Contacting SafeNet

We work closely with our reseller partners to offer the best worldwide technical support services. Your reseller is the first line of support when you have questions about products and services. However, if you require additional assistance you can contact the SafeNet technical support team helpdesk which is available 24 hours a day, seven days a week:

<table>
<thead>
<tr>
<th>Country/Region</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td>+1-800-545-6608</td>
</tr>
<tr>
<td>International</td>
<td>+1-410-931-7520</td>
</tr>
</tbody>
</table>

For further assistance submit additional questions to the SafeNet technical support team at the following web page:

http://c3.safenet-inc.com/secure.asp

For assistance via email to SafeNet technical support send the request to the following address:

support@safenet-inc.com

About This Guide

This guide provides instructions for setting up and administering SafeNet’s strong authentication solution to enable certificate-based (CBA) or one-time password (OTP) user authentication to a VMware View environment.

The information in this guide includes the following:

- Solution requirements and deployment scenarios for SafeNet CBA and OTP solutions, including specific issues related to large deployments
- Step-by-step instructions for implementing the SafeNet CBA solution
- Step-by-step instructions for implementing the SafeNet OTP solution

Note

In this document, the following terms are used interchangeably:

- authenticator and token
- View Manager and View Connection Server
Target Audience

This guide is intended for information technology professionals responsible for the organization’s network security.

Additional Information

For a detailed reference guide to SAM 8.0 SP3, other SafeNet products mentioned in this guide, and the other infrastructure components involved in the solution, refer to the product-specific documentation.

For additional information on Microsoft and other VMware software and hardware components mentioned in this guide, refer to the relevant manufacturer’s documentation.
# Table of Contents

**Introduction** .................................................................................................................. 7

**Certificate-Based Authentication** .................................................................................. 9

  Solution Overview ................................................................................................. 9
  Software Requirements .......................................................................................... 10
  Token Requirements .............................................................................................. 10
  Key Activities ........................................................................................................... 11
  Authentication Flow for CBA Tokens .................................................................. 11
  Microsoft CA Configuration .................................................................................. 11
    Adding a Template to the CA ........................................................................ 11
    Changing a Template’s Minimum Key Size .................................................. 13
  SAM 8.0 SP3 Configuration .................................................................................. 14
    Installing and Configuring SAM .................................................................... 15
    Configuring SAM’s Connector for Microsoft CA ...................................... 15
  Smart Card Logon Certificate Token Enrollment .............................................. 20
  SAC 8.1 SP2 Configuration .................................................................................. 21
  View Manager Configuration ................................................................................ 25
    Exporting the Microsoft Root CA Certificate ............................................ 26
    Importing the Root CA Certificate to a Truststore .................................. 27
    Adding the Truststore to the View Connection Server .......................... 30
    Defining Smart Card Authentication Policies ........................................... 31
  View Agent Configuration ................................................................................... 33
    Setting the GPO ................................................................................................. 36
  View Client Configuration ..................................................................................... 40
  CBA Using SafeNet Tokens ................................................................................. 41
    Typical CBA Example ...................................................................................... 41
    CBA Using Tokens on Wyse P20 .................................................................. 44
    CBA Using SafeNet eToken 7300 on Ceedo ............................................... 47

**OTP-Based Authentication** ......................................................................................... 51

  Solution Overview ................................................................................................. 51
  Software Requirements .......................................................................................... 53
  Token Requirements .............................................................................................. 53
  Key Activities ........................................................................................................... 53
Authentication Flow for MobilePASS Messaging Tokens ........................................54
Authentication Flow for Standard OTP Tokens ............................................55
SAM 8.0 SP3 Configuration ........................................................................55
  Installing and Configuring SAM .................................................................56
  Configuring SAM’s Connector for OTP Authentication .........................57
  Configuring MobilePASS Messaging Settings .....................................58
  Configuring Mail Settings ....................................................................59
  Configuring SMS Provider Settings ......................................................60
  Preparing the User Store Messaging Information ..................................61
OTP Token Enrollment .............................................................................62
  Enrolling MobilePASS Messaging Tokens .............................................62
  Enrolling Standard OTP Tokens ...........................................................65
  Enrolling USB OTP Tokens ..................................................................65
Microsoft IAS Configuration .................................................................68
  Identifying the View Connection Server as a RADIUS Client for IAS ....68
  Enabling PAP Authentication for IAS ....................................................70
Microsoft NPS Configuration .................................................................72
  Identifying the View Connection Server as a RADIUS Client for NPS ....72
  Enabling PAP Authentication for NPS ....................................................73
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration ..............84
  Installing the OTP Plug-In .................................................................84
  Configuring OTP Plug-In Authentication Settings ................................87
View Manager Configuration .................................................................89
RADIUS Configuration ..........................................................................89
  Configuring the RADIUS for Messaging .............................................90
  Configuring the RADIUS for Standard OTP Tokens ...........................94
OTP Authentication Using SafeNet Tokens .............................................98
  Authenticating Using MobilePASS Messaging Tokens ........................98
  Authenticating Using Standard OTP Tokens ........................................100
Chapter 1

Introduction

Customers today are looking to desktop virtualization to transform static desktops into dynamic mobile workspaces that can be centrally and securely managed from the datacenter, and accessed across a wide range of devices and locations. End-users can access their corporate desktops from within the Local Area Network (LAN) - on-premise, and also from the Wide Area Network (WAN) - remotely.

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users – often remote users – requesting access to resources is a critical consideration in achieving a secure desktop virtualization solution. Deploying desktop virtualization without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat. A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

An effective strong authentication solution must be able to address the diverse set of user stories that “anywhere, using any device” access makes possible with VDI. Matching the authentication method (OTP, C-R OTP, OOB, PKI, etc.) and the authenticator form factor (hardware or software) to the functional, security, and compliance requirements is often not easily achievable with a one-size-fits-all authentication solution. A versatile authentication solution that enables a mix-and-match approach is required to allow the assignment of the right authenticators to address the specific needs of the user and user-case.

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 authenticator lifecycle.

This guide describes how to use SafeNet Authentication Manager 8.0 SP3 to add certificate-based or OTP user authentication to VMWare View environments.
The guide also describes the relevant configuration settings for the VMware View environment, Microsoft Active Directory, and Microsoft NPS or IAS, to enable SafeNet Authentication Manager’s OTP and CBA solutions.
Chapter 2
Certificate-Based Authentication

This chapter contains the following:

- Solution Overview
- Software Requirements
- Token Requirements
- Key Activities
- Authentication Flow for CBA Tokens
- Microsoft CA Configuration
- SAM 8.0 SP3 Configuration
- Smart Card Logon Certificate Token Enrollment
- SAC 8.1 SP2 Configuration
- View Manager Configuration
- View Agent Configuration
- View Client Configuration
- CBA Using SafeNet Tokens

Solution Overview

A certificate is a signed document approving the identity of the private key on a token. The private key acts as a unique identifier for each user. It enables users to securely access networks and protected resources, and it provides proof of authenticity to digitally sign data and transactions.

In a strong authentication solution, users connect to network resources from within a secured perimeter by providing the secure smart card certificate on their token device.

Certificate-based authentication (CBA) provides two-factor authentication by verifying both what the user has (the smart card) and what the user knows (the Token Password).
VMware View offers full-fledged smart card certificate authentication for both PCoIP and RDP protocols.

The following diagram illustrates the basic components in a typical certificate-based authentication (CBA) environment using VMware View. The diagram illustrates how an end-user uses a View Connection Server (also called View Manager) together with smart card authentication to validate incoming authentication requests.

**Software Requirements**

In this scenario, the following software is required:

- VMware View 5.1 working environment
- Microsoft Enterprise CA
- SAM 8.0 SP3
- SAC 8.1 SP2

**Token Requirements**

- SafeNet tokens having smart card support
Key Activities

In this scenario, the following activities must be performed:

- Microsoft CA Configuration
- SAM 8.0 SP3 Configuration
- Smart Card Logon Certificate Token Enrollment
- SAC 8.1 SP2 Configuration
- View Manager Configuration
- View Agent Configuration
- View Client Configuration
- CBA Using SafeNet Tokens

Authentication Flow for CBA Tokens

The SafeNet CBA token solution entails the following steps:

1. The end-user connects a SafeNet CBA token to the Windows client computer.
2. The user opens View Client.
3. The View Client connects to the View Connection Server.
4. The user is prompted to enter her Token Password.
5. Upon successful authentication, the user is prompted to select a virtual desktop.

Microsoft CA Configuration

The Microsoft CA must be configured before it is connected to SafeNet Authentication Manager. This involves adding the appropriate templates, and setting the security properties.

Adding a Template to the CA

A certificate template must be deployed so that the CA can issue certificates based on it.
To add a template to the CA:

1. From the Windows taskbar, select **Start > Programs > Administrative Tools > Certification Authority**.

   The *Certification Authority* window opens.

   ![Certification Authority Window](image1.png)

2. In left pane, navigate to **Certification Authority (Local) > CA > Certificate Templates**.

   Templates that are in the database and in the CA are displayed in the right pane.

   ![Certificate Templates](image2.png)

3. In the left pane, right-click the **Certificate Templates** node, and select **New > Certificate Template to Issue**.

   The *Enable Certificate Templates* window opens.

   ![Enable Certificate Templates](image3.png)
4. Depending on your organization’s policy, select one of the following certificate templates:
   - Smartcard Logon
   - Smartcard User

5. Click OK.

The added certificate template is included in the right pane of the Certification Authority window.

**Changing a Template’s Minimum Key Size**

The new Smartcard Logon or Smartcard User template has a default key size of 512. For smartcard logon with SafeNet’s Java-based tokens, a minimum key size of 1024 is required.

**To change the template’s minimum key size:**

1. From the Windows taskbar, go to Start > Programs > Administrative Tools > Certification Authority.

   The Certification Authority window opens.

2. In left pane, navigate to Certification Authority (Local) > CA > Certificate Templates.

   Templates that are in the database and in the CA are displayed in the right pane.

3. In the right pane, right-click Smartcard Logon or Smartcard User, and select Duplicate Template.

   The Properties of New Template window opens.

4. Select the Request Handling tab.
5. In the **Minimum key size** field, select **1024** or **2048**, as required by your organization policy, and click **OK**.

   A template named *Copy of Smartcard Logon* or *Copy of Smartcard User* is added to the list of certificate templates.

### SAM 8.0 SP3 Configuration

SafeNet Authentication Manager (SAM) 8.0 SP3 enables complete user authenticator life cycle management. SafeNet Authentication Manager links tokens with users, organizational rules, and security applications to enable streamlined handling of users’ needs throughout the various user authenticator lifecycle stages.

To install SafeNet Authentication Manager and to modify your authentication infrastructure to include a certificate-based authentication (CBA) solution, perform the tasks below in the order listed.

<table>
<thead>
<tr>
<th>Order</th>
<th>Action</th>
<th>Chapter in SAM 8.0 SP3 Administrator’s Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Installing and Configuring SAM</td>
<td><em>Installation of SAM 8.0 GA,</em> <em>Upgrade from SAM 8.0 or Later,</em> and <em>Basic Configuration</em></td>
</tr>
<tr>
<td>2</td>
<td>Configuring SAM’s Connector for Microsoft CA</td>
<td><em>Connector Configuration</em></td>
</tr>
<tr>
<td>3</td>
<td>Smart Card Logon Certificate Token Enrollment</td>
<td><em>Deployment</em></td>
</tr>
</tbody>
</table>
For a checklist of the main tasks required to install, configure, and deploy SAM 8.0 SP3 in a CBA usage scenario, see the *SAM 8.0 SP3 Administrator’s Guide*.

**Installing and Configuring SAM**

See the *SAM 8.0 SP3 Administrator’s Guide* for SAM installation and configuration instructions.

**Configuring SAM’s Connector for Microsoft CA**

SafeNet Authentication Manager’s Connector for Microsoft CA (MSCA) enables user certificates to be generated on tokens using the Microsoft Certificate Authority (CA) services.

Two types of certification authorities (CAs) are provided by Windows Server 2003 / 2003 R2 / 2008 / 2008 R2 Certificate Services:

- **Standalone**: permits the generation of certificates for anyone
- **Enterprise**: permits the generation of certificates for authenticated users only, and requires Active Directory to be installed

The Connector for Microsoft CA interacts with both types of CAs, enabling certificates to be generated for these CAs. For *Smart Card Logon* and *Smart Card User* certificate authentication using VMware View, Enterprise CA is used.

For more information on certificates and CAs, see Microsoft documentation.

Use SAM’s *Token Policy Object Editor* to set the connector’s policies.

**To create a request to use Smart Card Logon on a specific CA:**

1. Open the *TPO Editor*. For more information, see the *SAM 8.0 SP3 Administrator’s Guide*.
2. In the left pane, click **Connector Settings**.
   
   The list of installed SafeNet Authentication Manager connectors opens in the right pane.
3. In the right pane, right-click **Connector for Microsoft CA**, and select **Properties**.

The **Connector for Microsoft CA Properties** window opens.

4. Select **Define this policy setting**, select **Enabled**, and click **Definitions**.

The **Connector Policy Object Editor** opens.
5. By default, there is no limit to the number of certificates that can be enrolled to a token. To limit the number of certificates on a token, do the following:

   i. In the right pane, right-click **Maximum number of certificates on token**, and select **Properties**.

   The Properties window opens.

   ![](image)

   ii. Select **Define this policy setting**.

   iii. From the drop-down menu, select the maximum number of certificates that can be enrolled to each token, and click **OK**.

6. In the left pane of the **Connector Policy Object Editor** window, right-click **Connector for Microsoft CA**, and select **Create new request**.

   The Create New Request window opens.
7. For each request, enter the fields as follows:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Name</td>
<td>May be any name. If a request with the same request name exists in a different TPO definition, the new parameters are merged with that request’s parameters during token enrollment. If the request name does not exist in a TPO for the enrolled user, the request is added. Default: <strong>New Request</strong>, followed by the next sequential number</td>
</tr>
<tr>
<td>Name</td>
<td>CA from the list of CAs installed in the AD tree. Default: the first CA in the drop-down menu</td>
</tr>
<tr>
<td>Type</td>
<td>Select <strong>Enterprise</strong>. No default</td>
</tr>
</tbody>
</table>
| Windows Version      | Windows version on the CA computer:  
  - Server 2000  
  No default                                                                                                                                         |
| Certificate Usage    | Select **Smartcard Logon**.                                                                                                                                                                                  |
| Templates            | A certificate template from one or both of the template lists appropriate for the **Certificate Usage** selected:  
  - **Administrator-generated certificate template**: used when enrollment is performed by the administrator  
  - **User-generated certificate template**: used during SAM Self Service Center enrollment  
  No default                                                                                                                                        |
In the example below, the new request is named **VMwareView**.

8. Click **OK**.

9. In the **Connector Policy Object Editor** window, select the node of the request to see its policies.

   ![Connector Policy Object Editor](image)

   **Note**

   The first four policies in the list are set when the request is created. After request creation, these policies cannot be modified. If a change is required in any of these four policies, delete the request, and create a new request with the appropriate settings.

10. Configure the remaining request policies. For more information on the request policies, see the **SAM 8.0 SP3 Administrator’s Guide**.

11. Click **OK** repeatedly to close the **Connector** and **TPO** windows.

   The updated connector settings are applied.
Smart Card Logon Certificate Token Enrollment

Administrators use SAM’s Management Center to enroll new smartcard or USB tokens for users. If SAM’s Connector for Microsoft CA is configured, SAM enrolls smart card logon certificates on the tokens during enrollment.

**To enroll a certificate on a smartcard or USB token:**
1. Connect the token to be enrolled, and disconnect all other tokens not yet assigned.
2. Use the SAM Management Center’s Deployment page to search for the appropriate users.
3. Select the Account Name of the user for whom the token will be enrolled.
4. Click Enroll.

The Enroll a Smartcard or USB Token window opens.

5. Depending on your SAM configuration, you may be able to select Initialize token to initialize the token.
6. Click Run to begin the enrollment.

The certificate is installed on the token, and a Token successfully enrolled message is displayed.
7. Click **Done**.

The token details are displayed in the list of deployed tokens.

**SAC 8.1 SP2 Configuration**

SafeNet Authentication Client (SAC) enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. Generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications offering secure web access, secure network
logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely from within hardware or software tokens.

SAC must be installed on each computer on which a SafeNet token or smartcard is to be used.

SAC must be installed on VMware View virtual desktops, and on the Windows client computers where View Client is installed.

**Note**

SAC need not be installed in the following situations:
- When using Wyse P20 Zero Client, which is a thin client
- When using SafeNet eToken 7300 tokens burned with a Ceedo image

SAC can be deployed and updated using any standard software distribution system, such as Windows Group Policy Objects (GPO) or Microsoft System Management Server (SMS).

For more information, see the *SAC 8.1 SP2 Administrator’s Guide*.

The simplest way to install SafeNet Authentication Client 8.1 SP2 is to use the .msi installer file. The installer file does not support customization.

**To install SafeNet Authentication Client 8.1 SP2:**

1. Depending on your environment, run one of the following:
   - SafeNetAuthenticationClient-x32-8.1-SP2.msi (32-bit)
   - SafeNetAuthenticationClient-x64-8.1-SP2.msi (64-bit)

   The *SafeNet Authentication Client Installation Wizard* opens.

   ![SafeNet Authentication Client Installation Wizard](image)

2. Click Next.

   The *Interface Language* window opens.
3. From the drop-down menu, select the language in which the SafeNet Authentication Client user interface will be displayed. If configuration settings are detected from a previous version, you can select **Use the existing configuration settings**.

4. Click **Next**. The *End-User License Agreement* window opens.

5. Read the license agreement, and select the option, **I accept the license agreement**.

6. Click **Next**. The *Installation Type* window opens.
7. Select one of the following:

- **Standard**: Supports all SafeNet and iKey tokens.
- **BSec-compatible**: Supports all SafeNet and iKey tokens. Select this option to support third-party applications developed with the BSec SDK.

8. Click **Next**.

The *Destination Folder* window opens, displaying the default installation folder.

9. If there are no other SafeNet Authentication applications or eToken legacy products, you can click **Browse** to select a different destination folder.

10. Click **Next**.

The installation proceeds.
When the installation is complete, a confirmation message is displayed.

11. Click **Finish** to complete the installation.

**View Manager Configuration**

Perform the following steps to configure the View Manager:

i. Exporting the Microsoft Root CA Certificate
ii. Adding JRE Utilities to the Command Path
iii. Importing the Microsoft Root CA Certificate Using JRE
iv. Adding the Truststore to the View Connection Server
v. Defining Smart Card Authentication Policies
Exporting the Microsoft Root CA Certificate

Export the Root CA certificate so that it can be accessed by the View Connection Server.

**To export the Microsoft Root CA Certificate:**

1. Click the Microsoft Root CA certificate file to open the Certificate Properties window.
2. Select the Details tab, and select **Copy to File**.
   
   The Certificate Export Wizard opens.
3. Click **Next**.
4. Select **DER encoded binary x.509 (.CER)**, and click **Next**.
5. Browse to the location in which to save the resulting certificate, assign a name to the certificate, and click **Save**.
   
   In this example, we export the file to C:, and save it as **Root CA.crt**.

   The Completing the Certificate Export Wizard window opens.
6. Click **Next**.

   A message is displayed that the export completed successfully.

   ![Certificate Export Wizard](image)

7. Click **OK**, and click **Finish**.

   The certificate file is exported to the selected location. In this example, the exported file is **Root CA.crt**.
Importing the Root CA Certificate to a Truststore

Add JRE utilities to your command path so that you can import the exported Microsoft Root CA certificate to create a truststore.

Adding JRE Utilities to the Command Path

To add JRE Utilities to your command path:

1. Press the Windows + Break keys.
   The System Properties window opens.
2. Select the Advanced tab.
3. Click **Environment Variables**.

The *Environment Variables* window opens.

![Environment Variables window](image)

4. In the **System variables** area, select **Path**, and then click **Edit**.

The *Edit System Variable* window opens.

![Edit System Variable window](image)

5. In the **Variable value** field, enter the path to the JRE installation directory, and delimit it with a semicolon (;) from any other entries present in the field.

**Note**

The JRE installation directory is the VMware server installation directory followed by `jre\bin`

The default installation path for 32-bit systems is:

```
C:\Program Files\VMware\VMware View\Server\jre\bin
```

**Note**

We recommend that you open the JRE installation directory to ensure that the bin folder location is correct.
6. Click OK three times to close the System Properties windows.

**Importing the Microsoft Root CA Certificate Using JRE**

After JRE Utilities has been added to your command path, use the `keytool` key and certificate management utility to create a truststore by importing the exported Microsoft Root CA certificate.

A *truststore* is a database of trusted entities and their associated X.509 certificate chains that authenticate the corresponding public keys. A truststore contains the CA certificates and the certificates of the other party to which this entity intends to send encrypted data. This file must contain the public key certificates of the CA and the client’s public key certificate.

A *keystore* is a database of private keys that control the operation of a cryptographic algorithm, and their associated X.509 certificate chains that authenticate the corresponding public keys.

**To import the Microsoft Root CA certificate to a trust.key file:**

1. Click **Start > Run** to open a command prompt.

2. Enter the following:

   ```shell
   keytool -import -alias <alias> -file <certificate> -keystore <truststore_filename>
   ```

   where:

   ♦  `<alias>` is a unique, case-insensitive entity name by which the certificate you are about to import will be identified in the truststore
   ♦  `<certificate>` is the name of the root CA certificate you previously exported
   ♦  `<truststore_filename>` is the name of the truststore output file in the format `<anyname>.key`

   Example:
   ```shell
   keytool -import -alias demo_SCardcrt -file RootCA.crt -keystore trust.key
   ```
You may be asked to create a password for the keystore. You will need this password in the future; for example, when adding additional certificates to the truststore or when adding an additional View Connection Server.

Adding the Truststore to the View Connection Server

To add the truststore to the View Connection Server:

1. Copy the newly created trust.key containing the Microsoft Root CA certificate to the SSL gateway configuration folder on the View Connection Server.

   **Note**
   The SSL gateway configuration folder is the VMware server installation directory followed by `sslgateway\conf`.

   The default SSL gateway configuration folder path for 32-bit systems is:  
   `C:\Program Files\VMware\VMware View\Server\sslgateway\conf`

2. Create and save a text file named `locked.properties` that contains the following entries:
trustKeyfile=trust.key
trustStoretype=JKS
useCertAuth=true

Note
The text file is case sensitive.

Defining Smart Card Authentication Policies

Enable smart card authentication in the VMware View Administrator.

To enable smart card authentication and to set its policies:

1. On any Web browser, enter https://hostname/admin to log in to the Connection Server.
   The VMware View Administrator login opens.

2. Enter your logon credentials, and click Login.
3. In the left pane, select View Configuration > Servers.
4. In the right pane, select the Connection Servers tab, and right-click the appropriate connection server.
5. From the drop-down menu, select **Edit**.

The *Edit View Connection Server Settings* window opens.

6. Select the **Authentication** tab.

7. Select policy settings appropriate for your security needs.

   In this example:
   - From the *Smart card authentication* drop-down menu, **Optional** is selected, indicating that smart card authentication is optional.
   - **Disconnect user sessions on smart card removal** is selected, indicating that the user session will be disconnected and the user desktop locked when the smart card is removed.

---

**Note**

If View Client has been configured with the *Log in As Current User* option when accessing the connection server, the smart card removal policy defined in step 7 will not apply.
View Agent Configuration

Install the View Agent on the following machines:

- All virtual desktops that are managed by the VMware vCenter Server to enable communication with the View Connection Server
- All virtual desktops that you use as templates for automated desktop pools, parents for linked-clone desktop pools, and desktop sources in manual desktop pools

To install and configure View Agent:

1. Double-click the View Agent installer file.

   The View Agent window opens.

The Welcome window opens.
2. Click Next.

The License Agreement window opens.

3. Read the VMware license agreement, select I accept the terms in the license agreement, and click Next.

4. Select Custom.

The Custom Setup window opens.

5. Right-click PCoIP Smartcard, which is disabled by default, and from the drop-down menu, select This feature will be installed on local hard drive.

PCoIP Smartcard is enabled.
6. Click **Next**.

The installation details are displayed.

7. Click **Install**.

When the installation completes, the **Installer Completed** window opens.
8. Click Finish.

A prompt is displayed to restart your computer.

9. Click Yes to restart the virtual desktop.

**Setting the GPO**

With single sign-on, users enter their Token Password once to authenticate to the View Connection Server. The Token Password is transmitted to the broker during authentication, and the broker remembers the encrypted Token Password while the session is active. VMware View automatically uses the encrypted Token Password to log the user on to their next remote desktop.

To configure single sign-on at the domain level, import the View Agent policy file to the Active Directory server.

To enable smartcard support at the domain level, import the PCoIP policy file to the Active Directory server.

**To define GPO settings for single sign-on and PCoIP:**

1. Create an Organizational Unit (OU) for your VMware View virtual desktops, and a GPO for VMware View group policies. Link the GPO to the OU.
See the **Active Directory Group Policy Example** in the *Configuring Policies* chapter of the *VMware View Administration Guide*.

2. From the **GroupPolicyFiles** folder on View Connection Server host, copy the following View Agent configuration template files to a location on the Active Directory server:

- vdm_agent.adm
- pcoip.adm

**Note**

The **GroupPolicyFiles** folder is the VMware server installation directory followed by `extras\GroupPolicyFiles`.

The default installation **GroupPolicyFiles** folder location is:

```markdown
C:\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles
```

You will need the destination location in step 7.

3. On the Active Directory server, do the following to navigate to the **Group Policy Object Editor**.

- For Windows 2003:
  
  i. Select **Start > All Programs > Administrative Tools > Active Directory Users and Computers**.

  ii. Right-click the OU that contains your VMware View virtual desktops, and select **Properties**.

  iii. On the **Group Policy** tab, click **Open** to open the Group Policy Management plug-in.

  iv. In the right pane, right-click the GPO that you created for the group policy settings, and select **Edit**.

- For Windows 2008:

  i. Select **Start > Administrative Tools > Group Policy Management**.

  ii. Expand your domain, right-click the GPO that you created for the group policy settings, and select **Edit**.

The **Group Policy Object Editor** window opens.

4. In the left pane, expand **Computer Configuration**, and right-click **Administrative Templates**.
5. From the drop-down menu, select **Add/Remove Templates**. The **Add/Remove Templates** window opens.

6. Click **Add**.

7. Navigate to the location where you copied the `vdm_agent.adm` template file in step 2, and click **Open**.

   The template is displayed in the **Add/Remove Templates** window.

8. Click **Add**.

9. Navigate to the location where you copied the `pcoip` template file in step 2, and click **Open**.

   The template is displayed in the **Add/Remove Templates** window.
10. Click Close.

The View Agent group policy settings are added to the Active Directory environment and are available for configuration.


In the right pane, the settings are displayed.

12. To enable single sign-on, do the following:

i. In the right pane, double-click **AllowSingleSignon**.

The **AllowSingleSignon Properties** window opens.

ii. Select **Enabled**, and click **OK**.
13. In left pane of the Group Object Policy Editor, navigate to Computer Configuration > Administrative Templates > Classic Administrative Templates (ADM) > PCoIP Session Variables > Overridable Administrator Defaults.

In the right pane, the settings are displayed.

14. In the right pane, double-click Configure PCoIP virtual channels.

The Configure PCoIP virtual channels Properties window opens.

15. Select Disabled, and click OK.

16. Close the Group Policy Editor.

**View Client Configuration**

View Clients for Windows, Mac, Linux, iPad, and Android allow you to connect to your VMware View virtual desktop from your device, giving you on-the-go access from any location.

You can obtain the Windows-based View Client installer either from the VMware Web site or from View Portal, a Web access page provided by View Connection Server.

**To install View Client 5.1:**

1. Log in to the client system as a user with administrator privileges.
2. On the client system, download the latest View Client installer file from the VMware product page: http://www.vmware.com/products/.

3. Double-click the installer file.
4. Follow the prompts to install the appropriate components.

The View Client service is installed on the Windows client computer.

CBA Using SafeNet Tokens

After the environment is configured, users connect their enrolled SafeNet tokens to their physical computers, open View Client, and authenticate to their virtual desktops.

Typical CBA Example

The user connects a SafeNet USB token to the Windows client computer. When the View Client connects to the View Connection Server, the user is prompted to enter their Token Password. Upon successful authentication, the user is prompted to select a virtual desktop.

The example below is for CBA to a Windows 7 virtual desktop.

Logging On

To log on to Windows 7:

1. Connect your SafeNet USB token to the computer.
2. If View Client is not started, double-click the desktop shortcut, or go to Start > Programs > VMware > VMware View Client.

The Connection Server window opens.

3. From the Connection Server drop-down menu, select the host name or IP address of the View Connection Server, and click Connect.

The PIN window opens.
4. Enter your Token Password, and click **OK**.

Once connected, a list of virtual desktops is displayed.

5. Select the appropriate virtual desktop, and click **Connect**.

In VMware View 4.5 and above, smart card authentication can be used with single sign-on. See step 12 of *Setting the GPO*, on page 39.

If single sign-on is not used, the virtual desktop’s *Smart card logon* window opens.
6. Enter your Token Password to log on to the virtual desktop.

   You are logged on.

**Disconnecting the Token**

The *Pool Setting Automatically logoff after disconnect*, determines the logoff behavior when the token is removed during online mode.

By default, the *Automatically logoff after disconnect* setting is set to **Never**. This means that when the smart card is removed during online mode, the remote desktop disconnects, but it does not log the user out. The virtual desktop remains in the pool and is not refreshed, and unsaved content is still available.

If the *Automatically logoff after disconnect* setting has been changed, the session disconnects and then logs the user out when the smart card is removed. Unsaved content is not saved, and the following message is displayed.
CBA Using Tokens on Wyse P20

SafeNet and Wyse have partnered to deliver a powerful, flexible, and secure solution that enables seamless, secure access to corporate applications and resources, accessed via thin client devices. The integrated solution addresses the challenge of providing secure local and remote access to corporate resources for employees, customers, and partners. The Wyse P20 zero client for VMware View is a secure, easily managed zero client that provides stunning graphics performance for advanced applications such as CAD, 3D solids modeling, video editing and advanced worker-level office productivity applications.

Currently, Wyse P20 supports pre-session secure user authentication via smart card, which is CAC (Common Access Card) only. SafeNet token pre-session support is planned for Wyse P20’s next official release.

The following link describes how to bypass pre-session secure user authentication via smart card now:


Token Device Bridging

When SafeNet USB tokens are used with Wyse P20, the connected tokens must terminate on the VMware itself. However, PCoIP Zero Client attempts to terminate authentication devices locally.

To prevent PCoIP Zero Client from terminating token devices locally, the devices must be bridged in the Web Interface on the Zero Client.

To enable token device bridging:
1. Ensure that Teradici’s firmware version 3.3.0 or higher is installed.
2. Connect your SafeNet USB token.
3. Log in to the PCoIP Zero Client’s Administrative interface.
4. From the Main menu, select Info > Attached Devices.
The Attached Devices window opens.

5. Record the VID (Vendor ID) and PID (Product ID) of the USB token to be bridged to a virtual desktop. They will be needed in step 8.

6. From the Main menu, select Permissions > USB. The USB window is displayed.

7. In the Bridged Devices area, click Add New. The Vendor ID and Product ID fields are displayed.

8. Enter the token’s VID and PID recorded in step 5, and click Add.
In the *Bridged Devices* area, the token’s information is displayed.

9. Click **Apply**.
   
   A *Success* message is displayed.

10. Click **Continue** to restart the PCoIP session.
Logging On Using Bridged Tokens

Whenever the user connects a token that is the same type as a bridged token, the following takes place:

1. The token is automatically bridged to the VMware Client session.
2. The list of virtual desktops is displayed.
3. The user selects the appropriate virtual desktop.
4. The user is connected to the virtual desktop.
5. The user is prompted to enter the Token Password.

CBA Using SafeNet eToken 7300 on Ceedo

Deploying a View Client with authentication certificates on un-managed devices can be technically challenging for end-users. This often results in support calls to assist in configuration and resolution of common software conflicts.

Through its technology partnership with Ceedo, SafeNet enables the delivery of a pre-packaged, pre-configured client application workspace. This includes View Client and SafeNet Authentication Client that are dynamically run from a removable storage device connected to the end-user’s computer, without requiring any installation or configuration of software on the user’s machine. The end-user simply connects her SafeNet eToken 7300 device to the client host machine, which either launches the application workspace from the secure flash storage of the token, or downloads and launches the application workspace from the Web. The application workspace ensures that all components are pre-configured, interoperable, and ready-for-use.
The View Client application hosting technology utilizes VMware View PCoIP protocol, providing virtualization and streaming technologies to enable desktop delivery to users’ computers, in this case the Ceedo work environment. SafeNet eToken 7300 combines SafeNet security with Ceedo and VMware technologies, enabling a secure portable version of the View Client platform.

**Note**

SafeNet eToken 7300 is a USB CCID compliant device which requires a generic Windows driver (usbccid.sys), provided with Windows Vista and later versions. If the SafeNet eToken 7300 is connected to a Windows XP machine, you must install the CCID drivers manually using Windows Update.

To enable token authentication using eToken 7300 on Ceedo:

1. Connect your SafeNet eToken 7300.
   
   The *Token Logon* window opens.

2. Enter the Token Password, and click **OK**.

3. Browse to the SafeNet eToken 7300 flash partition on your computer, and double-click it.

![SafeNet eToken 7300 Flash Partition](image)

The applications on the flash partition are displayed.
4. Select **StartCeedo**.

The Ceedo applications are displayed.

5. Select **View Client**.

The **Connection Server** window opens.

6. From the **Connection Server** drop-down menu, select the host name or IP address of the **View Connection Server**, and click **Connect**.

The **PIN** window opens.
7. Enter your Token Password, and click **OK**.

   The *Connecting* message is displayed.

Once connected, a list of virtual desktops is displayed.

