Using Vasco IDENTIKEY Server with NetScaler

Deployment Guide

This deployment guide describes the process for deploying Vasco IDENTIKEY server with NetScaler to enable secure authentication for application delivery.
NetScaler is the industry’s leading application delivery controller (ADC), with a wide ranging set of features including application optimization and advanced authentication capabilities. NetScaler’s integration with Vasco IDENTIKEY Server, a widely adopted enterprise authentication system, enables secure application delivery for enterprises that use Vasco’s robust system for security.

This deployment guide focuses on describing the process for integrating a Vasco IDENTIKEY server based authentication system with NetScaler for application delivery and authentication.

**Overview of Vasco IDENTIKEY Authentication**

Vasco DIGIPASS/IDENTIKEY is a popular and robust enterprise second-factor authentication system. The system consists of two major components –

- The DIGIPASS authentication token system
- The IDENTIKEY authentication server

IDENTIKEY Authentication Server (IAS) is an off-the-shelf centralized authentication server that supports the deployment, use and administration of DIGIPASS strong user authentication. It offers complete functionality and management features without the need for significant budgetary or personnel investments.

IDENTIKEY Authentication Server (IAS) is supported on 32-bit systems as well as on 64-bit systems.

For a standard deployment, DIGIPASS tokens are imported into an IDENTIKEY authentication server. Users, policies and authentication clients are defined within the IDENTIKEY server, and then imported DIGIPASS tokens can be assigned to individual users.

**Configuration Details**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vasco IDENTIKEY Server</td>
<td>3.6 (64-bit)</td>
</tr>
<tr>
<td>NetScaler VPX</td>
<td>10.1 and above (Enterprise License)</td>
</tr>
</tbody>
</table>
Common enterprise use cases
The most common enterprise deployment use case for Vasco IDENTIKEY with NetScaler is as a second factor for authentication, with the enterprise LDAP or AD serving as the first factor. Alternatively, the Vasco IDENTIKEY server can also be used as the only authentication factor for extremely secure deployments. While this guide will describe how to setup Vasco as the primary authentication factor, the steps for deploying Vasco IDENTIKEY in a two-factor authentication system will also be mentioned in the guide.

NetScaler features to be enabled
The following features are necessary for enabling authentication with Exchange 2013 for NetScaler. Please ensure these features are enabled.

- Load Balancing and Content Switching (depending on load balancer configuration)
- SSL offload
- AAA-TM (Authentication, Authorization and Auditing)

Other considerations -
- Make sure you have at least a NetScaler Enterprise license installed.

Configuring the Vasco IDENTIKEY server
Note: The installation of an IDENTIKEY server and the procurement of DIGIPASS files are not covered in this guide. It is assumed that IDENTIKEY server installation has been completed successfully without errors and DIGIPASS (.dpx) files are available for importing and assigning to users. Demo/Trial versions of these two tools can be downloaded from the Vasco website for evaluation.

Creating users and policies
The IDENTIKEY server policies define the behavior of the authentication system. These policies can be defined by logging in to the IAS Web Administration portal, which is accessible from the shortcut menu created by the Vasco IAS setup.
Once login is completed, go to the policies tab and select Create in the dropdown as shown below –

![Create new Policy](image)

Here, create a policy with a name of your choice (here we use the name Test with a demo description) and set the Inherits from parameter to the base policy.

Create new Policy

- **Policy ID**: Test
- **Description**: Demo Policy
- **Inherits From**: Base Policy

This new policy will have the same behavior as the policy it inherits from, in this case the base policy. Now, edit the policy by clicking on the Click here to manage <policy name> link, as shown below –

Create new Policy

- **Policy Test1 created. Create another policy below or Click here to manage Test1**
Here, set Local authentication to Digipass/Password, then click Save.

![Edit Policy Settings](image)

The most common enterprise deployment use case for Vasco IDENTIKEY with NetScaler is as a second factor for authentication, with the enterprise LDAP or AD serving as the first factor. Alternatively, the Vasco IDENTIKEY server can also be used as the only authentication factor for extremely secure deployments. While this guide will describe how to setup Vasco as the primary authentication factor, the steps for deploying this system in a two-factor authentication system will also be described later in the guide.

**Adding the RADIUS client**

The client definition defines where the IAS receives authentication requests from and which protocol to use. For NetScaler, we will set up a RADIUS client.

![Create a client by completing the details below. * indicates mandatory fields.](image)
Choose the client type as RADIUS Client and type the IP of the NetScaler box (NSIP) in the Location box, as that is the IP from which the IAS will receive the RADIUS request that is configured. The Protocol ID should be set as RADIUS; set a shared secret phrase here and note it down, as it will also be used when configuring the NetScaler policy.

Create a test user
For testing your setup, create a test user with user ID set to Demo and password set to Test12345. To create the user, navigate to Users>Create in the navigation tabs panel near the top of the screen.

Integrating the DIGIPASS
The IAS is aimed at allowing enterprise user authentication using OTPs (One Time Passwords). For enabling users to use OTPs, a DIGIPASS has to be assigned to the user. The DIGIPASS is a device that generates the OTPs. Vasco provides multiple forms of hardware and software tokens, which have corresponding DPX files which should be imported into the IAS. These files can be imported at the Digipass>Import subpanel as shown on the next page -
To assign a DIGIPASS to a user, open the user’s management profile by navigating to Users>Lists and then clicking on the user’s name. Alternatively, you can select the user and click on the Assign Digipass button at the bottom of the list.

At the profile, click on Assigned Digipass, then click on the Assign button.

At the Search Digipass screen, leave the settings as is and click Next. (this page defines the search criteria for the DIGIPASS accounts that can be used if there are any specific parameters when choosing the DIGIPASS to assign to the user)
At the next screen, Assign Digipass. (when no search criteria is specified, the next available DIGIPASS is auto selected for assignment as shown) set the grace period to an appropriate time. This is the period for which a user is allowed to log in using his or her static password. It is recommended that this be set to a low number, preferably 0. The grace period automatically expires when a user logs on with their DIGIPASS. After setting the grace period, click on Assign.

Verify the selected options and click Assign to proceed assigning the DIGIPASS. Click Cancel to abort the assign DIGIPASS operation.

The final screen shows you that DIGIPASS assignment is complete. Click Finish to exit this workflow.

Assign DIGIPASS

Follow the steps below to select users and assign them DIGIPASS.
Configuring NetScaler for Vasco IDENTIKEY authentication

Setting up front end authentication at the LB/CS vserver

To enable authentication on the NetScaler for the front end (Client to NetScaler authentication), click on the Authentication subsection on the LB/CS vserver Basic Settings page. Note that this action has to be performed on the settings screen for the CS vserver, not the AAA vserver.

To create a new LB or CS vserver, navigate to Traffic Management>Load Balancing/Content Switching>Servers and click on Add.

After clicking on Add, the following screen allows you to create a new LB/CS vserver:

After creating the virtual server, select it from the list that is shown (also shown under Traffic Management>Load Balancing/Content Switching>Servers) and click on Edit. You will then be taken to the Basic Settings page for the vserver.

To get to the Authentication section, scroll down on the page or, if you don’t see the section, look on the right-hand side of the page for the Authentication link and click it. In this section, you have two options – to enable either 401-based authentication, in which case users will be presented with a standard authentication popup prompt, or Form based authentication, in which case NetScaler will present an authentication form to the user. In the second case, you will also have to provide the authentication FQDN (Fully Qualified Domain Name) – which is the domain name for the AAA vserver. This will be the host domain for the form that will be presented to the user.
The authentication profile defines settings such as the authentication domain and level. The authentication level is important, as it defines the vserver levels that authentication with this profile will allow the user to access. A user authenticated with an authentication vserver at a certain level cannot access a vserver running at a higher level. The level setting for LB or CS vservers is an optional parameter, used when access restriction is required.

**RADIUS authentication**

To enable authentication on the NetScaler for the front end (Client to NetScaler authentication), click on the Authentication subsection on the LB/CS vserver Basic Settings page. Note that this action has to be performed on the settings screen for the CS vserver, not the AAA vserver.

To create a new LB or CS vserver, navigate to Traffic Management>Load Balancing/Content Switching>Servers and click on Add.

Before creating a policy, ensure you have defined the settings for your RADIUS server in the Servers tab. If you haven’t, click on the Servers tab and then click Add to create a new RADIUS server definition.

Here, you will see the window shown on the next screen. Enter the settings for the Vasco server as shown.
Here, Enable NAS IP address extraction, set password encoding to PAP and Accounting to OFF.

After adding a new server, you can add the same to your RADIUS authentication policy; go back to the Policies tab and click Add. On the prompt that follows, add the necessary details with the name of the server you have just created. Set the expression to ns_true.

Note: For certain specific applications, different expression settings and policies may need to be defined based upon their authentication parameters.
After creating the policy, bind it to an authentication vserver.

Creating the AAA vserver
The AAA vserver on NetScaler handles authentication requirements. This versatile feature allows a combination of multiple authentication factors in a primary/secondary prioritized setup and policy-driven authentication mechanisms to be used from a single interface. For this deployment, the Vasco_Auth AAA vserver was created. To create a new AAA vserver, navigate to Security>AAA Application Traffic>Virtual Servers and click the Add button.

Upon clicking on the Add button, the following screen is presented, where settings for the AAA vserver (IP address, authentication domain, etc.) can be entered. Context-sensitive help is provided (a small question mark shows up next to each text field) if you need assistance with providing details.

Once created, the AAA vserver shows up on the Authentication Virtual Servers listing screen (where the Add button was clicked earlier) as shown below.
Upon selecting the **Vasco_Auth** AAA vserver and clicking Edit, the following screen is displayed. This is the configuration screen for the virtual server. It allows exhaustive changes to the vserver configuration.

**Authentication Virtual Server**

<table>
<thead>
<tr>
<th>Basic Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name: Vasco_Auth</td>
</tr>
</tbody>
</table>

**Certificates**

- 1 Server Certificate
- **No** CA Certificate

**Advanced Authentication Policies**

- **No** Authentication Policy

**Basic Authentication Policies**

- 1 RADIUS Policy

Here, click on the + sign next to Basic Authentication policies to add the RADIUS policy created earlier for the VASCO server.

**Choose Type**

<table>
<thead>
<tr>
<th>Policies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose Policy*: RADIUS</td>
</tr>
<tr>
<td>Choose Type*: Primary</td>
</tr>
</tbody>
</table>

Choose policy as RADIUS and Type as Primary, then proceed.
Here, click on **Click to Select** under Select Policy. Here, bind the policy created earlier by selecting it and clicking on OK.

This completes the configuration. To test it, navigate to the URL for the LB/CS vserver bound to the AAA vserver, where you will be presented with a password prompt (if 401 based authentication is enabled) or a form as shown below (if form based authentication is enabled).

As described earlier, the Vasco IDENTIKEY server interacts with NetScaler by adding it as a RADIUS client. The Vasco system supports RADIUS as one of the protocols over which authentication into the Vasco IDENTIKEY server can happen, and therefore hosts a RADIUS server interface on port 1812. This is the port the NetScaler device interacts with.
Packet flow between NetScaler and the Vasco IDENTIKEY server during a client authentication transaction

The diagram below describes the rough packet flow between the various elements of the client authentication transaction for Vasco.

Vasco IDENTIKEY for dual factor authentication

To enable two-factor authentication, complete configuration authentication servers (Vasco RADIUS and the other authentication factor) servers as described earlier in the guide. Then, navigate to the Basic Settings page for the AAA vserver configured earlier (Security>AAA — Application Traffic>Virtual Servers) and then, click on the plus sign (+) next to Basic Authentication Policies. Here, in the Choose Type dropdown, select Secondary. After clicking Continue, you are taken to the following screen where you can select or add a new authentication policy.

After selecting/adding a new policy (the process for adding a new RADIUS policy is the same as described earlier), click on Bind. This completes the configuration for two-factor authentication.
Conclusion
Citrix NetScaler enables a secure and optimized experience with the integration of Vasco IDENTIKEY/DIGIPASS as direct or two factor authentication. NetScaler’s integration capabilities with Vasco and other leading secure authentication vendors makes it a device of choice for enterprises of all sizes. Citrix NetScaler is deployed in thousands of networks across the globe, is the only ADC that fully integrates into Cisco’s unified fabric and delivers optimizes application delivery and security in both software and hardware-based options. To learn more about how NetScaler can integrate with various authentication systems or to address other application delivery requirements, please visit http://www.citrix.com.

About Citrix
Citrix (NASDAQ:CTXS) is leading the transition to software-defining the workplace, uniting virtualization, mobility management, networking and SaaS solutions to enable new ways for businesses and people to work better. Citrix solutions power business mobility through secure, mobile workspaces that provide people with instant access to apps, desktops, data and communications on any device, over any network and cloud. With annual revenue in 2014 of $3.14 billion, Citrix solutions are in use at more than 330,000 organizations and by over 100 million users globally. Learn more at www.citrix.com.