

# POLICIES

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](mailto:info@rcdevs.com).

# Policies

[Policy](#) [Policies](#) [Restrictions](#) [Conditional Access](#) [Agreement based logical access](#) [Access Restrictions](#) [Users Policies](#) [Groups Policies](#)

## 1. Overview

This documentation will explain policies configurable for Web Services and Web Applications under WebADM admin GUI. WebADM provides different kinds of policies :

- > default application configuration (weight 1),
- > per-group (weight 2),
- > per-user (weight 3),
- > per-application (weight 4-6).

Settings with the highest weight override settings with the lowest weight.

(e.g. for OpenOTP: My default OpenOTP settings require a LoginMode=LDAP only but the user who is trying to log in has a policy configured on his account with the LoginMode=LDAP+OTP. To be able to log in, this user will have to provide LDAP password+OTP).

## 2. Default policy (weight 1)

The first level of setting is defined under the applications configuration itself. Login on [WebADM Admin GUI](#) > [Applications](#) tab > [APPLICATION\\_NAME](#) > [CONFIGURE](#) . All web services and web applications provided by RCDevs can be configured here for the first level of settings. If no other settings are configured on a user, a group or in a client policy, then the default configuration will be applied.

## 3. Per-group policy (weight 2)

Applications can be configured per-group. Per-group policies override the default applications configuration. Login on [WebADM Admin GUI](#) , select a group on which you want to apply other settings than the default settings already configured on the application configuration itself. To be able to configure a policy on a group, the group must be activated under WebADM. When you are on the group object, click on [Activate](#) button > [Proceed](#) > [Extend Object](#) .

Object CN=master,CN=Users,DC=yorcdevs,DC=com ⓘ

**LDAP Actions**  
Delete this object  
Copy this object  
Move this object  
Export to LDIF  
Add members  
Advanced edit mode

**Object Details**  
Object class(es): group  
Group activated: **No Activate Now!** ⓘ

Object Name: master Rename  
Add Attribute (2): Description / Note Add  
Add Extension (2): UNIX Group Add

Group Member: [add values] [delete attribute] CN=Administrateur,CN=Users,DC=yorcdevs,DC=com Goto  
Account Created: 24-05-2018 [delete attribute]  
Account Modified: 29-04-2019 [delete attribute]  
Object GUID: {9332121f-a348-4aaf-aeaa-e77e993caa86} [delete attribute]  
Object SID: S-1-5-5-352321536-651592091-2289946412-94239843-3372482560 [delete attribute]  
Login Name: master  
Account Type: SAM Group Object [delete attribute]  
Group Type: Security (Global)

Apply Changes / Delete Selected

Your group is now Activated and ready for per-group policy. On the group object > **Object Details** > **WebADM settings: NONE [CONFIGURE]** click on **CONFIGURE** button.

Object CN=master,CN=Users,DC=yorcdevs,DC=com ⓘ

**LDAP Actions**  
Delete this object  
Copy this object  
Move this object  
Export to LDIF  
Add members  
Advanced edit mode

**Object Details**  
Object class(es): group  
WebADM settings: **None [CONFIGURE]**  
Group activated: **Yes Deactivate** ⓘ

**Application Actions**  
[Secure Password Reset \(1 actions\)](#)  
[User Self-Registration \(1 actions\)](#)  
[SMS Hub Server \(1 actions\)](#)

Object Name: master Rename  
Add Attribute (3): Description / Note Add  
Add Extension (1): UNIX Group Add

Group Member: [add values] [delete attribute] CN=Administrateur,CN=Users,DC=yorcdevs,DC=com Goto  
Account Created: 24-05-2018 [delete attribute]  
Account Modified: 29-04-2019 [delete attribute]  
Object GUID: {9332121f-a348-4aaf-aeaa-e77e993caa86} [delete attribute]  
Object SID: S-1-5-5-352321536-651592091-2289946412-94239843-3372482560 [delete attribute]  
Login Name: master  
Account Type: SAM Group Object [delete attribute]  
Group Type: Security (Global)

Apply Changes / Delete Selected

On the next page, you can select which application you want to reconfigure for the selected group.

Application Settings for CN=master,CN=Users,DC=yorcdevs,DC=com

Applications

- ✓ MFA Authentication Server
- Shared Session Server
- SSH Public Key Server
- QR Login & Signing Server
- OpenID & SAML Provider
- Secure Password Reset
- User Self-Service Desk
- User Self-Registration
- YubiKeys Self-Registration

### Authentication Policy

☐ **Login Mode** LDAPOTP (Default)

The login mode (required login factors) should be adjusted via Client Policies.

- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

☒ **OTP Type** SMS

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- PROXY: Forward requests to another RADIUS server (for migrations).

☐ **OTP Fallback** TOKEN

Fallback OTP Type to be used as secondary authentication method.  
LASTOTP let users use the last validated OTP which expires after a delay.  
Use DISABLED to disabled fallback if there is a configuration by default.

☐ **OTP Password Length** 6 (Default)

Note: This setting is ignored for OCRA Tokens as OTP length is part of the OCRA Suite.  
Warning: Changing this setting after having registered OATH Tokens will invalidate these Tokens.

☒ **OTP PIN Prefix** Yes No (default)

When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP].  
The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.

☐ **Challenge Session Timeout** 90 (Default)

Timeout to wait for a challenge response (in seconds).  
Note: SMS OTP and MAIL OTP may requires longer timeouts.

In this example, I reconfigure some settings for OpenOTP: **OTP Type** and I enabled the **OTP PIN Prefix** for that group.

### ⚠ Note

With this extra-settings configured on the group, if a member of that group doesn't have a phone number and a PIN Prefix already configured on his account, then the login will be a failure with an error message like: Account missing required data.

## 4. Per-user policy (weight 3)

Applications can be configured per-user. Per-user policies override the default applications configuration and the per-group policies. Login on **WebADM Admin GUI**, select a user account on which you want to apply other settings than the default settings. To be able to configure a policy on a user account, the user must be activated under WebADM. When you are on the user object, click on **Activate** button > **Proceed** > **Extend Object**.



Object cn=Administrator,CN=Users,DC=yorcdevs,DC=com ⓘ

LDAP Actions

- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Advanced edit mode

Object Details

Object class(es): **person, user**

User activated: **No Activate Now!** ⓘ

Object Name	Administrator	Rename
Add Attribute (16)	Country	Add
Add Extension (3)	Inetorgperson	Add

Account Created [delete attribute]	29-04-2019
Account Modified [delete attribute]	29-04-2019
Object GUID [delete attribute]	{dd7cb055-3c7e-4556-8047-76bb8aa0a681}
Account Flags [delete attribute]	Normal Account      Flags: Keep Unchanged
Last Bad Logon Password [delete attribute]	Never      Reset
Last Logoff [delete attribute]	Never      Reset
Last Logon [delete attribute]	Never      Reset
Last Password Set [delete attribute]	29-04-2019      Reset
Object SID [delete attribute]	S-1-5-5-352321536-651592091-2289946412-94239843-1275854848
Account Expires [delete attribute]	Never      Reset
Logon Count [delete attribute]	0
Login Name	Administrator
Account Type [delete attribute]	SAM User Account

Apply Changes / Delete Selected

Your user is now Activated and ready for per-user policy. On the user object > **Object Details** > **WebADM settings: NONE [CONFIGURE]** click on **CONFIGURE** button.

Object cn=Administrator,CN=Users,DC=yorcdevs,DC=com ⓘ

LDAP Actions

- Delete this object
- Copy this object
- Move this object
- Export to LDIF
- Change password
- Create certificate
- Unlock WebApp access
- Advanced edit mode

Object Details

Object class(es): **webadmAccount, person, user**

**WebADM settings: NONE [CONFIGURE]**

WebADM data: **NONE [EDIT]**

User activated: **Yes Deactivate** ⓘ

Logs and inventory: [WebApp](#), [WebSrv](#), [Inventory](#)

Application Actions

- Secure Password Reset (1 actions)
- User Self-Registration (1 actions)
- MFA Authentication Server (13 actions)
- SMS Hub Server (1 actions)
- SSH Public Key Server (3 actions)

Object Name	Administrator	Rename
Add Attribute (18)	Country	Add
Add Extension (2)	Inetorgperson	Add

Account Created [delete attribute]	29-04-2019
Account Modified [delete attribute]	29-04-2019
Object GUID [delete attribute]	{dd7cb055-3c7e-4556-8047-76bb8aa0a681}
Account Flags [delete attribute]	Normal Account      Flags: Keep Unchanged
Last Bad Logon Password [delete attribute]	Never      Reset
Last Logoff [delete attribute]	Never      Reset
Last Logon [delete attribute]	Never      Reset
Last Password Set [delete attribute]	29-04-2019      Reset
Object SID [delete attribute]	S-1-5-5-352321536-651592091-2289946412-94239843-1275854848
Account Expires [delete attribute]	Never      Reset
Logon Count [delete attribute]	0
Login Name	Administrator
Account Type [delete attribute]	SAM User Account

Apply Changes / Delete Selected

On the next page, you can select which application you want to reconfigure for the selected user.

Application Settings for cn=Administrator,CN=Users,DC=yorcdevs,DC=com

**Applications**

- ✓ MFA Authentication Server
- Shared Session Server
- SSH Public Key Server
- QR Login & Signing Server
- OpenID & SAML Provider
- Secure Password Reset
- User Self-Service Desk
- User Self-Registration
- YubiKeys Self-Registration

**Authentication Policy**

☒ **Login Mode** LDAPU2F

The login mode (required login factors) should be adjusted via Client Policies.

- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

☐ **OTP Type** TOKEN (Default)

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- PROXY: Forward requests to another RADIUS server (for migrations).

☒ **OTP Fallback** MAIL

Fallback OTP Type to be used as secondary authentication method.  
LASTOTP let users use the last validated OTP which expires after a delay.  
Use DISABLED to disabled fallback if there is a configuration by default.

☐ **OTP Password Length** 6 (Default)

Note: This setting is ignored for OCRA Tokens as OTP length is part of the OCRA Suite.  
Warning: Changing this setting after having registered OATH Tokens will invalidate these Tokens.

☐ **OTP PIN Prefix** Yes No (default)

When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP].  
The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.

☐ **Challenge Session Timeout** 90 (Default)

Timeout to wait for a challenge response (in seconds).  
Note: SMS OTP and MAIL OTP may requires longer timeouts.

In this example, I changed the **LoginMode** to **LDAPMFA** and **OTP Fallback** to **SMS** for the user.

## ⚠ Note

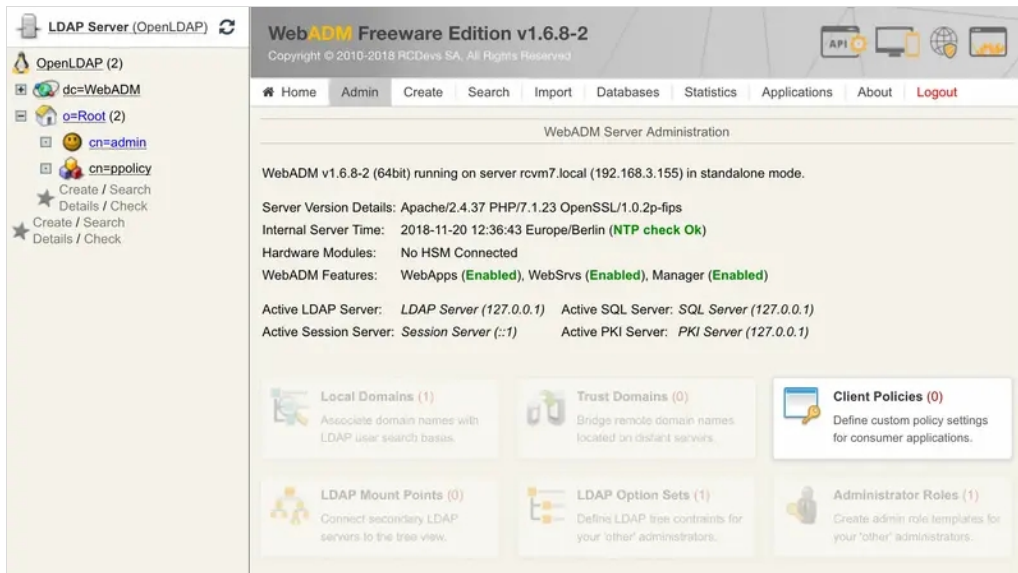
With that extra-settings configured on the user account, if the user doesn't have a FIDO key or phone number already configured on his account, then the login will be a failure with an error message like : Account missing required data.

## 5. Client policy

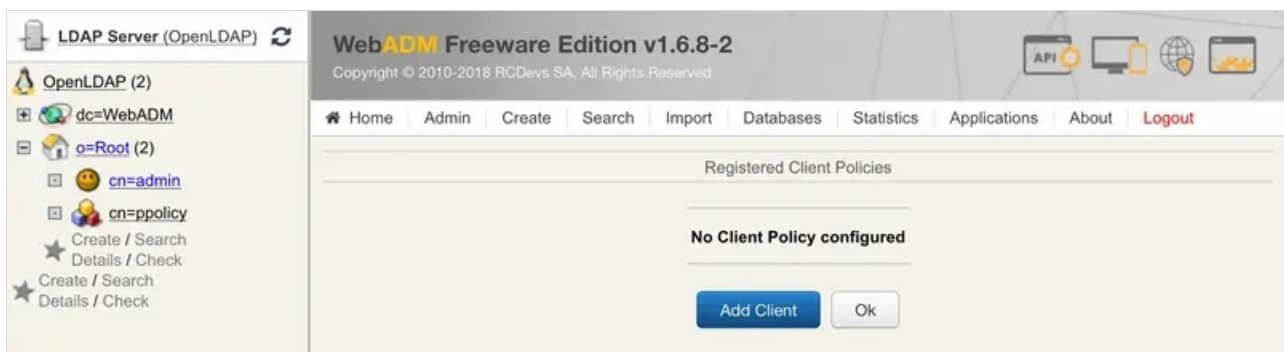
### 5.1 Default client policy (weight 4)

A policy can be configured per-application. Client policy overrides every other policy already configured on a group or on a user account. A client policy can also be defined per-group (weight 5) and per-network (weight 6) under the client policy configuration itself.

First, log in on the WebADM Graphical Unit Interface. Click on the **Admin** tab and you will find a box named **Client Policies**.



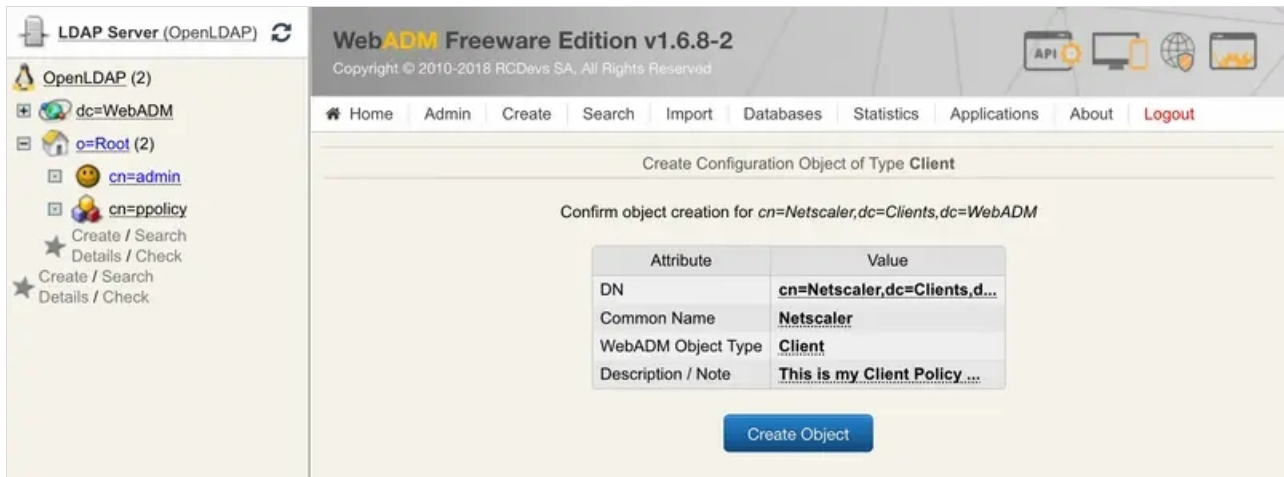
Click on it and on the next page, click on **Add Client** :



Enter a Common Name, if you want a description and click on **Proceed** :



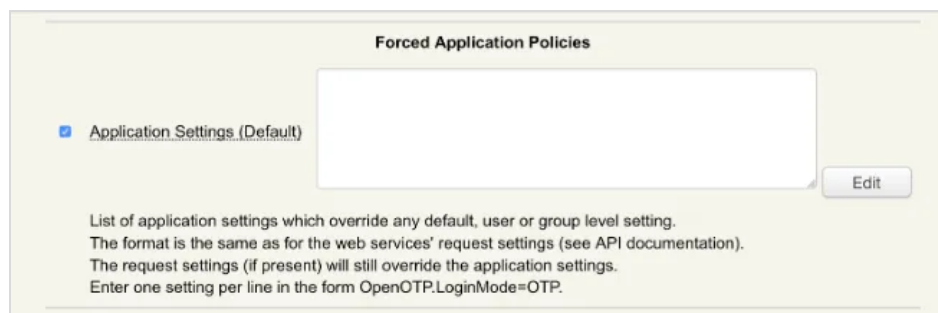
On the next screen, click on the **Create Object** button.



A client Policy object has now been created. We are now able to configure this client policy.

Many settings can be applied here like which users/groups/networks the client policy will be applied, allowed/excluded hours, which domain...

If you scroll down a little bit, you will find the setting named **Forced Application Policies**.



Check the box on left and click on the **Edit** button. On the next screen, you are able to completely reconfigure an application.

In our example, we will choose OpenOTP:



Applications

☒ OpenOTP
 

OpenSSO

SpanKey

TiQR

Application Settings

Authentication Policy

☒ Login Mode
 

OTP

The login mode (required login factors) should be adjusted via Client Policies.

- LDAPOTP: Require both LDAP and OTP passwords.
- LDAPU2F: Require both LDAP and FIDO response.
- LDAPMFA: Require LDAP and either OTP or FIDO.
- LDAP: Require LDAP password only.
- OTP: Require OTP password only.

☒ OTP Type
 

MAIL

- TOKEN: OATH HOTP/TOTP/OCRA, YubiKey or MobileOTP Token.
- SMS: SMS one-time password (On-demand or Prefetched).
- MAIL: Email one-time password (On-demand or Prefetched).
- LIST: Pre-generated OATH OTP password list (to be printed).
- PROXY: Forward requests to another RADIUS server (for migrations).

☐ OTP Fallback
 

TOKEN

Fallback OTP Type to be used as secondary authentication method.

LASTOTP let users use the last validated OTP which expires after a delay.

Use DISABLED to disabled fallback if there is a configuration by default.

☐ OTP Password Length
 

6 (Default)

Note: This setting is ignored for OCRA Tokens as OTP length is part of the OCRA Suite.

Warning: Changing this setting after having registered OATH Tokens will invalidate these Tokens.

☒ OTP PIN Prefix
 

☒ Yes
 ☐ No (default)

When enabled a static prefix has to be prepended to any OTP password in the form [PIN][OTP].

The OTP Prefix must be registered first and must be at least 4 alpha-numeric characters.

☒ Challenge Mode Supported
 

☐ Yes (default)
 ☒ No

You can disable challenged OTP/FIDO if your client applications does not support it.

OpenOTP assumes concatenated OTP passwords when disabled with simpleLogin requests.

Note: Challenge is required for Simple-Push, FIDO, OATH-OCRA and on-demand SMS/Mail OTP.

☐ Challenge Session Timeout
 

90 (Default)

Timeout to wait for a challenge response (in seconds).

Note: SMS OTP and MAIL OTP may requires longer timeouts.

☐ Challenge Session Protection
 

☐ Yes
 ☒ No (default)

Prevent a new challenge session to override a previously started session for a user.

When enabled users must wait the session timeout when a previous challenge was not responded.

☐ Challenge Password Retry
 

☐ Yes
 ☒ No (default)

Allow one password retry with challenge mode.

Retry uses multiple challenges and is not compatible with many integrations.

So, you can choose every setting you want and reconfigure the OpenOTP application for your client application. The client policy overrides the default application settings, user and group settings.

After editing the configuration, you can click on the **Apply** button to save the configuration.

## 5.2 Per-group extra policy (weight 5)

In the same way, a client policy can be overridden for a specific group. In **Per-Group Extra Policies** menu, enable the **group list** setting and then click the **Select** button. You are now in the edition mode, and you can select the group you want in the left LDAP tree just by clicking on it.

**Per-Group Extra Policies**

☒ **Group List**

CN=domain admins,CN=Users,DC=yorcdevs,DC=com

Select

List of LDAP groups with dedicated settings (override any defined Application Setting).

☒ **Application Settings (Group)**

OpenOTP.LoginMode=LDAPU2F

Edit

If the users belong to one of the above group(s), these additional settings are enforced.

In this example, I reconfigure the setting **LoginMode** to **LDAPMFA** for the group **CN=domain admins,CN=Users,DC=yorcdevs,DC=com**.

Per-group policy overrides the default policy configuration.

### 5.3 Per-network extra policy (weight 6)

In the same way, a client policy can be overridden for login coming from a specific network. In **Per-Network Extra Policies** section, check the box on the left of **Internal Networks** setting and put the network value for which network you want to reconfigure the policy. In **Application Settings (Internal)**, click the **Edit** button, and you can now reconfigure the application you want for the specified network.

**Per-Network Extra Policies**

☒ **Internal Networks**

192.168.3.0/24

Comma-separated list of IP addresses with netmasks corresponding to your internal network(s).

☒ **Application Settings (Internal)**

OpenOTP.LoginMode=LDAP

Edit

If the client is used from the above internal network(s) these additional settings are enforced.  
If both Group and Internal settings are enforced, Network settings apply last (higher weight).

In this example, I reconfigure the setting **LoginMode** to **LDAP** for login requests coming from 192.168.3.0/24 network.

Per-Network policy overrides per-group policy.

#### Note

WebADM can match a policy with a client application through a client ID, NAS-Identifier or IP of the client application. A dedicated section for Client ID is described below.

## ⚠ Warning

To be able to use that setting, your client application should be configured to forward the user IP address to WebADM.

### 5.4 Dynamic Application Settings

The Dynamic application settings allow you to dynamically change setting of Web applications or Web Services when source IP is coming from a botnet or public VPN endpoints.

- › Level 1: This policy mode will enter in the **Step-Up** mode where Step-Up settings can be defined below.
- › Level 2: This policy mode completely deny the access to the system when IP source is considered as botnet IP and apply the **Step-Up** settings when IP source is considered as public VPN endpoints.

Botnet and public VPN endpoints are coming from a database hosted nad maintained on RCDevs cloud infrastructure and are fetched from ...

In the following example, I configured the Step-Up mode for:

- › LDAP + OTP authentication,
- › A PIN Prefix must be provided,
- › Send back a fake OTP challenge when a wrong LDAP password or OTP Prefix is entered

**Dynamic Application Settings**

☒ **Risk-Based Policy Mode** Level1 ▾

Automatically enforce Step-Up settings or access deny when the source IP matches a blacklist:  
- Use 'Level1' for Step-Up-only when the source IP matches a botnet or a VPN endpoint.  
- Use 'Level2' for denying access for botnet IPs and Step-Up settings for VPN endpoints.

☒ **Step Up Settings**

`OpenOTP.LoginMode=LDAPOTP  
OpenOTP.OTPPrefix=Yes  
OpenOTP.ChallengeFake=Yes`

Edit

Overrides application settings when the policy is enforced in step-up mode (increased security).  
Note: Dynamic settings do not apply when Group Members or Internal Networks are matched.

☒ **Step Down Settings**

`OpenOTP.LoginMode=LDAP`

Edit

Overrides application settings when the policy is enforced in step-down mode (decreased security).

Once my setting are applied, you can see the following from the Policy menu:

➤ **Nextcloud** (CN=Nextcloud,OU=Clients,OU=WebADM,OU=YOAA...)

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

Mode: **Normal (Risk-Based Level1)** [CHANGE MODE] ⓘ

Default Domain: SUPPORT

Application Settings: OpenOTP: 4

You can click on the **CHANGE MODE** button to manually change the applied mode. For example, you can manually **Step-Down**, **Step-Up** or **Deny** the access for a specific period. This settings can also be enforced when it matches Per-Group and/or Per-Network policies. By default, it is applied to the default application setting policy (weight 4) if nothing else specified is specified.

## 5.5 Contract Signing Settings

In client policies, you now have the possibility to request your users that want to log in on a system to sign a document before they can access it.

- The document can be an HTML form, a PDF located on the file system or accessible through a URL. In that example I used a document stored on the file system. For Cloud tenants, only HTTP(S) scheme is allowed.
- Once the document has been signed by your user(s), the signed version can be sent to a recipient. Only one recipient can be configured. If you want more than one person to receive the signed document, you have to create a mailing list on your mail server which include the desired recipients.
- Once the document is signed, you can also choose if you want to store it in the SQL database of WebADM server in the Record table or not.
- The desired **Signing mode** can be configured, you can choose between **Standard** and **Advanced**. Please refer to [OpenOTP Signature documentation](#) to get details on the signature types. If **Advanced** mode is chosen, you can configure the **scope** (Local CA, Global CA or eIDAS) that you want to use. This can be configured under **Default Application Settings > MFA Authentication Server > Confirmation & Signing** section:

**Confirmation & Signing**

☐ **Offline Confirmation** ☒ Yes (default) ☐ No  
Allows the mobile Token to display a fallback OTP when the Mobile Endpoint cannot be reached.  
Offline confirmation is not supported with signing or when a file or form is provided.

☐ **Reject Comment** ☒ Yes (default) ☐ No  
The user is prompted for an optional comment when rejecting a configuration or signature.

☐ **Upload Signed Files** ☐ Yes ☒ No (default)  
Update the signed file at its original location when the file was provided via a download URI.  
If successfully uploaded, the prepared file is not returned via the Confirm / Sign API.

☐ **Advanced Signature Scope**   
- Local: Advanced signature with user certificates issued by internal WebADM CA.  
- Global: Advanced signature with user certificates issued by RCDevs Root CA.  
- eIDAS: Qualified signature with external eIDAS signing devices (ex. eID Cards).

☐ **CaDES Packaging Mode**   
Return CaDES detached signature or file embedding format (default).

☐ **eIDAS Signature Check** ☐ Yes ☒ No (default)  
Allow eIDAS signing only for trusted EUTL identities (recommended).

- › The signature timeout is corresponding to the time that the signature request is available on the backends and the time the user has to sign the document. Once reached, the signature request is expired on the backends and user will have to restart the login from scratch to trigger a new signature request. Once the document is signed, the user will be able to log in.
- › Signature validity correspond to the validity of the signed document. Once exceeded, the document will need to be signed again by the user.

If the document had any modification then the user will be automatically prompted to sign the new version before being able to authenticate on the system.

### Contract Signing Settings

☒ **Document URI** /opt/webadm/conf/login\_agreement.pdf

With HTML documents: The consent form to be displayed and confirmed by users.  
 With other document types: The agreement to be signed or approved at login time.  
 A 'file' 'http(s)', 'redis' or 'couchbase' URI must be used (ex. https://my.server.com/myfile.pdf).  
 Only http(s) scheme is allowed with Cloud tenants!

☒ **Send to Email** legal@company.com

Email address to which the signed agreements should be forwarded.

☒ **Store as Record** 
☒ Yes ☐ No (default)

Stores the signed agreements as downloadable attachments in the 'Record' database.

☒ **Signing Mode** Advanced ▼

Only PDF contracts can be signed with 'Standard' mode.  
 Non-PDF files in 'Standard' mode are signed with 'Advanced' mode anyway.

☒ **Signature Timeout** 5 ▼

Mobile signature request timeout in minutes.

☒ **Signature Validity** 90 ▼

Require re-signing after the configured number of days.

## 6. How to match my client policy with my client application

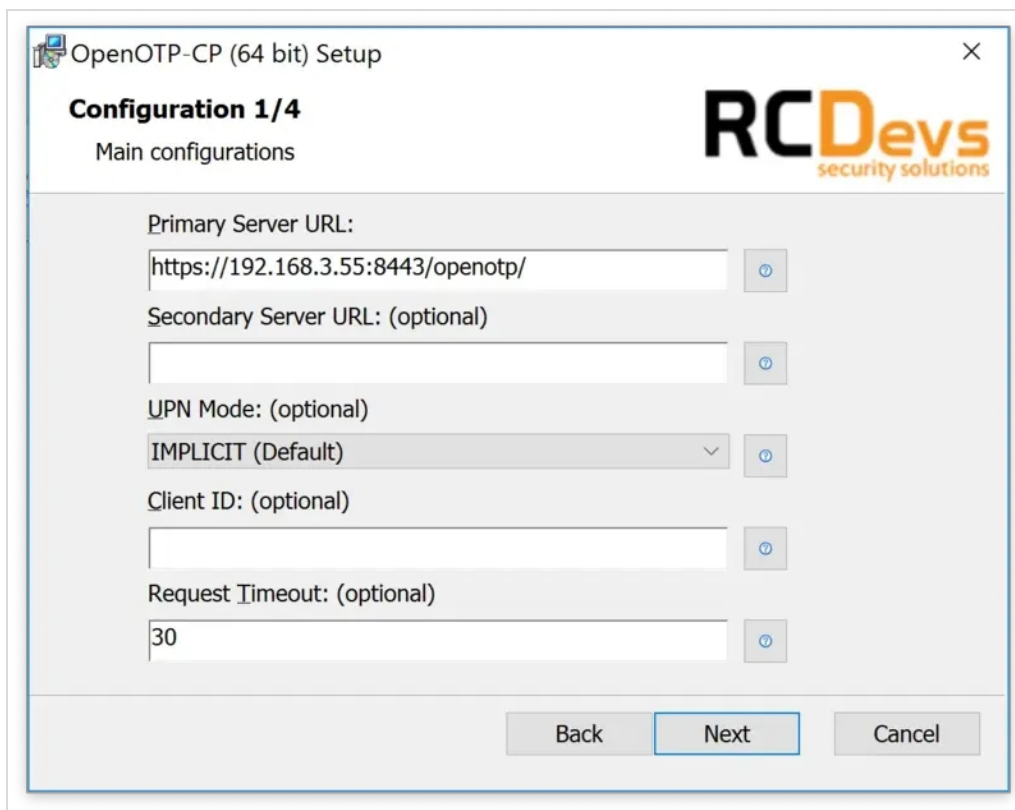
The matching between a client policy configured under WebADM and a client application can be done in different ways.

### 6.1 Client ID

With RCDevs products/plugins (e.g : OpenOTP Credential Provider, ADFS plugin, Spankey client...) a setting named **Client ID** can be configured during the plugin/application installation.

For OpenOTP Credential provider for Windows:





**OpenOTP-CP (64 bit) Setup**

**Configuration 1/4**  
Main configurations

**RCDevs**  
security solutions

Primary Server URL:  
 ⓘ

Secondary Server URL: (optional)  
 ⓘ

UPN Mode: (optional)  
 ⓘ

Client ID: (optional)  
 ⓘ

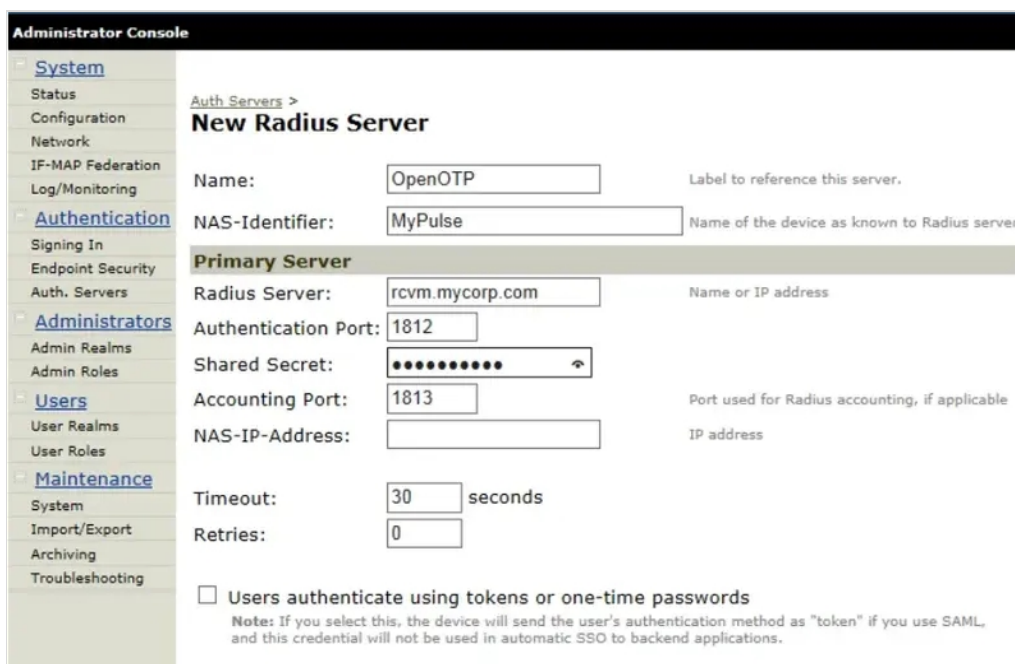
Request Timeout: (optional)  
 ⓘ

Back Next Cancel

I can put **WINDOWS** in the Client ID field and create a client policy named **WINDOWS** on WebADM and then the matching will operate.

## 6.2 Nas-Identifier

In some third-party product, you can define a setting named **NAS-Identifier**. In this example with Pulse Secure, I configured a **NAS-Identifier** named **MyPulse**. So I will create a client policy named **MyPulse** in WebADM to match the policy with my Pulse VPN.



**Administrator Console**

**System**

- Status
- Configuration
- Network
- IF-MAP Federation
- Log/Monitoring

**Authentication**

- Signing In
- Endpoint Security
- Auth. Servers

**Administrators**

- Admin Realms
- Admin Roles

**Users**

- User Realms
- User Roles

**Maintenance**

- System
- Import/Export
- Archiving
- Troubleshooting

**Auth Servers > New Radius Server**

Name:  Label to reference this server.

NAS-Identifier:  Name of the device as known to Radius server

**Primary Server**

Radius Server:  Name or IP address

Authentication Port:

Shared Secret:  ⓘ

Accounting Port:  Port used for Radius accounting, if applicable

NAS-IP-Address:  IP address

Timeout:  seconds

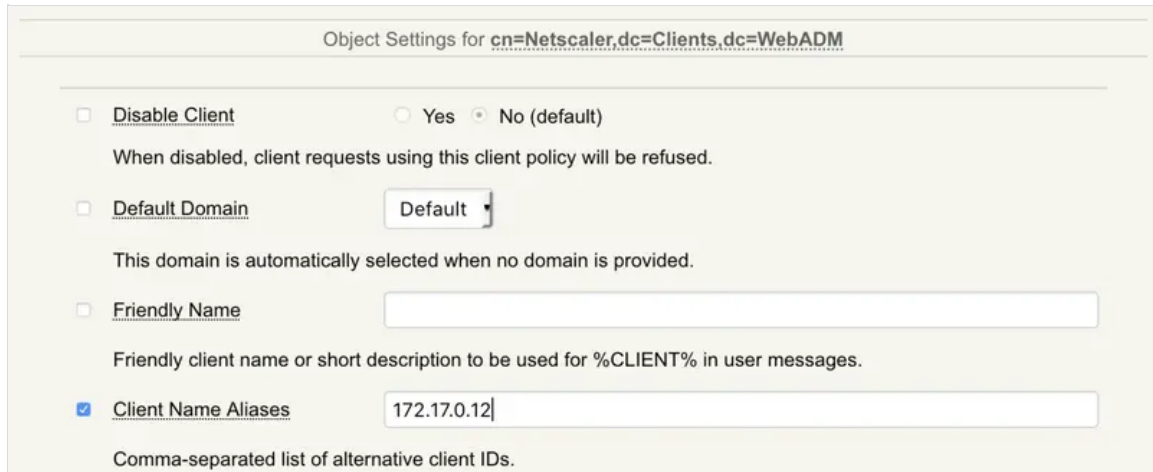
Retries:

☐ Users authenticate using tokens or one-time passwords

Note: If you select this, the device will send the user's authentication method as "token" if you use SAML, and this credential will not be used in automatic SSO to backend applications.

## 6.3 Client application IP(s)

If you are not able to configure a NAS-ID or Client ID on your application, you can match a client policy with the IP address of your client application. The IP address of your client should be configured in the client policy itself. When you edit the client policy, you can find a setting named **Client Name Aliases**. Put the IP address of your client here and policy will match during an authentication.



Object Settings for **cn=Netscaler,dc=Clients,dc=WebADM**

☐ **Disable Client** ☐ Yes ☒ No (default)  
When disabled, client requests using this client policy will be refused.

☐ **Default Domain**   
This domain is automatically selected when no domain is provided.

☐ **Friendly Name**   
Friendly client name or short description to be used for %CLIENT% in user messages.

☒ **Client Name Aliases**   
Comma-separated list of alternative client IDs.

### Note

With the Client Name Aliases setting, you are able to match many clients with only one client policy. You just have to put IPs comma-separated.

## 7. Web Application policy

You can define client policy for Self-User registration, Self-Service Desk and Password Reset applications. To do it, you just have to create a client policy with the short name of the application. Short names are:

- > pwreset
- > selfdesk
- > selfreg

Create a client policy for the application you want and reconfigure the Application settings under the client policy configuration menu.

## 8. Check policy matching through WebADM logs

Try an authentication on your client application, log in on the WebADM GUI and click on **Databases** tab. In the **System Log Files** section, click on **WebADM Server Log file**.

```

[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] New openotpSimpleLogin SOAP request
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Username: administrateur
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Domain: yorcdevs.com
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Password: xxxxxxxx
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Client ID: NETSCALER
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Source IP: 172.17.0.12
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Enforcing client policy: NETSCALER (matched
client ID)
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Registered openotpSimpleLogin request
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Resolved LDAP user:
CN=Administrateur,CN=Users,DC=yorcdevs,DC=com (cached)
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Resolved LDAP groups: proprietaires
crateurs de la stratgie de groupe,admins du domaine,administrateurs de
\entreprise,administrateurs du schma,administrateurs,utilisateurs du bureau
\distance,groupe de rpllication dont le mot de passe rod c est refus
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Started transaction lock for user
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found user language: EN
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 1 user mobiles: +3520000000
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 1 user emails: xxxxxx@rcdevs.com
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 3 user certificates
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 38 user settings:
LoginMode=LDAPOTP,OTPTType=TOKEN,OTPLength=6,ChallengeMode=Yes,ChallengeTimeout=90,MobileTim
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTTime=300,ListChallengeMode=
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 10 user data:
LoginCount,RejectCount,OTPPrefix,TokenType,TokenKey,TokenState,TokenID,Device1Name,Device1Data,De
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Found 1 registered OTP token (TOTP)
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Requested login factors: LDAP & OTP
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] LDAP password Ok
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Challenge required
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Sent push notification for token #1
[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Waiting 28 seconds for mobile push response
[2017-12-06 14:21:05] [192.168.3.56] [OpenOTP:LZ33NOWW] Received mobile request (authentication)
[2017-12-06 14:21:05] [192.168.3.56] [OpenOTP:LZ33NOWW] > Session: kq7sxP3OabLXpygl
[2017-12-06 14:21:05] [192.168.3.56] [OpenOTP:LZ33NOWW] > Encoded OTP Password: xxxxxx
[2017-12-06 14:21:05] [192.168.3.56] [OpenOTP:R8MFCYSQ] Found challenge session started 2017-12-
06 14:21:01
[2017-12-06 14:21:06] [172.17.0.12] [OpenOTP:R8MFCYSQ] PUSH password Ok (token #1)
[2017-12-06 14:21:06] [172.17.0.12] [OpenOTP:R8MFCYSQ] Updated user data
[2017-12-06 14:21:06] [172.17.0.12] [OpenOTP:R8MFCYSQ] Sent success response

```

You can show in the previous transaction logs, that the Nas-Identifier passed by the client application is NETSCALER and the client match with the corresponding policy.

[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] > Client ID: NETSCALER

...

[2017-12-06 14:21:01] [172.17.0.12] [OpenOTP:R8MFCYSQ] Enforcing client policy: NETSCALER  
(matched client ID)

So my client policy is applied and settings defined in this policy will be required/available during an authentication coming from that client.

You can check in the same way if a Client ID or IP address match with your client policy.

*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*