Integrating Microsoft Intune/Enterprise Mobility Suite with NetScaler (LDAP+OTP Scenario)

This guide focuses on defining the process for integrating Microsoft Intune with NetScaler for scenarios where LDAP and OTP (One Time Password) based authentication is required.
Table of Contents

Contents
Introduction          3
Pre-requisites          3
Deployment diagram         4
Configuration Steps         5
Part 1: Convert existing NetScaler Gateway Authentication policies from classic to advanced and NAC configuration         5
Step 1: Convert exiting NetScaler Gateway Authentication policies from classic to advanced 5
Step 2: Configure Azure Gateway App (this is a prerequisite to configure OAuth policy in NetScaler) 6
Step 3: Setup NetScaler for NAC compliance       16
Part 2: Test Citrix VPN plugin
Troubleshooting          22
Appendix            23
Classic NetScaler Gateway Configuration       23
Fresh configuration of NetScaler Gateway with Advance Policies and NAC configuration 23
Introduction

In this document, we are going to discuss how to configure the existing gateway used for connecting to internal network from a mobile device (iOS and Android) with an extra layer of security called Network Access Compliance (NAC) offered by Microsoft Intune.

When a user tries to connect to NetScaler Gateway from iOS/Android VPN client, first a call is made to the Intune Cloud service to check whether the device is:
1. Managed: The device has been enrolled using Intune Company Portal client.
2. Compliant: Required policies that were pushed from the Intune MDM server have been applied.

Once the device is both Managed and Compliant, the VPN session is established and the user is then able to access internal resources.

The document details the following:
Part 1: Conversion of the classic policy in existing NetScaler Gateway to advanced policy and NAC configuration
Part 2: Test of the VPN Plugin
This document covers CLI related configuration. In case of a fresh NetScaler Gateway deployment for EMS/Intune integration, you can refer to the following document for UI configuration:

Prerequisites

The deployment steps are applicable to NetScaler version 11.1.51.21 and above. It also needs latest versions of iOS (1.0.6) and Android VPN (2.0.13) clients, which support Intune NAC. In the NetScaler Gateway all the existing authentication policies have to be converted from classic to advanced policies.

<table>
<thead>
<tr>
<th>Citrix Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Netscaler</td>
<td>11.1.51.21 or above</td>
</tr>
<tr>
<td>iOS VPN</td>
<td>1.0.6 or above</td>
</tr>
<tr>
<td>Android VPN</td>
<td>2.0.13 or above</td>
</tr>
</tbody>
</table>
Microsoft
- Azure AD Access (having Tenant Admin privileges)
- Intune Enabled tenant

Firewall Rule
- Enable Firewall rule to allow DNS and SSL traffic from subnet ip to https://login.microsoftonline.com and https://graph.windows.net (port 53 and 443)

Deployment Diagram

All the deployment steps are written in accordance with the reference deployment given below:

<table>
<thead>
<tr>
<th>Resource</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain</td>
<td>Example.com</td>
</tr>
<tr>
<td>LDAP Server (Secondary Auth)</td>
<td>10.1.1.50</td>
</tr>
<tr>
<td>RADIUS Server (Primary Auth)</td>
<td>10.1.1.74</td>
</tr>
<tr>
<td>Gateway VIP</td>
<td>10.2.1.52</td>
</tr>
<tr>
<td>Password (For LDAP and Radius)</td>
<td>Password</td>
</tr>
<tr>
<td>Admin BIND username</td>
<td><a href="mailto:administrator@example.com">administrator@example.com</a></td>
</tr>
</tbody>
</table>

Deployment without EMS/Intune integration

Deployment with EMS/Intune integration
Configuration Steps

Part 1: Convert existing NetScaler Gateway Authentication policies from classic to advanced and NAC configuration

The following sections assumes that you have an existing Netscaler configured as per the deployment diagram shown above. For a fresh installed NetScaler, please refer to Appendix section: Fresh configuration of NetScaler Gateway with Advance Policies and NAC configuration.

Step 1: Convert existing NetScaler Gateway Authentication policies from classic to advanced

The following is a basic example of converting classic policy to advance. For more information on how to convert from classic to advanced policies, please refer to: https://support.citrix.com/article/CTX131024

The sample NetScaler Gateway before conversion has the following:
- LDAP Policy named “example_ldap_pol”
- Radius Policy named “example_radius_pol”
- VPN VServer named “gw1_vpn”
  - First authentication policy will be “example_radius_pol”
  - Second authentication policy will be “example_ldap_pol”

For the full configuration, please refer to Appendix: Classic NetScaler Gateway Configuration

Unbind existing classic authentication policies from VPN Vserver

The following commands unbind the existing classic authentication policies from the VPN VServer

unbind vpn vserver gw1_vpn -policy example_radius_pol
unbind vpn vserver gw1_vpn -policy example_ldap_pol -secondary

Create new advanced authentication policy for Radius and LDAP

We will create a new set of authentication policies for Radius and LDAP. We can reuse all the actions created earlier as they are not being affected. It should look like this:

add authentication Policy example_ldap_adv_pol -rule true -action example_ldap_action
add authentication Policy example_radius_adv_pol -rule true -action example_radius_action

Create new Authentication vServer, AuthnProfile and update the VPN vServer with the AuthnProfile

In order to support the newly created advanced authentication policies, create the following:
- Authentication VServer (This virtual server processes the associated authentication policies and accordingly provides access to the application using AuthnProfile)
- AuthnProfile (To allow other vserver e.g., gateway or lb to reuse AuthVServer)

For more reference, please refer to https://docs.citrix.com/en-us/netscaler/11-1/aaa-tm/authentication-virtual-server.html

add authentication vserver auth_vsl SSL 0.0.0.0
add authentication authnProfile authn_prof1 -authnVsName auth_vsl
set vpn vserver gw1_vpn -authnProfile authn_prof1

The last command, associates the authnProfile to the VPN gateway.
Create loginSchemaPolicy for Dual Factor Auth and bind it to Authentication vServer

As part of the advanced policy’s design, the UI and authentication logics are being separated. The login scheme allows the administrator to define UI requirements to be presented to the client devices e.g., browser. In this example, a two-factor authentication login schema is defined and the same is attached to the authentication vserver:

```bash
add authentication loginSchemaPolicy ls_2factor_pol -rule true -action lschema_dual_factor_deviceid
bind authentication vserver auth_vs1 -policy ls_2factor_pol -priority 100 -gotoPriorityExpression END
```

`lschema_dual_factor_deviceid` is a built-in login schema which requests clients to supply device_id (for mobile) on top of the radius and ldap challenges.

Create PolicyLabel with NoSCHEMA and bind it with Secondary Auth (in this case LDAP)

This policy label is created to ensure that NetScaler will terminate the authentication flow:

```bash
add authentication policylabel pol_label_ldap -loginSchema LSCHEMA_INT
bind authentication policylabel pol_label_ldap -policyName example_ldap_adv_pol -priority 90 -gotoPriorityExpression NEXT
```

Bind the Primary auth (in this case RADIUS) to Authentication vServer and choose the next factor as the PolicyLabel created for Secondary auth (in this case LDAP)

```bash
bind authentication vserver auth_vs1 -policy example_radius_adv_pol -priority 80 -nextFactor pol_label_ldap -gotoPriorityExpression NEXT
```

At this point, use the Citrix VPN client to connect to the NetScaler Gateway to ensure VPN connectivity before moving on to the next step.

**Step 2: Configure Azure Gateway App (this is a prerequisite to configure OAuth policy in NetScaler)**

Prerequisite:
- Azure global admin credentials.
- Intune licensing is enabled

For Intune Integration you need to create a NetScaler Gateway application on Azure portal. Once the NetScaler Gateway application is created, configure the OAuth policy on NetScaler Gateway using the following application specific information:
1. Client ID / Application ID
2. Client Secret / Application Key
3. Azure Tenant ID

NetScaler uses the app client id and client secret to communicate with Azure and check for NAC compliance. Follow the steps below to create NetScaler Gateway App on Azure:

NOTE: This can be also configured using manage.windowsazure.com portal.

