

MOUNTPOINTS

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs Security.

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to info@rcdevs.com.

1. Overview

Generally, WebADM is configured to connect with a remote AD/LDAP domain for two reasons:

- › For an admin to be able to browse (and optionally modify) remote domain contents such as user objects via a web browser (and optionally delegate that work to sub-administrators).
- › To act as a gateway to allow the OpenOTP server to read and use remote user data for authentication purposes (i.e. fetch user mobile phone number from AD account).

Remote AD/LDAP connections are configured with a mechanism called **MountPoints** in WebADM, which as indicated is a method of creating virtual folders (containers) in the local WebADM directory to which the remote AD/LDAP contents are dynamically mounted to.

The steps are:

- › Create a new OU or a new container on your WebADM server.
- › Connect the additional LDAP and mount it in the OU/container previously created.
- › Create a new WebADM domain object, this object is required to define the **User Search Base** for your additional LDAP server.

In this documentation, WebADM is natively connected with Active Directory and the secondary LDAP will be an Active Directory too.

Note

Note that you can connect any kind of LDAP like Novell, OpenLDAP... as a mount point. Conversely, you can also have a WebADM natively connected with an OpenLDAP or Novell directory and connect an Active Directory as mount point.

2. Create a New Container

We will start by creating a new Organizational Unit/Container. As I said before, this new OU/Container will contain the remote LDAP virtually mounted.

Log in to your WebADM server with your super_admin account:

LDAP Server 1 (Active Directory)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

API

Home Admin Create Search Import Databases Statistics Applications About Logout

Hello Administrator (*CN=Administrator,CN=Users...*)
Connected as **Super Administrator** to webadm1.yorcdevs.com

Application Status

OpenID & SAML Provider:	Not Registered
Secure Password Reset:	Not Registered
User Self-Service Desk:	Not Registered
User Self-Registration:	Not Registered
MFA Authentication Server:	Not Registered
Single Sign-On Server:	Not Registered
SMS Hub Server:	Not Registered
SSH Public Key Server:	Not Registered
QR Login & Signing Server:	Not Registered

Configurations Objects

Local Domains: 1 (Details)	Trust Domains: 0 (Details)
Mount Points: 0 (Details)	Option Sets: 1 (Details)
Client Policies: 0 (Details)	Admin Roles: 0 (Details)

DC=yorcdevs (14)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users**
- CN=WebADM
- OU=Domain Controllers

Create / Search
Details / Check

And click on **Create** button below the left tree, and you are now in the creation menu:

LDAP Server 1 (Active Directory)

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

API

Home Admin Create Search Import Databases Statistics Applications About Logout

Create New LDAP Object

<input type="radio"/> WebADM Option Set OptionSet, Mountpoint, Domain, Client...	<input type="radio"/> WebADM Account LDAP user with WebADM attributes
<input type="radio"/> User / Administrator Administrator or Domain user	<input type="radio"/> Container LDAP generic container
<input type="radio"/> Group LDAP group of users	<input type="radio"/> UNIX Account UNIX POSIX Account
<input type="radio"/> UNIX Group UNIX POSIX Group	<input type="radio"/> Contact LDAP contact
<input checked="" type="radio"/> Organizational Unit LDAP organizational unit container	<input type="radio"/> Organisation LDAP organization container
<input type="radio"/> Country LDAP country container	<input type="radio"/> Domain LDAP domain container

Proceed

DC=yorcdevs (14)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users**
- CN=WebADM
- OU=Domain Controllers

Create / Search
Details / Check

Select **Organizational Unit** or **Container** and click on **Proceed**:

LDAP Server 1 (Active Directory)

- DC=yorcdevs (14)
 - CN=Builtin
 - CN=Computers
 - CN=ForeignSecurityPrincip...
 - CN=Infrastructure
 - CN=Keys
 - CN=LostAndFound
 - CN=Managed Service Accoun...
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users
 - CN=WebADM
 - OU=Domain Controllers
- Create / Search
- Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

Create Object of Type **Organizational Unit**

Mandatory attributes

Container
DC=yorcdevs,DC=com
Select

Organizational Unit
LAB

Optional attributes

Country

UNIX Password

Common Name

Description / Note
Additional LDAP Server connected to WebADM.

