

NETIQ

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

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.

2. NetIQ Installation and Initial Configuration

- › We used the NetIQ appliance version 4.3 downloaded from the Microfocus website (trial version).
- › ISO file name: `AM_43_AccessManagerAppliance_Eval-0831.iso`
- › It's SUSE Linux:

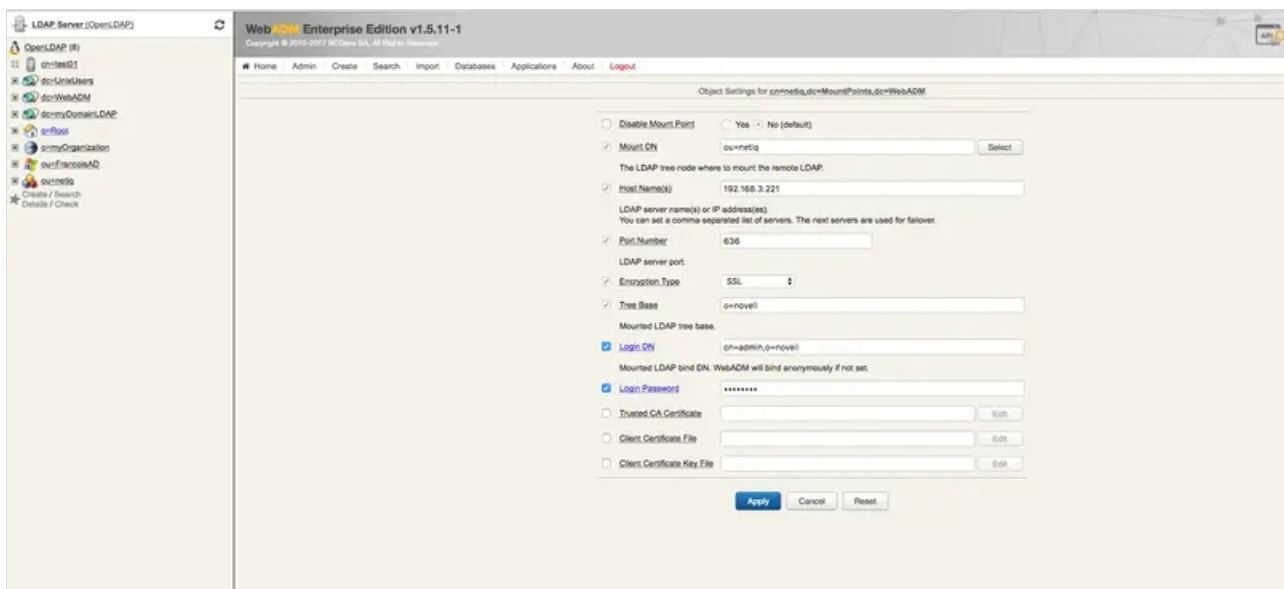
```
netiqam:~ # cat /etc/SuSE-release
SUSE Linux Enterprise Server 11 (x86_64)
VERSION = 11
PATCHLEVEL = 4
NetIQ Access Manager Appliance 4.3.0.0-391 (x86_64)
```

- › NetIQ is a resource-hungry application, we used the following setup:
 - › 2 Cores VM
 - › 8 GB RAM
 - › 50GB HDEven with this configuration, we received one warning about disk size (the minimum requirement is 100GB). *Lack of resources, especially RAM, can cause erratic behavior and failures to start.*
- › NetIQ is configured during the initial boot of the VM, using all default values when possible.
- › *Remember to take note of all configuration details.*
- › The admin account DN for WebADM is: `cn=admin,o=novell`
- › Our settings for the WebADM mount point:

Mount DN:	ou=netiq
Host Name(s):	192.168.3.221
Port Number:	636
Encryption Type:	SSL
Tree Base:	o=novell
Login DN:	cn=admin,o=novell
Login Password:	It's set during the initial setup.

3. Mount eDirectory on WebADM

- › Create a container (e.g. an OU) - our one is called `netiq`.
- › Create the mount point using:
 - › The container as `Mount DN`.
 - › `Login DN` set to “cn=admin,o=novell” (in our case).
 - › The NetIQ specific details (see above table as an example).



- › Extend the eDirectory schema (You must have write access to the LDAP schema to complete the operation).

LDAP Server (OpenLDAP)

WebADM Enterprise Edition v1.5.11-1

Object: ou=netiq (20)

LDAP Actions:

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

Object Details:

Object classes: Organization
 Mountpoint object: oDirectory
 Server type: Novell (SSL)
 Server info: [Details] [Schema]
 Schema extended: No [Extend]

Object Name: netiq

Add Attribute (116): AccountBalance

Permissions:

2#entry#o=netiq,ou=netiq,dc=netiq,dc=com
 RO Entry on loginScript for o=netiq
 2#entry#o=netiq,ou=netiq,dc=netiq,dc=com
 RO Entry on printJobConfiguration for o=netiq
 32#subtree#o=netiq,ou=netiq,dc=netiq,dc=com
 RW Subtree on All Attributes Rights for o=netiq,ou=netiq,dc=netiq,dc=com
 16#subtree#o=netiq,ou=netiq,dc=netiq,dc=com
 RW Subtree on Entry Rights for o=netiq,ou=netiq,dc=netiq,dc=com

DelectIntruder: TRUE

IntruderAttemptInterval: 1800

LoginIntruderLimit: 7

Organization: novell

Objectclass: organization, ndslogproperties, ndscontainerlogproperties, top

Apply Changes / Delete Selected

LDAP Server (OpenLDAP)

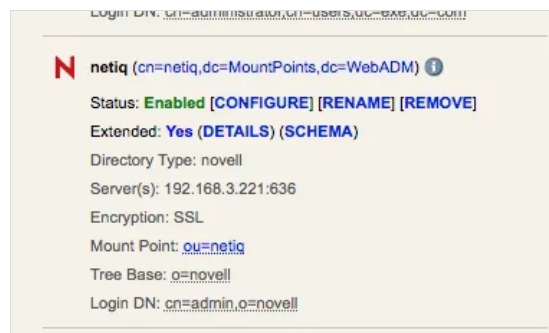
WebADM Enterprise Edition v1.5.11-1

LDAP Schema Setup

Adding attribute 'webadmsettings'... Success
 Adding attribute 'webadmdata'... Success
 Adding attribute 'webadmtype'... Success
 Adding objectclass 'webadmmaccount'... Success
 Adding objectclass 'webadmconfig'... Success
 Adding objectclass 'webadmgroup'... Success

OK

> In the end, you should have the eDirectory mounted on WebADM.



4. Create a Local Domain

- › Select the container used for the eDirectory mount point - in our case `netiq`.

Home Admin Create Search Import Databases Applications About Logout

Object Settings for cn=netiq,dc=Domains,dc=WebADM

☐ 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

☐ Allowed Groups

5. Configure the User for Testing (in WebADM)

- › Create a new user in WebADM within the eDirectory domain (in our case **netiq**).
- › Activate the user in WebADM (this add WebADM attributes to the user in eDirectory).

LDAP Server (OpenLDAP)

OpenLDAP (8)

- cn=test01
- dc=UnixUsers
- dc=WebADM
- dc=myDomainLDAP
- o=Root
- o=myOrganization
- ou=FrancoisAD
- ou=netiq (22)
 - cn=DNS AG netiq.test.com ...
 - cn=Http Server - netiq
 - cn=IP AG 192.168.3.221 - ...
 - cn=LDAP Group - netiq
 - cn=LDAP Server - netiq

WebADM Enterprise Edition v1.5.11-1
Copyright © 2010-2017 RCDevs SA, All Rights Reserved

Home Admin Create Search Import Databases Applications About

LDAP Actions

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

Object Details

Object class(es): Person

User activated: **No** [Activate Now!](#) ⓘ

Object Name

Add Attribute (8)

- › Set up the OTP features for the user.

