SafeNet Authentication Service
Integration Guide

SAS Using RADIUS Protocol with Microsoft DirectAccess
SafeNet Authentication Service: Integration Guide
SAS Using RADIUS Protocol with Microsoft DirectAccess

Document Information

<table>
<thead>
<tr>
<th>Document Part Number</th>
<th>007-012842-001, Rev. A</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date</td>
<td>November 2014</td>
</tr>
</tbody>
</table>

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017, USA</td>
</tr>
<tr>
<td>Email</td>
<td><a href="mailto:TechPubs@safenet-inc.com">TechPubs@safenet-inc.com</a></td>
</tr>
</tbody>
</table>
# Contents

Third-Party Software Acknowledgement.............................................................................................................. 4  
Description.......................................................................................................................................................... 4  
Applicability....................................................................................................................................................... 4  
Environment ..................................................................................................................................................... 4  
Audience.............................................................................................................................................................. 5  
RADIUS-based Authentication using SAS Cloud................................................................................................. 5  
RADIUS-based Authentication using SAS-SPE and SAS-PCE............................................................................. 6  
RADIUS Authentication Flow using SAS ............................................................................................................. 6  
RADIUS Prerequisites......................................................................................................................................... 7  
Configuring SafeNet Authentication Service...................................................................................................... 7  
  Synchronizing User Stores to SafeNet Authentication Service ................................................................................. 7  
  Assigning Authenticator in SAS .......................................................................................................................... 8  
  Adding Microsoft DirectAccess as an Authentication Node in SAS ................................................................. 9  
  Checking the SAS RADIUS IP Address ........................................................................................................... 11  
  Creating DAProbeUser ...................................................................................................................................... 12  
Configuring Microsoft DirectAccess .................................................................................................................. 13  
  Creating and Deploying a Certificate Template for Signing the OTP Certificate Requests ........................... 13  
  Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA .................. 20  
  Configuring OTP for DirectAccess .................................................................................................................. 29  
  Confirming DirectAccess Configuration for OTP ........................................................................................... 30  
  Configuring the DirectAccess Client ................................................................................................................. 30  
Running the Solution ........................................................................................................................................ 31  
Troubleshooting................................................................................................................................................ 33  
  DirectAccess Not Prompting for OTP Credentials ............................................................................................. 33  
Support Contacts................................................................................................................................................ 37
Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft DirectAccess.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Service delivers a fully automated, versatile, and strong authentication-as-a-service solution.

With no infrastructure required, SafeNet Authentication Service provides smooth management processes and highly flexible security policies, token choice, and integration APIs.

DirectAccess is a VPN-like technology that provides intranet connectivity to the client computers when they are connected to the Internet. Unlike many traditional VPN connections, which must be initiated and terminated by explicit user action, DirectAccess connections are designed to connect automatically as soon as the computer connects to the Internet. DirectAccess was introduced in Windows Server 2008 R2, providing this service to Windows 7 and Windows 8 Enterprise edition clients.

This document describes how to:

- Configure Microsoft DirectAccess to work with SafeNet Authentication Service in RADIUS mode.

It is assumed that the Microsoft DirectAccess environment is already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Service.

Microsoft DirectAccess can be configured to support multi-factor authentication in several modes. The RADIUS protocol will be used for the purpose of working with SafeNet Authentication Service.

Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** — SafeNet’s cloud-based authentication service.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** — A server version that is used by Service Providers to deploy instances of SafeNet Authentication Service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** — A server version that is used to deploy the solution on-premises in the organization.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Service** — SafeNet’s cloud-based authentication service
- **Microsoft DirectAccess** - Windows Server 2012 R2
Audience

This document is targeted to system administrators who are familiar with Microsoft DirectAccess and are interested in adding multi-factor authentication capabilities using SafeNet Authentication Service.

RADIUS-based Authentication using SAS Cloud

SAS Cloud provides two RADIUS mode topologies:

- **SAS cloud hosted RADIUS service** – A RADIUS service that is already implemented in the SAS cloud environment and can be used without any installation or configuration requirements.

- **Local RADIUS hosted on-premises** - A RADIUS agent that is implemented in the existing customer’s RADIUS environment. The agent forwards the RADIUS authentication requests to the SAS cloud environment. The RADIUS agent can be implemented on a Microsoft NPS/IAS or FreeRADIUS server.

For more information on how to install and configure SAS Agent for IAS/NPS, refer to: http://www2.safenet-inc.com/sas/implementation-guides/sfnt-updates/SAS-Agents-IASNPS.pdf

For more details on how to install and configure FreeRADIUS, refer to the **SAS FreeRADIUS Agent Configuration Guide**.

This document demonstrates the solution using the SAS cloud hosted RADIUS service.
RADIUS-based Authentication using SAS-SPE and SAS-PCE

In addition to the pure cloud-based offering, SafeNet Authentication Service comes with two on-premises versions:

- **SafeNet Authentication Service – Service Provider Edition (SPE)** – An on-premises version of SafeNet Authentication Service targeted at service providers interested in hosting SAS in their data center.

- **SafeNet Authentication Service – Private Cloud Edition (PCE)** – An on-premises version of SafeNet Authentication Service targeted at organizations interested in hosting SAS in their private cloud environment.

For both on-premises versions, SAS can be integrated with the following solutions that serve as local RADIUS servers:

- **Microsoft Network Policy Server (MS-NPS) or the legacy Microsoft Internet Authentication Service (MS-IAS)** — SafeNet Authentication Service is integrated with the local RADIUS servers using a special on-premises agent called SAS Agent for Microsoft IAS and NPS.
  
  For more information on how to install and configure the SAS Agent for Microsoft IAS and NPS, refer to the following document:
  

- **FreeRADIUS** — The SAS FreeRADIUS Agent is a strong authentication agent that is able to communicate with SAS through the RADIUS protocol.

  For more information on how to install and configure the SAS FreeRADIUS Agent, refer to the SafeNet Support Portal.

RADIUS Authentication Flow using SAS

SafeNet Authentication Service communicates with a large number of VPN and access-gateway solutions using the RADIUS protocol.

The image below describes the dataflow of a multi-factor authentication transaction for Microsoft DirectAccess.

1. A user attempts to log on to Microsoft DirectAccess using an OTP authenticator.
2. Microsoft DirectAccess sends a RADIUS request with the user’s credentials to SafeNet Authentication Service for validation.
3. The SAS authentication reply is sent back to Microsoft DirectAccess.
4. The user is granted or denied access to Microsoft DirectAccess based on the OTP value calculation results from SAS.
RADIUS Prerequisites

To enable SafeNet Authentication Service to receive RADIUS requests from Microsoft DirectAccess, ensure the following:

- End users can authenticate through the Microsoft DirectAccess environment with a static password before configuring the Microsoft DirectAccess to use RADIUS authentication.
- Port 1812 is open to and from Microsoft DirectAccess.
- A shared secret key has been selected, providing an added layer of security by supplying an indirect reference to a shared secret key. It is used by a mutual agreement between the RADIUS server and the RADIUS client for encryption, decryption, and digital signature purposes.
- The user **DAProbeUser** exists in SAS. For more information, refer to the section “Creating DAProbeUser” on page 12.

**NOTE:** For RADIUS authentication, DirectAccess should be set up using this guide: http://www.microsoft.com/en-us/download/details.aspx?id=29031

**NOTE:** RADIUS authentication does not work with DirectAccess set up on a single server.

Configuring SafeNet Authentication Service

The deployment of multi-factor authentication using SAS with Microsoft DirectAccess using the RADIUS protocol requires the following:

- Synchronizing User Stores to SAS
- Assigning Authenticator in SAS
- Adding Microsoft DirectAccess as an Authentication Node in SAS
- Checking the SAS RADIUS IP address
- Creating DAProbeUser

Synchronizing User Stores to SafeNet Authentication Service

Before SAS can authenticate any user in your organization, you must create a user store in SAS that reflects the users that would need to use multi-factor authentication. User records are created in the SAS user store using one of the following methods:

- Manually, one user at a time using the **Create User** shortcut
- Manually, by importing one or more user records via a flat file
- Automatically, by synchronizing with your Active Directory / LDAP server using the SAS Synchronization Agent
For further details on importing users to SafeNet Authentication Service, refer to the section on “creating users” in the SafeNet Authentication Service Subscriber Account Operator Guide.


All SafeNet Authentication Service documentation can be found on the SafeNet Knowledge Base site.

Assigning Authenticator in SAS

SAS supports a number of authentication methods that can be used as second authentication factor for users who are authenticating through Microsoft DirectAccess.

The following authenticators are supported:

- eToken PASS
- KT-4 token
- SMS token
- MP-1 software token
- MobilePASS

Authenticators can be assigned to users in two ways:

- **Manual provisioning** – Assign an authenticator to users one by one.
- **Provisioning rules** – The administrator can set provisioning rules in SAS so that the rules will be triggered when group memberships and other user attributes change; an authenticator will be assigned automatically to the user.

Refer to “provisioning rules” in the SafeNet Authentication Service - Subscriber Account Operator Guide to learn how to provision the different authentication methods to the users in the SAS user store.

Adding Microsoft DirectAccess as an Authentication Node in SAS

Add a RADIUS entry in the SAS Authentication Nodes module to prepare it to receive RADIUS authentication requests from Microsoft DirectAccess. You will need the IP address of Microsoft DirectAccess and the shared secret to be used by both SAS and Microsoft DirectAccess.

**To add an Authentication Node in SAS:**

1. Log in to the SAS console with an Operator account.

2. Click the **COMMS** tab, and then select the **Auth Nodes** module.

3. In the **Auth Nodes** module, click the **Auth Nodes** link.
4. Click **Add**.

5. In the **Add Auth Nodes** section, complete the following fields, and then click **Save**:

   - **Agent Description**: Enter a host description.
   - **Host Name**: Enter the name of the host that will authenticate with SAS.
   - **Low IP Address In Range**: Enter the IP address of the host.
   - **Configure FreeRADIUS Synchronization**: Select this option.
   - **Shared Secret**: Enter the shared secret key.
   - **Confirm Shared Secret**: Re-enter the shared secret key to confirm it.

The Auth Node is added to the system.
Checking the SAS RADIUS IP Address

Before adding SafeNet Authentication Service as a RADIUS server in Microsoft DirectAccess, check the IP address of the SAS RADIUS server. The IP address will then be added to Microsoft DirectAccess as a RADIUS server at a later stage.

To check the IP address of the SAS RADIUS server:

1. Log in to the SAS console with an Operator account.

2. Click the COMMS tab, and then select the Auth Nodes module.

3. Click the Auth Nodes link.
The SAS RADIUS server details are displayed.

Creating DAProbeUser

DirectAccess uses an internal built-in user, **DAProbeUser**, to check the RADIUS connectivity. There is no need to allocate a token to **DAProbeUser**. You must create a user with the same name in SAS.