8. Select the appropriate virtual desktop, and click **Connect**.

   You are logged in to the virtual desktop.
Chapter 3
OTP-Based Authentication

This chapter contains the following:
- Solution Overview
- Software Requirements
- Token Requirements
- Key Activities
- Authentication Flow for MobilePASS Messaging Tokens
- Authentication Flow for Standard OTP Tokens
- SAM 8.0 SP3 Configuration
- OTP Token Enrollment
- Microsoft IAS Configuration
- Microsoft NPS Configuration
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration
- View Manager Configuration
- RADIUS Configuration
- OTP Authentication Using SafeNet Tokens

Solution Overview

Sometimes users are not physically located in the organization’s premises where they can connect to network resources from a secured perimeter. These remote users connect to the organization’s View Connection Server and virtual desktop resources from external networks, where physical security is not assured. Simple passwords do not provide adequate security for remote user access to the organizational network.

The ideal solution for these situations is OTP (one-time password) authentication. The two-factor OTP authentication solution requires users to provide their network password in addition to an OTP generated by their
OTP token. This combined action strengthens authentication, enabling secure remote access to the organization’s network using VMware View and similar technologies.

When OTP tokens are used for authentication, it is much more difficult for attackers to guess the password because it’s random. This enables remote users to access the organization’s network more securely.

SafeNet’s two-factor authentication solutions are managed by SAM (SafeNet Authentication Manager), which can be installed on multiple servers. The SAM servers must be configured and accessible to the View Connection Server host.

In organizations with multiple View Connection Server instances, OTP authentication can be configured on some instances, and certificate-based authentication (CBA) configured on others. In a typical organization, OTP authentication would be configured for users who access VMware View virtual desktops remotely over the Internet.

The following diagram illustrates the basic components in a standard OTP environment using VMware View. The diagram illustrates how an end-user uses a View Connection Server together with RADIUS servers to validate incoming authentication requests.
Network Policy Server (NPS) has replaced the Internet Authentication Service (IAS) Server in Windows Server 2008 and above. In this document, the terms IAS and NPS are sometimes used interchangeably.

**Software Requirements**

In this scenario, the following software is required:

- VMware View 5.1 working environment
- Microsoft Active Directory
- SAM 8.0 SP3
- IAS or NPS with SafeNet’s OTP Plug-In for Microsoft RADIUS Client

**Note**

To use SMS or email messaging, version 8.0 SP4 of the SAM OTP Plug-In for Microsoft RADIUS Client must be installed.

**Token Requirements**

The following SafeNet OTP-generating tokens have been tested for authentication with VMware View:

- **MobilePASS Messaging applications** that send generated OTPs to users either as SMS (Short Message Service) messages to their mobile devices, or as email messages
- **Standard OTP tokens** on which users initiate OTP generation

**Key Activities**

In this scenario, the following activities must be performed:

- SAM 8.0 SP3 Configuration
- OTP Token Enrollment
- Microsoft IAS Configuration, or Microsoft NPS Configuration
- SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration
- View Manager Configuration
- RADIUS Configuration
• OTP Authentication Using SafeNet Tokens

Authentication Flow for MobilePASS Messaging Tokens

The SafeNet OTP solution for MobilePASS Messaging tokens entails the following steps:

1. The end-user connects to the View Connection Server through View Client.
2. The View Connection Server requests the user’s credentials.
3. The user provides the View Client with her logon credentials for the View Connection Server:
   ♦ User name
   ♦ Network password
4. The View Connection Server forwards the user’s credentials to the RADIUS server.
5. SAM’s OTP Plug-In for Microsoft RADIUS Client validates the user’s credentials with the SAM authentication server via web services (SOAP over HTTPS).
6. If the request is not disqualified, the authentication server sends an OTP passcode to the user’s MobilePASS Messaging token via SMS or email message.
7. The RADIUS server notifies the View Connection Server that a Challenge Code has been sent to the user.
8. The View Client prompts the user to enter a Response Code.
9. The user types in the OTP passcode received as a message, with or without her OTP PIN (depending on the TPO setting).
10. The View Client sends an authentication request to the View Connection Server.
11. The View Connection Server checks the RADIUS server to determine if the request is valid.
12. Based on the OTP value calculation results and the IAS/NPS remote access policies authorization, the RADIUS server sends a RADIUS Access Accept response to the View Connection Server.
13. Based on the response received from the RADIUS server, the View Connection Server either authorizes network entry, or denies it.

**Authentication Flow for Standard OTP Tokens**

The SafeNet OTP solution for standard tokens entails the following steps:

1. The end-user connects to the View Connection Server through View Client.
2. The View Connection Server requests the user’s credentials.
3. The user generates an OTP passcode using her enrolled token.
4. The user provides the View Client with her logon credentials for the View Connection Server:
   - User name
   - Generated OTP passcode, with or without her OTP PIN (depending on the TPO setting)
   - Network password
5. The View Connection Server forwards the user’s credentials to the RADIUS server.
6. SAM’s OTP Plug-In for Microsoft RADIUS Client validates the user’s credentials with the SAM authentication server via web services (SOAP over HTTPS).
7. Based on the OTP value calculation results and the IAS/NPS remote access policies authorization, the RADIUS server sends a RADIUS Access Accept response to the View Connection Server.
8. The View Connection Server forwards the user’s network password to Active Directory.
9. Based on the responses received from the RADIUS server and Active Directory, the View Connection Server either authorizes network entry, or denies it.

**SAM 8.0 SP3 Configuration**

SafeNet Authentication Manager (SAM) 8.0 SP3 enables complete user authenticator life cycle management. SafeNet Authentication Manager links tokens with users, organizational rules, and security applications to enable
streamlined handling of users’ needs throughout the various user authenticator lifecycle stages.

To install SafeNet Authentication Manager and to modify your authentication infrastructure to include an OTP (one-time password) solution, perform the tasks below in the order listed.

<table>
<thead>
<tr>
<th>Order</th>
<th>Action</th>
<th>Chapter in SAM 8.0 SP3 Administrator’s Guide</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Installing and Configuring SAM</td>
<td>Installation of SAM 8.0 GA, Upgrade from SAM 8.0 or Later, and Basic Configuration</td>
</tr>
<tr>
<td>2</td>
<td>Configuring SAM’s Connector for OTP Authentication</td>
<td>Connector Configuration</td>
</tr>
<tr>
<td>3</td>
<td>When using MobilePASS Messaging tokens, do all of the following:</td>
<td>Token Policy Object Settings</td>
</tr>
<tr>
<td></td>
<td>• Configuring MobilePASS Messaging Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Configuring Mail Settings, or Configuring SMS Provider Settings</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Preparing the User Store Messaging Information</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Depending on the token type, do one of the following:</td>
<td>Deployment</td>
</tr>
<tr>
<td></td>
<td>• Enrolling MobilePASS Messaging Tokens</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Enrolling Standard OTP Tokens</td>
<td></td>
</tr>
</tbody>
</table>

For a checklist of the main tasks required to install, configure, and deploy SAM 8.0 SP3 in an OTP usage scenario, see the SAM 8.0 SP3 Administrator’s Guide.

**Installing and Configuring SAM**

See the SAM 8.0 SP3 Administrator’s Guide for SafeNet Authentication Manager installation and configuration instructions.

During SAM 8.0 SP3 configuration, you can select a Simplified OTP-only configuration. This configures SAM with the basic requirements for a working OTP solution.

The simplified OTP-only configuration includes the following:

- **Connectors**: SAM’s Connector for OTP Authentication is installed and is configured to default values
• **SAM Backend Service:** Activated on this server, scheduled to operate every 24 hours

• **Hourly Distribution charts:** Not used (not relevant for OTP tokens)

• **Token initialization settings:** OTP support, required for authentication using OTP tokens, is set as the default SAM policy

### Configuring SAM’s Connector for OTP Authentication

Use the *TPO Editor* to define OTP authentication behavior in SAM’s *Connector for OTP Authentication*. For more information, see the *SAM 8.0 SP3 Administrator’s Guide*.

![Connector Policy/Object Editor](image)

The following policies must be set:

<table>
<thead>
<tr>
<th>Policy</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Code</td>
<td>Determines which information users must provide in a single string for SAM authentication using OTP</td>
<td>Set to OTP only or OTP PIN and OTP</td>
</tr>
<tr>
<td>Allow dial-in access</td>
<td>Determines if a user’s dial-in permission fields are changed to allow access during OTP token enrollments</td>
<td>Set to <strong>Enabled</strong></td>
</tr>
</tbody>
</table>
Note

When using VMware View with MobilePASS Messaging, users submit their network passwords during step 3 of the Authentication Flow for MobilePASS Messaging Tokens on page 54.

When using VMware View with standard OTP tokens, users submit their network passwords as a second authentication factor during the step 4 of the Authentication Flow for Standard OTP Tokens on page 55.

Therefore, when using the VMware View solution, we recommend setting the Authentication Code to **OTP only**, or to **OTP PIN and OTP**, and not to **Windows password and OTP**.