HomeAdminCreateSearchImportDatabasesApplicationsAboutLogout

Inventoried Items

LDAP Actions

Object Details

Application Actions

Object cn=test01,ou=netiq

Object Name

test01

Rename

Add Attribute (9)

Description / Note

Add

Permissions

[add values] [delete attribute]

RO Subtree on All Attributes Rights for cn=test01,ou=netiq

RW Entry on loginScript for cn=test01,ou=netiq

RO Entry on messageServer for Public

RO Entry on groupMembership for Root

RW Entry on printJobConfiguration for cn=test01,ou=netiq

RO Entry on networkAddress for Root

Full Name

[add values] [delete attribute]

test01 test01

First Name

[add values] [delete attribute]

test01

Preferred Language

[delete attribute]

EN

Last Name

[add values]

test01

Login Name

[add values]

test01

Apply Changes / Delete Selected

HomeAdminCreateSearchImportDatabasesApplicationsAboutLogout

Inventoried Items

LDAP Actions

Object Details

Application Actions

Object cn=test01,ou=netiq

Object Name

test01

Rename

Add Attribute (9)

Description / Note

Add

Permissions

[add values] [delete attribute]

RO Subtree on All Attributes Rights for cn=test01,ou=netiq

RW Entry on loginScript for cn=test01,ou=netiq

RO Entry on messageServer for Public

RO Entry on groupMembership for Root

RW Entry on printJobConfiguration for cn=test01,ou=netiq

RO Entry on networkAddress for Root

Full Name

[add values] [delete attribute]

test01 test01

First Name

[add values] [delete attribute]

test01

Preferred Language

[delete attribute]

EN

Last Name

[add values]