1. Log in to the SAS console with an Operator account.
2. In the left pane, click **Create User**.

3. On the **Create User** window, complete the following, and then click **Add**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name</td>
<td>Enter the first name of the user.</td>
</tr>
<tr>
<td>Last Name</td>
<td>Enter the last name of the user.</td>
</tr>
<tr>
<td>User ID</td>
<td>Enter <strong>DAProbeUser</strong>.</td>
</tr>
<tr>
<td>E-mail</td>
<td>Enter the email ID of the user.</td>
</tr>
</tbody>
</table>

![Create User window](image)
Configuring Microsoft DirectAccess

Configuring Microsoft DirectAccess for RADIUS authentication requires the following:

- Creating and Deploying a Certificate Template for Signing the OTP Certificate Requests—page 13
- Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA—page 20
- Configuring OTP for DirectAccess—page 29
- Confirming DirectAccess Configuration for OTP—page 30
- Configuring the DirectAccess Client—page 30

Creating and Deploying a Certificate Template for Signing the OTP Certificate Requests

You must create and configure a certificate template, which will be used to sign the OTP certificate requests.

1. Log in to the system on which the Certificate Authority server is installed.
2. Start the Windows Command Prompt application, and run the `certtmpl.msc` application.
3. On the Certificate Templates Console window, right-click the Computer template, and then click Duplicate Template.
4. On the **Properties of New Template** window, on the **Compatibility** tab, complete the following fields.

| Certificate Authority | Select an appropriate Certification Authority; for example, **Windows Server 2012**. On the **Resulting changes** window, click **OK**. |
| Certificate recipient  | Select an appropriate Certificate recipient; for example, **Windows 8/Windows Server 2012**. On the **Resulting changes** window, click **OK**. |

![Properties of New Template](image)

- **Subject Name**
- **Server**
- **Issuer Requirements**
  - **Superseded Templates**
  - **Extensions**
  - **Security**
- **Compatibility**
  - **General**
  - **Request Handling**
  - **Cryptography**
  - **Key Attestation**

The template options available are based on the earliest operating system versions set in Compatibility Settings.

- **Show resulting changes**

**Compatibility Settings**

- **Certification Authority**
  - Windows Server 2012
- **Certificate recipient**
  - Windows 8 / Windows Server 2012

These settings may not prevent earlier operating systems from using this template.
5. On the **Properties of New Template** window, on the **General** tab, complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template display name</td>
<td>Enter the template name for display; for example, <strong>DAOTPRA</strong>.</td>
</tr>
<tr>
<td>Validity period</td>
<td>Set the validity period to 2 days.</td>
</tr>
<tr>
<td>Renewal period</td>
<td>Set the renewal period to 1 day.</td>
</tr>
</tbody>
</table>

**NOTE:** If the Certificate Templates warning is displayed, click **OK**.

![Properties of New Template](image)
6. On the **Properties of New Template** window, on the **Security** tab, click **Add**.

![Properties of New Template](image1.png)

7. On the **Select Users, Computers, Service Accounts, or Groups** window, perform the following steps:
   a. Click **Object Types**.
   b. On the **Object Types** window, select **Computers**, and then click **OK**.
   c. In the **Enter the object names to select** field, enter the name of server on which DirectAccess is configured, and then click **OK**.

![Select Users, Computers, Service Accounts, or Groups](image2.png)
8. On the **Properties of New Template** window, on the **Security** tab, select a group or a user in the **Group or user names** section and then set permissions for that group or user in the **Permissions** section, as explained in the table below:

<table>
<thead>
<tr>
<th>Group or user names</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA</td>
<td>Set only the <strong>Read</strong>, <strong>Enroll</strong>, and <strong>Autoenroll</strong> permissions.</td>
</tr>
<tr>
<td>Authenticated Users</td>
<td>Set only the <strong>Read</strong> permission.</td>
</tr>
<tr>
<td>Domain Computers</td>
<td>Remove the <strong>Enroll</strong> permission and keep the other default permissions.</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Set the <strong>Full Control</strong> permission.</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>Set the <strong>Full Control</strong> permission.</td>
</tr>
</tbody>
</table>

![Properties of New Template window](image-url)
9. On the Properties of New Template window, on the Subject Name tab, perform the following, and then click Apply:
   a. Select Build from this Active Directory information.
   b. In the Subject name format field, select DNS name.
   c. Under Include this information in alternate subject name, select DNS name.
10. On the **Properties of New Template** window, on the **Extensions** tab, perform the following steps, and then click **OK**.

   a. In the **Extensions included in the template** list, select **Application Policies**, and then click **Edit**.
   
   b. On the **Edit Application Policies Extension** window, remove all the existing application policies, and then click **Add**.
   
   c. On the **Add Application Policy** window, click **New**, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter DAOTPRA.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Object identifier</td>
<td>Enter 1.3.6.1.4.1.311.81.1.1.</td>
</tr>
</tbody>
</table>

   d. On the **Add Application Policy** window, click **OK**.
   
   e. On the **Edit Application Policies Extension** window, click **OK**.

![Properties of New Template](image)
Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA

You must create and configure a certificate template for OTP certificates, which is issued by the corporate Certificate Authority.

1. Log in to the system on which the Certificate Authority server is installed.
2. Start the **Windows Command Prompt** application, and run the `certtmpl.msc` application.
3. On the **Certificate Templates Console** window, right-click the **Smartcard Logon** template, and then click **Duplicate Template**.

<table>
<thead>
<tr>
<th>Template Display Name</th>
<th>Schema Version</th>
<th>Version</th>
<th>Intended Purposes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Authenticated Session</td>
<td>1</td>
<td>3.1</td>
<td></td>
</tr>
<tr>
<td>Basic EPS</td>
<td>1</td>
<td>3.1</td>
<td></td>
</tr>
<tr>
<td>CA Exchange</td>
<td>2</td>
<td>105.0</td>
<td>Private Key Archival</td>
</tr>
<tr>
<td>CEP Encryption</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Code Signing</td>
<td>1</td>
<td>3.1</td>
<td></td>
</tr>
<tr>
<td>Computer</td>
<td>1</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>Cross Certification Authority</td>
<td>2</td>
<td>105.0</td>
<td></td>
</tr>
<tr>
<td>Directory Email Replication</td>
<td>1</td>
<td>115.0</td>
<td>Directory Service Email Replica</td>
</tr>
<tr>
<td>Domain Controller</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Domain Controller Authentication</td>
<td>2</td>
<td>110.0</td>
<td>Client Authentication, Server A</td>
</tr>
<tr>
<td>EFS Recovery Agent</td>
<td>1</td>
<td>6.1</td>
<td></td>
</tr>
<tr>
<td>Enrollment Agent</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Enrollment Agent (Computer)</td>
<td>1</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>Exchange Enrollment Agent (Offline request)</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Exchange Signature Only</td>
<td>1</td>
<td>6.1</td>
<td></td>
</tr>
<tr>
<td>Exchange User</td>
<td>1</td>
<td>7.1</td>
<td></td>
</tr>
<tr>
<td>IPSec</td>
<td>1</td>
<td>8.1</td>
<td></td>
</tr>
<tr>
<td>IPSec (Offline request)</td>
<td>1</td>
<td>7.1</td>
<td></td>
</tr>
<tr>
<td>Kerberos Authentication</td>
<td>2</td>
<td>110.0</td>
<td>Client Authentication, Server A</td>
</tr>
<tr>
<td>Key Recovery Agent</td>
<td>2</td>
<td>105.0</td>
<td>Key Recovery Agent</td>
</tr>
<tr>
<td>OCSP Response Signing</td>
<td>3</td>
<td>101.0</td>
<td>OCSP Signing</td>
</tr>
<tr>
<td>RAS and IAS Server</td>
<td>2</td>
<td>101.0</td>
<td>Client Authentication, Server A</td>
</tr>
<tr>
<td>Root Certification Authority</td>
<td>1</td>
<td>5.1</td>
<td></td>
</tr>
<tr>
<td>Router (Offline request)</td>
<td>1</td>
<td>4.1</td>
<td></td>
</tr>
<tr>
<td>Smartcard Logon</td>
<td>1</td>
<td>6.1</td>
<td></td>
</tr>
<tr>
<td>Smartcard User</td>
<td>1</td>
<td>11.1</td>
<td></td>
</tr>
</tbody>
</table>
4. On the **Properties of New Template** window, on the **Compatibility** tab, complete the following fields.

| Certificate Authority | Select an appropriate Certification Authority; for example, **Windows Server 2012**. On the **Resulting changes** window, click **OK**. |
| Certificate recipient | Select an appropriate Certificate recipient; for example, **Windows 8/Windows Server 2012**. On the **Resulting changes** window, click **OK**. |
5. On the Properties of New Template window, on the General tab, complete the following fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template display name</td>
<td>Enter the template name for display; for example, DAOTPLogon.</td>
</tr>
<tr>
<td>Validity period</td>
<td>Set the validity period to 1 hour.</td>
</tr>
<tr>
<td>Renewal period</td>
<td>Set the renewal period to 0 hour.</td>
</tr>
</tbody>
</table>

6. On the Properties of New Template window, on the Security tab, select a group or a user in the Group or user names section and then set permissions for that group or user in the Permissions section, as explained in the table below:

<table>
<thead>
<tr>
<th>Group or user names</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticated Users</td>
<td>Set only the Read and Enroll permissions.</td>
</tr>
<tr>
<td>Domain Admins</td>
<td>Set the Full Control permission.</td>
</tr>
<tr>
<td>Enterprise Admins</td>
<td>Set the Full Control permission.</td>
</tr>
</tbody>
</table>

![Properties of New Template Window](image_url)
7. On the **Properties of New Template** window, on the **Subject Name** tab, perform the following steps, and then click **Apply**:
   a. Select **Build from this Active Directory information**.
   b. In the **Subject name format** field, select **Fully distinguished name**.
   c. Under **Include this information in alternate subject name**, select **User principal name (UPN)**.
8. On the **Properties of New Template** window, on the **Server** tab, perform the following steps, and then click **Apply**:
   a. Select **Do not store certificates and requests in the CA database**.
   b. Clear **Do not include revocation information in issued certificates**.
9. On the **Properties of New Template** window, on the **Issuance Requirements** tab, complete the following fields, and then click **Apply**:

<table>
<thead>
<tr>
<th>This number of authorized signatures</th>
<th>Select this option and then set the value to 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy type required in signature</td>
<td>Select <strong>Application policy</strong>.</td>
</tr>
<tr>
<td>Application policy</td>
<td>Select <strong>DAOTPRA</strong>.</td>
</tr>
</tbody>
</table>

![Properties of New Template window](image)
10. On the **Properties of New Template** window, on the Extensions tab, perform the following steps, and then click **OK**.
   a. In the **Extensions included in the template** list, select **Application Policies**, and then click **Edit**.
   b. On the **Edit Application Policies Extension** window, delete **Client Authentication** and keep **SmartCardLogon**.
   c. On the **Edit Application Policies Extension** window, click **OK**.

![Properties of New Template](image)

11. Close the **Certificate Templates Console** window.

12. Start the **Windows Command Prompt** application, and run the **certsrv.msc** application.
13. On the Certificate Authority window, in the left pane, expand Certification Authority, right-click Certificate Templates, and then click New > Certificate Template to Issue.

![Certificate Authority window](image)

14. On the Enable Certificate Templates window, select DAOTPRA and DAOTPLogon, and then click OK.

![Enable Certificate Templates window](image)
15. On the Certificate Authority window, in the right pane, the DAOTPRA and DAOTPLogon certificate templates are added.

![Certificate Authority window](image)

16. Restart the Certification Authority services.

17. Close the Certificate Authority window.

18. Start the Windows Command Prompt application as an administrator, and run the following command:

```
CertUtil.exe –SetReg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

## Configuring OTP for DirectAccess

To configure OTP authentication for DirectAccess:

1. Log in to the server on which DirectAccess is installed.
2. Run **PowerShell** as an administrator, and run the following command:

```
```

Where,

- **RADIUS server name/IP Address** is the FQDN of the RADIUS server or its IP address.
- **Shared Secret** is the shared password used for communication between the RADIUS server and DirectAccess.
- **Certificate Authority Name** is the Certification Authority (CA) servers that issue certificates for OTP authentication. Specify a server in the following format:
  
  `-- CAServer_Name\CAService_Name`

- **Certificate Template Name** is the name of the certificate template configured in the section “Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA” on page 20.

- **Signing Certificate Template Name** is the name of the certificate template configured in the section: “Creating and Deploying a Certificate Template for Signing the OTP Certificate Requests” on page 13.

**NOTE:** The same steps can be done using the Remote Access Management Console as well. Currently, Windows Server 2012 R2 does not automatically detect CAServer. Thus, the PowerShell command is used to configure OTP for DirectAccess.
Confirming DirectAccess Configuration for OTP

Verify whether the configurations for OTP on DirectAccess were successfully applied or not.

2. In the left pane, click **Operations Status**.

3. In the right pane, verify that the status of OTP is **Working**.

Configuring the DirectAccess Client

Update the group policies of DirectAccess client to receive the DirectAccess settings.

1. Connect the DirectAccess client to the corporate network.
2. Open **PowerShell** as an administrator.
3. Type `Get-DnsClientNrptPolicy` and press **ENTER**. The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed.
4. Type `Get-NCSIPolicyConfiguration` and press **ENTER**. The network connectivity status indicator settings deployed by the wizard are displayed.
5. Type `gpupdate /force` and press **ENTER**.
Running the Solution

To run the DirectAccess solution with SafeNet Authentication Service, perform the following steps:

1. Connect the DirectAccess client to the Internet.
2. In the System Notification area, click the network icon. Click the name of the DirectAccess connection and then click Continue.

3. When a message is shown to press Ctrl+Alt+Delete to enter the credentials, do so.
4. Click One-time password (OTP).

5. Generate the OTP and enter it in the Enter your OTP credentials field. Click OK.

If the credentials are correct, the user will be logged in and will get connected to DirectAccess.
Troubleshooting

DirectAccess Not Prompting for OTP Credentials

Even when DirectAccess is configured for two-factor authentication, the client machine may not ask for the OTP and gets automatically connected to the DirectAccess server. This can happen because the client machine has access to internal resources without OTP authentication. To troubleshoot this problem, perform the following steps:

1. Log in to the machine on which the Domain Name Server is present, and then open DNS Manager.

![DNS Manager screenshot](image-url)
2. In the left pane, expand **Forward Lookup Zones**, right-click the Domain name and click **New Host (A or AAAA)**.

3. On the **New Host** window, enter a host name in the **Name** field (for example, **fileshare**) and then enter the IP address of NLS server in the **IP address** field. Click **Add Host**.
4. Log in to the machine on which DirectAccess is configured and open **Remote Access Management Console**.

5. On the **Remote Access Management Console** window, in the left pane, click **DirectAccess and VPN**. Under **Step 1**, click **Edit**.

6. In the left pane, click **Network Connectivity Assistant**.
7. In the right pane, right-click on the empty row, and then click **New**.

![Remote Access Setup](image)

8. On the **Configure Corporate Resources for NCA** window, enter the URL of the new host added (for example, `http://fileshare`), and then click **Validate**. If connectivity is successfully validated, click **Add**.

![Configure Corporate Resources for NCA](image)

9. Click **Finish**.

10. Click **Finish** again to apply the configuration.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>SafeNet, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td></td>
</tr>
<tr>
<td>United States</td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td>Technical Support</td>
<td></td>
</tr>
<tr>
<td>Customer Portal</td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td></td>
<td>Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.</td>
</tr>
</tbody>
</table>