Proceed

Name your object and click on **Proceed** again:

LDAP Server 1 (Active Directory)

- DC=yorcdevs (14)
 - CN=Builtin
 - CN=Computers
 - CN=ForeignSecurityPrincip...
 - CN=Infrastructure
 - CN=Keys
 - CN=LostAndFound
 - CN=Managed Service Accoun...
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users
 - CN=WebADM
 - OU=Domain Controllers
- Create / Search
- Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home
Admin
Create
Search
Import
Databases
Statistics
Applications
About
Logout

Create Object of Type **Organizational Unit**

Confirm object creation for *ou=LAB,DC=yorcdevs,DC=com*

Attribute	Value
DN	ou=LAB,DC=yorcdevs,DC=com
Organizational Unit	LAB
Description / Note	Additional LDAP Server co...
UNIX Password	****

Create Object

Click on **Create Object** and your OU/Container is created.

3. Connect the Additional LDAP to WebADM

We will now connect the remote LDAP to WebADM. Always through the WebADM Admin GUI, click on **Admin** tab, **LDAP Mount Points**:

LDAP Server 1 (Active Directory)

DC=yorcdevs (15)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
- CN=WebADM
- OU=Domain Controllers
- OU=LAB

Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

WebADM Server Administration

WebADM v1.6.8-2 (64bit) running on server webadm1.yorcdevs.com (192.168.3.155) in standalone mode.

Server Version Details: Apache/2.4.37 PHP/7.1.23 OpenSSL/1.0.2p-fips
Internal Server Time: 2018-11-22 11:56:40 Europe/Berlin (NTP check Ok)
Hardware Modules: No HSM Connected
WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)

Active LDAP Server: LDAP Server 1 (192.168.3.131) Active SQL Server: SQL Server (127.0.0.1)
Active Session Server: Session Server (::1) Active PKI Server: PKI Server (127.0.0.1)

Local Domains (1)
Associate domain names with LDAP user search bases.

Trust Domains (0)
Bridge remote domain names located on distant servers.

Client Policies (0)
Define custom policy settings for consumer applications.

LDAP Mount Points (0)
Connect secondary LDAP servers to the tree view.

LDAP Option Sets (1)
Define LDAP tree constraints for your 'other' administrators.

Administrator Roles (0)
Create admin role templates for your 'other' administrators.

Now click on **Add MountPoint** button.

LDAP Server 1 (Active Directory)

DC=yorcdevs (14)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas

Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Registered LDAP Mount Points

No LDAP MountPoint configured

Add MountPoint Ok

Name your MountPoint object and optionally enter a description. On my side, I keep **LAB** name. Click on **Proceed** button.

LDAP Server 1 (Active Directory)

DC=yorcdevs (15)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
- CN=WebADM
- OU=Domain Controllers
- OU=LAB

Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Create Configuration Object of Type MountPoint

Mandatory attributes

Container: cn=MountPoints,cn=WebADM,dc=yorcdevs,dc=com Select

Common Name: LAB

Optional attributes

WebADM Object Type: WebADM Mount Point (MountPoint)

Organization:

Organizational Unit:

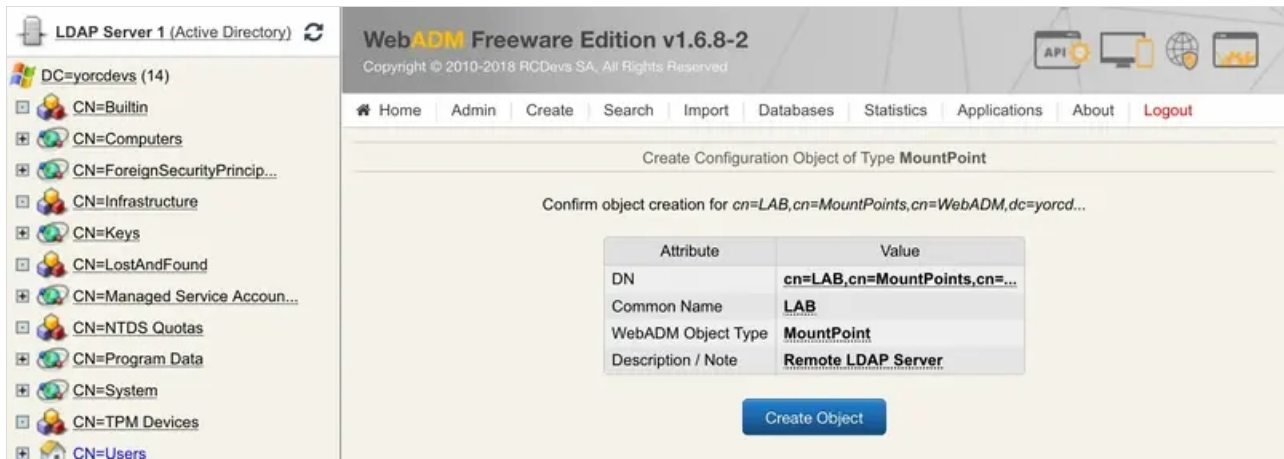
Description / Note: Remote LDAP Server

WebADM Settings: You can edit this attribute once object is created.

WebADM User Data: This attribute cannot be created manually.

Proceed

On the next screen, click on **Create Object**.



You are now in the MountPoint configuration. You have to configure:

- > **Mount DN**: This setting is the location where the remote LDAP will be mounted on your WebADM server. We previously created a blank OU for this. So select your OU or the container previously created.
- > **Host Name(s)**: You have to configure here, the name or IP address of the remote LDAP server(s).
- > **Port Number**: Set by default to 389 port but can be changed to 636 for LDAP SSL.
- > **Encryption type**: None, SSL or TLS encryption are available.
- > **Tree Base**: Enter the tree base of the remote LDAP (e.g: for the domain `rcdevs.com`, the tree base is `dc=rcdevs,dc=com`).
- > **Login DN**: The login DN will be used to write WebADM metadata on users account on the remote LDAP.
- > **Login password**: Password of the login DN user.
- > The last 3 options are optional.

LDAP Server 1 (Active Directory)

- DC=yorcdevs (15)
 - CN=Builtin
 - CN=Computers
 - CN=ForeignSecurityPrincip...
 - CN=Infrastructure
 - CN=Keys
 - CN=LostAndFound
 - CN=Managed Service Accoun...
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users
 - CN=WebADM
 - OU=Domain Controllers
 - OU=LAB
- Create / Search
- Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Object Settings for cn=LAB,cn=MountPoints,cn=WebADM,dc=yorcdevs,dc=com

☐ Disable Mount Point

☐ Yes
☒ No (default)

☒ Mount DN

OU=LAB,DC=yorcdevs,DC=com
Select

The LDAP tree node where to mount the remote LDAP.

☒ Host Name(s)

192.168.3.194

LDAP server name(s) or IP address(es).
You can set a comma-separated list of servers. The next servers are used for failover.

☒ Port Number

389

LDAP server port.

☒ Encryption Type

None (Default)

☒ Tree Base

dc=exe,dc=com

Mounted LDAP tree base or base DN (mandatory with most LDAP servers).

☒ Login DN

cn=administrator,cn=users,dc=exe,dc=com

Mounted LDAP bind DN. WebADM will bind anonymously if not set.

☒ Login Password

.....

☐ Trusted CA Certificate

Edit

☐ Client Certificate File

Edit

☐ Client Certificate Key File

Edit

Apply

Cancel

Reset

When your configuration is done, you can click on **Apply**.

Your MountPoint is now created. At this step, you should be able to see the remote LDAP tree in your container.

LDAP Server 1 (Active Directory)

- DC=yorcdevs (15)
 - CN=Builtin
 - CN=Computers
 - CN=ForeignSecurityPrincip...
 - CN=Infrastructure
 - CN=Keys
 - CN=LostAndFound
 - CN=Managed Service Accoun...
 - CN=NTDS Quotas
 - CN=Program Data
 - CN=System
 - CN=TPM Devices
 - CN=Users
 - CN=WebADM
 - OU=Domain Controllers
 - OU=LAB
- Create / Search
- Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Registered LDAP Mount Points

LAB (CN=LAB,CN=MountPoints,CN=WebADM,DC=yorcdevs,dc=com)

Status: **Enabled** [CONFIGURE] [RENAME] [REMOVE]

Extended: **Yes** (DETAILS) (SCHEMA)

Directory Type: microsoft

Server(s): 192.168.3.194:389

Encryption: NONE

Mount Point: ou=lab,dc=yorcdevs,dc=com

Tree Base: dc=exe,dc=com

Login DN: cn=administrator,cn=users,dc=exe,dc=com

Add MountPoint

Ok

WebADM Server Administration

WebADM v1.6.8-2 (64bit) running on server webadm1.yorcdevs.com (192.168.3.155) in standalone mode.

Server Version Details: Apache/2.4.37 PHP/7.1.23 OpenSSL/1.0.2p-fips

Internal Server Time: 2018-11-22 12:10:01 Europe/Berlin (**NTP check Ok**)

Hardware Modules: No HSM Connected

WebADM Features: WebApps (**Enabled**), WebSrvs (**Enabled**), Manager (**Enabled**)

Active LDAP Server: *LDAP Server 1 (192.168.3.131)* Active SQL Server: *SQL Server (127.0.0.1)*

Active Session Server: *Session Server (::1)* Active PKI Server: *PKI Server (127.0.0.1)*

**Local Domains (1)**

Associate domain names with LDAP user search bases.

**Trust Domains (0)**

Bridge remote domain names located on distant servers.

**Client Policies (0)**

Define custom policy settings for consumer applications.

**LDAP Mount Points (1)**

Connect secondary LDAP servers to the tree view.

**LDAP Option Sets (1)**

Define LDAP tree constraints for your 'other' administrators.

**Administrator Roles (0)**

Create admin role templates for your 'other' administrators.

Licensing and Configurations

[Software License Details](#)



[LDAP Server Details](#)



[LDAP Server Schema](#)



[Memory Usage Details](#)



[Hardware Modules Details](#)



[Remote Manager Interface](#)



[Config Object Statuses](#)



[WebADM Base Settings](#)

Runtime Actions

[Download WebADM CA Certificate](#)



[Download WebADM SSL Certificate](#)



[Issue Server or Client SSL Certificate](#)



