SafeNet Authentication Service

Integration Guide

Strong Authentication for Juniper Networks SSL VPN

SafeNet. THE DATA PROTECTION COMPANY

Document Information

Document Part Number	007-012641-001, Rev A
Release Date	Sept 2010

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.

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

Preparation and Prerequisites

- Ensure end users can authenticate through the Juniper SSL VPN with a static password before configuring RADIUS authentication.
- For SAS Server:
  - SAS ID NPS IAS Agent 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 Server or SAS Cloud:
  - Create or define a “Test” account that will be used to verify that the Juniper SSL VPN has been properly configured. Ensure that the user name for this account exists in SAS by locating it in the **Assignment** tab.
  - Verify that the “Test” user account can successfully authenticate with a static password, to the 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.

Configuration

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, click **Auth Servers**.
3. From the **New** list, and select **Radius Server**.
4. Click the **New Server** button.

5. Enter a name for the new RADIUS server.
6. Enter the IP address or DNS name of the Primary SAS RADIUS server in the **Radius Server** field.
7. Enter a shared secret in the **Shared Secret** field.
8. Select the **Users authenticate using tokens and one-time passwords** option.

9. Click **Save Changes**.

Optional: If there is a Secondary SAS RADIUS Server, complete all fields in the **Backup Server** section.

NOTE: If the Juniper SSL VPN has other realms created, skip the rest of this section and go to the “Advanced Configuration” section.

Applying a RADIUS Server to a User Realm

After the new RADIUS server has been created, it needs to be applied to a User Realm.

1. On the left side, select **User Realms**.
2. Select **Users > General**.
3. Under **Servers**, make the following settings:
   - **Authentication:** Select the new RADIUS Server was just created.
   - **Directory/Attribute:** Change to **Same as above**.
   - **Accounting:** Select the new RADIUS Server was just created.
4. Click **Save Changes** when completed.

5. Next is to check the Sign-in Policies section to ensure that the default User URL is set to allow all User Realms to authenticate.

6. Ensure that the Authentication Realm(s) section has say ALL. This means that any User Realms created within the Juniper SSL VPN can authenticate to this User URL.

Testing SAS Authentication

Next, step is to test authentication against SAS via RADIUS with the newly configured Juniper SSL VPN web login portal.

1. Open up a web browser and go to: http://JuniperSSLVPN.DNS.Name/
2. Enter in a username and the one-time password from a SafeNet token.
3. Click **Sign In**.

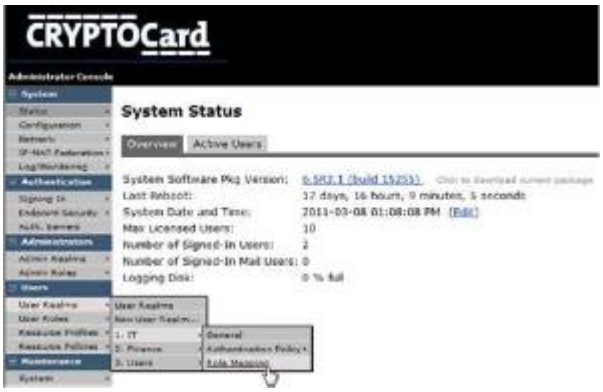
4. If the authentication is successful, the user will see the following screen.

Advanced Configuration

After configuring the Juniper SSL VPN for Radius authentication, the Juniper device may have issues applying the proper User Realm to the user that is authenticating. This is due to the RADIUS Server returns an access-accept, but the Juniper SSL VPN does not know which role to map to that user. To resolve this issue, a RADIUS Return Attribute of Filter-Id is added to the role mapping.

Adding Filter-Id to a User Realm in Juniper SSL VPN

1. Log in to the Juniper SSL VPN Administrative web portal.
2. Go down to the **Users** section.
3. Highlight **User Realms**.
4. Highlight the User Realm where the Filter-Id attribute will be added.
5. Click **Role Mapping**.