Configuring MobilePASS Messaging Settings

For users with enrolled MobilePASS Messaging tokens, SAM initiates OTP generation after authenticating the user’s network password during the logon process. The OTP passcode is sent to the user’s mobile phone or email address that is defined in the user’s AD fields.

These policies apply to MobilePASS Messaging tokens only.
The following policies must be set:

<table>
<thead>
<tr>
<th>MobilePASS Messaging</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable MobilePASS Messaging</td>
<td>Determines if MobilePASS Messaging enrollment is enabled</td>
<td>Set to <strong>Enabled</strong></td>
</tr>
<tr>
<td>Automatic OTP message generation</td>
<td>Determines if MobilePASS Messaging enrollment is enabled</td>
<td>Set to User name and network password</td>
</tr>
</tbody>
</table>

**Configuring Mail Settings**

SafeNet Authentication Manager can be configured to send the OTP generated on the user’s MobilePASS Messaging token to the user’s email as an email message.

Use the **TPO Editor** to define information about the email server and sender. This information is in the **Mail Configuration** settings. For more information, see the **SAM 8.0 SP3 Administrator’s Guide**.

The following policies must be set:

<table>
<thead>
<tr>
<th>Mail Configuration Settings</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail server name</td>
<td>URL of the SMS provider’s API that implements the “Send SMS” function</td>
<td>Fill in your provider URL address</td>
</tr>
</tbody>
</table>
Mail sender | Username required for logging on to the account with the service provider

**Note:** This information is automatically passed to the service provider during each SMS request.

| Fill in the username provided by the SMS provider to access your account |

**Note**

To enable email messaging, the **Mail server name** and **Mail sender** policies must be entered.

### Configuring SMS Provider Settings

SafeNet Authentication Manager can be configured to send the OTP generated on the user’s MobilePASS Messaging token to the user’s mobile phone as an SMS message.

Use the **TPO Editor** to define information about the SMS service provider and about the account used to initiate SMS message requests from the provider. This information is in the **SMS Provider Configuration** settings. For more information, see the **SAM 8.0 SP3 Administrator’s Guide**.

![TPO Editor screenshot](image.png)

The following policies must be set:

<table>
<thead>
<tr>
<th>SMS Provider Settings</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMS provider URL</td>
<td>URL of the SMS provider’s API that implements the “Send SMS” function</td>
<td>Fill in your provider URL address</td>
</tr>
</tbody>
</table>
### Preparing the User Store Messaging Information

MobilePASS Messaging tokens send OTP passcodes generated by the SAM server to users’ mobile devices or email addresses, without the need for physical tokens.

Before a MobilePASS Messaging token can be enrolled, the user’s mobile phone number or email address must be available in the user store.

To edit the user’s properties in the Active Directory user store:

1. From the Windows taskbar, do one of the following, depending on your environment:
   - Select Start > Programs > Administrative Tools > Active Directory Users and Computers.
   - Select Start > All Programs > Microsoft Exchange > Active Directory Users and Computers.

   The Active Directory Users and Computers window opens.

2. In the left pane, expand the domain node, and select Users.

3. In the right pane, right-click the appropriate user, and from the drop-down menu, select Properties.
   - In this example, the user is vmadmin.

   The user’s Properties window opens.
4. For MobilePASS Messaging token users to receive OTP passcodes as SMS messages, select the *Telephone* tab, and in the *Mobile* field, enter the user’s mobile phone number.

5. For MobilePASS Messaging users to receive OTP passcodes as email messages, select the *General* tab, and in the *E-mail* field, enter the user’s email address.

### OTP Token Enrollment

When you enroll an OTP token, the OTP profile on the token becomes associated with a specific user in the SAM inventory.

SAM manages various OTP token types. For information on OTP token enrollment not described in this document, see the *SAM 8.0 SP3 Administrator’s Guide*.

### Enrolling MobilePASS Messaging Tokens

**To enroll a MobilePASS Messaging token for a user:**

1. Ensure that the following conditions are met:
♦ OTP authentication is enabled for the user.
♦ The user’s messaging information (email address or mobile phone number) in the user store is correct.
   See Preparing the User Store Messaging Information on page 61.

2. Use the SAM Management Center’s Deployment page to search for the appropriate user.

3. Select the Account Name of the user for whom the MobilePASS Messaging token will be enrolled.

4. Click Messaging.
   The Enroll a MobilePASS Messaging token window opens.

5. Click Run to begin the enrollment.
Depending on your SAM configuration, you may be required to set an OTP PIN.

When the token enrollment completes, a *Token successfully enrolled* message is displayed.

6. Click **Done**.

The *MobilePASS Messaging* token details are displayed in the list of deployed tokens.
Enrolling Standard OTP Tokens

Hardware OTP tokens, such as eToken PASS, are hand-held passcode generators programmed with the same unique cryptographic algorithm used by the authentication server. The token has a button to initiate passcode generation, and a Liquid Crystal Display (LCD) to display the generated passcodes.

Use the SAM Management Center’s Deployment page to enroll OTP tokens for users. For more information, see the SAM 8.0 SP3 Administrator’s Guide.

Enrolling USB OTP Tokens

This solution was tested using an eToken NG-OTP, an integrated hybrid USB smartcard and OTP token. These authenticators operate as a smartcard when connected to a PC using the USB connector, and as an OTP token when disconnected.

Like the standard SafeNet OTP tokens, these are hand-held passcode generators programmed with the same unique cryptographic algorithm used by the authentication server. The token has a button to initiate passcode generation, and a Liquid Crystal Display (LCD) to display the generated passcodes.

To enroll a USB OTP token for a user:

1. Connect the USB token to be enrolled, and disconnect all other tokens not yet assigned.
2. Use the SAM Management Center’s Deployment page to search for the appropriate user.
3. Select the Account Name of the user for whom the token will be enrolled.
4. Click Enroll.

The Enroll a Smartcard or USB Token window opens.
5. Depending on your SAM configuration, you may be able to select Initialize token to initialize the token.

6. Depending on your SAM configuration, you can click Customize enrollment to enroll only some of the default connector applications onto the token.

The Applications to Enroll window opens, displaying the available connectors.

Ensure that Connection for OTP Authentication is selected, and click OK.

7. Click Run to begin the enrollment.

8. Depending on your SAM configuration, you may be required to set an OTP PIN.
When the token enrollment completes, a *Token successfully enrolled* message is displayed.

9. **Click Done.**

The token details are displayed in the list of deployed tokens.
Microsoft IAS Configuration

Configure the Windows service running a RADIUS server. For servers earlier than Windows Server 2008, this Windows service is the Microsoft Internet Authentication Service (IAS).

Identifying the View Connection Server as a RADIUS Client for IAS

To identify the View Connection Server as a RADIUS client on IAS:

1. Open the IAS snap-in.
   The Internet Authentication Service console opens.

2. In the left pane, right-click Internet Authentication Service (Local), and from the drop-down menu, select Register Server in Active Directory.

   ![Register Internet Authentication Server in Active Directory window](image)

   The Register Internet Authentication Server in Active Directory window opens.

3. Click OK to authorize the IAS server.

4. In the left pane of the Internet Authentication Service console, right-click Radius Clients, and from the drop-down menu, select New Radius Client.

   The Name and Address window opens.
5. Do the following:
   i. Enter a friendly name for the View Connection Server. In this example, we enter *Vmware View Server*.
   ii. Enter the IP address of the View Connection Server.
   iii. Click **Next**.

The *Additional Information* window opens.

6. In the *Shared secret* and *Confirm shared secret* fields, enter a secret. You will need this secret in step 8 of the Configuring the RADIUS for Messaging section on page 92, or in step 8 of the Configuring the RADIUS for Standard OTP Tokens section on page 96.

7. Click **Finish**.

In the *Internet Authentication Service* console, the friendly name you assigned to the new RADIUS and its IP address are displayed in the right pane.
Enabling PAP Authentication for IAS

To allow communication with the View Connection Server, select PAP as the authentication method in the *Remote Access Policies*.

**To enable PAP authentication on the IAS server:**

1. Open the IAS snap-in.

   The *Internet Authentication Service* console opens.

2. In the left pane, select *Remote Access Policies*.

3. In the right pane, right-click *Connections to other access servers*, and from the drop-down menu, select *Properties*.

   The *Connections to other access servers Properties* window opens.
4. Click Edit Profile.

   The Edit Dial-in Profile window opens.

5. Select the Authentication tab, and select Unencrypted authentication (PAP,SPAP).

6. Click OK repeatedly to close all the windows.

   PAP authentication is enabled on the IAS.
Microsoft NPS Configuration

Configure the Windows service running a RADIUS server. For Windows Server 2008 and above, this Windows service is the Microsoft Network Policy Server (NPS).

