SafeNet Authentication Service

Integration Guide

Strong Authentication for Juniper Networks SSL VPN SSO and OWA

Document Information

Document Part Number	007-012640-001, Rev A
Release Date	Oct 2009
Software Version	1.2

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 Juniper Networks SSL VPN SSO and OWA.

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, Juniper SSL VPN logons 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 generated by a SafeNet token using the implementation instructions below.

Applicability

Security Partner Information	
Security Partner	Juniper Networks
Product Name and Version	SA 700 / 6.2R1 (Build 13255)
Protection Category	SSL Remote Access

Authentication Service Delivery Platform Compatibility	
SAS Authentication	All versions

Prerequisites

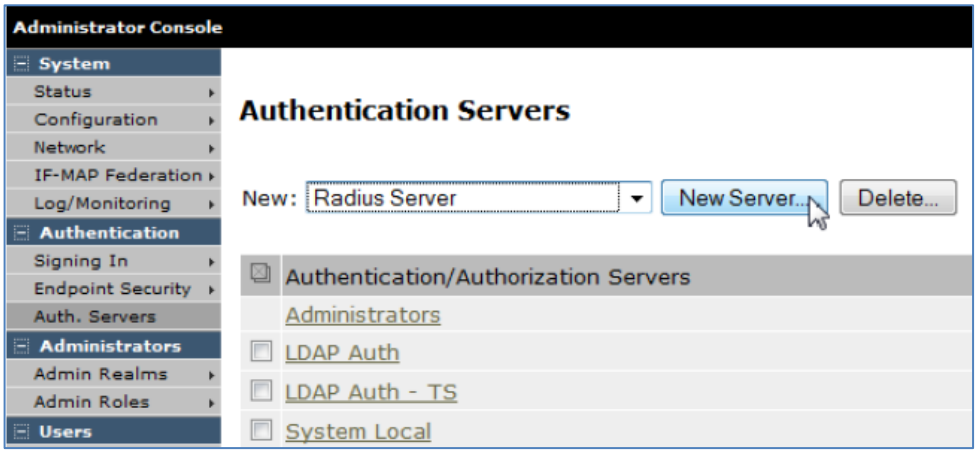
- Ensure end users can authenticate through Juniper SSL VPN with a static password before configuring RADIUS authentication.
- For SAS PCE/SPE:
  - SAS Agent for NPS IAS has been installed and configured on the NPS IAS server to accept RADIUS authentication from the Juniper SSL VPN.
  - Ensure that Ports 1812 UDP and 1813 UDP are open to the NPS IAS server.
  - The NPS IAS Agent must be configured to use either port 80 or port 443 to send authentication requests to the SAS server.

- For SAS Cloud:
  - Add a RADIUS Auth Node configured to accept authentication requests from the Juniper SSL VPN.
- For SAS PCE/SPE or SAS Cloud:
  - Create or define a “Test” account that will be used to verify that Citrix Web Interface has been properly configured. Ensure that the user name for this account exists in SAS by locating it on the **Assignment** tab.
  - Verify that the “Test” user account can successfully authenticate with a static password to Juniper SSL VPN before attempting to apply changes and test authentication using a token.
  - A “Test” user account has been created and assigned with a SafeNet token.

Configuring Juniper SSL VPN for Two-Factor Authentication

1. Log in to the Juniper SSL VPN Admin web portal.
2. To add a new RADIUS Server, in the left pane, click **Auth Servers**.

3. In the right pane, in the **New** field, select **Radius Server** and then click the **New Server** button.



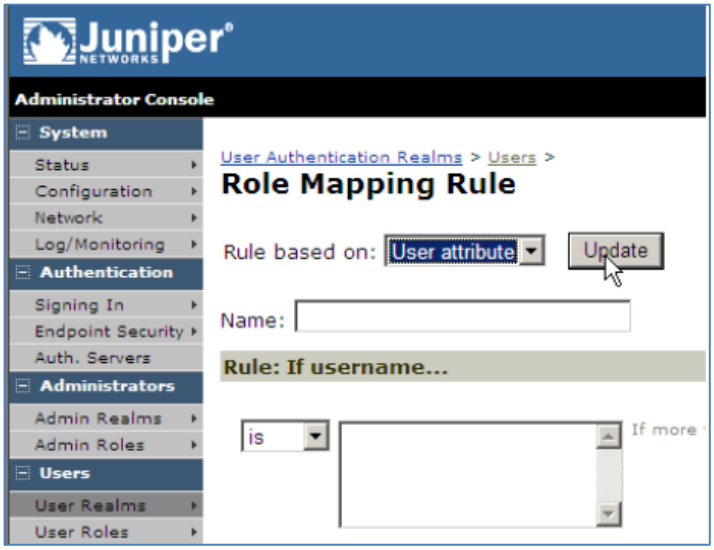
4. On the **New Radius Server** window, provide the following information:
   - **Name:** Enter **New Radius Server**.
   - **Radius Server:** Enter the IP address or DNS name of the Primary SAS RADIUS server.
   - **Shared Secret:** Enter a shared secret.

- **Users authenticate using tokens and one-time passwords:** Select this option.

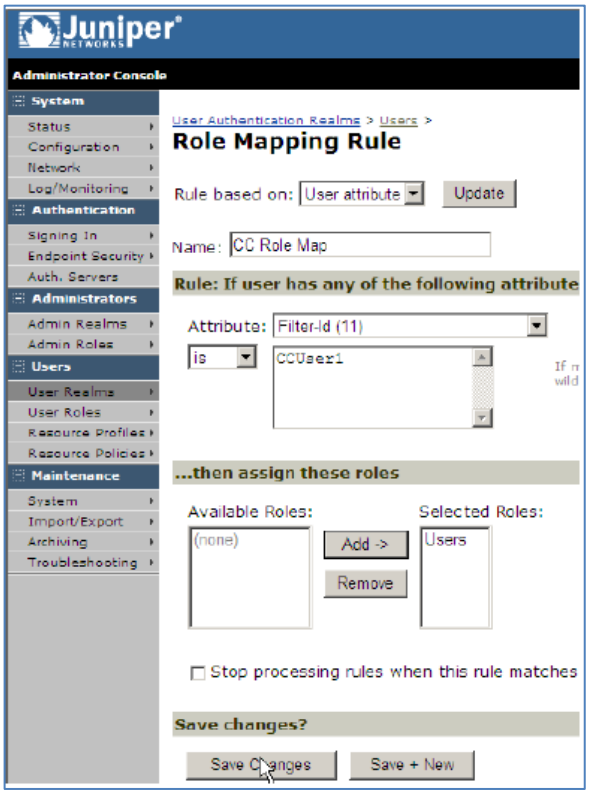
5. Click **Save Changes**.
6. **Optional:** If there is a Secondary SAS RADIUS server, complete all fields in the **Backup Server** section.
7. Under **Authentication Realm**, click **Users**.

8. Select the **Role Mapping** tab and then click **New Rule**.

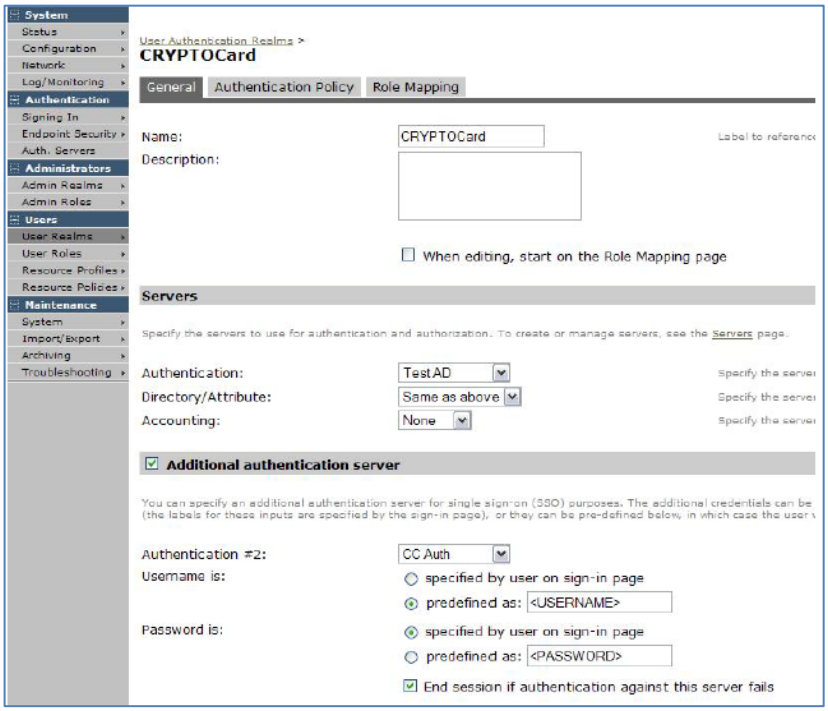
9. In the **Rule based on** field, select **User attribute**, and then click **Update**.



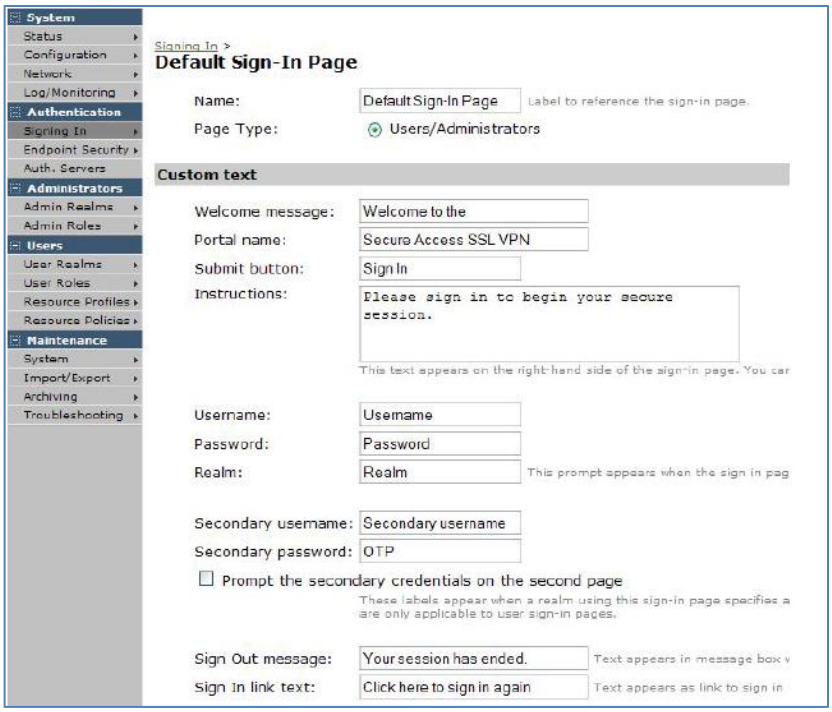
10. In the **Name** field, enter a name for reference. In this example “CC Role Map” was used.
11. Select Filter-Id (11) for the attribute, and enter **CCUser1** for the attribute name.
12. Click **Save Changes**.



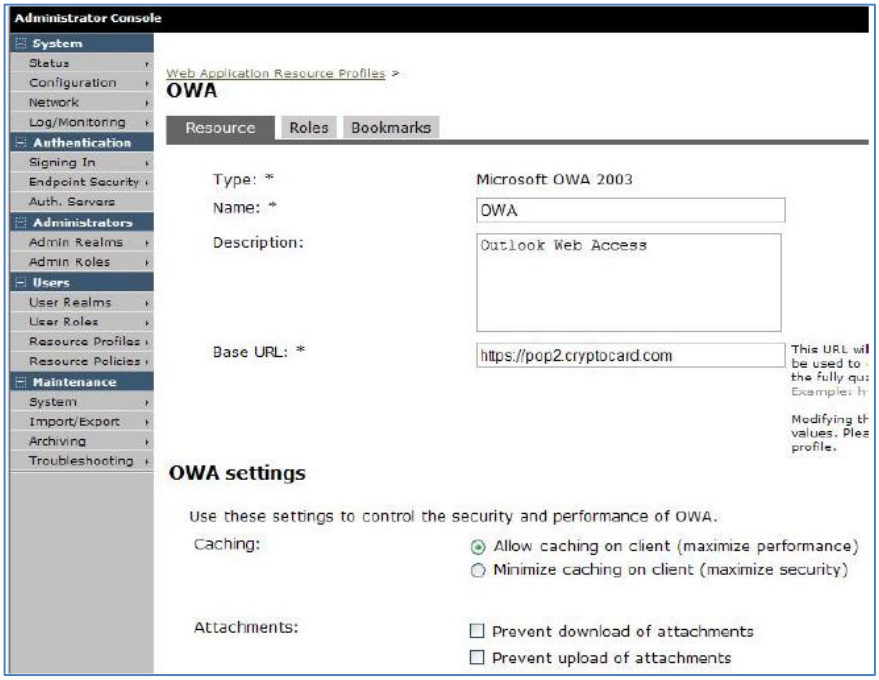
13. In the left pane, click **User Realms**.
    a. On the **General** tab, add the Active Directory Authentication as the first server.
    b. Select the **Additional authentication server** option, and then add the RADIUS authentication.
    c. In the **Username** field, select **predefined as:** and enter **<USERNAME>**. Do not enter **<USER>**.



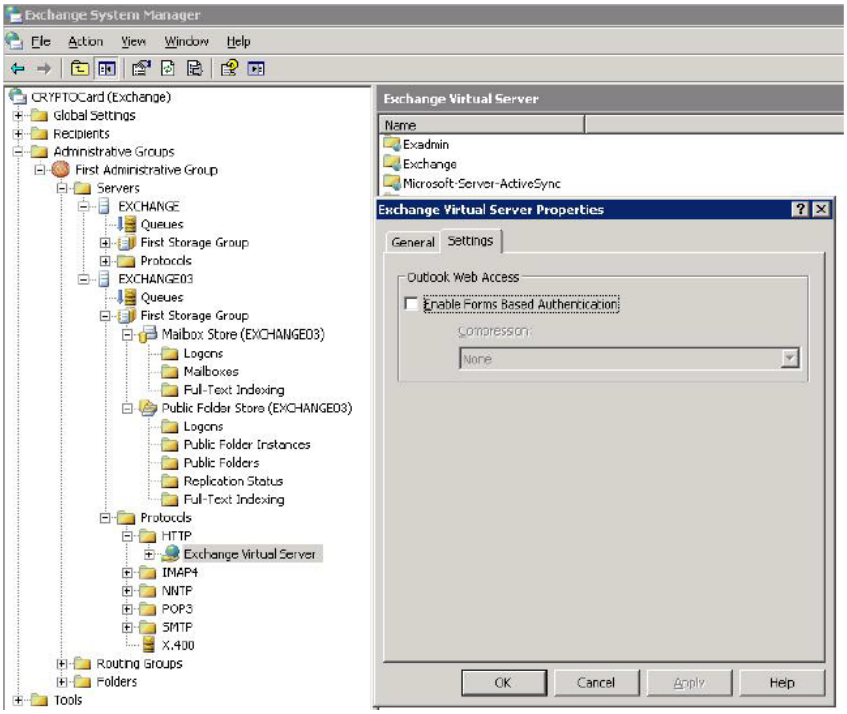
14. Edit the **Default Sign-In Page** or the page that you are using so that the **Secondary password** field reads **OTP**.



15. In **Resource Profiles / Web**, add a new Profile for OWA. Make sure to add the users on the **Roles** tab.



16. In the Exchange System Manager, clear the **Enable Forms Based Authentication** option. The SSO will not work with Forms Based Authentication.

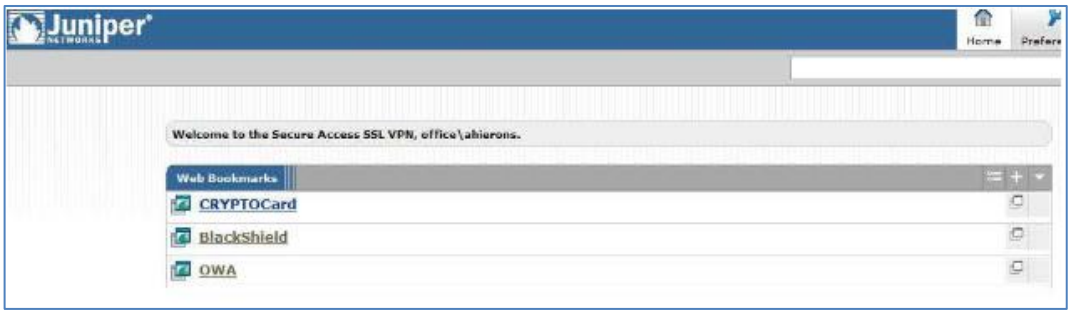


Testing Authentication

The next step is to test the newly configured two-factor authentication.

1. Open a web browser and go to: **http://JuniperSSLVPN.DNS.Name/**
2. Enter your username, Active Directory password, and an OTP passcode.
3. Click **Sign In**.

4. If you successfully authenticate, the following screen should appear:



Troubleshooting

Failed Logons

Symptom	Login Failed
Indication	11/19/2008 12:36:49 PM Henry Authentication Failure 312191514 192.168.2.1 Invalid OTP
Possible Causes	The one-time password provided for the user is incorrect.
Solution	Attempt to re-authenticate against SAS. If it comes up as invalid OTP again, test the token out via the SAS Manager.

Symptom	Login Failed
Indication	11/19/2008 12:47:24 PM Henry Authentication Failure 312191514 192.168.2.1 Invalid PIN
Possible Causes	The PIN provided for the user is incorrect.
Solution	Attempt to re-authenticate against SAS. If it comes up as invalid PIN again, changing the initial PIN back to default and forcing a PIN change would solve the issue, or have the user access the SAS Self-Service page.

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.

Table 1: Support Contacts

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.	