This guide focuses on describing the configuration required for integrating Azure MFA (Multi-Factor Authentication) with NetScaler.
NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications.

Azure Multi-Factor Authentication (MFA) is Microsoft's two-step verification solution. It delivers authentication through multiple verification methods, including phone call, text message, or mobile app verification. By integrating with NetScaler, the time required for configuring Azure MFA as part of an enterprise authentication solution is significantly reduced by configuring Azure MFA as an authentication factor for NetScaler.

This deployment guide focuses on integrating Microsoft Azure Multi Factor Authentication (MFA) with NetScaler. This integration will allow use of the Azure MFA server as one of the authentication factors on NetScaler. This will allow users to use NetScaler for all authentication while being able to utilize Azure’s multi factor authentication capabilities.

NetScaler is a world-class application delivery controller (ADC) with the proven ability to load balance, accelerate, optimize and secure enterprise applications.

Azure Multi-Factor Authentication seamlessly integrates with NetScaler to provide additional security for logins and portal access. Multi-factor authentication (MFA) is combined with standard user credentials to increase security for user identity verification. NetScaler also supports similar capabilities as Azure MFA; this enables enterprise users to choose how they want their authentication landscape to be built.

In this guide, we will be looking at LDAP based integration for Azure MFA.

The following software versions are used and recommended for this configuration:

<table>
<thead>
<tr>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>NetScaler VPX (Enterprise/Platinum)</td>
<td>11.1</td>
</tr>
<tr>
<td>Azure MFA Server</td>
<td>7.3.0.3</td>
</tr>
</tbody>
</table>

Configuration Details

The test deployment topology is shown in Figure 1. This features an authentication setup with one NetScaler appliance, one Azure MFA server and a backend Active Directory/LDAP server for authentication.

*Figure 1: Deployment Topology*
Part 1: Configure Azure MFA Server

The following configuration is for the Azure MFA Server.
2. Connect Azure MFA to the directory service (Active Directory), then configure a default authentication method.
3. Import accounts to the MFA Users group.

Configuring Azure MFA authentication
1. Connect and log in to the Windows server where Azure MFA is installed.
2. Open the Apps screen. (Windows Server 2012)
3. Click the Multi-Factor Authentication Server icon under Multi-Factor Authentication Server (shown below)

4. The Multi-Factor Authentication Server window will open as shown below.
1. Now, enable LDAP authentication and add NetScaler as a client. Click the LDAP authentication icon in the left hand side panel as shown below -

![LDAP Authentication Icon](image1.png)

2. When the LDAP Authentication section is opened, select **Enable LDAP Authentication**.

![Enable LDAP Authentication](image2.png)
1. Select the Clients tab and change the port number, if necessary. The default ports are 389 for plaintext and 636 for SSL encryption.

2. If secure LDAP (LDAPS) is in use, click Browse and add the SSL certificate.
1. Click Add in the last dialog box shown to add a new LDAP client. Enter the following details here:
   - **IP address**: enter the NetScaler SNIP that will be used to communicate with Azure MFA
   - **Application name**: enter a descriptive name for the NetScaler client connection
   - **Require Multi-Factor Authentication user match**: If selected, only users who are included in the MFA Users list will be granted access; otherwise, only users who are included in the MFA Users list will need to authenticate with MFA. Other domain users will be able to authenticate without MFA.

2. Select the **Target** tab and verify that it shows LDAP. This completes the adding of NetScaler as an LDAP client and enabling of LDAP authentication.
Directory Integration

1. On the Multi-Factor Authentication Server window, click on Directory Integration in the navigation section.

2. When the Directory Integration tool opens, select the Settings tab.
1. Select Use Specific LDAP configuration.

2. Click Edit to open the Edit LDAP Configuration dialog box.
1. Enter the following settings:
   • Server – enter the directory server host name or IP address.
     NOTE: An FQDN is required if the Bind type below is set to SSL.
   • Base DN – enter the directory path.
   • Bind type – select the protocol to use for directory searches and authentication.
     NOTE: assigning the correct bind type is essential for security.
   • Queries – search options are:
     • Anonymous
     • Simple
     • SSL
     • Windows
   • Authentication – authentication options are:
     • Anonymous
     • Simple
     • SSL
     • Windows
   • Bind DN – only required for the SSL Bind type; enter a domain\user account with administrator privileges.
   • Bind Password – only required for the SSL Bind type; enter the password for the account.
   • Query size limit – specify the maximum number of users a search will return.

