



SWIFT ALLIANCE ACCESS

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.

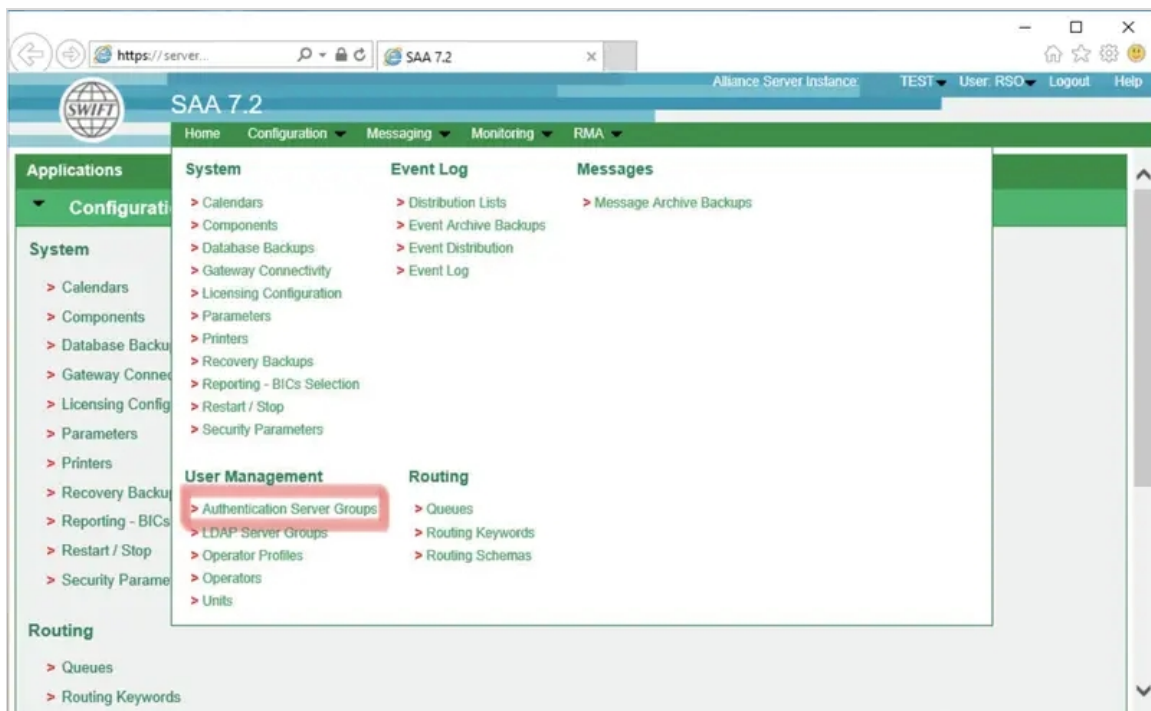
1. Overview

In this documentation, we will demonstrate how to integrate OpenOTP with Swift Alliance Access 7.2 (AA). LDAP and Radius protocols can be used to integrate AA with OpenOTP. Here, we will demonstrate the Radius integration. This guide has been written with the help of the official Swift Alliance Access 7.2 Administrator Guide. So here, we will use RADIUS one-time passwords authentication method and not the embedded two-factor authentication module implemented in AA. WebADM and OpenOTP server(s) should be already configured with Radius Bridge component(s).

2. Swift Alliance Access Configuration

2.1. Authentication Server Groups

First, we will configure the Radius servers at the AA level. Log into the AA Web management page with the LSO (Left Security Officer) account and configure a new authentication server group.



Once you are under Radius Authentication Servers Group, you are able to configure the required information to communicate with Radius Bridge.

Authentication Server Group Details Help

General Primary Server Secondary Server

Current Configuration

Host Address

Key Left

Key Right

Show Clear Text

Port Number

Local Port Number

Future Configuration

Host Address

Key Left

Key Right

Show Clear Text

Port Number

Local Port Number

Cancel Save

Configure the Primary Server in the Future configuration section.

Authentication Server Group Details Help

General Primary Server Secondary Server

Current Configuration

Host Address

Key Left

Key Right

Show Clear Text

Port Number

Local Port Number

Future Configuration

Host Address

Key Left

Key Right

Show Clear Text

Port Number

Local Port Number

Cancel Save

- > **192.168.3.54** : Is my Radius Bridge, WebADM & OpenOTP Server IP.
- > **Key Left** : This should be a value of 16 characters.
- > **Key Right** : This should be a value of 16 characters.
These two keys (bilateral key) will be used as Radius secret in the Radius Bridge clients definition.
- > **Port Number** : This is the port used by the Radius Bridge service.

Once this configuration is done, you can click on the save button. If you have a WebADM/OpenOTP cluster then configure the secondary server the same way. These changes should be approved by the RSO (Right Security Officer) account. Once the RSO has approved the new configuration, the Radius server configuration on Alliance Access is done.

