Contents

[Publishing Web Server 1](#_Toc25641784)

[Create a Virtual Server 1](#_Toc25641785)

[Configure Load Balancer 2](#_Toc25641786)

[Bind Virtual Server 3](#_Toc25641787)

[Bind Certificate 4](#_Toc25641788)

[Protecting Application with Azure AD 6](#_Toc25641789)

[Setting up Azure AD SAML SSO 6](#_Toc25641790)

[Citrix ADC SAML Profile 9](#_Toc25641791)

[Create Authentication Policy 9](#_Toc25641792)

[Create Authentication Virtual Server 10](#_Toc25641793)

[Configure the Authentication Virtual Server to use Azure AD 11](#_Toc25641794)

[Configuring Kerberos Based Authentication 13](#_Toc25641795)

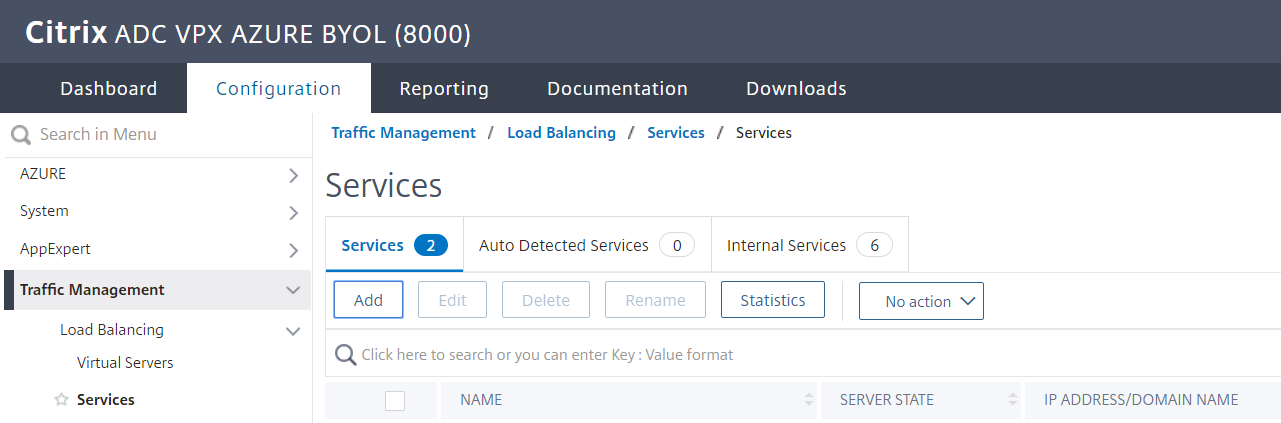
[Configuring Header Based Authentication 13](#_Toc25641796)

[Configuring LDAP Lookup 13](#_Toc25641797)

