Native OTP (One Time Password) Authentication with NetScaler

This guide focuses on defining the process for deploying native OTP (One time Password) with NetScaler.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>4</td>
</tr>
<tr>
<td>Current Limitations</td>
<td>5</td>
</tr>
<tr>
<td>Deployment Environment</td>
<td>4</td>
</tr>
<tr>
<td>Active Directory Configuration</td>
<td>5</td>
</tr>
<tr>
<td>Using existing attributes</td>
<td>5</td>
</tr>
<tr>
<td>Device Registration and Management Page UI Flow</td>
<td>6</td>
</tr>
<tr>
<td>NetScaler Configuration</td>
<td>8</td>
</tr>
<tr>
<td>Troubleshooting</td>
<td>13</td>
</tr>
</tbody>
</table>
Citrix NetScaler is a world-class product with the proven ability to load balance, accelerate, optimize, and secure enterprise applications.

Native OTP Support in NetScaler now enables users to support OTP authentication based use cases without requiring a third party solution. This guide describes the generic configuration required with a sample, along with policy definitions.

**Introduction**

The NetScaler One Time Password (OTP) feature is introduced with NetScaler 12.0 FR1. This feature offers OTP authentication capabilities without having to use a third party server, thus greatly reducing capex and opex for customers. In addition, it consolidates configuration within the NetScaler, thus offering great control to administrators.

For end users to take advantage of NetScaler OTP, they must first be registered on the NetScaler Gateway vsrerver. Registration is required only once per unique device. Once registration is complete, validation of OTP is as simple as configuring an additional authentication policy.

Since NetScaler OTP eliminates the need for third party servers, the gateway has the additional capability for offering an interface to manage user devices along with being able to validate those devices.

This document describes guidelines for deploying the management interface and also provides an example configuration. In addition, this document also describes the policy required for validating OTPs from end users.
Prerequisites
NetScaler
• Version 12.0 Feature Release 1 or above
• Available in nFactor authentication flow only
• Advanced policies is required to configure it.
• For more details, refer to https://support.citrix.com/article/CTX222713

Active Directory
• Supported versions are 2012 and 2008 Active Directory domain function level
• Netscaler ldapBind username needs to have write access to the user’s AD path
• Current supported logon and registration rate is at 300 devices per minute for single AD server.

TOTP Client
• Netscaler supports RFC6238 TOTP generation i.e., any TOTP client which complies with RFC 6238 TOTP generation will be supported (https://tools.ietf.org/html/rfc6238)
• TOTP supported length is 6
• Tested client: Google Authenticator

Time Sync
• Both Netscaler and user’s device have to be in-sync
• It is recommended that both entities are synced to a common Network Time Server.

Current Limitations
There are limitations to this feature:
• Number of register device is depending on the AD attribute selected by the AD admin (Please see Active Directory Configuration).
• Web based only: all the major browsers on major platforms (desktop or mobile) should be supported.
• Native clients do not support nFactor configuration fully. Please refer to: https://support.citrix.com/article/CTX223386

Deployment Environment
The following diagram shows a typical deployment for Netscaler OTP:
We are assuming that this is an existing two-factor deployment, and the system would have a third party OTP provider. The following sections will explain the detail on how to retire the mentioned OTP provider by replacing it with Active Directory server.

**Active Directory Configuration**

Netscaler OTP leverages Active Directory attribute as users’ secret key storage. There are a few requirements to the attribute to be selected:

- Attribute length must be at least 128 characters
- Attribute type must be 'DirectoryString'
- Attribute string type should be Unicode, if device name will be in non-english characters.
- Netscaler ldap admin should have write access to the selected AD attribute.

**Using existing attributes**

The attribute we will use in this example will be ‘UserParameters’. As this is existing attribute within the AD user, we do not need to make any changes to AD itself. However, we have to make sure that the attribute is not being used.

To check it, go to ‘ADSI > select user > right click on it > scroll down to attribute list”. You shall see ‘not set’ within the attribute like this:

![CN=aaa1 Properties](image)

This indicates that the attribute is not being used at the moment.
Device Registration and Management Page UI Flow
This section describes the user interface flow for the Native OTP capability. Before beginning with this flow, please complete the NetScaler configuration presented in the next section.

Accessing via url e.g., https://otpauth.server.com/manageotp (alternatively, you can use https://alt.server.com if you have configured host-based management page), we will be presented with initial logon page that only requires ldap logon credential:

After login with valid credential, we will see the manage device page as follow:

After click ‘+‘, type in the device name, click ‘go‘, and click ‘done‘, we will see a QR code generated. This indicates the device has been registered:
A passcode can be entered to test the newly registered device.
**Netscaler Configuration**

The Netscaler OTP solution requires configuration of two parts: device registration and OTP validation.

**Device Registration and Management Page**

This section concerns with the OTP device management page. We will require the following before we start the configuration:

- IP assigned to authentication vserver
- FQDN corresponding to the assigned IP
- Server certificate for authentication vserver

To setup device registration and management page, all we required is authentication vserver. The logical flow looks as follow:

![Device Registration and Management Diagram](image)

**Create Authentication VServer**

We will create an instance of authentication vserver

```plaintext
add authentication vserver authvs SSL 1.2.3.5 443
bind authentication vserver authvs -portaltheme RFWebUI
bind ssl vserver authvs -certkeyname otpauthcert
```
In this example, we create an instance of authentication vserver named "authvs”. It is recommended that "RFWebUI" portal theme to be used by the authentication Vserver. We will have to bind server certificate to it as well. Please note that the server ip '1.2.3.5' will have to have a corresponding FQDN i.e., otpauth.server.com, which we will need for later.

**Create LDAP Logon Action**

As shown in the flow above, the users are required to enter their valid AD credential. The following command will create that:

**Syntax:**

```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT>
```

**Example:**

```
add authentication ldapAction ldap_logon_action -serverIP 1.2.3.4 -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName userprincipalname
```

**Authentication Policy for LDAP Logon**

In this example, we will be setting it to ‘true’ for simplicity:

```
add authentication Policy auth_pol_ldap_logon -rule true -action ldap_logon_action
```

**Presenting UI via LoginSchema**

We need to show the username and password fields to users when they logon. The following commands will do so:

```
add authentication loginSchema lschema_single_auth_manage_otp -authenticationSchema "/nsconfig/loginschema/LoginSchema/SingleAuthManageOTP.xml"
```

We recommend two ways of showing the device registration and management page: 'by url' or 'by hostname'

**By URL**

When the url contains '/manageotp' e.g., https://otpauth.server.com/manageotp, we will provide an ldap logon
```
add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_url -rule "http.req.cookie.value("NSC_TASS").eq("manageotp")" -action lschema_single_auth_manage_otp
bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_url -priority 10 -gotoPriorityExpression END
```

**By Host**

When the hostname is 'alt.server.com'
```
add authentication loginSchemaPolicy lpol_single_auth_manage_otp_by_host -rule "http.req.header("host").eq("alt.server.com")" -action lschema_single_auth_manage_otp
bind authentication vserver authvs -policy lpol_single_auth_manage_otp_by_host -priority 20 -gotoPriorityExpression END
```
**User Logon Page**

In this example, we will assume that the first factor is LDAP logon and followed by OTP passcode validation. Before we start configuring the user logon page, please have the following items available:

- IP for loadbalancing virtual server
- Corresponding FQDN for the load balancing vserver
- Server certificate for the load balancer

The logical flow looks as follows:

Please note that we will be re-using the existing authentication vserver (authvs) for multi-factor authentication as well.
Create Load Balancer VServer
To access the internal website, we will have to create a LB Vserver to front the backend service and delegate the authentication logic to the authentication vserver (authvs)

```
add lb vserver lbvs _https SSL 1.2.3.162 443 -persistenceType NONE -cltTime-out 180 -AuthenticationHost otpauth.server.com -Authentication ON -authnVsName authvs
bind ssl vserver lbvs _https -certkeyname lbvs _server _cert
```

This is how we represent the back end service in LB:
```
add service iis _backendsso _server _com 1.2.3.210 HTTP 80
bind lb vserver lbvs _https iis _backendsso _server _com
```

Create OTP Passcode Validation Action
The following command will create an OTP passcode validation action:
Syntax:
```
add authentication ldapAction <LDAP ACTION NAME> -serverIP <SERVER IP> -serverPort <SERVER PORT> -ldapBase <BASE> -ldapBindDn <AD USER> -ldapBindDnPassword <PASSWORD> -ldapLoginName <USER FORMAT> -authentication DISABLED -OTPSecret <LDAP ATTRIBUTE>
```

Example:
```
add authentication ldapAction ldap_otp_action -serverIP 1.2.3.4 -serverPort 636 -ldapBase "OU=Users,DC=server,DC=com" -ldapBindDn administrator@ctxnsdev.com -ldapBindDnPassword PASSWORD -ldapLoginName userprincipalname -authentication DISABLED -OTPSecret userParameters
```

The differences between LDAP logon and OTP action are the need to disable the authentication (authentication = Disable) and introduction for new argument OTPSecret, which the value has to be an unused AD attribute (Please see Active Directory Configuration)

Authentication Policy for OTP Passcode Validation
In this case, it will be set to ‘true’ for simplicity:
```
add authentication Policy auth _pol _otp _validation -rule true -action ldap_otp_action
```

Presenting UI via LoginSchema
We will add the UI for two factor authentication
```
add authentication loginSchema lscheme _dual _factor -authenticationSchema "/nsconfig/loginSchema/LoginSchema/DualAuth.xml"
add authentication loginSchemaPolicy lpol _dual _factor -rule true -action lscheme _dual _factor
```

Creating Passcode Validation Factor via Policy Label
We will create a manage OTP flow policy label for our next factor (assuming the first factor is LDAP logon)
```
add authentication loginSchema lschema _noschema -authenticationSchema noschema
add authentication policymlabel manage _otp _flow _label -loginSchema lschema _noschema
```
Now, we will bind the OTP policy to the policy label:

```bash
bind authentication policylabel manage_otp_flow_label -policyName auth_pol_otp_validation -priority 10 -gotoPriorityExpression NEXT
```

**Bind the flow**

We would like to have the following flow: LDAP logon then OTP validation. Here is how it is done with authentication vserver:

```bash
bind authentication vserver authvs -policy auth_pol_ldap_logon -priority 10 -nextFactor manage_otp_flow_label -gotoPriorityExpression NEXT
```

We will bind the complete UI flow:

```bash
bind authentication vserver authvs -policy lpol_dual_factor -priority 30 -gotoPriorityExpression END
```

We will try to show single auth for 'device registration', if the conditions are not met, we will show multi-factor authentication.

**User Logon UI Flow**

Upon entering the LB vserver url e.g., https://lb.server.com, we will be presented with multi-factor authentication.
Troubleshooting

OTP Counters
We introduced new counters for OTP. To show the OTP related counters, please type the following:
nsconmsg -g otp -d stats

Example output:
root@ns# nsconmsg -g otp -d stats
Displaying current counter value information
NetScaler V20 Performance Data
reltime:mili second between two records Thu Jun 15 21:00:38 2017
Index reltime counter-value symbol-name&device-no
1 2883995 1 mem_tot_slotpages_allocated
3 0 0 mem_tot_slotpages_freed
5 0 0 mem_err_slotpages_allocationfailed
7 0 22 aaa_otp_tot_verify_success
9 0 3 aaa_otp_tot_verify_fail
11 0 158 aaa_otp_tot_manager_success
13 0 0 aaa_otp_tot_manager_fail
15 0 0 dns_totpipeline_request
Done.

• aaa_otp_tot_verify_success: total number of successful passcode verification
• aaa_otp_tot_verify_fail: total number of failed passcode verification
• aaa_otp_tot_manager_success: total number of successful device registration
• aaa_otp_tot_manager_success: total number of failed device registration

NS Log
Before analyzing the log, it is better to set the log level to debug like this:
> set syslogparams -loglevel DEBUG

Manage Device

Registration
The following entries will indicate a successful device registration:
"OTP registration succeeded, next factor: , for user: aaal@ctxnsdev.com"

Passcode Validation
"AAAD sent success while managing otp, operation: 5, user: <aaal@ctxnsdev.com>"

Delete Device
"AAAD sent success while managing otp, operation: 2, user: <aaal@ctxnsdev.com>"
User Logon

Successful Logon

extracted OTP secret from aaad, current factor: manage_otp_flow_label, for user: aaal@ctxnsdev.com, verifying incoming otp "0-311" Authentication succeeded, current factor: manage_otp_flow_label, for user: aaal@ctxnsdev.com"