Citrix Systems, Inc.
NetScaler Gateway

RSA SecurID Ready Implementation Guide

Last Modified: October 28th, 2014

Partner Information

Product Information	
Partner Name	Citrix Systems, Inc.
Web Site	www.citrix.com
Product Name	NetScaler Gateway
Version & Platform	10.5
Product Description	Citrix NetScaler Gateway, formerly Access Gateway, is a secure application and data access solution that provides administrators granular application- and data-level control while empowering users with remote access from anywhere. It gives IT administrators a single point to manage access control and limit actions within sessions based on both user identity and the endpoint device, providing better application security, data protection, and compliance management.

Solution Summary

Citrix NetScaler Gateway can be configured to communicate with RSA Authentication Manager via RADIUS protocol. This integration allows RSA SecurID to be used to authenticate users accessing Citrix NetScaler Gateway-protected network resources.

Citrix NetScaler Gateway's web-based sign-in page can be customized to use RSA Risk-Based Authentication (RBA), which allows you to strengthen web-based access with step-up authentication for access attempts that are deemed high-risk by RSA Authentication Manager's risk engine.

! Important: Configuring NetScaler Gateway for RBA when combined with StoreFront or Web Interface requires that the user logon twice. The user must logon at the RSA Secure Logon page and then again at the Citrix Web Interface or StoreFront page. Refer to the Known Issues section of this document for more information.

RSA Authentication Manager supported features	
NetScaler Gateway 10.5	
RSA SecurID Authentication via Native RSA SecurID Protocol	No
RSA SecurID Authentication via RADIUS Protocol	Yes
On-Demand Authentication via Native SecurID Protocol	No
On-Demand Authentication via RADIUS Protocol	Yes
Risk-Based Authentication	Yes
RSA Authentication Manager Replica Support	Yes
Secondary RADIUS Server Support	Yes
RSA SecurID Software Token Automation	No
RSA SecurID SD800 Token Automation	No
RSA SecurID Protection of Administrative Interface	No

Agent Host Configuration

To facilitate communication between the NetScaler Gateway and the RSA Authentication Manager / RSA SecurID Appliance, an Agent Host record must be added to the RSA Authentication Manager database. The Agent Host record identifies the NetScaler Gateway and contains information about communication and encryption.

RSA Authentication Manager 8.0 introduced a new TCP-based authentication protocol and corresponding agent API. RSA Authentication Manager 8.0 and newer also maintains support for the existing UDP-based authentication protocol and agents. The agent host records for TCP and UDP agents are configured similarly, but there are some important differences.

Include the following information when configuring a UDP-based agent host record.

- Hostname
- IP addresses for network interfaces

> **Note: The UDP-based authentication agent's hostname must resolve to the IP address specified.**

Include the following information when configuring a TCP-based agent host record.

- RSA agent name (in the hostname field)

> **Note: The RSA agent name is specified in the rsa_api.properties file.**

Set the Agent Type to "Standard Agent" when adding the Authentication Agent. This setting is used by the RSA Authentication Manager to determine how communication with NetScaler Gateway will occur.

Citrix NetScaler Gateway will be communicating with RSA Authentication Manager via RADIUS, so a RADIUS client that corresponds to the agent host record must be created in the RSA Authentication Manager. RADIUS clients are managed using the RSA Security Console.

The following information is required to create a RADIUS client:

- Hostname
- IP Addresses for network interfaces
- RADIUS Secret

> **Note: The RADIUS client's hostname must resolve to the IP address specified.**

Please refer to the appropriate RSA documentation for additional information about creating, modifying and managing Authentication Agents and RADIUS clients.

Risk-Based Authentication Integration Script

To protect a web-based application with Risk-Based Authentication (RBA), you must generate an integration script using the RSA Security Console, and deploy it to the applications default logon page. The script redirects the user from the web-based application's default logon page to a customized logon page that allows RSA Authentication Manager to authenticate the user with RBA.

The following steps should be taken prior to generating the integration script.

- Download the integration script template for the NetScaler Gateway from the following link: **https://sftp.rsa.com/human.aspx?Username=partner&password=rsasecured&arg01=920284651&arg12=downloaddirect&transaction=signon&quiet=true**
- Verify that the most recent RBA integration script template is installed on your Authentication Manager system by comparing the header of the installed integration script template to the header of the downloaded integration script template.
- Install the downloaded integration script template if it is newer than the installed script template, or if the script template for your agent is not installed.

Please refer to the “Install the RBA Integration Script Template” section from the RSA Authentication Manager Administrator’s Guide for more information.

Partner Product Configuration

Before You Begin

This section provides instructions for configuring the Citrix NetScaler Gateway with RSA SecurID Authentication. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Citrix NetScaler Gateway components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Integration Summary

Configure NetScaler Gateway Virtual Server for RSA SecurID

- Configure the Primary Authentication Policy
  or
- Configure the Secondary Authentication Policy

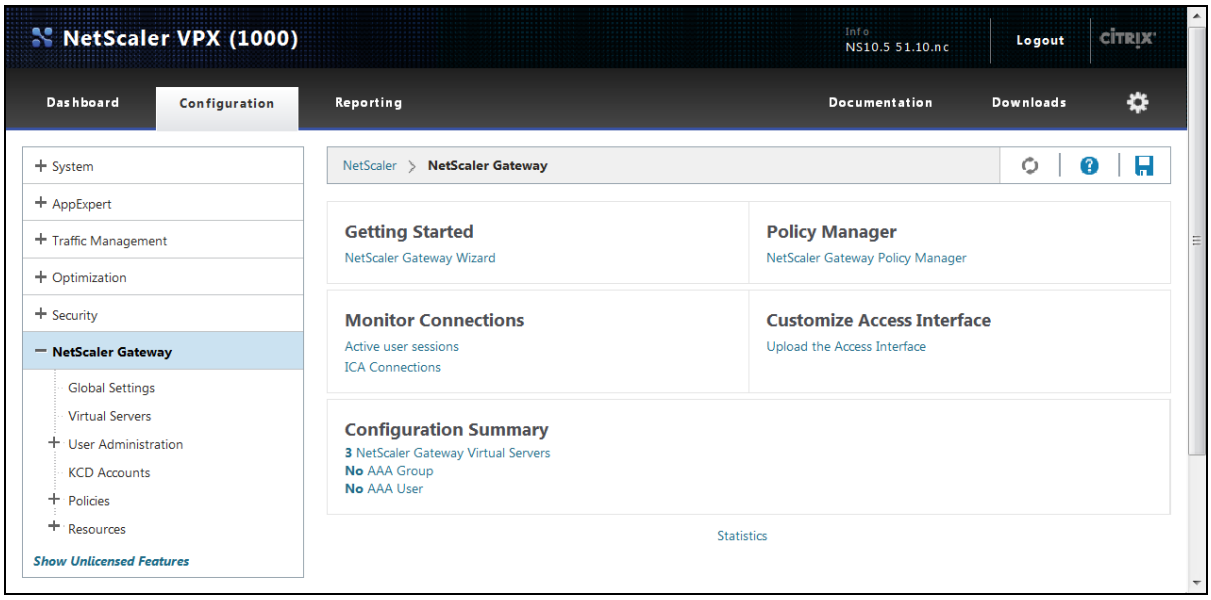
Configure NetScaler Gateway Virtual Server for Risk-Based Authentication

- Configure the Authentication Policy
- Integrate the RBA Script
- Configure the Responder

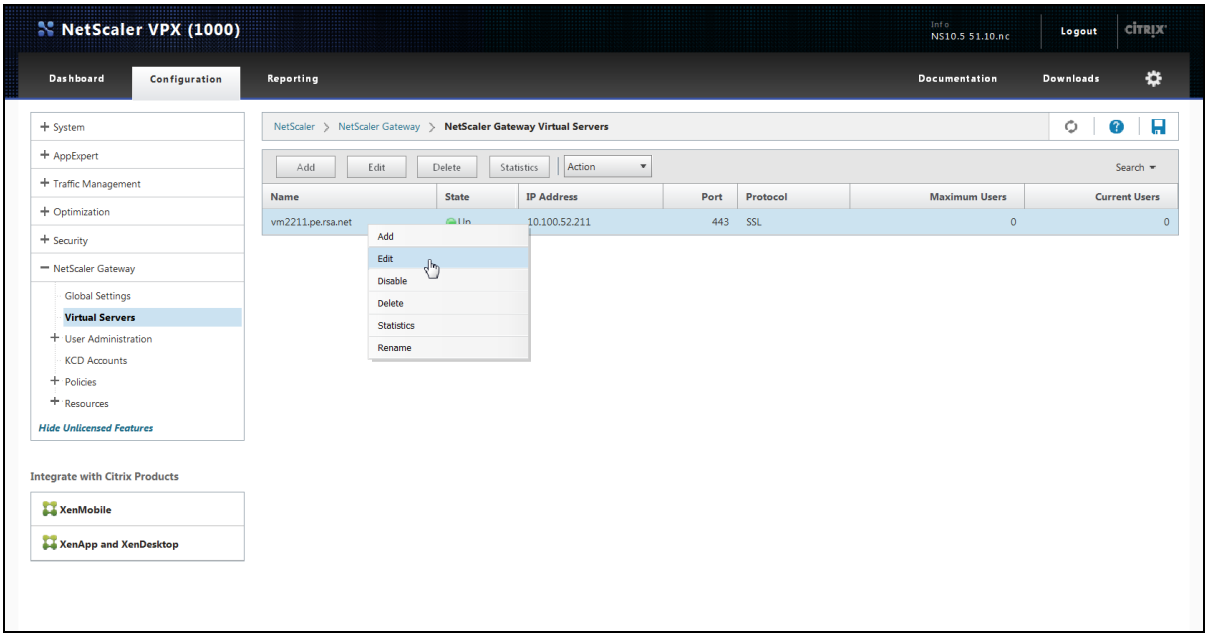
Important: In order to enable RBA for individual virtual servers, the NetScaler Gateway must be licensed for the Responder feature, and this feature must be enabled. Refer to CTX123736 for more details.

Configure NetScaler Gateway Virtual Server for RSA SecurID

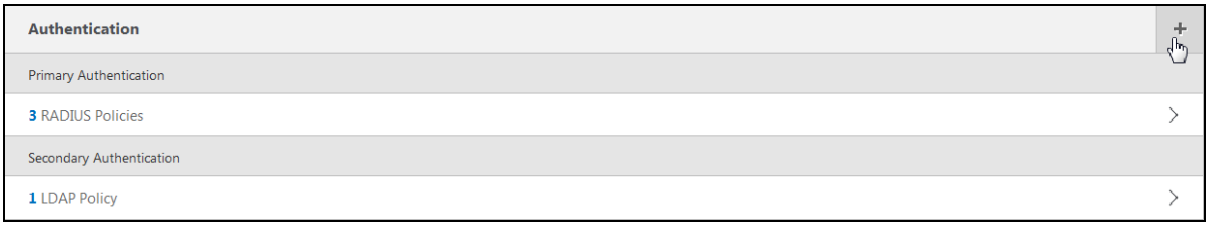
1. Logon to the NetScaler Gateway administrative Web page.



