Steel Belted RADIUS (SBR) to Pulse Policy Secure Migration Guide

The information in this document is current as of the date on the title page.

END USER LICENSE AGREEMENT

The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at www.pulsesecure.net. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”
Contents

Executive Overview ........................................................................................................... 4

Introduction ...................................................................................................................... 4
  Supported Migration Use cases .................................................................................... 4

RADIUS Configuration Migration .................................................................................. 5

Exporting SBR XML Configuration .............................................................................. 6

Importing SBR XML file to PPS ................................................................................... 7
  Authentication Server on PPS ..................................................................................... 7
  User Creation on PPS ................................................................................................. 9
  Sign-In Page on PPS ................................................................................................... 9
  Sign-In Policy ............................................................................................................. 10
  Authentication Protocol Sets ...................................................................................... 10
  Roles .......................................................................................................................... 11
  User Realms ............................................................................................................... 12
  Network Location Group Configured on SBR ............................................................ 12
  Location Group on PPS .............................................................................................. 13
  RADIUS Client Configured on SBR .......................................................................... 14
  Creating a new RADIUS Client on PPS ................................................................. 15
  RADIUS Return Attribute on SBR .......................................................................... 16
  Configuring RADIUS Return Attribute Policies on PPS ........................................ 17

MAC Address Authentication Migration ........................................................................ 18
  Importing MAC Address from SBR into PPS ........................................................ 18

References ...................................................................................................................... 18
Executive Overview

Pulse Secure is a leader in providing the industry’s best Next-Gen Network Access Control solutions. Pulse Policy Secure (PPS) with inbuilt RADIUS server offers scalable 802.1X deployment with Role-based access control that reduces network threat exposure and mitigates risks to zero-trust security.

PPS migration tools enable seamless deployment of authentication mechanisms, allowing customers to easily migrate from Steel Belted Radius (SBR) to PPS. Migration tools also provide customers with the flexibility of migrating 802.1X/RADIUS, MAC Address Authentication configurations.

PPS migration helps customers to achieve contextual based endpoint visibility, a much stronger security posture with unified access policies that extend from BYOD systems to their perimeter defenses. Customers are also going to benefit from comprehensive NAC solutions, Visibility, Policy Management, Sponsored-based Guest Access, BYOD/Mobility, Endpoint Compliance, Ecosystem Integrations and Zero-Trust Internet of Things (IoT) Security.

Introduction

This document provides detailed information about the migration steps from SBR to Pulse Policy Secure (PPS). The document captures the manual migration approach for the 802.1X/RADIUS, MAC Address authentication use cases. Export the configurations from SBR and then import them into PPS. The default configurations are created for smooth migration.

The migration procedure starts with comparing the configuration settings from SBR and then configuring on PPS. Ensure that you understand the configuration flow of Pulse Policy Secure and verify them against the access policies of SBR.

PPS supports role-based access control. The level of access to the network is determined based on the user roles and various other attributes. For example, an individual with the engineer role in an organization might be allowed access to the certain company's resources, but blocked access to employee records.

However, SBR is profile-based access control. The access is determined based on the profiles associated with Users or RADIUS clients or Location groups. The access is determined based on the check properties of the request against the configured checklist of attributes.

Note:

Ensure that you configure the PPS based on the configuration flow for easy migration. The equivalent SBR terminologies for configuration is documented in RADIUS Configuration Migration and MAC Address Authentication Migration sections. Plan your migration carefully to ensure smooth migration and to decrease any risk of migration failure.

Supported Migration Use cases

You can migrate all the RADIUS configurations such as Location groups, RADIUS Clients and Profiles and MAC addresses configurations from SBR to PPS.
RADIUS Configuration Migration

The configuration flow for RADIUS based authentication on PPS and the equivalent configuration on SBR is described in the below table. The examples documented in this guide is based on SBR latest Release version.

Table 1 describes the recommended configuration flow for PPS

<table>
<thead>
<tr>
<th>Step</th>
<th>Configuration on SBR</th>
<th>Equivalent configuration on PPS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Configure Users &gt; Native &gt; Add Native Users.</td>
<td>Configure Authentication Server</td>
</tr>
<tr>
<td>Step 2</td>
<td>SBR profile-based authentication.</td>
<td>Configure the Authentication Realm, Role mapping rules and Sign-In Policy.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure SBR &gt; Location Groups.</td>
<td>Configure the Location Group</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure SBR &gt; Radius Client</td>
<td>Configure a RADIUS client</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure SBR &gt; Profiles.</td>
<td>Create RADIUS return attribute policy</td>
</tr>
</tbody>
</table>
Exporting SBR XML Configuration

To export the SBR configurations:

1. Run the SBR Administrator.
2. Choose File > Export.
3. In the Export dialog, select the information to export. Each tab in the dialog lists exportable items of a particular category. For each category, select the appropriate tab and click each item you'd like to export. To select a contiguous range of items, select the first item in the range, hold down the Shift key, and click the last item in the range.
   - To select a non-contiguous set of items, hold down the Ctrl key as you click each item you want.
   - To select all items in a category, click All.
   - To select all items in all categories, click Select All.

4. After you have selected the items to export, click OK.

5. In the Export to XML file dialog, enter the file name and click Save.
Importing SBR XML file to PPS

To import the SBR XML file to PPS from PPS Admin console:

1. Select **Maintenance > Import/Export > XML Import/Export > Import SBR Configuration**.
2. Click **Browse** and browse the SBR xml file which needs to be imported.
3. Click **Import**.

![Import SBR Configuration](image1)

Authentication Server on PPS

PPS provides a seamless migration from SBR server to PPS server. Once it is migrated it can be easily paired with an organization’s other identity databases, such as LDAP, RADIUS server and Active Directory (AD) to leverage existing credentials.

Import the SBR xml file to PPS. After importing the file:

1. Select **Authentication > Authentication Server**. You can see the imported file on PPS authentication server. Local Auth Server named as **SBRMigrationAuthServer** is created for SBR migration.
2. Auth Server will be created with default values.
3. Password storage type will be set to clear text by default.
4. Password must be different from user name and New Passwords must be different from previous password options will be disabled.

Figure – Authentication Server

![Authentication Servers](image2)
## Figure – Authentication Server Settings

### Settings

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>SPMigrationAuthServer</td>
<td></td>
</tr>
</tbody>
</table>

#### Password Options

| Minimum length | 10 characters |  
| Maximum length | 128 characters |  

- **Password must have at least** 1 digit(s)  
- **Password must have at least** 1 letter(s)  
- **Password must be different from username**  
- **New passwords must be different from previous password**  

#### Password Storage Type

- **Strong Hash**  
  - Note: Highly secure, but not compatible with some of the authentication protocols e.g. CHAP, EAP-MSCHAP and MS-CHAP V1/V2.  
- **Legacy Hash**  
  - This option can only be set during creation  
  - Note: Compatible with all authentication protocols e.g. CHAP, EAP-MSCHAP, Microsoft V1/V2 although not secure  
- **Clear Text**  
  - This option can only be set during creation  
  - Note: Compatible with all authentication protocols e.g. CHAP, EAP-MSCHAP, Microsoft V1/V2 although not secure  

#### Password Management

- **Allow users to change their password**  
- **Force password change after** 10 days before current password expires  

Note: Use options on the Administrators/Users > Authentication > [EAP]** Authentication Policy > Password page to specify which realms should inherit the server’s password management capabilities.  

#### Account Lockout

- **Enable Account Lockout for users**  
- **Maximum wrong password attempts** 3 and above  
- **Account Lockout period (minutes)** 10 and above  

#### Guest Access

- **Guest User Account Managers**  
  - **Enable Guest User Account Managers to administer Guest Accounts**  
  - **Instructions for Guest User Account Manager**  
    - **Guest User Account Manager**  
    - **Maximum Account Validity Period** 24 hours  
      - Set the Guest Account length limit and time minus the start time in hours. This is valid for guest accounts created by Guest Admin. Does not impact waiting user expirations.  

#### Guest Self-Registration

- **Send guest user credentials via**  
  - **Email**  
  - **Configure SAML**  
  - **Guest Self-Registration**  
  - **Show credentials on screen after guest completes registration**  
  - **Enable Sponsoring Guest Access**  
  - **Maximum Account Validity Period for Self Registered Guests** 1 day  
  - **Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact waiting user expirations.**  

Note: To enable Guest Self-Registration navigate to (Logging in > SAML Policies > User (AR) > [Edit] > Configure Guest Settings.  

### Common configuration for Guest User Account Managers and Guest Self-Registration

- **Guest User Name Prefix**  
- **Guest User Info Fields**  
  - Enter additional fields for guest user information, use field by field. For example  
    - **Company Name**  
    - **Sponsor**
User Creation on PPS

The Users are created on **SBRMigrationAuthServer**.

- Password will be stored in plain text.
- Default password will be *pulsesecure*.
- User must change password if next sign-in flag is enabled.
- If user in SBR contains attributes, it will added into attribute table of that user in PPS.
- If user in SBR has a profile associated with it, then attributes in the associated profile will be added into attribute table of that user in PPS.

![Users](image1)

Figure - Users

Sign-In Page on PPS

Select **Authentication > Signing In > Sign-In Pages**. You can see the SBR Sign-In Page created by default.

![Sign-In Pages](image2)

Figure - Sign-In Pages
Sign-In Policy

Select Authentication > Sign-In Policies.

The Sign-In policy user url */SBR/ with sign-in page as SBR Sign-In Page and Authentication Realm(s) as SBRMigRelam (802.1X) is created by default.

Figure - Sign-In Policies

Authentication Protocol Sets

Select Signing In > Authentication Protocol Sets. SBRmigration802.1X is created by default.

Figure – Authentication Protocol Set
Roles

Select Users > User Role > User Authentication Role. You can see the SBRMigRole user role created by default.

Figure – SBR Migration Role
User Realms

Select Users > User Realms > User Authentication Realms. You can see the SBRMigrationRealm realm.

Figure - Realm

SBRMigrationRole is added in the role mapping rules.

Figure – Role Mapping Rules

Network Location Group Configured on SBR

Select Steel-Belted Radius > Location Groups to view the location groups.

Figure – SBR Location Group
Location Group on PPS

Select **Endpoint Policy > Network Access > Location Group.** Location group contains */SBR/* in sign-in policies. Default **SBRMigLocGroup** is created for those Radius Client which is not using any profile and location group.

**Figure: Location Group**
RADIUS Client Configured on SBR

Select Steel-Belted Radius > RADIUS Clients to view the configured RADIUS client.

Figure SBR RADIUS client
Creating a new RADIUS Client on PPS

Select **Endpoint Policy > Network Access > RADIUS Client**.

For example, SBRMigrationRadiusClientPPS is configured as a RADIUS client.

![Figure – RADIUS client](image)

Note: If RADIUS client is not using profile and location group then the default Location group is used.

If a RADIUS Client is using Profiles then:

- If the profile is used by any of Location group: then will associate the RADIUS client with that location group
- If profile is not used by any location group, then a location group with name “SBRMigProfile<ProfileID/Name>” is created on PPS which will be associated to RADIUS Client.
RADIUS Return Attribute on SBR

Select Return List and note down the attribute and value.
Configuring RADIUS Return Attribute Policies on PPS

1. Select Endpoint Policy > Network Access > RADIUS Attributes > RADIUS Return Attributes.
2. Click Return Attributes tab to see the configured policies.

For example, SBRMigrationRadRetAttrdef

Figure – Return Attributes

Note:
- If Location group is using profile then will use those location group into profile.
- If RADIUS Client is using profile and no location group is using that profile, then the Location Group used during the creation of RADIUS client will be attached to that profile.
- If profile is not used by any location group or profile then it will not be imported.
- Only PPS supported attributes will be imported. For example, if SBR supports attribute_a, attribute_b and attribute_c and PPS supports attribute_a and attribute_b then profile will contain only attribute_a and attribute_b.
MAC Address Authentication Migration

Importing MAC Address from SBR into PPS

1. The username should be in MAC address format (‘:’, '-' or no separator).
   For example, 00-11-85-bb-c-67, 00:11:85:bb:8c:66 or 001185bb8c69
2. For MAC user, password will be username (Mac address.) by default.
3. Password is stored in plain text by default.
4. User must change password in next sign-in option will be disabled by default.

References

For more information on 802.1X authentication and troubleshooting, see 802.1X Authentication with Cisco Switch.