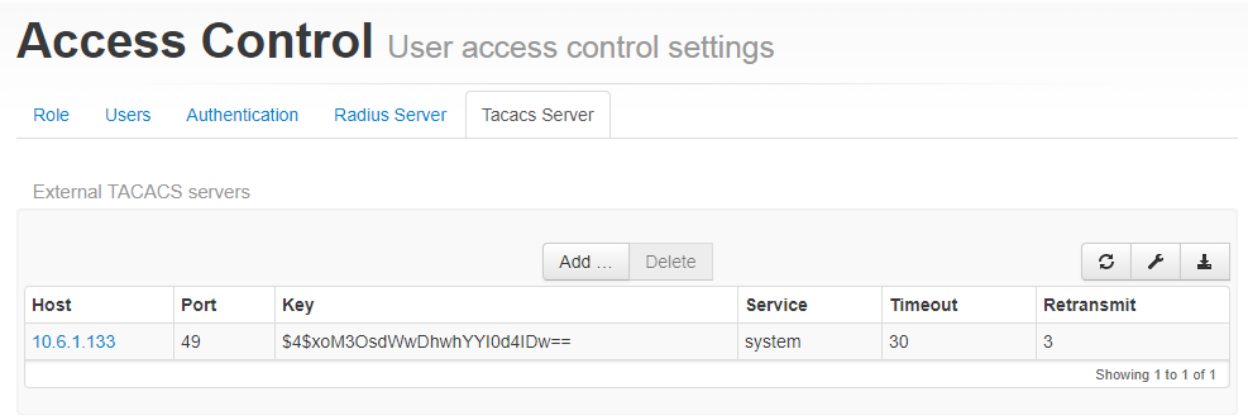
# Cisco Identity Services Engine (ISE) TACACS+ SETUP WITH PFS5000/6000 series

**Tech Note**

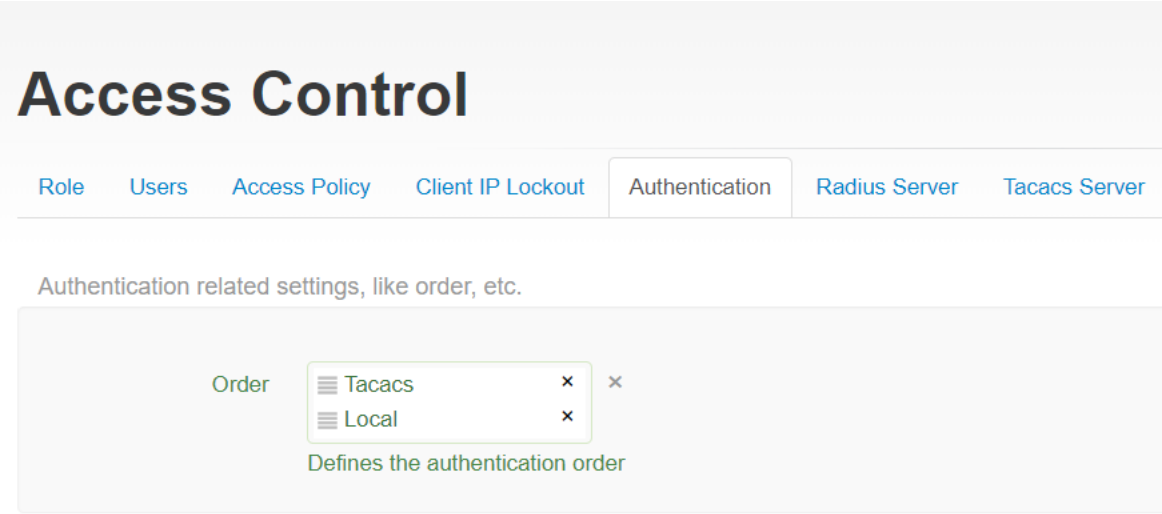
Rev. 1.0

Under PFS GUI or similar Fabric Manager pages:

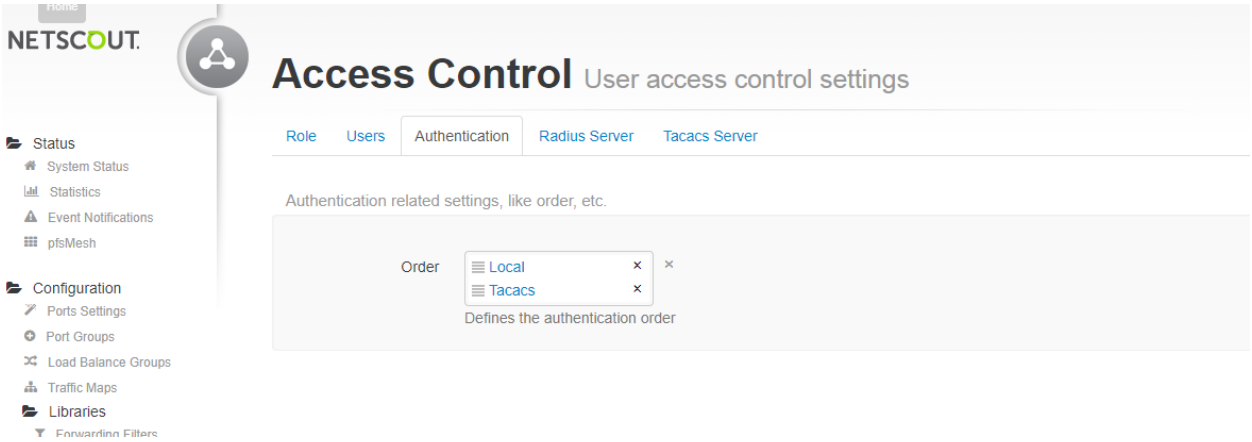
Go to Access Control:
Enter TACACS server information. Important:
Key value must the same as shared secret configured on the server.
Service must be configured as “system” (service is not configurable on the server side)




Add “TACACS” Authentication and assign it as higher priority than “Local” users.

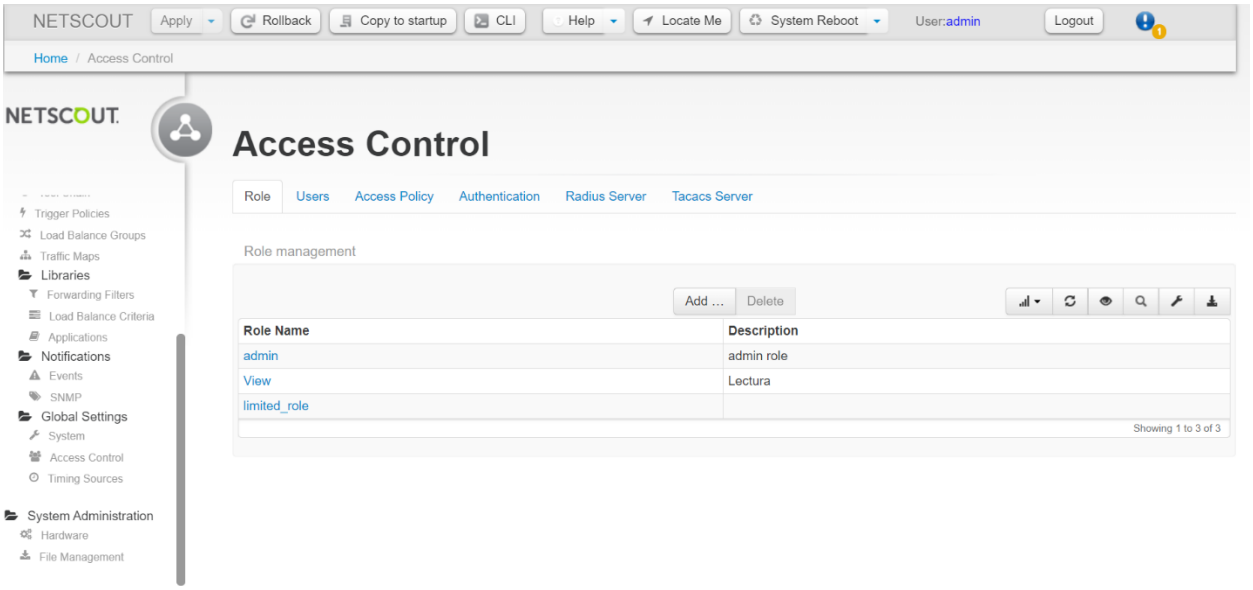


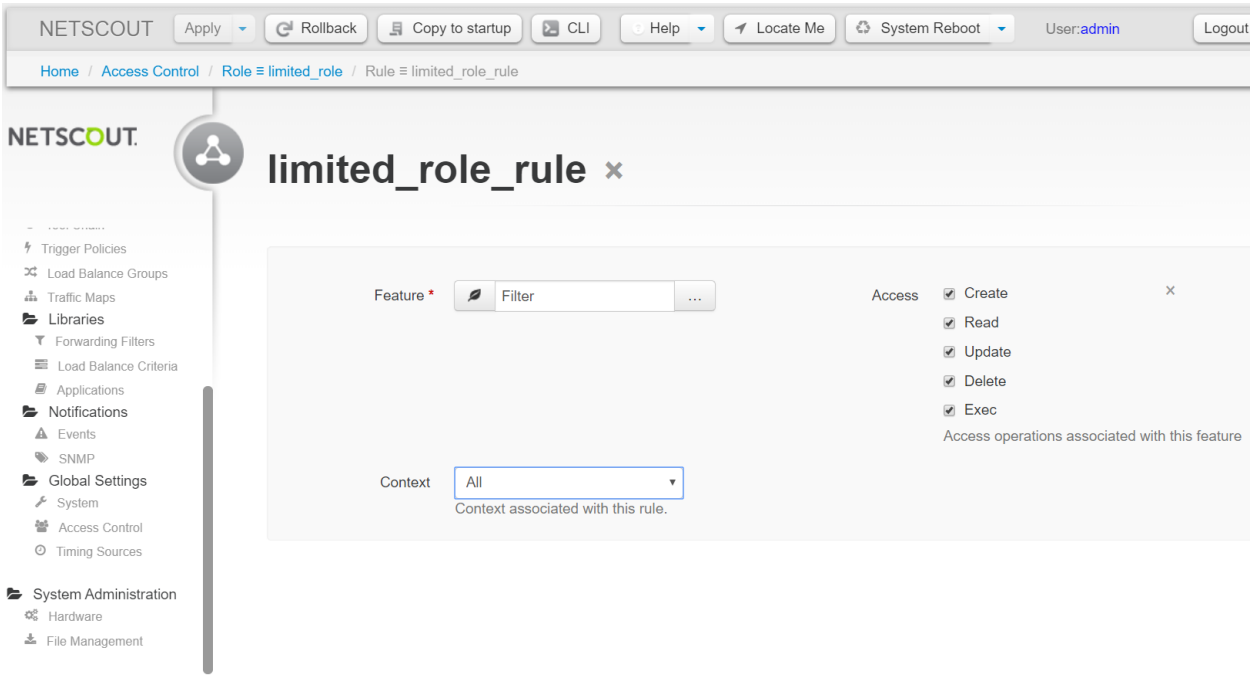

The following priority is local 1st and may not work for TACACS+:



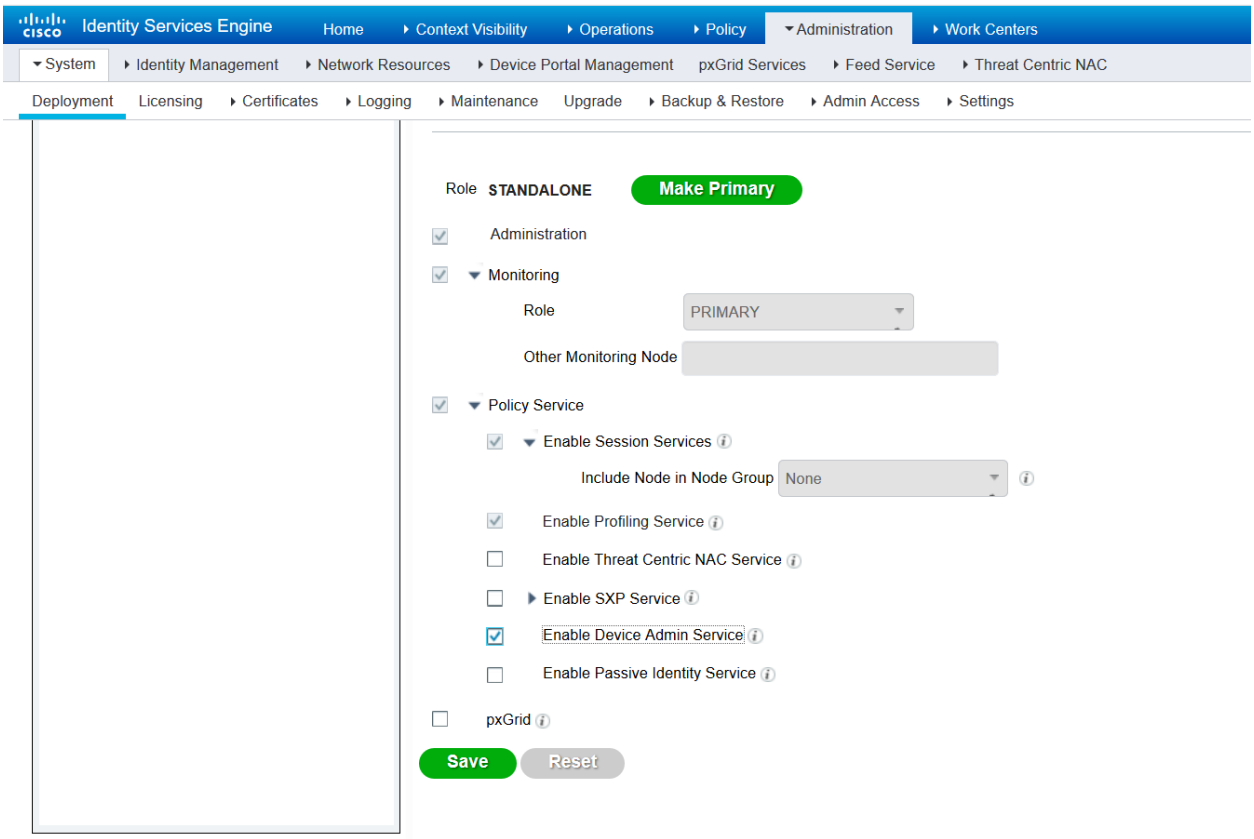

Configure user roles. These should match with those on TACACS shell profile string. For example, if user role is “limited_user_role”, then TACACS shell ACL should use “groups=limited_user_role”.

Note: “admin” role is already built-in on PFS and does not need to be configured. In many deployments built-in admin role is sufficient for TACACS+ implementation.