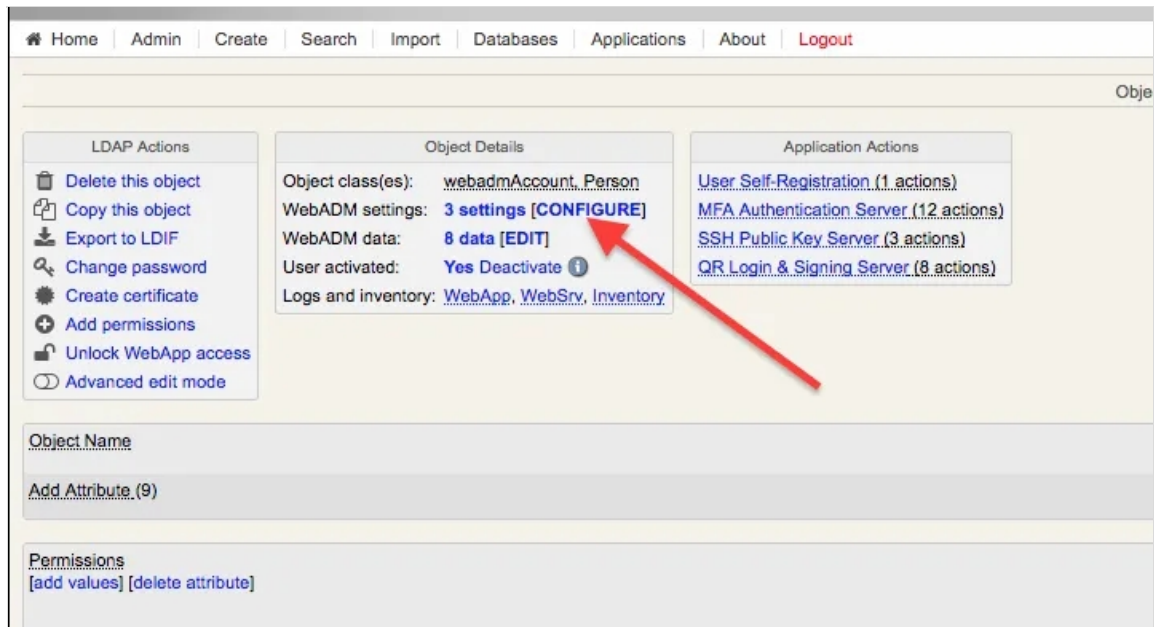
test01

Login Name

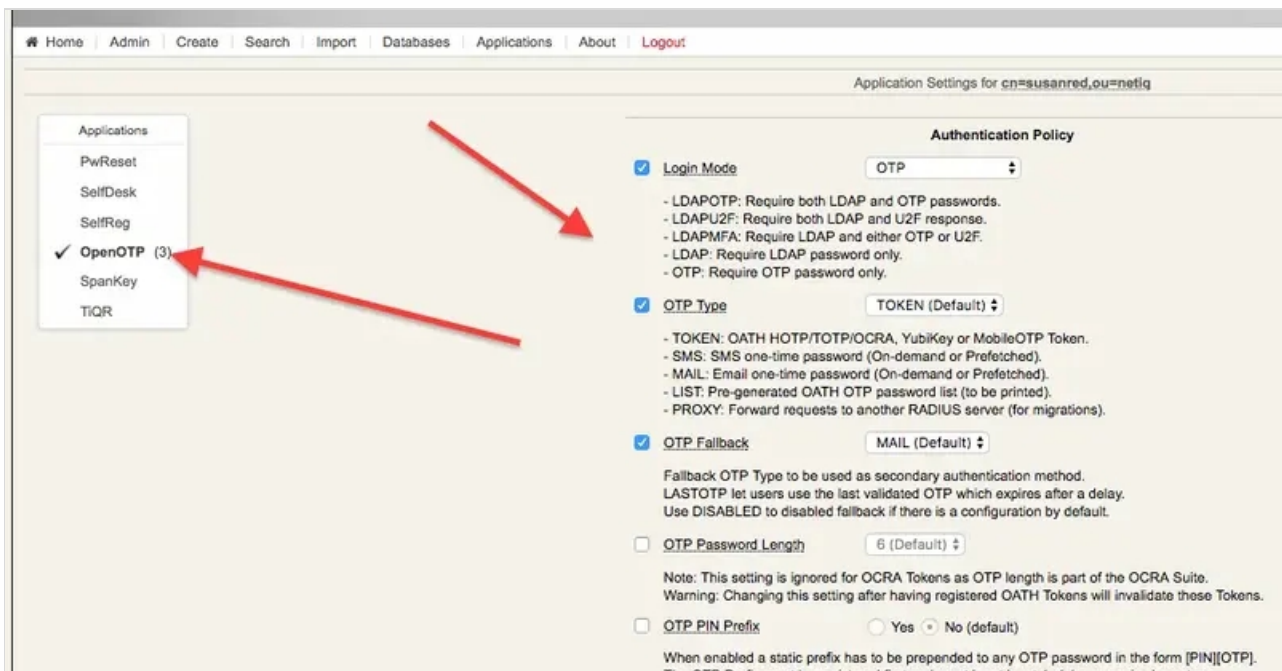
[add values]

test01

Apply Changes / Delete Selected



› This is an example setup that can be customized based on specific needs.



› Register a soft token (we used RCDevs own mobile application).

WebADM Freeware Edition v1.5.11-1
Copyright © 2010-2017 RCD Networks SA. All Rights Reserved

Home Admin Create Search Import Databases Applications About Logout

Register / Unregister OTP Tokens for cn=test02,ou=netiq

You must register a Hardware or Software Token for the user to start using it.
The registration consists in synchronizing a Secret Key and an Initial Token state.

1/3 Token is already registered for user:

Primary Token: **TOTP** Remove Disable

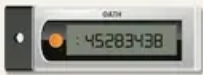
Instructions to register an inventoried Hardware Token:

1. Type the serial number displayed on the back side of the Token.
2. Click the 'Register' button below.

Register Token: Primary Token

WARNING: Primary Token is already registered.
You must remove Token first in order to re-register!

☒ I use a Hardware Token (Inventoried)
☐ I use a Yubikey Token (Inventoried or YubiCloud)
☐ I use a QRCode-based Authenticator (Time-based)
☐ I use a QRCode-based Authenticator (Event-based)
☐ I use another Token (Manual Registration)



Token Serial:

Register Cancel

6. Create the Radius Class in NetIQ

From the Dashboard, go to Devices -> Identity Servers and select the entry (in our case there is only one, IDP-Cluster).