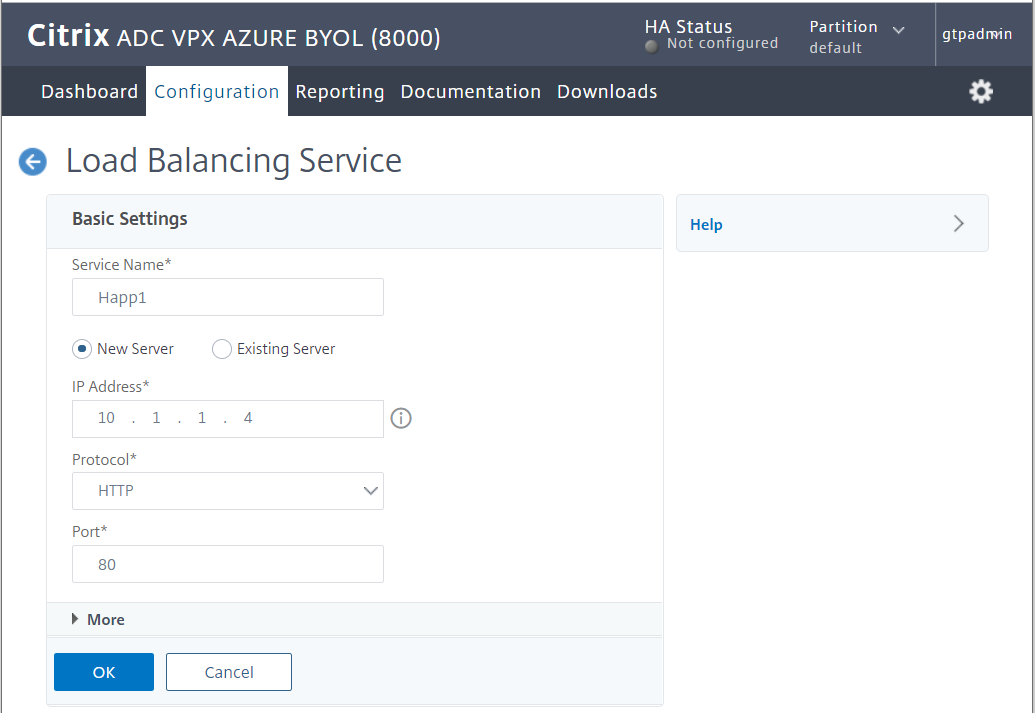
## Publishing Web Server

### Create a Virtual Server

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

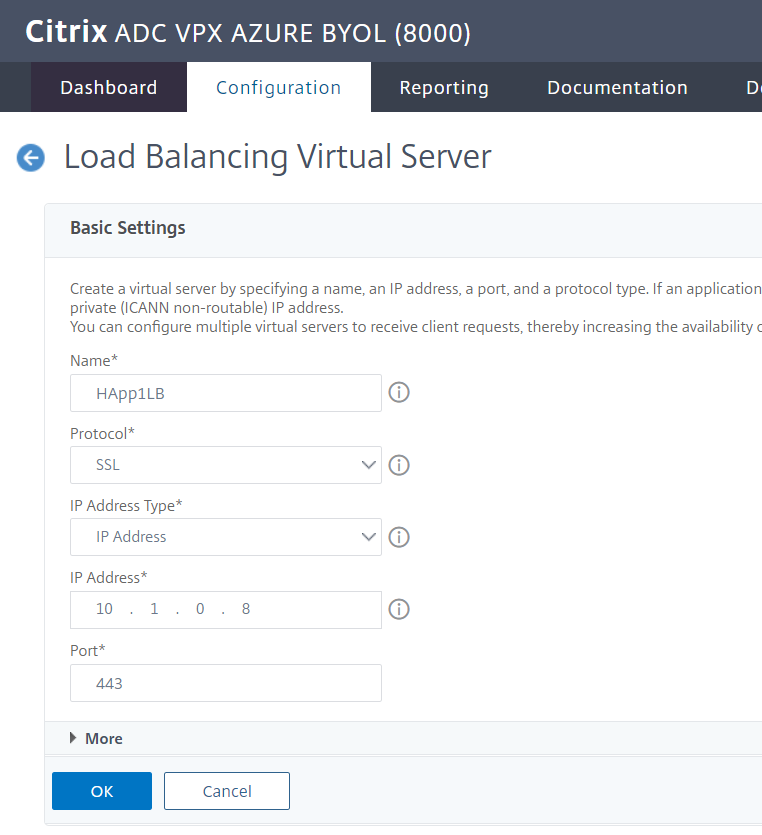


1. Specify the Details of the Web Server running the Applications
   1. Service Name
   2. Server IP/ Existing Server
   3. Protocol
   4. Port



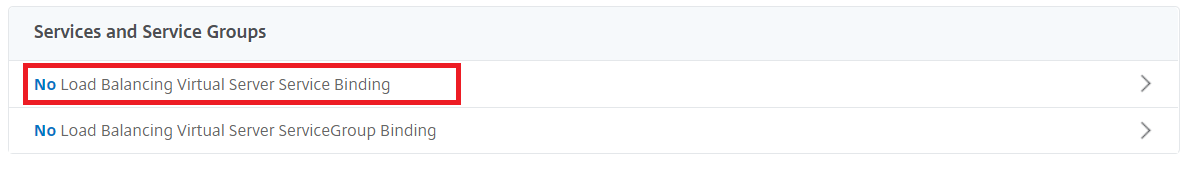
### Configure Load Balancer

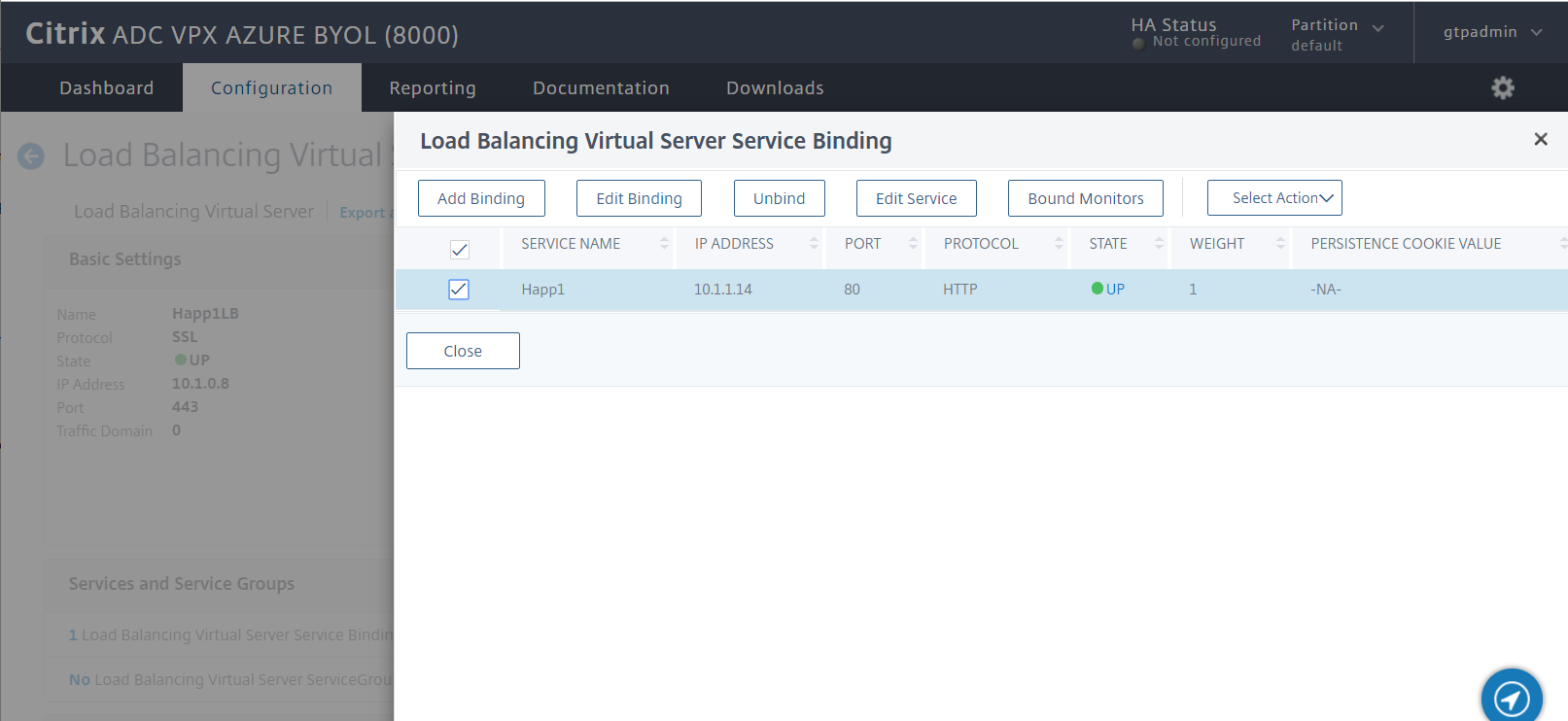
1. Go to **Traffic Management** > **Load Balancing** > **Virtual Servers**
2. Click Add
3. Specify the below details
   1. Name
   2. Protocol
   3. IP Address
   4. Port
4. Click ok



### Bind Virtual Server

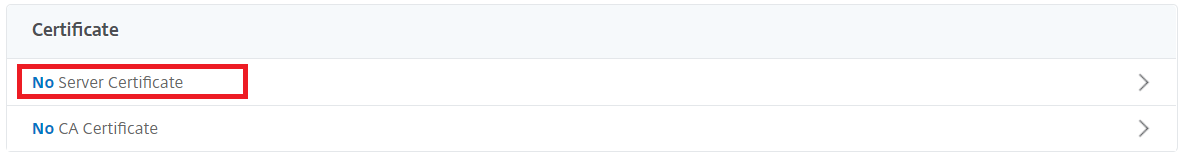
Bind the Load Balancer with the Virtual Server Created Previously

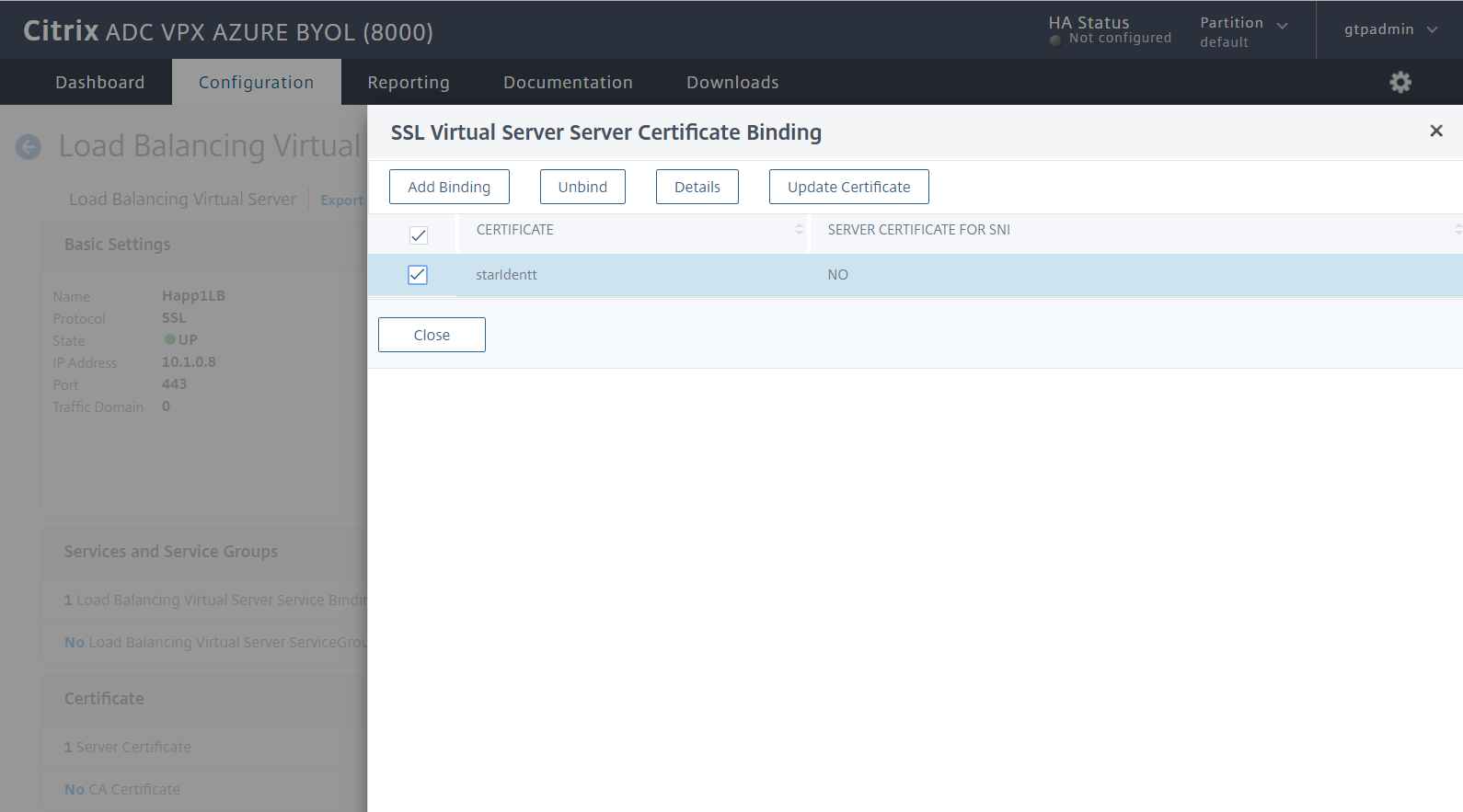




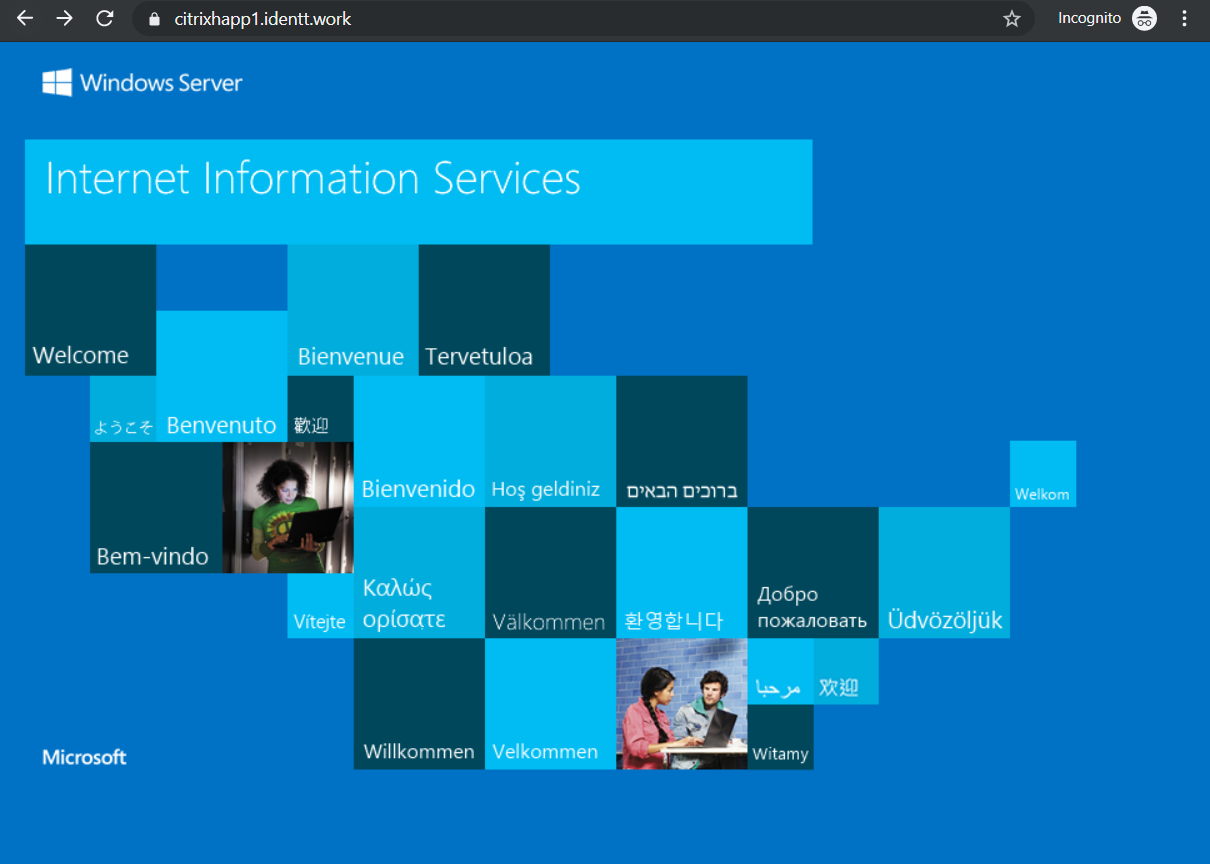
### Bind Certificate

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

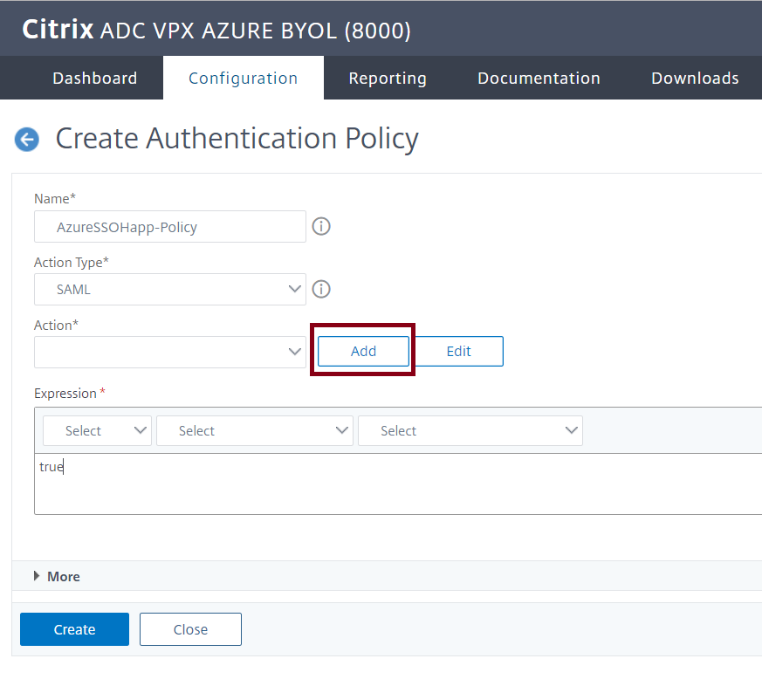
