Contents

[Publishing Web Server 1](#_Toc25736986)

[Create a Virtual Server 1](#_Toc25736987)

[Configure Load Balancer 2](#_Toc25736988)

[Bind Virtual Server 3](#_Toc25736989)

[Bind Certificate 4](#_Toc25736990)

[Protecting Application with Azure AD 6](#_Toc25736991)

[Setting up Azure AD SAML SSO 6](#_Toc25736992)

[Citrix ADC SAML Profile 8](#_Toc25736993)

[Create Authentication Policy 8](#_Toc25736994)

[Create Authentication Virtual Server 9](#_Toc25736995)

[Configure the Authentication Virtual Server to use Azure AD 10](#_Toc25736996)

[Configuring Kerberos Based Authentication 13](#_Toc25736997)

[Create a Kerberos Delegation Account for Citrix ADC 13](#_Toc25736998)

[Citrix AAA KCD ( Kerberos Delegation Accounts) 14](#_Toc25736999)

[Citrix Traffic Policy and Traffic Profile 15](#_Toc25737000)

[Citrix Bind Traffic Policy to Virtual Servers 17](#_Toc25737001)

[Configuring Header Based Authentication 19](#_Toc25737002)

[Azure AD Claims Mapping 19](#_Toc25737003)

[Citrix ADC Configuration 20](#_Toc25737004)

[Create an Rewrite Action 20](#_Toc25737005)

[Create a Rewrite Policy. 21](#_Toc25737006)

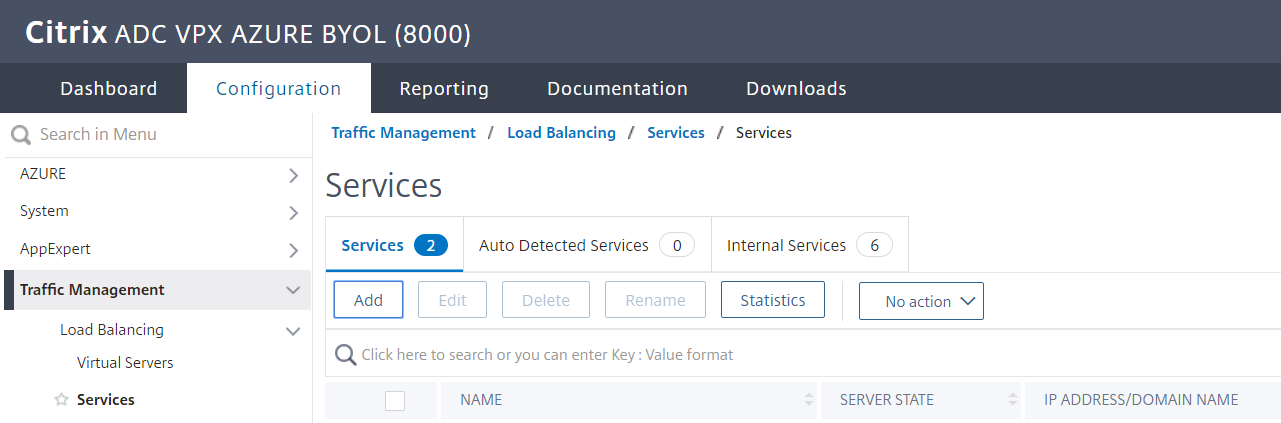
[Bind Rewrite Policy to Virtual Servers 22](#_Toc25737007)

[Modify SAML Server to Extract Attributes from Claim 24](#_Toc25737008)

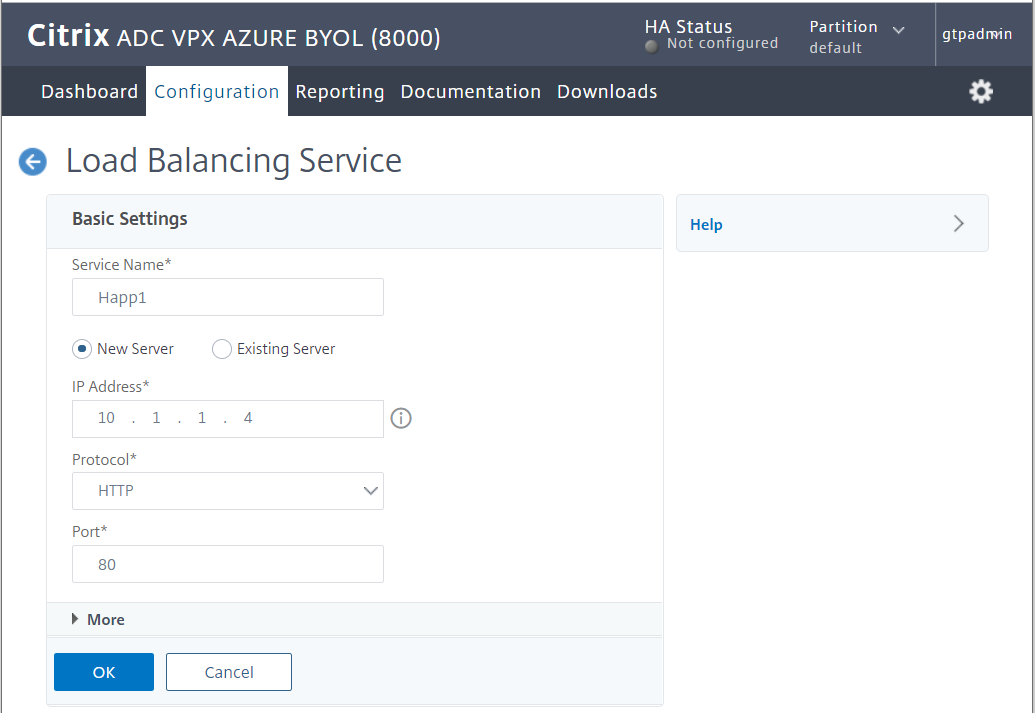
## Publishing Web Server

### Create a Virtual Server

1. Goto Traffic Management > Load Balancing > Services
2. Click Add

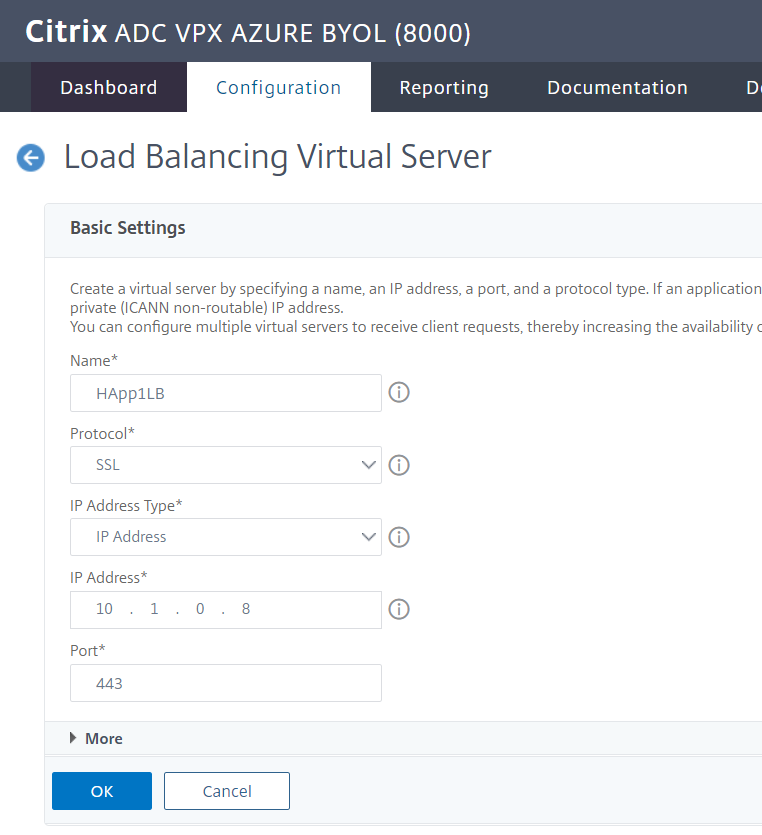


1. Specify the Details of the Web Server running the Applications
   1. Service Name
   2. Server IP/ Existing Server
   3. Protocol
   4. Port