2. Browse to **Configuration** > **NetScaler Gateway** > **Virtual Servers**. Select the Virtual Server for which you are configuring RSA SecurID and click **Edit**.

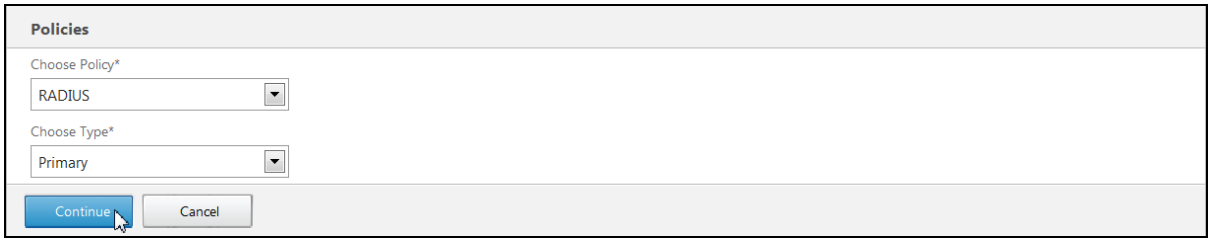


3. Browse down to the **Authentication** tab, and click the "**+**" icon to add a new authentication policy.



4. Select **RADIUS** from the **Choose Policy** drop-down, either **Primary** or **Secondary** from the **Choose Type** drop-down menu and click **Continue**.

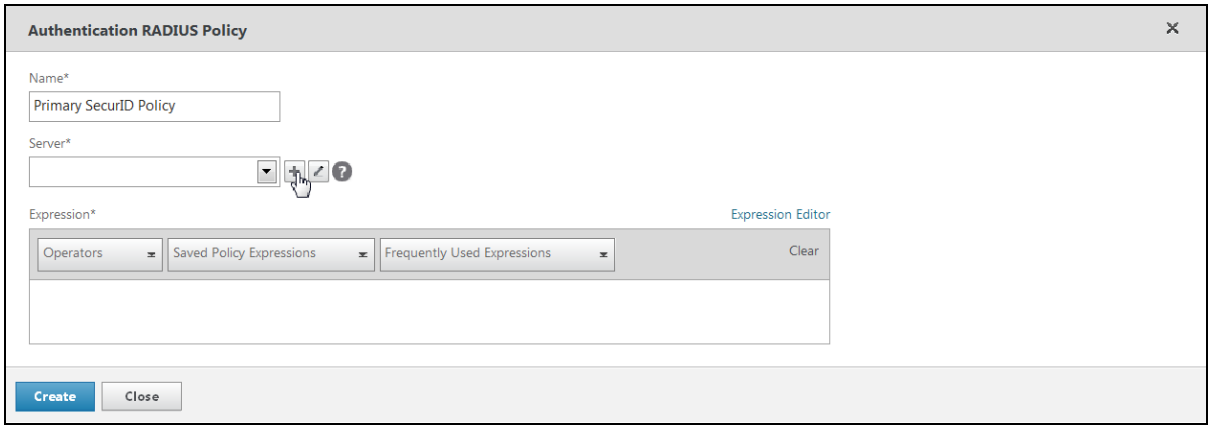
> **Important: Different Citrix deployments have different authentication policy requirements. For example: Deployments using Citrix Receiver require that RSA SecurID is Primary and Active Directory is Secondary. Refer to Citrix documentation for more information on authentication policies.**



5. Click **Bind**.

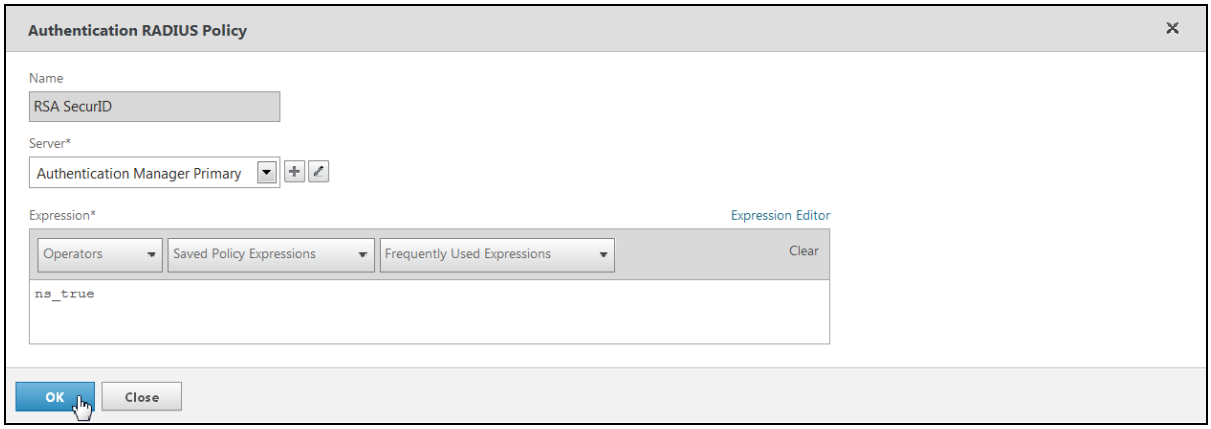
6. Click **Add**.