6. On the **Role Mapping** tab, click the **New Rule** button.
7. On the **Role Mapping Rule** web page, do the following:
   a. Under the **Rule based on**, select **User attribute**.
   b. Click the **Update** button
   c. Under the **Attribute** section, select **Filter-Id (11)**.
   d. In the text box, type in a name for the Filter-Id (e.g., Information Technology)
   e. Under **…then assign these roles**, select the role(s) that will be assigned users after a successful authentication and the correct Filter-Id has been returned to the Juniper SSL VPN device.
   f. Click **Save Changes**.

8. Next, check the **Sign-in Policies** section to ensure that the default User URL is set to use the User Realm that has the Filter-Id added as a Role Mapping.

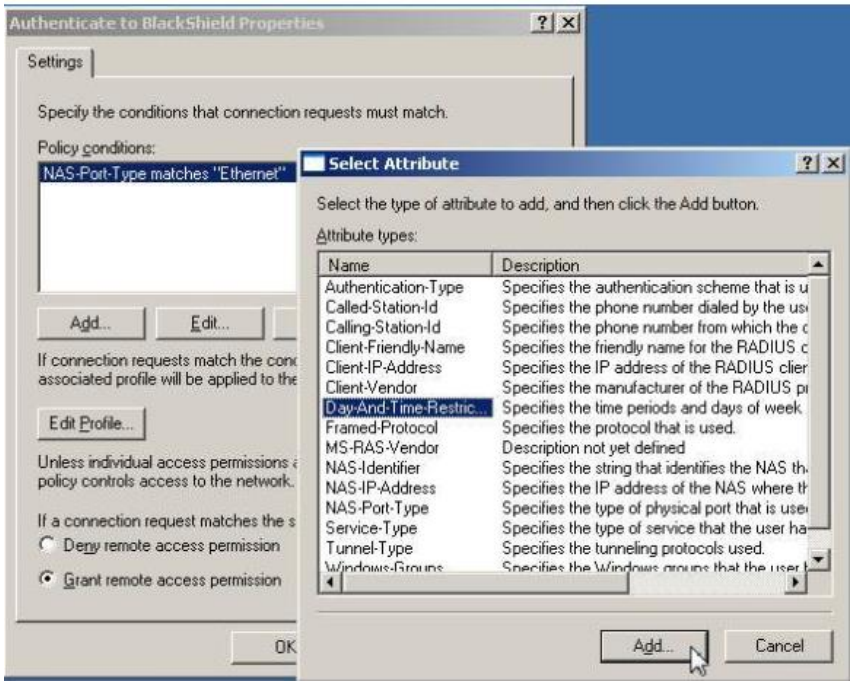
9. Ensure that the Authentication Realm(s) section has only the correct User Realm displayed. This means that that User Realms created within the Juniper SSL VPN can authenticate to this User URL.

Adding Filter-Id attribute to Remote Access Policy (Windows 2003)

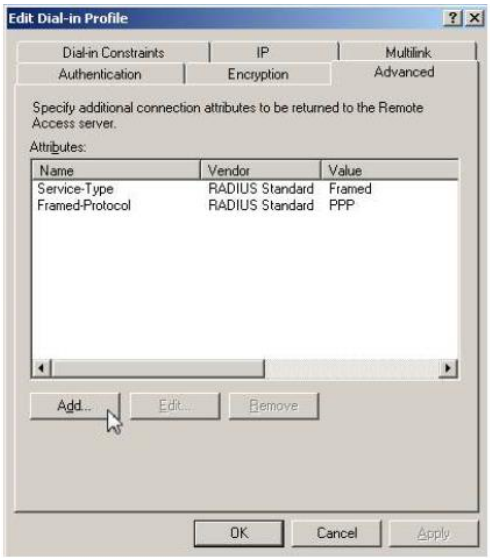
This is section is specifically for adding a Filter-Id attribute to a Remote Access Policy within Windows 2003 Internet Authentication Service (IAS). To add a new Network Policy with a Filter-Id in Microsoft Network Policy Server, on Windows 2008, refer to “Creating a New Network Policy with Filter-Id Attribute (Windows 2008)” on page 13.

1. Open Microsoft Internet Authentication Service (2003).
2. Select **Remote Access Policies**.

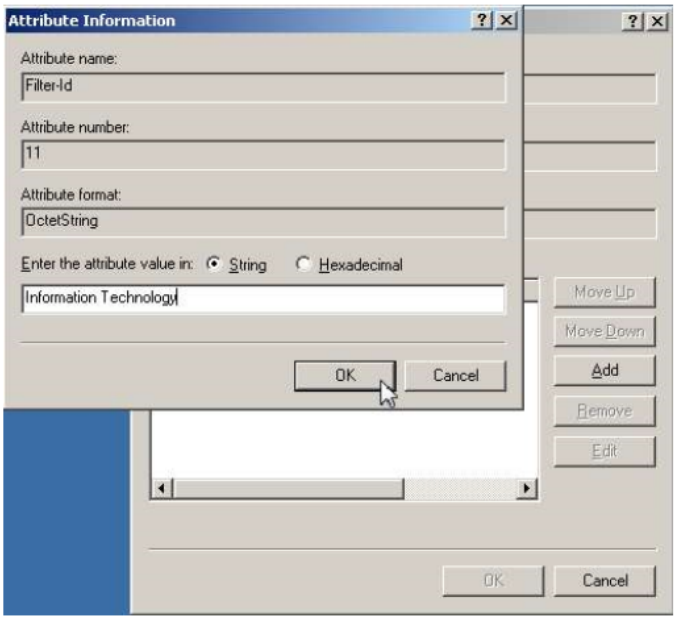
3. Right-click **Authenticate to SAS** and select **Properties**.
   - Verify that the **NAS-Port-Type** is **Ethernet**.
   - Click the **Remove** button, and then click the **Add** button
   - Select **Day-And-Time-Restrictions**, then and click **Add**.



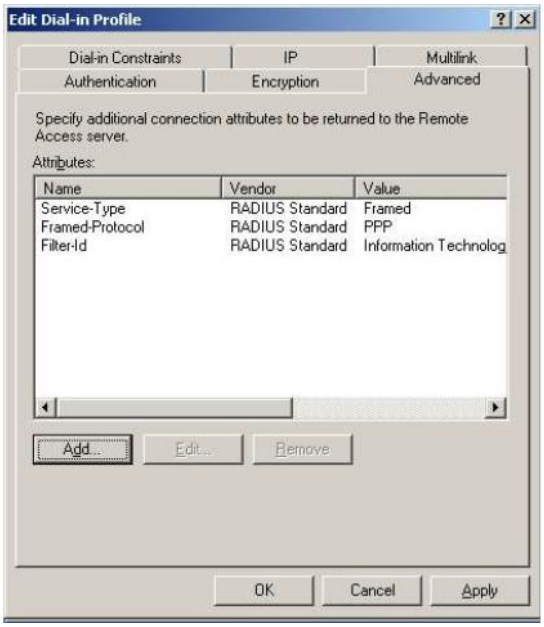
4. Select the **Permitted** radio button
5. Click **OK > Apply**.
6. In the **Authenticate to SAS Properties** window, click **Edit Profile**.
7. In the **Edit Dial-in Profile** window, click the **Advanced** tab.
8. Click the **Add** button.
9. Select the Filter-Id, and then click **Add**.



10. In the new window, click the **Add** button
11. Another window appears. Select the **Filter-Id** value that was created previously.
12. Click **OK > OK > Close**.

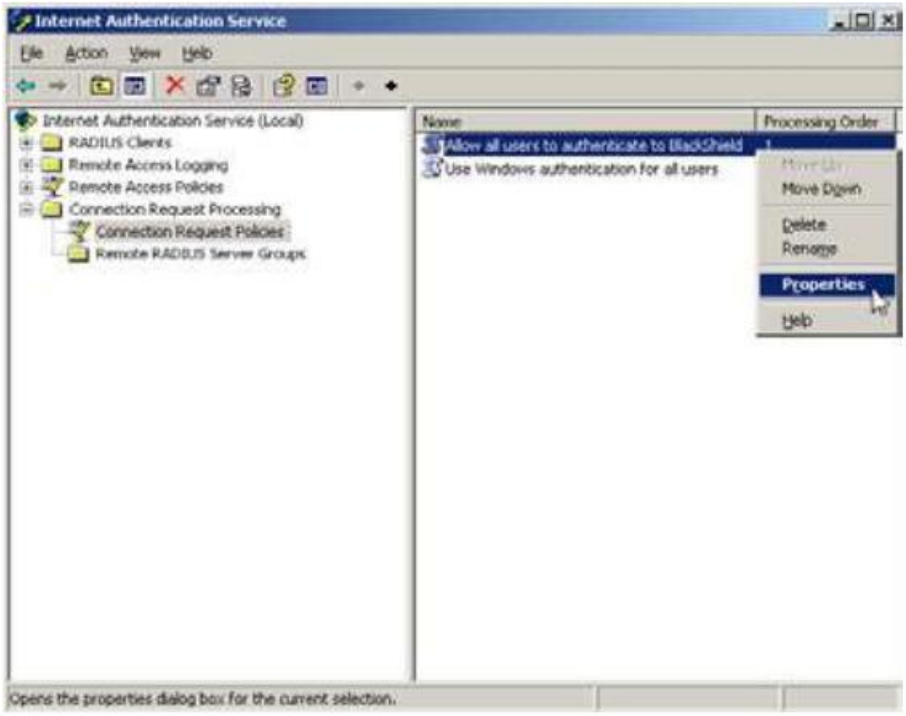


13. The **Advanced** tab will now display the new Filter-Id that has been added to this Remote Access Policy.
14. Click **OK > OK**.

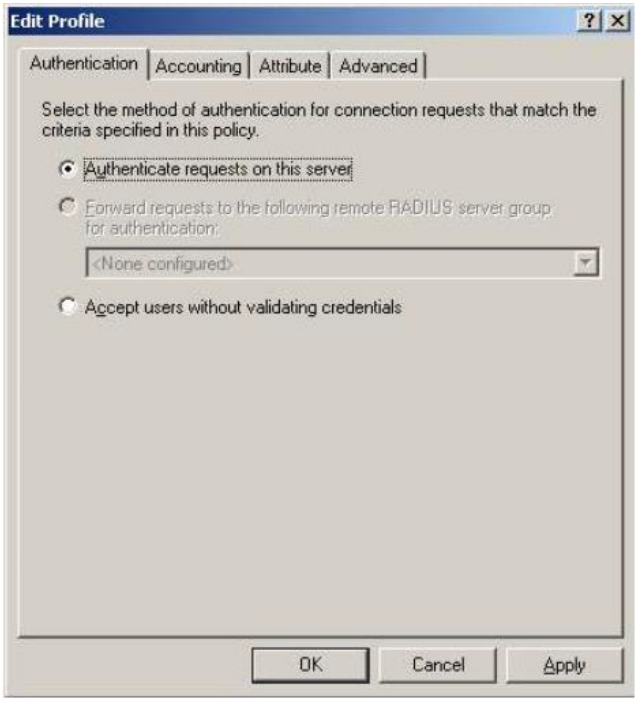


15. Expand **Connection Request Processing** in IAS
16. Select **Connection Request Policies**.

17. Right-click on the policy that was created for SAS and select **Properties**.



18. In the **Authentication** tab, select the **Authenticate requests on this server** option.
19. Click **OK**.



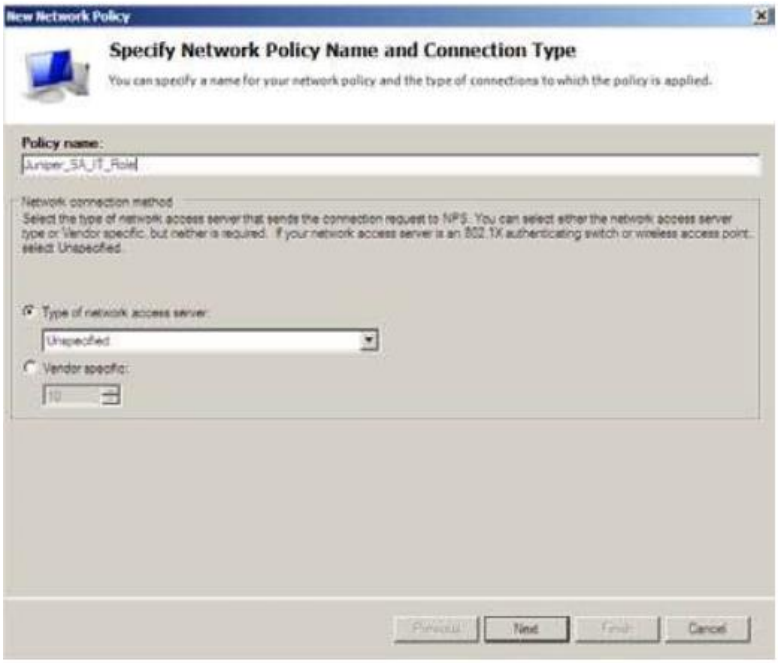
20. After all changes have been made, open Windows Services and restart Internet Authentication Service.

Creating a New Network Policy with Filter-Id Attribute (Windows 2008)

This is section is specifically for adding a new Network Policy along with a Filter-Id attribute to Network Policy within Windows 2008 Network Policy Server (NPS). To add a Filter-Id attribute to a Remote Access Policy in Microsoft Internet Authentication Service on Windows 2003, refer to “Adding Filter-Id attribute to Remote Access Policy (Windows 2003)” on page 9.

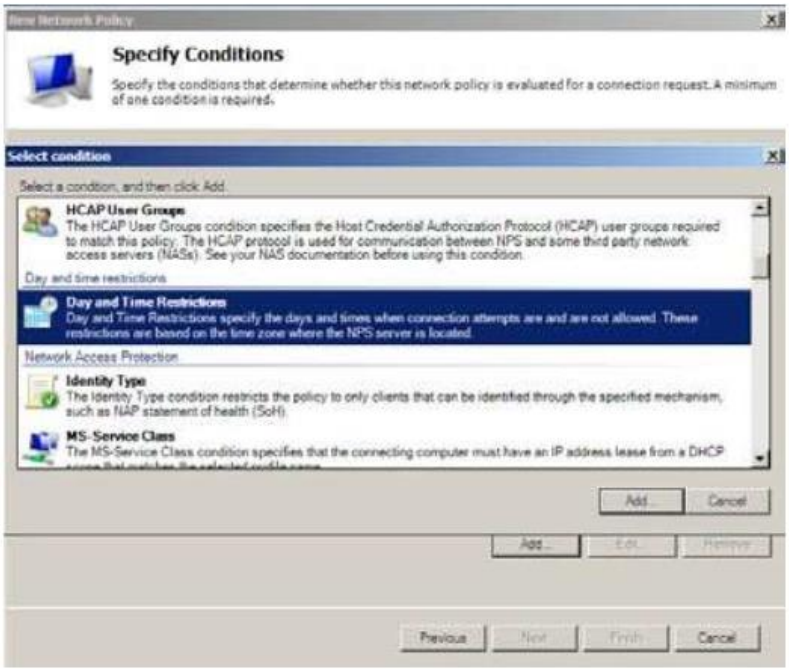
1. Open Microsoft Network Policy Server (2008)
2. Expand **Policies**.
3. Select **Network Policies**.
4. Right-click **Network Policies** and select **New**.

5. Enter in a name for the new Network Policy in the **Policy name** field.
6. Ensure **Type of network access server** is set to **Unspecified**.
7. Click **Next** to continue.

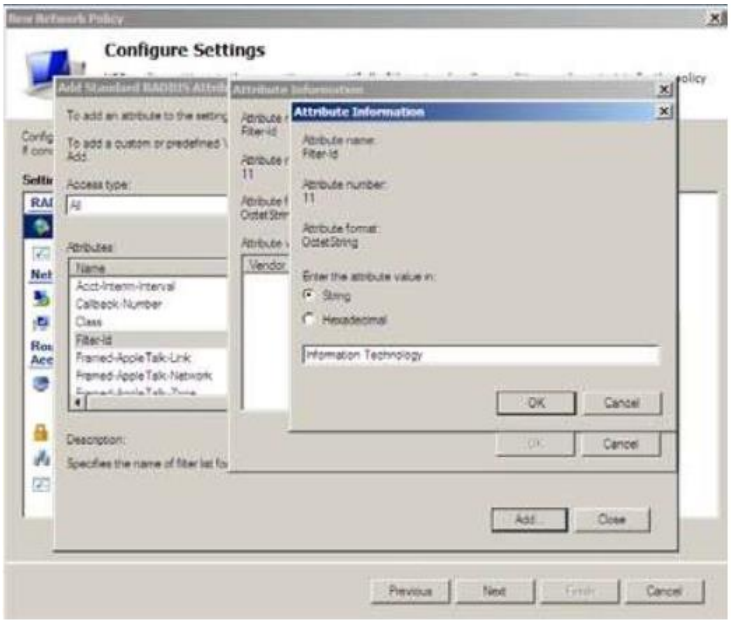


8. Click the **Add** button to add a new condition.

9. Scroll down and select **Day and Time Restrictions** and click **Add**.

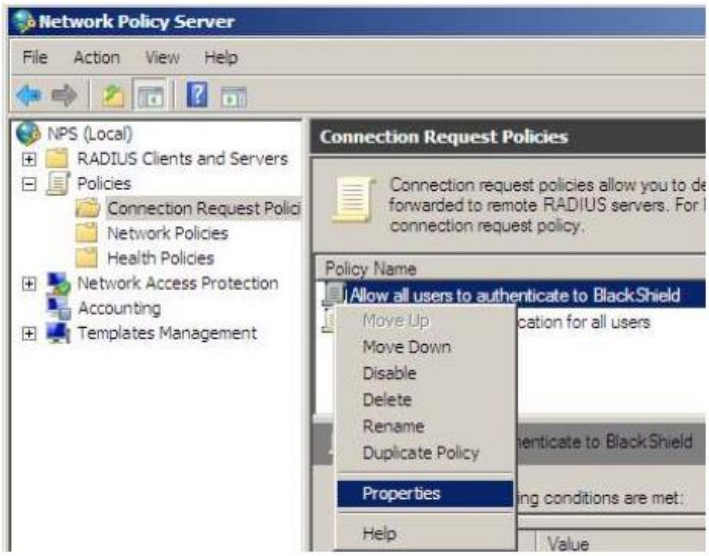


10. Select the **Permitted** radio button, and then click **OK**.
11. Click **Next** to continue.
12. Select the **Access granted** radio button
13. Click the **Next** button three times
14. Click the **Add** button to add a new attribute
15. Select **Filter-Id** and click **Add**.
16. Click the **Add** button, and then select the **Filter-Id** value that was created previously.



17. Click **OK > OK**.
18. Click the **Close** button.

19. Click **Next**.
20. Click **Finish** to create the new network policy.
21. Select **Connection Request Policies** in NPS.
22. Right-click on the policy that was created for SAS and select **Properties**.



23. Select the **Settings** tab and then select **Authentication** on the left side.
24. On the right side, select the **Authenticate requests on this server** option.
25. Click **OK**.
26. After all changes have been made, open Windows Services and restart Network Policy Server.

Juniper SSL VPN and GrIDsure Support

The Juniper SSL VPN login page can be configured to authenticate hardware and GrIDsure token users.

1. The user enters the Juniper SSL VPN URL into their web browser.
2. The Juniper SSL VPN login page displays a Username and OTP field as well as a Login and Get GrID button.
3. The user enters their username into the Username field then selects Get Grid. The request is submitted from the user's web browser to the SAS Self-Service site.
4. The SAS Self-Service site displays the user's GrIDsure Grid within the Juniper SSL VPN login page.
5. The user enters their GrIDsure password into the OTP field then submits the request.
6. The Juniper SSL VPN device performs a RADIUS authentication request against the SAS server. If the SafeNet credentials entered are valid, the user is presented with their Juniper SSL VPN portal otherwise, the attempt is rejected.

Prerequisites

1. The Juniper SSL VPN device must support uploading custom login pages (Juniper SSL VPN model SA 2500 or higher).
2. The SAS Self-Service Site must be publicly accessible to SSL VPN clients.
3. The Juniper device must already be configured to perform RADIUS authentication against the SAS server.

Adding the SAS Self-Service URL to the gridsure.js file

1. Open **gridsure.js** with a text editor.
2. Change the value of gridMakerURL to reflect the location of your SAS Self-Service website then save the file.

   Example: var gridMakerURL = "https://www.mycompany.com/blackshieldss/index.aspx?getChallengeImage=true&userNa me=";

Adding the GrIDsure-enabled Sign-in Page

1. Log in as an administrator to the Juniper device.
2. Select **Authentication > Signing In > Sign-In Pages**.
3. Select the **Upload Custom Pages** button.
4. In the **Sample Templates Files** section select **Sample**. Download **sample.zip** to a Juniper SSL VPN and GrIDsure support temporary folder.
5. Rename the **sample.zip** file to **safenet.zip**.
6. Add the **gridsure.js** and **LoginPage.thtml** file to **safenet.zip** (if prompted, overwrite the existing **LoginPage.thtml** file).
7. In **Upload Custom Sign-In Pages**, enter **SafeNet GrID Enabled** into the **Name** field and in **Page Type** select **Access**. In **Templates File**, browse to the **safenet.zip** file and then select the **Upload Custom Pages** button.

Assigning the SafeNet GrIDsure-enabled Sign-in page to a Sign-in Policy

1. Login as an administrator to the Juniper device.
2. Select **Authentication > Signing In > Sign-In Policies**.
3. Select the SAS authentication-enabled **User URL**.
4. In the **Sign-In** page section, select **SafeNet GrID Enabled** and then save the settings.

Login as a SafeNet GrIDsure-enabled User

1. Open a web browser and browse to the SafeNet-enabled Juniper SSL VPN sign-in page.
2. Enter the username then select the **Get Grid** button, a grid will appear in the screen.
3. Enter the PIP into the password field then select **Sign-in**.

Optional - Enable Challenge-response Requests

1. Log in as an administrator to the Juniper device.
2. Select **Authentication > Auth. Servers**.
3. Select the SafeNet RADIUS enabled authentication server.
4. In **Custom Radius Rules**, select **New Radius Rule**.
   - In **Display Name**, enter **Display challenges**.
   - Set **Response Packet Type** to **Access Challenge**.
   - In **Attribute criteria**, set **Radius Attribute** to **Reply-Message(18)** with a "Value" of "*".
   - In **Then take action...**, select **show Generic Login page**.
5. Save the changes.

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.	