Under the tab Local, perform all the following sub tab configurations:

- > "Classes"
- > "Methods"
- > "Contracts"
- > "Defaults"

NetIQ Access Manager
from Micro Focus

Dashboard Devices Policies Security

Identity Servers

IDP-Cluster

General Local Liberty SAML 1.1 SAML 2.0 WS Federation Brokering WS-Trust OAuth & OpenID Connect

User Stores | Classes | Methods | Contracts | Defaults

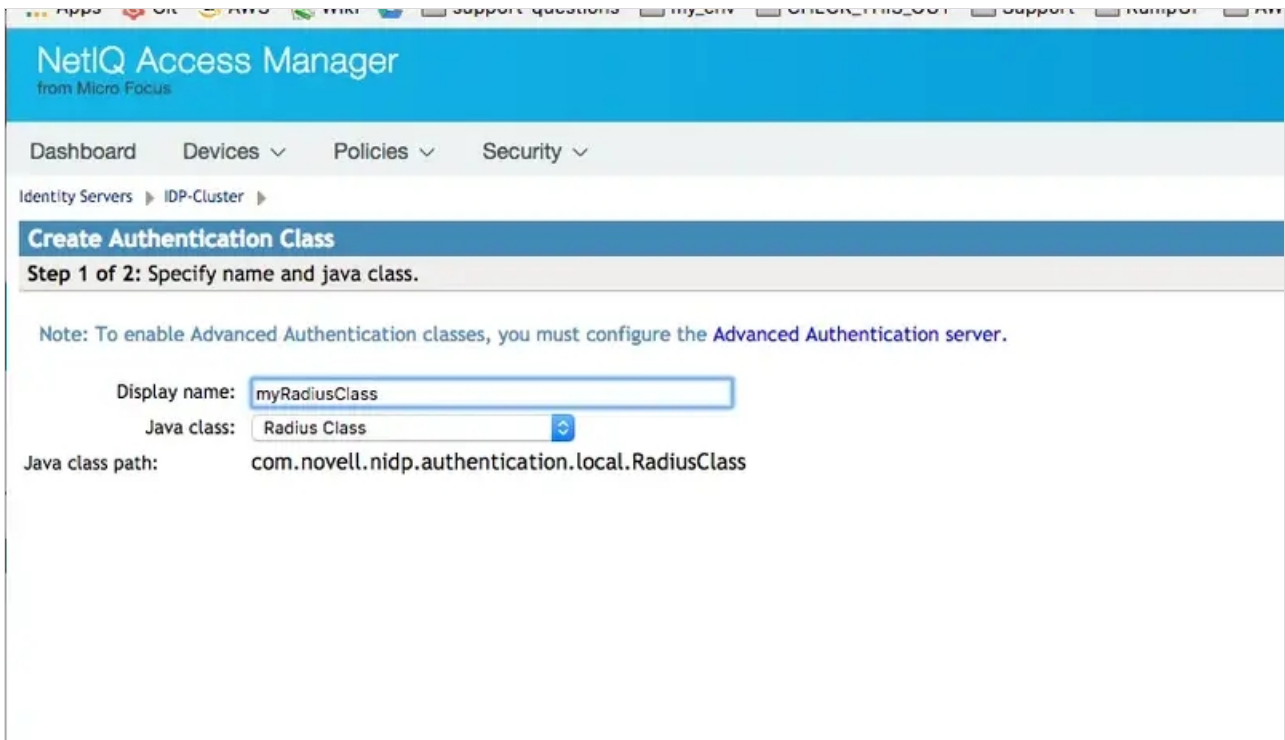
New | Delete 1 Item(s)

Name	Type	Default
SingleBoxUserStore	eDirectory	<input checked="" type="checkbox"/>

Classes

Use the “Radius Class” Java class with the following Java classpath:

“com.novell.nidp.authentication.local.RadiusClass”



The screenshot shows the NetIQ Access Manager web interface. The top navigation bar includes 'Dashboard', 'Devices', 'Policies', and 'Security'. Below this, the breadcrumb trail shows 'Identity Servers' > 'IDP-Cluster'. The main heading is 'Create Authentication Class', followed by 'Step 1 of 2: Specify name and java class.' A note states: 'Note: To enable Advanced Authentication classes, you must configure the Advanced Authentication server.' The configuration fields are: 'Display name' with the value 'myRadiusClass', 'Java class' with a dropdown menu showing 'Radius Class', and 'Java class path' with the value 'com.novell.nidp.authentication.local.RadiusClass'.