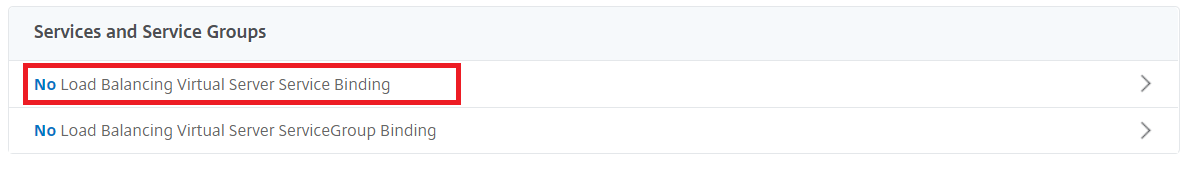
### Configure Load Balancer

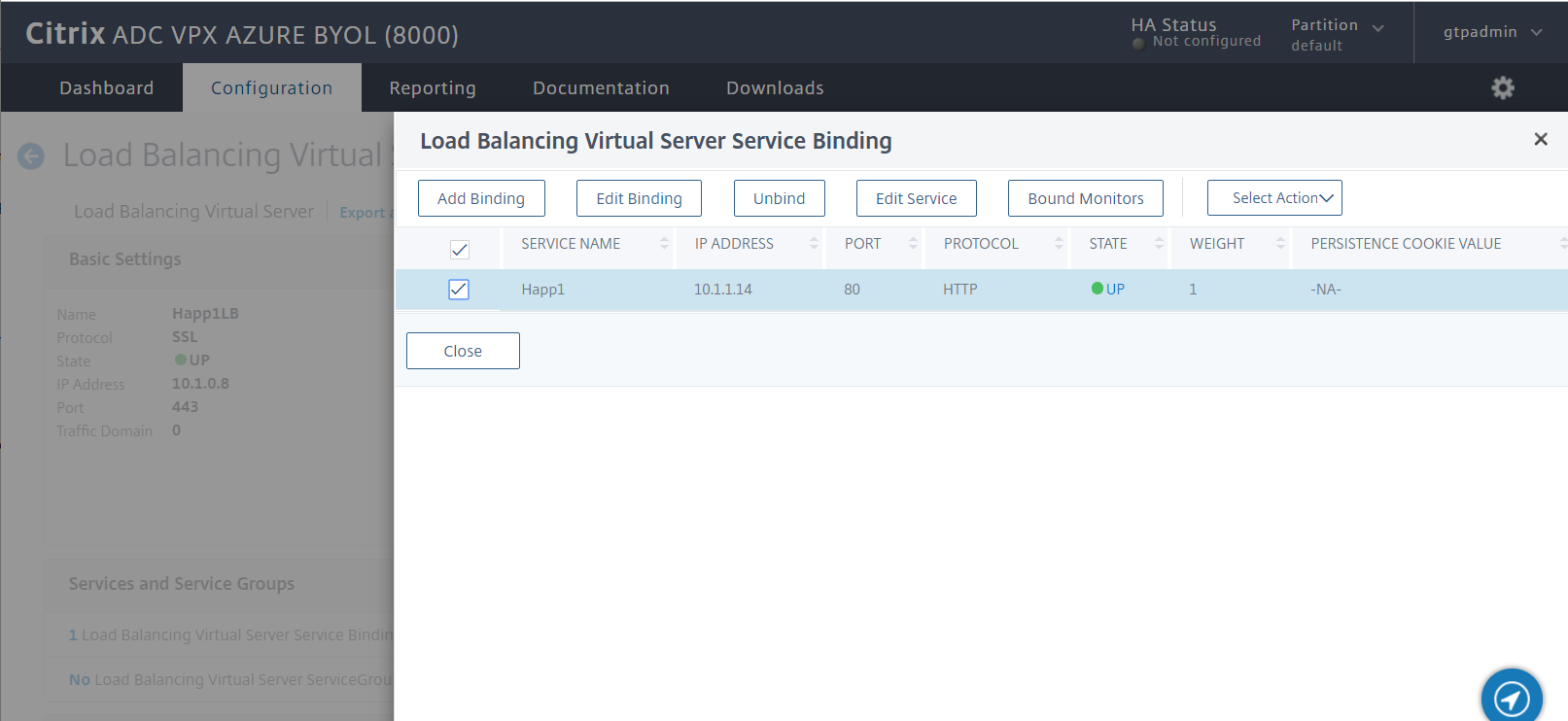
1. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers**
2. Click Add
3. Specify the below details
   1. Name
   2. Protocol
   3. IP Address
   4. Port
4. Click ok



### Bind Virtual Server

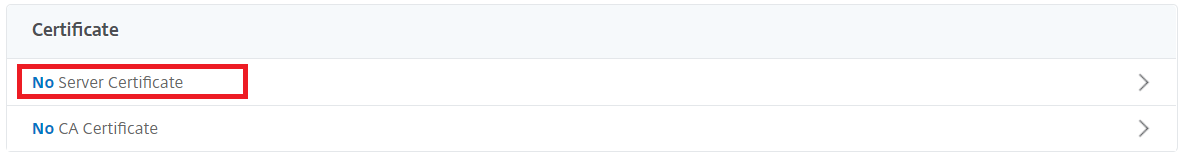
Bind the Load Balancer with the Virtual Server Created Previously