⚠ Important note from Swift

The usage of one-time passwords is set per operator. To activate the use of one-time passwords, in the Operator Details for each security officer, the Authentication Type must be set to RADIUS one-time password and the Authentication Server Group must be selected. Each change must be approved by RSO and LSO account.

3. Radius Bridge Configuration

3.1 Clients Configuration

To allow Swift Alliance Access to communicate over Radius protocol, we have to configure the AA Radius client in Radius Bridge configuration. To configure the client edit `/opt/radiusd/conf/clients.conf` file. At the end of this file, you will find the client definition.

```
[root@webadm ~]# vi /opt/radiusd/conf/clients.conf
```

Add a new client for allowing Swift AA:

```
client Swift_AA {
    ipaddr = 192.168.3.56
    secret = Left_key_1234567Right_key_123456
}
```

- > `192.168.3.56`: Is the Swift AA IP who will contact Radius Bridge.
- > `Left_key_1234567Right_key_123456`: Is the concatenation of left and right keys defined in Alliance Access configuration.

Once the Swift Alliance Access client is configured in `clients.conf` file, you will have to restart Radius Bridge service:

```
[root@webadm ~]# /opt/radiusd.bin/radiusd restart
```

These changes must be done on each Radius Bridge if you are working with a WebADM/OpenOTP cluster.

3.2 Radiusd Advanced Configuration (Optional)

To map the User IP information in `WebADM WebSrv logs`, you will have to configure the attribute used by Swift which contains the User IP in Radius Bridge configuration in the `source_attribute` setting.

```
[root@webadm ~]# vi /opt/radiusd/conf/radiusd.conf
```

```
# Source attribute
# This is the RADIUS attribute in which the RADIUS client can pass the end user source IP address to
# OpenOTP. Attribute must be of type IPAddr.
# By default the source attribute is set to Calling-Station-Id & PaloAlto-Client-Source-IP.
source_attribute = "Swift_user_ip_attribute"
```

Restart radius bridge service after modifying this file.

4. OpenOTP Client Policy Configuration

We will now configure a client policy for Swift authentications. Login on the WebADM Administrator GUI > **Admin** tab > **Client Policies** > **Add Client**.

Name the client policy object which will be created, on my side **Swift** and optionally add a description.

The screenshot shows the WebADM Freeware Edition v1.6.8-4 Administrator GUI. The left sidebar displays the LDAP Server 1 (Active Directory) tree with various organizational units. The main content area is titled 'Create Configuration Object of Type Client'. The form includes the following fields:

- Mandatory attributes:**
 - Container:** cn=Clients,cn=WebADM,dc=yorcdevs,dc=com (with a 'Select' button)
 - Common Name:** Swift
- Optional attributes:**
 - WebADM Object Type:** WebADM Client Policy (Client)
 - Organization:** (empty field)
 - Organizational Unit:** (empty field)
 - Description / Note:** Authentication Policy for Alliance Access
 - WebADM Settings:** You can edit this attribute once object is created.
 - WebADM User Data:** This attribute cannot be created manually.

A blue 'Proceed' button is located at the bottom of the form.

Click on **Proceed** button and then **Create Object**.

You are now in the Swift Client Policy configuration menu. The first setting you will have to configure is the **Client Name Aliases** where you will configure the AA IP which will contact the OpenOTP. On my side **192.168.3.56**.

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 (24)
 - [-] CN=Administrator
 - [-] CN=Allowed RODC Password...

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Object Settings for cn=Swift,cn=Clients,cn=WebADM,dc=yorcdevs,dc=com

Disable Client Yes No (default)

When disabled, client requests using this client policy will be refused.

Default Domain Default

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.

Next step is to configure the authentication policy to require MFA on Swift AA. You will have to edit the **Forced Application Policies** under the client policy menu. Please, activate **Application Settings** and then click on **Edit**.

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

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA, All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Forced Application Policies

Application Settings (Default)

List of application settings which override any default, user or group level setting.
The format is the same as for the web services' request settings (see API documentation).
The request settings (if present) will still override the application settings.
Enter one setting per line in the form OpenOTP.LoginMode=OTP.

Now, activate **Login Mode: LDAPOTP**, **OTP Type: TOKEN**, **Challenge Mode Supported: No** and **Challenge Password Retry: No**. Finally, click on **Apply**.

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

Application Settings

Applications

- ✓ OpenOTP
- OpenSSO
- SpanKey
- TiQR

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 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 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.

You should have this result like below:

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 (24)
 - ✓ CN=Administrator
 - ✓ CN=Allowed RODC Password...
 - ✓ CN=Cert Publishers

WebADM Freeware Edition v1.6.8-4
Copyright © 2010-2018 RCDevs SA. All Rights Reserved

Home Admin Create Search Import Databases Statistics Applications About Logout

If set, the client cannot be used during the specified week hours.

UID Attributes

Restricted list of LDAP login attributes replacing the attributes configured via uid_attrs in webadm.conf.

Forced Application Policies

Application Settings (Default)

```
OpenOTP.LoginMode=LDAPOTP
OpenOTP.OTPType=TOKEN
OpenOTP.ChallengeMode=No
OpenOTP.ChallengeRetry=No
```

Edit

List of application settings which override any default, user or group level setting.
The format is the same as for the web services' request settings (see API documentation).
The request settings (if present) will still override the application settings.
Enter one setting per line in the form OpenOTP.LoginMode=OTP.

Configuration was modified. Press 'Apply' to save changes!

Click on the `Apply` button to save your changes.

⚠ Important Note

OpenOTP.ChallengeMode=No is mandatory with Swift AA because Swift didn't implement the Radius challenge in their product. So even with Radius, you will have only 2 fields on the AA login page, one for the Username and the other for the password. In the password field, you will have to put LDAP password and OTP password in concatenated mode.

Your client policy for Swift is now configured. You can test a login on AA with OpenOTP.

⚠ Push Login Authentication method

Swift can work with OpenOTP and Push login but if the Push Notification is not received on your phone, or if you are not able to Approve the login with your phone, the authentication will fail because no fallback method is available in that scenario. You will have to retry the authentication and the failed login counter will be increased at Swift level. After x login failure for the same account, the account will be blocked at the Swift level.

5. LDAP User and Swift user mapping

If your Swift users already have an account in your Directory then it's possible to do mapping at the LDAP level between the LDAP account and the Swift local account. This mapping is done by adding the Swift login name value in an LDAP attribute. This attribute must be configured in `/opt/webadm/conf/webadm.conf` file in `uid_attrs` setting. By default, with the Active Directory template, the following ones are available.

```
uid_attrs      "cn", "samAccountName", "userPrincipalName"
```

If one of these attributes is not used then you can use one of them and configure the Swift username on that attribute. If the default attributes are already used in your organization, then you can use another one. For example `uid`, in that case, you have to add the `uid` attribute in `uid_attrs` setting in `webadm.conf` like below:

```
uid_attrs      "cn", "samAccountName", "userPrincipalName", "uid"
```

When you will perform a login from Swift with your Swift account, then the Swift username will be sent to WebADM/OpenOTP and will match with the corresponding LDAP account.

6. Authentication Logs

After performing authentication on Swift Alliance Access, you are able to check logs on the WebADM side. Through the WebADM Admin GUI > `Databases` > `WebADM Server Log Files` you should have something like this below:


```

[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] New openotpSimpleLogin SOAP request
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] > Username: Administrateur
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] > Password: xxxxxxxxxxxxxxxx
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] > Options: RADIUS,-U2F
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Enforcing client policy: Swift (matched server IP)
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Registered openotpSimpleLogin request
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Resolved LDAP user:
CN=Administrateur,CN=Users,DC=yorcdevs,DC=com
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Resolved LDAP groups: master,propriétaires
créateurs de la stratégie de groupe,admins du domaine,administrateurs de l'entreprise,administrateurs
du schéma,utilisateurs du bureau à distance,administrateurs,groupe de réplication dont le mot de passe
rodc est refusé
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Started transaction lock for user
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found user fullname: administrateur
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found user language: EN
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 1 user mobiles: xxxxxxxxxxxx
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 1 user emails: support@rcdevs.com
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 1 user certificates
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 43 user settings:
LoginMode=LDAPOTP,ExpireNotify=MAIL,OTPTType=TOKEN,OTPLength=6,ChallengeMode=No,ChallengeTime
1:HOTP-SHA1-6:QN06-
T1M,DeviceType=FIDO2,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,PrefetchExpire=10,
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 20 user data:
LoginCount,RejectCount,LastOTP,ListInit,ListState,OTPPrefix,NowaitState,TokenType,TokenKey,TokenState,T
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Found 1 registered OTP token (TOTP)
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Challenge mode disabled (checking
concatenated passwords)
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Requested login factors: LDAP & OTP
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] LDAP password Ok
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] TOTP password Ok (token #1)
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Updated user data
[2018-12-11 17:43:07] [192.168.3.54] [OpenOTP:4IT5D3I6] Sent success response

```

And under [Databases](#) > [WebSrv Logs](#) you should have something like this below:

| Event Time | Application | Client | User DN | User IP | Host IP | Session ID | Details |
|------------------------|-------------|---------|-----------------------------------|---------|--------------|------------|--|
| 2018-12-11 17:43:07... | OpenOTP | ✓ Swift | CN=Administrateur.CN=Users.DC=... | [NA] | 192.168.3.56 | 4IT5D3I6 | Authentication success (LDAP & TOKEN #1) |
| 2018-12-11 17:43:07... | OpenOTP | ✓ Swift | CN=Administrateur.CN=Users.DC=... | [NA] | 192.168.3.56 | 4IT5D3I6 | New openotpSimpleLogin.request (yorcdevs/Administrateur) |

As you can see here, we only see the host IP which is the Swift AA IP in the audit logs. To map the User IP information, please refer to 3.2 chapter.

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