In the second page, add details of the server running the Radius Bridge daemon (normally the same server running WebADM). Here we used the default values that you can find in `/opt/radiusd/conf/client.conf` (port and `Shared secret`).

NetIQ Access Manager
from Micro Focus

Dashboard Devices Policies Security

Identity Servers IDP-Cluster

radius

General Properties

Servers

New | Delete | 1 Item(s)

- ☐ Server
- ☐ 192.168.3.108

Port: 3001

Shared secret:

Reply time: 7000 milliseconds

Resend time: 2000 milliseconds

Failed server retry: 5 minutes

JSP:

User Lookup Attribute Name: cn

☒ Require password

Make sure the port (in this case 3001, the default), it's open between the NetIQ AM server and the WebADM/Radius server.

Methods

Create a new entry using the Radius class from the list in `Class`.

NetIQ Access Manager

from Micro Focus

Dashboard

Devices

Policies

Security

Identity Servers > IDP-Cluster >

myRadiusMethod

Display name:

myRadiusMethod

Class:

myRadiusClass

☒ Identifies User

☐ Overwrite Temporary User

☐ Overwrite Real User

User stores:

SingleBoxUserStore

Available user stores:

<Default User Store>

↑

↓

Properties

New

Delete

0 Item(s)

☐ Name

Value

No items

“Contracts”

Create a new entry adding the method for Radius in the bottom box from the list on the right.

Create Authentication Contract

Step 1 of 2: Configuration

Display name:

URI:

Password expiration servlet:

☐ Allow user interaction

Login Redirect URL:

☒ Allow user interaction

Authentication Level:

Authentication Timeout: Minutes

Activity Realm(s):

☐ Satisfiable by a contract of equal or higher level

☒ Satisfiable by External Provider

Requested By:

Allowable Class:

If you add more than one X509 method, only the first one will be used and it will automatically be moved to the top of the list.

Methods:

Available methods:

- Name/Password - Basic
- Name/Password - Form
- Secure Name/Password - Basic
- Secure Name/Password - Form

Create Trusted Identity Provider

Step 2 of 2: Enter authentication card values

ID:

Text:

Image:

☒ Show Card

☐ Passive Authentication Only



Defaults

Create new entry selecting the Radius contract.

The screenshot shows the NetIQ Access Manager web interface. The browser address bar indicates the URL is `https://netiqam.test.com:8443/nps/servlet/webacc`. The page title is "NetIQ Access Manager from Micro Focus". The navigation bar includes "Dashboard", "Devices", "Policies", and "Security". The "Identity Servers" section is expanded, showing "IDP-Cluster". The "Local" tab is selected, and the "Defaults" sub-tab is active. The "User Store" is set to "SingleBoxUserStore" and the "Authentication Contract" is set to "radius". Below this, a table lists authentication types and their default contracts:

Authentication Type	Default Contract
Name Password:	<None>
Secure Name Password:	<None>
X509:	<None>
Smart Card:	<None>
Smart Card PKI:	<None>
Token:	<None>

7. Update the NetIQ Configuration and Make Sure The Server Is Operational

Once you have created all the above entries, you need to update the server configuration in Server Health -> Health tab.

The update can take several minutes depending on your VM configuration and in our limited experience sometimes it might be necessary to restart the entire system.

Login as root to the VM and execute:

```
netiq:/etc/init.d # ./novell-appliance restart
```

Repeat the "Update from server" and "Refresh" until it gets green or investigates what went wrong.

