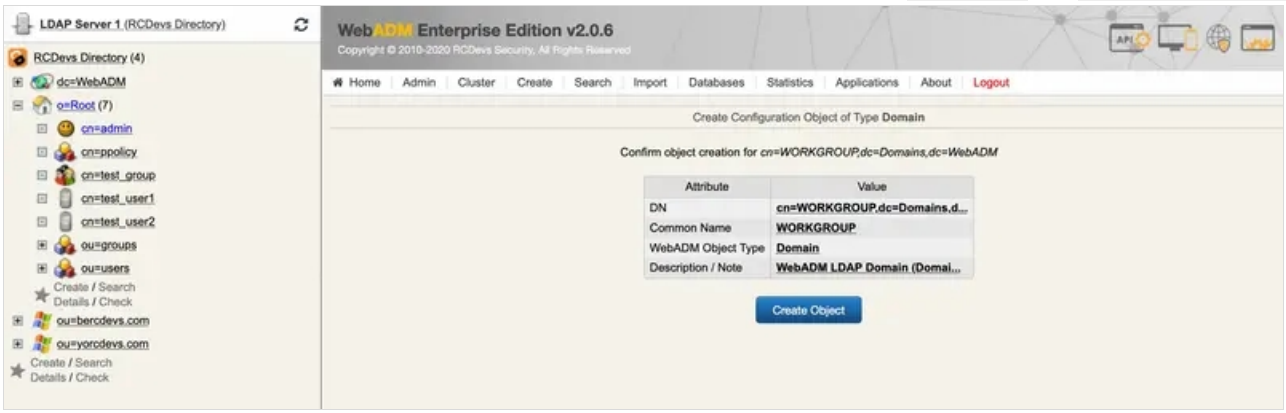
Scenario 1:

› Create a new WebADM domain, name it like your workgroup name and configure the user search base of your “local user” OU.

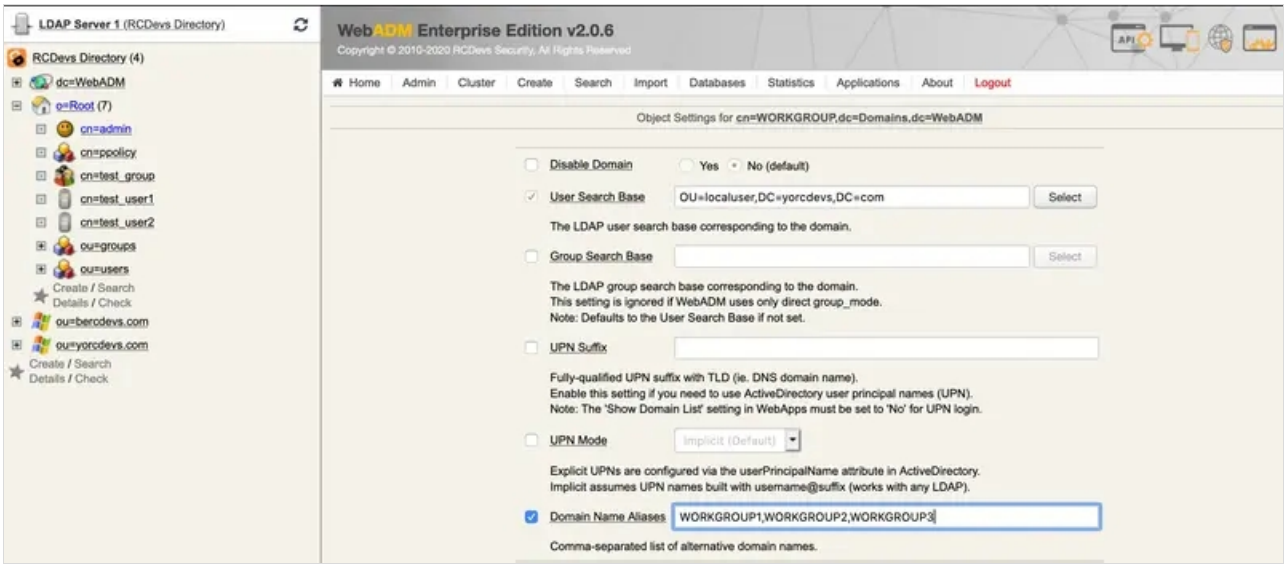
To perform this, click on `Add Domain` button.



I named my new domain like my workgroup (by default it is **WORKGROUP**), and I click on `Proceed` and `Create Object`.



You are now on the local domain configuration page. The only settings who interest us here are the `User Search Base` and the `Domain Name Aliases`.



