Security, Simplified.

HOTPin Integration Guide: DirectAccess

celestix

Disclaimer

Disclaimer of Warranties and Limitation of Liabilities

All information contained in this document is provided 'as is'; Celestix assumes no responsibility for its accuracy and/or completeness.

In no event will Celestix be liable for damages arising directly or indirectly from any use of the information contained in this document.

Updated: November 7, 2013

Copyright

1 Introduction

This document describes how to integrate HOTPin with DirectAccess 2012 configured for VPN access.

DirectAccess in Windows Server® 2012 helps IT offer users seamless, more secure access to corporate data from virtually any Internet connection.

Celestix HOTPin® provides two-factor authentication (2FA) for remote access and cloud solutions (like SSL VPN, IPSec VPN and Web authentication). Our 2FA solution uses a PIN and one-time-password (OTP). OTP generation has multiple options: client software, hard token devices, or token providers that use email, SMS, or web technologies. Thus HOTPin OTPs can support a variety of devices for strong authentication. Configure the device options that best suit your environment:

- Client software leverages already deployed smart devices
- Token providers use any email/SMS-enabled device
- Hard token devices are available from Celestix, or bring your own OATH-compliant PSKC

HOTPin is designed to be an easy to deploy, easy to use technology. It integrates directly with Microsoft's Active Directory® and negates the need for additional user security databases. HOTPin consists of two core elements: a RADIUS Server and authentication server. The authentication server directly integrates with LDAP or Active Directory (AD) in real time.

1.1 Overview

Illustration 1 provides an overview of a DirectAccess (DA) environment using HOTPin 2FA.

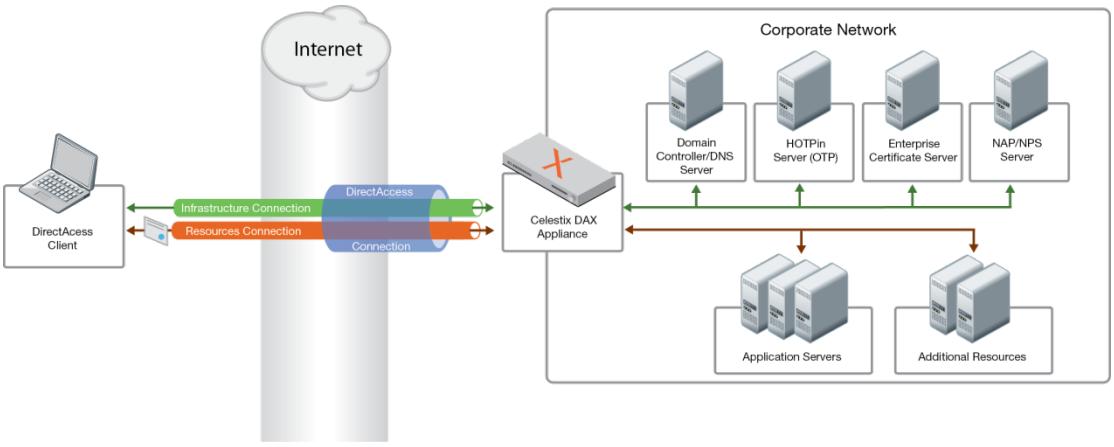


Illustration 1

1.2 Summary

This integration guide covers the set up for a basic installation in which HOTPin provides 2FA for DA connections. It may be helpful to set up a test environment before rolling out to production; as such, some of the example settings suggest test information.

The content is excerpted from the article “Steps for Configuring the Test Lab|STEP 2: Configure APP1” on the TechNet website; it is revised for your convenience to aid in setting up HOTPin 2FA. You can access the full, original article at:

http://technet.microsoft.com/en-us/library/hh831635.aspx

1.3 Prerequisites

The integration covered in this document requires the following components:

- Enterprise certificate server
  - Windows Server 2008 R2 or 2012
- HOTPin
  - HOTPin HSA
    - or -
    Windows Server 2008 R2 64-bit (Standard or Enterprise) with:
    - IIS installed with SSL certificate (required for management and remote administration)
    - HOTPin 3.7 server software
- Celestix DAX appliance
- Windows® client computer to test configuration

  Clients must be Windows 7 or 8 and either Enterprise or Ultimate editions

Note: each item listed is a separate server.

1.4 Assumptions

This document assumes the following are true:

- HOTPin Server has been provisioned.
- DirectAccess 2012 has been configured.
- Readers are familiar with AD management .
- Readers are familiar with RADIUS administration.

2 Certificate Server Configuration

The enterprise certificate server component serves as the root certificate authority (CA). HOTPin uses the DA Remote Access with OTP feature to support 2FA. This requires configuration for Web Server certificate templates.

2.1 Configure the Template for OTP Certificate Requests

This template will be used to sign OTP certificate requests.

1. On the enterprise certificate server, click “Start”.
2. In the search box, enter “certtmpl.msc”.
3. In the Certificate Templates Console details pane, right-click the “Computer” template and select “Duplicate Template”.
4. In the “Properties of New Template” dialog box, complete the following:
    a. Select the “Compatibility” tab.
    b. In the “Certification Authority” list, select the appropriate Windows Server version for your CA server.
    c. In the “Resulting changes” dialog box click “OK”.
    d. In the “Certificate recipient” list click “Windows 8/ Windows Server 2012”.
    e. In the “Resulting changes” dialog box click “OK”.
5. In the “Properties of New Template” dialog box, click the “General” tab, complete the following:
    a. In “Template display name”, type “DAOTPRA”.
    b. Set the “Validity period” to 2 days.
    c. Set the “Renewal Period” to 1 day.
    Note: If the “Certificate Templates” warning is displayed, click “OK”.
6. Click the “Security” tab, and then click “Add”. Complete the following:
    a. In the “Select Users, Computers, Service Accounts, or Groups” dialog box, click “Object Types”.
    b. In the “Object Types” dialog box, select “Computers”, and then click “OK”.
    c. In the “Enter the object names to select” box, enter the name of the DAX appliance.
    d. Click “OK”.
    e. In the “Allow” column, select the “Read”, “Enroll”, and “Autoenroll” check boxes.
    f. Click “Authenticated Users”, select the “Read” check box under the Allow column, and then clear all other check boxes.
    g. Click “Domain Computers”, and uncheck “Enroll” under the Allow column.
    h. Click “Domain Admins” and “Enterprise Admins” and click “Full Control” under the Allow column for both.
    i. Click “Apply”.

7. Click the “Subject Name” tab, and complete the following:
    a. Click “Build from this Active Directory information”.
    b. In the “Subject name format” list select “DNS name”.
    c. Make sure that the “DNS name” box is checked.
    d. Click “Apply”.
8. Click the “Extensions” tab, select “Application Policies” and then click “Edit”. Complete the following:
    a. Remove all existing application policies.
    b. Click “Add”.
    c. In the “Add Application Policy” dialog box, click “New”.
    d. Enter “DA OTP RA” in the “Name” field.
    e. Enter "1.3.6.1.4.1.311.81.1.1” in the “Object identifier” field.
    f. Click “OK”.
    g. In the “Add Application Policy” dialog box, click “OK”.
    h. In “Edit Application Policies Extension”, click “OK”.
    i. In the “Properties of New Template” dialog box, click “OK”.

2.2 Configure Template for OTP Certificates Issued by the Corporate CA

This template will be used to issue certificates from the CA root.

1. The Certificate Templates Console should still be open on the enterprise certificate server; if not, open it.
2. In details pane, right-click the “Smartcard Logon” template and select “Duplicate Template”.
3. In the “Properties of New Template” dialog box, navigate to Certification Authority|Compatibility, click “Windows Server 2012”.
4. In the “Resulting changes” dialog box, click “OK”.
5. In the “Certificate recipient” list click “Windows 8/Windows Server 2012”.
6. In the “Resulting changes” dialog box click “OK”.
7. In the “Properties of New Template” dialog box, click the “General” tab. Complete the following:
    a. In “Template display name”, enter “DAOTPLogon”.
    b. In the “Validity period” drop-down list, click “hours”.
    c. In the “Certificate Templates” dialog box, click “OK”.
    d. Make sure that the number of hours is set to “1”.
    e. In “Renewal period”, enter “0”.
    Note: In situations where the CA server is a Windows Server 2003 computer, then the template must be configured on a different computer. This is due to the fact that setting the “Validity period” in hours is not possible when running

Windows versions prior to 2008/Vista. If the computer that you use to configure the template does not have the Certification Service role installed, or it is a client computer, then you may need to install the Certificate Templates snap-in. For more information on this subject refer to http://technet.microsoft.com/en-us/library/cc732445.aspx

8. Click the "Security" tab, select "Authenticated Users", and complete the following:
    a. In the "Allow" column, and select the "Read" and "Enroll" check boxes.
    b. Click "OK".
    c. Click "Full Control" under the "Allow" column.
    d. Click "Domain Admins" and "Enterprise Admins", and then click "Full Control" under the Allow column for both.
    e. Click "Apply".
9. Click the "Subject Name" tab, and complete the following:
    a. Click "Build from this Active Directory information".
    b. In the "Subject name format" list, select "Fully distinguished name".
    c. Make sure that the "User principal name (UPN)" box is checked.
    d. Click "Apply".
10. Click the "Server" tab and complete the following:
    a. Select the "Do not store certificates and requests in the CA database" check box.
    b. Clear the "Do not include revocation information in issued certificates" check box.
    c. In the "Properties of New Template" dialog box, click "Apply".
11. Click the "Issuance Requirements" tab, and complete the following:
    a. Select the "This number of authorized signatures" check box.
    b. Set the value to "1".
    c. In the "Policy type required in signature" list, select "Application policy".
    d. In the "Application policy" list select "DA OTP RA".
    e. In the "Properties of New Template" dialog box, click "OK".
12. Click the "Extensions" tab, and complete the following:
    a. In "Application Policies" click "Edit".
    b. Delete "Client Authentication".
    c. Keep "SmartCardLogon".
    d. Click "OK" twice.
13. Close the Certificate Templates Console.
14. Click "Start" on the desktop.
15. In the search box, enter "certsrv.msc".
16. In the Certification Authority console tree, completer the following:
    a. Expand the tree in the navigation pane..
    b. Click "Certificate Templates".
    c. Right-click "Certificate Templates", point to "New", and click "Certificate Template to Issue".

17. In the list of certificate templates, click “DAOTPRA” and “DAOTPLogon”, and click “OK”.
18. In the details pane of the console, you should see:
    - The “DAOTPRA” certificate template with an “Intended purpose” of “DA OTP RA.”
    - The “DAOTPLogon” certificate template with an “Intended Purpose” of “Smart Card Logon, Client Authentication”.
19. Restart the services.
20. Close the Certification Authority console.
21. Open an elevated command prompt. Enter “CertUtil.exe –SetReg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS”.

This completes configuration steps on the enterprise certificate server. Next you will set up HOTPin Server DA requirements.

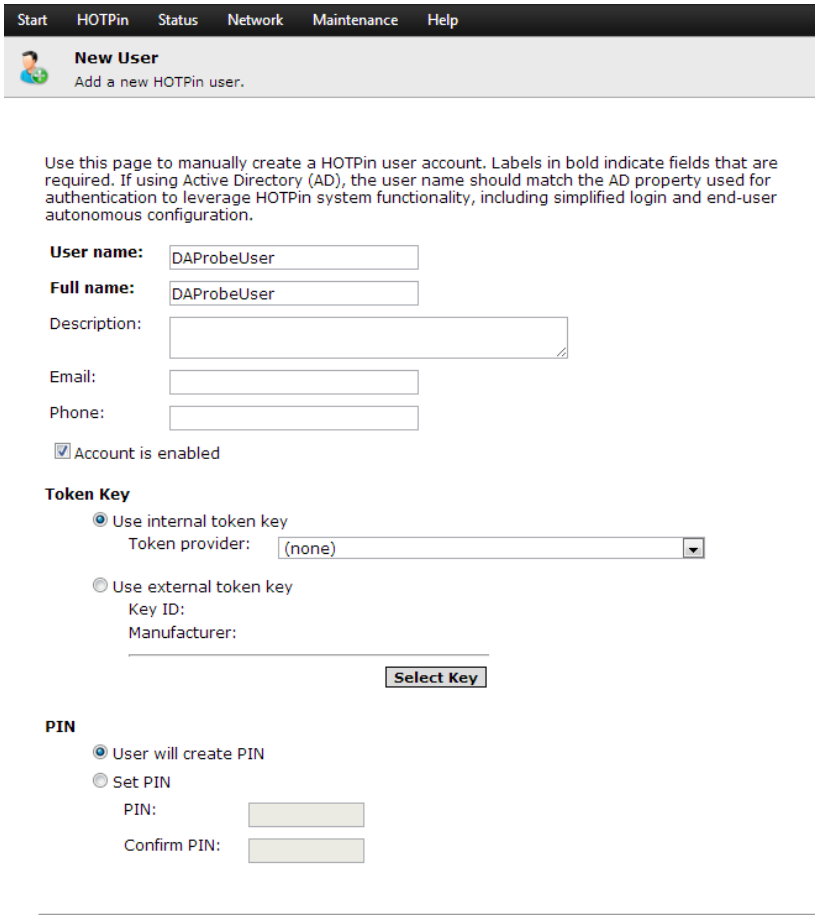
3 HOTPin Server Configuration

HOTPin configuration includes setting up a user account for DA use and adding a RADIUS client.

3.1 Add a HOTPin Account for DA

You need configure a HOTPin account that DA will use as a probe mechanism. The mechanism facilitates using DA as a HOTPin RADIUS client.

1. Open the HOTPin Server web UI.
2. Navigate to Users|New.
3. Create a user with the name “DAProbeUser”
   Important: This account is required for DA probe only; it should not be used for authentication or anything else.
   Note: If PINs are required for accounts, the PIN can be set to any value.
   See the illustration for reference:



3.2 Configure DA as a RADIUS Client

HOTPin uses RADIUS to serve as an OTP server for DA. The following instructions explain how to add DA as a HOTPin RADIUS client.

Note: Only configuration applicable to a basic deployment is discussed.

1. Navigate to HOTPin|NPS RADIUS|RADIUS Clients.
2. Click “New”.
3. The RADIUS Clients screen opens.
4. On the “Settings” tab, complete the following:
    a. Enable this RADIUS client – select.
    b. Friendly name – enter a descriptive name to help identify the NAS.
    c. Address (IP or DNS) – the client address can be either the IP address or DNS name.
    Note: If using the DNS name, it must be resolvable from the HOTPin server; otherwise, use the IP address.
    d. Shared Secret – enter a password for use between RADIUS components (clients, proxies, and servers); can include up to 64 characters:

- Select “Manual” to create your own entry.
- Select “Generate” and click the “Generate” button to create one automatically.

Important: The shared secret will need to be entered on the DA server, so take note of the string value before completing the client configuration. To reveal an entry, select “Change shared secret”, then select “Generate”; the shared secret string will display in the text field.

5. Click “OK”.

This completes configuration steps on HOTPin Server. Next you will set up the DA server for 2FA.

4 DirectAccess OTP Support Configuration

The following instructions provide the configuration steps to add HOTPin as the OTP server. Topics also include steps to confirm configuration for necessary components.

4.1 Configure HOTPin as an OTP Server

You need to add HOTPin as an OTP RADIUS server to facilitate 2FA.

1. On the DA server, open “Server Manager”, and click “Remote Access Management” in the left pane.
2. Click “Configuration”.
3. In the “DirectAccess Setup” window, click “Edit” under “Step 2 – Remote Access Server”. Complete the following:
4. Select “Authentication” in the navigation pane.
5. Select “Two factor authentication” and “Use OTP”.