← → ↻ ⚠ Not Secure <https://netiqam.test.com:8443/nps/servlet/webacc>

Apps Git AWS Wiki support-questions my_env CHECK_THIS_OUT Support RumpUP AWS4RCDEVS demo_sw toc

NetIQ Access Manager

from Micro Focus

Dashboard Devices Policies Security

Servers ▸ **Health**

Server Health: 192.168.3.221

General **Health** Alerts Command Status Statistics

Refresh | Update from Server

Status	Description
🟢	Server is operational (Passed)

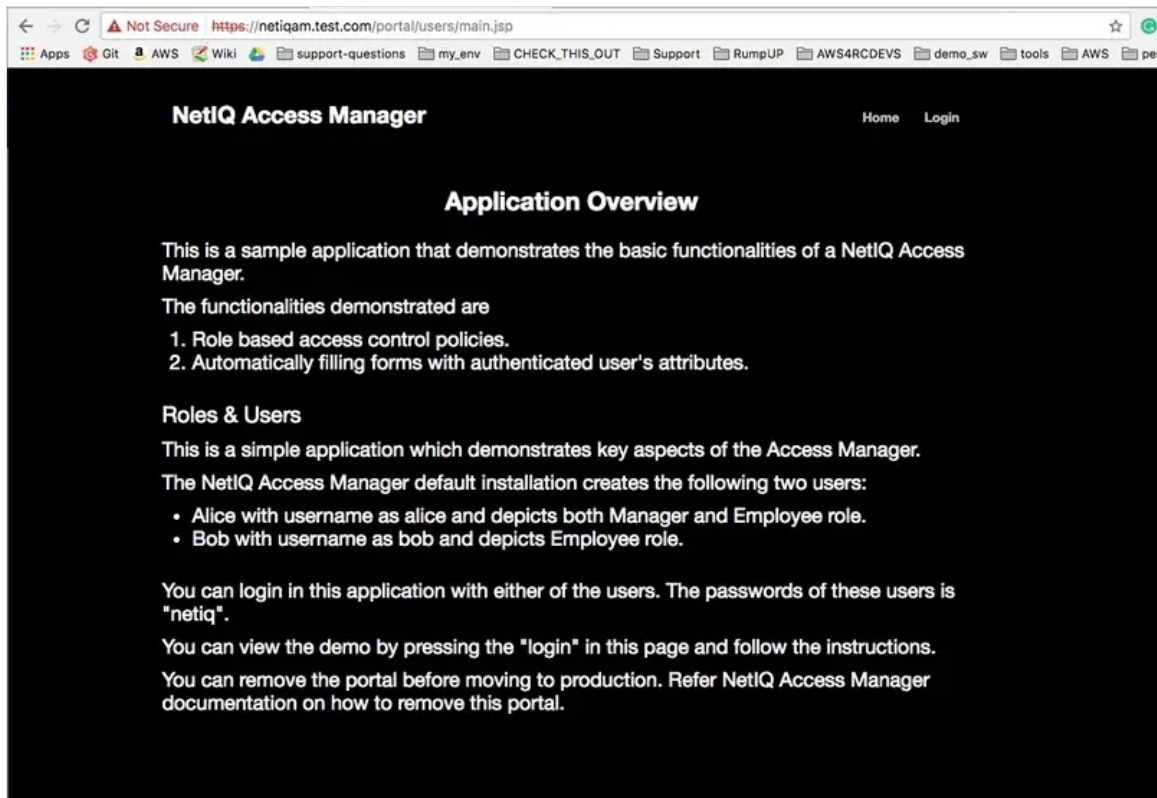
Services Detail

Type	Status	Message
Services	🟢	Identity Server Configuration ▼
Identity Server Configuration	🟢	Fully applied
Configuration Datastore	🟢	Operating properly
User Datastores	🟢	Operating properly
Signing, Encryption and SSL Connector Keys	🟢	Signing key available ,Certificate Subject Name = CN=netiqam.test.com ,Validity in Days = 3649 ▼
Evaluation Version	🟢	This evaluation version will expire on Thu, Aug 31, 2017.

Close

8. Test User Login

- › To test the user login I used the default NetIQ portal app. In our case, that's <https://netiq.test.com/portal/> (netiq.test.com resolves to the local IP address of the NetIQ VM).
- › Please keep in mind that the password is authenticated by NetIQ/eDirectory, while the token is authenticated by OpenOTP via Radius.



The screenshot shows the "Access Manager" login interface. It has a blue header with the "Access Manager" logo and a navigation menu. Below the header, there is a section titled "Sign in to use available applications".