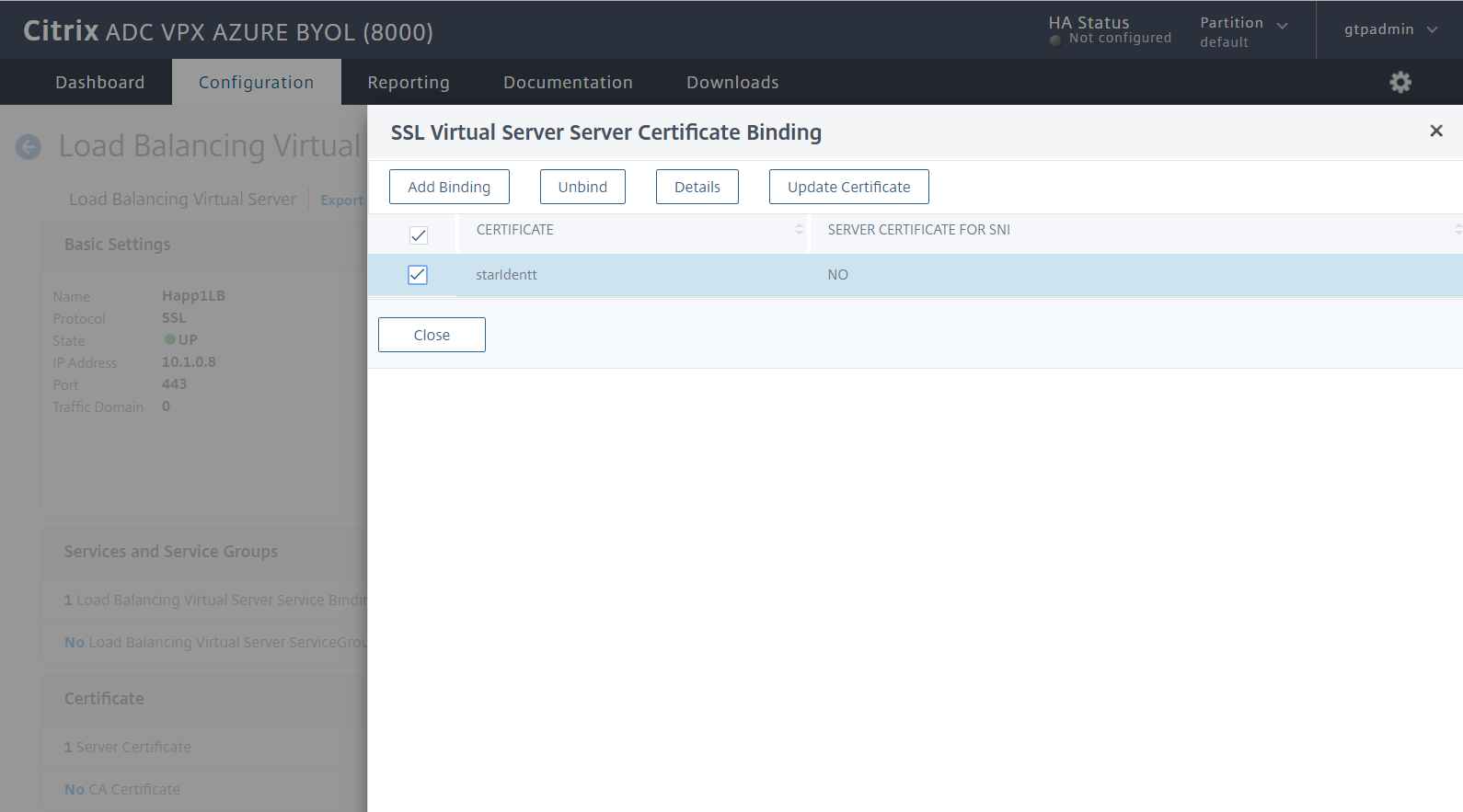




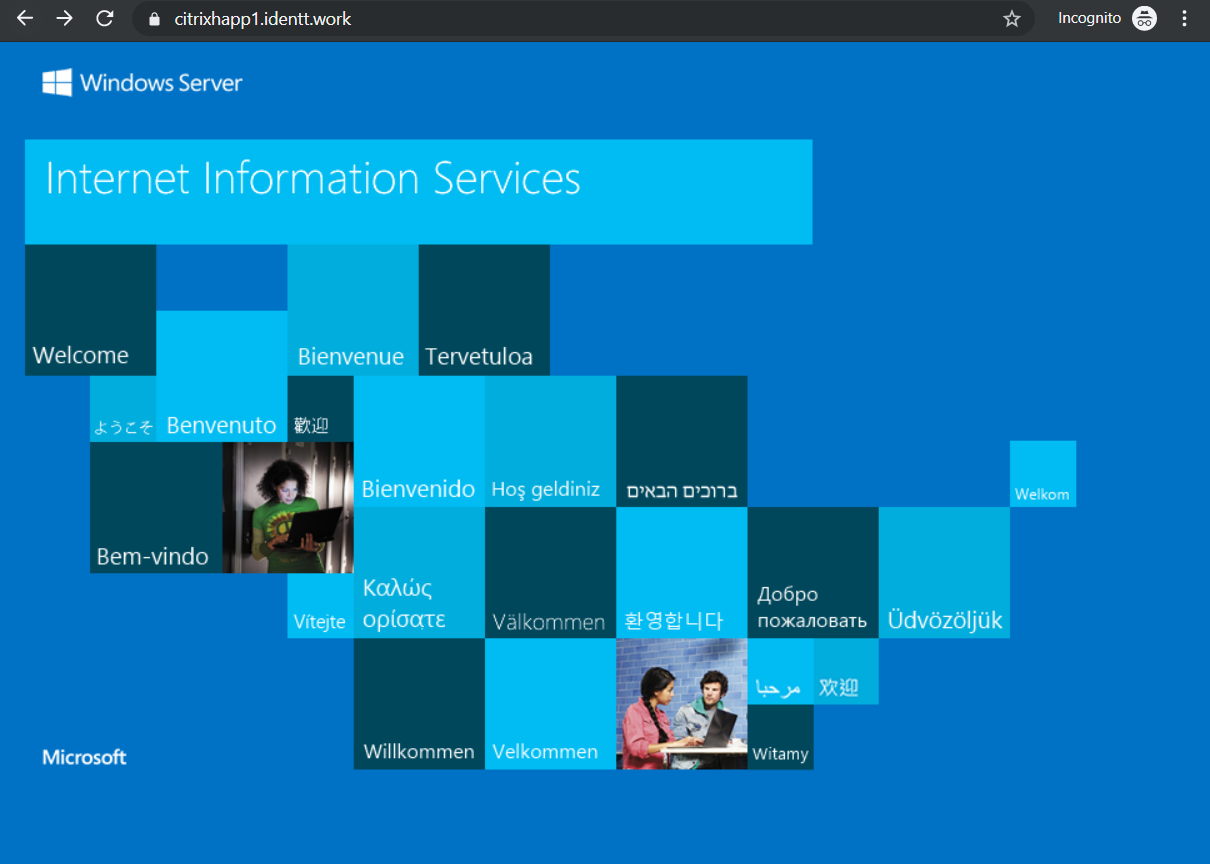
### Bind Certificate

Since we will be publishing this service as SSL bind the Server Certificate





Test Your Application



Note: We have the DNS Updated to use CitrixHapp1.identt.work

## Protecting Application with Azure AD

### Setting up Azure AD SAML SSO

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

Description automatically generated

Note: In the above example. the application is published as <https://citrixhapp1.identt.work> on the Citrix ADC

A screenshot of a cell phone

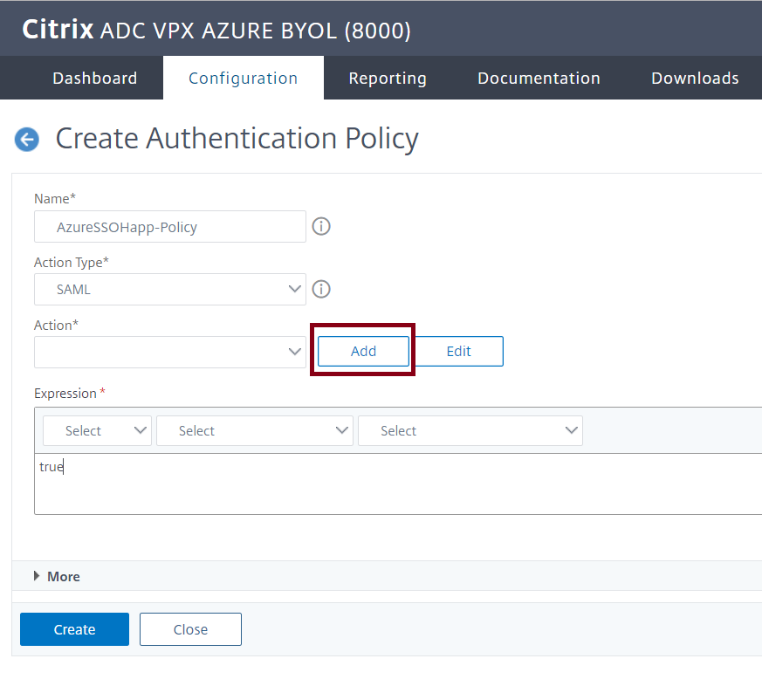
Description automatically generated

### Citrix ADC SAML Profile

### Create Authentication Policy

Go to **Security** > **AAA – Application Traffic** > **Policies** > **Authentication > Authentication Policies**

1. Click Add
2. Specify Details
   1. Name for the **Authentication Policy**
   2. Expression : **true**
   3. Action type **SAML**

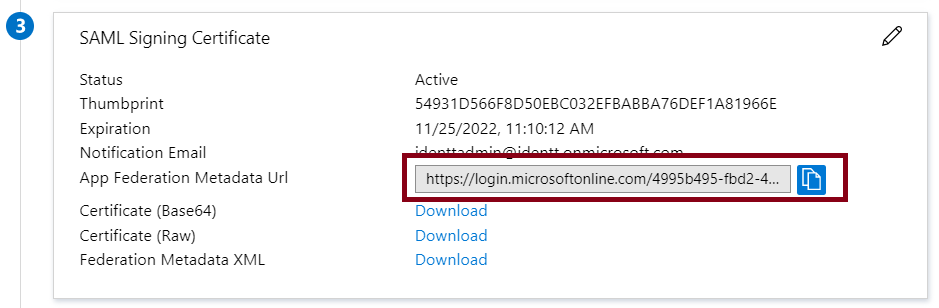
****

* 1. Action = Click Add (follow the Create Authentication SAML Server Wizard)
  2. Click Create on the **Authentication Policy**

