Trademarks

Deepnet Unified Authentication, MobileID, QuickID, PocketID, SafeID, GridID, FlashID, SmartID, TypeSense, VoiceSense, MobilePass, DevicePass, RemotePass and Site Stamp are trademarks of Deepnet Security Limited. All other brand names and product names are trademarks or registered trademarks of their respective owners.

Copyrights

Under the international copyright law, neither the Deepnet Security software or documentation may be copied, reproduced, translated or reduced to any electronic medium or machine readable form, in whole or in part, without the prior written consent of Deepnet Security.

Licence Conditions

Please read your licence agreement with Deepnet carefully and make sure you understand the exact terms of usage. In particular, for which projects, on which platforms and at which sites, you are allowed to use the product. You are not allowed to make any modifications to the product. If you feel the need for any modifications, please contact Deepnet Security.

Disclaimer

This document is provided “as is” without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the document. Deepnet Security may make improvements of and/or changes to the product described in this document at any time.

Contact

If you wish to obtain further information on this product or any other Deepnet Security products, you are always welcome to contact us.

Deepnet Security Limited
Building 3
North London Business Park
London N11 1GN
United Kingdom

Tel: +44(0)20 3668 1580
Fax: +44(0)20 8446 3182
Web: www.deepnetsecurity.com
Email: support@deepnetsecurity.com
# Table of Contents

Overview .................................................................................................................. 4

Preparation ................................................................................................................. 5

RADIUS Authentication ............................................................................................... 6
  DualShield Configuration ........................................................................................... 6
    Create a RADIUS logon procedure .................................................................. 6
    Create a RADIUS application ....................................................................... 7
    Register the Citrix NetScaler as a Radius client ........................................ 8

NetScaler Configuration ............................................................................................... 9
  Register DualShield Radius Server .................................................................. 9
  Create Authentication Policies for Web Browsers ........................................ 10
  Create Authentication Policies for Citrix Receivers .................................... 10

One-Time Password .................................................................................................. 13
  Edit Logon Procedure......................................................................................... 13
  Configure Citrix NetScaler ............................................................................... 13
  Configure Citrix Receiver ................................................................................ 14
  Test Logon in Web Browser ............................................................................. 15
  Customise Logon Form ..................................................................................... 15
  Test Logon in Web Browser ............................................................................. 16
  Test Logon in Citrix Receiver ........................................................................... 17

On-Demand Password ............................................................................................... 18
  Edit Logon Procedure......................................................................................... 18
  Configure Citrix NetScaler ............................................................................... 18
  Configure Citrix Receiver ................................................................................ 19
  Test Logon in Web Browser ............................................................................. 20
  Test Logon in Citrix Receiver ........................................................................... 21

SAML 2.0 ..................................................................................................................... 22
  DualShield Configuration ..................................................................................... 22
    Create a Web logon procedure ...................................................................... 22
    Create a Web application .............................................................................. 23
    Create a web application Service provider ................................................. 24

NetScaler Gateway Configuration ............................................................................. 25
  Install the DualShield SSO Server certificate ............................................... 25
  Create SAML authentication server ............................................................... 26
  Create SAML Authentication policy ............................................................... 28
  Create NetScaler Gateway Virtual Server ...................................................... 29
  Configure Citrix Receiver ............................................................................... 31

Authentication ........................................................................................................... 32
  Test Logon in Web Browser ............................................................................. 32
  Test Logon in Citrix Receiver ........................................................................... 33
Overview

This implementation guide describes how to integrate Citrix NetScaler appliance with the DualShield unified authentication platform in order to add two-factor authentication into the Access Gateway login process.

Citrix NetScaler supports external RADIUS server as its authentication server. DualShield unified authentication platform includes a fully compliant RADIUS server – DualShield Radius Server. DualShield provides a wide selection of portable one-time password tokens in a variety of form factors, ranging from hardware tokens, software tokens, mobile tokens to USB tokens. These include:

- Deepnet SafeID
- Deepnet MobileID
- Deepnet GridID
- Deepnet CryptoKey
- RSA SecurID
- VASCO DigiPass Go
- OATH-compliant OTP tokens

In addition to the support of one-time password, DualShield also supports on-demand password for RADIUS authentication. The product that provides on-demand password in the DualShield platform is Deepnet T-Pass. Deepnet T-Pass is an on-demand, token-less strong authentication that delivers logon passwords via SMS texts, phone calls, twitter direct messages or email messages.