Under this section, there is a card for "RCDevs" with the application name "OpenOTPLLogin".

The login form contains three input fields:

- A username field containing "susanred".
- A password field with masked characters ".....".
- A second password field with masked characters "....." and a toggle icon (an eye with a slash) to show/hide the password.

Below the input fields is a "Sign in" button.



9. WebADM Log Entries

This is the log entry of a failed login where I provided the wrong OTP.

```
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] New openotpSimpleLogin SOAP request
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Username: test02
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Password: xxxxxxxx
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Client ID: 192.168.3.221
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] > Options: RADIUS,-U2F
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Enforcing client policy: netiq
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Registered openotpSimpleLogin request
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Resolved LDAP user: cn=test02,ou=netiq
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Started transaction lock for user
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found user language: EN
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 37 user settings:
LoginMode=OTP,OTPTType=TOKEN,OTPFallback=DISABLED,OTPLength=6,ChallengeMode=Yes,ChallengeTim
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTTime=300,ListChallengeMode=

[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 5 user data:
LoginCount,LastOTP,TokenType,TokenKey,TokenState
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Last OTP expired 2017-06-13 14:48:21
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Found 1 registered OTP token (TOTP)
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Requested login factors: OTP
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Wrong TOTP password (token #1)
[2017-06-13 14:48:35] [192.168.3.108] [OpenOTP:UJM5WOBB] Updated user data
[2017-06-13 14:48:36] [192.168.3.108] [OpenOTP:UJM5WOBB] Sent failure response
```

This is the log of a successful login:

```

[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] New openotpSimpleLogin SOAP request
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Username: test02
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Password: xxxxxx
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Client ID: 192.168.3.221
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] > Options: RADIUS,-U2F
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Enforcing client policy: netiq
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Registered openotpSimpleLogin request
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Resolved LDAP user: cn=test02,ou=netiq
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Started transaction lock for user
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found user language: EN
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 37 user settings:
LoginMode=OTP,OTPTType=TOKEN,OTPFallback=DISABLED,OTPLength=6,ChallengeMode=Yes,ChallengeTim
1:HOTP-SHA1-6:QN06-
T1M,SMSType=Normal,SMSMode=Ondemand,MailMode=Ondemand,LastOTPTTime=300,ListChallengeMode=

[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 7 user data:
LoginCount,RejectCount,LastOTP,TokenType,TokenKey,TokenState,TokenOffset
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Last OTP expired 2017-06-13 11:59:12
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Found 1 registered OTP token (TOTP)
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Requested login factors: OTP
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] TOTP password Ok (token #1)
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Updated user data
[2017-06-13 13:12:12] [192.168.3.108] [OpenOTP:9VDX08GZ] Sent success response

```

- › Example of a failed login - notice the token value (from the Radius bridge log). Please note that “User-Password” is actually the content of the token field, as the actual password is authenticated directly by NetIQ and unknown to OpenOTP.


```
rad_recv: Access-Request packet from host 192.168.3.221 port 34761, id=6, length=48
User-Name = "susanred"
User-Password = "wrong"
# Executing section authorize from file /opt/radiusd/conf/radiusd.conf
+group authorize {
[pap] WARNING! No "known good" password found for the user. Authentication may fail because of this.
++[pap] = noop
++[openotp] = ok
+} # group authorize = ok
Found Auth-Type = openotp
# Executing group from file /opt/radiusd/conf/radiusd.conf
+group authenticate {
rlm_openotp: Sending openotpSimpleLogin request
rlm_openotp: OpenOTP Authentication failed
rlm_openotp: Reply message: Invalid username or password
rlm_openotp: Sending Access-Reject
++[openotp] = reject
+} # group authenticate = reject
Failed to authenticate the user.
Login incorrect: [susanred] (from client any port 0)
Using Post-Auth-Type Reject
WARNING: Unknown value specified for Post-Auth-Type. Cannot perform requested action.
Sending Access-Reject of id 6 to 192.168.3.221 port 34761
Reply-Message = "Invalid username or password"
Finished request 2.
Going to the next request
Waking up in 9.9 seconds.
Cleaning up request 2 ID 6 with timestamp +686
```

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