2. MFA server is able to successfully connect to the LDAP server.
3. Once the test completes successfully, click OK.
4. Click OK to close the completion prompt. This completes MFA server directory service setup.

**Default Authentication Method**

The Default Authentication Method defines the default authentication method that will be automatically assigned to MFA users; this method is required when users are not allowed to change authentication methods to ensure that there is a base authentication option assigned to every user. This is optional when users are allowed to change authentication methods.
1. Next, configure Company Settings. Click on Company Settings in the Navigation area:

2. Select the General tab
1. Leave default settings except for the following:
   • User defaults – select one of the options below:
     • Phone call – select Standard from the dropdown menu.
   • Text message – select Two-Way and OTP from the dropdown menus:
Mobile app – select Standard from the drop menu:
(this option requires device registration through the Azure Authentication app)

This completes the configuration for the Company Information Section for LDAP authentication.

Now, as the NetScaler is configured as an LDAP client, access is restricted to the vserver to only MFA users. To avoid the need for LDAP requests to require MFA, the administrator account has to be configured, and user accounts must be imported from the LDAP directory.

**Importing of User Accounts**

1. Click the Users icon in the navigation section as shown below -
1. In the Users section, Click Import from LDAP.

2. Select a user group on the Import screen -
1. Select the user accounts you want to import. Leave the settings as is, in this deployment flow the Import Phone option is set to Mobile. (Other options are also available)

![Import from LDAP dialog box]

2. Click the Import button. Then, click OK in the Import Success dialog box.

![Import Success dialog box]

Click Close on the Import screen to go back to the Users pane.
Configuring the MFA Administrator Account

Now, configure the MFA administrator account to allow LDAP requests without requiring MFA requests.

1. Select the Administrator account in the Users screen.
2. Click Edit.

1. Select the General tab.
1. Clear the Enabled checkbox.

![Edit User screenshot](image)

1. Select the Advanced tab.

![Edit User screenshot](image)
1. Leave the default settings, except for the following:
   - When user is disabled – select **Succeed Authentication**.
   - Account is used for LDAP Authentication password changes – this will allow end users to change their own passwords.

2. Click Apply, then click Close.

This completes configuration of the MFA server.
Part 2: Configure the NetScaler Appliance

The following configuration is required on the NetScaler appliance:
- LDAP authentication policy and server for domain authentication
- SSL certificate with external and internal DNS configured for the FQDN presented by the certificate (Wildcard certificates are supported.)
- VPN virtual server

This guide covers the configuration described above. The SSL certificate and DNS configurations should be in place prior to setup.

Configuring LDAP domain authentication

For domain users to be able to log on to the NetScaler appliance by using their corporate email addresses, you must configure an LDAP authentication server and policy on the appliance and bind it to your VPN VIP address. (Use of an existing LDAP configuration is also supported)

1. In the NetScaler configuration utility, in the navigation pane, select NetScaler Gateway > Policies > Authentication > LDAP.
2. To create a new LDAP policy: On the Policies tab click Add, and then enter LDAP_Policy as the name. In the Server field, click the ‘+’ icon to add a new server. The Authentication LDAP Server window appears.
   - In the Name field, enter LDAP_Server.
   - Select the bullet for Server IP. Enter the IP address of one of your Active Directory domain controllers. (You can also point to a virtual server IP for the purpose of redundancy if you are load balancing domain controllers)
   - Specify the port that the NetScaler will use to communicate with the domain controller. Use 389 for LDAP or 636 for Secure LDAP (LDAPS).