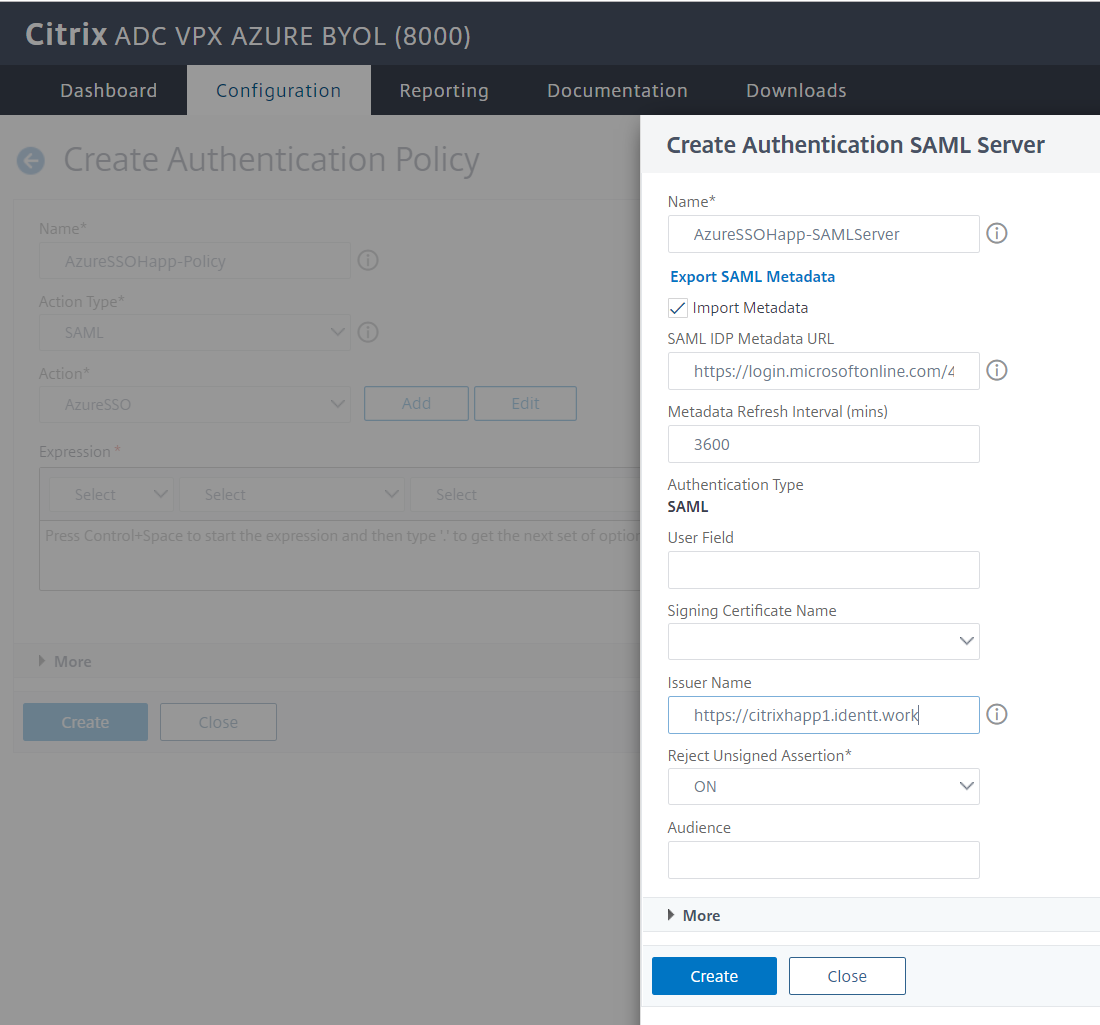
Create Authentication SAML Server

1. **Specify the Name**
2. **Import Metadata (specify the federation metadata URL from Azure SAML UI)**

**Reference below**

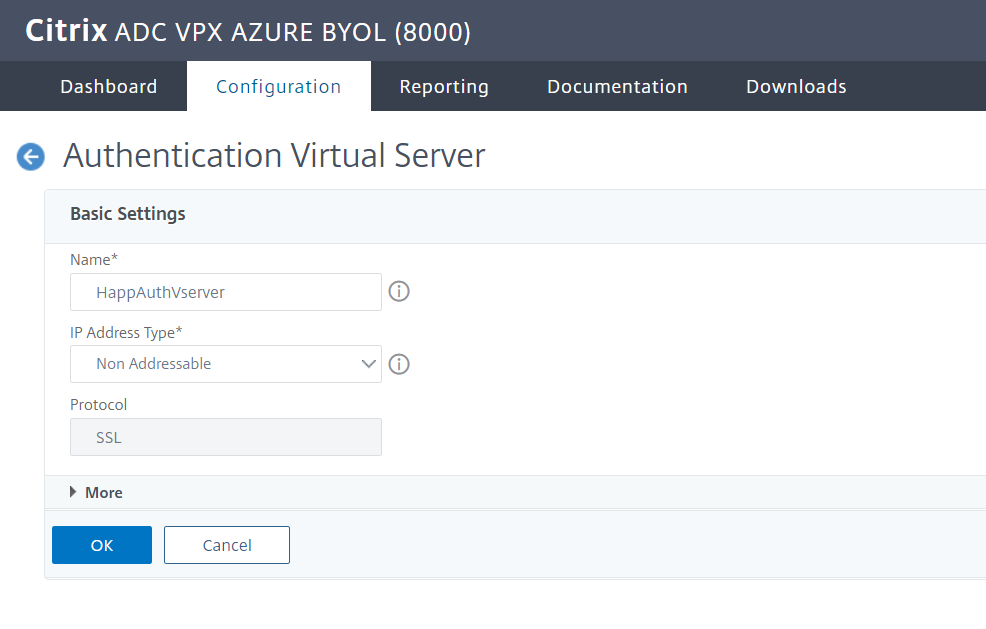
****

1. **Specify Issuer Name**
2. **Click create**



### Create Authentication Virtual Server

1. Goto **Security** > **AAA - Application Traffic** >> **Authentication Virtual Servers**
2. Click Add
   1. Provide a Name
   2. Choose Non-Addressable
   3. Protocol SSL

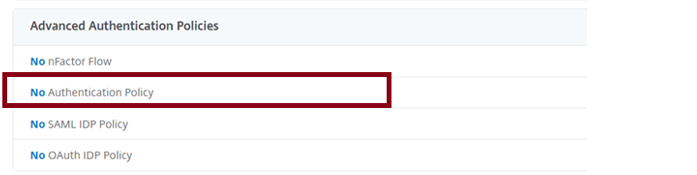


* 1. **Click OK**
  2. **Click Continue**

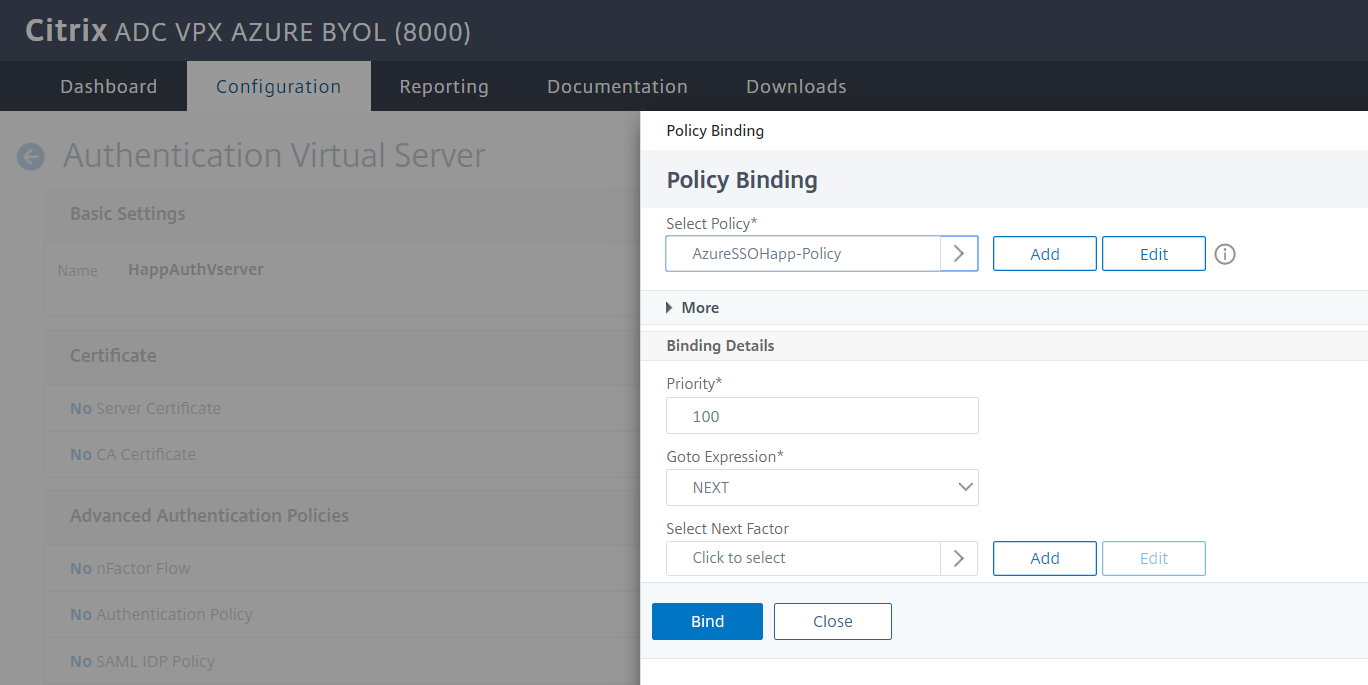
### Configure the Authentication Virtual Server to use Azure AD

You will need to modify the 2 sections of the Authentication Virtual Server

1. Advanced Authentication Policies



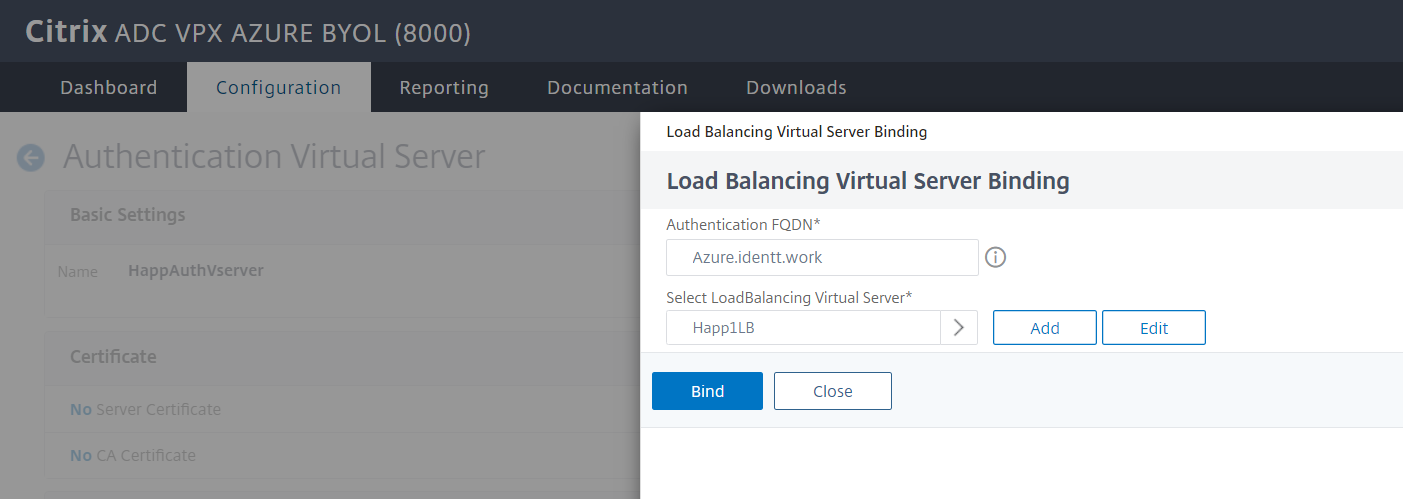
1. Select the Authentication Policy that you created previously
2. Click Bind



1. Form Based Virtual Servers



1. You will need to Provide an FQDN since its enforced by UI.
2. Choose the Virtual Server Load Balancer that you would like to protect with Azure AD Authentication
3. Click Bind

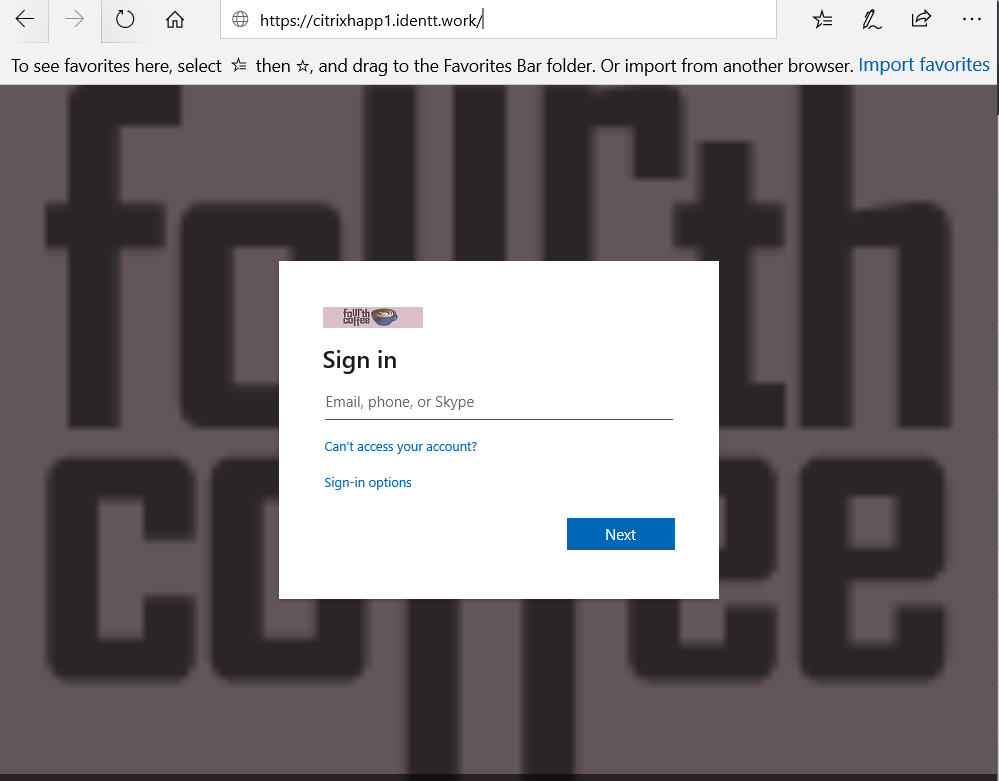


Note : Ensure you click Done on the Authentication Virtual Server Configuration page as well

Verify the changes

Browse to the application URL

You should see your tenanted login page instead of unauthenticated access previously.



## Configuring Kerberos Based Authentication

### Create a Kerberos Delegation Account for Citrix ADC

1. Create a user Account ( in this example AppDelegation )

A screenshot of a cell phone

Description automatically generated

1. Set up a HOST SPN on this accounts

setspn -S HOST/AppDelegation.IDENTT.WORK identt\appdelegation

**Note: In the example above**

1. Identt.work ( Domain FQDN )
2. Identt ( Domain Netbios Name)
3. AppDelegation ( delegation user account Name)
4. Configure Delegation for the WebServer

A screenshot of a cell phone

Description automatically generated

Note : In the example above the Internal Webserver name running WIA Site is cweb2

### Citrix AAA KCD ( Kerberos Delegation Accounts)

1. Go to Citrix Gateway > AAA KCD (Kerberos Constrained Delegation) Accounts
2. Click Add
   1. Specify Name
   2. Realm
   3. Service SPN **http/<host/fqdn>@DOMAIN.COM** \* note @DOMAIN.com is **mandatory** and in uppercase.
   4. Specify Delegated user account
   5. Check the Password for the Delegated user and Specify Password
   6. Click OK

A screenshot of a cell phone

Description automatically generated

### Citrix Traffic Policy and Traffic Profile

1. Goto Security > AAA - Application Traffic > Policies > Traffic Policies, Profiles and Form SSO ProfilesTraffic Policies
2. Select **Traffic Profiles**
3. Click Add
4. Configure Traffic Profile
   1. Specify **Name**
   2. Specify **Single Sign-on**
   3. Specify the **KCD Account** created in previously step from drop down
   4. Click OK

A screenshot of a cell phone

Description automatically generated

1. Select **Traffic Policy**
2. Click Add
3. Configure Traffic Policy
   1. Specify Name
   2. Choose the previously created **Traffic Profile** from the drop down
   3. Set expression to true
   4. Click Ok

A screenshot of a cell phone

Description automatically generated

### Citrix Bind Traffic Policy to Virtual Servers

To bind a Traffic policy to a specific virtual server by using the GUI

* Navigate to Traffic Management > Load Balancing > Virtual Servers.
* In the details pane list of virtual servers, select the virtual server to which you want to bind the rewrite policy, and then click Open.
* In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab. All policies configured on your NetScaler appear on the list.

A screenshot of a cell phone screen with text

Description automatically generated

A close up of a logo

Description automatically generated

1. Select the check box next to the name of the policy you want to bind to this virtual server.

A screenshot of a cell phone

Description automatically generated

A screenshot of a cell phone

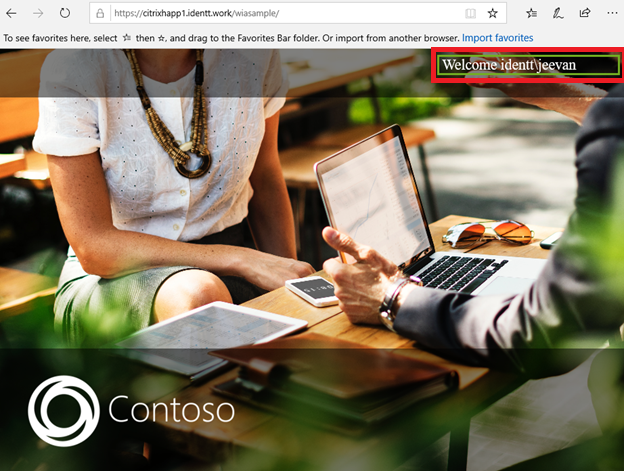
Description automatically generated

Only the policy is bound , Click Done

A close up of a logo

Description automatically generated

Test using the Windows Integrated Website.

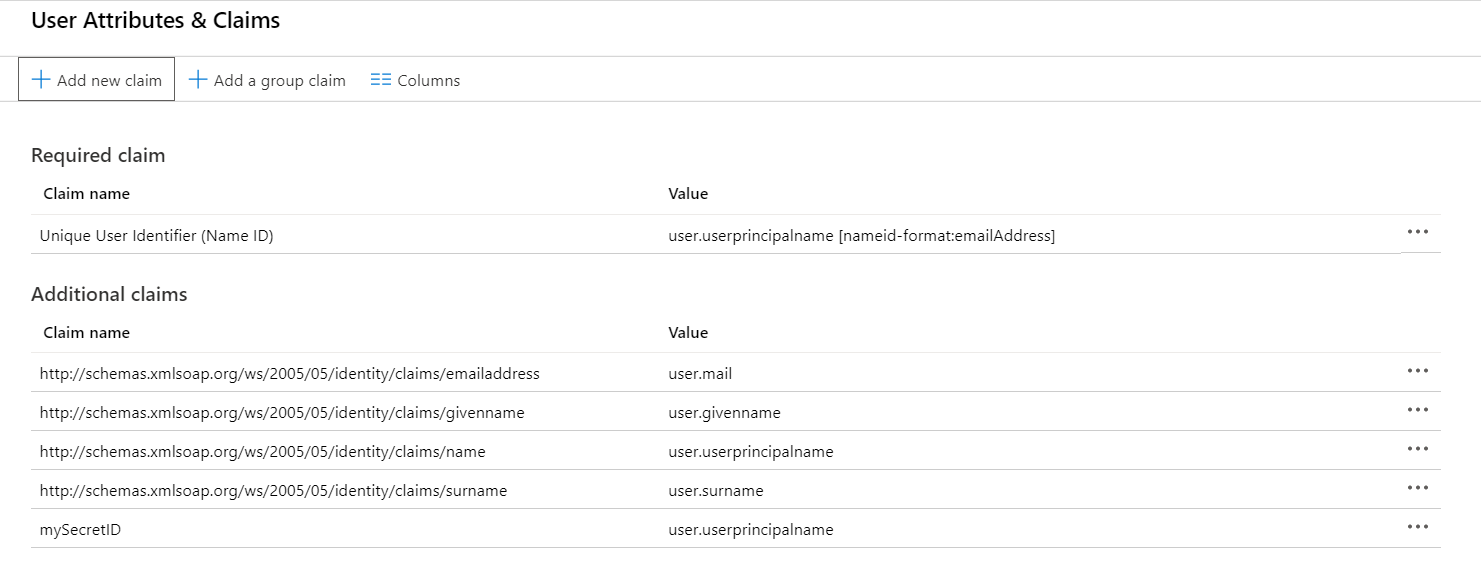


## Configuring Header Based Authentication

### Azure AD Claims Mapping

1. In the Azure AD SAML Claim Mapping ensure the claim Name is mapped correctly.

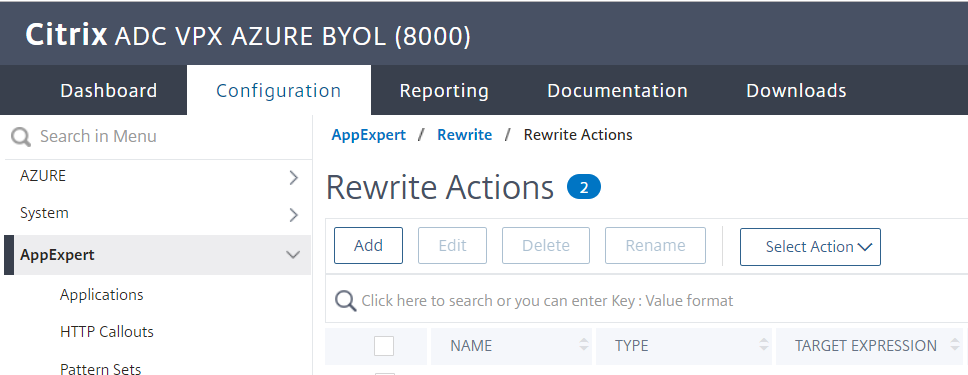
In this case we will use the **mySecretID** as claim and map it to the header for applications access.



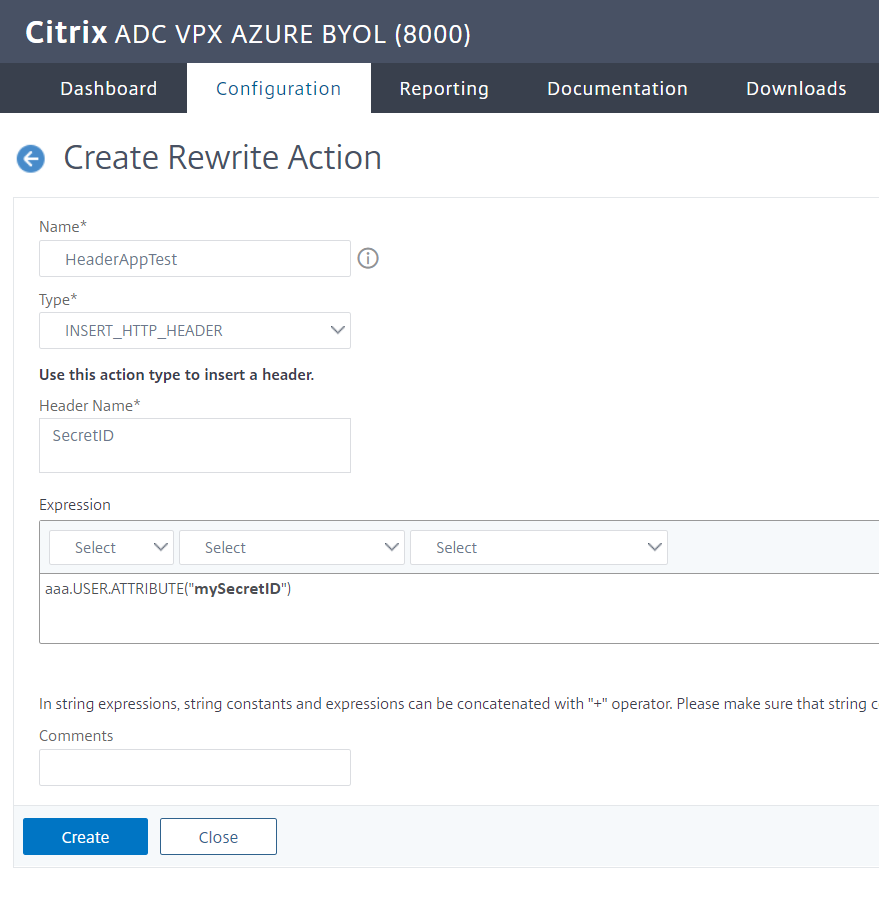
### Citrix ADC Configuration

### Create an Rewrite Action

1. Go to AppExpert > Rewrite > Rewrite Actions

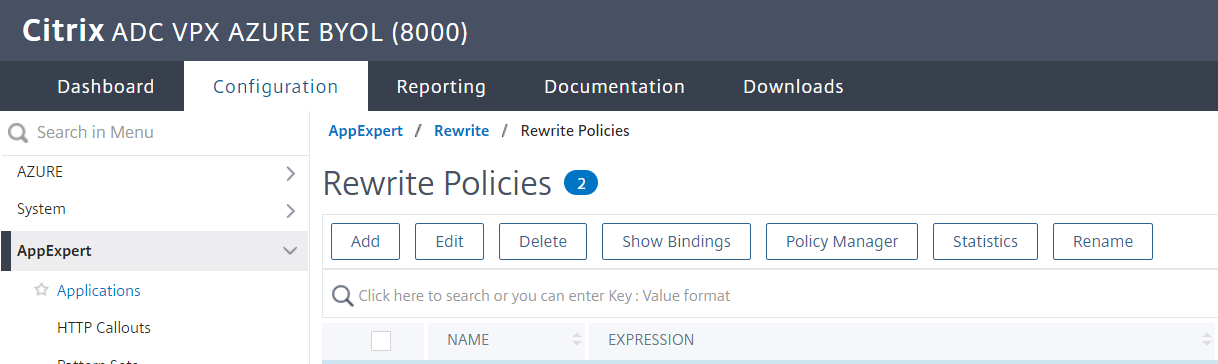


1. Click Add
   1. Specify Name
   2. Type = INSERT\_HTTP\_HEADER
   3. Specify the HEADER NAME\* ( SecretID in this example )
   4. Specify the expression aaa.USER.ATTRIBUTE("**mySecretID**")
      1. Where **mySecretID** is the Azure AD SAML Claim sent to Citrix ADC
   5. Click Create

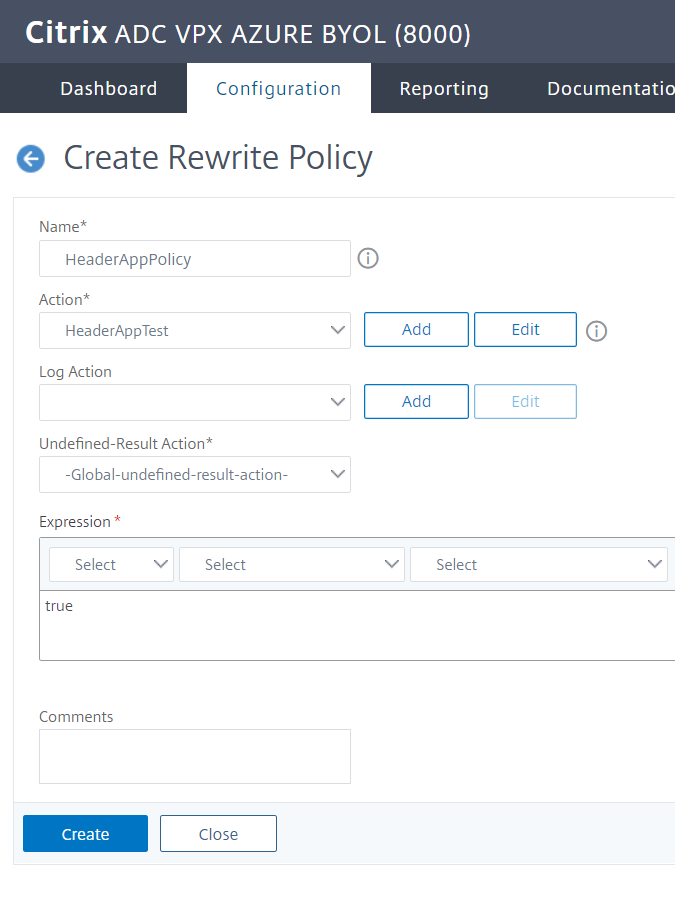


### Create a Rewrite Policy.

1. Go to AppExpert > Rewrite > Rewrite Policies



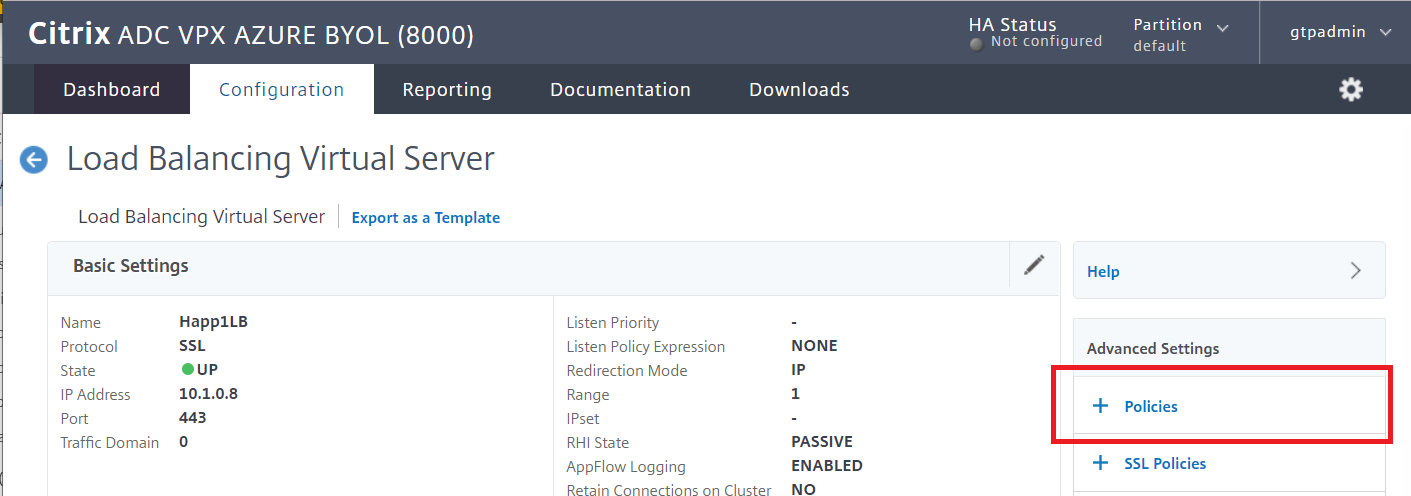
1. Click Add
   1. Specify the Name
   2. Choose the action created previously
   3. Expression specify **true**
   4. **Click create**

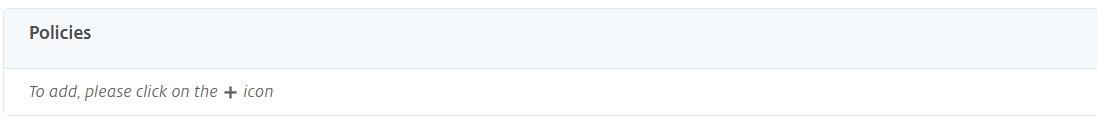


### Bind Rewrite Policy to Virtual Servers

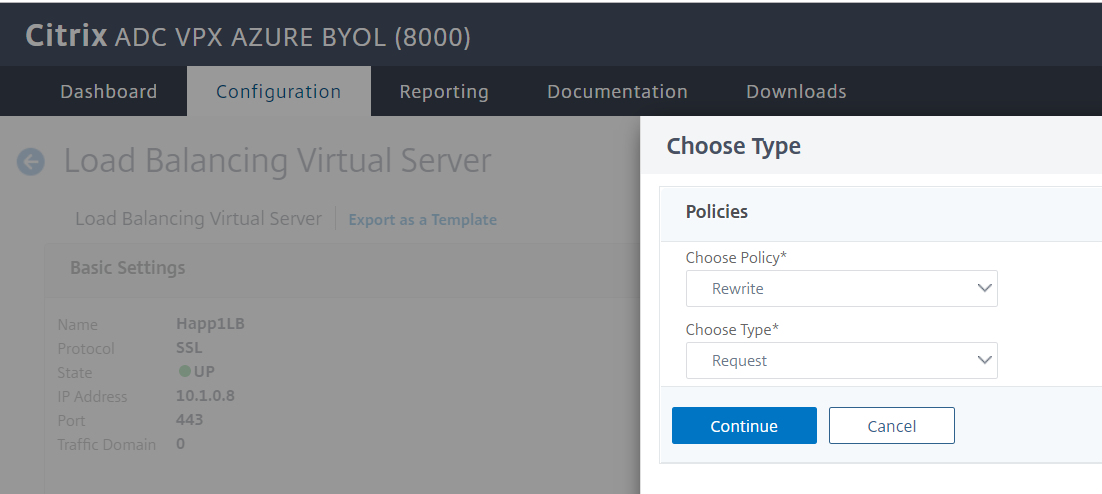
To bind a rewrite policy to a specific virtual server by using the GUI