7. Enter the RADIUS Policy **Name** and then click "**+**" to add **Server**.



8. Enter RADIUS Server **Name**, **Server IP** or **Server Name**, **Port**, **Secret Key** and click **Create**.

9. Enter **ns_true** in the **Expression** text field and click **OK**.



10. Click **Done** to complete the configuration.

The NetScaler Gateway virtual server is now configured for RSA SecurID authentication.

Configure NetScaler Gateway Virtual Server for Risk-Based Authentication

To configure a NetScaler Gateway Virtual Server for Risk-Based Authentication, you must first configure your authentication policy for SecurID, and then integrate the RBA script downloaded from the RSA Security Console.

> **Important: Once a Virtual Server has been integrated with RSA RBA, it will not be usable with other authentication methods including SecurID RADIUS. If your deployment requires authentication methods other than RSA RBA, additional virtual servers must be deployed to support them.**

Configure the Authentication Policy

Configure the primary authentication policy for RSA SecurID on the Virtual Server(s) for which you are enabling Risk-Based Authentication.

For NetScaler Gateway RBA with Citrix StoreFront or Citrix Web Interface as next hop:

1. Configure primary authentication policy as SecurID via RADIUS.
2. Disable 'Pass-through from NetScaler Gateway / Access Gateway' from your Web Interface or StoreFront site.

> **Important: Configuring NetScaler Gateway for RBA when combined with StoreFront or Web Interface requires that the user logon twice. The user must logon at the RSA Secure Logon page and then again at the Citrix Web Interface or StoreFront page. Refer to the Known Issues section of this document for more information.**

Integrate the RBA Script

1. Download the **am_integration.js** integration script from the NetScaler's Authentication Agent in the RSA Security Console.
2. Download the virtual server logon page file, **index.html** from the NetScaler Gateway appliance using an SCP client. The file is located in **/netscaler/ns_gui/vpn/** on the NetScaler Gateway file system.
3. Make a copy of index.html and name it **index_rba.html**.
4. Insert the following lines of code near the bottom of the **index_rba.html** file. These lines should be immediately prior to the </BODY> and </HTML> tags:

```
<script type="text/javascript" language="javascript"
src="am_integration.js"></script>
<script type="text/javascript" language="javascript">
      window.onload=redirectToIdP();
</script>
</BODY>
</HTML>
```

5. Upload the **am_integration.js** and **index_rba.html** files to the **/netscaler/ns_gui/vpn** directory on the NetScaler Gateway file system.
6. Execute the following shell commands on the device to copy these two files to the customization directory:

```
> shell
> cd /netscaler/ns_gui/vpn
> cp am_integration.js /var/customizations/am_integration.js.mod
> cp index_rba.html /var/customizations/index_rba.html.mod
```

> **Note: Create the /var/customizations/ directory if it does not already exist.**

7. If the **/nsconfig/rc.netscaler** file does not yet exist, create it:

```
> touch /nsconfig/rc.netscaler
```

8. Add the following lines to **rc.netscaler**. These commands will instruct the NetScaler Gateway to re-copy your modified files into the vpn directory during each boot sequence:

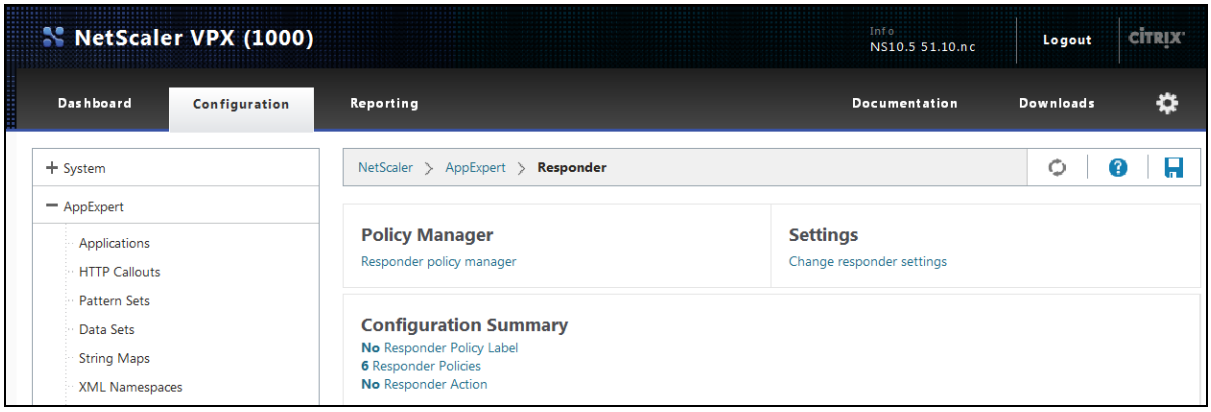
```
> echo cp /var/customizations/am_integration.js.mod
/netscaler/ns_gui/vpn/am_integration.js >> /nsconfig/rc.netscaler

> echo cp /var/customizations/index_rba.html.mod
/netscaler/ns_gui/vpn/index_rba.html >> /nsconfig/rc.netscaler
```