1. Login to portal.azure.com
2. Click on “Azure Active Directory”
Create loginSchemaPolicy for Dual Factor Auth and bind it to Authentication vServer

As part of the advanced policy’s design, the UI and authentication logics are being separated. The login scheme allows the administrator to define UI requirements to be presented to the client devices e.g., browser. In this example, a two-factor authentication login schema is defined and the same is attached to the authentication vserver:

```bash
add authentication loginSchemaPolicy ls_2factor_pol -rule true -action lschema_dual_factor_deviceid
bind authentication vserver auth_vs1 -policy ls_2factor_pol -priority 100 -gotoPriorityExpression END

'lschema_dual_factor_deviceid' is a built-in login schema which requests clients to supply device_id (for mobile) on top of the radius and ldap challenges.

Create PolicyLabel with NoSCHEMA and bind it with Secondary Auth (in this case LDAP)

This policy label is created to ensure that NetScaler will terminate the authentication flow:

```bash
add authentication policylabel pol_label_ldap -loginSchema LSCHEMA_INT
bind authentication policylabel pol_label_ldap -policyName example_ldap_adv_pol -priority 90 -gotoPriorityExpression NEXT
```

Bind the Primary auth (in this case RADIUS) to Authentication vServer and choose the next factor as the PolicyLabel created for Secondary auth (in this case LDAP)

```bash
bind authentication vserver auth_vs1 -policy example_radius_adv_pol -priority 80 -nextFactor pol_label_ldap -gotoPriorityExpression NEXT
```

At this point, use the Citrix VPN client to connect to the NetScaler Gateway to ensure VPN connectivity before moving on to the next step.

**Step 2: Configure Azure Gateway App (this is a prerequisite to configure OAuth policy in NetScaler)**

Prerequisite:
- Azure global admin credentials.
- Intune licensing is enabled

For Intune Integration you need to create a NetScaler Gateway application on Azure portal. Once the NetScaler Gateway application is created, configure the OAuth policy on NetScaler Gateway using the following application specific information:
1. Client ID / Application ID
2. Client Secret / Application Key
3. Azure Tenant ID

NetScaler uses the app client id and client secret to communicate with Azure and check for NAC compliance. Follow the steps below to create NetScaler Gateway App on Azure:

NOTE: This can be also configured using manage.windowsazure.com portal.

1. Login to portal.azure.com
2. Click on “Azure Active Directory”
Create `loginSchemaPolicy` for Dual Factor Auth and bind it to Authentication vServer

3. Click “App registrations” and click “Add”

4. In the ADD screen (shown below) provide Name and choose Application Type as Web App / API. For Sign-on URL, provide the FQDN of NetScaler Gateway and then, click Create.

5. Once the App is created, select the App and under Settings click “Required Permission”:
6. In the Required Permission UI, you need to set correct permission for the following:
   A. Windows Azure Active Directory
   B. Microsoft Intune API
   C. Microsoft Graph API

A. Setting permission for Windows Azure Active Directory

   a. Select “Windows Azure Active Directory” and under Enable Access UI ensure that the following Delegated Permissions are selected and then save the changes.
b. After the required permissions for Windows Azure Active Directory are set, the wizard should appear as follows:

![Required permissions](image1)

B. Setting permission for Microsoft Intune API

a. Click "+Add" Under Required Permission:

![Settings](image2)

b. Under Add API access, click "Select an API":

![Add API access](image3)
c. Search for “Microsoft Intune API” and click Select:

```
c. Search for “Microsoft Intune API” and click Select:

<table>
<thead>
<tr>
<th>Add API access</th>
<th>Select an API</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Select an API</td>
<td>Microsoft Intune API</td>
</tr>
<tr>
<td>2 Select permissions</td>
<td>Microsoft Intune API</td>
</tr>
</tbody>
</table>
```

d. Click “Get device state and compliance information from Microsoft Intune” option and then click Select. Click Done to add the Microsoft Intune API permissions.

```
d. Click “Get device state and compliance information from Microsoft Intune” option and then click Select. Click Done to add the Microsoft Intune API permissions.

![Enable Access](image)
```

e. After adding the Microsoft Intune API the required permissions UI should look like this:

```
e. After adding the Microsoft Intune API the required permissions UI should look like this:

<table>
<thead>
<tr>
<th>API</th>
<th>APPLICATION PERMISSIONS</th>
<th>DELEGATED PERMISSIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Azure Active Directory</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Microsoft Intune API</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```
C. **Setting permission for “Microsoft Graph API” under Required permission:**

a. Click “Add API Access” and search for Microsoft Graph. Click “Microsoft Graph” and then click Select:

![Add API access](image1)

![Select an API](image2)

b. Select the following four (4) delegated permissions:
   - Sign in and read user profile
   - Sign Users in
   - View users’ email address
   - View users’ basic profile

![Enable Access](image3)
c. After selecting the four permissions mentioned above, click Done under Add API access UI:

At this point, you can also choose to grant permission for all tenant accounts to use the app without providing credentials. To do so, choose Grant permissions and accept the confirmation prompt. When you run the application for the first time, you’re prompted to grant the app permission to perform the selected roles.
d. Once the Microsoft Graph API permission is set, the Required Permission user-interface should appear as follows:

![Required permissions](image)

<table>
<thead>
<tr>
<th>API</th>
<th>APPLICATION PER...</th>
<th>DELEGATED PERM...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Azure Active Directory</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>Microsoft Intune API</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

7. Once the required permissions are configured, make sure the “App ID URI” and “Home Page URL” are set to the NetScaler Gateway FQDN:

![Properties](image)

- App ID URI: `https://fqdn_of_netscaler_gateway`
8. Make sure that the Reply URLs under settings also have NetScaler Gateway FQDN configured:

9. Click “Keys” under Settings UI and choose the desired value for “Description & Expires” and click “Save”:

10. Copy the key value (This is the client secret for the NetScaler Gateway configuration):

⚠️ Copy the key value. You won’t be able to retrieve after you leave this blade.
11. Make sure to note down the application ID (This is the client id for the NetScaler Gateway configuration) of the app and tenant ID as well:

![NetScaler Gateway Configuration](image)

Tenant ID can be found from the Endpoints:
https://login.windows.net/aaaaaaaa-c829-4012-8b56-03570ec4ef85/federationmetadata/2007-06/federationmetadata.xml

![Endpoints](image)

From the steps described above we obtain the following values:
1. Client ID / Application ID
2. Client Secret / Application Key
3. Azure Tenant ID

**Step 3: Setup NetScaler for NAC compliance**

Prerequisites: Client ID, Client Secret and Tenant ID from Azure Gateway app from Step 2 above.

Here we create a New Authentication Policy associated with OAuth Action and bind it to Authentication vServer. The LDAP Authentication Policy is associated as NEXT factor to this new authentication policy and RADIUS is NEXT LDAP. When a user tries to access the gateway, the OAuth Policy is triggered first to check the device state. If the device is enrolled and Compliant, then the user is authenticated with the supplied credentials.

**Adding Intune/EMS authentication action**

```
#Create OAuthAction
```

![NetScaler Gateway Configuration](image)
Once OAuth action is added, you can run the command given below to check the OAuth status. If the status shows COMPLETE, the configuration is a success.

```
> sh OAuthAction
```

If the status says COMPLETE, then the OAuthAction is a success.

NOTE: If you see the OAuth Status other than COMPLETE, please refer to the Troubleshooting section.

**Adding Authentication Policy for NAC check**

#Create Authentication Policy with proper rule to detect User-Agent containing NAC, then bind it to the OAuth Action

```
add authentication Policy oauth_gw1_intune_pol -rule "HTTP.REQ.header("User-Agent").contains("NAC/1.0") && (http.REQ.header("User-Agent").contains("iOS") || http.REQ.header("User-Agent").contains("Android"))" -action intune_example_action
```

bind authentication vserver auth_vsl -policy intune_example_action_pol -priority 70

**Rewiring the Authentication policy**

#UnBind Primary Factor (RADIUS Auth) from Auth vServer for the earlier config

```
unbind authentication vserver auth_vsl -policy example_radius_adv_pol
```

#Create PolicyLabel with loginSchema we used earlier for two factor auth and then bind with Primary auth policy (in this case RADIUS) and NEXTFACTOR being Secondary auth (in this case LDAP)

```
add authentication policylabel pol_label_radius -loginSchema ls_2factor_pol
```

```
bind authentication policylabel pol_label_radius -policyName example_radius_adv_pol -priority 100 -gotoPriorityExpression NEXT -nextFactor pol_labelldap
```
Optional: Supporting Non NAC aware VPN plugin

In cases when admin wants to enable access to VPN client that do not support network access check like, Windows/MAC and older iOS and Android VPN client, a policy like the one given below can be created and attached to Authentication vServer:

```plaintext
add authentication Policy non-nac-comp-auth gw1 intune pol
-rule "!(http.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0") && ((http.REQ.HEADER("User-Agent").CONTAINS("iOS") && http.REQ.HEADER("User-Agent").contains("NSGiOSplugin")) || (http.REQ.HEADER("User-Agent").CONTAINS("Android") && http.REQ.HEADER("User-Agent").contains("CitrixVPN"))))" -action NO_AUTHN
```