[Clear Admin Session Cache \(2 KB\)](#) ⓘ



[Clear WebADM License Cache](#) ⓘ



[Clear WebADM Local Caches \(552 KB\)](#) ⓘ



[Flush WebADM Cluster Caches \(844 KB\)](#) ⓘ



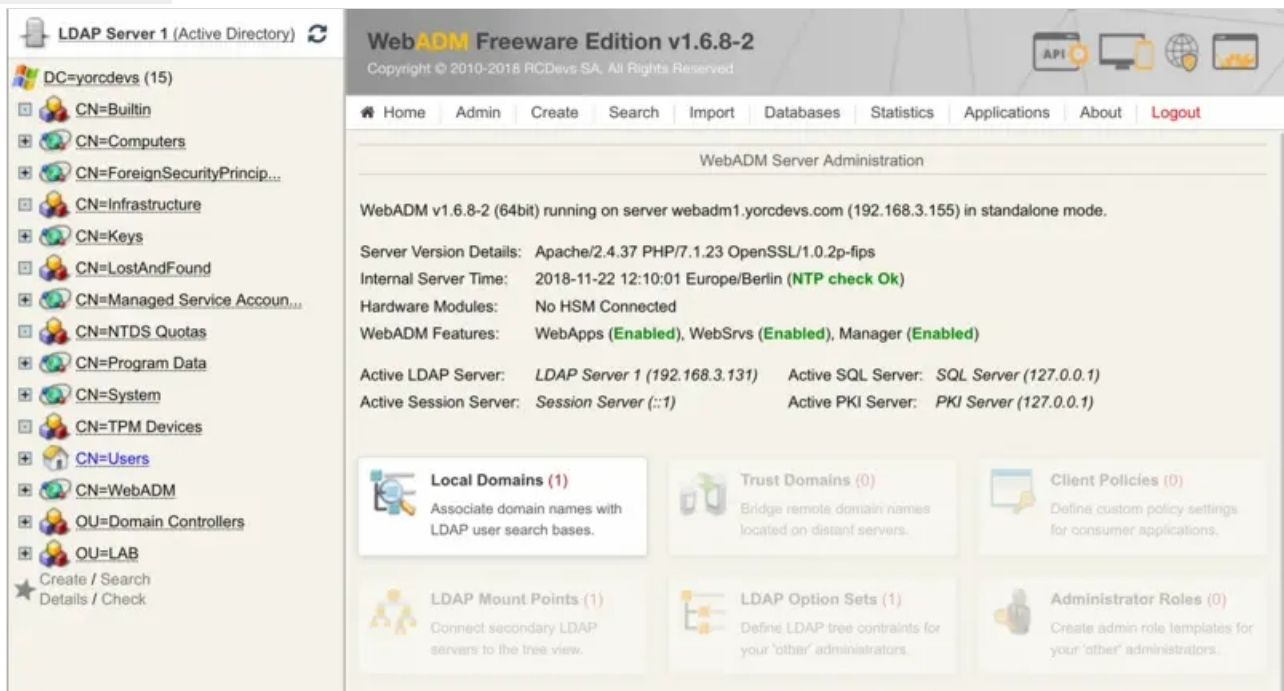
[Reload WebADM Configurations](#)

Note

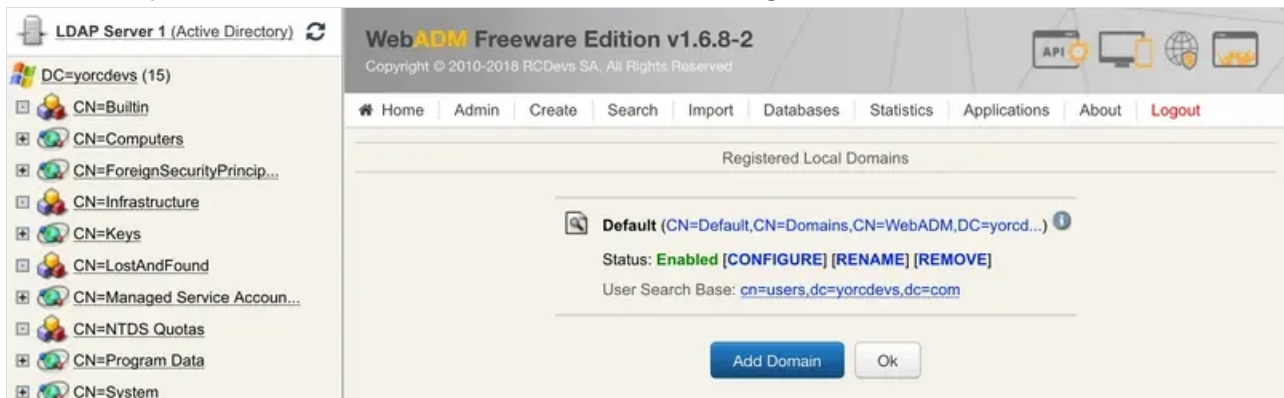
If WebADM is mainly configured with an AD and the LDAP MountPoint is also an AD, the schema setup will be the same as the main AD is configured with WebADM. This means, if your schema is extended on the main LDAP configured with WebADM, the remote LDAP will have the schema extension too.