9. Make a note of your RBA target URL.

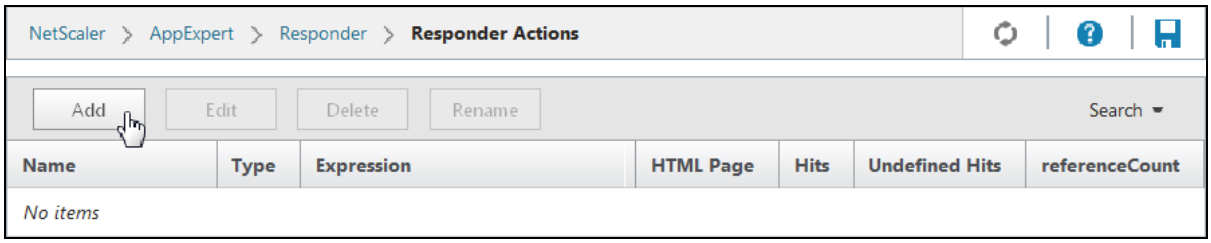
```
https://virtual_server_hostname/vpn/index_rba.html
```

Configure the Responder

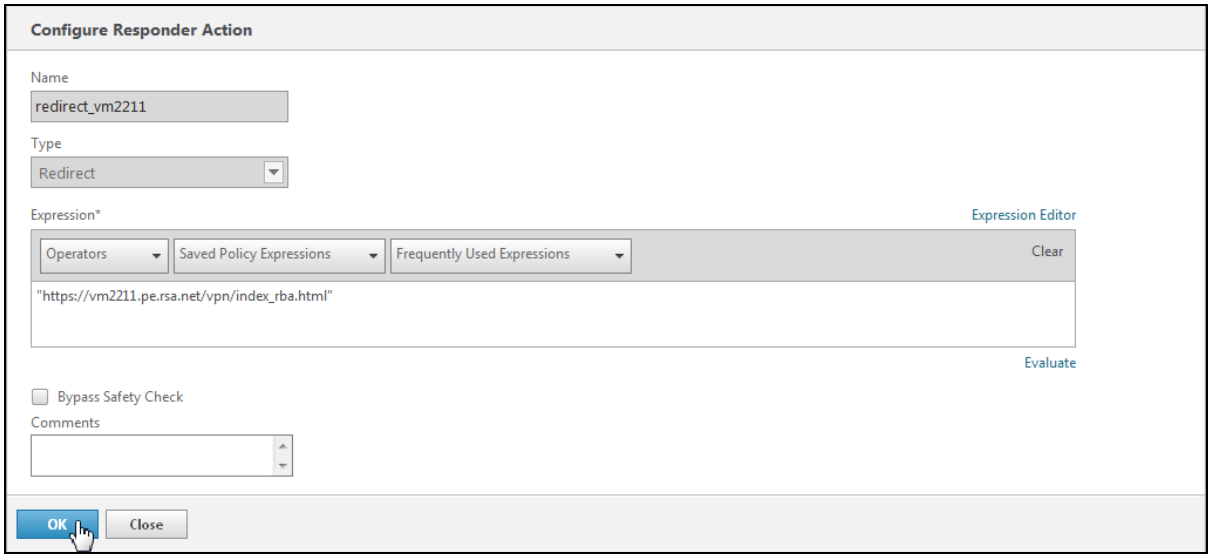
1. Logon to the NetScaler Gateway administrative page.



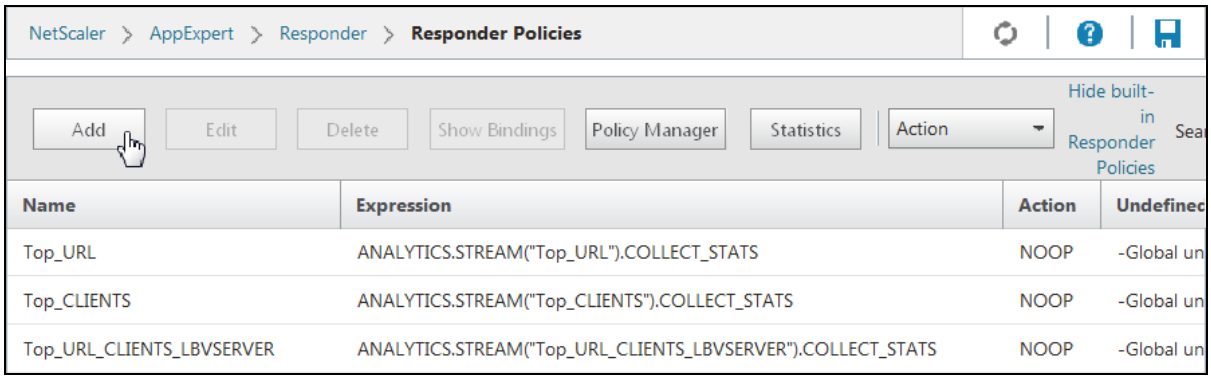
2. Browse to **Configuration** > **AppExpert** > **Responder** > **Actions** and click **Add**.



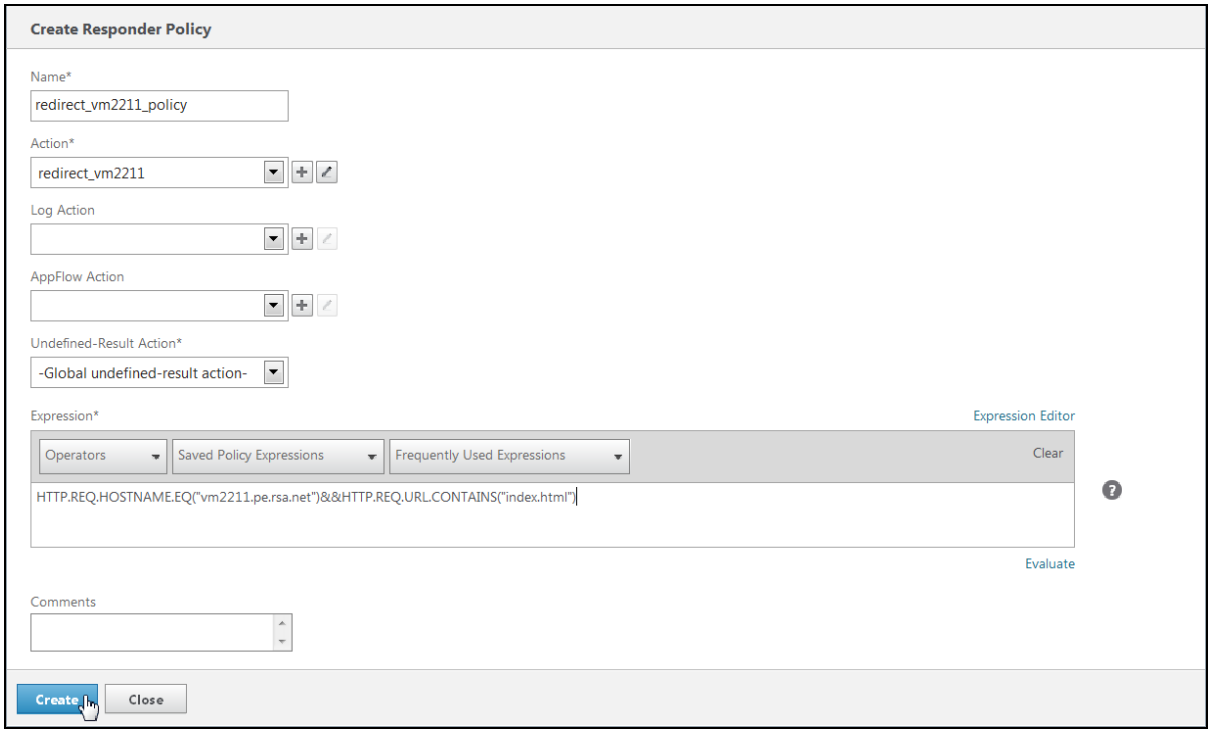
3. Enter **Name**, select **Redirect** from the **Type** drop-down menu, the RBA target URL into the **Expression** field and click **Create**.



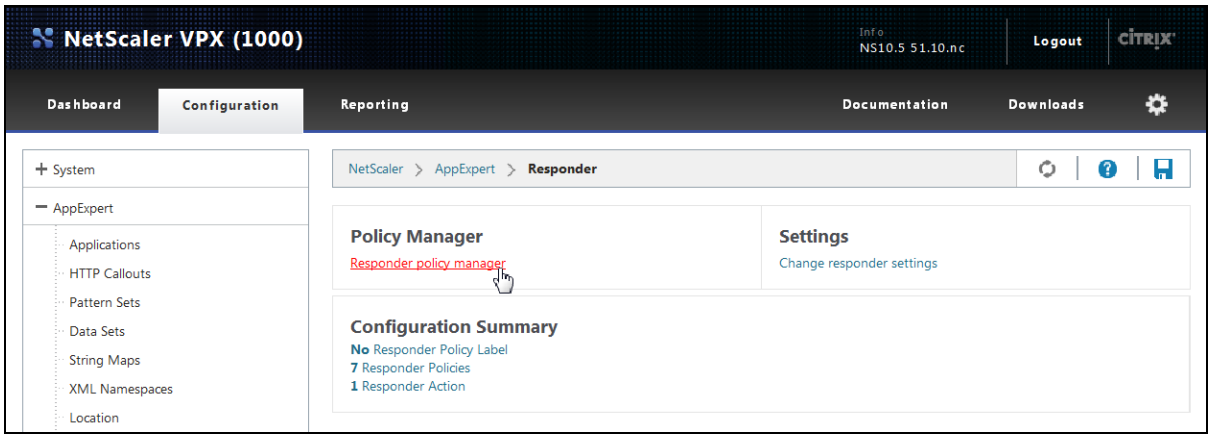
4. Browse to **Configuration** > **AppExpert** > **Responder** > **Policies** and click **Add**.



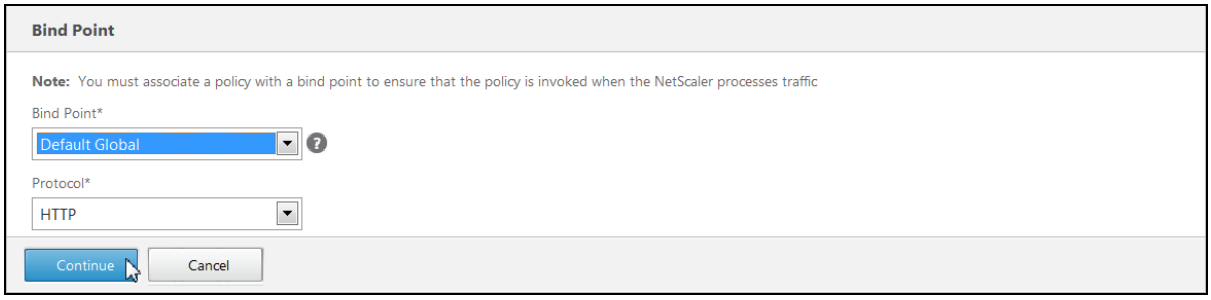
5. Enter **Name**, select your Responder action from the **Action** drop-down menu, enter the **Expression** (as shown in the image below, replacing the hostname with the hostname of your virtual server) and click **Create**.