Create a policy label with just dual factor loginSchema (for non NAC enabled clients) and bind the policy label to same radius authentication policy (primary) and then have the next factor as ldap (secondary):

```plaintext
add authentication policy label pol_label_radius_non_nac -loginSchema lschema_dual_factor
bind authentication policy label pol_label_radius_non_nac -policyName example_radius_adv_pol -priority 100 -gotoPriorityExpression NEXT -nextFactor pol_label_intune_ldap
```

After creating the authentication policy for non NAC compliant client, the policy need to be bound to the Authentication vserver with the next factor as "pol_label_radius_non_nac":

```plaintext
bind authentication vserver auth_vs1 -policy non-nac-comp-auth gw1 intune pol -priority 100 -nextFactor pol_label_radius_non_nac -gotoPriorityExpression NEXT
```

### Part 2: Test Citrix VPN plugin

Assuming everything is configured properly, you see the flow as described below. Following are the states of the client during NAC check:

<table>
<thead>
<tr>
<th>Device</th>
<th>isManaged (Device is Enrolled)</th>
<th>ComplianceState (Device is Compliant)</th>
<th>NAC Check (Pass / Fail)</th>
<th>Citrix VPN Client Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>iOS/Android</td>
<td>True</td>
<td>True</td>
<td>Pass</td>
<td>Establish VPN</td>
</tr>
<tr>
<td>iOS/Android</td>
<td>True</td>
<td>False (User has not changed the passcode set on the MDM policy)</td>
<td>Fail</td>
<td>Display message stating device is not Compliant</td>
</tr>
<tr>
<td>iOS/Android</td>
<td>False</td>
<td>False</td>
<td>Fail</td>
<td>Display message stating device is not managed</td>
</tr>
</tbody>
</table>
If the user enrolls an iOS/Android device using Intune Company Portal app and connects to VPN using the Citrix VPN client, then user will be allowed to connect to VPN as the NAC check will have the following state in /var/log/ns.log:

```
Jan 6 22:01:48 <local0.debug> 10.207.85.24 01/07/2017:06:01:48 GMT gw2 0-PPE-0 : default AADHM Message 1439 0 : "AUTH RESP: ns aaa auth resp handler, response from Server is: {"azureDeviceId": "C6947F2F-7B77-49B0-972D-3A5D89F45D13", "managedState": 
ComplianceState: "Failed", "imei": null, "managedId": null, "model": "iPad Air 2", "osVersion": "10.3.2", "serialNumber": "D729F8W"}, "uid": "d2e07035-15f6-457d-8740-f0ab577663f1"}
```

In case the device is not enrolled, when connecting to the NAC enabled Gateway with a NAC compatible VPN client (latest version of Gateway client from App Store) we should see connection error in the UI and the below entries in /var/log/ns.log:

```
Jan 7 16:38:26 <local0.debug> 10.207.85.24 01/07/2017:00:38:26 GMT gw2 0-PPE-0 : default AADHM Message 2548 0 : "AUTH RESP: ns aaa auth resp handler, response from Server is: {"azureDeviceId": "00000000-0000-0000-0000-000000000000", "managedState": null, "imei": null, "managedId": null, "model": "null", "osVersion": null, "serialNumber": null, "uid": "null"}
```

**iOS:**

![iOS connection error screenshot](image)
Android:

In case the device is enrolled but not Compliant, when connecting to the NAC enabled Gateway with a NAC compatible VPN client (latest version of Gateway client from App Store) we should see connection error in the UI and the below entries in /var/log/ns.log:

```
Jan 9 20:28:45 <local0.debug> 11.11.11.11 01/09/2017:20:28:45 GMT nsng2 0-PPE-0 : default AAAAT Message 6382822 0 : "CAUTH RESP: ns aaa cauth resp handler, response from Server is: ("macAddress": "\w{12}", "meid": ", isManaged": true, "complianceState": false, "imei": "\w{14}", "osVersion": "6.0", "manufacturer": "super", "azureDeviceId": "\w{36}", "sn": "\w{12}", "uid": ", "serialNumber": "\w{12}", "lastContactTimeUtc": "08/16/2016 08:23:31", "model": "MotoG3-TE")"
```
iOS:

Android:
### Troubleshooting

Few common issues and their solutions are highlighted below. For troubleshooting, enable more logs and check them by doing the following:

1. On CLI run the following command:
   ```bash
   set audit syslogParams -logLevel ALL
   ```
2. Check the logs from shell using:
   ```bash
   tail -f /var/log/ns.log
   ```

<table>
<thead>
<tr>
<th>Issue</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The permissions required to be configured for Gateway App on Azure</td>
<td>Check if proper Intune license is available. Try using the manage.windowsazure.com portal to see if the permission can be added. Contact Microsoft support if the issue persists.</td>
</tr>
<tr>
<td>are greyed out</td>
<td></td>
</tr>
<tr>
<td>NetScaler Gateway cannot reach login.microsoftonline.com and</td>
<td>From NS Shell check if you are able to reach Microsoft website:</td>
</tr>
</tbody>
</table>
| graph.windows.net                                                   |   ```bash
   curl -v -k https://login.microsoftonline.com
   ```                                                                          |
|                                                                      | Check whether DNS is configured on NetScaler and firewall settings are proper (in case DNS requests are firewall). |
| Getting error in ns.log after configuring OAuthAction                | Check if Intune licensing is enabled and the Azure Gateway app has proper permission set. |
| Sh OAuthAction command does not show OAuth status as complete        | Check DNS and configured permission on Azure Gateway App                  |
| Android and iOS device does not show dual authentication prompt      | Check if Dual Factor Device ID logonSchema is bound to Authentication vServer |

### OAuth Error Condition and Status:

<table>
<thead>
<tr>
<th>Status</th>
<th>Error Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>COMPLETE</td>
<td>Success</td>
</tr>
<tr>
<td>AADFORGRAPH</td>
<td>Invalid client id/secret, URL not resolved, connection timeout</td>
</tr>
<tr>
<td>MDMINFO</td>
<td>manage.microsoft.com is down or unreachable</td>
</tr>
<tr>
<td>GRAPH</td>
<td>Graph endpoint is down or unreachable</td>
</tr>
</tbody>
</table>
Appendix

Classic NetScaler Gateway Configuration

add authentication ldapAction example_ldap_action -serverIP 10.1.1.50 -ldap-Base "dc=example,dc=com" -ldapBindDn administrator@example.com -ldapBindDnPassword Password -ldapLoginName userPrincipalName

add authentication radiusAction example_radius_action -serverIP 10.1.1.74 -serverPort 1812 -radKey Password

add authentication radiusPolicy example_radius_pol NS_TRUE example_radius_action

add authentication ldapPolicy example_ldap_pol NS_TRUE example_ldap_action

add vpn vserver gw1_vpn SSL 10.2.1.52 443 -Listenpolicy NONE
bind vpn vserver gw1_vpn -policy example_radius_pol
bind vpn vserver gw1_vpn -policy example_ldap_pol -secondary

add vpn sessionAction session_action -transparentInterception ON -defaultAuthorizationAction ALLOW -icaProxy OFF -ClientChoices ON -clientlessVpnMode OFF

add vpn sessionPolicy session_pol NS_TRUE session_action
set vpn parameter -forceCleanup none -clientConfiguration all -UITHEME DEFAULT
bind vpn vserver gw1_vpn -policy session_pol
bind ssl vserver gw1_vpn -certkeyName wild-example-cert

Fresh configuration of NetScaler Gateway with Advance Policies and NAC configuration

#These features in NetScaler needs to be enabled
enable ns feature WL SP SSL SSLVPN AAA

#Create CertKey
add ssl certKey wild-example-cert -cert wild-example -key wild-example

#Add DNS Server (This is must and should be able to resolve Microsoft URL for NAC Check - If Firewall is in place then make sure that login.microsoftonline.com is accessible by NS)

add dns nameServer 10.1.1.50
#Create Authentication Policies
add authentication radiusAction example _ radius _ action -serverIP 10.1.1.74 -serverPort 1812 -radKey Password
add authentication Policy example _ radius _ adv _ pol -rule true -action example _ radius _ action

add authentication ldapAction example _ ldap _ action -serverIP 10.1.1.50 -ldapBase "dc=example,dc=com" -ldapBindDn administrator@example.com -ldapBindDnPassword Password -ldapLoginName userPrincipalName