4. Create a new WebADM Domain Object

We will now create a WebADM domain for this remote LDAP. Always through the WebADM Admin GUI, click on the **Admin** tab, **Local Domains**.



You should already have one domain created for the main LDAP server configured with WebADM.



Click on **Add Domain** button and configure a name for this object. I keep **LAB**.

LDAP Server 1 (Active Directory)

DC=yorcdevs (15)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
- CN=WebADM
- OU=Domain Controllers
- OU=LAB

Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Create Configuration Object of Type Domain

Mandatory attributes

Container: cn=Domains,cn=WebADM,dc=yorcdevs,dc=com [Select]

Common Name: LAB

Optional attributes

WebADM Object Type: WebADM LDAP Domain (Domain)

Organization: []

Organizational Unit: []

Description / Note: WebADM Domain for LAB LDAP MountPoint

WebADM Settings: You can edit this attribute once object is created.

WebADM User Data: This attribute cannot be created manually.

Proceed

Click on **Proceed**.

LDAP Server 1 (Active Directory)

DC=yorcdevs (15)

- CN=Builtin
- CN=Computers
- CN=ForeignSecurityPrincip...
- CN=Infrastructure
- CN=Keys
- CN=LostAndFound
- CN=Managed Service Accoun...
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users

WebADM Freeware Edition v1.6.8-2
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Create Configuration Object of Type Domain

Confirm object creation for cn=LAB,cn=Domains,cn=WebADM,dc=yorcdevs,...

Attribute	Value
DN	cn=LAB,cn=Domains,cn=WebA...
Common Name	LAB
WebADM Object Type	Domain
Description / Note	WebADM Domain for LAB LDA...

Create Object

And click **Create Object**. You are now in the object configuration. The only mandatory setting that you need to configure here is the **User Search Base**. Configure this setting to point to the OU/container where the remote LDAP is mounted. Another setting you may need to configure is the **Domain Name Alias** setting.

For example, during an authentication request, the domain or the workgroup is passed into the request. If the domain passed in the request doesn't match exactly with the WebADM domain name previously configured, on my side **LAB**, WebADM will not be able to perform the authentication because, for WebADM, the domain doesn't exist. So have a look at `/opt/webadm/logs/webadm.log` to see which domain is passed. If the authentication fails then add the domain passed in the request into the **Domain Name Alias** setting in your WebADM domain configuration.

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home

Admin

Create

Search

Import

Databases

Statistics

Applications

About

Logout

Object Settings for cn=LAB,cn=Domains,cn=WebADM,dc=yorcdevs,dc=com

☐ Disable Domain

☐ Yes
 ☒ No (default)

☒ User Search Base

The LDAP user search base corresponding to the domain.

☐ Group Search Base

The LDAP group search base corresponding to the domain.
This setting is ignored if WebADM uses only direct group_mode.
Note: Defaults to the User Search Base if not set.

☒ Domain Name Aliases

Comma-separated list of alternative domain names.

User Access Policy

Click on **Apply** , and you are now able to authenticate users from your both LDAP servers with only one WebADM/OpenOTP server. The number of MountPoint that you can configure is unlimited.

This manual was prepared with great care. However, RCDevs Security S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs Security S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs Security S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs Security S.A. The latter especially applies for data processing systems. RCDevs Security S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs Security. © 2024 RCDevs Security S.A., All Rights Reserved