SafeNet Authentication Manager
Integration Guide

SAM using RADIUS Protocol with Microsoft DirectAccess
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description ................................................................................................................................................................. 4
Applicability ............................................................................................................................................................... 4
Environment ................................................................................................................................................................. 4
Audience ....................................................................................................................................................................... 5
RADIUS-based Authentication using SAM .................................................................................................................. 5
RADIUS Authentication Flow using SAM .................................................................................................................. 5
RADIUS Prerequisites ................................................................................................................................................ 6
Configuring SafeNet Authentication Manager .......................................................................................................... 6
  Synchronizing User Stores to SafeNet Authentication Manager ........................................................................... 6
  Configuring SAM’s Connector for OTP Authentication .......................................................................................... 7
  Token Assignment in SAM ......................................................................................................................................... 7
  Adding DirectAccess as a RADIUS Client in IAS/NPS ........................................................................................... 8
  SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ........................................................................ 10
Configuring DirectAccess ........................................................................................................................................ 11
  Creating and Deploying a Certificate Template for Signing OTP Certificate Requests ........................................ 11
  Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA ............................. 18
  Configuring OTP for DirectAccess ........................................................................................................................ 27
  Confirming DirectAccess Configuration for OTP .................................................................................................. 28
  Configuring the DirectAccess Client ....................................................................................................................... 28
Running the Solution .................................................................................................................................................. 29
Troubleshooting ......................................................................................................................................................... 31
  DirectAccess Not Prompting for OTP Credentials ................................................................................................. 31
Support Contacts ......................................................................................................................................................... 34
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 Manager (SAM) is a versatile authentication solution that allows you to match the authentication method and form factor to your functional, security, and compliance requirements. Use this innovative management service to handle all authentication requests and to manage the token lifecycle.

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

This document describes how to:

- Deploy multi-factor authentication (MFA) options in Microsoft DirectAccess using SafeNet OTP tokens managed by SafeNet Authentication Manager.
- Configure Microsoft DirectAccess to work with SafeNet Authentication Manager 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 Manager and that the SafeNet Authentication Manager OTP plug-in for Microsoft RADIUS Client was installed as part of the simplified installation mode of SAM. For more information on SafeNet Authentication Manager Installation modes, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.

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 Manager.

Applicability

The information in this document applies to:

- SafeNet Authentication Manager - A server version of SAM 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 Manager 8.2 HF 493 – A server version of SAM that is used to deploy the solution on-premises in the organization.
- 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 Manager.

RADIUS-based Authentication using SAM

SafeNet's OTP architecture includes the SafeNet RADIUS server for back-end OTP authentication. This enables integration with any RADIUS-enabled gateway or application. The SafeNet RADIUS server accesses user information in the Active Directory infrastructure via SafeNet Authentication Manager (SAM).

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS, providing strong authenticated remote access through the IAS or NPS RADIUS server.

When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet OTP plug-in for Microsoft RADIUS Client, refer to SafeNet Authentication Manager 8.2 Administrator’s Guide.

RADIUS Authentication Flow using SAM

SafeNet Authentication Manager 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 Manager for validation.
3. The SAM 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 SAM.
RADIUS Prerequisites

To enable SafeNet Authentication Manager 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 Microsoft DirectAccess to use RADIUS authentication.
- The 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.
- A user DAProbeUser exists in SAM. Direct Access uses this user to check the RADIUS connectivity.


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

Configuring SafeNet Authentication Manager

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

- Synchronizing User Stores to SafeNet Authentication Manager—page 6
- Configuring SAM’s Connector for OTP Authentication—page 7
- Token Assignment in SAM—page 7
- Adding Microsoft DirectAccess as a RADIUS Client in IAS/NPS—page 8
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration—page 10

Synchronizing User Stores to SafeNet Authentication Manager

SAM manages and maintains OTP token information in its data store, including the token status, the OTP algorithm used to generate the OTP, and the token assignment to users. For user information, SAM can be integrated with an external user store. During the design process, it is important to identify which user store the organization is using, such as Microsoft Active Directory.

