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
Oakleigh Road South
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

1. Overview ........................................................................................................................................... 4
2. Prerequisites .......................................................................................................................................... 5
3. DualShield Configuration ..................................................................................................................... 6
   3.1 Create a RADIUS logon procedure ................................................................................................. 6
   3.2 Create a RADIUS application ......................................................................................................... 7
   3.3 Register Network Policy Server as a Radius Client........................................................................... 7
4. NPS Configuration ............................................................................................................................... 9
   4.1 Create a RADIUS Client .................................................................................................................. 9
   4.2 Create a Remote RADIUS Server Group ......................................................................................... 9
   4.3 Create a Connection Request Policy .............................................................................................. 10
   4.4 Create a Network Policy ................................................................................................................ 12
5. RAS Configuration .............................................................................................................................. 15
6. Dial-up Client Configuration ............................................................................................................... 16
7. Authentication Test ............................................................................................................................... 17
1. Overview

This document describes how to integrate the Microsoft Windows Routing and Remote Access Service via Network Policy Server with the DualShield unified authentication platform in order to add two-factor authentication while access to the internal corporate network.

DualShield unified authentication platform includes a fully compliant RADIUS server – DualShield Radius Server. DualShield provides a wide selection of portable OTP tokens in a variety of form factors, ranging from hardware tokens, software tokens, and 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 support the one-time password, DualShield also supports on-demand password for RADIUS authentication. The produce that provides on-demand passwords in DualShield platform is Deepnet T-Pass. Deepnet T-Pass in 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:

- DualShield Authentication Server
- DualShield Radius Server
- Microsoft Network Policy Server
- VPN Gateway
- VPN Client
2. **Prerequisites**

It is expecting the Network Policy Server and Remote Routing Access Service have already been setup and operating.

You must have the DualShield Authentication Server and DualShield Radius Server installed and operating. For the installation, configuration and administrator of the DualShield Authentication and Radius server, 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
3. **DualShield Configuration**

3.1 **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 a name and select "RADIUS" as the type

![Logon Procedure -- New](image1)

5. Click "Save"
6. Click the context menu icon of the newly create logon procedure, select "Logon steps"
7. In the popup window, click the "Create" button on the toolbar
8. Select the desire authenticator, e.g. "static password + one-time password"

![Logon Step -- 1](image2)

9. Click "Save"
3.2 Create a RADIUS application

1. In the main menu, select "Authentication | Applications"
2. Click the "Create" button on the toolbar
3. Enter a name and select a realm
4. Select the newly created logon procedure

   ![Application Info -- New](image)

5. Click "Save"
6. Click the Context menu of the newly created application, select "Agent"

   ![Assign to Agents](image)

   Select your DualShield Radius Server, e.g. "win2004x86-RADIUS"

7. Click "Save" and use the "Self-Test" function to verify that the application is correctly set up and ready.

   ![Self Test](image)

3.3 Register Network Policy Server as a Radius Client

1. In the main menu, select "RADIUS | Client"
2. Click the "Register" button on the toolbar
3. Select the application that was created in the previous steps.
4. Enter Network Policy Server's IP in the IP address field
5. Enter the Share Secret which will be used in Network Policy Server
6. Click "Save"
4. NPS Configuration

4.1 Create a RADIUS Client

1. Click "New" on the Radius Clients Context Menu

2. Enter the RRAS’s IP in the IP address filed, e.g. "192.168.1.104"
3. Enter the Shared secret password
4. Click "OK"

4.2 Create a Remote RADIUS Server Group

1. Click "New" on the Remote RADIUS Server Group Context Menu
2. Create the Remote RADIUS Server Group, e.g. "DualShield Radius Server Group"
3. Enter the name or IP address of the DualShield Radius Server
4. Select "Authentication/Accounting" tab on the Radius Clients Context Menu, enter the shared secret password.

5. Select "Load Balancing" tab, allocate the weight and click "OK"

4.3 Create a Connection Request Policy

1. Create the connection request policies, e.g. "DualShield Radius Connection Policy"
2. Change type of network access server to "Remote Access Server (VPN-Dial up)" and click "Next"
3. Add a new condition "Day and Time Restrictions" and select "Permitted" to allow certain time of connection and press "OK" and "Next"

4. Select "Forward requests to the following remote RADIUS server group for authentication" and select the newly server group "DualShield Radius Server Group"
5. Click "Next" and "Finish"

4.4 Create a Network Policy

1. Create Network Policies, e.g. "DualShield Radius Network Policy"
2. Change type of network access server to "Remote Access Server (VPN-Dial up)" and click "Next"
3. Add a new condition "Day and Time Restrictions" and select "Permitted" to allow certain time of connection and press "OK" and "Next"

4. Specify Access Permission and click "Next"
5. Select the authentication methods

6. Click "Next" and "Finish"
5. **RAS Configuration**

1. Select "Routing and Remote Access", right click and select "Properties"
2. Select the "Security" tab and click "Authentication methods", select the authentication methods and click "OK"

3. Click the "Configure", and the Server IP address which is the host name or IP address of NPS Server, e.g. "192.168.1.108" and shared secret password.

4. Click "OK"
6. **Dial-up Client Configuration**

1. Launch the Remote Access Client

2. Click the "Properties", and select the "Security" tab

3. Select the "Data Encryption" option from the dropdown list

4. Check the "PAP" option
7. Authentication Test

1. Enter the Username, e.g. "demo.test"
2. Enter the password, e.g. "Password123456"

Note

CHAP and MS-CHAP.v2 is not supported when the passcode consists of the AD password (Static Password). In other words, if the User Directory or Identity Source of a VPN application is an external AD or LDAP server, and the passcode is "Static Password", "One-Time Password + Static Password" or "Static Password + One-Time Password", then CHAP and MS-CHAP.v2 cannot be supported.

If you have to use CHAP and MS-CHAP.v2, then the passcode should not include AD password, or the User Directory or Identity Source of the VPN application is created in the internal SQL Server.

===END===

Copyright © 2013, Deepnet Security. All Rights Reserved.