

---

# 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 be the same as shared secret configured on the server.

Service must be configured as "system" (service is not configurable on the server side)

## Access Control User access control settings

Role Users Authentication Radius Server Tacacs Server

External TACACS servers

| Host       | Port | Key                           | Service | Timeout | Retransmit |
|------------|------|-------------------------------|---------|---------|------------|
| 10.6.1.133 | 49   | \$4\$xoM3OsdWwDhwhYY10d4IDw== | system  | 30      | 3          |

Showing 1 to 1 of 1

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

## Access Control

Role Users Access Policy Client IP Lockout Authentication Radius Server Tacacs Server

Authentication related settings, like order, etc.

Order      
Defines the authentication order

The following priority is local 1<sup>st</sup> and may not work for TACACS+:

NETSCOUT. **Access Control** User access control settings

Role Users **Authentication** Radius Server Tacacs Server

Authentication related settings, like order, etc.

Order

Defines the authentication order

- Status
  - System Status
  - Statistics
  - Event Notifications
  - pfsMesh
- Configuration
  - Ports Settings
  - Port Groups
  - Load Balance Groups
  - Traffic Maps
  - Libraries
    - Forwarding Filters

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.

NETSCOUT Apply Rollback Copy to startup CLI Help Locate Me System Reboot User:admin Logout

Home / Access Control

NETSCOUT. **Access Control**

Role Users Access Policy **Authentication** Radius Server Tacacs Server

Role management

Add ... Delete

| Role Name            | Description |
|----------------------|-------------|
| admin                | admin role  |
| <a href="#">View</a> | Lectura     |
| limited_role         |             |

Showing 1 to 3 of 3

- Trigger Policies
- Load Balance Groups
- Traffic Maps
- Libraries
  - Forwarding Filters
  - Load Balance Criteria
- Applications
- Notifications
  - Events
  - SNMP
- Global Settings
  - System
  - Access Control
  - Timing Sources
- System Administration
  - Hardware
  - File Management

NETSCOUT Apply Rollback Copy to startup CLI Help Locate Me System Reboot User:admin Logout

Home / Access Control / Role  $\equiv$  limited\_role / Rule  $\equiv$  limited\_role\_rule

# NETSCOUT limited\_role\_rule $\times$

- Trigger Policies
- Load Balance Groups
- Traffic Maps
- Libraries
  - Forwarding Filters
  - Load Balance Criteria
  - Applications
- Notifications
  - Events
  - SNMP
- Global Settings
  - System
  - Access Control
  - Timing Sources
- System Administration
  - Hardware
  - File Management

Feature  $\star$   ...

Access  Create  Read  Update  Delete  Exec  $\times$   
Access operations associated with this feature

Context   $\downarrow$   
Context associated with this rule.

Enable TACACS+ device admin service on ISE:

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Role **STANDALONE** **Make Primary**

- Administration
- Monitoring
  - Role: PRIMARY
  - Other Monitoring Node: [Text Field]
- Policy Service
  - Enable Session Services
    - Include Node in Node Group: None
  - Enable Profiling Service
  - Enable Threat Centric NAC Service
  - Enable SXP Service
  - Enable Device Admin Service
  - Enable Passive Identity Service
- pxGrid

**Save** **Reset**

Create Identity user group if needed:

Identity Services Engine 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

**Identity Groups**

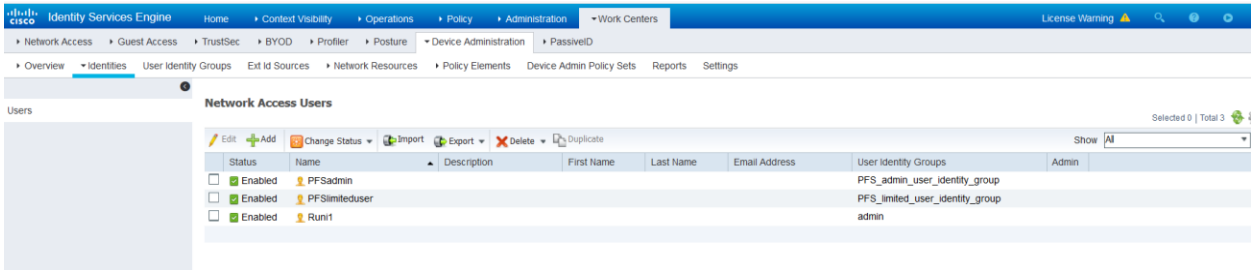
- Endpoint Identity Groups
- User Identity Groups**

**User Identity Groups**

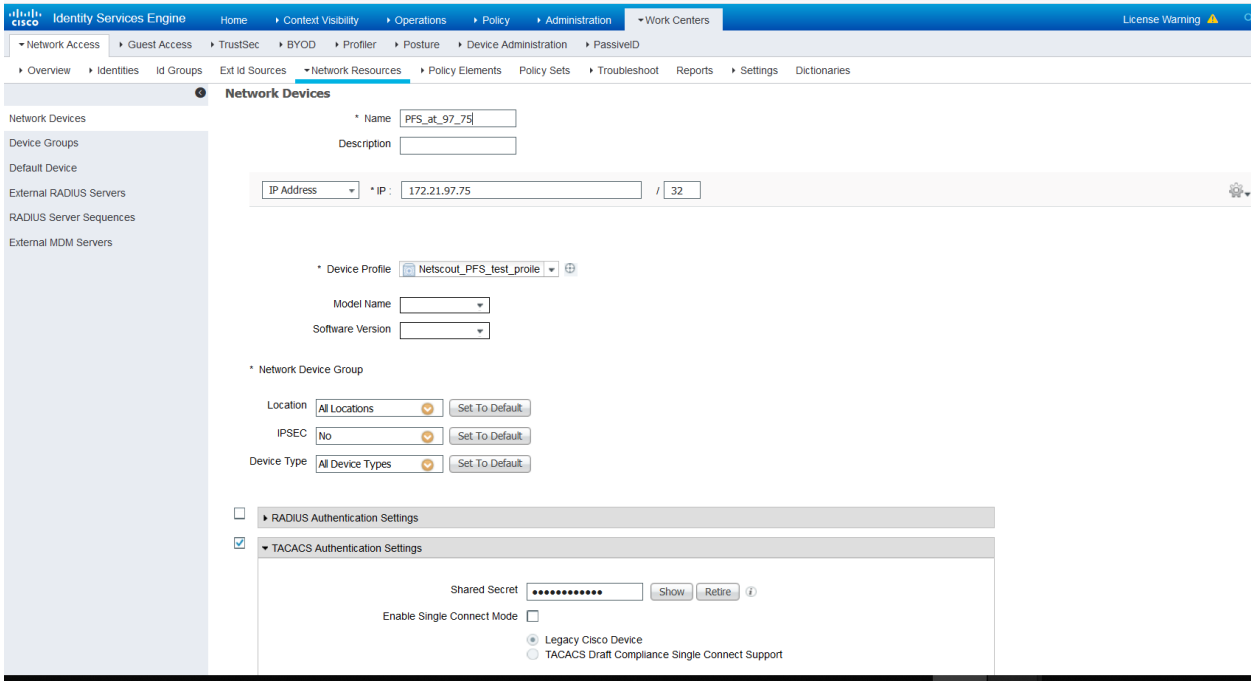
Edit Add Delete Import Export

| Name   | Description                                 |
|--|---|
| <input type="checkbox"/> ALL_ACCOUNTS (default)          | Default ALL_ACCOUNTS (default) User Group   |
| <input type="checkbox"/> Employee                        | Default Employee User Group                 |
| <input type="checkbox"/> GROUP_ACCOUNTS (default)        | Default GROUP_ACCOUNTS (default) User Group |
| <input type="checkbox"/> GuestType_Contractor (default)  | Identity group mirroring the guest type     |
| <input type="checkbox"/> GuestType_Daily (default)       | Identity group mirroring the guest type     |
| <input type="checkbox"/> GuestType_SocialLogin (default) | Identity group mirroring the guest type     |
| <input type="checkbox"/> GuestType_Weekly (default)      | Identity group mirroring the guest type     |
| <input type="checkbox"/> OWN_ACCOUNTS (default)          | Default OWN_ACCOUNTS (default) User Group   |
| <input type="checkbox"/> PFS_admin_user_identity_group   | PFS user group with full admin privileges   |
| <input type="checkbox"/> PFS_limited_user_identity_group | PFS user group with limited privileges      |
| <input type="checkbox"/> admin                           |   |

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

TACACS Profiles > PFS\_admin\_role\_shell\_profile

### TACACS Profile

Name: PFS\_admin\_role\_shell\_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=admin" (Select true or false)
- 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

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" (Select true or false)
- Auto Command

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

### TACACS Profiles

0 Selected Rows/Page 6

Refresh Add Duplicate Trash Edit

| <input type="checkbox"/> | Name                         | Type  | Description            |
|--------------------------|------------------------------|-------|------------------------|
| <input type="checkbox"/> | Default Shell Profile        | Shell | Default Shell Profile  |
| <input type="checkbox"/> | Deny All Shell Profile       | Shell | Deny All Shell Profile |
| <input type="checkbox"/> | PFS_admin_role_shell_profile | Shell |                        |
| <input type="checkbox"/> | PFS_limited_role_profile     | Shell |                        |
| <input type="checkbox"/> | WLC ALL                      | WLC   | WLC ALL                |
| <input type="checkbox"/> | WLC MONITOR                  | WLC   | WLC MONITOR            |

Edit TACACS policy by starting dialog with right arrow icon:

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

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

### Policy Sets

ResetAll Hitcounts Reset Save

| + Status                            | Policy Set Name | Description               | Conditions | Allowed Protocols / Server Sequence | Hits | Actions | View |
|-------------------------------------|-----------------|---------------------------|------------|-------------------------------------|------|---------|------|
| <input type="text" value="Search"/> | +               |                           |            |                                     |      |         |      |
| <input checked="" type="checkbox"/> | Default         | Tacacs Default policy set |            | Default Device Admin                | 0    | ⚙️      | ➡️   |

Insert new row above  
Reset Save

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.



Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

### 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

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

### 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

Close Use

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

### Conditions Studio

**Library**

Search by Name

- EAP-MSCHAPv2
- EAP-TLS
- Guest\_Flow
- is\_PFS\_network\_device\_group
- limited user group profile
- Network\_Access\_Authentication\_Pas...

**Editor**

IdentityGroup-Name

Equals | Choose from list or type

- 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

Set to 'Is not'

Duplicate Save

Close Use

| Status | Rule Name                     | Conditions   | Results          | Hits                         | Actions |
|--------|-------------------------------|--|------------------|------------------------------|---------|
|        |                               |  | Command Sets     | Shell Profiles               |         |
| ✔      | TACACS for admin user group   | IdentityGroup Name EQUALS User Identity Groups.PFS_limited_user_identity_group | Select from list | PFS_admin_role_shell_profile | 0       |
| ✔      | TACACS for limited user group | IdentityGroup Name EQUALS User Identity Groups.PFS_admin_user_identity_group   | Select from list | PFS_admin_role_shell_profile | 0       |
| ✔      | Default                       |  | DenyAllCommands  | Deny All Shell Profile       | 0       |

Another example of authorization policy logic: