SafeNet Authentication Service

Integration Guide

Juniper Steel Belted RADIUS 6.x

Document Information

Document Part Number	007-012643-001, Rev A
Release Date	Oct 2009

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 Steel Belted RADIUS. 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

This document presents the necessary steps to configure Steel Belted RADIUS for use with SafeNet tokens.

The SAS server works in conjunction with Steel Belted RADIUS to replace static passwords with strong two-factor authentication that prevents the use of lost, stolen, shared, or easily guessed passwords when establishing a tunnel to gain access to protected resources:

1. A user establishes a connection using their logon name and SafeNet token-generated one-time password.
2. The network device passes the authentication information via RADIUS to Steel Belted RADIUS. Steel Belted RADIUS identifies the Authentication Policy as SafeNet and then forwards the authentication request to the SAS server.
3. The SAS server verifies the username and password and an “Access-Accept” message is returned to Steel Belted RADIUS, allowing the user to access the network.

Solution Overview

Summary	
Product Name	Steel Belted RADIUS 6.x
Vendor Site	http://www.juniper.net
Authentication Method	SafeNet Agent

Supported SAS and RADIUS Functionality	
RADIUS Authentication Encryption	PAP
Authentication Mode	• One-time password • Challenge-response • SAS static password
New PIN Mode	• User-changeable Alphanumeric 3-16 digit PIN • User-changeable Numeric 3-16 digit PIN • Server-changeable Alphanumeric 3-16 digit PIN • Server-changeable Numeric 3-16 digit PIN

Prerequisites

The following must be installed and operational prior to configuring Steel Belted RADIUS to use SAS authentication:

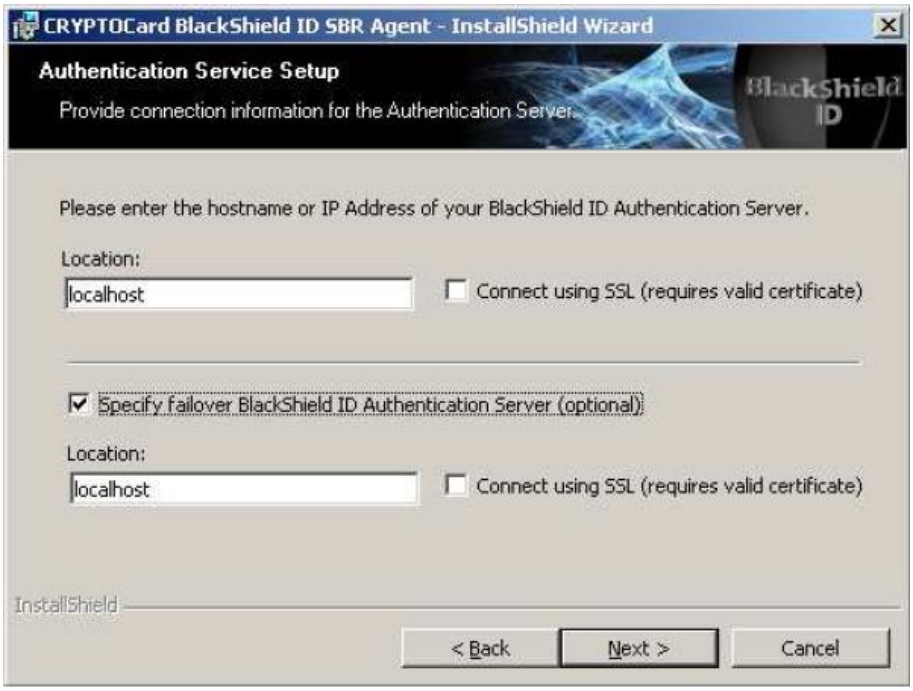
- Ensure end users can authenticate through Steel Belted RADIUS with a static password before enabling the SAS authentication method.
- The SAS server is installed and a user account assigned with a SafeNet token.

The following SAS server configuration information is required:

- IP Address of the Primary SAS server
- IP Address of the Secondary SAS server (optional)

Installing the SAS Steel Belted RADIUS Agent

1. On the Steel Belted RADIUS Server, launch the SAS Steel Belted RADIUS agent.
2. Accept the SafeNet License Agreement and select the destination folder.
3. In the **Location** field, enter the IP address or host name of the SAS server.
4. If required, select the **Specify failover server** option and then enter the IP address or host name of the SAS server in the **Location** field.



5. The **Connect using SSL** option can be used if the IIS Web Server where SAS resides has been configured to use SSL.
6. Restart the Steel Belted RADIUS service.
7. If a firewall exists between Steel Belted RADIUS and SAS, verify that TCP port 80 and/or 443 are available.

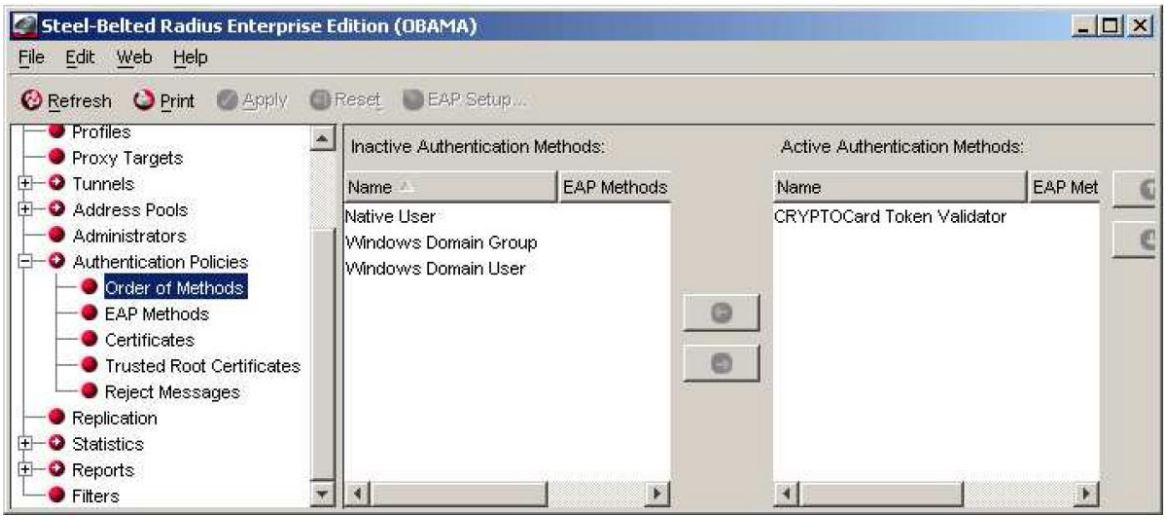
Configuring Steel Belted RADIUS

In order for Steel Belted RADIUS to authenticate SafeNet token users, SAS authentication must be enabled within Authentication Policies and Profile entries must be created.

Configuring Steel Belted RADIUS consists of 2 steps:

- Enabling SafeNet as an Authentication Policy
- Creating Profile entries

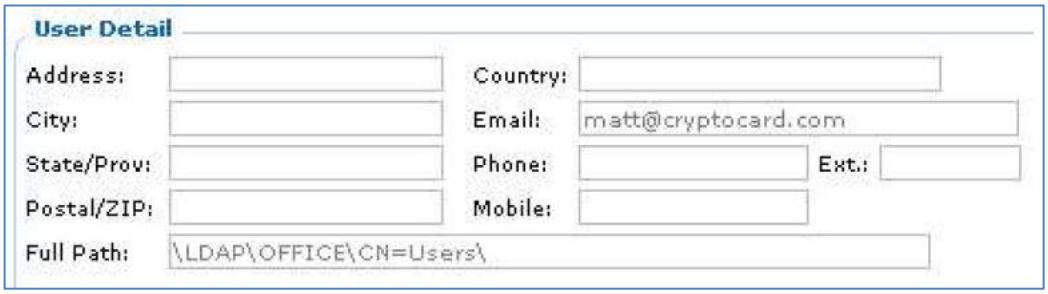
1. In the Steel Belted RADIUS Administrator, select **Authentication Policies > Order of Methods**.
2. In **Active Authentication Methods**, verify that the SafeNet Token Validator is the first or only entry in the list.
3. Apply the setting and then restart the Steel Belted RADIUS service for the setting to take effect.



Creating Profile entries

If users are located in an SQL or LDAP container, a profile with the same name must exist in Steel Belted Radius for the user to successfully authenticate.

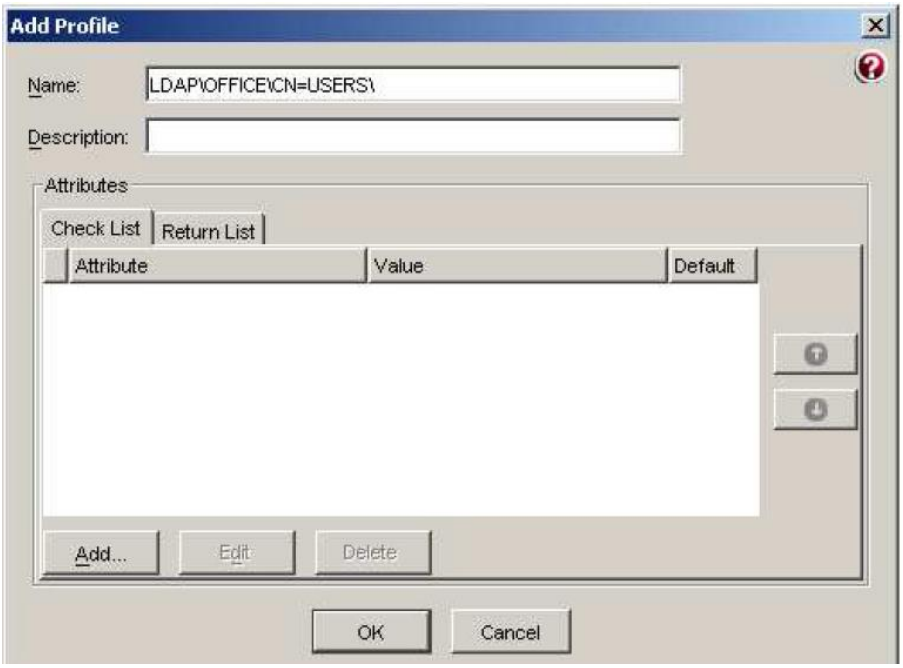
1. On the **Secured Users** or **Assignment** tab, make note of the **Full Path** location of the user.



Ex. Full Path: \LDAP\OFFICE\CN=Users\In the Steel Belted RADIUS Administrator select Profiles.

2. Enter the SAS **Full Path** entry as the name of the Steel Belted RADIUS Profile. The Profile name must not begin with a backslash.

   For example, if the **Full Path** in SAS is **\LDAP\OFFICE\CN=Users**, the Steel Belted RADIUS Profile name will be **LDAP\OFFICE\CN=Users**.



Customizing Reply Messages

The **ccAuthSBR.aut** file found in the **\Program Files\Juniper Networks\Steel-Belted Radius\Service** directory allows for customization of the text strings presented to users.

Any text after the equal sign may be changed to suit your companies' needs.

The following entries exist:

- CHALLENGE=Please respond to the challenge:
- SERVER_PIN_PROVIDED=Please re-authenticate, using the next response. Your new PIN is:
- USER_PIN_CHANGE=Please enter a new PIN.
- OUTER_WINDOW_AUTH=Please re-authenticate, using the next response.
- CHANGE_STATIC_PASSWORD=Your password has expired. Please select a new password.
- STATIC_CHANGE_FAILED=Password change failed. Please select a new password.
- PIN_CHANGE_FAILED=PIN change failed. Please select a new PIN.

Troubleshooting

Steel Belted RADIUS Logs

When troubleshooting authentication issues in Steel Belted RADIUS to refer to the log files in the **\Program Files\Juniper Networks\Steel-Belted Radius\Service** directory.

The Steel Belted RADIUS logging level can be changed in **the \Program Files\Juniper Networks\Steel-Belted Radius\Service\radius.ini** file. In the **[Configuration]** section, change **LogLevel** and **TraceLevel** to **3**. Restart the Steel Belted RADIUS server for the setting to take effect.

SAS Steel Belted RADIUS Agent Logs

All logging information for the SAS Steel Belted RADIUS Agent can be found in the **\Program Files\CRYPTOCard\BlackShield ID\SBR Agent\log** directory. The logging level can be changed in the Registry under the **HKEY_LOCAL_MACHINE\SOFTWARE\CRYPTOCard\AuthSBR** key. Change **LogLevel** from **3** to **5**. Restart the Steel Belted RADIUS server for the setting to take effect.

Common Errors

Symptom	Possible Causes and Solutions
The Steel Belted RADIUS log file displays the message "Profile <RANDOM_NAME> required for user <username> does not exist"	Verify the SAS **Full Path** in the **Assignment** or **Secured Users** tab for the user exists as a Profile in Steel Belted RADIUS.
The Steel Belted RADIUS log file displays the message "Unable to find user <username> with matching password."	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 SAS password does not match any tokens for that user. • The SAS Agent for Steel Belted RADIUS cannot contact the SAS Server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for Steel Belted RADIUS. • The SAS Agent for Steel Belted RADIUS Keyfile does not match the Keyfile stored on the SAS Server.
The SAS agent for Steel Belted RADIUS log file displays the message "Send Failed. Could not connect to host. Timed out [A connection with the server could not be established > msxml6.dll]."	This will occur when one or more of the following conditions occur: • The WWW Web service or Token Validator website is not running on the SAS server. • The Pre-Authentication Rules on the SAS server do not allow incoming requests from the SAS Agent for Steel Belted RADIUS. • The SAS Agent for Steel Belted RADIUS Keyfile does not match the Keyfile stored on the SAS Server.

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.	