add authentication Policy example _ ldap _ adv _ pol -rule true -action example _ ldap _ action

#Create Authentication vServer ad AuthnProfile
add authentication vserver auth _ vs1 SSL 0.0.0.0
add authentication authnProfile authn _ prof1 -authnVsName auth _ vs1 -authnVsPolicy auth _ vs1

#Create Gateway VIP and add the authnprofile. Bind proper certificate and set appropriate VPN parameters.
add vpn vserver gw2 _ vpn SSL 10.2.1.52 443 -Listenpolicy NONE -authnProfile authn _ prof1
bind ssl vserver gw2 _ vpn -certkeyName wild-example-cert
set vpn parameter -forceCleanup none -clientConfiguration all -UITHEME DEFAULT

#Create OAuthAction and Authentication policy that binds the OAuthAction to it.

# Create Dual factor device id LogonSchema & Policy Label for RADIUS (Primary Auth) & LDAP (Secondary Auth). As LDAP is going to be the last factor the loginSchema should be LSCHEMA _ INT (noSchema).
add authentication loginSchemaPolicy ls _ 2factor _ pol -rule true -action lschema _ dual _ factor _ deviceid
add authentication policylabel pol_label_ldap -loginSchema LSCHEMA_INT
  # Bind Policy Label with appropriate authentication policies and then bind the
  # Primary auth label to AuthvServer. The secondary auth label will be attached
  # as NextFactor to Primary Policy Label
  
  bind authentication policylabel pol_label_ldap -policyName example_ldap_adv_pol
  -priority 90 -gotoPriorityExpression NEXT

  bind authentication policylabel pol_label_radius -policyName example_radius_adv_pol
  -priority 100 -gotoPriorityExpression NEXT -nextFactor pol_label_ldap

  bind authentication vserver auth_vsl -policy intune_example_action_pol
    -priority 70 -nextFactor pol_label_intune_radius -gotoPriorityExpression NEXT

# To support non NAC Compliant clients create an Authentication policy with
# rule not to check for NAC User-Agent. Then bind the authentication policy to
# AuthvServer. Here we should not bind the OAuthAction.

add authentication Policy non_nac_comp_auth_gw2_intune_pol
  -rule "!(http.REQ.HEADER("User-Agent").CONTAINS("NAC/1.0") &&
    ((http.REQ.HEADER("User-Agent").CONTAINS("iOS") && http.REQ.HEADER("User-
    Agent").contains("NSGiOSplugin")) ||
    (http.REQ.HEADER("User-Agent").CONTAINS("Android") && http.REQ.HEADER("User-Agent").contains("CitrixVPN"))))"
  -action NO_AUTHN

# Create Dual factor LogonSchema & Policy Label for RADIUS (Primary Auth) &
# LDAP (Secondary Auth).

NOTE: This is different from the Dual Factory Device ID LogonSchema that we
created for NAC enabled device.

add authentication loginSchema lschema_dual_factor -authenticationSchema "/
  nsconfig/loginschema/LoginSchema/DualAuth.xml"

# Create a new Non NAC policylabel and add the above logonSchema to it. Then
# for primary auth (Radius) and bind it to the Radius policy and next factor being ldap

add authentication policylabel pol_label_radius_non_nac -loginSchema
  lschema_dual_factor

bind authentication policylabel pol_label_radius_non_nac -policyName ex-
  ample_radius_adv_pol -priority 100 -gotoPriorityExpression NEXT -nextFactor pol_label_intune_ldap

# Bind the NON NAC Authentication policy to Authentication VServer choosing the
# NEXT factor as the Primary auth

bind authentication vserver auth_vsl -policy non_nac_comp_auth_gw2_int-
  tune_pol -priority 100 -nextFactor pol_label_radius_non_nac -gotoPriori-
  tyExpression NEXT
# Create appropriate Session Policy and Actions and Bind it to VPN vServer

```bash
add vpn sessionAction session_action -transparentInterception ON -defaultAuthorizationAction ALLOW -icaProxy OFF -ClientChoices ON -clientlessVpnMode OFF
add vpn sessionPolicy session_pol NS_TRUE session_action
bind vpn vserver gw2_vpn -policy session_pol
```

# Bind the Dual Factor Device ID logonSchema to Authentication vServer. This is essential for the appropriate rendering of the UI on mobile Citrix VPN client (iOS and Android).

```bash
bind authentication vserver auth_vs1 -policy ls_2factor_pol -priority 100 -gotoPriorityExpression END
```

# Increase the logLevel to all for debugging. Make sure to set it to default level after debugging is done.

```bash
set audit syslogParams -logLevel ALL
```