Token2 TOTP Radius

V 0.1

Virtual appliance | a RADIUS server designed for two-factor authentication

Import OVF to VMWare or VirtualBox

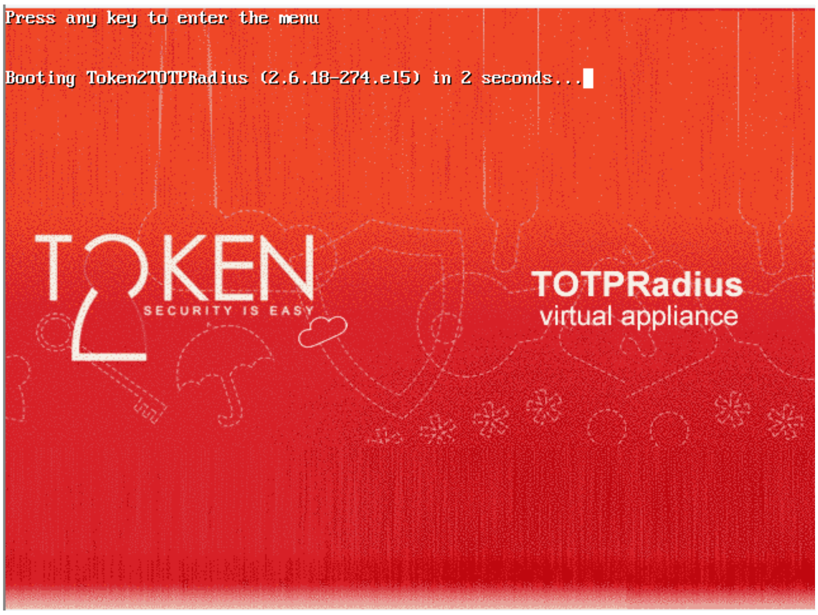
TOTPRadius is deployed in standard OVF format. Follow usual OVF import procedures to install the appliance.

Import VM to Hyper-V

TOTPRadius has been tested on a standard Windows 2012 R2 based Hyper-V host and has been exported using Hyper-V manager. To import, unzip the downloaded archive to a location visible from Hyper-V manager and import the appliance.

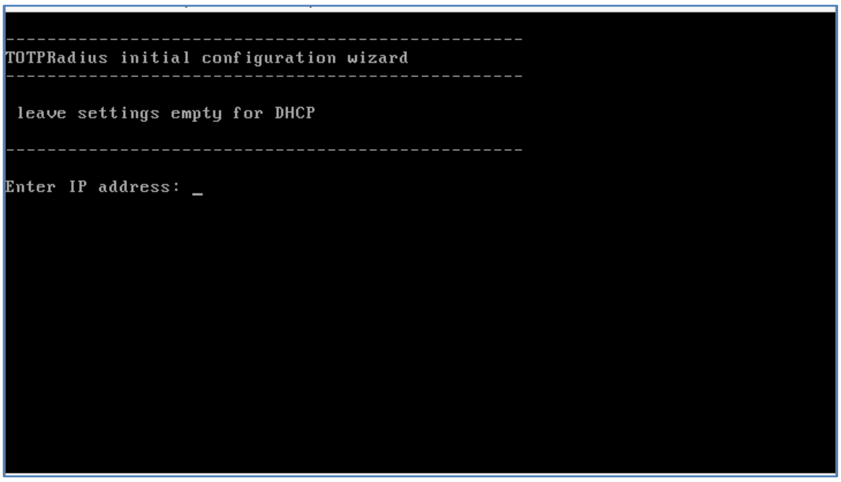
Initial configuration of the appliance

Power on the virtual machine and open its console.