Note

I previously configure a fresh Organizational Unit on my LDAP server and add my local user accounts in this fresh OU. I've decided to put my local users in a specific OU for an organizational point of view.

Here, my user search base will be `OU=localuser,DC=yorcdevs,DC=com`.

In the `Domain Name Aliases` field, I put every Windows workgroup of my machines.

Note

If a Windows machine is in the workgroup named WORKGROUP4, I have to add WORKGROUP4 in the `Domain Name Aliases` field else, you will have an error in WebADM logs saying "domain not found".

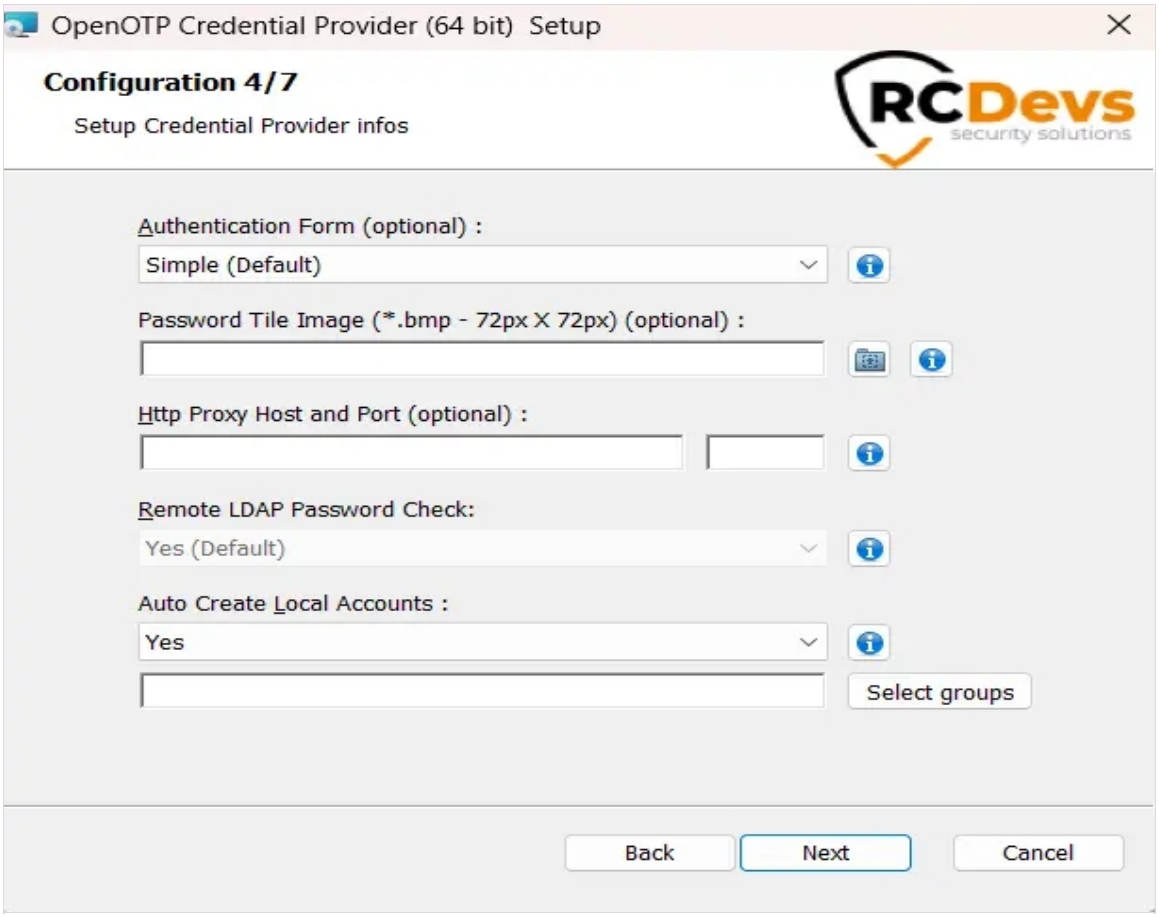
This is the proper way to perform this integration.

Scenario 2:

The other way is simply to add every workgroup names in the default domain configuration. Be careful with the User Search Base.

4. Auto Create Local Account

OpenOTP Credential Provider for Windows is able to auto create a local account when you perform a login.



That means, when you configure this setting to `Yes`, the Credential Provider will automatically create the same account locally if the account is not already present in case of the remote authentication is a success. Moreover, you can select local groups to be populated by these auto-created local accounts. The local password will also be transparently reset at each login with the provided password. For that reason, this setting is only available if the `Remote LDAP Password Check` option is enabled.