If the organization is not using an external user store, SAM uses an internal (“stand-alone”) user store created and maintained by the SAM server.

SAM 8.2 supports the following external user stores:

- Novell eDirectory
- Microsoft ADAM/AD LDS
- OpenLDAP
- Microsoft SQL Server 2005 and 2008
- IBM Lotus Domino
- IBM Tivoli Directory Server

**Configuring SAM’s Connector for OTP Authentication**

SafeNet Authentication Manager is based on open standards architecture with configurable connectors. This supports integration with a wide range of security applications, including network logon, VPN, web access, one-time password authentication, secure email, and data encryption.

If you selected the **Simplified OTP-only** configuration, SafeNet Authentication Manager is automatically configured with a typical OTP configuration, providing a working SafeNet Authentication Manager OTP solution.

The **Simplified OTP-only** configuration is as follows:

- **Connectors** - SAM Connector for OTP Authentication is installed
- **SAM Back-end Service** - Activated on this server; scheduled to operate every 24 hours

In addition, the SAM default policy is set as follows:

- OTP support (required for OTP) is selected in the **Token Initialization** settings.
- The **SAM Connector for OTP Authentication** is set, by default, to enable enrollment of OTP tokens without requiring changes in the TPO settings. For more information on how to install and configure the SafeNet Authentication Manager for simplified installation, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.

**Token Assignment in SAM**

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

The following tokens are supported:

- SafeNet eToken PASS
- SafeNet eToken NG-OTP
- SafeNet MobilePASS
- SafeNet MobilePASS Messaging
- SafeNet eToken 3400

Tokens can be assigned to users as follows:

- **SAM Management Center**: Management site used by SAM administrators and help desk for token enrollment and lifecycle management.
- **SAM Self-Service Center**: Self-service site used by end users for managing their tokens.
- **SAM Remote Service**: Self-service site used by employees not on the organization’s premises as a rescue website to manage cases where tokens are lost or passwords are forgotten.

For more information on SafeNet’s tokens and service portals, refer to the *SafeNet Authentication Manager 8.2 Administrator’s Guide*.
Adding Microsoft DirectAccess as a RADIUS Client in IAS/NPS

For Windows Server 2003, the Windows RADIUS service is Internet Authentication Service (IAS). The IAS is added as the RADIUS server in Microsoft DirectAccess.

For Windows Server 2008 and above, the Windows RADIUS service is the Microsoft Network Policy Server (NPS). The NPS server is added as the RADIUS server in Microsoft DirectAccess.

Microsoft DirectAccess must be added as a RADIUS client on the IAS/NPS server so that IAS/NPS will authorize Microsoft DirectAccess for authentication.

NOTE: It is assumed that IAS/NPS policies are already configured and working with static passwords prior to implementing multi-factor authentication using SafeNet Authentication Manager.

The details below refer to NPS, and are very similar to IAS.

To add a RADIUS client:
2. From the NPS web console, in the left pane, expand RADIUS Clients and Servers, right-click RADIUS Clients and then click New.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. On the **New RADIUS Client** window, complete the following fields on the **Settings** tab:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable this RADIUS client</strong></td>
<td>Select this option.</td>
</tr>
<tr>
<td><strong>Friendly name</strong></td>
<td>Enter a RADIUS client name.</td>
</tr>
<tr>
<td><strong>Address (IP or DNS)</strong></td>
<td>Enter the IP address or DNS of Microsoft DirectAccess.</td>
</tr>
<tr>
<td><strong>Manual/Generate</strong></td>
<td>Select <strong>Manual</strong>.</td>
</tr>
<tr>
<td><strong>Shared secret</strong></td>
<td>Enter the shared secret for the RADIUS client. The value must be the same</td>
</tr>
<tr>
<td></td>
<td>when configuring the RADIUS server in Microsoft DirectAccess.</td>
</tr>
<tr>
<td><strong>Confirm shared secret</strong></td>
<td>Re-enter the shared secret to confirm it.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)