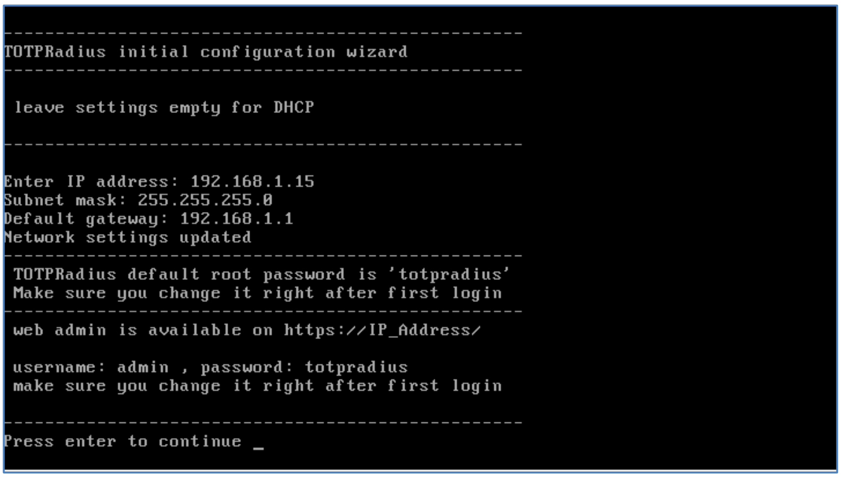
```
Press any key to enter the menu

Booting Token2TOTPRadius (2.6.18-274.el5) in 2 seconds...
```

Wait for the following window to appear.



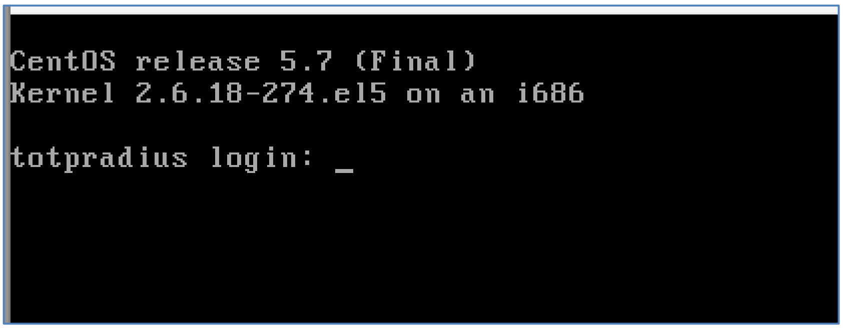
```
-------------------------------------------------
TOTPRadius initial configuration wizard
-------------------------------------------------

 leave settings empty for DHCP

-------------------------------------------------

Enter IP address: _
```

Enter IP address, Subnet mask and default gateway. After that, the machine will continue to boot up.

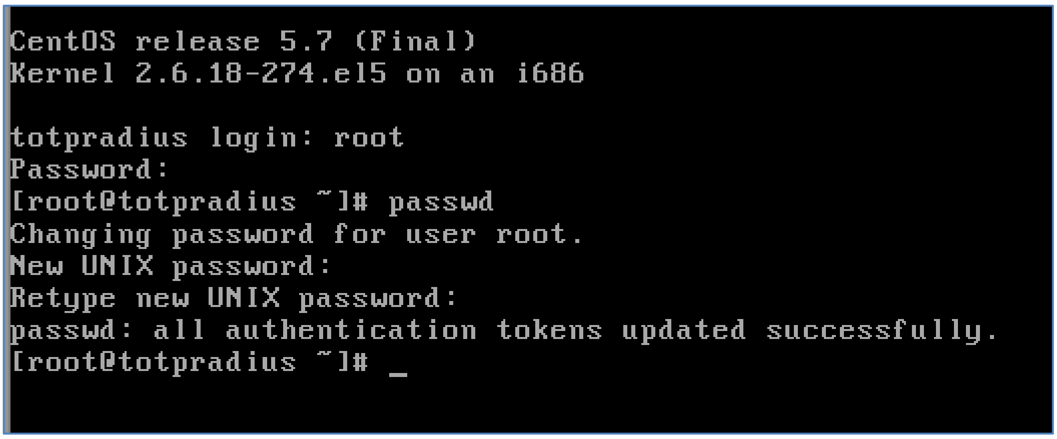


```
-------------------------------------------------
TOTPRadius initial configuration wizard
-------------------------------------------------

 leave settings empty for DHCP

-------------------------------------------------

Enter IP address: 192.168.1.15
Subnet mask: 255.255.255.0
Default gateway: 192.168.1.1
Network settings updated
-------------------------------------------------
 TOTPRadius default root password is 'totpradius'
 Make sure you change it right after first login
-------------------------------------------------
 web admin is available on https://IP_Address/

 username: admin , password: totpradius
 make sure you change it right after first login

-------------------------------------------------
Press enter to continue _
```

After you see the login prompt, TOTPRadius is ready to be used.



```
CentOS release 5.7 (Final)
Kernel 2.6.18-274.el5 on an i686

totpradius login: _
```

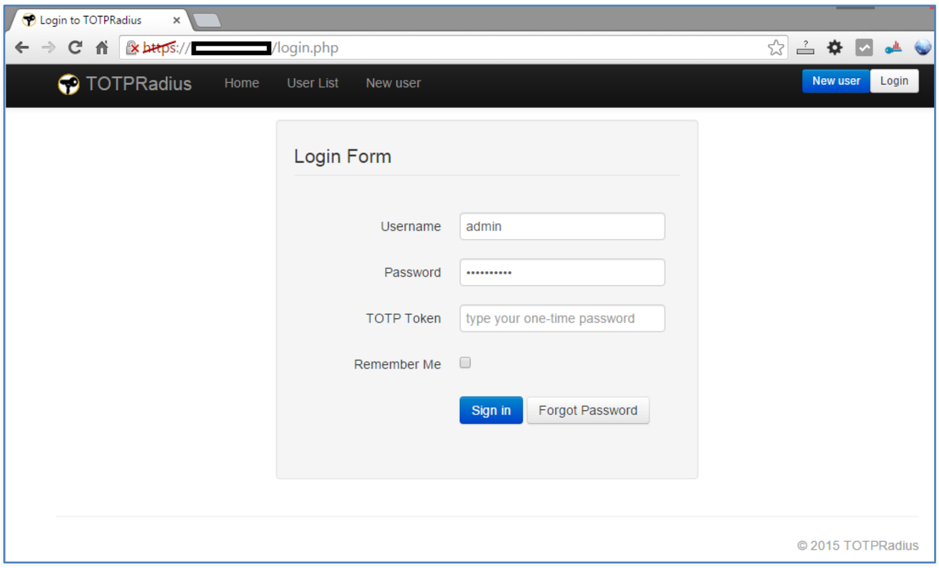


```
CentOS release 5.7 (Final)
Kernel 2.6.18-274.el5 on an i686

totpradius login: root
Password:
[root@totpradius ~]# passwd
Changing password for user root.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
[root@totpradius ~]# _
```

Accessing and configuring web interface

User management, API key and Radius configuration is done via TOTPRadius web interface. Navigate to http(s)://IP_Address/login.php and login with default password (admin/totpradius). Leave TOTP Token field empty.

It is **highly recommended to change the default admin password** of the appliance.