Description automatically generated

### 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**

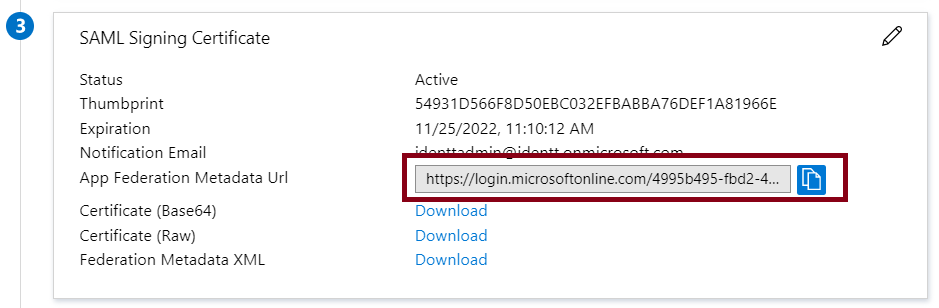
****

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

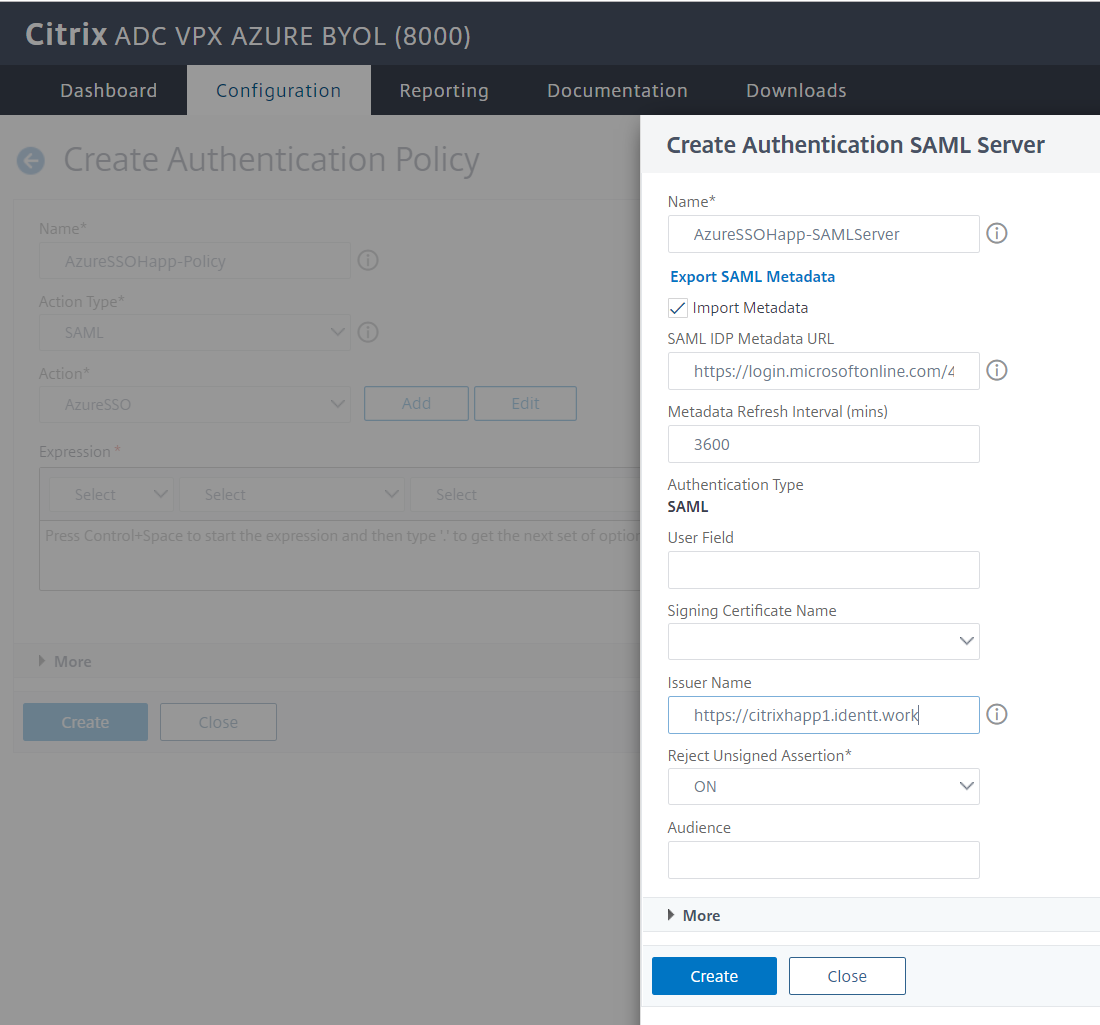
Create Authentication SAML Server

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

**Reference below**

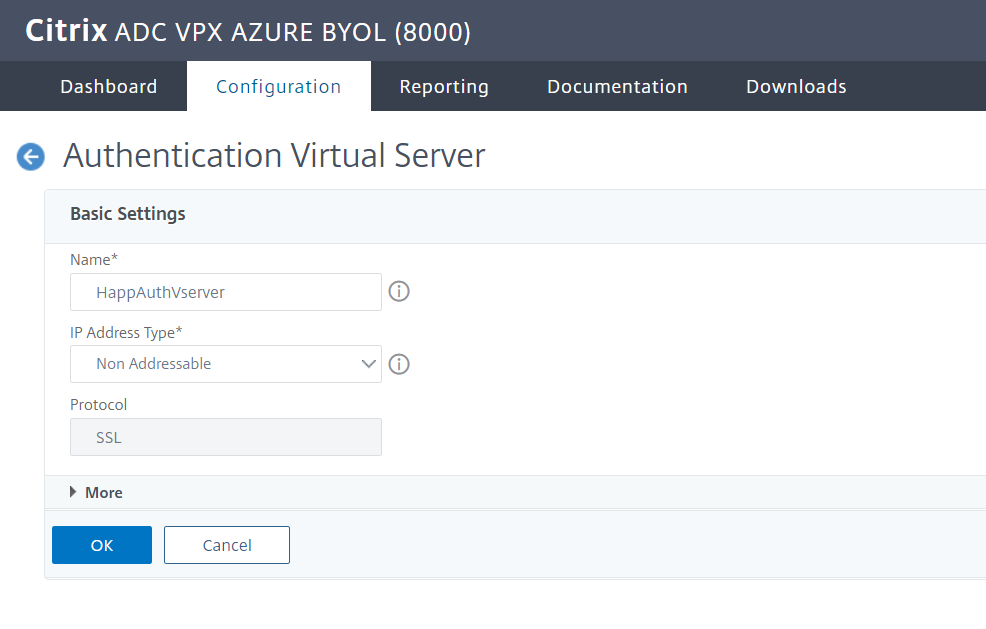
****

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

