SafeNet Authentication Service

Integration Guide

VMWare View 5.1

Document Information

Document Part Number	007-012628-001, Rev A
Release Date	July 2014

Trademarks

Disclaimer

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

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

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

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

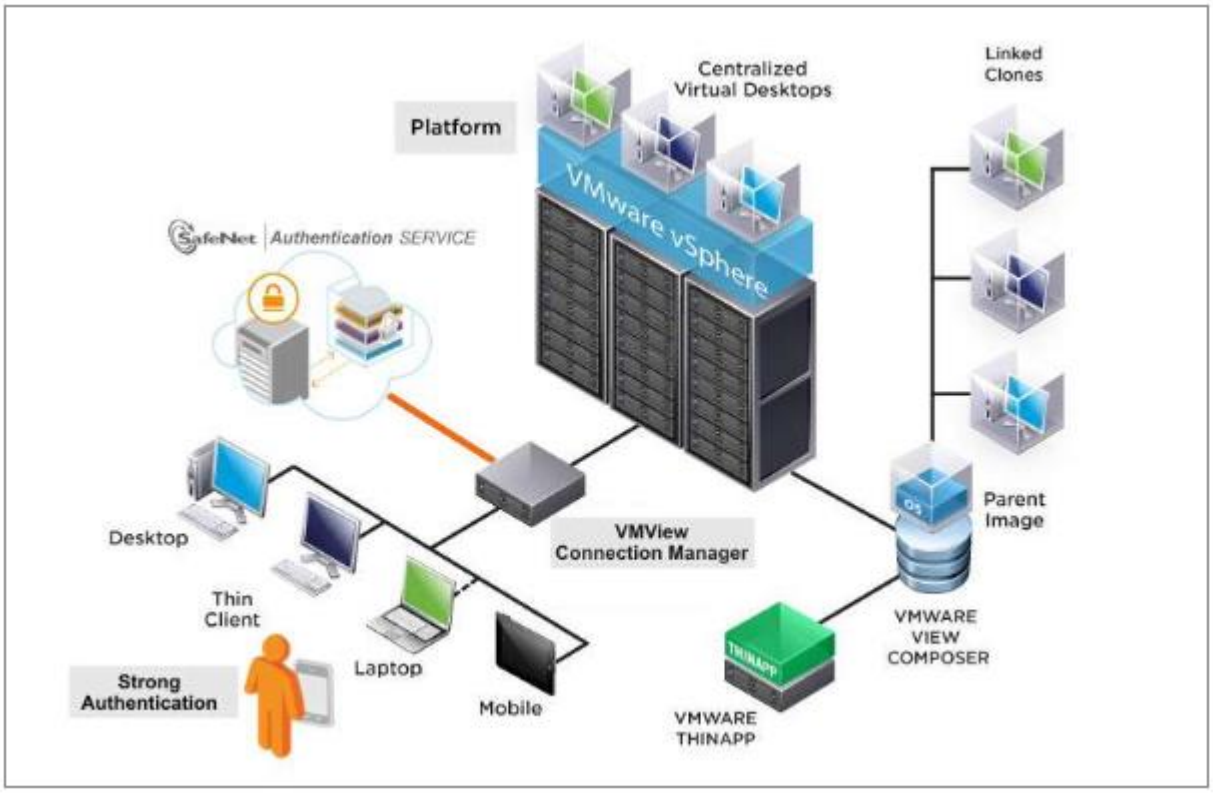
Introduction

Third-Party Software Acknowledgement

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

Overview

By default, VMWare View user authentication requires that a user provide a correct user name and password to successfully logon. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password, validated by SafeNet Authentication Service.



Applicability

The information in this document applies to:

- **SafeNet Authentication Service (SAS)** - A cloud authentication service of SafeNet, Inc.
- **SafeNet Authentication Service – Service Provider Edition (SAS-SPE)** - The software used to build a SafeNet authentication service.
- **SafeNet Authentication Service – Private Cloud Edition (SAS-PCE)** - A term used to describe the implementation of SAS-SPE on-premises.

Compatibility and Integration

Authentication Method	RADIUS (PAP, MSCHAPv2)
SafeNet Authentication Service	All versions
Failover/redundancy	Supported
Tokens	
Hardware Tokens	• SafeNet RB, KT Series • SafeNet eToken, Silver, Gold, Platinum, Alpine • Third-Party OATH Tokens • SecurID (via RADIUS Token Mode)
Software Tokens	• SafeNet MP-1 • Third-Party OATH Tokens (via RADIUS Token Mode) • SecurID (via RADIUS Token Mode)
GrID	Not supported

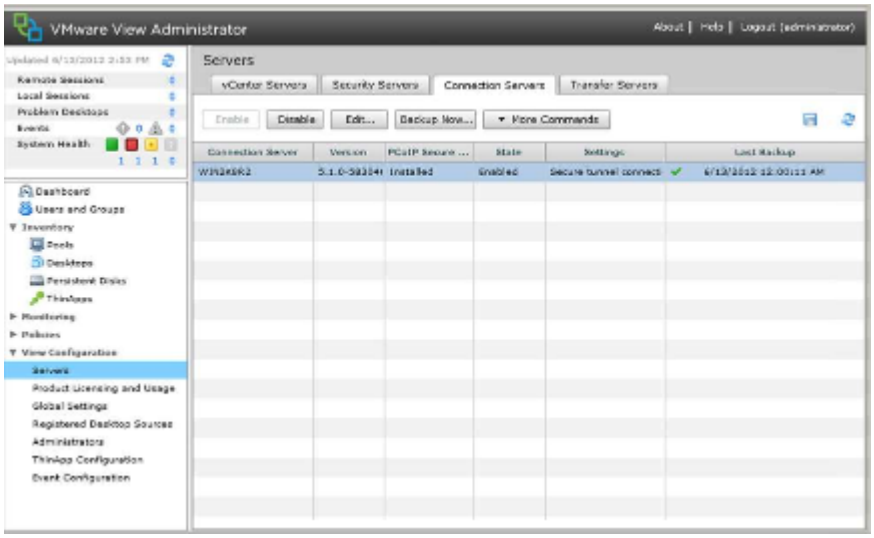
Prerequisites

- Ensure that ports 1812/1813 are open to the VMWare View Connection Manager.
- Create a valid user account in SAS with a token to be used to test RADIUS authentication.
- Ensure end users can authenticate through the VMWare View environment with a static password before configuring the VMWare View to use RADIUS authentication.
- Add a RADIUS entry in the SafeNet Authentication Service (SAS) Auth Nodes module to prepare it to receive RADIUS authentication requests from the VMWare View Connection Manager. You will need the IP address of VMWare View Connection Manager and the shared secret that will be used by both SAS and Connection Manager.

Configure VMWare View for RADIUS Two-Factor Authentication

Setting Up the RADIUS Authentication Server

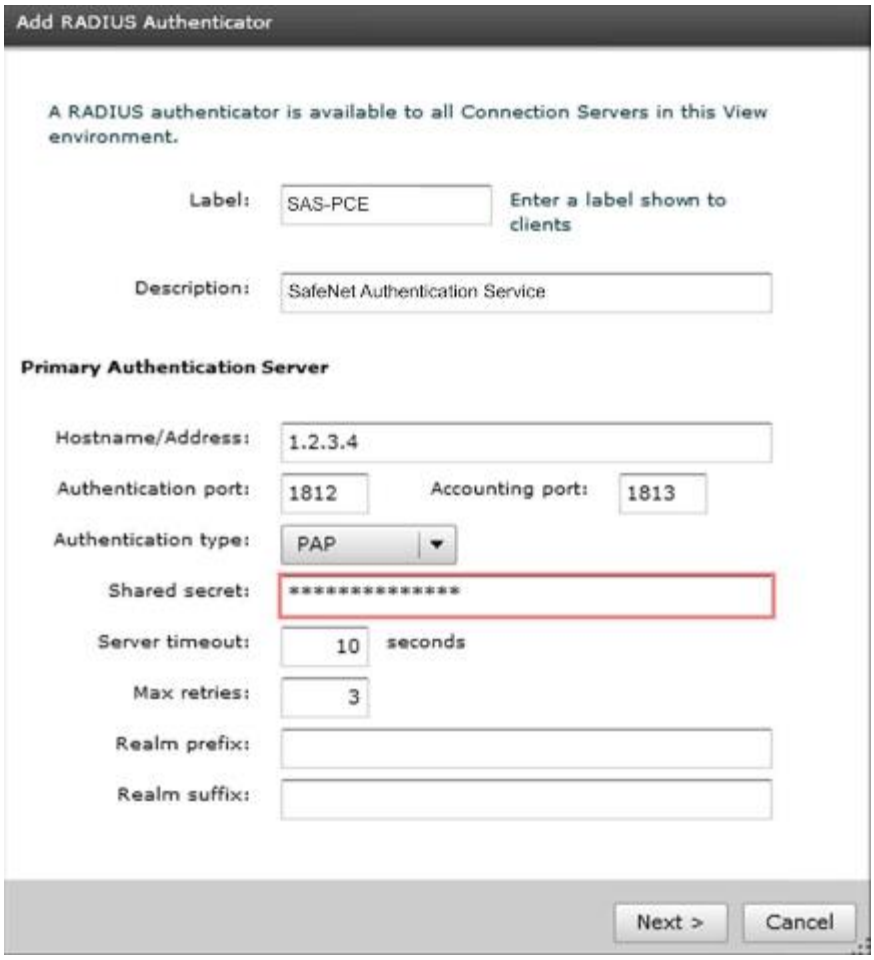
1. Log on to the VMWare View Administrator console on the VMWare View Connection server.
2. In the left pane, expand **View Configuration** and then choose **Servers**.
3. Highlight your VMWare View Connection server entry on the **Connection Servers** tab.



4. Click the **Edit** button.
5. In the **Edit View Connection Server Settings** window, click the **Authentication** tab.

6. In the **Advanced Authentication** section, choose **RADIUS** from the **2-factor authentication** list.
7. From the **Authenticator** list, select **Create New Authenticator**.

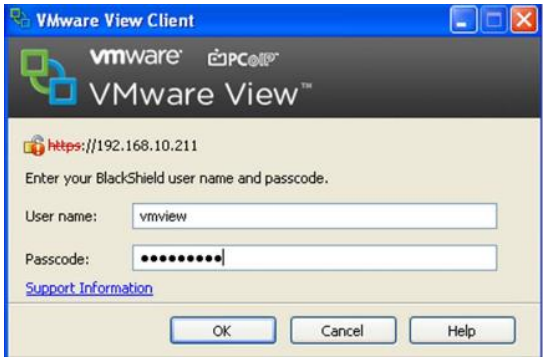
8. In the **Add RADIUS Authenticator** window, enter the details of the SAS Cloud RADIUS server or the details of your own on-premises SAS RADIUS server.



9. Click the **Next** button and enter the details of a secondary RADIUS authentication server if desired, then click **Finish**.
10. If you wish to enforce the RADIUS user names to match the user names in Active Directory, select the option **Enforce 2-factor and Windows user name** matching under the **Advanced Authentication** section in the **Edit View Connection Server Settings > Authentication**.
11. Click **OK** to apply your settings. The settings should take effect immediately.

Connecting with VMWare View Client

1. On a workstation with VMWare View 5.1 Client installed, launch the application and enter the IP address or DNS name of the VMWare View Connection server. Click the **Connect** button.
2. When prompted, enter your SAS user name and one-time password, then click **OK**.

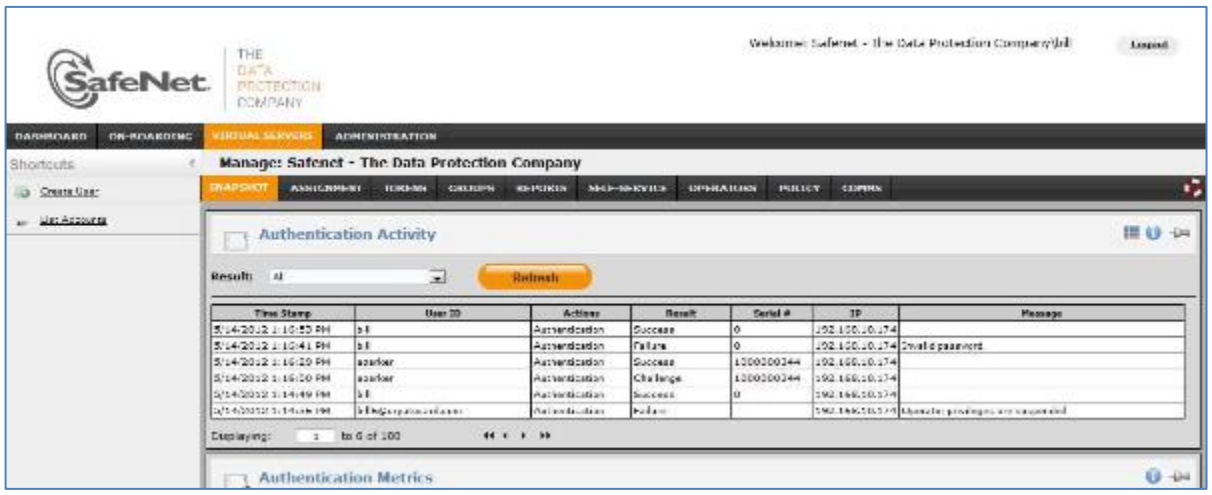


3. If the SAS authentication is successful, then continue the logon process by entering the required Active Directory credentials.

Troubleshooting

Authentication Requests Not Received

All authentication attempts received by SAS are recorded in the Authentication Activity Module on the virtual server's **Snapshot** tab. If, during testing, authentication attempts are not displayed in this list, this indicates that the authentication requests are not being received.



Possible causes include:

- An Auth Node entry has not been created in the SAS virtual server.
- An Auth Node entry has been created in the SAS virtual server but:
  - The entry contains an invalid IP address corresponding to the VMWare View Connection Manager. This is a common error often caused by NAT.
  - A firewall in your network is blocking the outbound RADIUS request. Ensure that ports 1812 and 1813 are open between VMWare View Connection Manager and SafeNet Authentication Service.
- VMWare View Connection Manager RADIUS configuration is not using ports 1812/1813.

Authentication Requests Captured in Snapshot Tab but Authentication Fails

If authentication requests are captured in the **Snapsho**t tab but authentication fails, a cause will be displayed in the **Message** column in the **Authentication Activity** list. Possible causes are:

- **Invalid Password.** This can occur if:
  - A static password is being used for testing and the password is invalid for this user. Reset the user's password in SafeNet Authentication Server and retry.
  - The shared secret is not identical in VMWare View Connection Manager and the SAS Auth Node configuration, resulting in incorrect decryption of the RADIUS packets.
- **Invalid OTP.** This can occur if the OTP provided during logon is not expected by SAS. This may be caused by:
  - Using a token for testing that is not assigned to the test user account.
  - The OTP is not being entered into the logon page exactly as shown on the token. OTPs are case sensitive, and all characters including "-" must be entered.
  - The token is "out of sync" with the server.

In both cases, the recommended approach is to assign a static password to the test user account in SAS and retry authentication. If this succeeds, retry with the token. If authentication fails again, resynchronize the token through the management UI or User Self-Service.

Other Troubleshooting Techniques

When troubleshooting RADIUS authentication issues refer to the VMWare View Administrator dashboard or monitor events in the VMWare View Administrator.

If using **SafeNet Authentication Service – PCE** with Microsoft Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS servers, refer to logging information found in the Windows Event Viewer. All logging information for the SAS IAS/NPS agent can be found in the **\Program Files\CRYPTOCard\BlackShield ID\IAS Agent\log** directory.

If using **SafeNet Authentication Service – PCE** with freeRADIUS, check the freeRADIUS server log files for authentication activity and results.

The following is an explanation of the logging messages that may appear in the event viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server.

Error Message	Solution
Packet DROPPED: A RADIUS message was received from an invalid RADIUS client.	Verify a RADIUS client authnode entry exists on the RADIUS server, or in the AuthNode section of your SAS Cloud virtual server. Authentication Rejected: Unspecified
Authentication Rejected: Unspecified	This will occur when one or more of the following conditions occur: • The username does not correspond to a user on the SAS Server. • The OTP password does not match any tokens for that user. The shared secret entered in VMWare View does not match the shared secret on the RADIUS server.
Authentication Rejected: The request was rejected by a third-party extension DLL file.	This will occur when one or more of the following conditions occur: • The SAS Agent for IAS\NPS cannot contact the SAS Server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for IAS\NPS. • The SAS Agent for IAS\NPS Keyfile does not match the Keyfile stored on the SAS Server. • The username does not correspond to a user on the SAS Server • The OTP password does not match any tokens for that user.

Known Limitations

Authentication Rejected: The request was rejected by a third-party extension DLL file.

This will occur when one or more of the following conditions occur:

- The SAS Agent for IAS\NPS cannot contact the SAS Server.
- The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for IAS\NPS.
- The SAS Agent for IAS\NPS Keyfile does not match the Keyfile stored on the SAS Server.
- The username does not correspond to a user on the SAS Server.
- The OTP password does not match any tokens for that user.

VMWare View Connection Manager RADIUS Challenge-Response Support

Please note that while VMWare View Connection Manager can use RADIUS challenge-response, the text displayed by the VMWare View client is limited. Currently, any challenge text sent from the RADIUS server is not displayed. Further details are in the *VMWare View 5.1 Administrator Guide*.

Therefore to perform tasks such as server-side PIN change, or token resynchronization, instruct your users to use the SAS self-service features. Another option is to configure the VMWare View Connection Manager to be excluded from PIN change requests. Refer to the SafeNet Authentication Service Administrator or Operator Guides for more details.

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 phone support is available to you.

Contact Method	Contact Information	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com 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.	