



ACTIVE DIRECTORY READ-ONLY MODE

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.

Active Directory Read-Only mode

[Active Directory](#) [Microsoft Active Directory](#) [Read Only LDAP](#)

How To Configure WebADM with a Read-Only Active Directory

Important Note

That setup require an enterprise license which can only be issued by RCDevs team. Self-generated Freeware/Trial licenses are not supported. Regular enterprise license bought through the RCDevs web store are not supported.

In some circumstances, we can not write in the LDAP backend. In that case, we need to store some configurations in a local LDAP database and users extra information in a SQL database.

In this example, we will start with a WebADM server running with a local MariaDB and RCDevs Directory Server. It could be the [VMWare Appliance](#) or a new installation [WebADM Installation Guide](#). We will configure it to use a read-only Active Directory server.

1. WebADM Configuration

We edit `/opt/webadm/conf/webadm.conf` and change `webadm_account_oclasses` and `webadm_group_oclasses` parameters. It should contain the following class:

```
webadm_account_oclasses "person"
webadm_group_oclasses "group", "groupOfNames", "groupOfUniqueNames", "groupOfURLs",
"posixGroup"
```

We change also the data store to SQL:

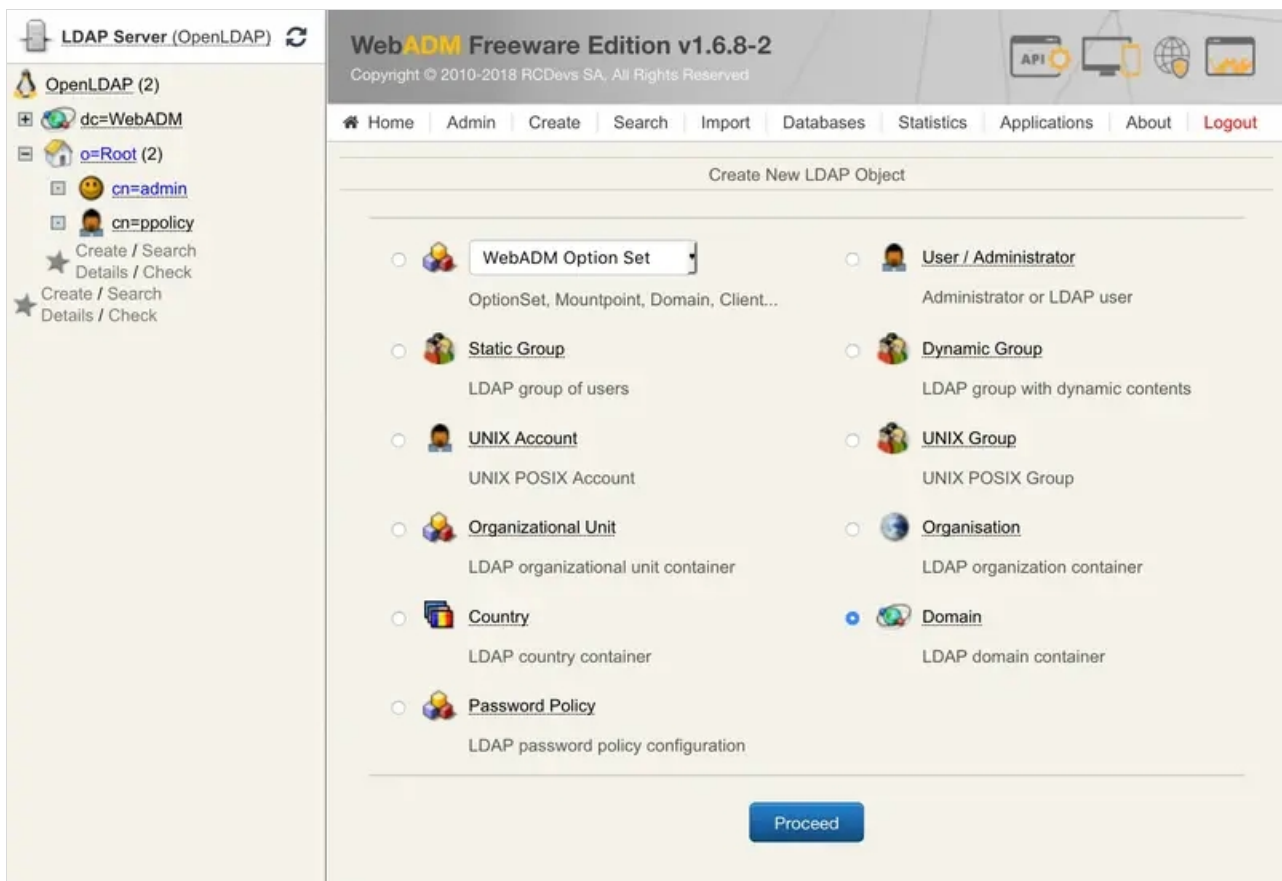
```
data_store SQL
```

We restart WebADM:

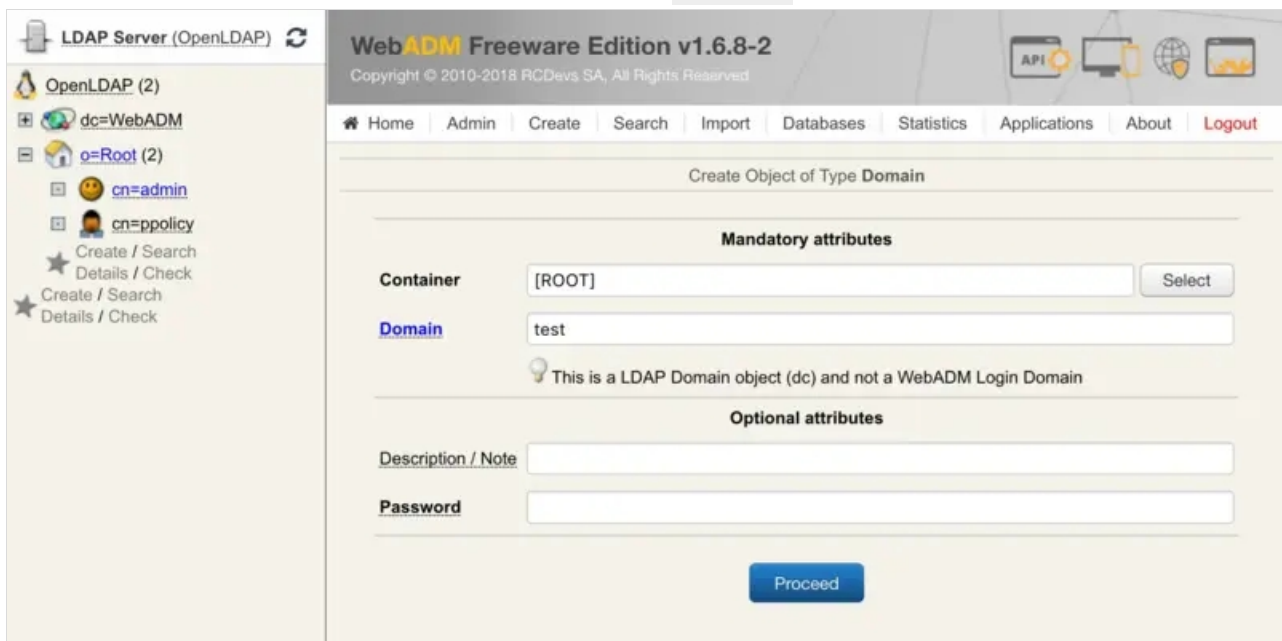
```
/opt/webadm/bin/webadm restart
```

2. Container Creation

In WebADM, we create a container for the mount point. We click on `Create`, we select `Domain` and we click on `Proceed`:



We enter a name for the domain, for example, `test`, and we click on **Proceed**:



We click on **Create Object**:

LDAP Server (OpenLDAP)

- OpenLDAP (2)
 - dc=WebADM
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
 - Create / Search
 - Details / Check
 - 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 Domain

Confirm object creation for domaincomponent=test

Attribute	Value
DN	domaincomponent=test
Domain	test

Create Object

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
 - Create / Search
 - Details / Check
 - 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 domaincomponent=test

LDAP Actions

- Delete this object
- Copy this object
- Export to LDIF
- Change password
- Advanced edit mode
- Create child object
- View child objects
- Export subtree

Object Details

Object class(es): domain

Object Name

test

Rename

Add Attribute (1)

Description / Note

Add

Domain

test

[delete attribute]

Apply Changes / Delete Selected

3. MountPoint Creation

To create a Mount Point, click on **Admin** tab and click on **LDAP Mount Points** box:

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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 rcvm7.local (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: 2018-11-19 14:26:42 Europe/Berlin (NTP check Ok)
Hardware Modules: No HSM Connected
WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)

Active LDAP Server: LDAP Server (127.0.0.1) 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 (1)
Create admin role templates for your 'other' administrators.