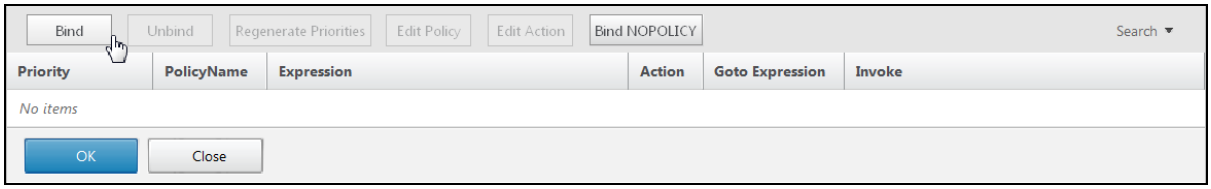
6. Browse to **Configuration** > **AppExpert** > **Responder** and click **Responder policy manager**.



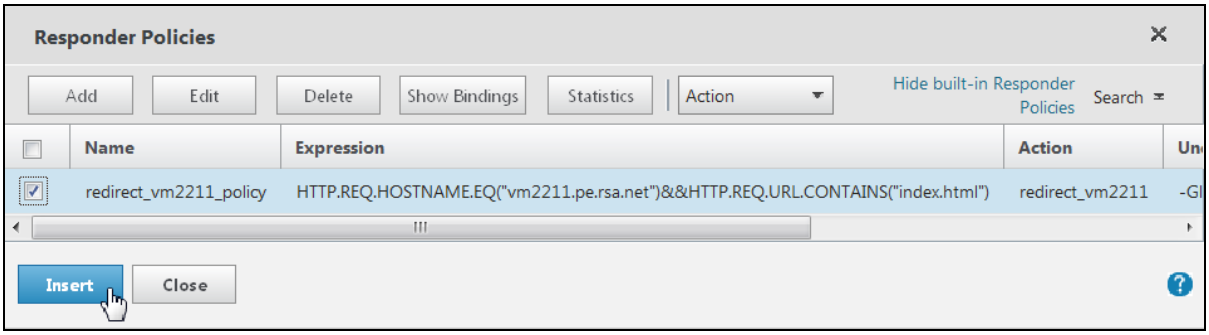
7. Select **Default Global** from the **Bind Point** drop-down menu, select **HTTP** from the **Protocol** drop-down menu and click **Continue**.



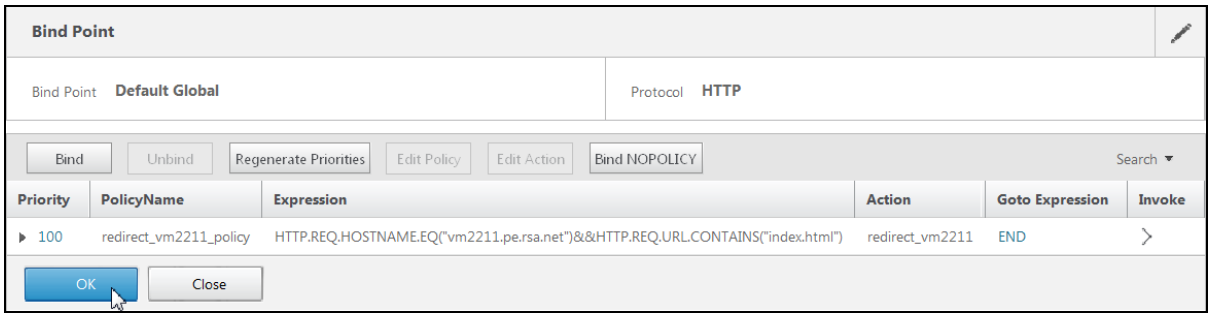
8. Click **Bind**.



9. Mark the checkbox next to your redirect policy and click **Insert**.



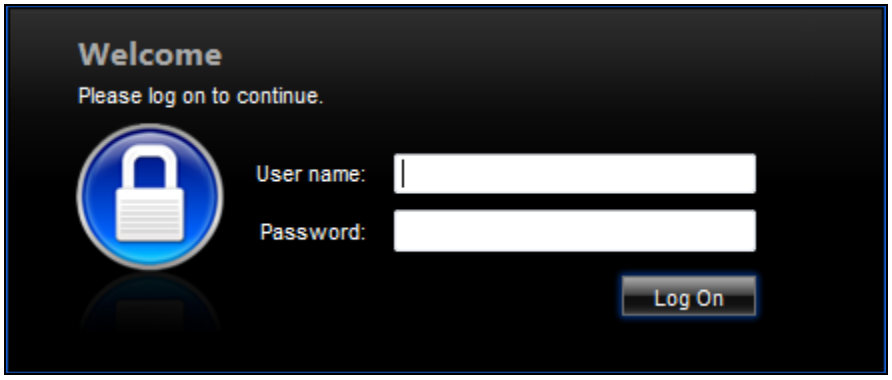
10. Review the settings and click **OK**.



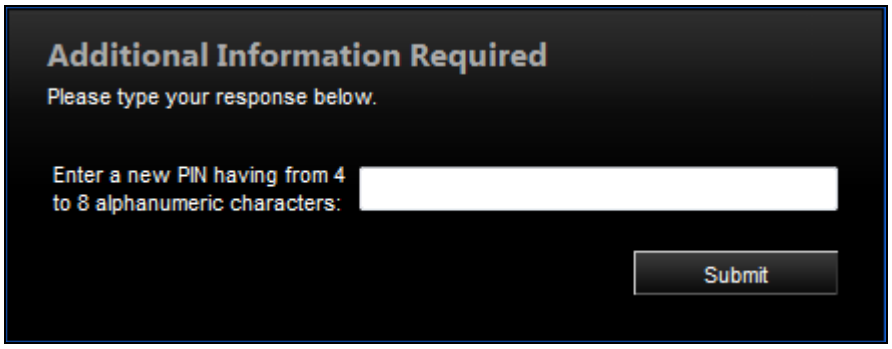
The NetScaler Gateway virtual server is now configured for Risk-Based Authentication.

RSA SecurID Login Screens

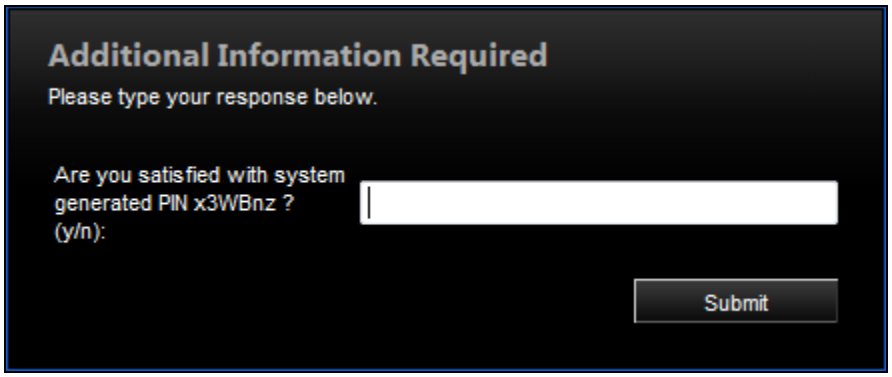
Login screen:



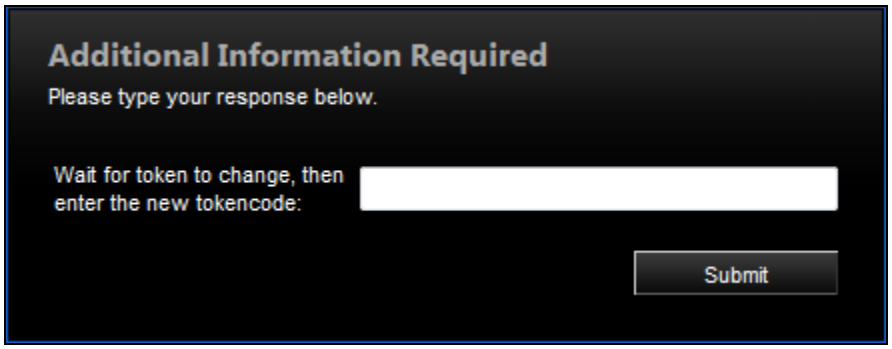
User-defined New PIN:



System-generated New PIN:



Next Tokencode:



Certification Test Checklist for RSA Authentication Manager

Certification Environment

Product Name	Version Information	Operating System
RSA Authentication Manager	8.1	Virtual Appliance
Citrix NetScaler Gateway	10.5 51.10.nc	VPX

RSA SecurID Authentication

Date Tested: August 26th, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
New PIN Mode			
Force Authentication After New PIN	N/A	N/A	✓
System Generated PIN	N/A	N/A	✓
User Defined (4-8 Alphanumeric)	N/A	N/A	✓
User Defined (5-7 Numeric)	N/A	N/A	✓
Deny 4 and 8 Digit PIN	N/A	N/A	✓
Deny Alphanumeric PIN	N/A	N/A	✓
Deny PIN Reuse	N/A	N/A	✓
Passcode			
16 Digit Passcode	N/A	N/A	✓
4 Digit Fixed Passcode	N/A	N/A	✓
Next Tokencode Mode			
Next Tokencode Mode	N/A	N/A	✓
On-Demand Authentication			
On-Demand Authentication	N/A	N/A	✓
On-Demand New PIN	N/A	N/A	✓
Load Balancing / Reliability Testing			
Failover (3-10 Replicas)	N/A	N/A	✓
No RSA Authentication Manager	N/A	N/A	✓

Risk-Based Authentication

Date Tested: October 8th, 2014

Mandatory Functionality	RSA Native UDP Agent	RSA Native TCP Agent	RADIUS Client
Risk-Based Authentication			
Risk-Based Authentication	N/A	N/A	✓

PEW

✓= Pass ✗= Fail N/A = Not Applicable to Integration

Known Issues

Double authentications required with RBA when NetScaler Gateway is integrated with Web Interface or StoreFront.

When you enable RBA with a NetScaler Gateway virtual server that is configured to pass through to a Citrix Web Interface or Citrix StoreFront server, the end user must logon twice. The user must first logon at the RSA Secure Logon page where RBA occurs, and then again at the Citrix Web Interface or StoreFront server.

Logon to StoreFront authentications fail when accessing through NetScaler Gateway without pass-through option enabled.

Citrix StoreFront has a documented bug in all versions which prevents users from logging in through a NetScaler Gateway without the pass-through option enabled.

http://support.citrix.com/proddocs/topic/dws-storefront-25/dws-known-issues.html

http://support.citrix.com/article/CTX136669

To work around the issue, edit the file \inetpub\wwwroot\<storename>\web.config

Search for the requireTokenConsistency="true", change it to "false" and save the file.