The complete solution consists of the following components:

- Citrix NetScaler Appliance
- DualShield Radius Server
- DualShield Authentication Server
Preparation

Prior to configuring Citrix NetScaler for two-factor authentication, you must have the DualShield Authentication Server and DualShield Radius Server installed and operating. For the installation, configuration and administration of DualShield Authentication and Radius servers please refer to the following documents:

- DualShield Authentication Platform – Installation Guide
- DualShield Authentication Platform – Quick Start Guide
- DualShield Authentication Platform – Administration Guide
- DualShield Radius Server - Installation Guide

You also need to have a RADIUS application created in the DualShield authentication server. The application will be used for the two-factor authentication in Citrix NetScaler. The document below provides general instructions for RADIUS authentication with the DualShield Radius Server:

VPN & RADIUS - Implementation Guide

Following outlines the key steps:

In DualShield

1. Create a logon procedure for RADIUS authentication
2. Create an RADIUS application for Citrix NetScaler
3. Register the Citrix NetScaler as a RADIUS client

In Citrix NetScaler

1. Register the DualShield RADIUS authentication server
RADIUS Authentication

DualShield Configuration

Create a RADIUS logon procedure

1. Login to the DualShield management console
2. In the main menu, select “Authentication | Logon Procedure”
3. Click the “Create” button on the toolbar
4. Enter “Name” and select “RADIUS” as the Type

5. Click “Save”
6. Click the Context Menu icon of the newly create logon procedure, select “Logon Steps”
7. In the popup windows, click the “Create” button on the toolbar
8. Select the “Static Password” as the authenticator

9. Click “Save”
Create a RADIUS application

1. In the main menu, select “Authentication | Applications”
2. Click the “Create” button on the toolbar
3. Enter “Name”
4. Select “Realm”
5. Select the logon procedure that was just created

6. Click “Save”
7. Click the context menu of the newly created application, select “Agent”

8. Select the DualShield Radius server, e.g. “win2004x86-RADIUS”
9. Click “Save”
10. Click the context menu of the newly created application, select “Self Test”
Register the Citrix NetScaler as a Radius client

1. In the main menu, select “RADIUS | Clients”
2. Click the “Register” button on the toolbar

3. Select the application that was created in the previous steps
4. Enter Citrix NetScaler Appliance’s IP in the IP address field
5. Enter the Shared Secret which will be used in Citrix NetScaler.
6. Click “Save”
NetScaler Configuration

It is assumed that the Citrix NetScaler is setup and operational. An existing Domain user can authenticate using a Domain AD password and access applications, your users can access through SSL using Domain accounts.

Register DualShield Radius Server

1. Log into the Citrix NetScaler administration console, navigate to NetScaler Gateway | Policies | Authentication | Radius, select the “Servers” tab
2. Click “Add” button on the bottom
3. Enter the details of your DualShield Radius server as highlighted above.
4. Click “Create”
Create Authentication Policies for Web Browsers

1. Log into the Citrix NetScaler administration console, navigate to NetScaler Gateway | Policies | Authentication | Radius, select the “Policies” tab
2. Click the “Add” button on the bottom
3. Select newly create the Radius server, e.g. “DualShield-RADIUS”
4. Create an “ns_true” expression
5. Click “Create”

Create Authentication Policies for Citrix Receivers

To support Citrix Receiver running on mobile devices, the following configuration steps are required. This will allow the NetScaler to detect the incoming request is from the Citrix receiver by checking the Host Header.

Create an LDAP policy for the Citrix Receiver

1. Log into the Citrix NetScaler administration console, navigate to NetScaler Gateway | Policies | Authentication | LDAP, select the “Policies” tab
2. Click the “Add” button on the bottom
3. Select the LDAP Server, e.g. “Deepnetqa” (Create server if you don’t have one)
4. Create use the following expression:
   
   `REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver`
5. Click “Create”

**Create a DualShield RADIUS policy for the Citrix Receiver**

1. Log into the Citrix NetScaler administration console, navigate to NetScaler Gateway | Policies | Authentication | Radius, select the “Policies” tab
2. Click the “Add” button on the bottom
3. Select newly create the Radius server, e.g. “DualShield-Radius”
4. Create the following expression:
   
   ```plaintext
   REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver
   ```
5. Click “Create”
One-Time Password

If you plan to deploy only the one-time password based authentication in your user base using OTP tokens such as Deepnet SafeID, MobileID, then you will configure your Citrix NetScaler in such way that it will use your AD as the primary authentication server and your DualShield as the secondary authentication server. Your AD will be responsible for verifying users’ AD passwords and your DualShield will be responsible for verifying users’ one-time passwords only.

Edit Logon Procedure

In the DualShield Management Console, edit the logon procedure for your NetScaler application. You will only need one logon step and typically the logon step will have “One-Time Password” as the authentication method:

Configure Citrix NetScaler

1. Go to the properties of your NetScaler Gateway | Virtual Server and go to the Authentication tab. On the Primary Authentication Policies, add the DualShield RADIUS receiver policy as top priority and the LDAP non-receiver policy as secondary priority.

2. On the Secondary Authentication Policies, add the DualShield LDAP receiver policy as top priority and the DualShield RADIUS non-receiver policy as secondary priority.
Configure Citrix Receiver

Select Domain + Security Token
**Test Logon in Web Browser**

Navigate to the Citrix NetScaler Access Gateway logon page:

![Citrix Access Gateway Logon Page](image)

The logon form consists of 3 fields:

- **User name**: User's domain account login name
- **Password1**: AD password
- **Password2**: One-time password

**Customise Logon Form**

You can customise NetScaler Access Gateway's logon page to make it more user friendly. For instance, you may want to change "Password1" to "Password" or "Ad Password", "Password2" to "Passcode" or "One-Time Password".

The article below is the general instruction for customising Access Gateway logon page:

[http://support.citrix.com/article/CTX126206](http://support.citrix.com/article/CTX126206)

The basis of the customisation is to change relevant HTML and Javascript files in the NetScaler appliance. These file can be accessed via SSH in the folder below:

```
/netcaler/ns_gui/vpn
```
As an example, if you just want to “Password1” to “Password” and “Password2” to “Passcode”, then you need to edit the “login.js” file and replace the function “ns_showpwd()” with the following code:

```javascript
function ns_showpwd()
{
    var pwc = ns_getcookie("pwcount");
    document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;">Password:</TD>');</
    document.write('<TD colspan=2 style="padding-right:8px;">Password:</TD>');
    if ( pwc == 2 )
    {
        document.write('<TR><TD align=right style="padding-right:10px;white-space:nowrap;">Passcode:</TD>');</
        document.write('<TD colspan=2 style="padding-right:8px;">Passcode:</TD>');
    }
    UnsetCookie("pwcount");
}
```

Test Logon in Web Browser

The Access Gateway logon page will be presented as:
Test Logon in Citrix Receiver

Enter AD/LDAP Password
Enter One-time Password
On-Demand Password

If you plan to deploy only the on-demand password based authentication in your user base using Deepnet T-Pass, then you will configure your Citrix NetScaler in such way that it will use your DualShield Radius server as the primary authentication server. Your DualShield server will be responsible for verifying both users’ AD password and one-time passwords. There should be no secondary authentication servers.

Edit Logon Procedure

In the DualShield Management Console, edit the logon procedure for your NetScaler application. You will need to define two logon steps: the first step requires users to enter their static password (AD password), which will also trigger the DualShield server to send the user’s on-demand password. The second step will then ask users to enter their on-demand password.

Configure Citrix NetScaler

1. Navigate to NetScaler Gateway | Virtual Servers
2. Select the virtual server you wish to configure and double click it
3. Click the “Authentication” tab
4. Select the “Primary” tab
5. Unbind the current authentication server if any
6. Bind the following policies
Configure Citrix Receiver

Turn off the Security Token
**Test Logon in Web Browser**

Navigate to the Citrix NetScaler Access Gateway logon page:

Enter your username and your AD password.

Your DualShield server will send an on-demand password via the delivery channel defined in your T-Pass policy, e.g. SMS text message or email message.

NetScaler will then prompt you to enter your T-Pass one-time password:
Test Logon in Citrix Receiver

Once your AD password is authenticated, DualShield server will send an on-demand password via the delivery channel defined in your T-pass policy.

Citrix Receiver will then prompt you to enter your T-Pass one-time password.
SAML 2.0

DualShield Configuration

Create a Web logon procedure

1. Login to the DualShield Management Console
2. In the main menu, select “Authentication | Logon Procedure”
3. Click the “Create” button on the toolbar
4. Enter “Name” and select “Web” as the type

5. Click “Save”
6. Click the Context Menu icon of the newly create logon procedure, select “Logon Steps”
7. In the popup windows, click the “Create” button on the toolbar
8. Select the authentication method, e.g.: “Static password”
Create a Web application

1. In the main menu, select “Authentication | Application”
2. Click the “Create” button on the toolbar
3. Enter “Name”
4. Select “Realm”
5. Select the newly created logon procedure
6. Click “Save”
7. Click the context menu of the newly created application, select “Agent”
8. Select the SSO Server
9. Click “Save”
10. Click the context menu of the newly created application, select “Self Test”

Create a web application Service provider
1. In the main menu, select “SSO | Service Providers”
2. Click the “Create” button on the toolbar
3. Select “SSO Server”
4. Enter “Name”
5. Select “SAML 2.0” as Type
6. Enter the Metadata

Below is a template of a SP metadata. You need to modify it accordingly with the domain name of your NetScaler Gateway virtual server and domain name of your DualShield server.
Install the DualShield SSO Server certificate

1. Log into the DualShield Authentication server, in the main menu, select “SSO”
2. Click the SSO Server context menu, select “Download IdP Certificate” and save the file.
3. Log in to the NetScaler VPX web console, select “Traffic Management | SSL | Certificates”, click “Install”
4. Enter the “Certificate-Key Pair Name”
5. Upload the DualShield SSO server certificate from local store
6. Expand the newly installed certificate, check the certificate information

<table>
<thead>
<tr>
<th>Certificate-Key Pair Name*</th>
<th>DualShieldIdp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate File Name*</td>
<td>DualShieldIdp.crt</td>
</tr>
<tr>
<td>Key File Name</td>
<td></td>
</tr>
<tr>
<td>Certificate Format</td>
<td>PEM + DER</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Certificate Bundle</td>
<td></td>
</tr>
<tr>
<td>Notify When Expires</td>
<td></td>
</tr>
<tr>
<td>Notification Period</td>
<td></td>
</tr>
</tbody>
</table>

Create SAML authentication server

1. Log into the DualShield Authentication Server, select “SSO”
2. Click the SSO Server context menu, select “Download IdP Metadata” and select the newly create application, e.g. “Access Gateway SAML”

3. Log into the NetScaler VPX web console, select “Configuration | NetScaler Gateway | Policies | Authentication | SAML”
4. Click the “Servers” tab, and click “Add”
5. Enter the “Name”
Notes:
Enter the location value in DualShield Access Gateway SAML application IdP Metadata as the “Redirect URL”.

```xml
<md:SingleSignOnService
  Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
  Location="http://DualShield.deepnetqa.com:8074/appsso/login?DASApplicationName=Access Gateway SAML"/>
```

Enter the “Entity ID” on the service provider metadata as the “SAML Issuer Name”

```xml
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  entityID="https://ageesaml.deepnetqa.com"/>
```

6. Select the newly installed DualShield SSO server certificate on “IDP Certificate name” field
7. Click “Create” and “Close”
Create SAML Authentication policy

1. Select “Configuration | NetScaler Gateway | Policies | Authentication | SAML”
2. Click the “Policy” tab, and click “Add”
3. Enter the “Name”
4. Create an “ns_true” expression
5. Select the newly created SAML authentication server, e.g. “DualShieldAGEE”

6. Click “OK”
Create NetScaler Gateway Virtual Server

1. Select “Configuration | NetScaler Gateway | Virtual Servers”
2. Enter the “Name” and “IP Address”
3. Select the Identity certificate by clicking “Add” button

4. Click “OK”
5. Click the “Authentication”, select the newly create SAML policy as the primary authentication policy by clicking “Insert Policy”
6. Click “OK”
Configure Citrix Receiver

Select the "Web Interface"
Authentication

Test Logon in Web Browser

Now, your NetScaler Gateway is enabled with two-factor authentication, and the access to the NetScaler Gateway virtual server “https://ageesaml.deepnetqa.com” requires two-factor authentication.

Launch your browser, browser the NetScaler Gateway Virtual server URL. For example: https://ageesaml.deepnetqa.com You will be directed to the DualShield SSO server to be authenticated with 2FA:

Test Logon in Citrix Receiver

Log in to application: Access Gateway SAML

Step 1
Login Name: demo.test
Authenticator: One-Time Password
One-Time Password: Enter the One-Time Password

----------------------------------- END -----------------------------------