   Important:
   - Ensure that “Use computer certificates” is checked.
   - Verify that the root CA is set to “CN=*(corp)*-APP-CA”, where *(corp)* is replaced with the certificate authority server name.
6. Click “Next”.
7. In the “OTP RADIUS Server” section, double-click the blank “Server Name” field.
8. In the “Add a RADIUS Server” dialog, complete the following:
   a. Enter “HOTPin” in the “Server name” field.
   b. Click “Change” next to the “Shared secret” field, enter the same password that you created when configuring the HOTPin server RADIUS client.
   c. Click “OK” twice, and then click “Next”.

   Note: If the RADIUS server is in a domain that is different than the Remote Access server, then the “Server Name” field must specify the FQDN of the RADIUS server.
9. In the “OTP CA Servers” section select the name of your CA server, then click “Add”.

10. Click “Next”.
11. On the “OTP Certificate Templates” page, complete the following:
    a. Click “Browse” to select the certificate template for OTP authentication enrolment.
    b. In the “Certificate Templates” dialog box, select “DAOTPLogon”.
    c. Click “OK”.
    d. Click “Browse” to select the certificate template for Remote Access server enrolment.
    e. In the “Certificate Templates” dialog box select “DAOTPRA”.
    f. Click Ok.
12. Click Next.
13. On the “Remote Access Server Setup” page click “Finish”.
14. Click “Finish” on the “DirectAccess Expert Wizard”.
15. On the “Remote Access Review” dialog box click “Apply”, then wait for the DA policy to be updated.
16. Click “Close”.
17. Click “Start” on the desktop. Complete the following:
    a. In the search box, type “powershell.exe”.
    b. Right-click “powershell”.
    c. Click “Advanced”.
    d. Click “Run as administrator”.
       If the UAC dialog box appears, review and then confirm the action.
    e. In the Windows PowerShell window, type “gpupdate /force” and press ENTER.
18. Close and reopen the Remote Access Management Console and verify that all OTP settings are correct.

4.2 Confirm Remote Access Setup for the Certificate Server

You need to confirm that the enterprise certificate server is included in DA Remote Access setup.

1. If the Remote Access Management Console is not still open, navigate to Server Manager|Remote Access Management|Configuration.
2. Click “Edit” in “Step 3”.
3. Select “Management” in the Infrastructure Server Setup dialog box.
4. Make sure the enterprise certificate server is listed under “Management Servers”. If it’s not listed, you need to add it.

4.3 Verify OTP Server Configuration

You can use DA health monitoring to check the HOTPin Server status.

1. On the DAX appliance, open the “Remote Access Management” console.
2. Click “Operations Status”.
3. Verify that the status of OTP server is “Working”.

4.4 Test OTP Functionality from a Client on the External Subnet

The following are 2FA login instructions for both Windows 7 and 8 clients. They assume that PINS are required for login passcodes.

4.4.1 Windows 8

1. On a Windows 8 client computer, make sure that you are logged on with a valid domain user/HOTPin account.
2. Click the “Network connections” icon in the notification area to access the DA Media Manager.
3. Click “Workplace Connection” or any other name specified in the DA configuration, and click “Continue”.
4. Press Control+Alt+Delete, and click the “One-time password (OTP)” tile.
5. Enter a valid PIN & OTP and click “OK”.
6. Wait for authentication to complete. The DirectAccess Workplace Connection status will be “Connected”.
7. Access any published application or intranet resource to verify connection to corporate resources.

4.4.2 Windows 7

1. On a Windows 7 client computer, make sure that you are logged on with a valid domain user/HOTPin account.
2. Click the “DirectAccess Connectivity Assistant” icon in the notification area to access the DA Client.
3. Click “Lock and unlock your computer with a smartcard or a one-time password” when prompted.

   Note: Two-factor authentication requires the lock/unlock process to establish a connection with the network.
4. Press Control+Alt+Delete to open the login prompt.
5. Click “One-time password”.
6. Enter the password for the logged in user account.
7. When prompted for smart card credentials, click “One-Time password (OTP)”.
8. Enter a valid PIN & OTP and click “OK”.

9. Wait for authentication to complete. The DirectAccess Connectivity Assistant status will be "Connected".
10. Access any published application or intranet resource to verify connection to corporate resources.

You have completed the steps necessary to set up a basic deployment of HOTPin two-factor authentication for DirectAccess.