Login Form

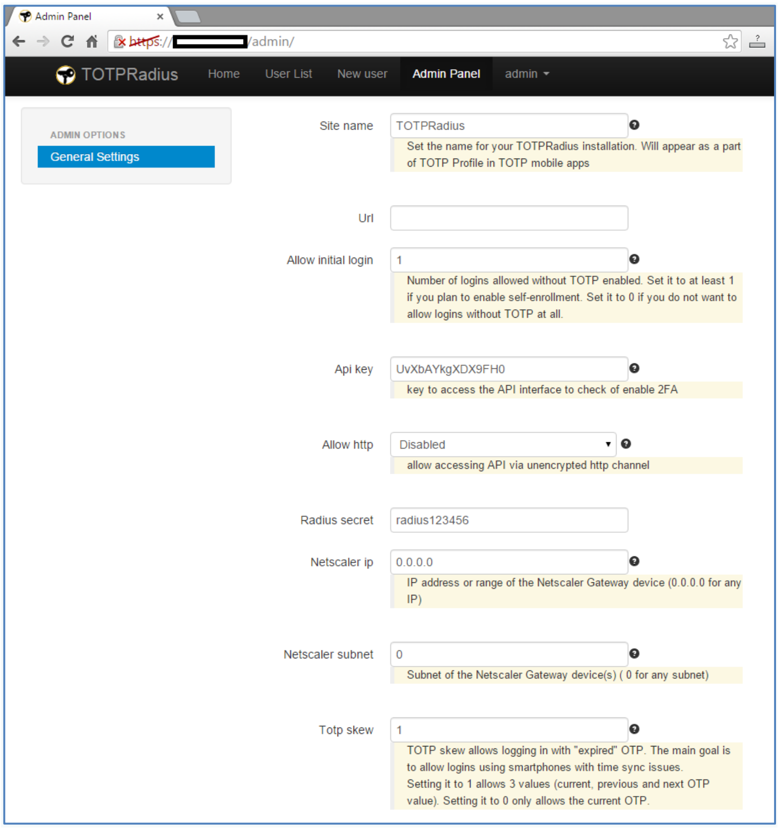
Username: admin

Password: ••••••••••

TOTP Token: type your one-time password

Remember Me □

Once logged in, click on "Admin Panel" link to modify API and Radius settings.



Site name: TOTPRadius
Set the name for your TOTPRadius installation. Will appear as a part of TOTP Profile in TOTP mobile apps

Url:

Allow initial login: 1
Number of logins allowed without TOTP enabled. Set it to at least 1 if you plan to enable self-enrollment. Set it to 0 if you do not want to allow logins without TOTP at all.

Api key: UvXbAYkgXDX9FH0
key to access the API interface to check of enable 2FA

Allow http: Disabled
allow accessing API via unencrypted http channel

Radius secret: radius123456

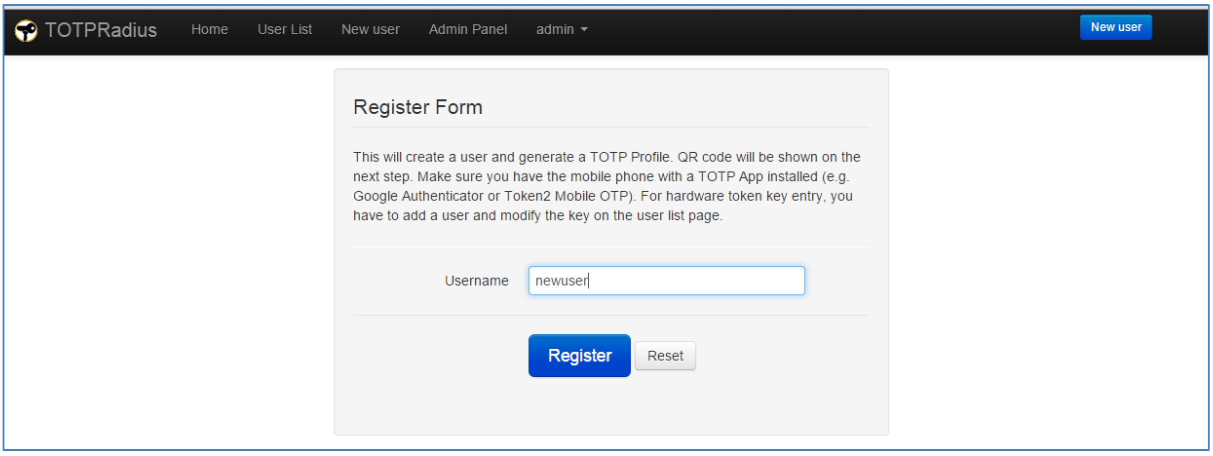
Netscaler ip: 0.0.0.0
IP address or range of the Netscaler Gateway device (0.0.0.0 for any IP)

Netscaler subnet: 0
Subnet of the Netscaler Gateway device(s) (0 for any subnet)

Totp skew: 1
TOTP skew allows logging in with "expired" OTP. The main goal is to allow logins using smartphones with time sync issues. Setting it to 1 allows 3 values (current, previous and next OTP value). Setting it to 0 only allows the current OTP.

Creating a TOTP profiles

In order to manually create a TOTP profile for a user, click on “New User” button. You only need to specify username and click “Register”. Username should be exactly the same as in Active Directory (case sensitive).

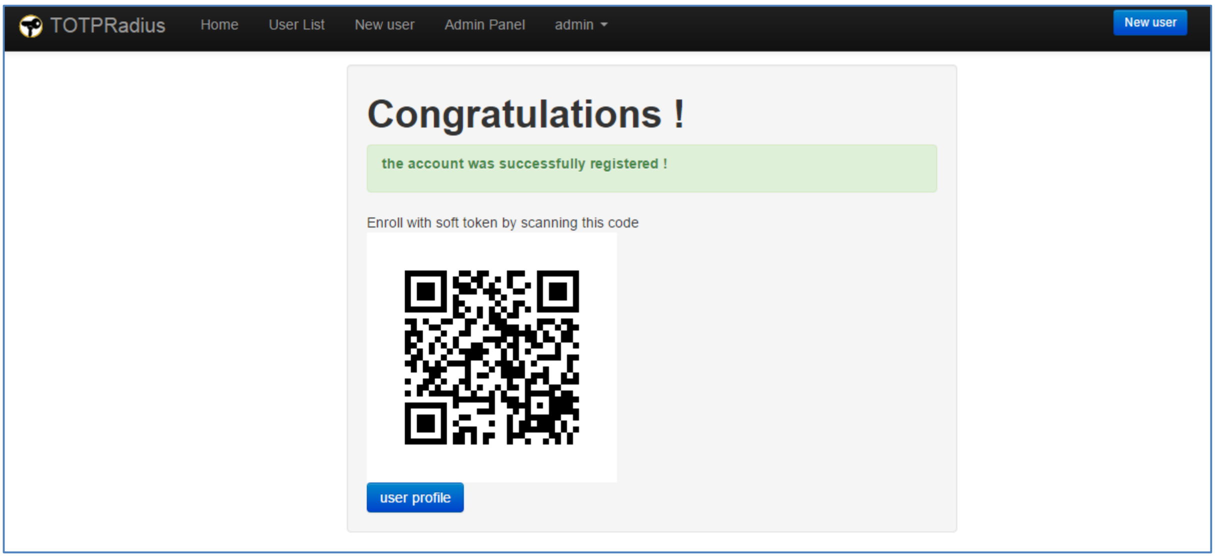


Register Form

This will create a user and generate a TOTP Profile. QR code will be shown on the next step. Make sure you have the mobile phone with a TOTP App installed (e.g. Google Authenticator or Token2 Mobile OTP). For hardware token key entry, you have to add a user and modify the key on the user list page.

Username: newuser

Upon creating a user, a QR code will be shown for the newly created user. Scan this QR code with user’s mobile TOTP application.

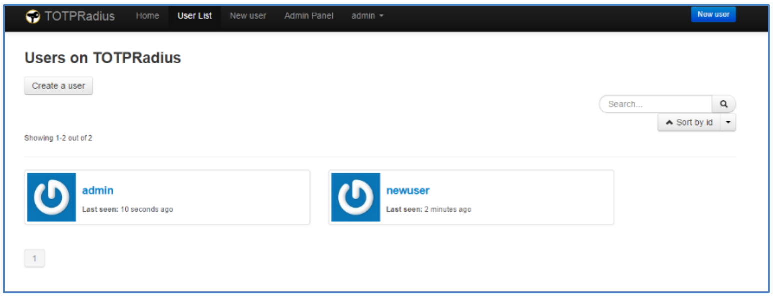


Congratulations !

the account was successfully registered !

Enroll with soft token by scanning this code

You can modify the users (delete, temporarily ban, recreate QR codes etc.) by clicking on the ”User List” link.