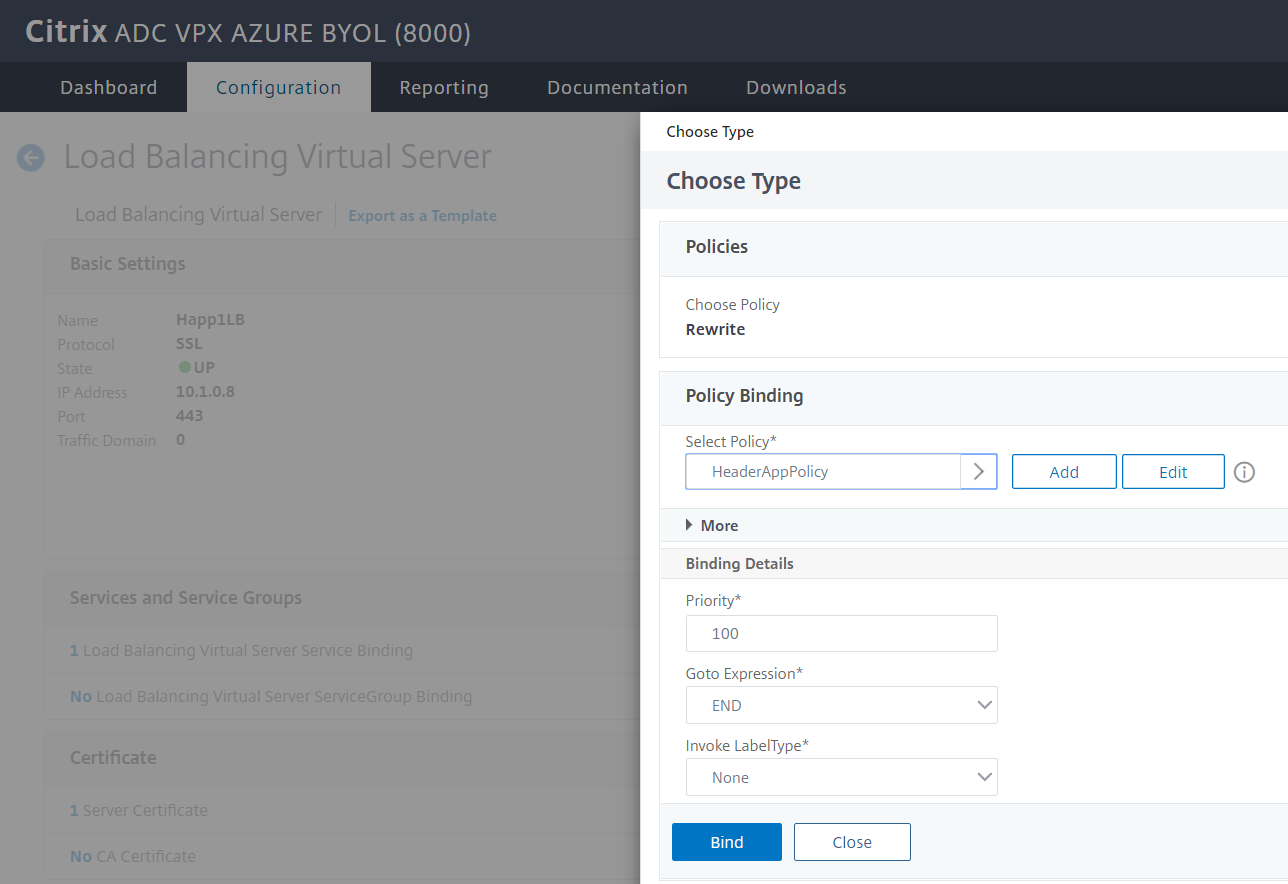
1. Navigate to Traffic Management > Load Balancing > Virtual Servers.
2. In the details pane list of virtual servers, select the virtual server to which you want to bind the rewrite policy, and then click Open.
3. In the Configure Virtual Server (Load Balancing) dialog box, select the Policies tab. All policies configured on your NetScaler appear on the list.





1. Select the check box next to the name of the policy you want to bind to this virtual server.

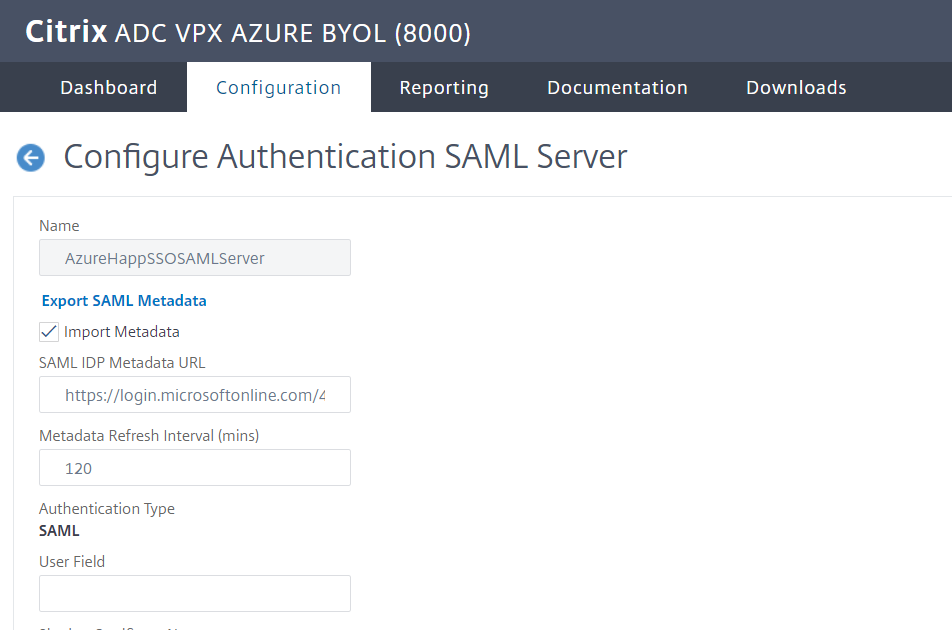




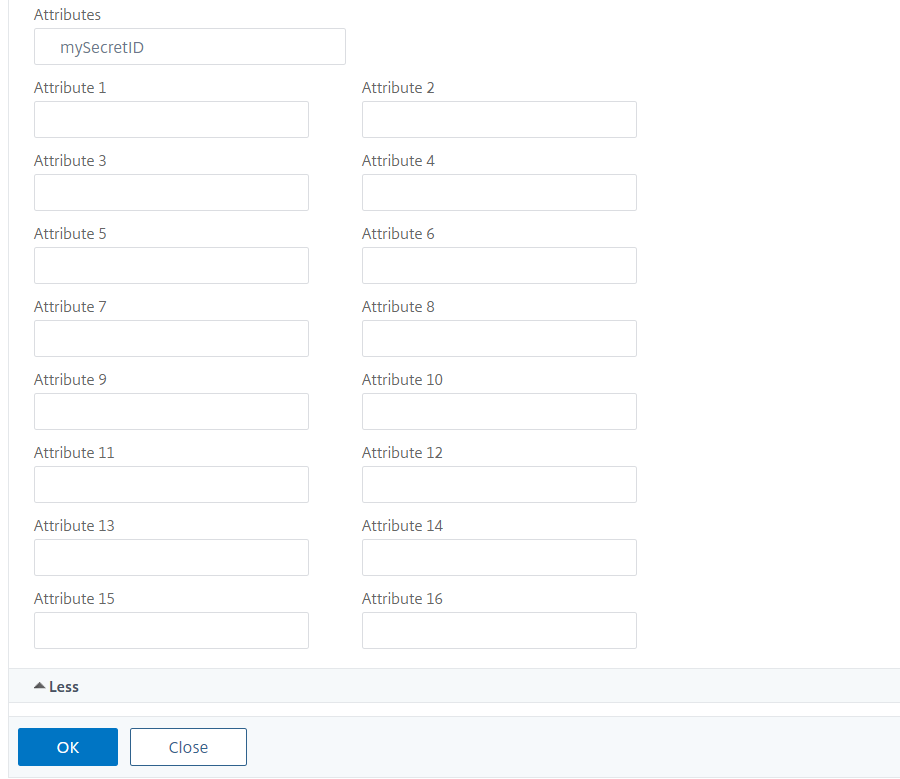
1. Click OK. A message appears in the status bar, stating that the Policy has been configured successfully.

### Modify SAML Server to Extract Attributes from Claim

1. Goto Security > AAA - Application Traffic >Policies > Authentication > Advanced Policies > Actions > Servers
2. Select the Appropriate Authentication SAML Server for the Application



Under the Attribute section type SAML Attributes that you want to extract using “ , “. In the case we specify the attribute called **mySecretID**



Verify my accessing the Applications