Identifying the View Connection Server as a RADIUS Client for NPS

To identify the View Connection Server as a RADIUS client on NPS:

1. From the Windows taskbar, select Start > Programs > Administrative Tools > Network Policy Server.

   The Network Policy Server console opens.

2. In the left pane, click NPS (Local), and from the drop-down menu, select Register server in Active Directory.

   A message is displayed.

3. Click OK to authorize the NPS.

   A message is displayed.

4. Click OK to close the message.
5. In the left pane of the Network Policy Server console, expand RADIUS Clients and Servers.

6. Click Radius Clients, and from the drop-down menu, select New. The New RADIUS Client window opens.

7. Do the following:
   
   i. Enter a friendly name for the View Connection Server.
   
   ii. Enter the IP address of the View Connection Server.
   
   iii. In the Shared secret field, enter a secret.
       
       You will need this secret in step 8 of the Configuring the RADIUS for Messaging section on page 92, or in step 8 of the Configuring the RADIUS for Standard OTP Tokens section on page 96.
   
   iv. Click OK.

   In the Network Policy Server console, the friendly name you assigned to the new RADIUS and its IP address are displayed in the right pane.

Enabling PAP Authentication for NPS

To allow communication with the View Connection Server, select PAP as the authentication method in Connection Request Policies and Network Policies.
Enabling PAP Authentication for Connection Request Policies

To enable PAP authentication for the Connection Request policy on NPS:

1. Open the Network Policy Server console.
2. In the left pane, expand the tree to Connection Request Policies.
   The Connection Request Policies area is displayed in the right pane.
3. In the left pane, right-click Connection Request Policies, and from the drop-down menu, select New.
   The Specify Connection Request Policy Name and Connection Type window opens.
4. Enter a Policy name, and click Next. In this example, the Policy name is VmwareView (OTP).

**Note**

Do not change the Type of network access server value, which is set to Unspecified.

The Specify Conditions window opens.

5. Click Add.

The Select condition window opens.

6. Select the appropriate condition for the connection type to be authenticated, and click Add. In this example, we select Day and Time Restrictions.
7. Click **Next**.

The *Specify Connection Request Forwarding* window opens.

8. Select **Authenticate requests on this server**, and click **Next**.

The *Specify Authentication Methods* window opens.
9. Click Next.

The Configure Settings window opens.

10. Click Next.

The Completing Connection Request Policy Wizard window opens.
11. Click Finish.

The new policy and its conditions are displayed in the Network Policy Server console’s Connection Request Policies area.

Enabling PAP Authentication for Network Policies

To enable PAP authentication for the Network policy on NPS:

1. Open the Network Policy Server console.

2. In the left pane, expand the tree to Network Policies.

The Network Policies area is displayed in the right pane.
3. In the left pane, click Network Policies, and from the drop-down menu, select New.

The Specify Network Policy Name and Connection Type window opens.

4. Enter a Policy name, and click Next.

In this example, the Policy name is PAP.

**Note**

Do not change the Type of network access server value, which is set to Unspecified.

The Specify Conditions window opens.
5. Click **Add**.

The *Select condition* window opens.

6. Select the appropriate condition for the connection type to be authenticated, and click **Add**.
   
   In this example, we select **Day and Time Restrictions**.
7. Click **Next**.

The **Specify Access Permission** window opens.

8. Select **Access granted**, and click **Next**.

The **Configure Authentication Methods** window opens.
9. Select **Unencrypted authentication (PAP, SPAP)**, and click **Next**.

   The **Configure Constraints** window opens.

![Configure Constraints](image)

10. Click **Next**.

   The **Configure Settings** window opens.
11. Click Next.

The Completing New Network Policy window opens.

12. Click Finish.

The new policy and its conditions are displayed in the Network Policy Server console’s Network Policies area.
SAM’s OTP Plug-In for Microsoft RADIUS Client Configuration

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 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.

Although this solution integrates with SAM 8.0 SP3 or later, the OTP solution requires installing the OTP Plug-In for Microsoft RADIUS Client for SAM 8.0 SP4.

Installing the OTP Plug-In

Use the Setup Manager to install the OTP Plug-In for Microsoft RADIUS Client on the IAS or NPS server.

Note

If your installation includes an earlier version of OTP Plug-In for Microsoft RADIUS Client, uninstall it, and install OTP Plug-In for Microsoft RADIUS Client for SAM 8.0 SP4.

To install the OTP Plug-In for Microsoft RADIUS Client:

1. Log on to the server as a user with administrative rights, and launch the SafeNet OTP Plug-In Package installer for SAM 8.0 SP4.
2. Double-click the executable file SetupManager.exe.

   The SafeNet OTP Plug-in Package Setup window opens.
3. Click **Next**.

   The *Plug-in Selection* window opens.

4. Select **OTP Plug-In for Microsoft RADIUS Client** only.

5. Click **Install**.

   The *Updating System* window may open.

6. Wait while *Microsoft Runtime* is installed.

   The *SafeNet OTP Plug-In for Microsoft RADIUS Client Installation Wizard* opens.
7. Click Next.

The License Agreement opens.

8. Read the license agreement carefully, select I accept the license agreement, and click Next.

The Destination Folder window opens.

9. Click Next.

The Updating System window opens.
When the installation is finished, a *successfully installed* message is displayed.

10. Click Finish.

11. If you are prompted to restart your computer, restart it.

**Configuring OTP Plug-In Authentication Settings**

To change the default OTP authentication behavior, modify the OTP configuration settings file, located on the Microsoft RADIUS (IAS or NPS) server.

The configuration settings are added to the `<ias_plugin_configuration>` section in the `otp_plugin_config.xml` file.

**To configure OTP authentication settings:**

1. In the SAM 8.0 SP4 *OTP Plug-In installation* folder, open the `otp_plugin_config.xml` file for editing.
2. In the `<ias_plugin_configuration>` section, make sure that the following keys are configured with the values specified:
### OTP Plug-In for Microsoft RADIUS Client Settings

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
<th>Type and Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable_otp_authentication</td>
<td>Ensure that this value is set to <code>true</code>.</td>
<td>This value determines whether OTP authentication is enabled.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value Type: Boolean</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Default: <code>true</code></td>
</tr>
<tr>
<td>otp_web_service_url</td>
<td>If SAM and the OTP plug-in are not installed on the same computer, enter the location address of SAM server. Do not include the &quot;OTPAuthentication/Service.asmx&quot; postfix.</td>
<td>This value defines the name of the SafeNet Authentication Web Service URL server that checks all necessary parameters and then authorizes or rejects the request. Value Type: String Default: <code>http://localhost</code></td>
</tr>
<tr>
<td>empty_password.messaging_support</td>
<td>When using MobilePASS Messaging, ensure that this value is set to <code>true</code>.</td>
<td>This value determines if submitting an empty password field triggers the MobilePASS Messaging token to send an OTP passcode to the mobile phone or email address. Value Type: Boolean Default: <code>false</code></td>
</tr>
</tbody>
</table>

For example:

```xml
<?xml version="1.0"?>
<ias_plugin_configuration>
    <enable_otp_authentication>true</enable_otp_authentication>
    <otp_web_service_url_list>
        <otp_web_service_url>http://10.9.11.3</otp_web_service_url>
    </otp_web_service_url_list>
    <no_otp_token_behavior>reject</no_otp_token_behavior>
    <user_not_found_behavior>reject</user_not_found_behavior>
    <protocol_not_supported_behavior>pass</protocol_not_supported_behavior>
    <return_pap_cred>false</return_pap_cred>
    <return_pap_cred_attribute_number>2</return_pap_cred_attribute_number>
    <web_service_request_timeout>15</web_service_request_timeout>
    <web_service_comm_error_behavior>fail</web_service_comm_error_behavior>
    <tms_db_offline_behavior>fail</tms_db_offline_behavior>
    <enable_full_log>false</enable_full_log>
    <AuthStatistics>
        <FailureThresh>1</FailureThresh>
        <AuthWindowSize>1000</AuthWindowSize>
```
View Manager Configuration

VMware View 5.1’s support for RADIUS authentication enables protection of external access via a View Connection Server, and two-factor authentication using RADIUS.

Configure a View Connection Server instance to require users to use one of the following OTP generation methods:

- MobilePASS Messaging
- Standard OTP token

The diagram below illustrates the basic components involved in this solution.

RADIUS Configuration

Configure the RADIUS for either messaging or standard OTP tokens.
Configuring the RADIUS for Messaging

Configure the RADIUS to support OTP transmission via SMS or email messaging in View Manager.

To configure the RADIUS for messaging:

1. On any Web browser, enter https://hostname/admin to log in to the Connection Server.
   
   The VMware View Administrator login opens.

2. Enter your logon credentials, and click Login.

3. In the left pane, select View Configuration > Servers.

4. In the right pane, select the Connection Servers tab, and right-click the appropriate connection server.
5. From the drop-down menu, select Edit. The Edit View Connection Server Settings window opens.

6. Select the Authentication tab.

7. In the Advanced Authentication area, do the following:
   i. From the 2-factor authentication drop-down menu, select RADIUS.
   ii. To force RADIUS user names to match user names in Active Directory, select Enforce 2-factor and Windows user name matching.
   iii. If the initial RADIUS authentication uses Windows authentication that triggers an out-of-band transmission of a token code, and this token code is used as part of a RADIUS challenge, select Use the same username and password for RADIUS and Windows authentication.
iv. From the **Authenticator** drop-down menu, select **Create New Authenticator**.

The *Add RADIUS Authenticator* window opens.

8. Set the following fields:

i. **Label** (required): Enter a value to identify the RADIUS authenticator in the VMware View connection logon window. In this example, we assign the name *Windows* to the new RADIUS authenticator.

![Add RADIUS Authenticator](image)

### Note

View Client will display this label in the user authentication prompt.

In this solution, users will be required to enter their Windows domain credentials. We recommend choosing a label that indicates to the users that the credentials they must enter are for their Windows network domain.

For an example of the VMware View connection logon window, see the window displayed before step 3 in the *Authenticating Using MobilePASS Messaging Tokens* section, on page 99.

ii. **Description**: Enter a value to describe the RADIUS authenticator.
iii. **Hostname/Address** (required): Enter the IP address of the RADIUS server hosting SafeNet’s OTP Plug-In for Microsoft RADIUS Client.

iv. **Authentication port**: Enter 1812 (default port).

v. **Authentication type** (required): Select PAP.

vi. **Shared secret** (required): Enter the secret of the RADIUS client on the RADIUS server.

For IAS, this was set in step 6 of the *Identifying the View Connection Server as a RADIUS Client for IAS* section on page 69.

For NPS, this was set in step 7 of the *Identifying the View Connection Server as a RADIUS Client for NPS* section on page 73.

9. Click Next.

The *Secondary Authentication Server* window opens.

10. To add a secondary RADIUS server, select the **Use a secondary server if primary is not available**, and define the secondary authentication server as described in step 8.

11. Click Finish.

12. In the *Edit View Connection Server Settings* window, click **Manage Authenticators**.

   The new RADIUS authenticator is added to the *Manage Authenticators* window.
Configuring the RADIUS for Standard OTP Tokens

Configure the RADIUS to support standard OTP tokens in View Manager.

To configure RADIUS for standard OTP tokens:

1. On any Web browser, enter https://hostname/admin to log in to the Connection Server.

   The VMware View Administrator login opens.

2. Enter your logon credentials, and click Login.

3. In the left pane, select View Configuration > Servers.

4. In the right pane, select the Connection Servers tab, and right-click the appropriate connection server.
5. From the drop-down menu, select **Edit**.

   The *Edit View Connection Server Settings* window opens.

6. Select the **Authentication** tab.

7. In the **Advanced Authentication** area, do the following:
   
i. From the **2-factor authentication** drop-down menu, select **RADIUS**.
   
ii. To force RADIUS user names to match user names in Active Directory, select **Enforce 2-factor and Windows user name matching**.
   
iii. Ensure that **Use the same username and password for RADIUS and Windows authentication** is not selected.
iv. From the Authenticator drop-down menu, select **Create New Authenticator**.

The **Add RADIUS Authenticator** window opens.

![Add RADIUS Authenticator window](image)

8. Set the following fields:

   i. **Label** (required): Enter a value to identify the RADIUS authenticator in the VMware View connection logon window. In this example, we assign the name **SafeNet OTP** to the new RADIUS authenticator.

   ![Example of VMware View connection logon window](image)

   **Note**

   View Client will display this label in the user authentication prompt.

   In this solution, users will be required to enter their user name and the generated OTP. We recommend choosing a label that indicates to the users that the logon credentials must include the OTP.

   For an example of the VMware View connection logon window, see the window displayed before step 3 in the **Authenticating Using Standard OTP Tokens** section, on page 101.

   ii. **Description**: Enter a value to describe the RADIUS authenticator.

   iii. **Hostname/Address** (required): Enter the IP address of the RADIUS server hosting SafeNet’s OTP Plug-In for Microsoft RADIUS Client.

   iv. **Authentication port**: Enter **1812** (default port).

   v. **Authentication type** (required): Select **PAP**.
vi. **Shared secret** (required): Enter the secret of the RADIUS client on the RADIUS server.
For IAS, this was set in step 6 of the *Identifying the View Connection Server as a RADIUS Client for IAS* section on page 69.
For NPS, this was set in step 7 of the *Identifying the View Connection Server as a RADIUS Client for NPS* section on page 73.

9. Click **Next**.

The *Secondary Authentication Server* window opens.

10. To add a secondary RADIUS server, select the **Use a secondary server if primary is not available**, and define the secondary authentication server as described in step 8.

11. Click **Finish**.

12. In the *Edit View Connection Server Settings* window, click **Manage Authenticators**.

The new RADIUS authenticator is added to the *Manage Authenticators* window.
OTP Authentication Using SafeNet Tokens

To authenticate, the user submits an OTP passcode.

Authenticating Using MobilePASS Messaging Tokens

The following describes how users authenticate to the virtual desktop with their MobilePASS Messaging tokens:

i. The user opens View Client on her computer.

ii. The user identifies herself to the system.

iii. An OTP (One-Time-Password) for authentication is sent as a message to the user’s mobile device, or to the user’s email address.

iv. The user copies the OTP, together with any other information required as part of the OTP Authentication Code, to the Logon window.

v. If all the information submitted is correct, the user is prompted to select a virtual desktop.

To authenticate using a MobilePASS Messaging token:

1. If View Client is not started, double-click the desktop shortcut, or go to Start > Programs > VMware > VMware View Client.

   The Connection Server window opens.

2. From the Connection Server drop-down menu, select the host name or IP address of the View Connection Server, and click Connect.
The RADIUS authenticator logon window opens.

![RADIUS Authenticator Logon Window]

Note

VMware View 5.1 has been configured for authentication using OTP through RADIUS. The prompt displayed in the logon window includes the name assigned to the RADIUS authenticator. In the example in this document, we assigned the label Windows to the RADIUS authenticator in step 8 of the Configuring the RADIUS for Messaging section, on page 92.

3. In the User name field, enter your Windows user name.
4. In the Passcode field, enter your Windows password.

Note

VMware View 5.1 always displays this field name as Passcode, even though you must enter your Windows password in it.

5. Click OK.

An OTP is sent as a message to your mobile device or to your email address.

The Next Response window opens.

![Next Response Window]

Enter your OTP Authentication Code.
Your SafeNet Authentication Manager configuration determines which information you need to include in an OTP Authentication Code. An OTP Authentication Code always includes the OTP passcode you received. It may also include your OTP PIN.

6. Click OK.

7. A list of virtual desktops is displayed.

8. Select the appropriate virtual desktop, and click Connect.

You are logged in to the virtual desktop.

**Authenticating Using Standard OTP Tokens**

In this solution, users generate OTP passcodes on their OTP tokens, and submit the OTP passcodes to authenticate to the virtual desktop.

**To authenticate using a standard OTP token:**

1. If View Client is not started, double-click the desktop shortcut, or go to Start > Programs > VMware > VMware View Client.

The Connection Server window opens.
2. From the *Connection Server* drop-down menu, select the host name or IP address of the View Connection Server, and click *Connect*.

   The RADIUS authenticator logon window opens.

   ![Image of RADIUS authenticator logon window](image)

   **Note**

   VMware View 5.1 has been configured for authentication using OTP through RADIUS. The prompt displayed in the logon window includes the name assigned to the RADIUS authenticator. In the example in this document, we assigned the label *SafeNet OTP* to the RADIUS authenticator in step 8 of the *Configuring the RADIUS for Standard OTP Tokens* section, on page 96.

3. Enter your user name.

4. Generate an OTP on your token.

5. In the *Passcode* field, enter your OTP Authentication Code.

   **Notes**

   VMware View 5.1 always displays this field name as *Passcode*, even though you must enter your OTP Authentication Code in it.

   Your SafeNet Authentication Manager configuration determines which information you need to include in an OTP Authentication Code. An OTP Authentication Code always includes the OTP value generated on your token. It may also include your OTP PIN.

6. Click *OK*. 
The domain credentials window opens.

7. Enter your Windows domain password, and click **Login**.

   A list of virtual desktops is displayed.

8. Select the appropriate virtual desktop, and click **Connect**.

   You are logged in to the virtual desktop.