4. Click **OK**.

Microsoft DirectAccess is added as a RADIUS client in NPS.
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration

RADIUS protocol is used for authentication and authorization. The SafeNet OTP solution supports the Microsoft IAS service (used in Windows 2003) and Microsoft NPS service (used in Windows 2008 and later) as Windows services running a RADIUS server. These services may be extended by adding plug-ins for the authentication process.

SAM's OTP plug-in for Microsoft RADIUS Client works with Microsoft’s IAS or NPS to provide strong, authenticated remote access through the IAS or NPS RADIUS server. When configured, users who access their network remotely using IAS or NPS are prompted for a token-generated OTP passcode for network authentication.

For more information on how to install and configure the SafeNet Authentication Manager OTP plug-in, refer to the SafeNet Authentication Manager 8.2 Administrator’s Guide.
Configuring Microsoft DirectAccess

Configuring Microsoft DirectAccess for RADIUS authentication requires the following:

- Creating and Deploying a Certificate Template for Signing OTP Certificate Requests—page 11
- Creating and Deploying a Certificate Template for OTP Certificates Issued by Corporate CA—page 18
- Configuring OTP for DirectAccess—page 27
- Confirming DirectAccess Configuration for OTP—page 28
- Configuring the DirectAccess Client—page 28

Creating and Deploying a Certificate Template for Signing 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.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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**. |

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the **Properties of New Template** window, on the **General** tab, complete the following fields:

<table>
<thead>
<tr>
<th>Template display name</th>
<th>Enter the template name for display; for example, <strong>DAOTPRA</strong>.</th>
</tr>
</thead>
<tbody>
<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**.

---

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. On the **Properties of New Template** window, on the **Security** tab, click **Add**.

![Properties of New Template](image1)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

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)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
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>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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**. |

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. On the Properties of New Template window, on the General tab, complete the following fields.

<table>
<thead>
<tr>
<th>Template display name</th>
<th>Enter the template name for display; for example, DAOTPLogon.</th>
</tr>
</thead>
<tbody>
<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>

For more information on setting the Validity period and Renewal period, see http://technet.microsoft.com/en-us/library/hh831715.aspx.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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)**.

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
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**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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><strong>This number of authorized signatures</strong></th>
<th>Select this option and then set the value to 1.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy type required in signature</strong></td>
<td>Select Application policy.</td>
</tr>
<tr>
<td><strong>Application policy</strong></td>
<td>Select DAOTPRA.</td>
</tr>
</tbody>
</table>

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
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)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

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)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

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

![Enable Certificate Templates window](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
15. On the **Certificate Authority** window, in the right pane, the DAOTPRA and DAOTPLLogon certificate templates are added.

![Certificate Authority window](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

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 Signing OTP Certificate Requests” on page 18.

- **Signing Certificate Template Name** is the name of the certificate template configured in the section: “Creating and Deploying a Certificate Template for Signing OTP Certificate Requests” on page 11.

**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**.

![Remote Access Management Console](image)

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 Manager, 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 Screen](image1.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

2. In the left pane, expand Forward Lookup Zones, right-click the Domain name and click New Host (A or AAAA).

   ![Forward Lookup Zones](image2.png)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
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**.

   ![New Host window](image)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

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**.

   ![Remote Access Management Console](image)

   *(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
6. In the left pane, click **Network Connectivity Assistant**.

![Network Connectivity Assistant](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*

7. In the right pane, right-click on the empty row, and then click **New**.

![Network Connectivity Assistant](image)

*(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)*
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**.

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><strong>Address</strong></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><strong>Phone</strong></td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td><strong>Technical Support Customer Portal</strong></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>