We click on **Add MountPoint** :

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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

We add a name and click on **Proceed** :

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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: dc=MountPoints,dc=WebADM Select

Common Name: test

WebADM Object Type: WebADM Mount Point (MountPoint)

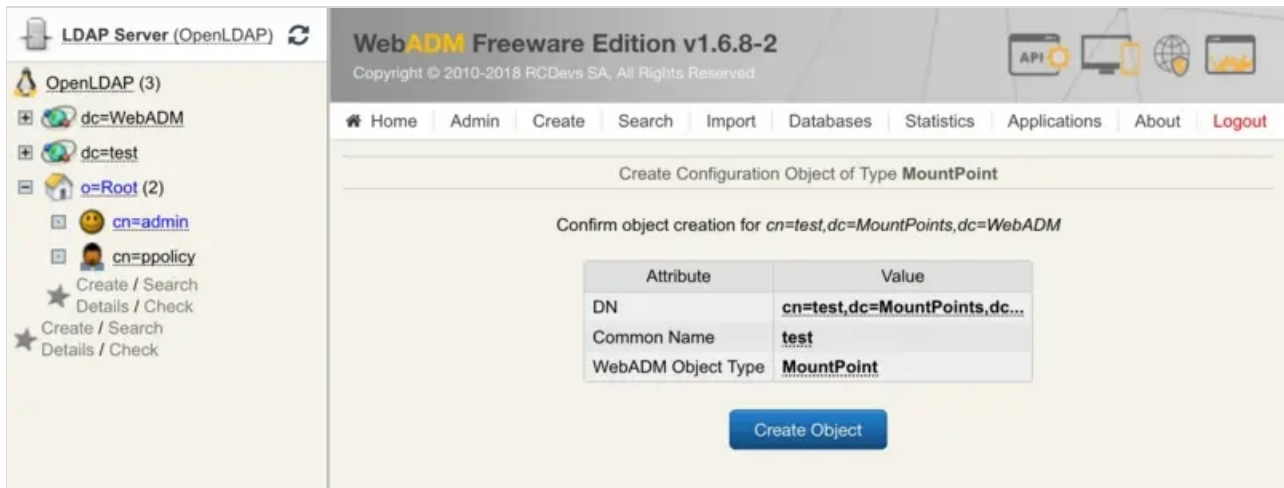
Optional attributes

WebADM Settings: This attribute is not available with SQL data store.

Description / Note:

Proceed

We click on **Create Object** :



We click on **Select** and choose the container previously created for *Mount DN*. Now, we add the IP address of the Active Directory server in *Host Name(s)* field, the port number, the tree base of the AD and AD user and password to connect to the LDAP.

Note

The AD user should have read access on the Active Directory.

We click on **Apply** :

LDAP Server (OpenLDAP)

OpenLDAP (3)

- dc=WebADM
- dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy

Create / Search
Details / Check

Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA. All Rights Reserved

HomeAdminCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

Object Settings for cn=test,dc=MountPoints,dc=WebADM

☐ Disable Mount Point

☐ Yes ☒ No (default)

☒ Mount DN

dc=test

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=test,dc=local

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

☒ Login DN

cn=administrator,cn=users,dc=test,dc=local

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

LDAP Server (OpenLDAP)

OpenLDAP (3)

- dc=WebADM
- dc=test (13)
 - 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
 - OU=Domain Controllers

Create / Search
Details / Check

o=Root (3)

- cn=admin
- cn=ppolicy
- cn=test_user

Create / Search
Details / Check


Create / Search
Details / Check

WebADM Freeware Edition v1.6.8-2

Copyright © 2010-2018 RCDevs SA. All Rights Reserved

HomeAdminCreateSearchImportDatabasesStatisticsApplicationsAboutLogout

Registered LDAP Mount Points

 test (cn=test,dc=MountPoints,dc=WebADM) ⓘ

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

Extended: **No** (EXTEND) (DETAILS) (SCHEMA)

Directory Type: microsoft

Server(s): 192.168.3.194:389

Encryption: NONE

Mount Point: [dc=test](#)

Tree Base: [dc=test,dc=local](#)

Login DN: [cn=administrator,cn=users,dc=test,dc=loc...](#)

Add MountPoint

Ok

4. Local Domain Creation

Now, we create a local domain for the mount point. A local domain works only with one LDAP backend, so the default local domain works only with OpenLDAP.

We click on **Admin** tab and on **Local Domains** box:

The screenshot shows the WebADM Freeware Edition v1.6.8-2 Admin interface. The left sidebar contains a tree view of LDAP servers under 'LDAP Server (OpenLDAP)'. The main content area displays 'WebADM Server Administration' with system status information and a grid of management boxes. The 'Local Domains (1)' box is highlighted, indicating one domain is currently configured.

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 rcvm7.local (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: 2018-11-19 17:09:59 Europe/Berlin (NTP check Ok)
Hardware Modules: No HSM Connected
WebADM Features: WebApps (Enabled), WebSrvs (Enabled), Manager (Enabled)

Active LDAP Server: LDAP Server (127.0.0.1) 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 (1)
Create admin role templates for your 'other' administrators.

Click on **Add Domain**:

The screenshot shows the 'Add Domain' dialog in the WebADM Freeware Edition v1.6.8-2 Admin interface. The dialog displays the details of the 'Default' domain, which is currently enabled and has a user search base of '[ROOT]'. The 'Add Domain' button is highlighted in blue.

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 Local Domains

Default (cn=Default,dc=Domains,dc=WebADM) ⓘ

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

User Search Base: [ROOT]

Add Domain Ok

We enter the name of the domain and click on **Proceed**.

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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
dc=Domains,dc=WebADM
Select

Common Name
test

WebADM Object Type
WebADM LDAP Domain (Domain)

Optional attributes

WebADM Settings
This attribute is not available with SQL data store.

Description / Note

Proceed

Click on **Create Object** :

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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

Confirm object creation for cn=test,dc=Domains,dc=WebADM

Attribute	Value
DN	cn=test,dc=Domains,dc=Web...
Common Name	test
WebADM Object Type	Domain

Create Object

We select the mount point as *User Search Base*. We can add domain name aliases, like *test.local* if needed, and we click on **Apply** :

LDAP Server (OpenLDAP)

- OpenLDAP (3)
 - dc=WebADM
 - dc=test
 - o=Root (2)
 - cn=admin
 - cn=ppolicy
- Create / Search Details / Check
- 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=test,dc=Domains,dc=WebADM

☐ Disable Domain
☐ Yes
☒ No (default)

☒ User Search Base
dc=test
Select

The LDAP user search base corresponding to the domain.

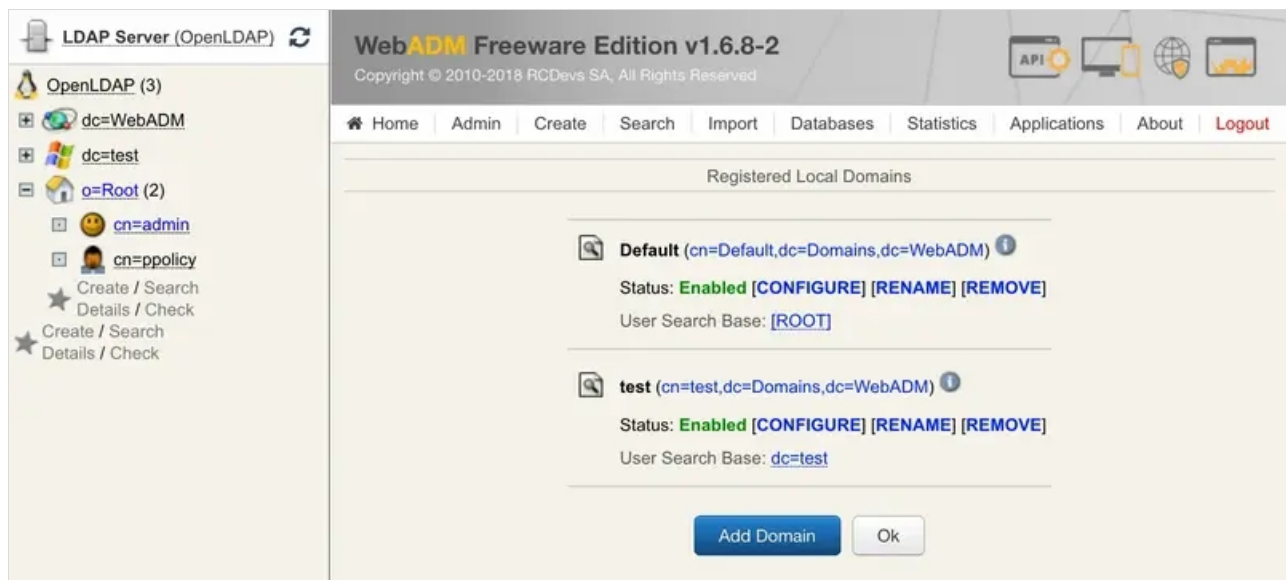
☐ Group Search Base
Select

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.

It's done:



Now, we can try an authentication by following this documentation [Authentication](#). We need to select the right local domain during the authentication. Otherwise, OpenOTP won't be able to find the user.

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