3. Under Connection Settings, enter the base domain name for the domain in which the user accounts reside within the Active Directory (AD) for which you want to allow authentication. The example below uses cn=Users,dc=ctxns,dc=net.
4. In the Administrator Bind DN field, add a domain account (using an email address for ease of configuration) that has rights to browse the AD tree. A service account is advisable, so that there will be no issues with logins if the account that is configured has a password expiration.
5. Check the box for Bind DN Password and enter the password twice.
6. Under Other Settings: Enter samaccountname as the Server Logon Name Attribute.
7. In the SSO Name Attribute field, enter UserPrincipalName. Enable the User Required and Referrals options. Leave the other settings as they are.

8. Click on More at the bottom of the screen, then add mail as Attribute 1 in the Attribute Fields section. Leave Nested Group Extraction in the Disabled state (we are not going to be using this option for this deployment).

9. Click the Create button to complete the LDAP server settings.
10. For the LDAP Policy Configuration, select the newly created LDAP server from the Server drop-down list, and in the Expression field type ns_true.
To Configure your VPN (NetScaler Gateway) Virtual Server

An employee trying to log in using is redirected to a NetScaler VPN virtual server that validates the employee’s corporate credentials. This virtual server listens on port 443, which requires an SSL certificate. External and/or internal DNS resolution of the virtual server’s IP address (which is on the NetScaler appliance) is also required. The following steps require a preexisting virtual server to be in place. In addition, they assume that DNS name resolution is already in place, and that the SSL certificate is already installed on your NetScaler appliance.

1. In the NetScaler Configuration tab navigate to NetScaler Gateway > Virtual Servers and click the Add button.

2. In the Gateway Virtual Server window, enter the virtual server’s name and IP address.
4. Click Continue.
5. In the Certificates section, select No Server Certificate.

6. In the Server Cert Key window, click Bind.
7. Under SSL Certificates, choose your AAA SSL Certificate and select Insert. (Note – This is NOT the SFDC SP certificate.)
8. Click Save, then click Continue.
9. Click Continue again to bypass the Advanced Policy creation option, instead opting to add a Basic Authentication Policy by selecting the ‘+’ icon on the right side of the window.
10. From the Choose Type window, select Choose Policy from the drop-down list, select LDAP, leaving Primary as the type, and select Continue.

11. Select Bind and from within the Policies window select the LDAP Policy created earlier.
12. Click OK to return to the Gateway Virtual Server screen.

Testing Authentication

Device Registration for Azure Authenticator Users
(This step only applies when the mobile app authentication method is used.)
The instructions below explain activation of a user device through the MFA server Users Portal.

Requirements
• A device with the Azure Authenticator mobile application installed. The application can be downloaded from the platform store for the following devices:
  • Windows Phone
  • Android
  • iOS
• The Azure Users Portal address.
• A computer to access the Users Portal.
• User credentials

Activate Device
1. Log in to the Azure user portal from a browser.
2. On the setup screen, click on Generate Activation Code
4. Activation code options are shown as below.

5. Activate the mobile authentication app on the test device.
6. There are two options:
   • Enter the Activation Code and URL displayed on the Users Portal screen on the device activation screen.
   • Use the device to scan the barcode displayed on Users Portal screen.

This completes device activation.

Login
Now you are ready to test MFA authentication. Please note the requirements listed below before you start.

General Requirements
• A computer to access the login screen.
• The SSL VPN appliance URL for network sign in.
• User credentials

Phone Call
Required: A phone with the number listed in the AD user account Mobile phone attribute.
1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the phone for a call.
NOTE: The call originates in the cloud from the Azure MFA application.
Example:

4. The phone call will provide instructions to complete authentication.

Text Message
Required: An SMS-capable phone with the number listed in the user account Mobile phone attribute
1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the phone for a text message with the verification code.
Example


4. Reply to the text message with the same verification code.

Mobile App
Required: A device with the Azure Authenticator app activated.
1. On a computer, open the login page in a web browser.
2. Enter user credentials.
3. Check the device with Azure Authenticator for a prompt.

Example

4. Click Verify.
5. The authentication application will communicate with the MFA server to complete authentication.

Successful authentication will grant access through the browser session.
This completes the setup and testing for Azure Multi-Factor Authentication using the LDAP protocol in a Citrix NetScaler SSL VPN appliance deployment.
Conclusion

Citrix NetScaler enables integration with Azure MFA, allowing a multitude of authentication use cases to be delivered successfully for enterprise customers.