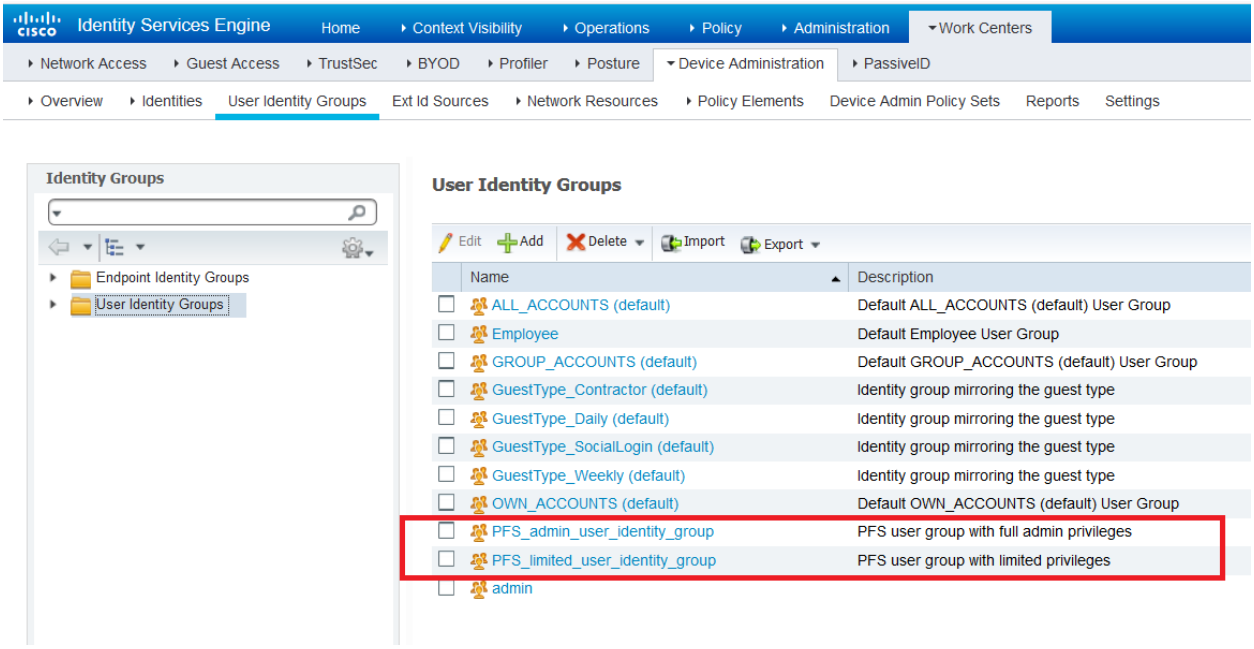




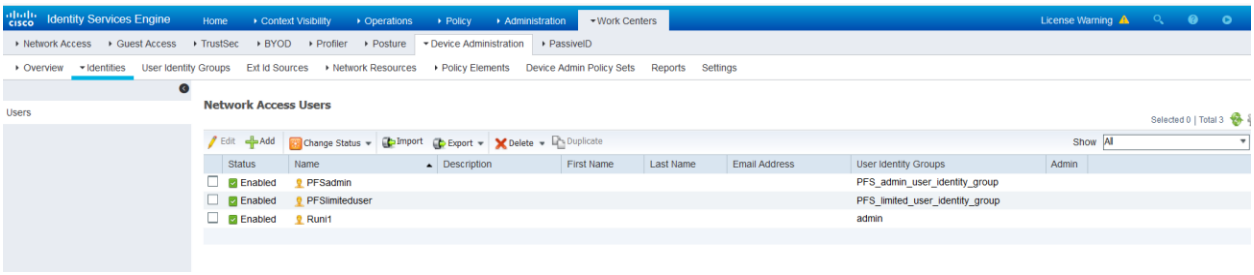

Enable TACACS+ device admin service on ISE:



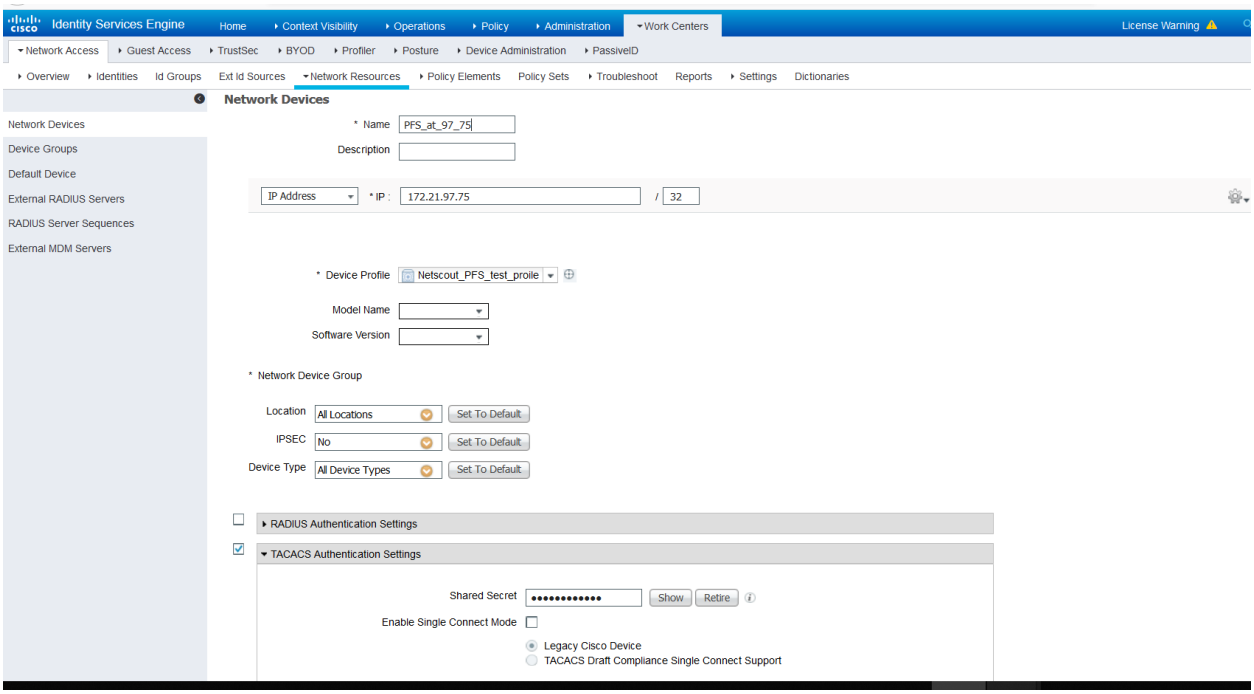

Create Identity user group if needed:




Create user identities. Assign to user groups if needed.

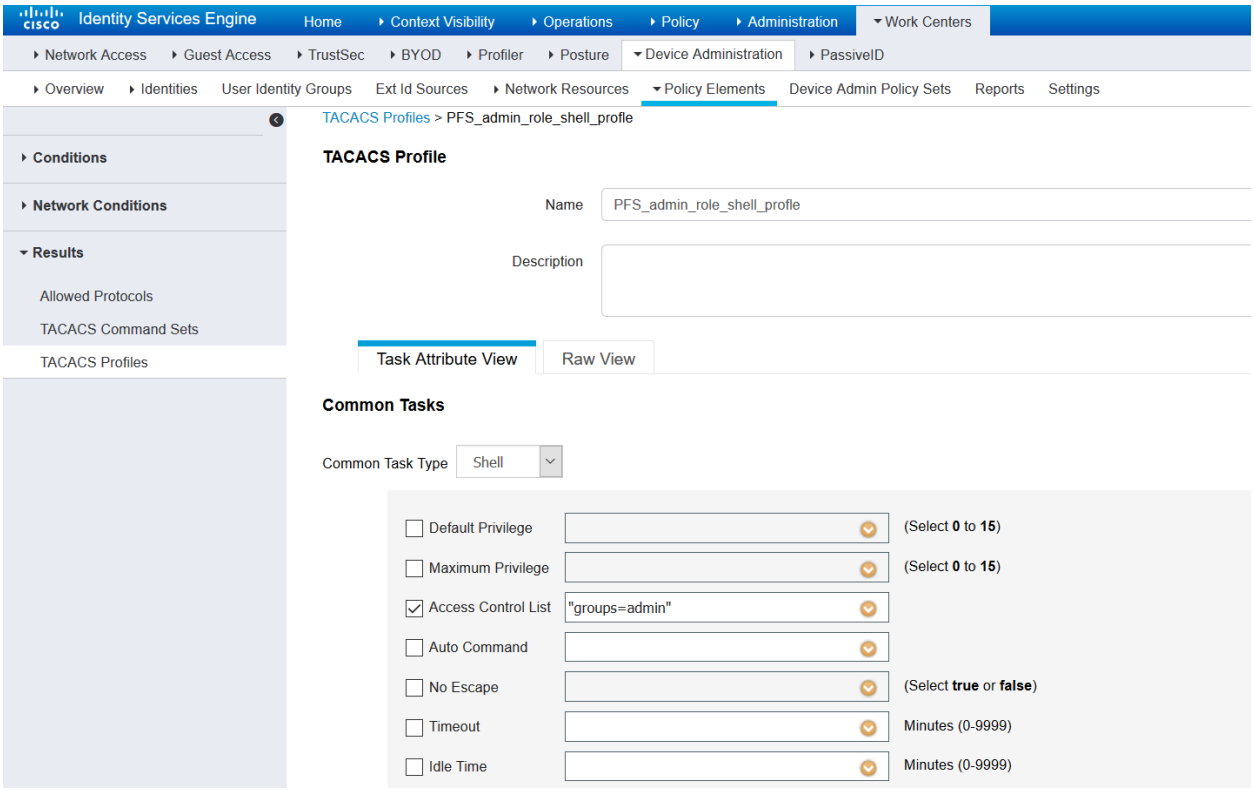


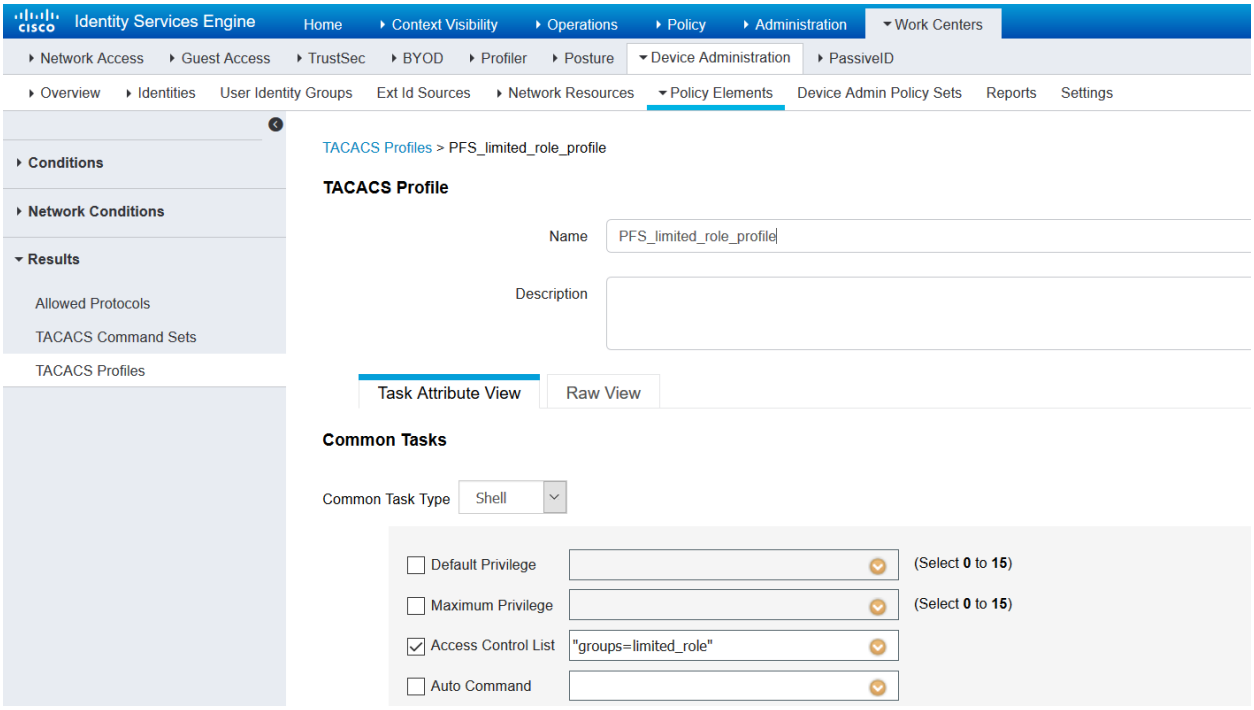

Assign network resources. Secret should match value on PFS:

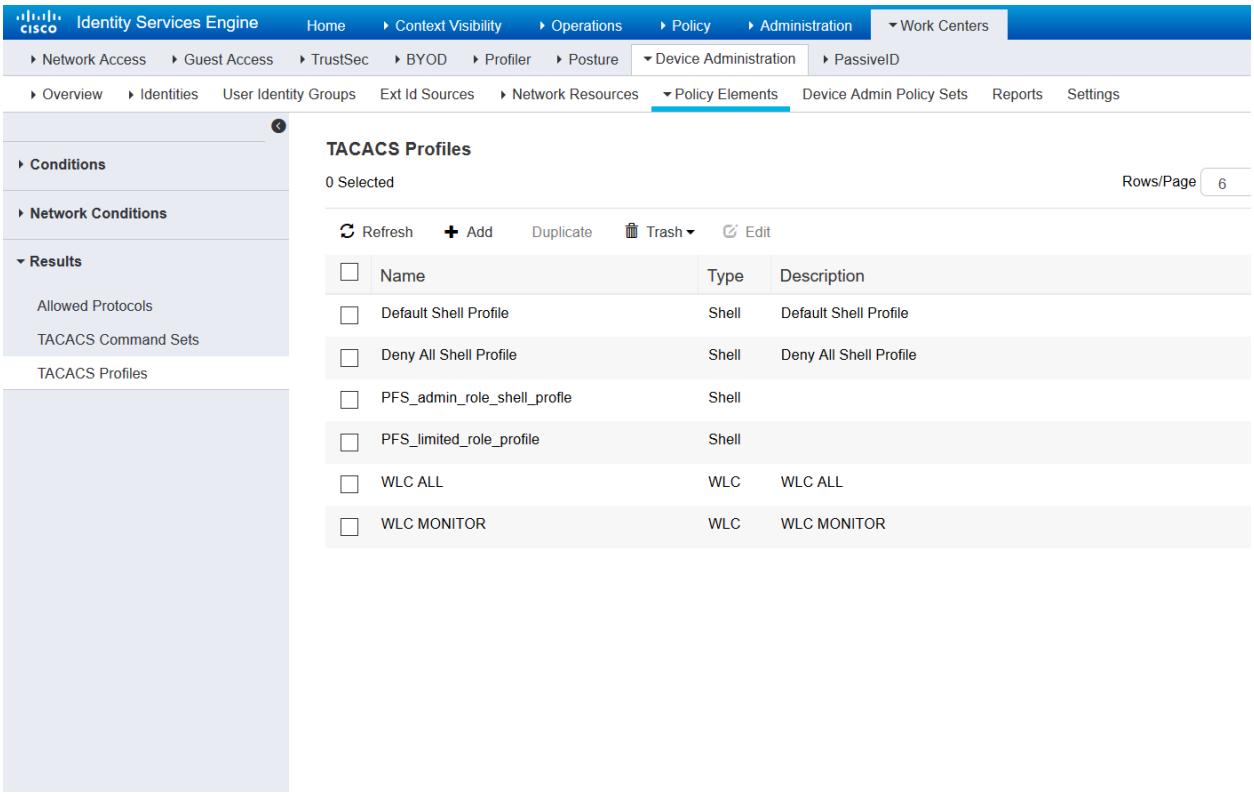



Under WorkCenters -> Device Administration -> Policy Results. Add TACACS profile. Profile edit -> Common tasks. Select privileges/shell/Access Control List (ACL).

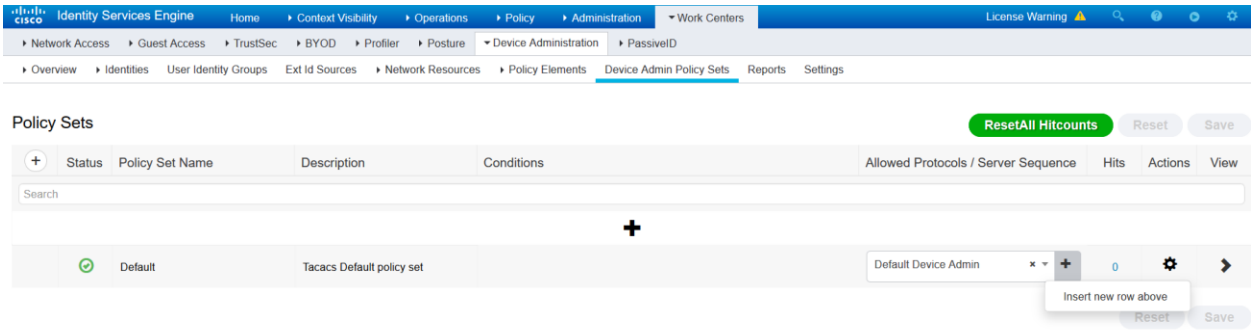
Enter string for the role.
If PFS role is admin then ACL value on the server should be: “groups=admin”.
If PFS role is “limited_user_role”, then ACL value on the server should be: “groups= limited_user_role”.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > PFS_admin_role_shell_profle
TACACS Profile
Name
PFS_admin_role_shell_profle
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
(Select 0 to 15)
Maximum Privilege
(Select 0 to 15)
Access Control List
"groups=admin"
Auto Command
No Escape
(Select true or false)
Timeout
Minutes (0-9999)
Idle Time
Minutes (0-9999)


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Conditions
Network Conditions
Results
Allowed Protocols
TACACS Command Sets
TACACS Profiles
TACACS Profiles > PFS_limited_role_profile
TACACS Profile
Name
PFS_limited_role_profile
Description
Task Attribute View
Raw View
Common Tasks
Common Task Type
Shell
Default Privilege
(Select 0 to 15)
Maximum Privilege
(Select 0 to 15)
Access Control List
"groups=limited_role"
Auto Command

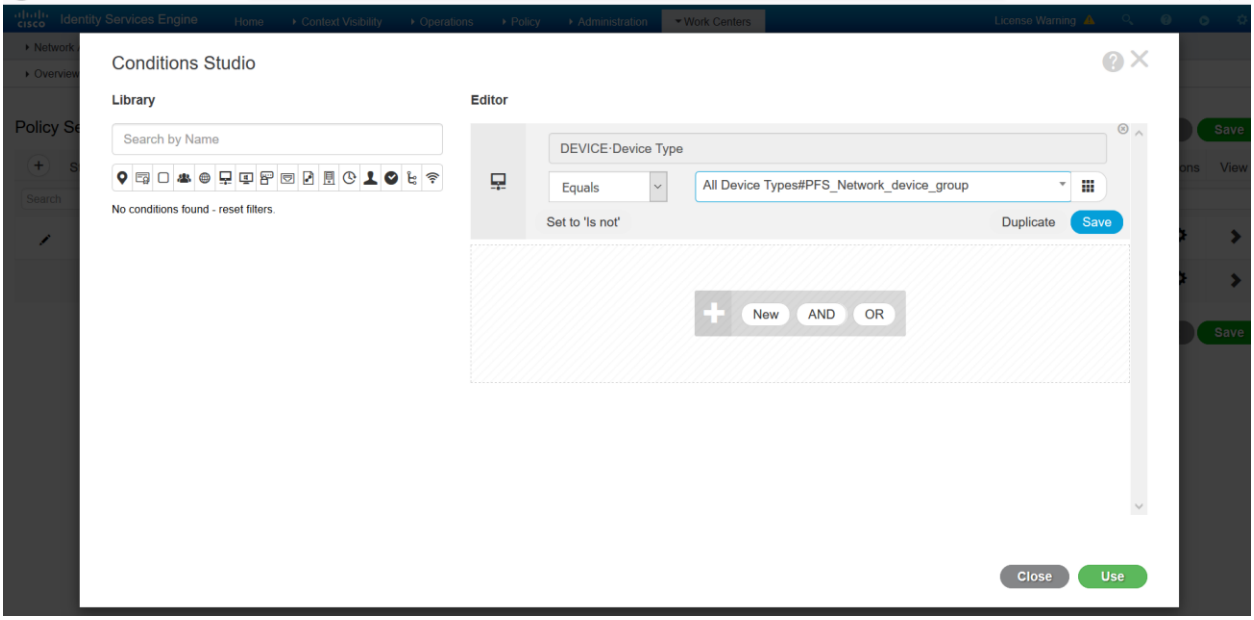


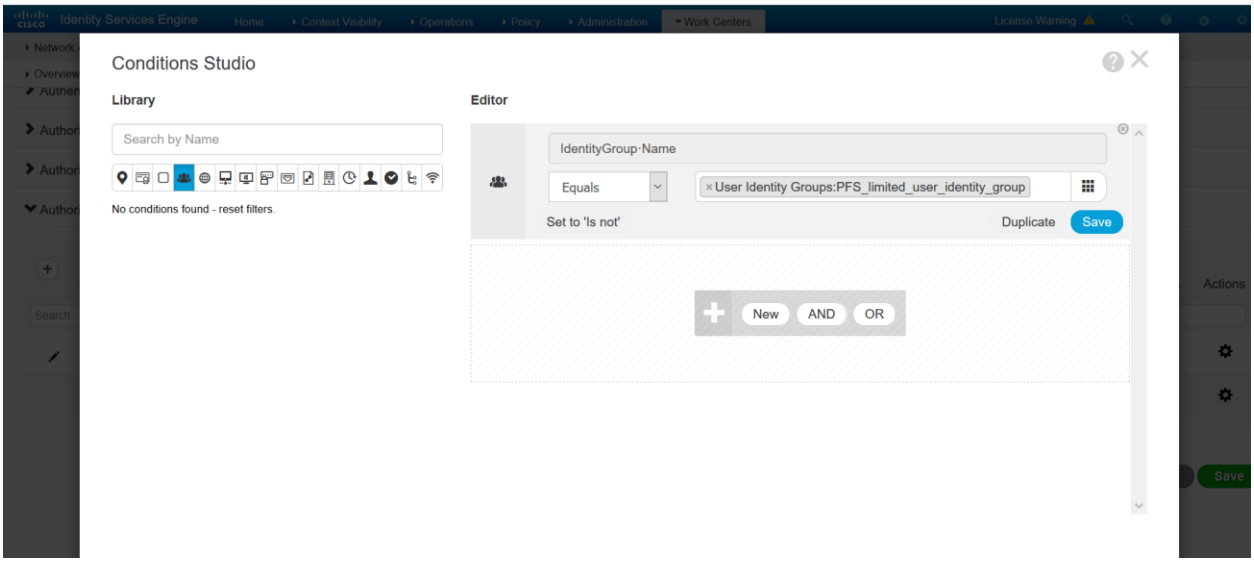

Edit TACACS policy by starting dialog with right arrow icon:

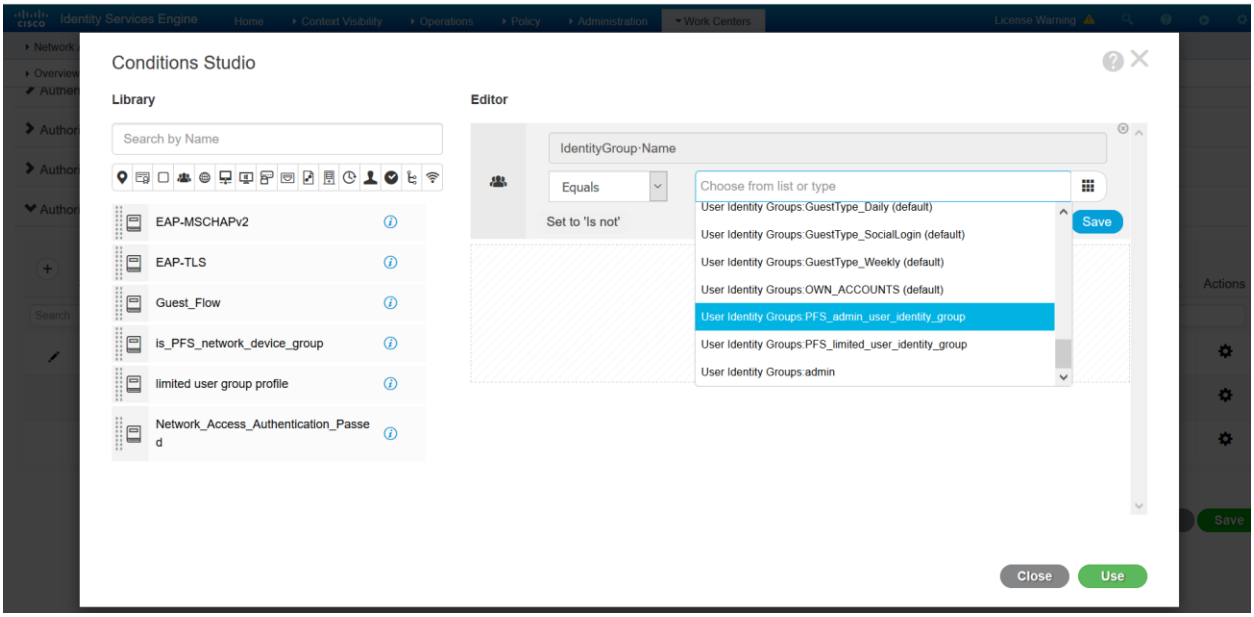


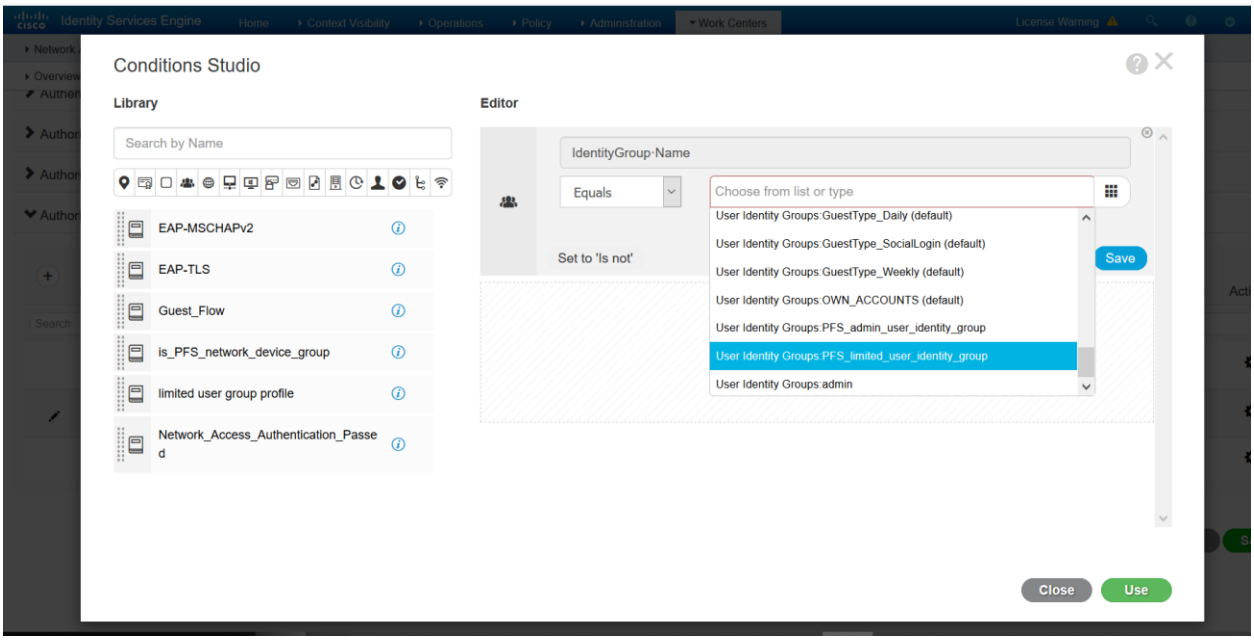

Configure Authorization policy for Netscout PFS devices. Details and logic would depend on your IT policies. Some examples below illustrate how this may be configured.

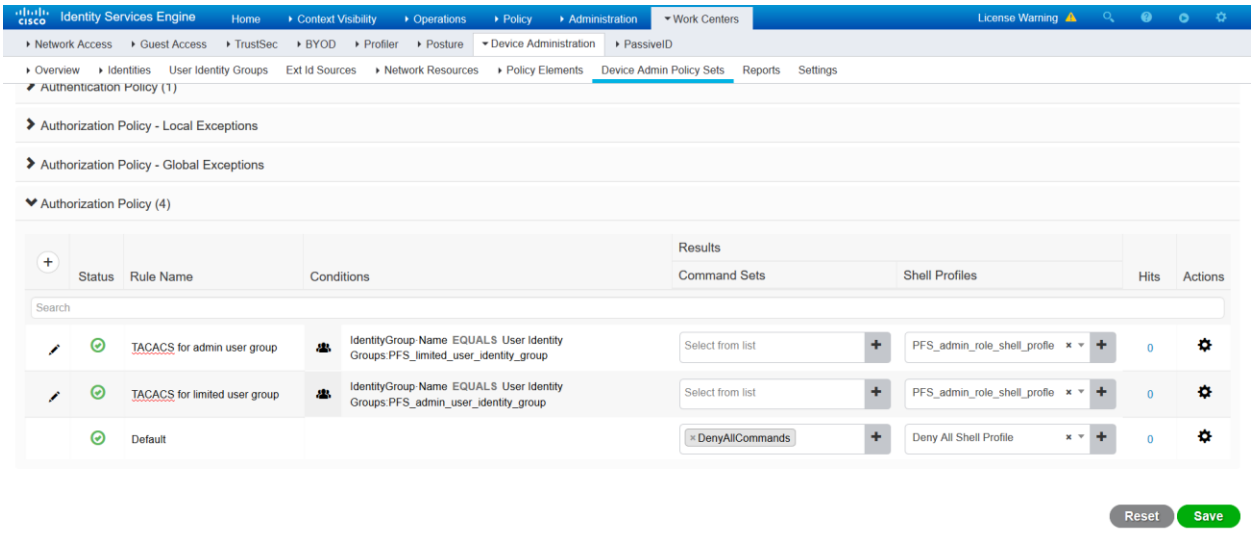
Ensure that a shell profile is chosen for specific Authorization policy.


Conditions Studio
Library
Search by Name
No conditions found - reset filters.
Editor
DEVICE·Device Type
Equals
All Device Types#PFS_Network_device_group
Set to 'Is not'
Duplicate
Save
New
AND
OR
Close
Use


Conditions Studio
Library
Search by Name
No conditions found - reset filters.
Editor
IdentityGroup·Name
Equals
User Identity Groups:PFS_limited_user_identity_group
Set to 'Is not'
Duplicate
Save
New
AND
OR


Conditions Studio
Library
Search by Name
EAP-MSCHAPv2
EAP-TLS
Guest_Flow
is_PFS_network_device_group
limited user group profile
Network_Access_Authentication_Passed
Editor
IdentityGroup·Name
Equals
Choose from list or type
Set to 'Is not'
Save
User Identity Groups:GuestType_Daily (default)
User Identity Groups:GuestType_SocialLogin (default)
User Identity Groups:GuestType_Weekly (default)
User Identity Groups:OWN_ACCOUNTS (default)
User Identity Groups:PFS_admin_user_identity_group
User Identity Groups:PFS_limited_user_identity_group
User Identity Groups:admin
Close
Use




Another example of authorization policy logic: