



Pulse Policy Secure: Steel Belted Radius Server

SBR to PPS Migration Guide

Pulse Secure, LLC
2700 Zanker Road, Suite 200 San Jose, CA 95134
www.pulsesecure.net

Pulse Secure and the Pulse Secure logo are trademarks of Pulse Secure, LLC in the United States. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Pulse Secure, LLC assumes no responsibility for any inaccuracies in this document. Pulse Secure, LLC reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

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
TACACS+ Migration	19
SBR TACACS+ config file	21
Importing SBR TACACS+ config file to PPS.....	21
Authentication Server	22
Users.....	22
Roles.....	23
Realm	23
Role Mapping	24
Device groups.....	24
Clients.....	25
Shell policies.....	26
References.....	28

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 and TACACS+ 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, 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

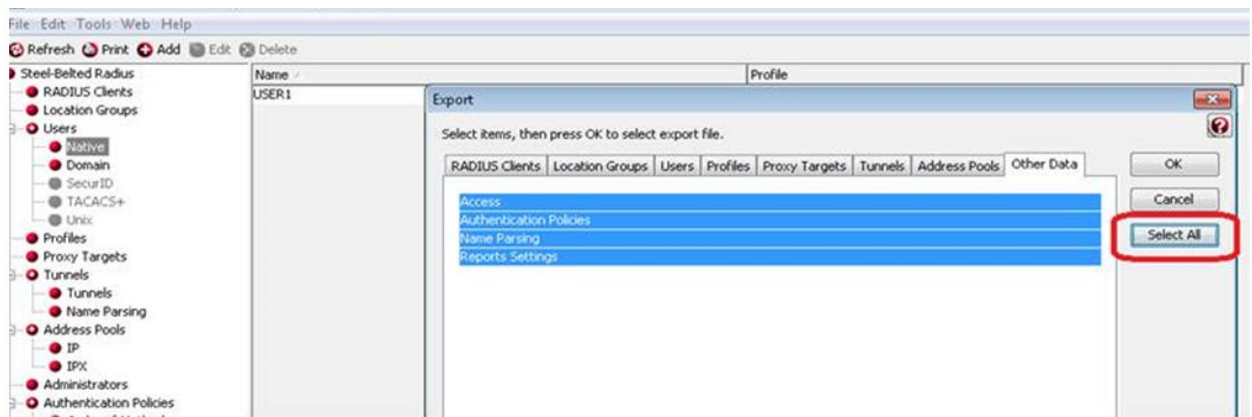
Table 1: Steps to Configure		
Step	Configuration on SBR	Equivalent configuration on PPS
Step 1	Configure Users > Native > Add Native Users.	Configure Authentication Server
Step 2	SBR profile-based authentication.	Configure the Authentication Realm, Role mapping rules and Sign-In Policy.
Step 3	Configure SBR > Location Groups.	Configure the Location Group
Step 4	Configure SBR > Radius Client	Configure a RADIUS client
Step 5	Configure SBR > Profiles.	Create RADIUS return attribute policy

Exporting SBR XML Configuration

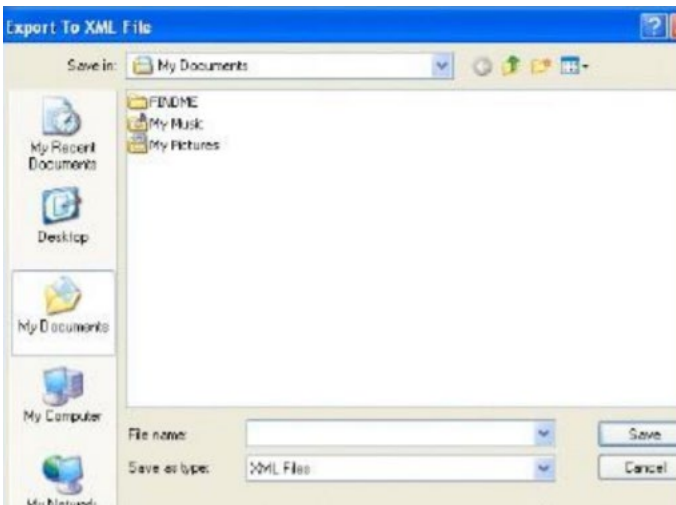
To export the SBR configurations:

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**.

Figure: Export



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

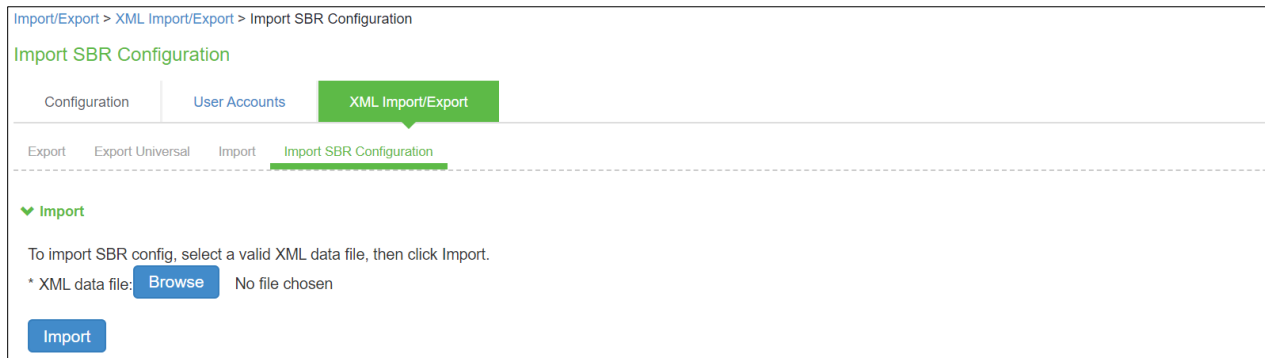


5. In the Export to XML file dialog, enter the file name and click **Save**.

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**.



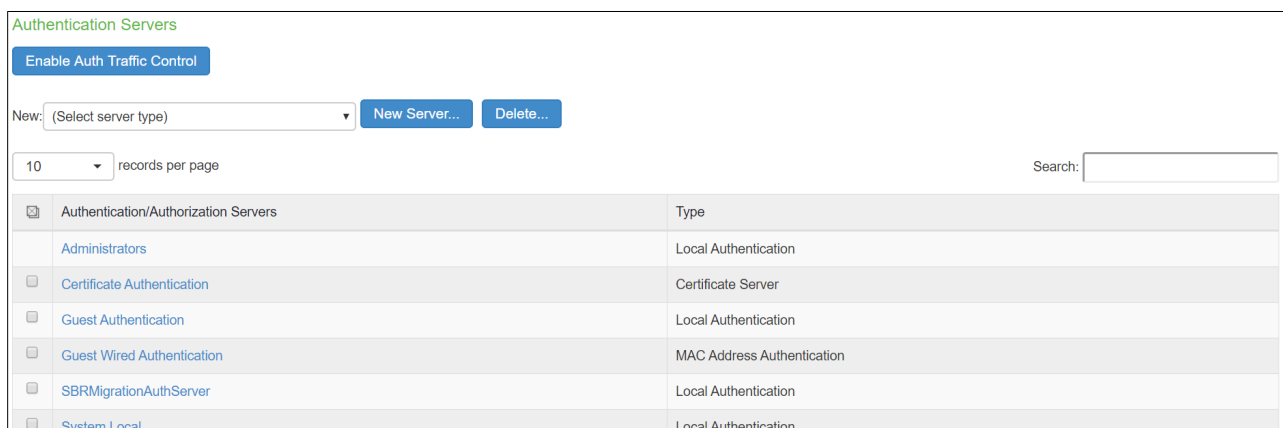
Authentication Server on PPS

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/Authorization Servers	Type
Administrators	Local Authentication
Certificate Authentication	Certificate Server
Guest Authentication	Local Authentication
Guest Wired Authentication	MAC Address Authentication
SBRMigrationAuthServer	Local Authentication
System Local	Local Authentication

Figure – Authentication Server Settings

Auth Servers > SBRMigrationAuthServer > Settings

Settings

UsersAdmin Users

*Name: SBRMigrationAuthServer Label to reference this server.

▼ Password Options

Minimum length: 10 characters

Maximum length: 128 characters

☐ Password must have at least 1 digits

☐ Password must have at least 1 letters

☐ Password must have mix of UPPERCASE and lowercase letters

☐ 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 i.e. CHAP, EAP-MD5 and MS-CHAP (V1/V2)

☐ Legacy Hash This option can only be set during create

Note: Compatible with MSCHAP(v1/v2) although less secure

☒ Clear Text This option can only be set during create

Note: Compatible with all authentication protocols i.e. CHAP, EAP-MD5, MSCHAP(v1/v2) although not secure

▼ Password Management

☒ Allow users to change their passwords

☐ Force password change after days

☐ Prompt users to change their password days before current password expires

Note: Use options on the Administrators/Users > Authentication > [Realm] > 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 (3 and above)

Account Lockout period (minutes): 10 (10 and above)

▼ Guest Access

Guest User Account Managers

☐ Enable Guest User Account Managers to administer Guest Accounts.[Configure system GUAM settings](#)

Instructions for Guest User Account Manager:

Instructions displayed for guest users creation and updation.
You can use ,
, , <noscript>, and <a href> tags to format the text.

☐ Maximum Account Validity Period: 24 Set the Guest Account length limit (end time minus start time) in hours. This is valid for guests created by Guest Admin. Does not impact existing user expirations.

Guest Self-Registration

Send guest user credentials via: ☐ SMS

☐ Email [Configure SMS/Email settings](#)

☐ Show credentials on screen after guest completes registration

☐ Enable Sponsored Guest Access

☐ Maximum Account Validity Period for Self Registered Guests: 1 Set the Guest Account length limit in hours. This is valid for self registered guests. Does not impact existing user expirations.

Note: To enable Guest Self-Registration navigate to Signing In > Sign-in Policies > User URLs > [url] > [Configure Guest Settings](#)

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

Guest User Name Prefix: Prefix applied to auto-generated user names.

Guest User Info Fields: Enter additional fields for guest user information, one field per line. For example:
Title
Company name
Sponsor

▼ Server Catalog

Attributes...

Save ChangesReset

* indicates required field

User Creation on PPS

The Users are created on **SBRMigrationAuthServer**.

- Password will be stored in plain text.
- The native user (Encrypted Passwords) stored in the SBR xml file will be decrypted and stored into PPS.
- The native user (with Hashed Passwords) in SBR will be imported with password "pulsesecure". Change password at next sign-in flag will be enabled for this user.
- 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.

Figure - Users

	!	Username ▲	Name	Usertype	Last Sign-In Statistic			
					Date&Time	IPAddress	Agent	Status
<input type="checkbox"/>		0021ccc236a1	Unspecified Name	Guest user				
<input type="checkbox"/>		0021ccc236a2	Unspecified Name	Guest user				
<input type="checkbox"/>		0021ccc236b1	Unspecified Name	Guest user				
<input type="checkbox"/>		0021ccc236b2	Unspecified Name	Guest user				
<input type="checkbox"/>		0021ccc236c1	Unspecified Name	Guest user				
<input type="checkbox"/>		005056836480	Unspecified Name	Guest user				
<input type="checkbox"/>		after	Unspecified Name	Guest user				
<input type="checkbox"/>		check	Unspecified Name	Guest user				
<input type="checkbox"/>		hdarshan	Unspecified Name	Guest user				
<input type="checkbox"/>		kaialkr	Unspecified Name	Guest user				

Sign-In Page on PPS

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

Figure -Sign-In Pages

Sign-In Page	Type
SBRMigration Sign-In Page	Standard page
Default Sign-In Page	Standard page

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

Signing In > Sign-In Policies

Sign-in Policies

☐ Restrict access to administrators only
Only administrator URLs will be accessible. Note that Administrators can attempt to sign in even if all rules on this page are disabled.
Warning: Enabling this option will immediately terminate all user sessions.

[New URL...](#) [Delete...](#) [Enable](#) [Disable](#) [Up](#) [Down](#) [Save Changes](#)

<input type="checkbox"/>	Administrator URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/>	*/admin/	Default Sign-In Page	Admin Users	✓

<input type="checkbox"/>	User URLs	Sign-In Page	Authentication Realm(s)	Enabled
<input type="checkbox"/>	*/SBR/	SBRMigration Sign-In Page	SBRMigrationRealm (SBRMigration802.1X)	✓
<input type="checkbox"/>	*/guest/	Default Sign-In Page	Guest (Guest)	✓
<input type="checkbox"/>	*/guestadmin/	Default Sign-In Page	Guest Admin (N/A)	✓
<input type="checkbox"/>	*/certauth/	Default Sign-In Page	Cert Auth (Cert Auth)	✓
<input type="checkbox"/>	*/	Default Sign-In Page	Users (802.1X)	✓
<input type="checkbox"/>	*/guestsponsor/	Default Sign-In Page	Guest Sponsor (N/A)	✓

Authentication Protocol Sets

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

Figure – Authentication Protocol Set

Signing In > Authentication Protocol Sets

Authentication Protocol Sets

[Sign-In Policies](#) [Sign-In Pages](#) [Sign-In Notifications](#) [Authentication Protocol Sets](#)

[New Authentication Protocol...](#) [Duplicate...](#) [Delete...](#) [Restore Factory Default](#)

10 records per page Search:

<input type="checkbox"/>	Name	Authentication Protocol	PEAP	TTLS
<input type="checkbox"/>	1 802.1X System created default authentication protocol required for UAC agents	EAP-TTLS EAP-PEAP	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard
<input type="checkbox"/>	2 802.1X-Phones System created default authentication protocol for phones	EAP-MD5-Challenge EAP-TLS		
<input type="checkbox"/>	3 Guest System created authentication protocol for guest users	PAP CHAP		
<input type="checkbox"/>	4 Cert Auth System created authentication protocol for Certificate Authentication	EAP-TLS EAP-TTLS EAP-PEAP	EAP-JUAC EAP-TLS	EAP-JUAC EAP-GenericTokenCard
<input type="checkbox"/>	5 SBRMigration802.1X	EAP-PEAP EAP-TTLS PAP CHAP EAP-MD5-Challenge	EAP-JUAC EAP-MS-CHAP-V2	EAP-JUAC PAP MS-CHAP-V2 EAP-MS-CHAP-V2 EAP-GenericTokenCard

Roles

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

Figure – SBR Migration Role

User Roles > Roles

Roles

New Role...

Duplicate...

Delete...

Default Options...

10 records per page

Search:

	Role	Enabled settings				
		Session Options	UI Options	UAC Agent	Host Enforcer	Agentless Access
<input type="checkbox"/>	Guest System created Guest Users role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Guest Admin System created Guest Admin role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Guest Sponsor System created Guest Sponsor role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Guest Wired Restricted System created Guest Wired Restricted role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SBRMigrationRole System created Users role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Users System created Users role.	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

New Role...

Duplicate...

Delete...

Default Options...

← Previous

1

Next →

User Roles > SBRMigrationRole > General > Overview

Overview

General

Agent

Agentless

Overview

Restrictions

Session Options

UI Options

* Name:

SBRMigrationRole

Description:

System created Users role.

Save Changes

Options

If these settings are not specified by any roles assigned to the user, the settings specified in [Default Options](#) will be used.

☒ Session Options

(Edit)

☒ UI Options

(Edit)

☐ Enable Guest User Account Management Rights

☐ Enable Sponsored Guest User Account Management Rights

Save Changes

* indicates required field

User Realms

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

Figure - Realm

Authentication Realm	Servers	Dynamic Policy Evaluation
<input type="checkbox"/> Cert Auth	Primary: Certificate Authentication	Disabled
<input type="checkbox"/> Guest	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Admin	Primary: Guest Authentication	Disabled
<input type="checkbox"/> Guest Sponsor	Primary: Guest Authentication	Disabled
<input type="checkbox"/> SBRMigrationRealm	Primary: SBRMigrationAuthServer Directory: SBRMigrationAuthServer	Disabled
<input type="checkbox"/> Users	Primary: System Local	Disabled

SBRMigrationRole is added in the role mapping rules.

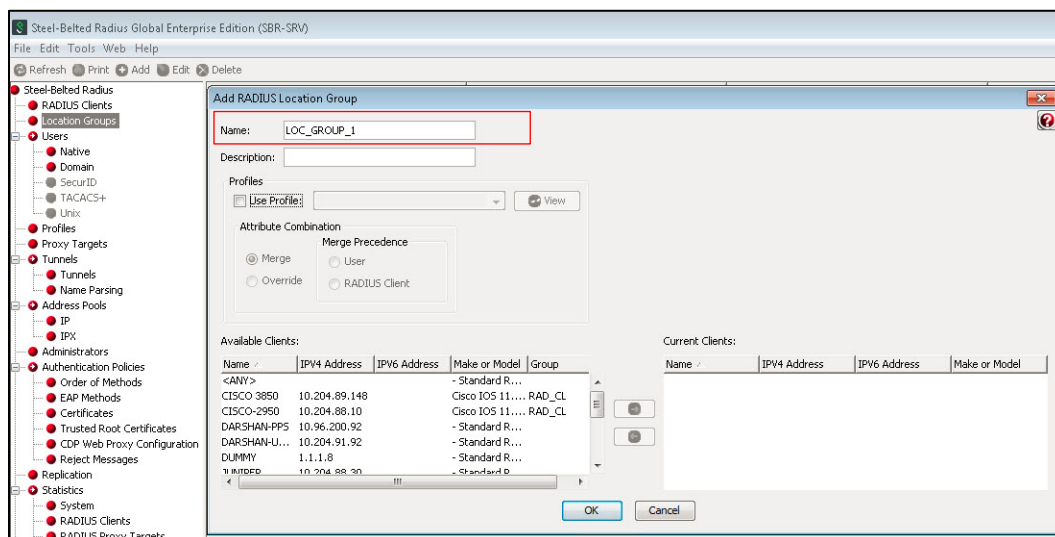
Figure – Role Mapping Rules

Rule Name	Stop
SBRMigrationRoleMapping	

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

Network Access > Location Group

Location Group

RADIUS DictionaryRADIUS VendorLocation GroupRADIUS ClientRADIUS AttributesNetwork Infrastructure DeviceSNMP Enforcement Policies

A location group policy logically groups network access devices by associating the devices with specific sign-in policies.

New Location Group...Duplicate...Delete...

10 records per pageSearch:

	Name	Sign-in Policy	MAC Auth Realm	RADIUS Clients
<input type="checkbox"/>	1 Default System created default location group.	*/		
<input type="checkbox"/>	2 Guest System created location group for guest users	*/guest/		
<input type="checkbox"/>	3 Guest Wired System created location group for wired guest users	*/guest/	Guest Wired	
<input type="checkbox"/>	4 Cert Auth System created location group for Certificate Authentication	*/certauth/		
<input type="checkbox"/>	5 SBRMigrationLGDefault	*/SBR/		SBRMigrationRadiusClientPCS-70, SBRMigrationRadiusClientP SBRMigrationRadiusClientP SBRMigrationRadiusClientP SBRMigrationRadiusClientP SBRMigrationRadiusClientP SBRMigrationRadiusClientY SBRMigrationRadiusClientC SBRMigrationRadiusClientD SBRMigrationRadiusClientD SBRMigrationRadiusClientD SBRMigrationRadiusClientJ SBRMigrationRadiusClientK SBRMigrationRadiusClientK
<input type="checkbox"/>	6 SBRMigrationLGBNG	*/SBR/		
<input type="checkbox"/>	7 SBRMigrationLGBNG_OVERRIDE	*/SBR/		SBRMigrationRadiusClientDUMMY
<input type="checkbox"/>	8 SBRMigrationLGBNG_PROFILE	*/SBR/		

RADIUS Client Configured on SBR

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

Figure SBR RADIUS client

The screenshot displays the Steel-Belted Radius configuration interface. On the left is a tree view with the following structure:

- Steel-Belted Radius
 - RADIUS Clients (selected)
 - Location Groups
 - Users
 - Native
 - Domain
 - SecurID
 - TACACS+
 - Unix
 - Profiles
 - Proxy Targets
 - Tunnels
 - Tunnels
 - Name Parsing
 - Address Pools
 - IP
 - IPX
 - Administrators
 - Authentication Policies
 - Order of Methods
 - EAP Methods
 - Certificates
 - Trusted Root Certificates
 - CDP Web Proxy Configuration
 - Reject Messages
 - Replication
 - Statistics
 - System
 - RADIUS Clients
 - RADIUS Proxy Targets
 - IP Address Pools
 - Reports
 - Current Sessions
 - Auth Logs
 - Locked Accounts
 - Settings
 - Filters

The main pane on the right is titled "Add RADIUS Client" and contains the following fields and options:

- Name:** CLIENT_1
- Description:** (empty)
- IPV4 address:** 10.204.60.70
- IPV6 address:** (empty)
- Range:** 1 (checked)
- Shared Secret:** (empty)
- ☐ Unmask
- Make or model:** - Standard Radius -
- Address pool:** (empty) [View]
- Location Group:** (empty) [View]
- Profiles:**
 - ☐ Use Profile: (empty) [View]
- Attribute Combination:**
 - ☒ Merge
 - ☐ Override
 - Merge Precedence:**
 - ☐ User
 - ☐ RADIUS Client
- Advanced:**
 - ☐ Use different shared secret for Accounting [Edit...]
 - ☐ Assume down if no keepalive packets after [] seconds

At the bottom of the dialog are "OK" and "Cancel" buttons.

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

Network Access > RADIUS Client

RADIUS Client

RADIUS Dictionary | RADIUS Vendor | Location Group | **RADIUS Client** | RADIUS Attributes | Network Infrastructure Device | SNMP Enforcement Policies

A RADIUS client policy specifies the information required for a 802.1X network access device to connect as a RADIUS client of the Pulse Policy Secure.

[New RADIUS Client...](#) [Duplicate...](#) [Enable](#) [Disable](#) [Delete...](#)

10 records per page Search:

	Name	IP Address	Range	Make	Group	Enabled
<input type="checkbox"/>	1 SBRMigrationRadiusClientCISCO 2960 This is Cisco rad client 88 10	10.10.10.10	1	- Standard Radius -	SBRMigrationLGDefault	✓
<input type="checkbox"/>	2 SBRMigrationRadiusClientCISCO 3850	10.10.10.10	1	- Standard Radius -	SBRMigrationLGDefault	✓
<input type="checkbox"/>	3 SBRMigrationRadiusClientDA...	10.10.10.10	1	- Standard Radius -	SBRMigrationLGDefault	✓
<input type="checkbox"/>	4 SBRMigrationRadiusClient[...] DARSHAN-UACQA	10.10.10.10	1	- Standard Radius -	SBRMigrationLGDefault	✓

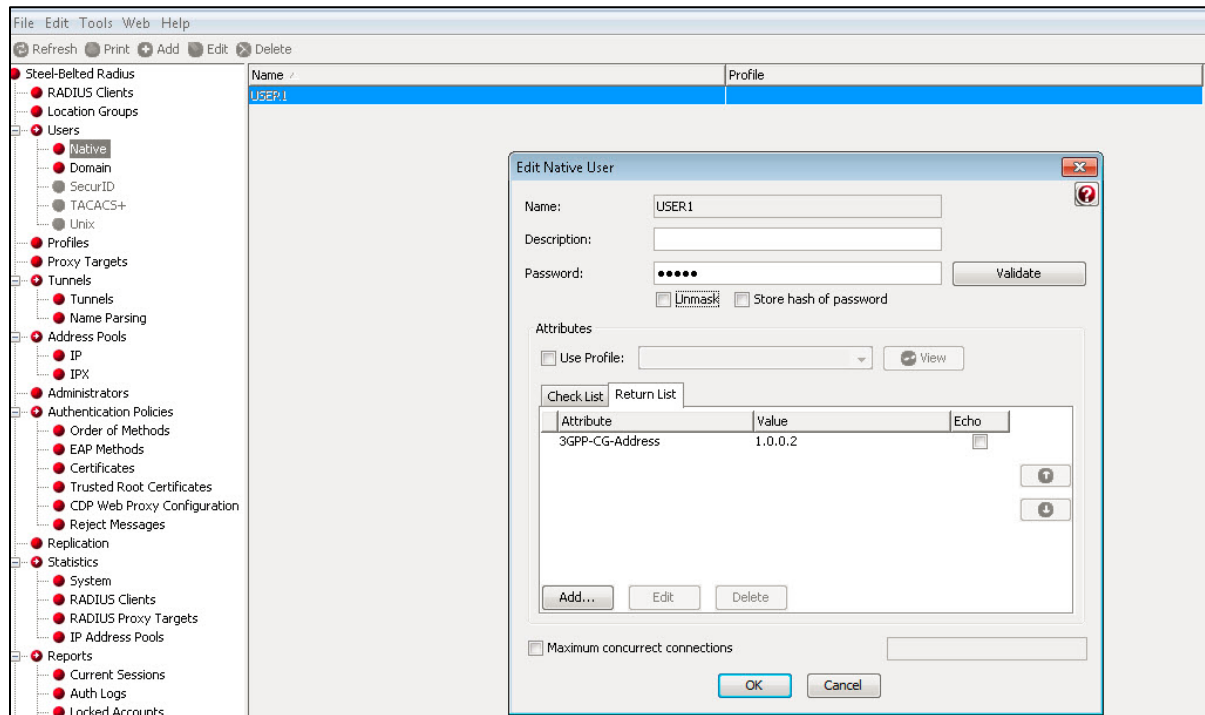
Note: If RADIUS client is not using profile and location group then the default Location group is used.

If a RADIUS Client is using Profiles then:

- If the profile is used by any of Location group then RADIUS client will be associated 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.
- The Radius client Shared secrets stored in SBR xml file will be decrypted and imported to the PPS Radius clients.

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

Network Access > Radius Attributes > RADIUS Return Attributes

RADIUS Return Attributes

RADIUS Dictionary RADIUS Vendor Location Group RADIUS Client **RADIUS Attributes** Network Infrastructure Device SNMP Enforcement Policies

Return Attributes Request Attributes Attribute Logging

Show policies that apply to:

A RADIUS return attributes policy specifies the return list attributes to send to an 802.1X network access device, such as which VLAN endpoints must use to access the network. If no policy applies, Open Port is the default action.

		Policies	ACL Settings	Attributes	Location Group	Interface	Applies to role
<input type="checkbox"/>	1.	SBRMigrationRadRetAttrTEST	N/A	Cisco-AVPair=url-redirect=https://10.96.69.26 Cisco-AVPair=ip:inac1#161=deny ip any any	SBRMigrationLGRAD_CL SBRMigrationLGBNG_OVERRIDE	N/A	All roles
<input type="checkbox"/>	2.	SBRMigrationRadRetAttr...	N/A	Cisco-AVPair=ip:inac1#141=permit ip any any Reply-Message=123456789	SBRMigrationLGBNG_PROFILE	N/A	All roles
<input type="checkbox"/>	3.	SBRMigrationRadRetAttrS...	N/A	Tunnel-Medium-Type=6 Tunnel-Private-Group-ID="65" Tunnel-Type=13	SBRMigrationLGProfSACHIN	N/A	All roles
<input type="checkbox"/>	4.	SBRMigrationRadRetAttrRC1_PROFILE	N/A	Filter-Id=limited	SBRMigrationLGProfRC1_PROFILE	N/A	All roles
<input type="checkbox"/>	5.	SBRMigrationRadRetAttrLG1_PROFILE	N/A	Filter-Id=compliant.in	SBRMigrationLGLG1PROFILE	N/A	All roles
<input type="checkbox"/>	6.	SBRMigrationRadRetAttrOpenPort	N/A	OpenPort	SBRMigrationLGBNG SBRMigrationLGDefault	N/A	All roles



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 RADIUS Client 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

The following are the important things to consider while importing the MAC address:

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

Figure –MAC Address Users

Auth Servers > SBRMigrationAuthServer > Users

Users

Settings Users Admin Users

Import Users from CSV file: No file chosen Overwrite Users: ☐ Note: Enabling the checkbox will overwrite the user having the same user name.

Show users named: Show users

Page 1 of 1

	Username ▲	Name	Usertype	Last Sign-in Statistic			
				Date&Time	IPAddress	Agent	Status
<input type="checkbox"/>	0021ccc236a1	Unspecified Name	Guest user				
<input type="checkbox"/>	0021ccc236a2	Unspecified Name	Guest user				
<input type="checkbox"/>	0021ccc236b1	Unspecified Name	Guest user				
<input type="checkbox"/>	0021ccc236b2	Unspecified Name	Guest user				
<input type="checkbox"/>	0021ccc236c1	Unspecified Name	Guest user				
<input type="checkbox"/>	005056836480	Unspecified Name	Guest user				
<input type="checkbox"/>	after	Unspecified Name	Guest user				
<input type="checkbox"/>	check	Unspecified Name	Guest user				
<input type="checkbox"/>	hedarshan	Unspecified Name	Guest user				
<input type="checkbox"/>	kaialkr	Unspecified Name	Guest user				

TACACS+ Migration

Terminal Access Controller Access Control System (TACACS) is a security protocol that provides centralized validation of users who are attempting to gain access to a router or Network Access Device (NAS). TACACS+, a more recent version of the original TACACS protocol, provides separate authentication, authorization, and accounting (AAA) services.

The TACACS+ protocol provides detailed accounting information and flexible administrative control over the authentication, authorization, and accounting process. The protocol allows a TACACS+ client to request detailed access control and allows the TACACS+ process to respond to each component of that request. TACACS+ uses Transmission Control Protocol (TCP) for its transport.

TACACS+ provides security by encrypting all traffic between the NAD and the process. Encryption relies on a secret key that is known to both the client and the TACACS+ process.

This feature is to import SBR TACACS+ configuration data to PPS so that Network Access Devices (routers and switches) with TACACS+ client can connect (migrate) to PPS for TACACS+ AAA services. The procedure is to get the SBR TACACS+ configuration file and then import it into PPS. The default configurations are created in PPS to make it compatible with TACACS+ server.

The sample text configuration file used for import is captured below.

```

#!/opt/PSsbr/radius/tac_plus

id = spawn {
    listen = { port = 49 }
    spawn = {
        instances min = 2
        instances max = 10
    }
    background = yes
}

id = tac_plus {
    debug = PARSE PACKET AUTHEN AUTHOR ACCT CONFIG HEX REGEX LOCK ACL CMD BUFFER PROC NET PATH CONTROL INDEX AV MAVIS LWRES

    access log = /opt/PSsbr/radius/tacplus_access.log
    accounting log = /opt/PSsbr/radius/tacplus_acct.log

    syslog facility = local6
    syslog level = debug

    retire limit = 1000
    mavis module = external {
        setenv SHADOWFILE = /etc/shadow
        exec = /opt/PSsbr/radius/mavis/mavis_tacplus_shadow.pl
        # see the MAVIS configuration manual for more options
    }
    login backend = mavis chpass

    mavis module = external {
        setenv LDAP_SERVER_TYPE = "microsoft"
        setenv LDAP_HOSTS = "1.1.1.1:389"
        setenv LDAP_SCOPE = sub
        setenv LDAP_BASE = "dc=64windows2008,dc=pulse,dc=com"
        setenv LDAP_FILTER = "(&(objectclass=user)(sAMAccountName=%s))"
        setenv LDAP_USER = test@64windows2008.pulse.com
        setenv LDAP_PASSWORD = $ENC$53616c7465645f5f4c105b186f4d2f271b3e33ce6d65672c
        setenv FLAG_USE_MEMBEROF = 1
        setenv AD_GROUP_PREFIX = tes

        exec = /opt/PSsbr/radius/mavis/mavis_tacplus_ldap.pl
        # see the MAVIS configuration manual for more options
    }
    login backend = mavis
    pap backend = mavis
    user backend = mavis

    host = world {
        welcome banner = "\nHitherto shalt thou come, but no further. (Job 38.11)\n\n"
        key = QaWsEdRfTgY
        address = 192.168.1.0/24
    }

    host = 10.204.88.14 {
        prompt = "Welcome to cisco switch \n"
        key = psecure
    }

    group = readwrite {
        default service = permit
        service = shell {
            default command = permit
            set priv-lvl = 15
        }
    }

    group = getconfig {
        enable 15 = clear secret
        service = shell {
            set priv-lvl = 1
            cmd = show { permit running-config }
            cmd = configure { deny terminal }
            cmd = telnet {
                deny ^131\.100\.13\.[0-9]+
                permit .*
            }
            cmd = show {
                deny version
                permit privilege
            }
            cmd = enable { permit .* }
        }
    }

    group = junipersuperadmin {
        service = junos-exec {
            set local-user-name = "remote-super-users"
            set user-permissions = "all"
        }
    }

    user = marc {
        password = crypt $1$xxxxxxx$hDZPHghXe8XvoHeFdqUwm/
        member = readwrite@world
    }

    user = john {
        password = clear john123
        member = junipersuperadmin@10.204.88.14
    }

    user = fred {
        password = clear kunkure
        member = getconfig@world
    }
}

```

SBR TACACS+ config file

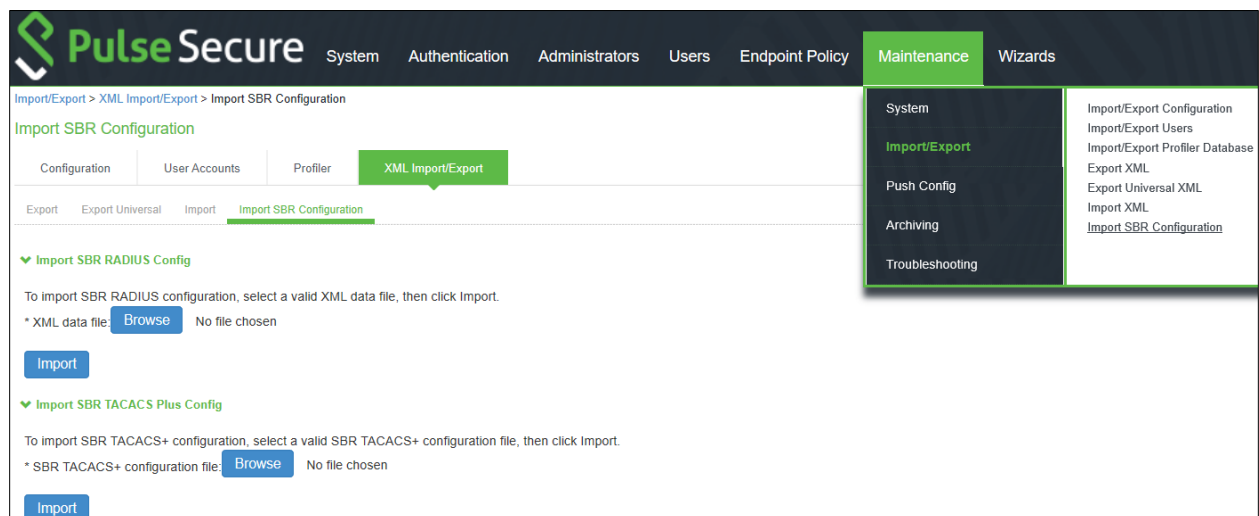
TACACS+ configurations are stored in a text configuration file available at:

/opt/PSsbr/radius/tac_plusd.cfg

Importing SBR TACACS+ config file to PPS

1. Select **Maintenance** > **Import/Export** > **XML Import/Export** > **Import SBR Configuration**.
2. Under Import SBR TACACS plus config, click **Browse** and browse the SBR TACACS+ configuration file which needs to be imported.
3. Click **Import**.

Figure –Import SBR TACACS + config



Note: You cannot import multiple TACACS+ cfg files simultaneously. The Admin must wait for the TACACS+.cfg file import to get completed to import another cfg file.

Authentication Server

For ease of migration **TacacsPlusMigrationAuthServer** is created by default.

Authentication Servers


Auth. Servers

Templates

Enable Auth Traffic Control

New: (Select server type) New Server... Delete...

10 records per page

	Authentication/Authorization Servers	Type
<input type="checkbox"/>	Administrators	Local Authentication
<input type="checkbox"/>	Certificate Authentication	Certificate Server
<input type="checkbox"/>	Guest Authentication	Local Authentication
<input type="checkbox"/>	Guest Wired Authentication	MAC Address Authentication
<input type="checkbox"/>	System Local	Local Authentication
<input type="checkbox"/>	TacacsPlusMigrationAuthServer	Local Authentication

Note: Any secondary LDAP/AD servers configured in SBR tac_plusd.cfg file are not migrated and admin should configure them manually in PPS.

Users

Navigate to **Auth Servers > TacacsPlusMigrationAuthServer > Users** to view the users successfully migrated from SBR to PPS.

Note: If the user has encrypted password in SBR. It will be migrated with the default password as **pulsesecure**.

Figure –Users

Auth Servers > TacacsPlusMigrationAuthServer > Users

Users

Settings


Users

Admin Users

Import Users from CSV file: Browse No file chosen Import

Show users named: * Show 200 users Update

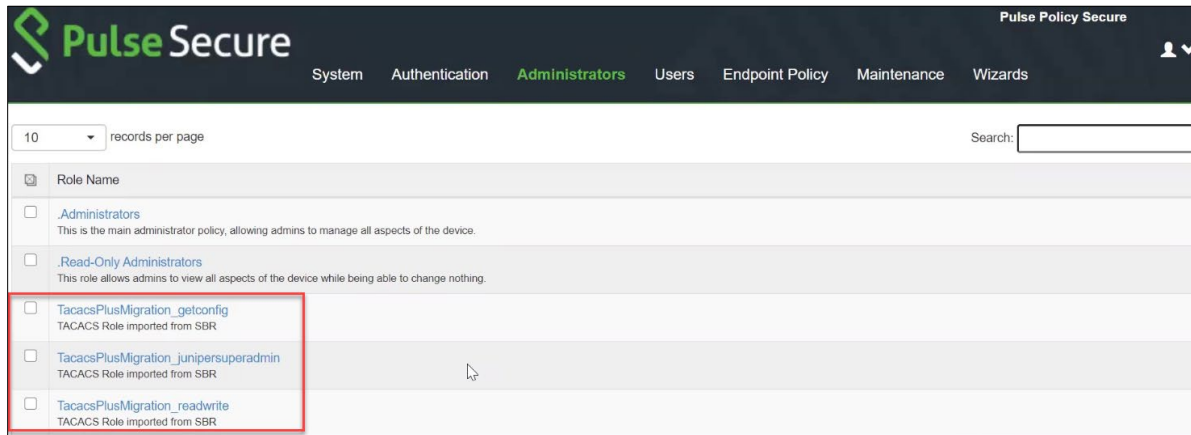
New... Delete... Unlock... Page 1 of 1 < < > >

	Username ▲	Name	Usertype	Last Sign-in Statistic			
				Date&Time	IPAddress	Agent	Status
<input type="checkbox"/>	fred	Unspecified Name	Normal				
<input type="checkbox"/>	john	Unspecified Name	Normal				
<input type="checkbox"/>	marc	Unspecified Name	Normal				

Roles

TACACS roles are imported from SBR. The roles imported are prefixed with TacacsPlusMigration.

Figure –TacacsPlus Roles



Pulse Secure		Pulse Policy Secure	
System Authentication Administrators Users Endpoint Policy Maintenance Wizards			
10 records per page		Search:	
Role Name			
<input type="checkbox"/> .Administrators	This is the main administrator policy, allowing admins to manage all aspects of the device.		
<input type="checkbox"/> .Read-Only Administrators	This role allows admins to view all aspects of the device while being able to change nothing.		
<input type="checkbox"/> TacacsPlusMigration_getconfig	TACACS Role imported from SBR		
<input type="checkbox"/> TacacsPlusMigration_junipersuperadmin	TACACS Role imported from SBR		
<input type="checkbox"/> TacacsPlusMigration_readwrite	TACACS Role imported from SBR		

Realm

For ease of migration **TacacsPlusMigrationRealm** is created by default. Navigate to **Admin Realms > Administrator Authentication Realms**. to view the realm.

Figure –Admin Realm



Admin Realms > Administrator Authentication Realms	
Administrator Authentication Realms	
New... Duplicate... Delete...	
10 records per page	
Search:	
Authentication Realm	Authentication Server
<input type="checkbox"/> Admin Users	Administrators
<input type="checkbox"/> TacacsPlusMigrationRealm	TacacsPlusMigrationAuthServer
← Previous 1 Next →	
Authentication realms specify what server to use for authentication, how policies are assigned to users, and restrictions on who can attempt to sign-in.	

Role Mapping

Navigate to **Admin Realms > TacacsPlusMigrationRealm > Role Mapping** to view the users mapped to the TacacsPlusmigration roles.

Figure –Role Mapping

Admin Realms > TacacsPlusMigrationRealm > Role Mapping

Role Mapping

General Authentication Policy Role Mapping

Specify how to assign delegated admin roles to users when they sign in. Users that are not assigned a role will not be able to sign in.

New Rule... Duplicate Delete Add Remove Save Changes

	When users meet these conditions	assign these roles	Rule Name	Stop
<input type="checkbox"/>	1. username is "fred"	→ TacacsPlusMigration_getconfig	TacacsPlusMigrationRoleMapping for fred	<input type="checkbox"/>
<input type="checkbox"/>	2. username is "john"	→ TacacsPlusMigration_junipersuperadmin	TacacsPlusMigrationRoleMapping for john	<input type="checkbox"/>
<input type="checkbox"/>	3. username is "marc"	→ TacacsPlusMigration_readwrite	TacacsPlusMigrationRoleMapping for marc	<input type="checkbox"/>

When more than one role is assigned to a user:
☒ Merge settings for all assigned roles
☐ User must select from among assigned roles
☐ User must select the sets of merged roles assigned by each rule

Note: Users that do not meet any of the above rules will not be able to sign into this realm.

Device groups

Navigate to **Network Device Administration > Device Group** to view the device group policy, which logically groups network devices by associating the devices with specific admin realm TacacsPlusMigrationRealm. The device groups imported from SBR are prefixed with TacacsPlusMigration.

Figure –TacacsPlus Device Group

Network Device Administration > Device Group

Device Group

Device Groups TACACS+ Clients Shell Policies

A device group policy logically groups network devices by associating the devices with specific admin realm.

New Device Group... Duplicate... Delete...

10 records per page Search:

	Name	Admin Realm	TACACS+ Clients
<input type="checkbox"/>	1 TacacsPlusMigration10.204.88.14	TacacsPlusMigrationRealm	TacacsPlusMigration10.204.88.14
<input type="checkbox"/>	2 TacacsPlusMigrationworld	TacacsPlusMigrationRealm	TacacsPlusMigration192.168.1.0

Network Device Administration > Device Group > TacacsPlusMigration10.204.88.14

TacacsPlusMigration10.204.88.14

▼ Device Group

* Name: Label to reference this Device Group.

Description:

* Admin Realm: To manage realm, see the [Admin Realms](#)

[Save Changes](#)

* indicates required field

Clients

Host details configured in SBR is migrated to PPS. The clients migrated from SBR will have the prefix TacacsPlusMigration.

Figure –Clients

Network Device Administration > TACACS+ Client

TACACS+ Client

Device Groups TACACS+ Clients Shell Policies

A TACACS+ client policy specifies the information required for this device to connect to Pulse Policy Secure for admin access control.

[New TACACS+ Client...](#) [Duplicate...](#) [Enable](#) [Disable](#) [Delete...](#)

10 records per page Search:

	Name ▲	IP Address	Range	Device Group	Enabled
<input type="checkbox"/>	1 TacacsPlusMigration10.204.88.14	10.204.88.14	1	TacacsPlusMigration10.204.88.14	✓
<input type="checkbox"/>	2 TacacsPlusMigration192.168.1.0	192.168.1.0	256	TacacsPlusMigrationworld	✓

Network Device Administration > TACACS+ Client > TacacsPlusMigration10.204.88.14

TacacsPlusMigration10.204.88.14

▼ TACACS+ Client

* Name: Label to reference this TACACS+ Client.

Description:

* IP Address: IP Address of this TACACS+ Client.

* IP Address Range: Number of IP Addresses for this TACACS+ Client

* Shared Secret: TACACS+ shared secret

* Device Group: To manage groups, see the [Device Group](#)

▼ TACACS+ Advance Settings

Allow Authorization (w/o authentication) ☐ Allow Authorization (w/o authentication)

[Save Changes](#)

* indicates required field

Shell policies

Navigate to **Endpoint Policy > Network Device Administration > Shell Policies** to view the migrated shell policies. The Shell Policies imported from SBR are prefixed with TacacsPlusMigration.

Note: The migration tool migrates only the first 13 custom attributes of the SBR shell policy to PPS and the remaining are not migrated.

Figure –Shell Policies

Network Device Management > Shell Policies

Shell Policies

Device Groups TACACS+ Clients **Shell Policies**

[New Policy](#) [Duplicate](#) [Delete](#) [Add](#) [Remove](#) [Save Changes](#)

10 records per page

	Name	Device Group	Default Privilege	Maximum Privilege	Command Set	Custom Attributes	Applies to
<input type="checkbox"/>	1 TacacsPlusMigration_getconfig	TacacsPlusMigrationworld	1	15	▶ Permitted Commands ▶ Denied Commands		TacacsPlusMigration_getconfig
<input type="checkbox"/>	2 TacacsPlusMigration_junipersuperadmin	TacacsPlusMigration10.204.88.14	1	1		▶ Mandatory Attributes	TacacsPlusMigration_junipersuperadmin
<input type="checkbox"/>	3 TacacsPlusMigration_readwrite	TacacsPlusMigrationworld	15	15			TacacsPlusMigration_readwrite

The example shell policy shows “TacacsPlusMigration_getconfig” shell policy mapped to the device group “TacacsPlusMigrationworld” and to role “TacacsPlusMigration_getconfig”.

Note: Service type can be configured in TACACS+ shell policy for TACACS+ authorisation. Service type value is different than the default value i.e shell sometimes. You must define correct value as desired by each vendor. For example, for Palo Alto Networks service type is "PaloAlto", for Juniper Networks service type is "junos-exec" and for Cisco Airspace WLC service type is "ciscowlc".

TacacsPlusMigration_getconfig

▼ New Shell Policy

* Name: Label to reference this policy.

Description:

▼ Device Group

- ☐ Policy applies to ALL groups
☒ Policy applies to SELECTED groups

Available Device Groups:

TacacsPlusMigration10.204.88.14

Add ->

Remove

Selected Device Groups:

TacacsPlusMigrationworld

▼ Shell Policy

* Default Privilege Shell Privilege Levels supported

* Maximum Privilege

Service: This is optional and default service is 'shell'

▼ Command Set

Delete

	Command	Arguments	Action	
	<input type="text"/>	<input type="text"/>	<input type="text" value="permit"/>	<input type="button" value="Add"/>
<input type="checkbox"/>	configure	terminal	deny	
<input type="checkbox"/>	enable	.*	permit	
<input type="checkbox"/>	show	running-config	permit	
<input type="checkbox"/>	show	version	deny	
<input type="checkbox"/>	show	privilege	permit	
<input type="checkbox"/>	telnet	^131\108\13\[0-9]*	deny	
<input type="checkbox"/>	telnet	.*	permit	

- ☒ Deny any command that does not hit any of the rule in the table above
☐ Permit any command that does not hit any of the rule in the table above

▼ Custom Attributes

Delete

	Attribute	Value	Requirement	
	<input type="text"/>	<input type="text"/>	<input type="text" value="Mandatory"/>	<input type="button" value="Add"/>

▼ Roles

- ☐ Policy applies to ALL roles
☒ Policy applies to SELECTED roles
☐ Policy applies to all roles OTHER THAN those selected below

Available roles:

.Administrators
.Read-Only Administrators
TacacsPlusMigration_junipersuperadmin
TacacsPlusMigration_readwrite

Add ->

Remove

Selected roles:

TacacsPlusMigration_getconfig

* indicates required field

References

For more information on 802.1X authentication and troubleshooting, see [802.1X Authentication with Cisco Switch](#).

For more information on TACACS+ authentication and troubleshooting, see:

http://www.pro-bono-publico.de/projects/tac_plus.html and <https://tools.ietf.org/id/draft-ietf-opsawg-tacacs-07.html>