MAC OSX CREDENTIAL PROVIDER

Limited Warranty

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

MAC OSX Credential Provider

Mac OSX

1. Product Documentation

This document is an installation guide for the OpenOTP Credential Provider for Mac OSX. Hence, the installation or configuration of WebADM, including token registration is not covered in this guide. For installation and usage guides to WebADM refer to the RCDevs WebADM Installation Guide and the RCDevs WebADM Administrator Guide available through the RCDevs online documentation Website.

2. Product Overview

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

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.

3. Preliminary Information

Administrative/elevated permissions are necessary on any Mac OS to correctly set up and/or change the OpenOTP Credential Provider's configuration.

To correctly setup the provider, please gather the following information. You will need to enter during the installation process:

- The URI(s)s of the OpenOTP web-service(s) (mandatory)
  - These URIs are mandatory, the client needs to know where the OpenOTP SOAP network API can be reached. At least one URI is necessary.
- A custom login text or tile caption (optional)
  - A text that is displayed on the Mac OS login pane.
- A client ID (optional)
  - An ID to identify a particular client on the server-side.
- The WebADM certificate authority (CA) file (mandatory for offline login)
- SOAP timeout delay (optional)

4. Installation and Configuration

The Credential Provider's setup and configuration are done in about 5 Minutes. The installer is the only utility that is needed to be set up and configures the provider. The provider can be automatically deployed to your clients.

4.1 Local Installation

First, you have to download OpenOTP Credential Provider for Mac OS available on RCDevs Website.

Extract files from the archive on your Mac and run the pkg file. The installer will start, on the first screen, click on the `Continue` button and then click `Install`. The installer will ask you to enter your credentials to continue the installation. Enter your credentials and click `Install software`.

After that another window is prompted: Click `Next` and you are on the first configuration page. On this page, you have to configure the OpenOTP `service URL(s)`. The `request timeout` is set to 30 seconds by default and we advise you to keep this default value. A `client ID` can be configured to match with a client policy on WebADM/OpenOTP server. To have more information on how to configure a client policy, have a look here. The UPN mode can be configured on `Implicit` or `Explicit`.

You can click on `Next`.

On the next screen, some advanced features can be configured. Every setting here is optional.

- Certificate Authority File, this setting attempts the CA certificate of your WebADM instance. The WebADM CA certificate can be downloaded at `https://webadm_ip/cacert`. Note that the WebADM CA is mandatory to use the `Offline authentication mode`.
- The next setting is HTTP Proxy. Configure your HTTP proxy and port if needed.
- Server Selection Policy setting allows you to set up how the failover will works. You have 3 options: `Ordered`, `Balanced` and `Consistent`.
- Next setting is the `Offline mode`. Offline mode allows users to login on the Machine, even if the WebADM/OpenOTP servers are not available. The offline mode requires a `Push Login Infrastructure` in place and OpenOTP Software Token Application on your mobile. Have a look here for more information about Push Login Infrastructure.
- The last settings allow you to configure a custom login text and a custom logo.

Configuration is done, you can click on the `Done` button and the installation is finished.

> ⚠ Note
>
> Before logout to perform a login with an OTP, we advise you to start an SSH session and keep this session open until you perform a success login. If for any reason, OpenOTP Credential Provider for Mac OS is not able to contact the WebADM/OpenOTP server, you will not be able to log in on your Mac anymore. If it's the case, with the SSH session previously opened, you will be able to execute the uninstall script provided with the installer package to remove the plugin from your Mac and log in again.

4.2 Modifying the Configuration

After the installation, you can modify the configuration by editing this file:

```
vi
/Library/Security/SecurityAgentPlugins/OpenOTPAuthPlugin.bundle/Contents/Resources/config
```

Witch looks like this:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
        <key>ca_file</key>
        <string>/Users/Shared/ca.crt</string>
        <key>client_id</key>
        <string>MacOS</string>
        <key>login_text</key>
        <string>Hello OTP User !</string>
        <key>logo_path</key>
        <string></string>
        <key>offline_mode</key>
        <string>0</string>
        <key>policy</key>
        <string>1</string>
        <key>proxy_host</key>
        <string></string>
        <key>proxy_port</key>
        <string></string>
        <key>server_url_1</key>
        <string>https://192.168.3.54:8443/openotp/</string>
        <key>server_url_2</key>
        <string></string>
        <key>soap_timeout</key>
        <string>30</string>
        <key>upn_mode</key>
        <string>0</string>
</dict>
</plist>
```

5. Online Authentication Logins

Now the CP is installed and configured then we will perform logins.

5.1 Push Login

In this scenario, WebADM and OpenOTP are configured to work in Push Login Mode. Please have a look here to know how to

configure a push login infrastructure.

I'm now on the login screen of my Mac, I have to enter my username and password:

I press enter and a push login request is sent to my mobile phone.

I press the `Approve` button and I log in to my Mac.

I'm now logged in to my Mac.

5.1.1 Push Login Logs

```
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] > Username: admin
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] > Domain: Default
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] > Client ID: MacOS
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] > Source IP: 192.168.3.237
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] > Options: -LDAP,OFFLINE
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Registered openotpSimpleLogin
request
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Resolved LDAP user:
CN=Admin,CN=Users,DC=yorcdevs,DC=com (cached)
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Started transaction lock for
user
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found user fullname: Admin
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found 1 user mobiles:
+33xxxxxxxx
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found 1 user emails:
xxxxxxx@rcdevs.com
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found 40 user settings:
LoginMode=LDAPMFA,ExpireNotify=MAIL,OTPType=TOKEN,OTPLength=6,ChallengeMode=Yes,Challenge
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=S

[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found 7 user data:
LoginCount,RejectCount,TokenType,TokenKey,TokenState,TokenID,TokenSerial
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Found 1 registered OTP token
(TOTP)
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] User has no U2F device
registered
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Requested login factors: OTP
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Authentication challenge
required
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Sent push notification for
token #1
[2018-08-14 10:07:48] [192.168.3.237] [OpenOTP:MW9OVN20] Waiting 28 seconds for mobile
push response
[2018-08-14 10:07:51] [192.168.3.56] [OpenOTP:LXAC4UUS] Received mobile request from
192.168.3.192 (authentication)
[2018-08-14 10:07:51] [192.168.3.56] [OpenOTP:LXAC4UUS] > Session: zUSOZQflEVexDiZG
[2018-08-14 10:07:51] [192.168.3.56] [OpenOTP:LXAC4UUS] > Encoded OTP Password: xxxxxx
[2018-08-14 10:07:51] [192.168.3.56] [OpenOTP:MW9OVN20] Found mobile session started
2018-08-14 10:07:48
[2018-08-14 10:07:51] [192.168.3.237] [OpenOTP:MW9OVN20] PUSH password Ok (token #1)
[2018-08-14 10:07:51] [192.168.3.237] [OpenOTP:MW9OVN20] Updated user data
[2018-08-14 10:07:51] [192.168.3.237] [OpenOTP:MW9OVN20] Sent success response
```

5.2 Challenge Login

I will now perform a login in Challenge mode. I'm on the login screen of my Mac and I have to enter my username and password:

I press enter and OpenOTP send me a challenge request to enter my OTP code:

I type in my OTP code and I log in to on my Mac.

5.2.1 Challenge Login Logs

```
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] New openotpSimpleLogin SOAP
request
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] > Username: admin
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] > Domain: Default
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] > Client ID: MacOS
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] > Source IP: 192.168.3.237
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] > Options: -LDAP,OFFLINE
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Registered openotpSimpleLogin
request
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Checking OpenOTP license for
YOANN
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] License Ok (12/50 active
users)
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Resolved LDAP user:
CN=Admin,CN=Users,DC=yorcdevs,DC=com
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Started transaction lock for
user
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found user fullname: Admin
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found 1 user mobiles:
+33658506140
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found 1 user
emails:supportt@rcdevs.com
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found 40 user settings:
LoginMode=LDAPMFA,ExpireNotify=MAIL,OTPType=TOKEN,OTPLength=6,ChallengeMode=Yes,Challenge
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTime=300,ListChallengeMode=S

[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found 6 user data:
LoginCount,RejectCount,LastOTP,TokenType,TokenKey,TokenState
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Last OTP expired 2018-08-14
10:15:17
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Found 1 registered OTP token
(TOTP)
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] User has no U2F device
registered
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Requested login factors: OTP
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Authentication challenge
required
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Updated user data
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Started OTP authentication
session of ID FrEobYpzXosxrVVd valid for 90 seconds
[2018-08-14 11:33:23] [192.168.3.237] [OpenOTP:NQR7W1V4] Sent challenge response
```

```
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] New openotpChallenge SOAP
request
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] > Username: admin
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] > Domain: Default
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] > Session: FrEobYpzXosxrVVd
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] > OTP Password: xxxxxx
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] Registered openotpChallenge
request
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] Found authentication session
started 2018-08-14 11:33:23
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] Started transaction lock for
user
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] TOTP password Ok (token #1)
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] Updated user data
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] No registered token supports
offline mode
[2018-08-14 11:33:35] [192.168.3.237] [OpenOTP:NQR7W1V4] Sent success response
```

6. Offline Authentication

An offline mode is available in our Mac OS Credentials Provider and I enabled this option during the configuration.

Note

Offline authentication is available for Windows and MacOS login and requires at least versions: WebADM 1.6, OpenOTP 1.3.6, OpenOTP Token 1.4.

Prerequisites

One online login is required to enable offline login mode! If you manage to directly login with an offline connection it will not work. You must have a working Push Login infrastructure to use the offline mode.

When your laptop is offline, you are now able to log in with an OTP. So for this test, I stop WebADM services to simulate the offline mode. Like above, enter your LDAP Credentials on the first screen.

OpenOTP Credential Provider for Mac OS is not able to contact OpenOTP server so, it will switch automatically to the offline mode. The offline mode will prompt you a QRCode.

You have to scan this QRCode with the OpenOTP Token application. Open your OpenOTP Token application, press on the camera button and scan the QRCode.

After scanning the QRCode, a window with an OTP is displayed on your smartphone like below:

Enter your OTP and you are logged on.

6.1 Offline Logs (Mac OS Logs)

```
Admins-Mac: admin$ log stream | grep OpenOTP
```

```
2018-08-14 12:59:47.420300+0300 0x8b23     Default     0x8000000000008f3a   1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:Deinit
2018-08-14 12:59:50.053045+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTPAuthPlugin:OpenOTPLogin:runMechanism
2018-08-14 12:59:50.060642+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) EndpointHelper:OpenOTPInit
2018-08-14 12:59:50.060750+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:ReadConfiguration
2018-08-14 12:59:50.060808+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:Init
2018-08-14 12:59:50.060854+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:Default
2018-08-14 12:59:50.060892+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:Default done
2018-08-14 12:59:50.061045+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:ReadConfiguration done
2018-08-14 12:59:50.061267+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTP: init ok
2018-08-14 12:59:50.061313+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTP: init status ok
2018-08-14 12:59:50.072328+0300 0x8b23     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTPAuthPlugin:loading view
2018-08-14 12:59:50.076728+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) CallEndpoint called
2018-08-14 12:59:50.108939+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTPAuth:General:OpenOTP Login
2018-08-14 12:59:50.111770+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Unable to connect to any address. Failed to open a
socket
2018-08-14 12:59:50.111903+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) No response
2018-08-14 12:59:50.112250+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) Searching for offline state for user: admin
2018-08-14 12:59:50.112340+0300 0x8d79     Default     0x0                  1890
SecurityAgent: (OpenOTPAuthPlugin) General:getOfflineState
2018-08-14 13:00:23.509089+0300 0x8b23     Default     0x8000000000008fad   1890
SecurityAgent: (OpenOTPAuthPlugin) OpenOTP:OfflineLogin:Vertification succeed
2018-08-14 13:00:23.509650+0300 0x8b23     Default     0x8000000000008fad   1890
SecurityAgent: (OpenOTPAuthPlugin) Configuration:Deinit
```

7. Uninstallation

7.1 SSH

In case you are not able to log in on your Mac after the plugin installation, you can log in to the machine over SSH and run the uninstall script.

```
ssh admin@192.168.3.237
Password:
Last login: Tue Aug 14 16:40:57 2018
Admins-Mac:~ admin$
```

Go on the OpenOTPAuthPlugin folder that you had previously extracted before the plugin installation:

```
cd /Users/admin/Desktop/OpenOTPAuthPlugin.x.x/
```

```
Admins-Mac:OpenOTPAuthPlugin.1.0 admin$ ls -l
total 12200
-rw-r--r--  1 admin  staff  6234934  8 aoû 17:51 OpenOTPAuthPlugin-1.0.pkg
-rw-r--r--@ 1 admin  staff      827 12 jul 12:40 README.md
-rwxr-xr-x@ 1 admin  staff      500  8 aoû 13:02 uninstall
```

Execute the uninstall script to remove the OpenOTP plugin for MacOS:

```
Admins-Mac:OpenOTPAuthPlugin.1.0 admin$ ./uninstall
Password:
YES (0)
YES (0)
Admins-Mac:OpenOTPAuthPlugin.1.0 admin$
```

The plugin has been removed and now you are able to log in on your Mac without any OTP.

7.2 Single-User Mode

⚠ Note

If you are not able to access your Mac through SSH then start your Mac in single-user mode.

For macOS High Sierra and Mojave:

Turn on your Mac, then immediately press and hold Command-S. Now you can enter the following UNIX commands.

```
...
*** Single-user boot ***
Root device is mounted read-only
...

localhost:/ root# mount -uw /
localhost:/ root# cd /Volumes/Macintosh\ HD/tmp
Macintosh HD is the name of my Hard Drive on my Mac.
localhost:tmp root# sudo security authorizationdb read system.login.console > tmp.plist
localhost:tmp root# nano tmp.plist
Remove the line with <string>OpenOTPAuthPlugin:OpenOTPLogin</string>
localhost:tmp root# sudo security authorizationdb write system.login.console <
tmp.plist
localhost:tmp root# rm tmp.plist
localhost:tmp root# rm -rf /Volumes/Macintosh\
HD/Library/Security/SecurityAgentPlugins/OpenOTPAuthPlugin.bundle
localhost:tmp root# rm -f /Volumes/Macintosh\
HD/var/db/securityagent/Library/Preferences/com.rcdevs.states.plist
localhost:tmp root# exit
```

The plugin has been removed and now you are able to log in on your Mac without any OTP.