Pulse Policy Secure: Steel Belted Radius Server

SBR to PPS Migration Guide

Published Date	December 2020
Document Version	1.1

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

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

Contents

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

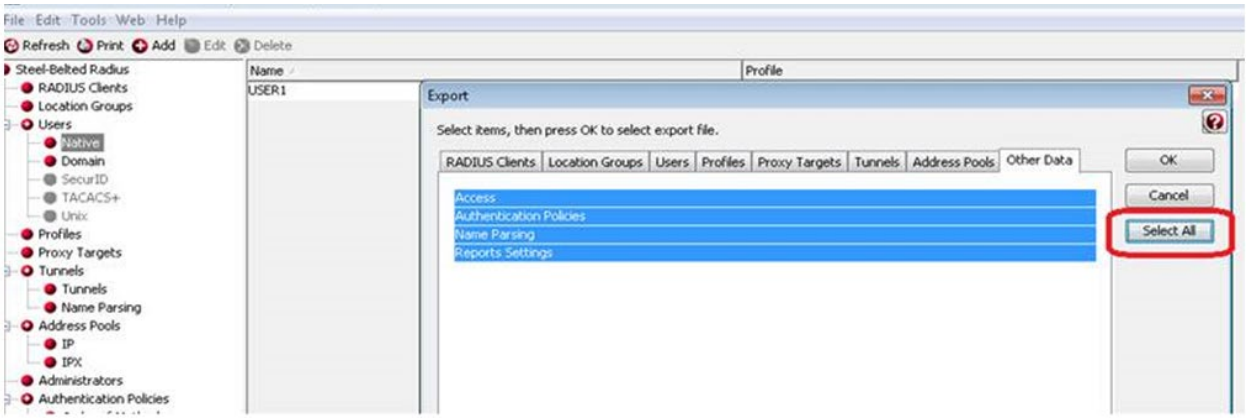
Step	Configuration on SBR	Equivalent configuration on PPS
Step 1	Configure Users > Native > Add Native Users.	Configure Authentication Server
Step 2	SBR profile-based authentication.	Configure the Authentication Realm, Role mapping rules and Sign-In Policy.
Step 3	Configure SBR > Location Groups.	Configure 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**.

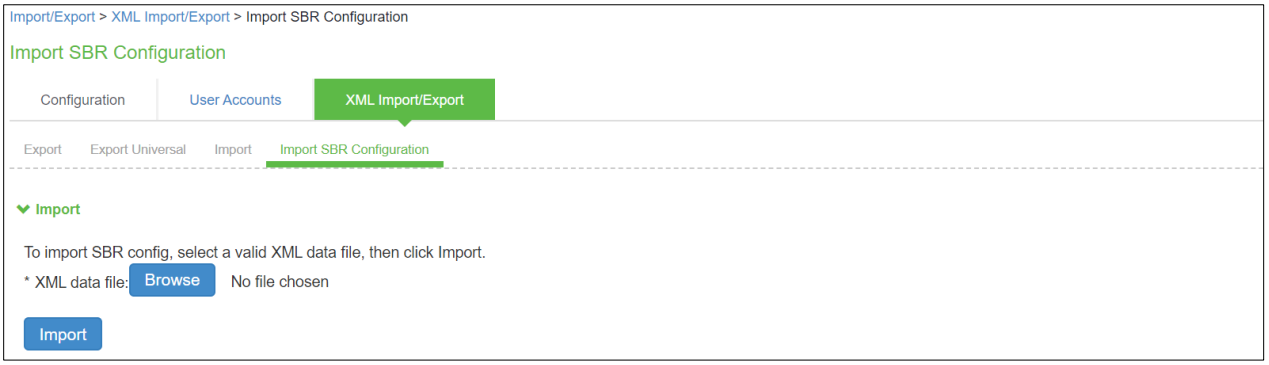
    

5. In the Export to XML file dialog, enter the file name and click **Save**.

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

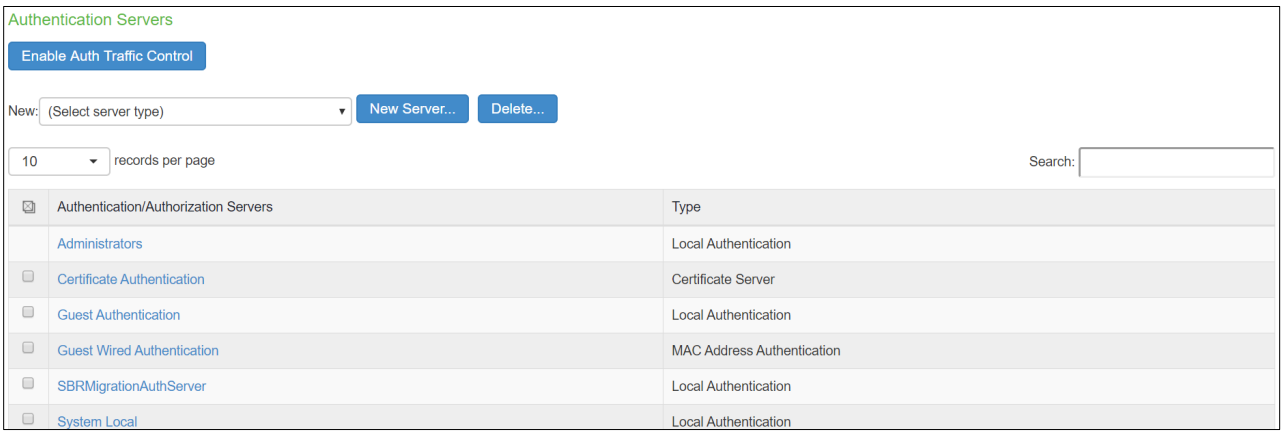
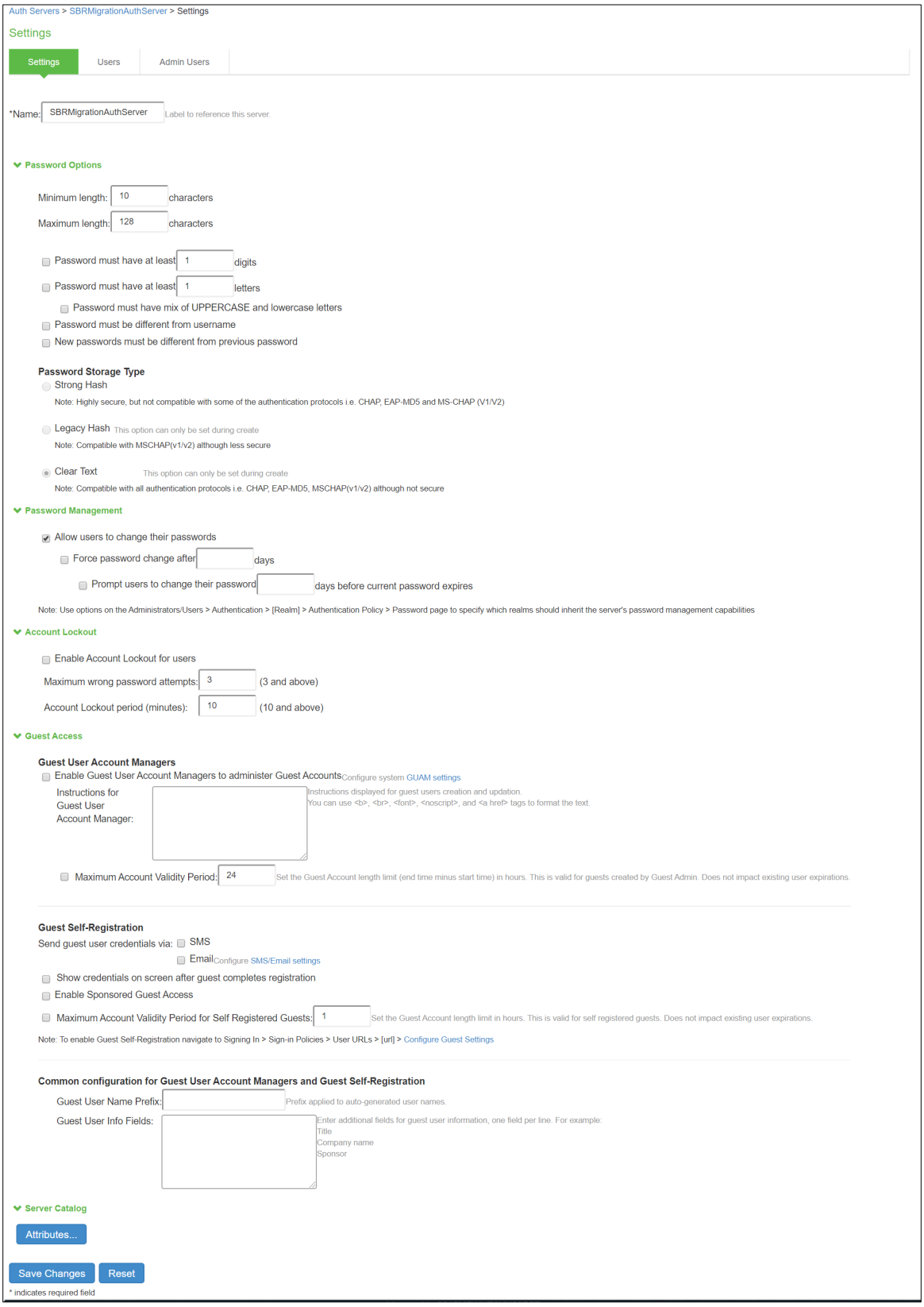


Figure – Authentication Server Settings

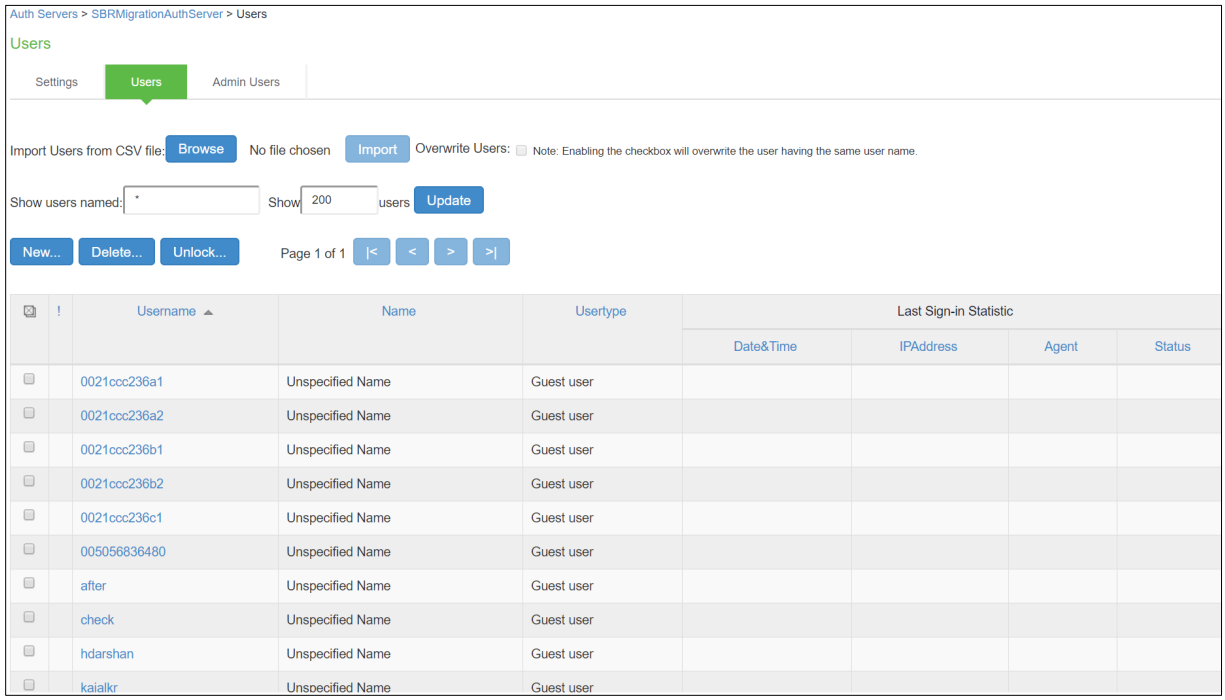


User Creation on PPS

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.

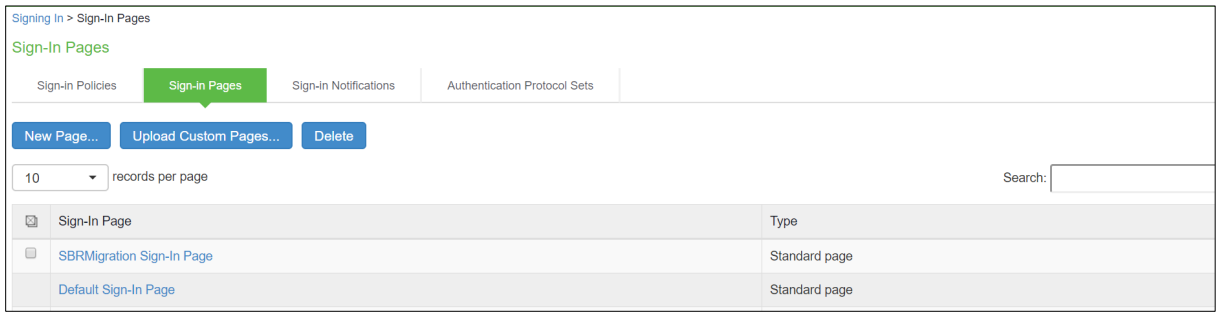
Figure - Users



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

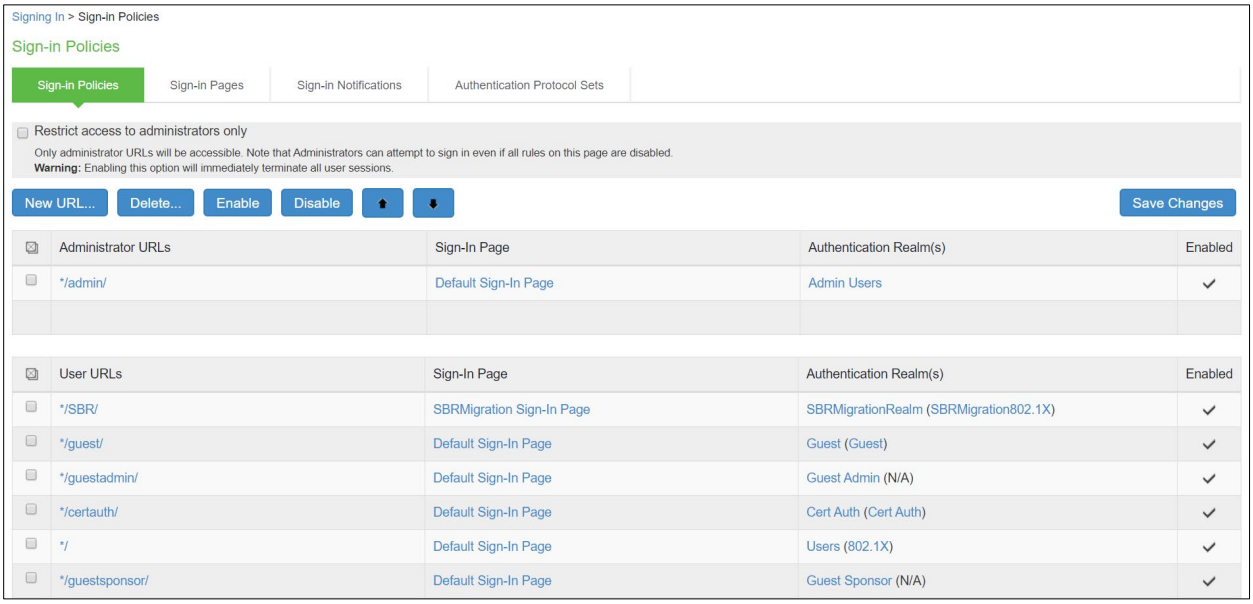


Sign-In Policy

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.

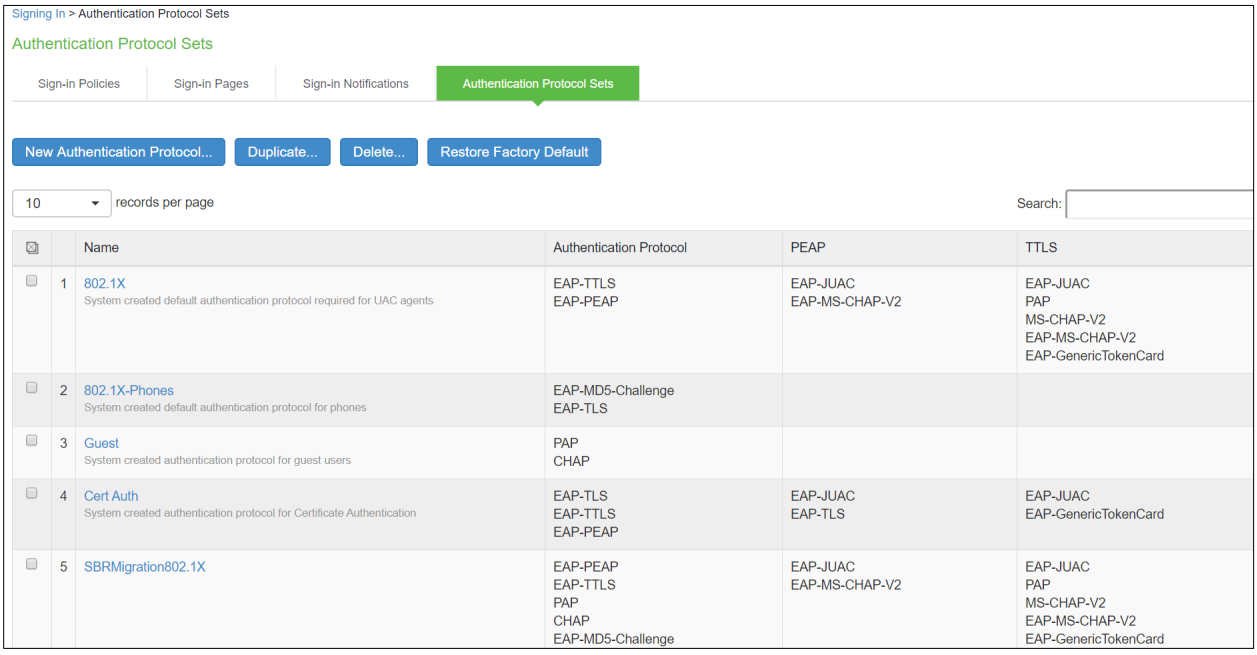
Figure -Sign-In Policies



Authentication Protocol Sets

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

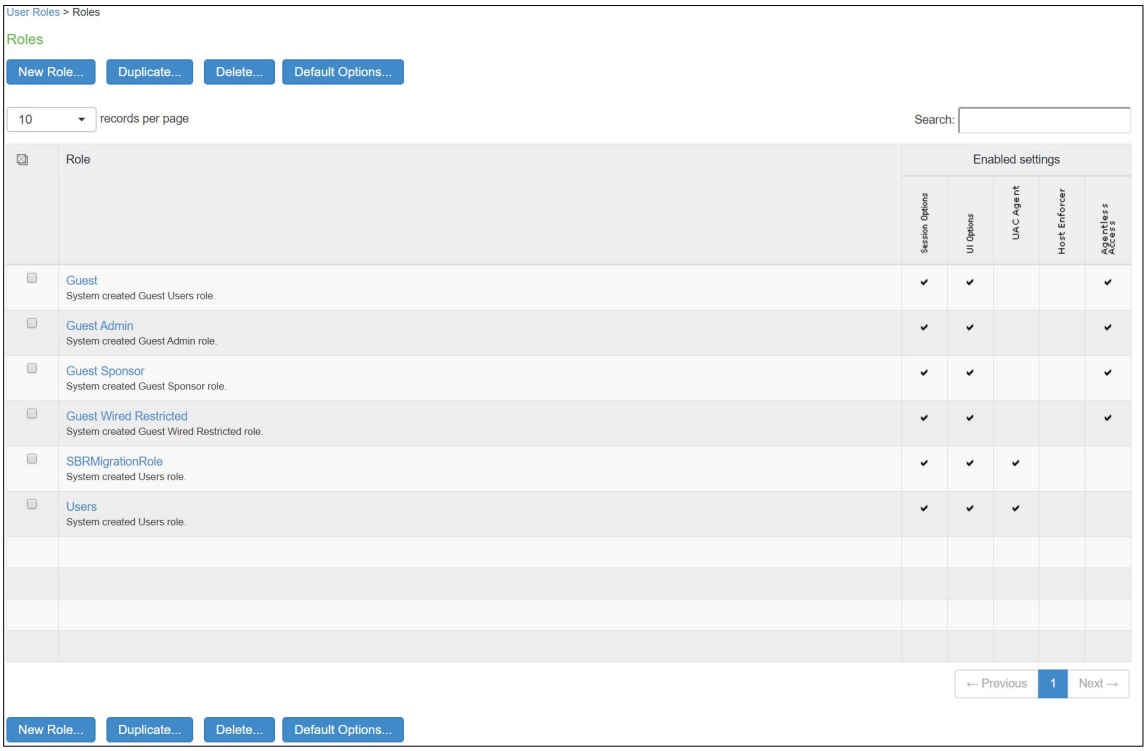
Figure – Authentication Protocol Set

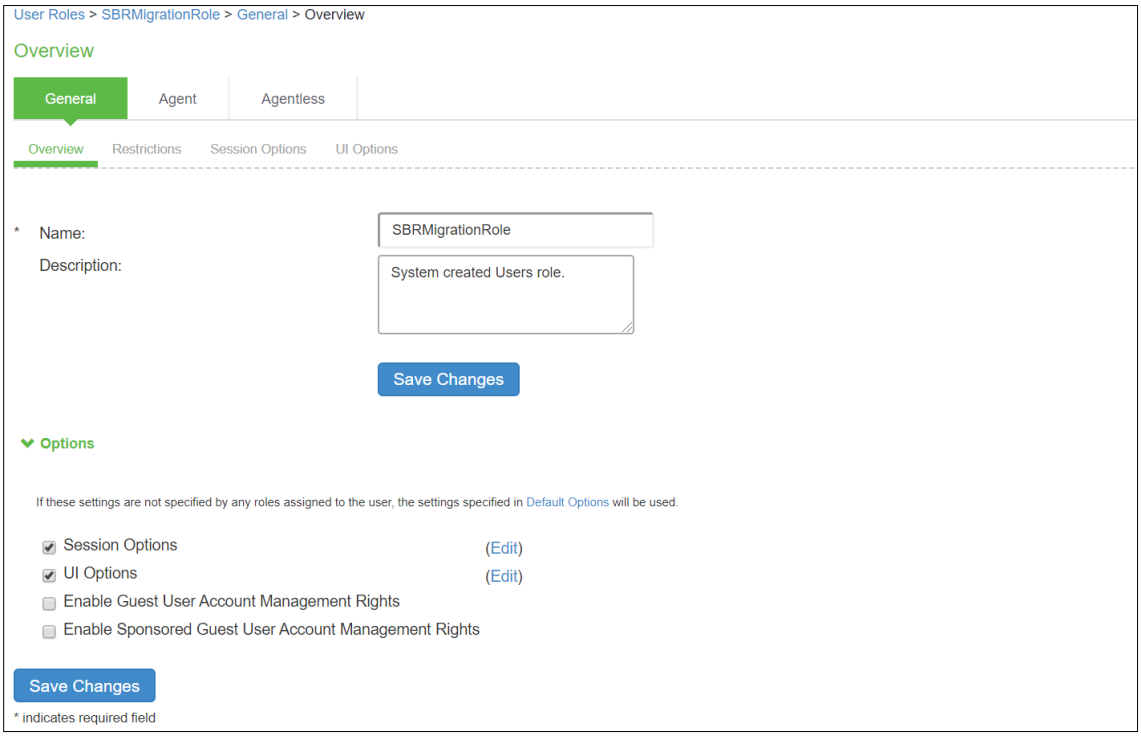


Roles

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

Figure – SBR Migration Role

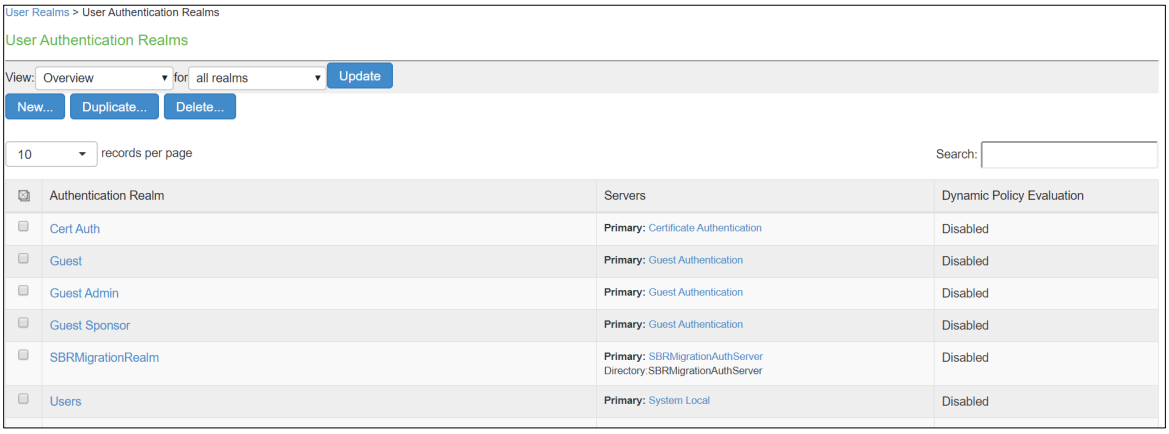




User Realms

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

Figure - Realm



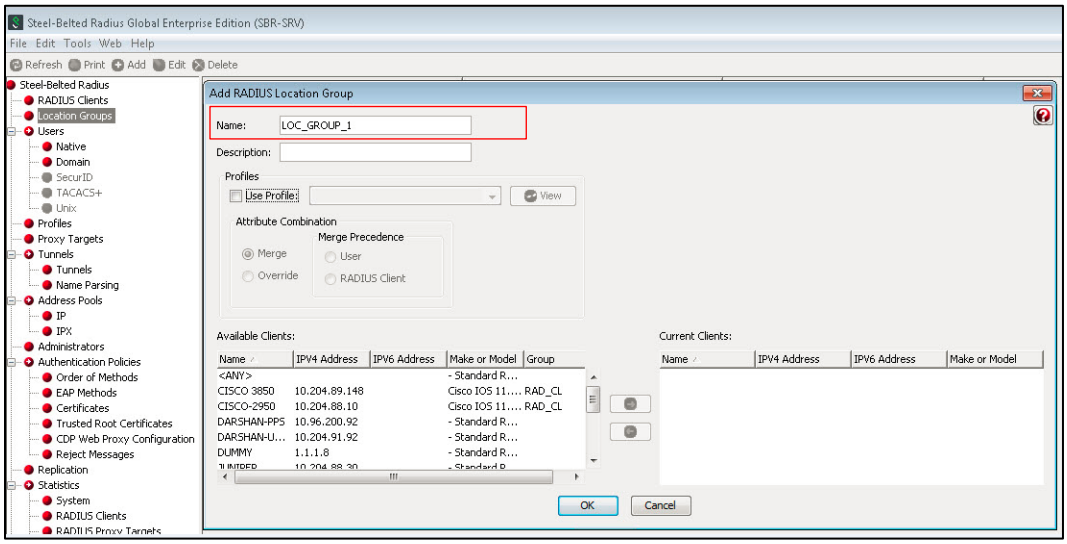
SBRMigrationRole is added in the role mapping rules.

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

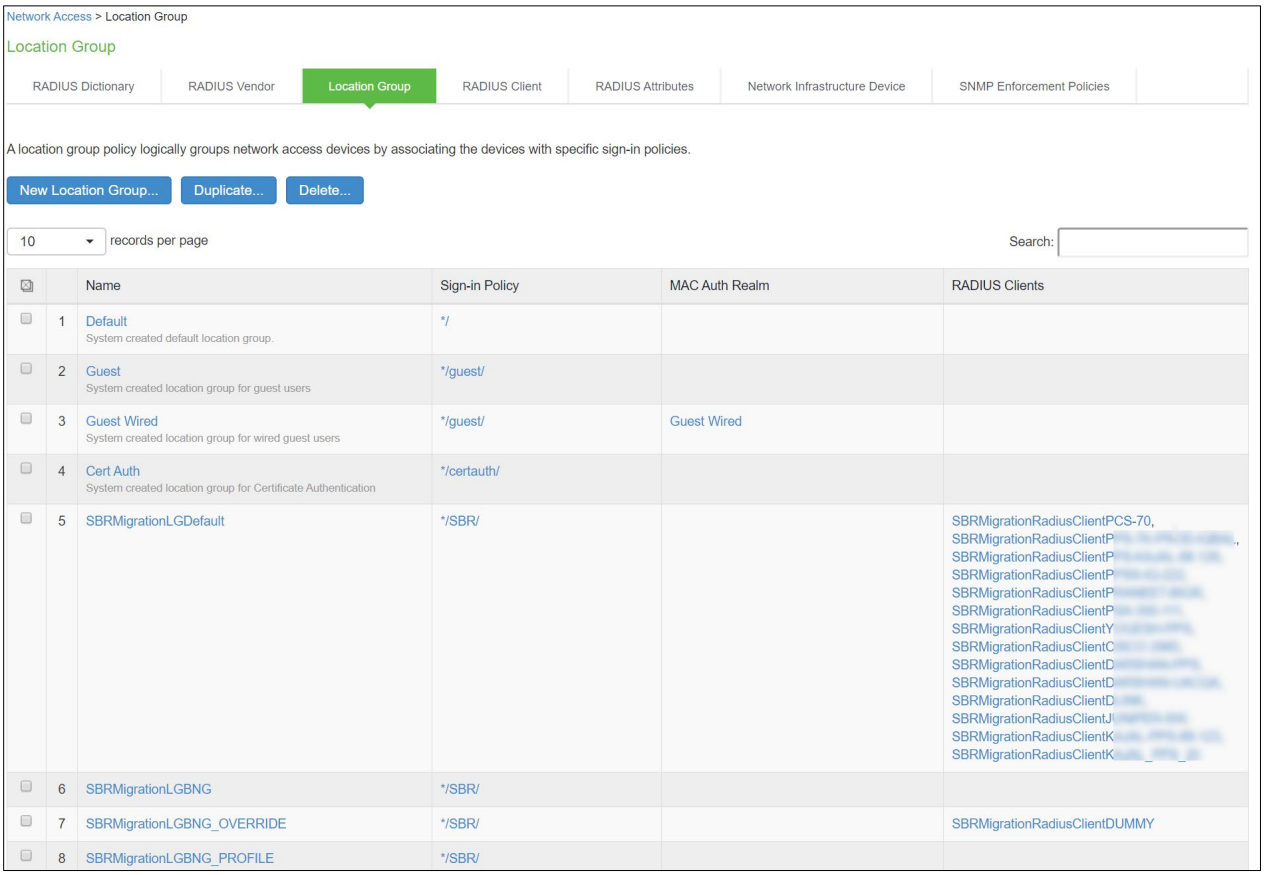


Location Group on PPS

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.

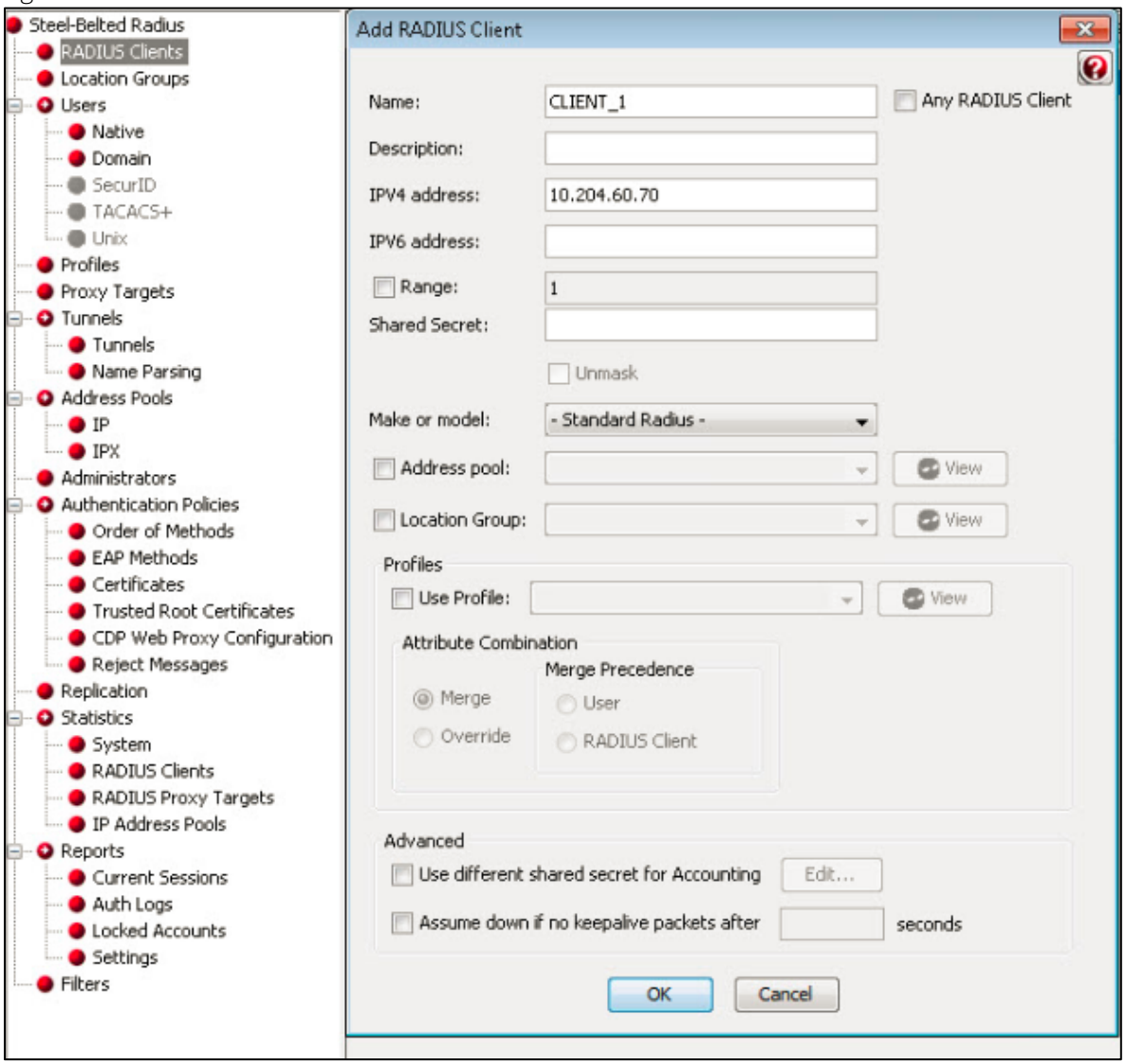
Figure: Location Group



RADIUS Client Configured on SBR

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

Figure SBR RADIUS client

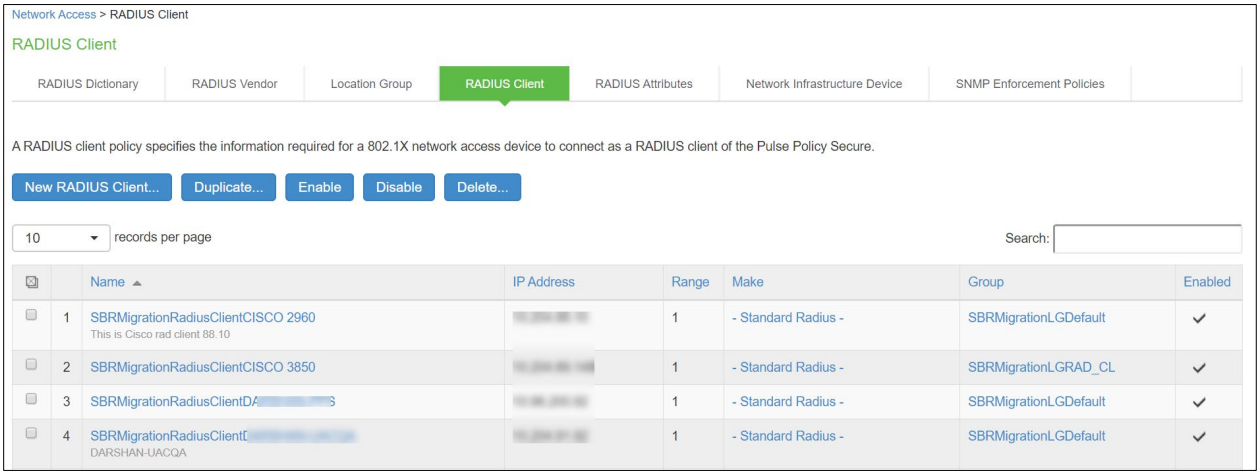


Creating a new RADIUS Client on PPS

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

For example, SBRMigrationRadiusClientPPS is configured as a RADIUS client.

Figure – RADIUS client



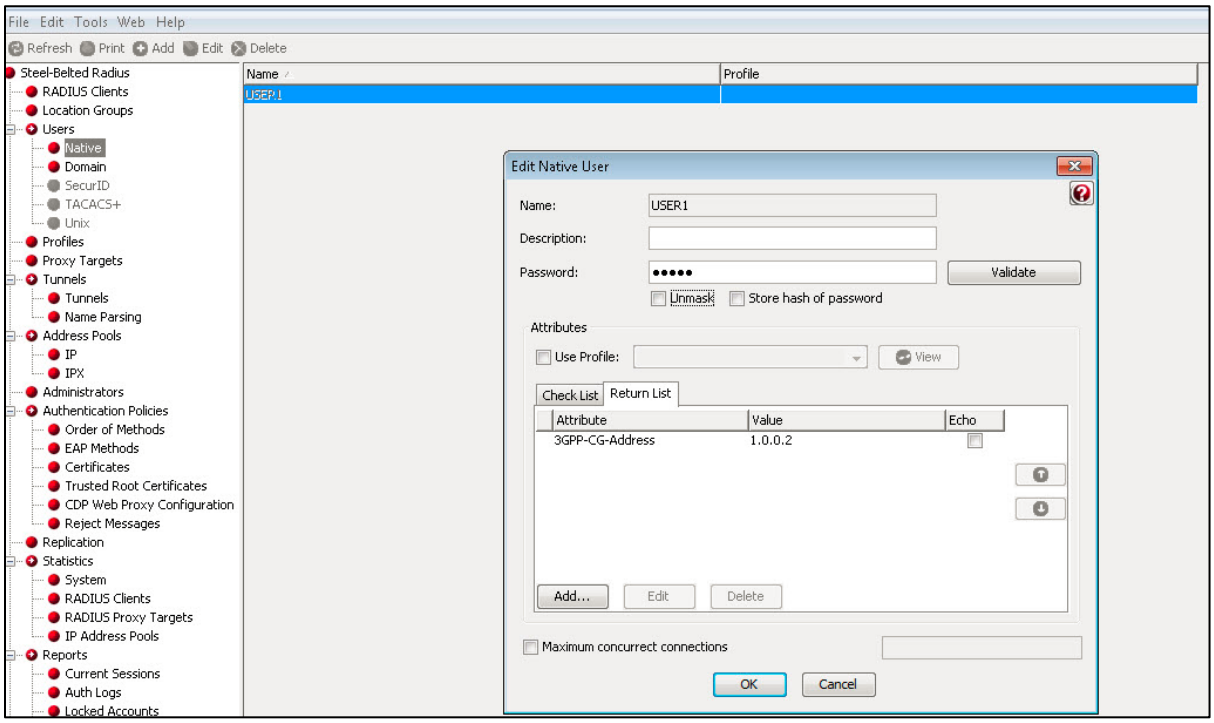
Note: If RADIUS client is not using profile and location group then the default Location group is used.

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.

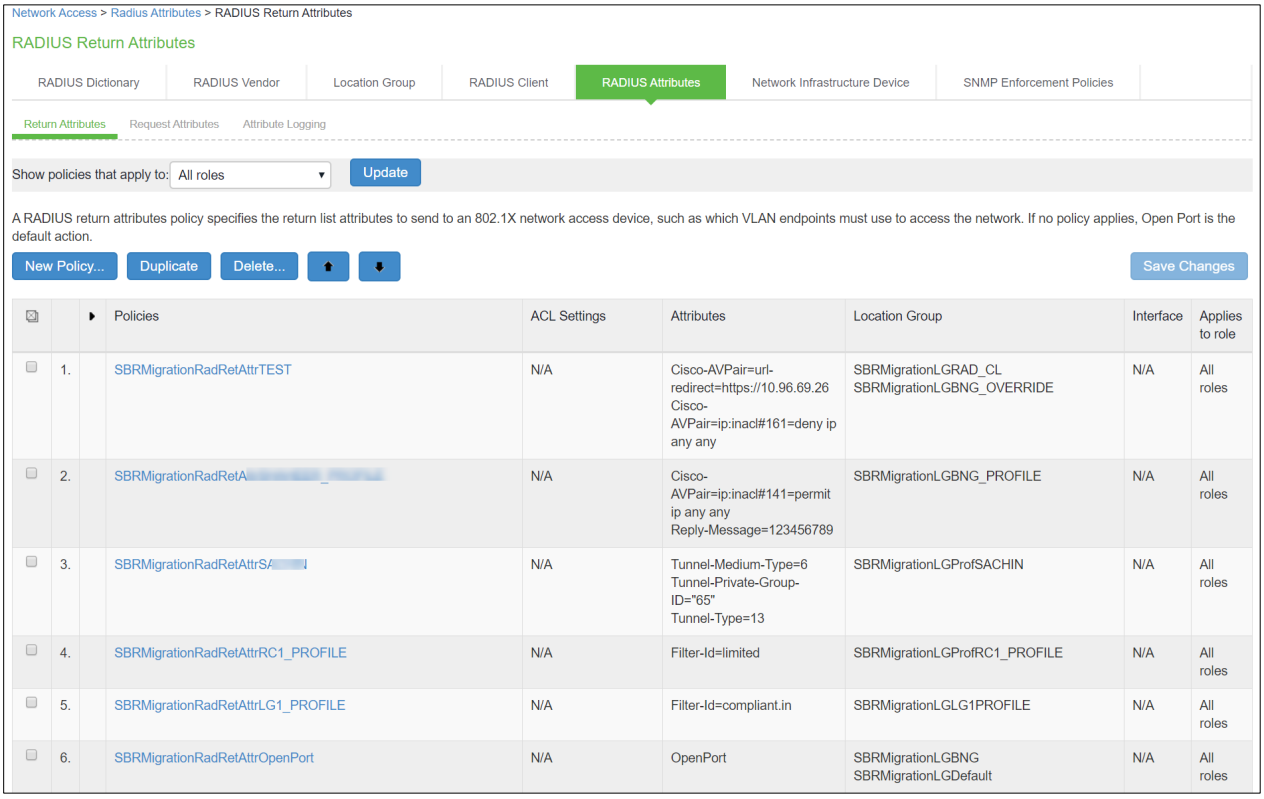


Configuring RADIUS Return Attribute Policies on PPS

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



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.

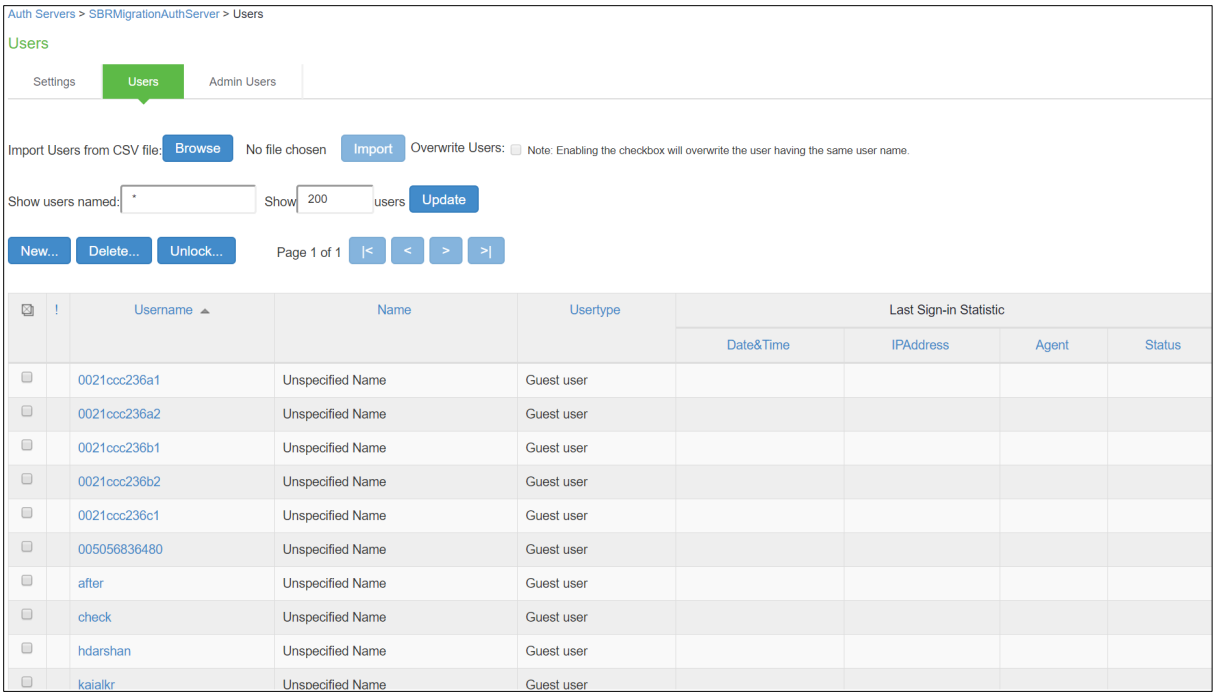
MAC Address Authentication Migration

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



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 = spawnd {
        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_PASSWD = $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\.108\.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 $1$xxxxxxxx$hDZPHghXe8XvoHeFdqUwm/
       member = readwrite@world
    }

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

    user = fred {
       password = clear kurkure
       member = getconfig@world
    }
}
```

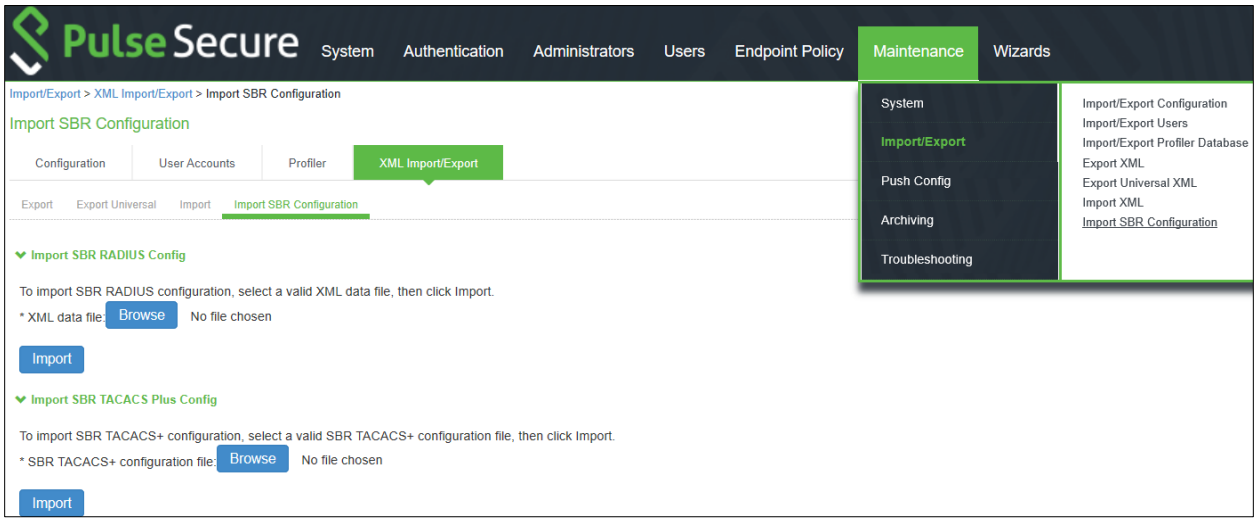
SBR TACACS+ config file

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**.

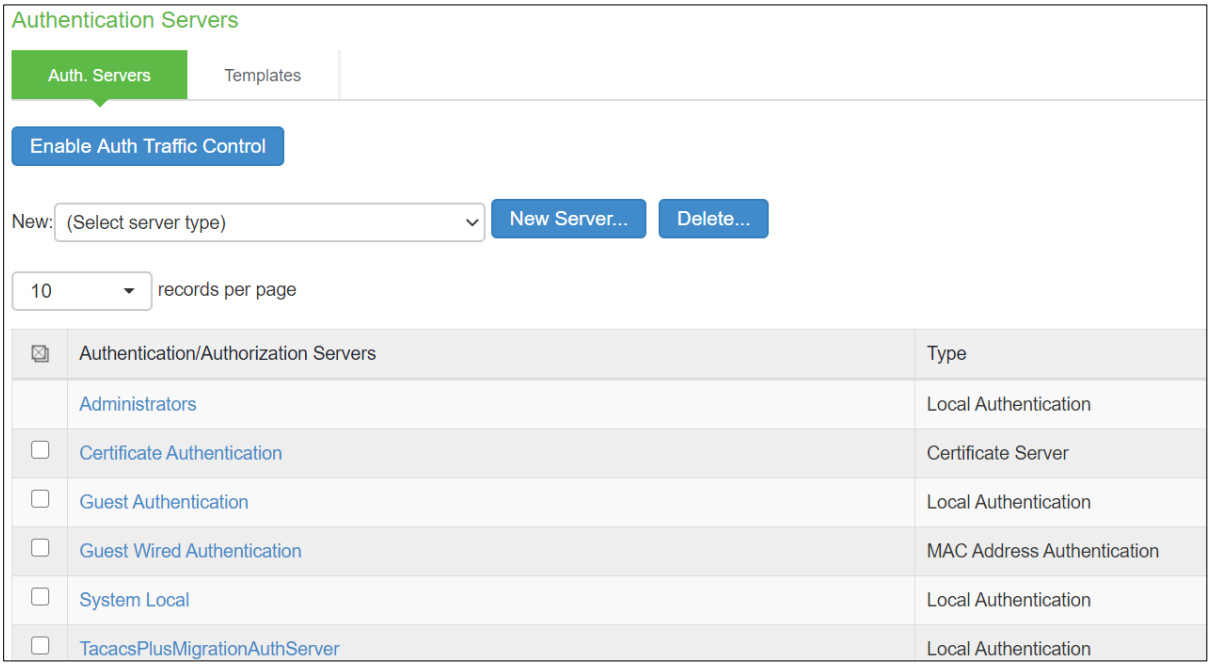
Figure –Import SBR TACACS + config



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.



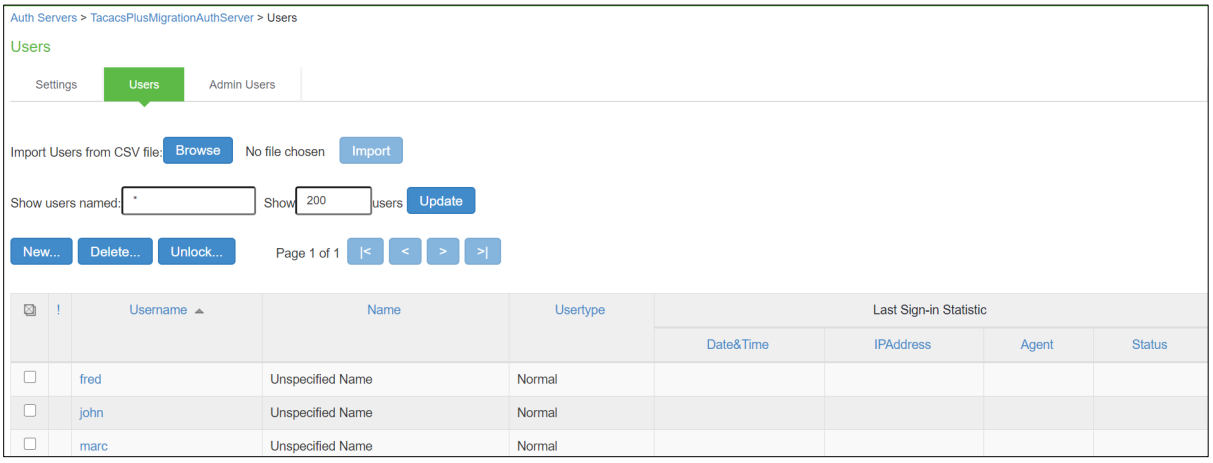
Note: Any secondary LDAP/AD servers configured in SBR tac_plusd.cfg file are not migrated and admin should configure them manually in PPS.

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**.

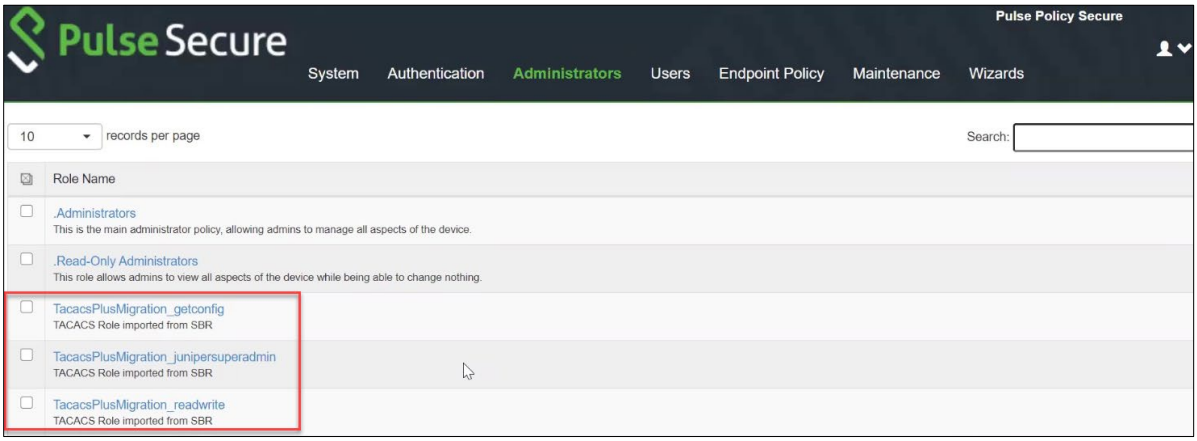
Figure –Users



Roles

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

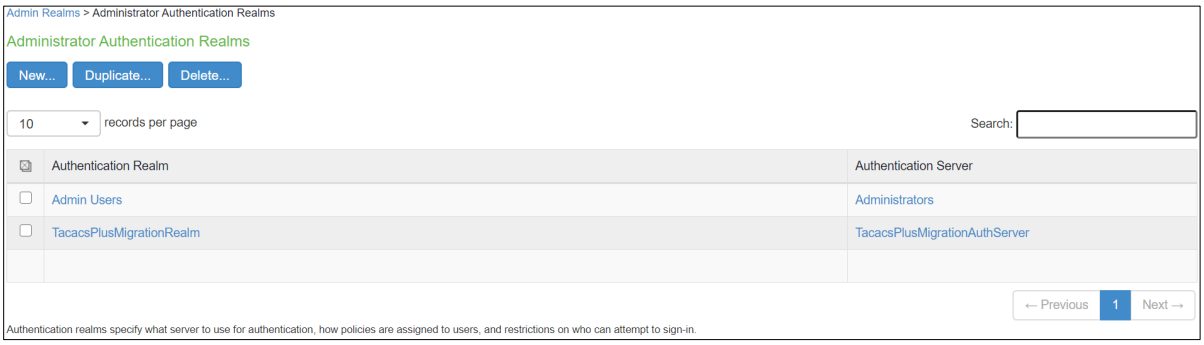
Figure –TacacsPlus Roles



Realm

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

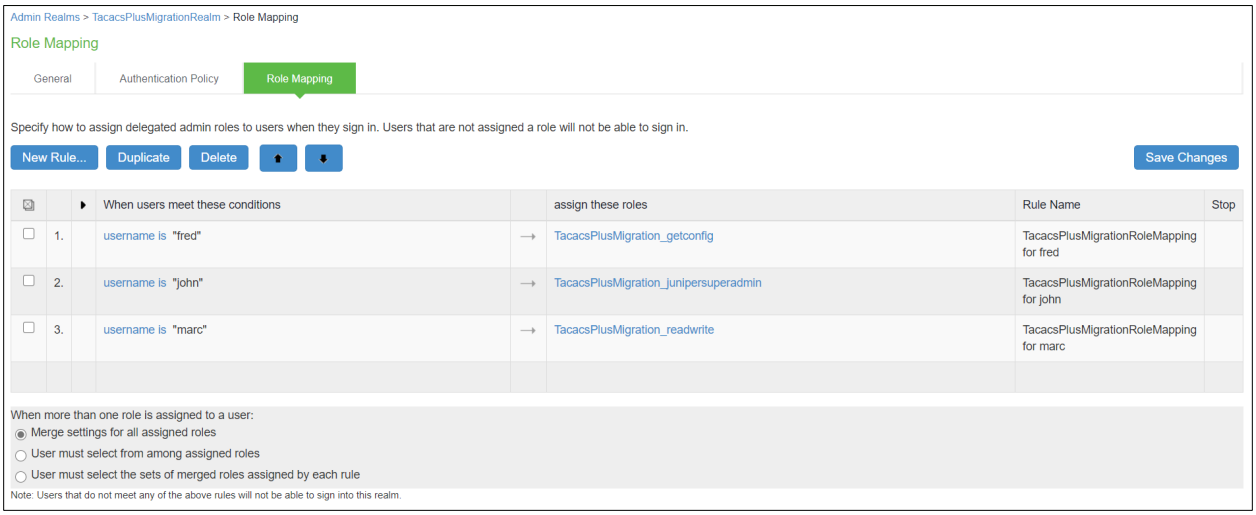
Figure –Admin Realm



Role Mapping

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

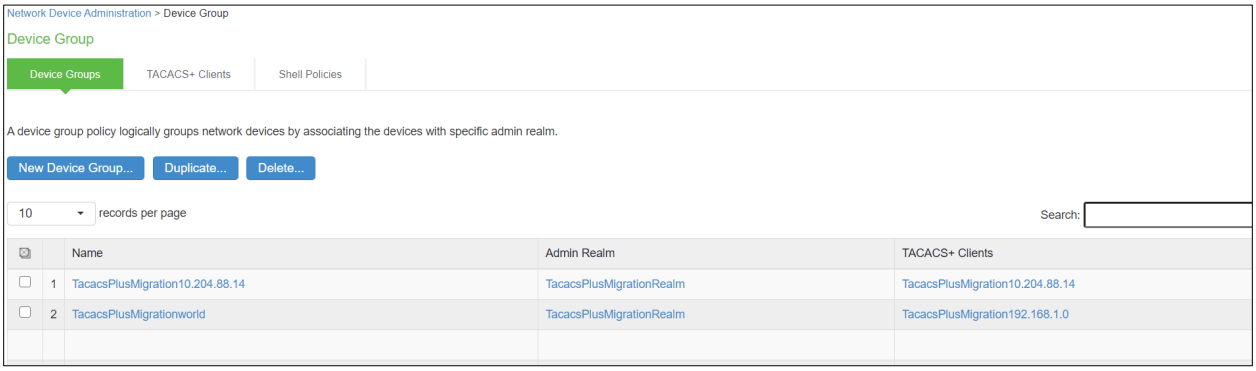
Figure –Role Mapping

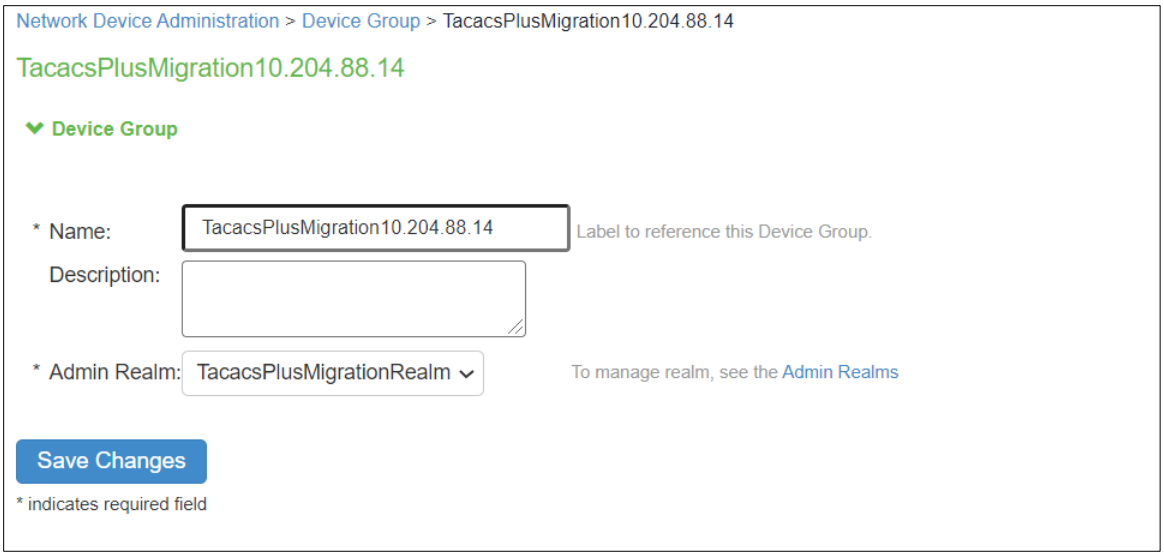


Device groups

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

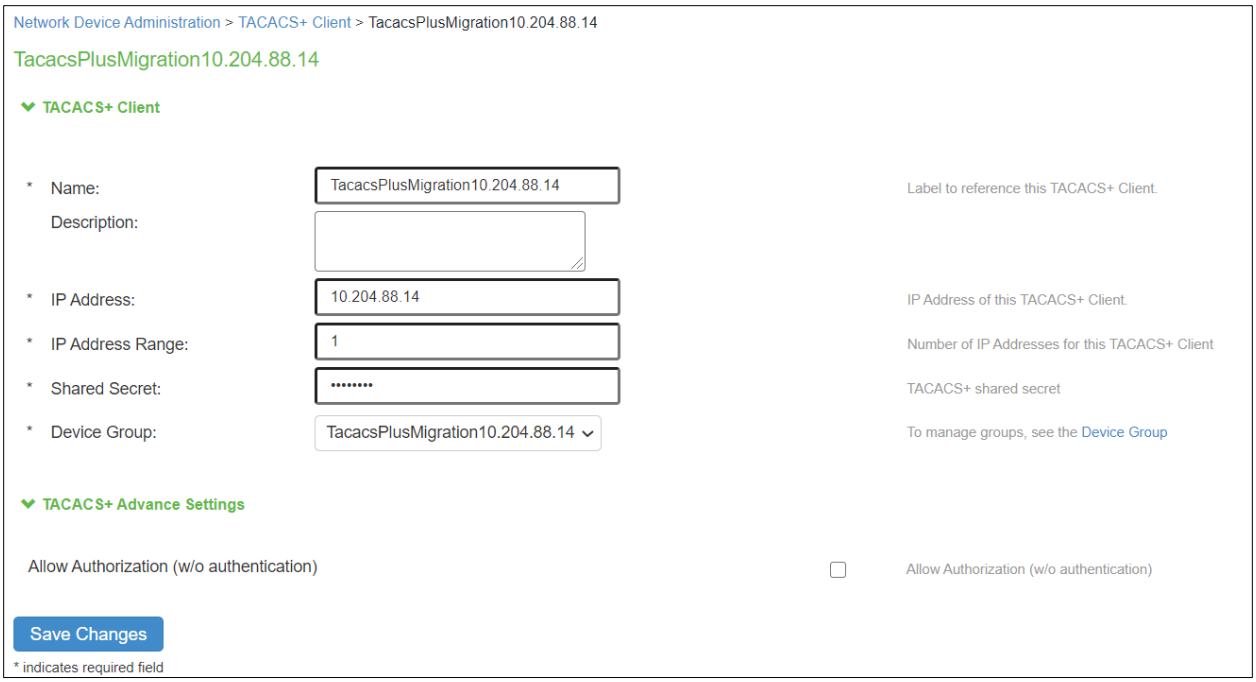




Clients

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

Figure –Clients

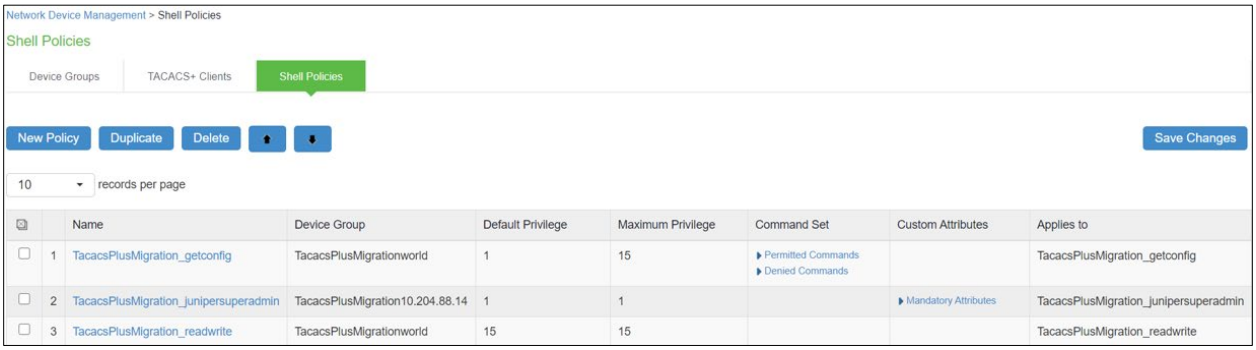


Shell policies

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.

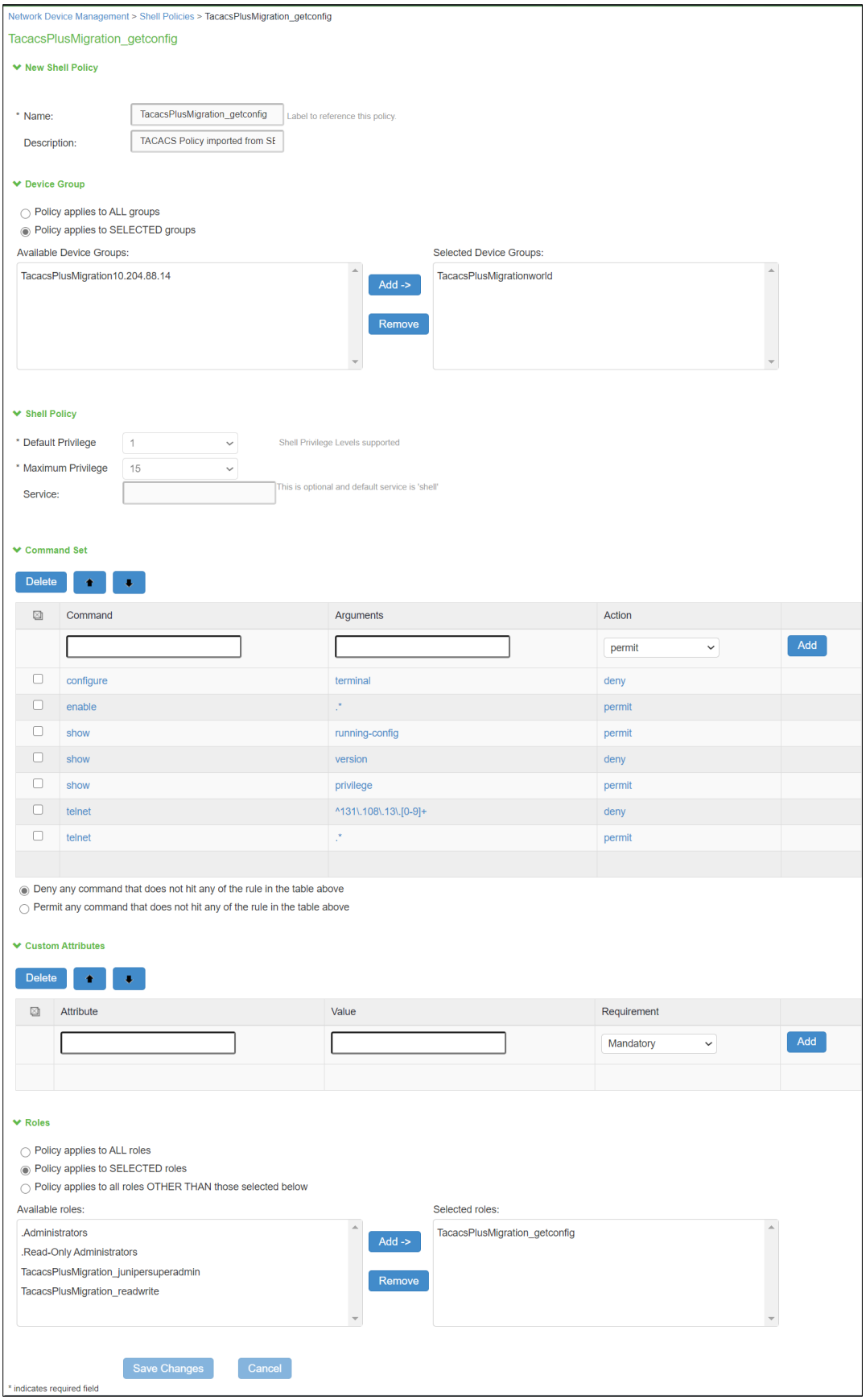
Note: The migration tool migrates only the first 13 custom attributes of the SBR shell policy to PPS and the remaining are not migrated.

Figure –Shell Policies



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".


Network Device Management > Shell Policies > TacacsPlusMigration_getconfig
TacacsPlusMigration_getconfig
New Shell Policy
* Name:
TacacsPlusMigration_getconfig
Label to reference this policy.
Description:
TACACS Policy imported from SE
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
1
Shell Privilege Levels supported
* Maximum Privilege
15
Service:
This is optional and default service is 'shell'
Command Set
Delete
Command
Arguments
Action
permit
Add
configure
terminal
deny
enable
.*
permit
show
running-config
permit
show
version
deny
show
privilege
permit
telnet
^131\.108\.13\.[0-9]+
deny
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
Mandatory
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
Save Changes
Cancel
* 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