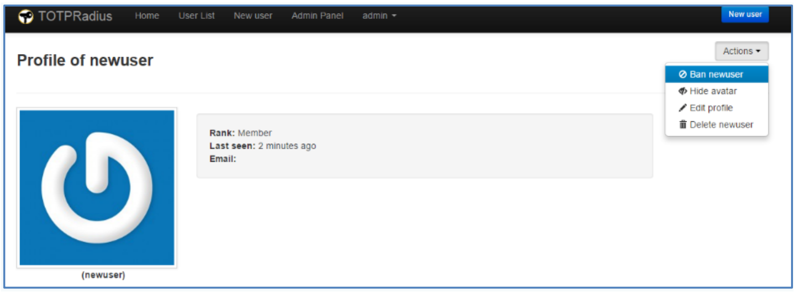


Users on TOTPRadius

Showing 1-2 out of 2

admin
Last seen: 10 seconds ago

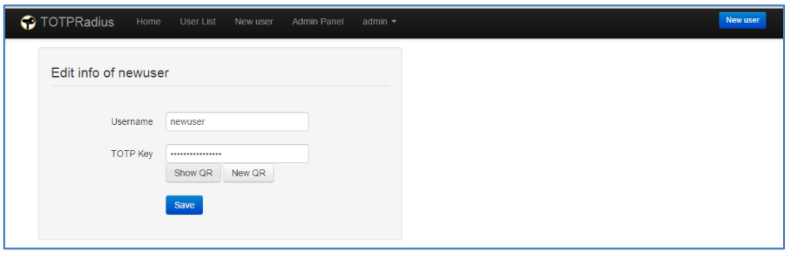
newuser
Last seen: 2 minutes ago



Profile of newuser

Rank: Member
Last seen: 2 minutes ago
Email:

(newuser)



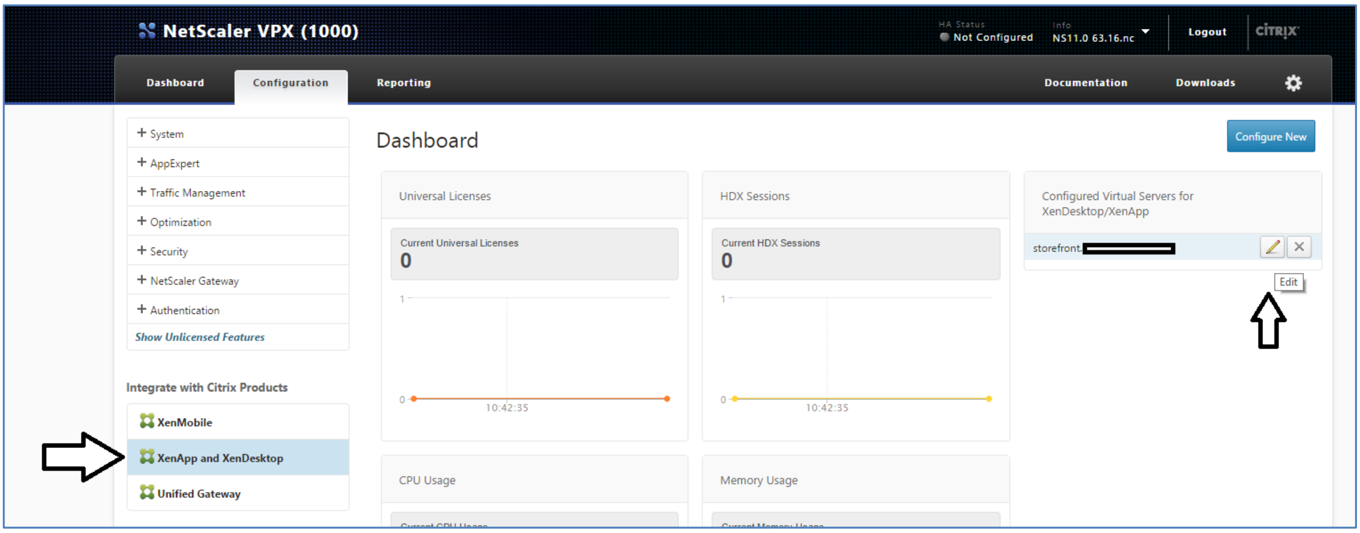
Edit info of newuser

Username: newuser
TOTP Key: ••••••••••••••••

Configuring Citrix Netscaler Gateway to use TOTPRadius

In order to enable two-factor authentication on Netscaler gateway, we have to specify TOTPRadius as secondary authentication for XenApp/XenDesktop site.

Login to Netscaler admin panel with nsroot and click on Configuration->XenApp and Xendesktop sites->Configured Virtual Servers… . Click on Edit button next to the site you want to configure two-factor authentication for.



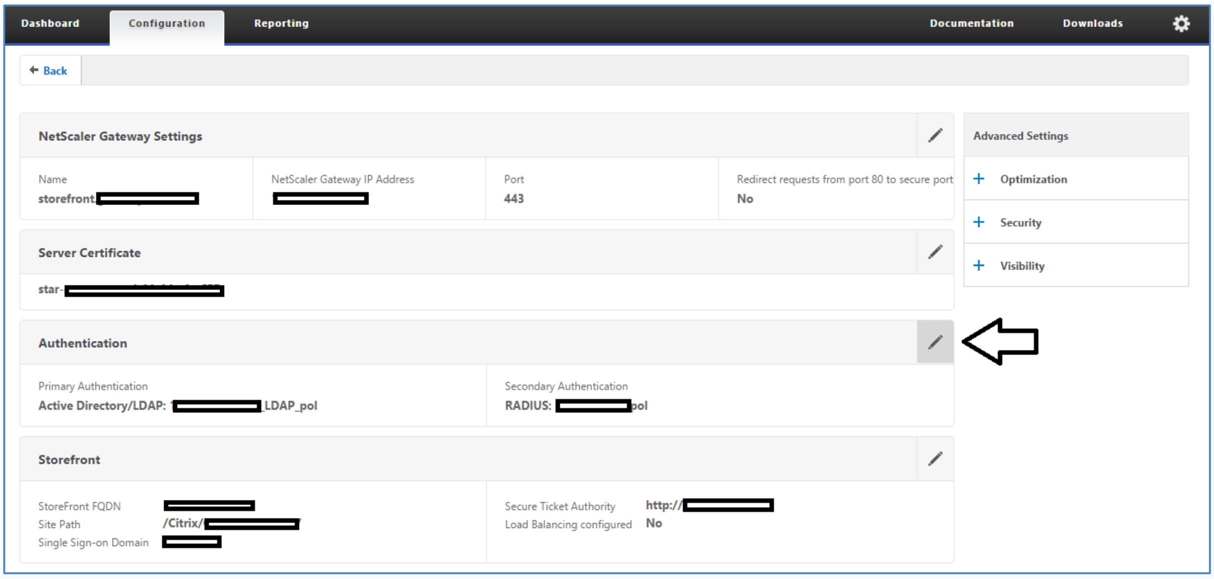
Current Universal Licenses
0

Current HDX Sessions
0

Configured Virtual Servers for XenDesktop/XenApp

storefront[redacted]

Click on edit icon on the Authentication box.



NetScaler Gateway Settings

Name	NetScaler Gateway IP Address	Port	Redirect requests from port 80 to secure port
storefront[redacted]	[redacted]	443	No

Server Certificate

star-[redacted]

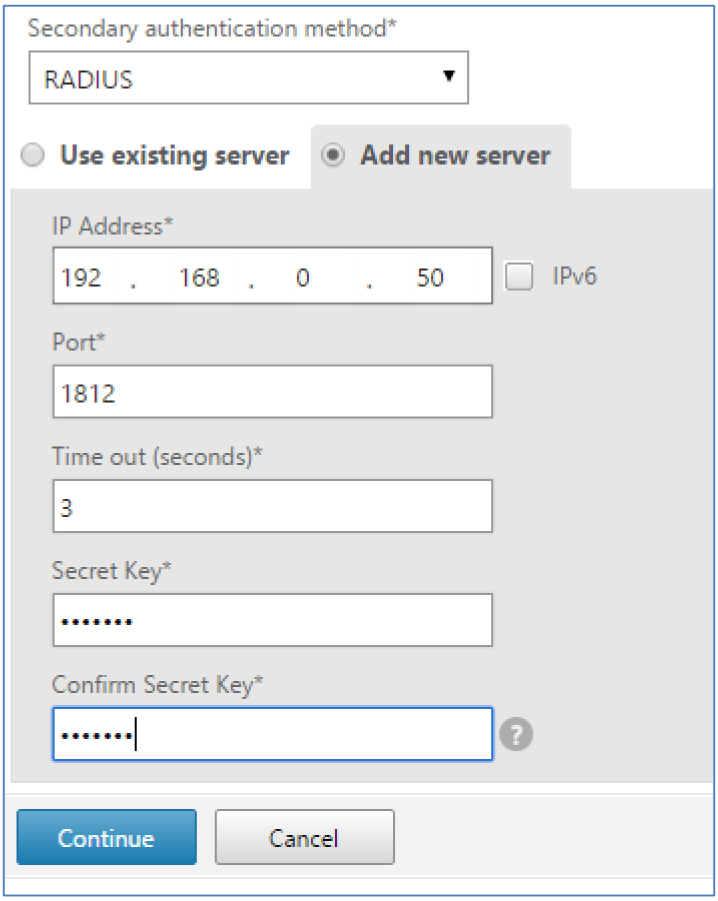
Authentication

Primary Authentication	Secondary Authentication
Active Directory/LDAP: [redacted]LDAP_pol	RADIUS: [redacted]pol

Storefront

StoreFront FQDN	[redacted]	Secure Ticket Authority	http://[redacted]
Site Path	/Citrix/[redacted]	Load Balancing configured	No
Single Sign-on Domain	[redacted]		

Set “Secondary Authentication Method” to RADIUS and enter the TOTPRadius appliance settings in the form below. Leave port as 1812. Radius secret is as specified in Admin Panel of TOTPRadius web interface.



Secondary authentication method*

RADIUS ▾

○ Use existing server ● Add new server

IP Address*

192 . 168 . 0 . 50 □ IPv6

Port*

1812

Time out (seconds)*

3

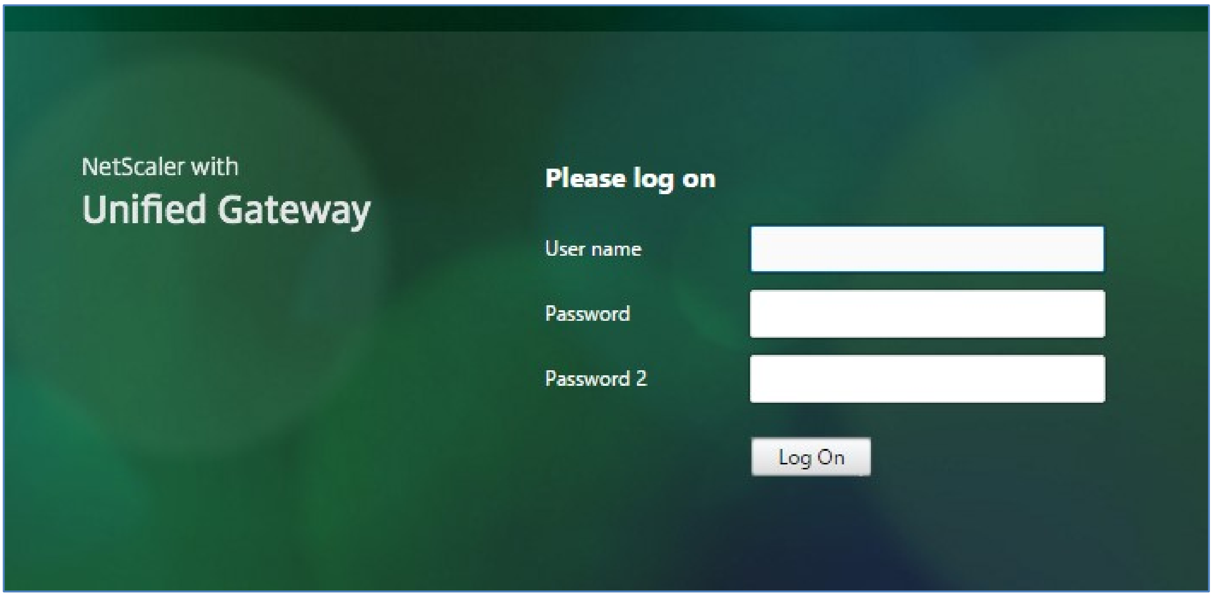
Secret Key*

•••••••

Confirm Secret Key*

•••••••

Click on "Continue", then "Done". Once done, Netscaler interface will ask for two passwords (Password 2 is the field for OTP).



NetScaler with
Unified Gateway
Please log on
User name
Password
Password 2
Log On