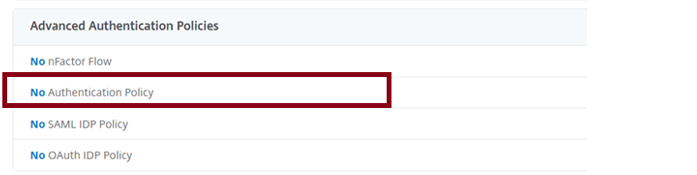


* 1. **Click OK**
  2. **Click Continue**

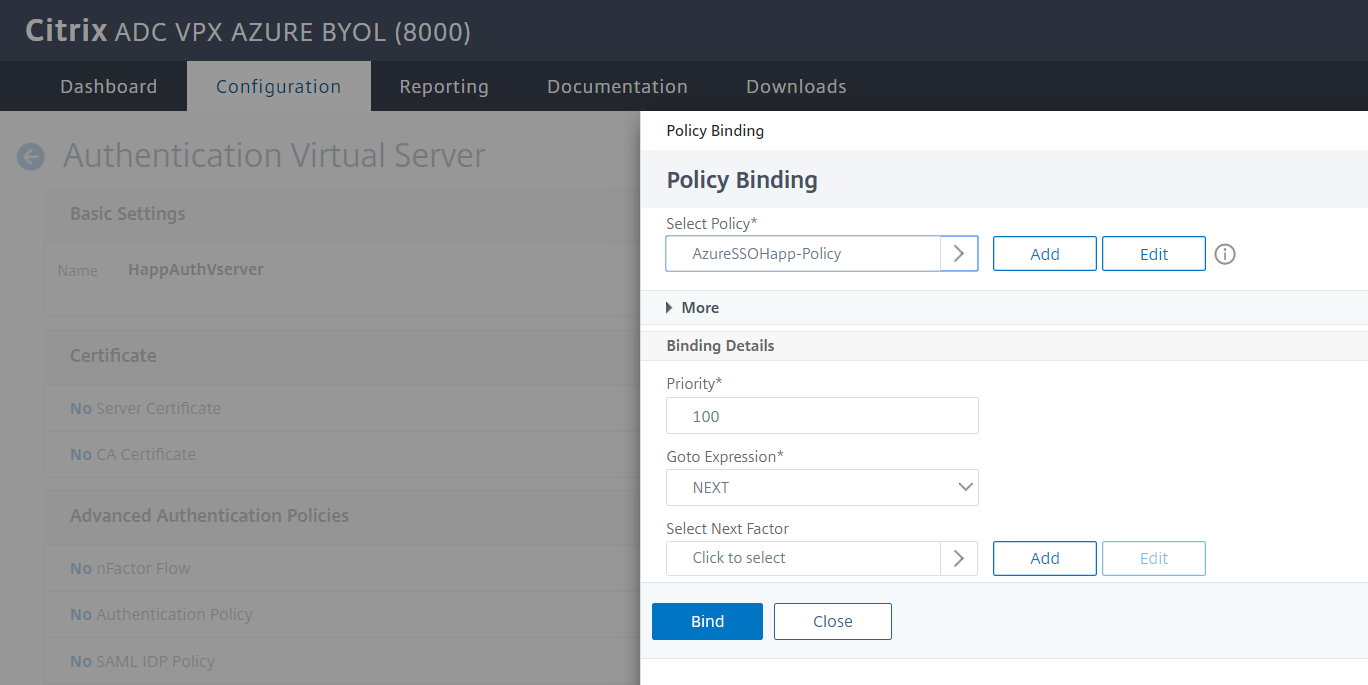
### Configure the Authentication Virtual Server to use Azure AD

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

1. Advanced Authentication Policies



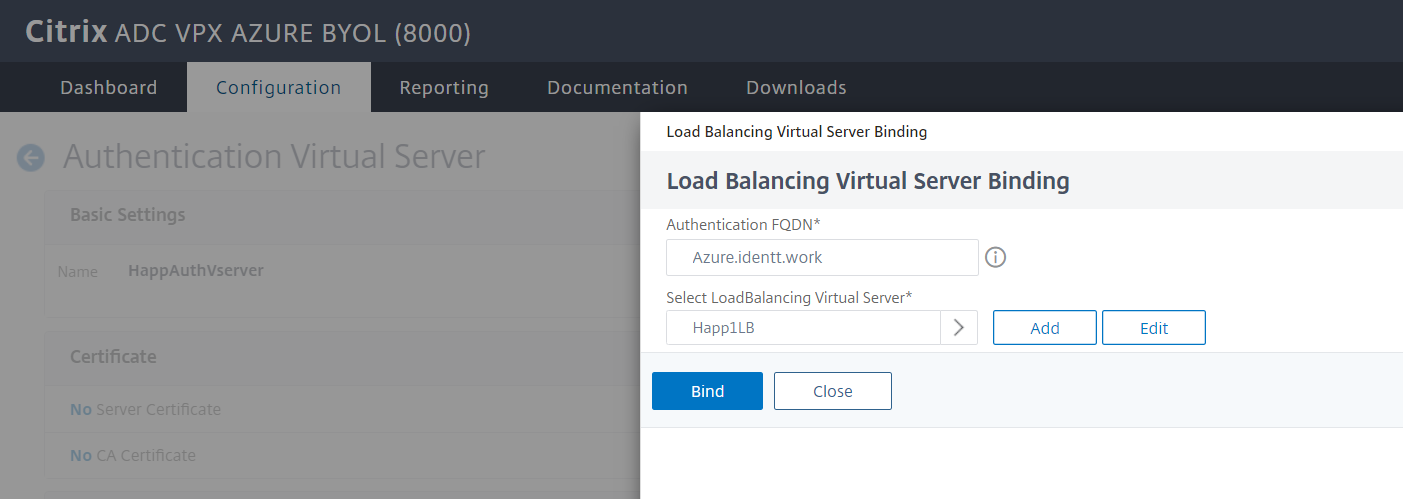
1. Select the Authentication Policy that you created previously
2. Click Bind



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

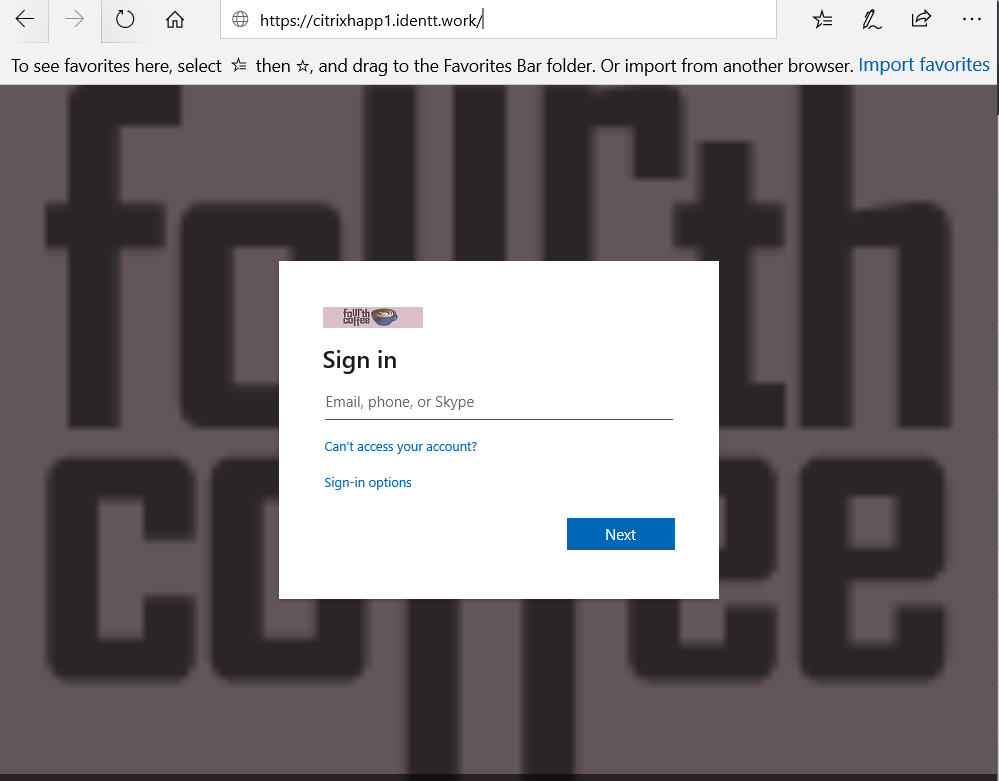


Note : Ensure you click Done on the Authentication Virtual Server Configuration page as well

Verify the changes

Browse to the application URL

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



## Configuring Kerberos Based Authentication

## Configuring Header Based Authentication

## Configuring LDAP Lookup