HP JetAdvantage Connect Discovery Server

Configure the search domain settings for Pulse VPN

Table of contents

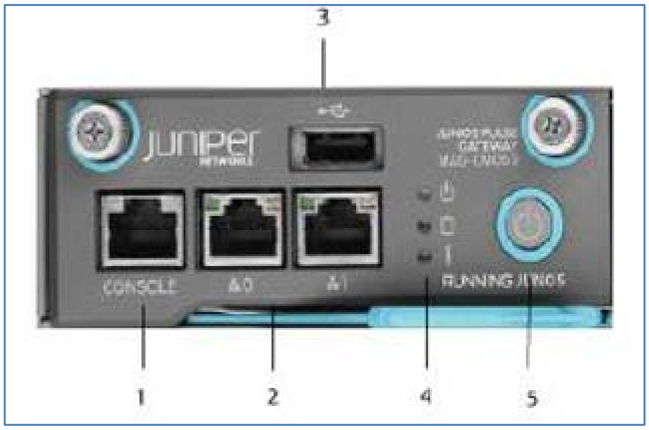
Introduction

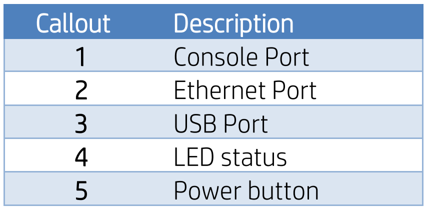
Note

The following documentation is provided as an example for configuring this VPN to provide a value for “Search Domains”. Some details may be different or may have changed depending upon the version of the VPN used. Please consult your VPN documentation for complete details.

The Pulse Gateway has three ports, three LED status, and a Power button.

Figure 1. Pulse Gateway CMC





Callout	Description
1	Console Port
2	Ethernet Port
3	USB Port
4	LED status
5	Power button

Set up and configure the settings for Pulse VPN

Set up the settings for Pulse VPN

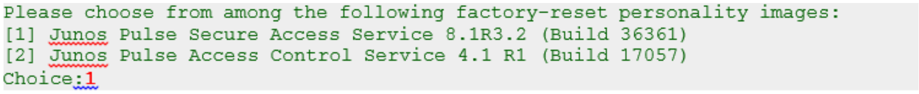
Follow these steps to set up the network settings:

1. Connect the RS232 console cable to Console Port (callout 1), and then connect the external WAN link (callout 2) to access the device after this setup.

2. With a console connection (or a roll over cable), set the following settings for a terminal connection:

    - Bits per sec: 9600
    - Data bits: 8
    - Stop bits: 1
    - Flow control: None

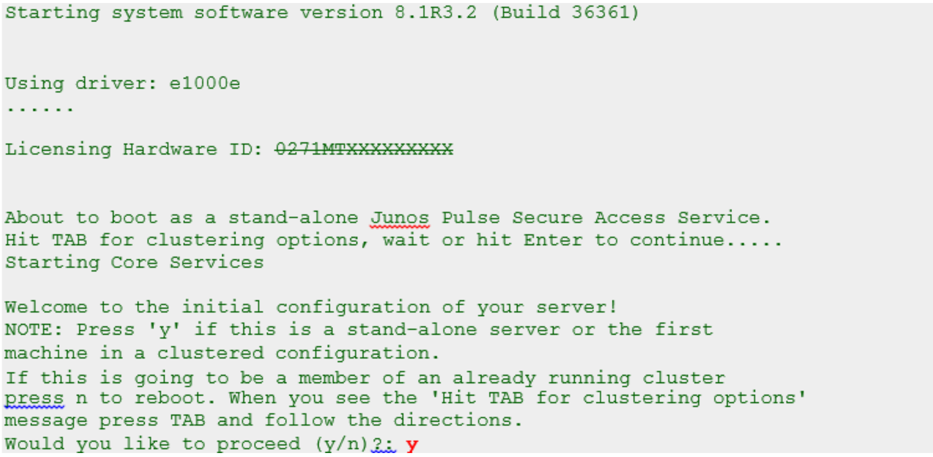
3. Select option **1** for the factory-reset personality images.



```
Please choose from among the following factory-reset personality images:
[1] Junos Pulse Secure Access Service 8.1R3.2 (Build 36361)
[2] Junos Pulse Access Control Service 4.1 R1 (Build 17057)
Choice:1
```

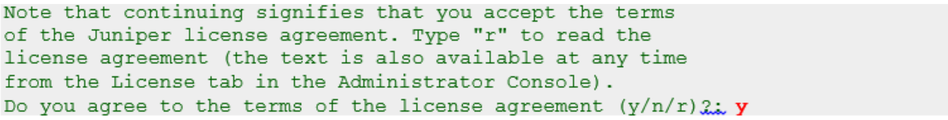
4. Agree to run the EzSetup procedure.

5. Type "*y*" to commit to the new configuration of the server and proceed.



```
Starting system software version 8.1R3.2 (Build 36361)


Using driver: e1000e
......

Licensing Hardware ID: ~~0271MTXXXXXXXXX~~


About to boot as a stand-alone Junos Pulse Secure Access Service.
Hit TAB for clustering options, wait or hit Enter to continue.....
Starting Core Services

Welcome to the initial configuration of your server!
NOTE: Press 'y' if this is a stand-alone server or the first
machine in a clustered configuration.
If this is going to be a member of an already running cluster
press n to reboot. When you see the 'Hit TAB for clustering options'
message press TAB and follow the directions.
Would you like to proceed (y/n)?: y
```

6. Type "y" to agree to the license agreement:

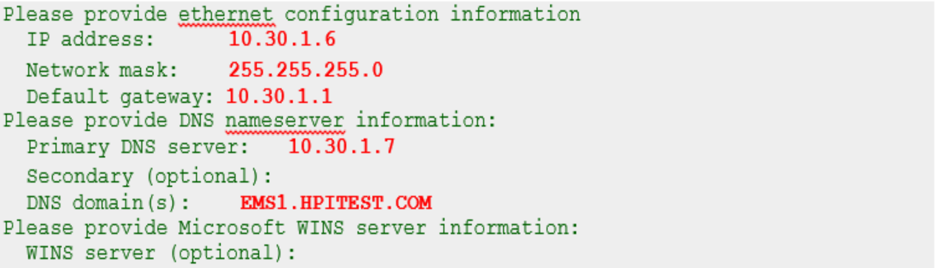


```
Note that continuing signifies that you accept the terms
of the Juniper license agreement. Type "r" to read the
license agreement (the text is also available at any time
from the License tab in the Administrator Console).
Do you agree to the terms of the license agreement (y/n/r)?: y
```

Configure the network settings

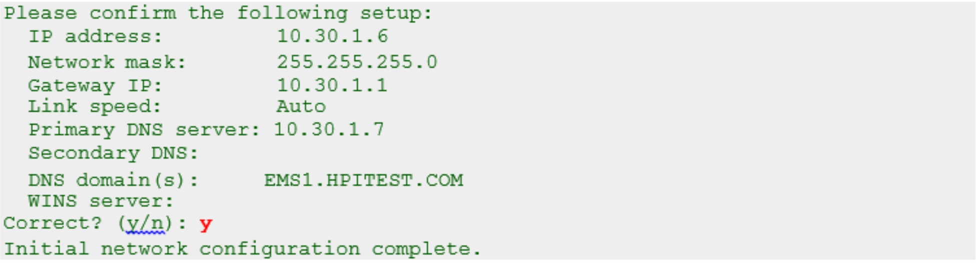
Follow these steps for the initial network configuration:

1. Type the information required for Ethernet configuration and DNS name server.



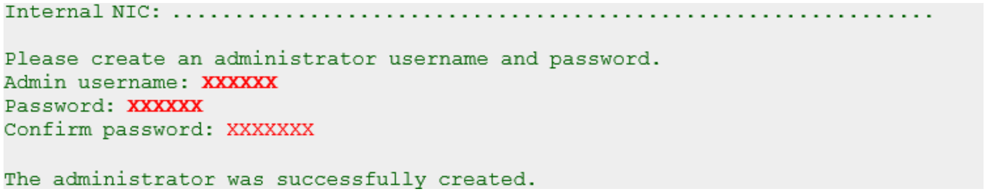
```
Please provide ethernet configuration information
  IP address:      10.30.1.6
  Network mask:    255.255.255.0
  Default gateway: 10.30.1.1
Please provide DNS nameserver information:
  Primary DNS server:   10.30.1.7
  Secondary (optional):
  DNS domain(s):     EMS1.HPITEST.COM
Please provide Microsoft WINS server information:
  WINS server (optional):
```

2. Confirm if all the settings are correct, and then type "*y*".



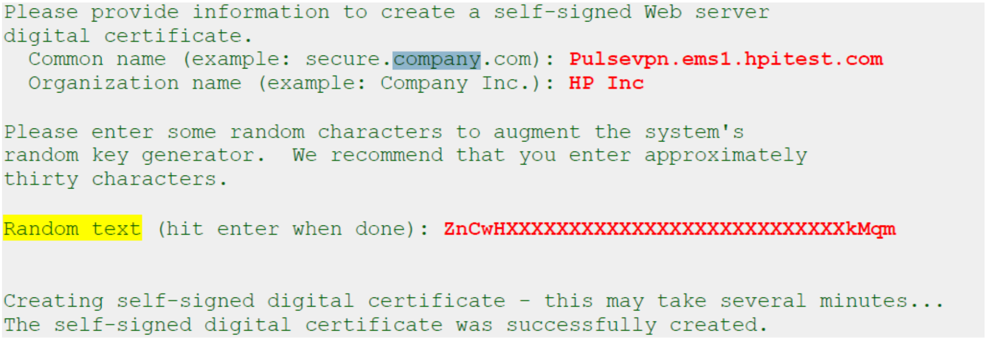
```
Please confirm the following setup:
  IP address:          10.30.1.6
  Network mask:        255.255.255.0
  Gateway IP:          10.30.1.1
  Link speed:          Auto
  Primary DNS server: 10.30.1.7
  Secondary DNS:
  DNS domain(s):      EMS1.HPITEST.COM
  WINS server:
Correct? (y/n): y
Initial network configuration complete.
```

3. Create a root username and password: Type an administrator username, password, and then type the password again to confirm it.

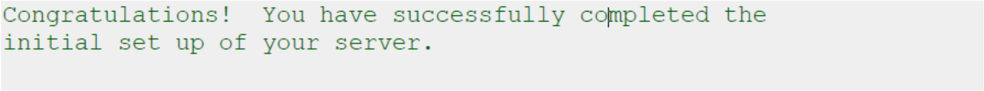


```
Internal NIC: .............................................................

Please create an administrator username and password.
Admin username: XXXXXX
Password: XXXXXX
Confirm password: XXXXXXX

The administrator was successfully created.
```

4. Set up a self-signed SSL certificate. Type a random text of 30 characters.



```
Please provide information to create a self-signed Web server
digital certificate.
  Common name (example: secure.company.com): Pulsevpn.ems1.hpitest.com
  Organization name (example: Company Inc.): HP Inc

Please enter some random characters to augment the system's
random key generator.  We recommend that you enter approximately
thirty characters.

Random text (hit enter when done): ZnCwHXXXXXXXXXXXXXXXXXXXXXXXXXXXXkMqm


Creating self-signed digital certificate - this may take several minutes...
The self-signed digital certificate was successfully created.
```



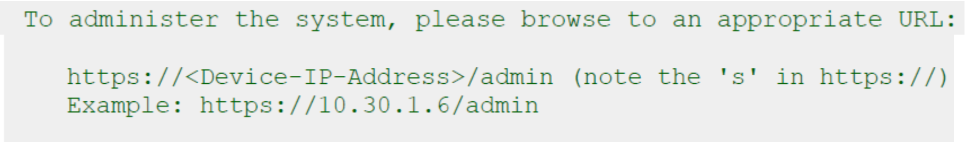
```
Congratulations!  You have successfully completed the
initial set up of your server.
```

Connect and configure the Pulse Connect Secure web interface

This section provides instructions on how to configure specific role settings on the Pulse server.

Follow these steps to connect to Pulse Connect Secure interface:

1. Open a web browser and type the IP address used for configuring the serial console network, and then press **Enter**. The url should be in the following format:
   https://< the IP address used for configuring the network>/admin
   Example: https://10.30.1.6/admin

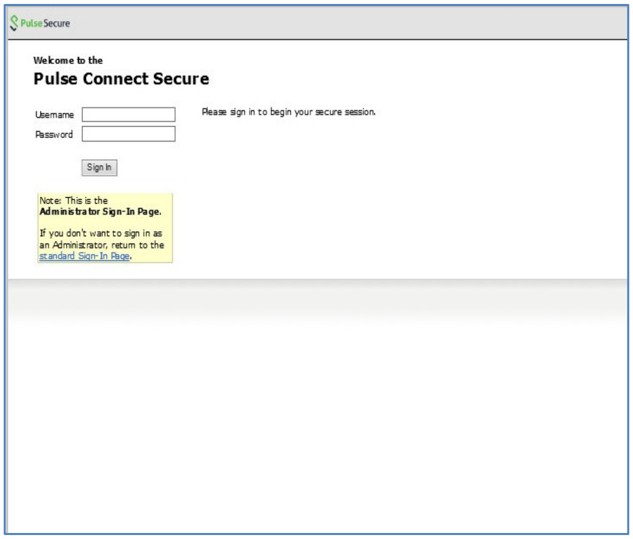


```
To administer the system, please browse to an appropriate URL:

   https://<Device-IP-Address>/admin (note the 's' in https://)
   Example: https://10.30.1.6/admin
```

2. On the login page, type your administrative username, password, and then click **Sign In**.

Note
After you login the main Systems Status page displays.

Figure 2. Login Page



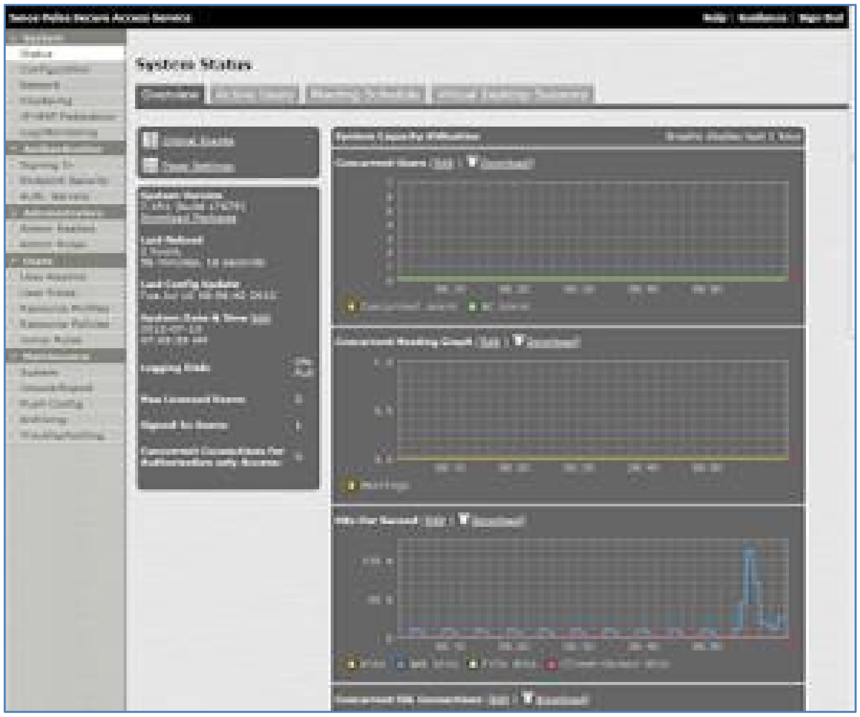
Welcome to the
Pulse Connect Secure

Please sign in to begin your secure session.

Note: This is the **Administrator Sign-In Page.**

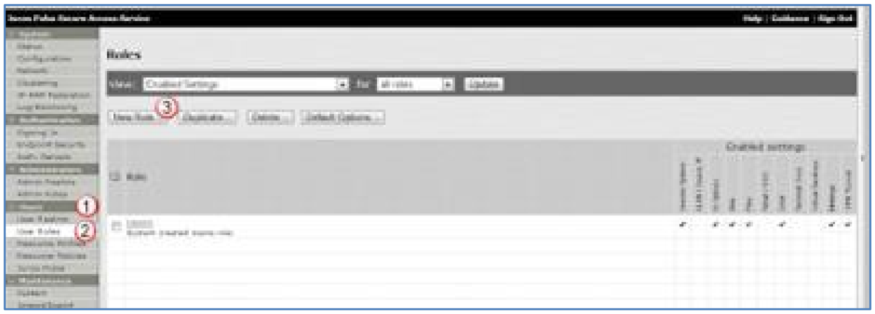
If you don't want to sign in as an Administrator, return to the standard Sign-In Page.

Figure 3. System Status



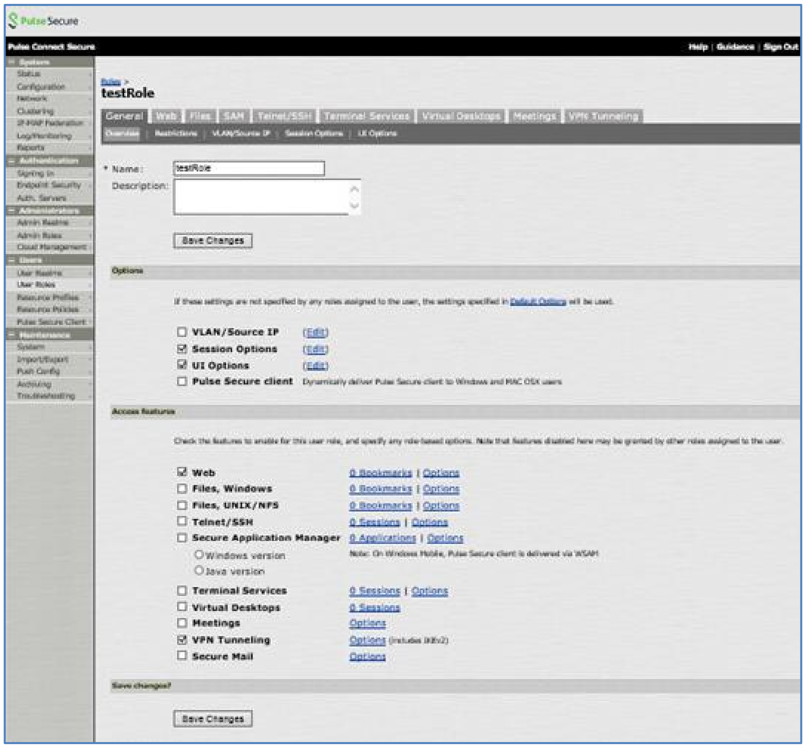
3. On the **System Status** page, in the left pane, under the **Users** (1) section, select **User Roles** (2).
4. In the **Roles** page, click the **New Role** (3) button.

Figure 4. Roles



5. In the **New Role** page, in the **Name** text box type *testRole* and then click **Save Changes** to save the changes.

Figure 5. testRole



testRole

* Name: testRole

Description:

Options

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

☐ VLAN/Source IP (Edit)
☑ Session Options (Edit)
☑ UI Options (Edit)
☐ Pulse Secure client Dynamically deliver Pulse Secure client to Windows and MAC OSX users

Access features

Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by other roles assigned to the user.

☑ Web 0 Bookmarks | Options
☐ Files, Windows 0 Bookmarks | Options
☐ Files, UNIX/NFS 0 Bookmarks | Options
☐ Telnet/SSH 0 Sessions | Options
☐ Secure Application Manager 0 Applications | Options
○ Windows version Note: On Windows Mobile, Pulse Secure client is delivered via WSAM
○ Java version
☐ Terminal Services 0 Sessions | Options
☐ Virtual Desktops 0 Sessions
☐ Meetings Options
☑ VPN Tunneling Options (includes IKEv2)
☐ Secure Mail Options

Save changes?

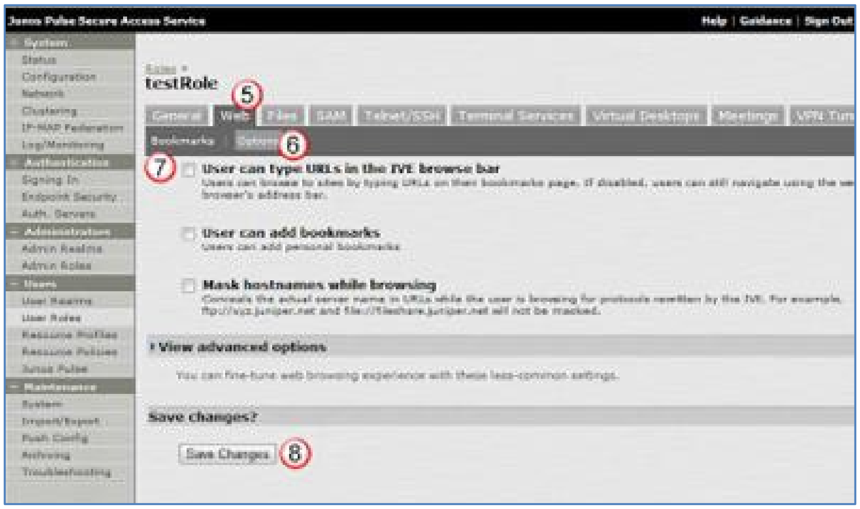
6. In the **Access features** section, select the **Web** check box, and then click the **Save Changes** button to save the changes. This enables web servicing from the MAG and **VPN Tunneling** to enable VPN.

7. Next to the **Web** features check box, select the **Options** link.

8. In the **testRole** page, select the **Web** tab (5), and then select the **Options** sub tab (6).

9. Select the **User can type URLs in the IVE browse bar** check box (7) and then click the **Save Changes** button (8).

Figure 6. Web tab in testRole page



testRole

☐ User can type URLs in the IVE browse bar
Users can browse to sites by typing URLs on their bookmarks page. If disabled, users can still navigate using the we
browser's address bar.

☐ User can add bookmarks
Users can add personal bookmarks

☐ Mask hostnames while browsing
Conceals the actual server name in URLs while the user is browsing for protocols rewritten by the IVE. For example,
ftp://xyz.juniper.net and file://fileshare.juniper.net will not be masked.

▸ View advanced options

You can fine-tune web browsing experience with these less-common settings.

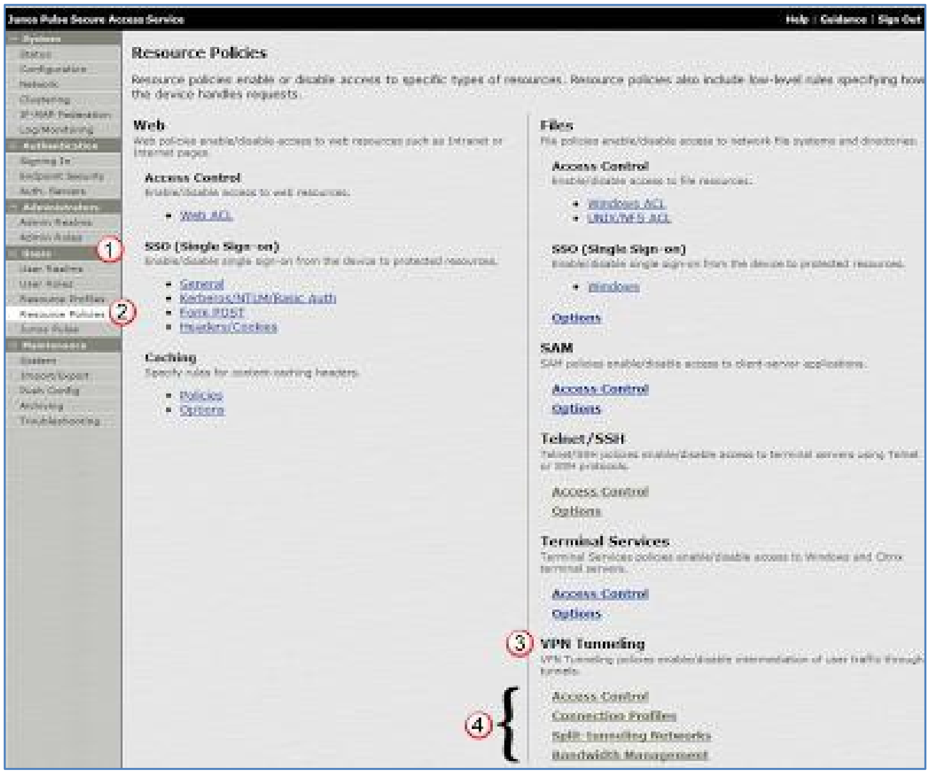
Save changes?

Create different VPN Resource Profiles

Follow these steps to create different VPN Resource Profiles:

1. In the left pane under the **Users** (1) section, select **Resource Policies** (2).
2. In the **Resources Policies** page, under **VPN Tunneling** (3), select **Access Control** (4).

Figure 7. Resource Policies page



Resource Policies

Resource policies enable or disable access to specific types of resources. Resource policies also include low-level rules specifying how the device handles requests.

Web

Web policies enable/disable access to web resources such as Intranet or Internet pages.

Access Control

Enable/disable access to web resources.

- Web ACL

SSO (Single Sign-on)

Enable/disable single sign-on from the device to protected resources.

- General
- Kerberos/NTLM/Basic Auth
- Form POST
- Headers/Cookies

Caching

Specify rules for custom caching headers.

- Policies
- Options

Files

File policies enable/disable access to network file systems and directories.

Access Control

Enable/disable access to file resources.

- Windows ACL
- UNIX/NFS ACL

SSO (Single Sign-on)

Enable/disable single sign-on from the device to protected resources.

- Windows

Options

SAM

SAM policies enable/disable access to client-server applications.

Access Control
Options

Telnet/SSH

Telnet/SSH policies enable/disable access to terminal servers using Telnet or SSH protocols.

Access Control
Options

Terminal Services

Terminal Services policies enable/disable access to Windows and Citrix terminal servers.

Access Control
Options

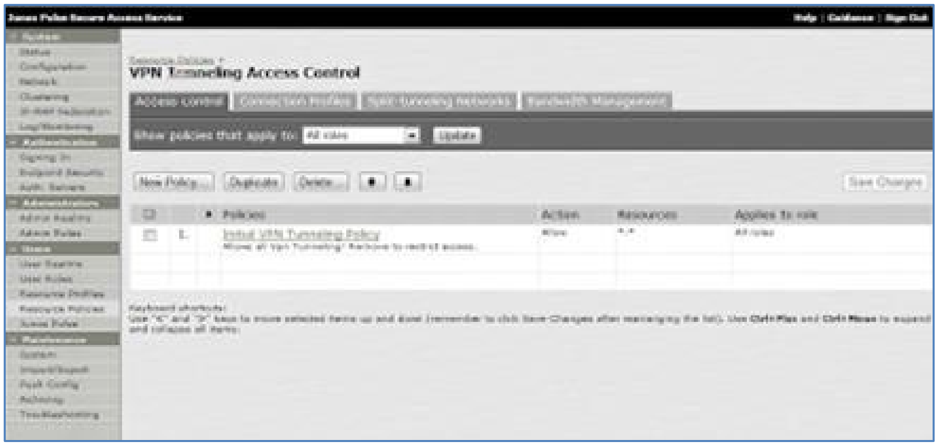
VPN Tunneling

VPN Tunneling policies enable/disable intermediation of user traffic through tunnels.

Access Control
Connection Profiles
Split-tunneling Networks
Bandwidth Management

3. On the **VPN Tunneling Access Control** page, select the **Access Control** tab, and then select the **New Policy** button.

Figure 8. VPN Tunneling Access Control



VPN Tunneling Access Control

Show policies that apply to: All roles

□		Policies	Action	Resources	Applies to role
□	1.	Initial VPN Tunneling Policy Allows all Vpn Tunneling' Remove to restrict access.	Allow	*.*	All roles

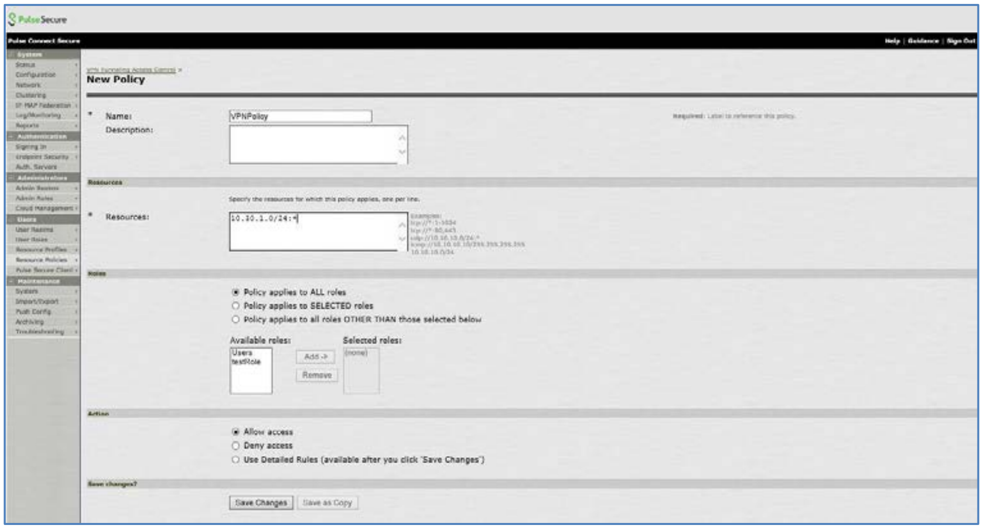
Keyboard shortcuts:
Use "<" and ">" keys to move selected items up and down (remember to click Save Changes after rearranging the list). Use Ctrl-Plus and Ctrl-Minus to expand and collapse all items.

4. In the **New Policy** page, complete the following sections:
   - **Name:** Type *VPN Policy*

- **Resources:** Type the IP address of the resources you want to access. For example, 10.30.1.0/24 :*
- **Roles:** Select **Policy applies to ALL roles**
- **Action:** Select the **Allow access** option.

Click **Save Changes** to save the new configuration.

Figure 9. New Policy



New Policy

* Name: VPNPolicy

Description:

Resources

Specify the resources for which this policy applies, one per line.

* Resources: 10.30.1.0/24:*

Roles

● Policy applies to ALL roles
○ Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Available roles: Users, testRole
Selected roles: (none)

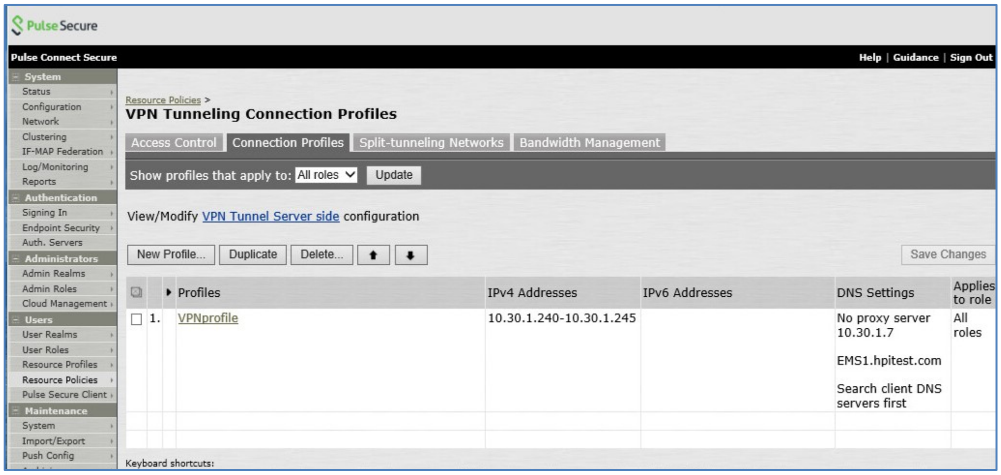
Action

● Allow access
○ Deny access
○ Use Detailed Rules (available after you click 'Save Changes')

Save changes?

5. Select the **Connection Profile** tab, and then select the **New Profile** button.

Figure 10. Connection Profile in the VPN Tunneling Access Control page



VPN Tunneling Connection Profiles

Show profiles that apply to: All roles

View/Modify VPN Tunnel Server side configuration

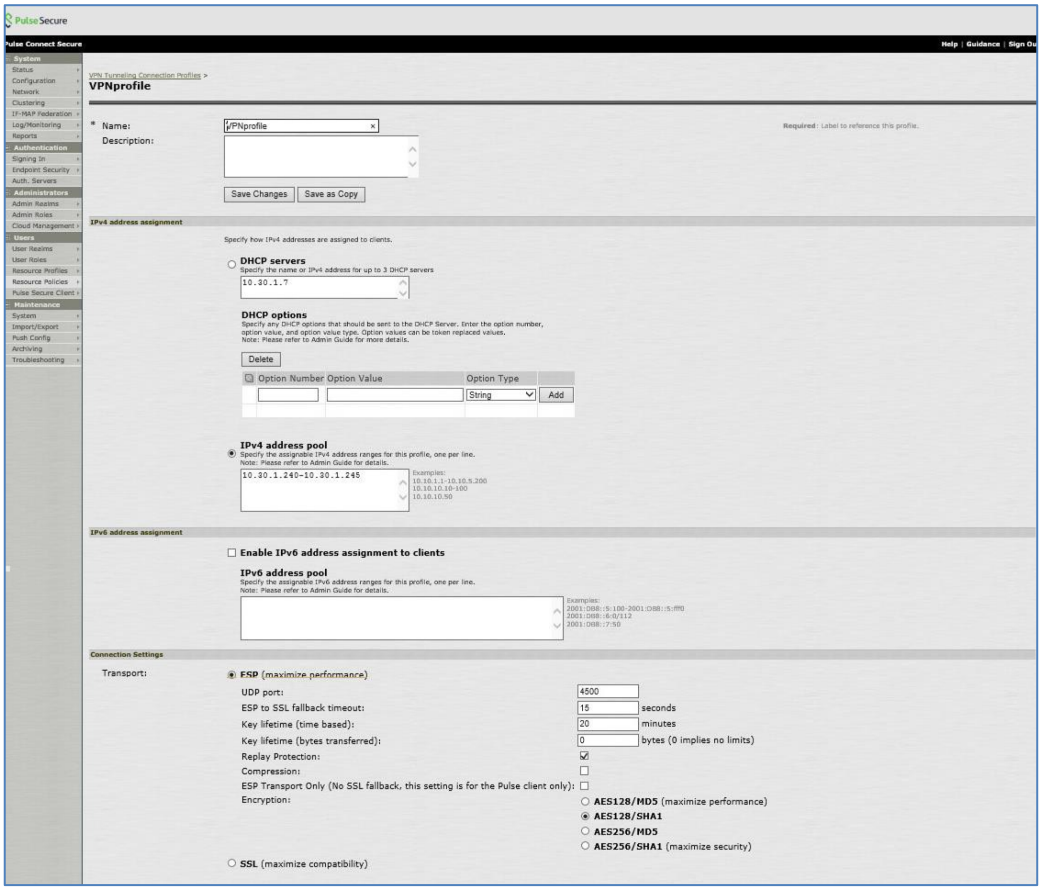
	Profiles	IPv4 Addresses	IPv6 Addresses	DNS Settings	Applies to role
□ 1.	VPNprofile	10.30.1.240-10.30.1.245		No proxy server 10.30.1.7 EMS1.hptest.com Search client DNS servers first	All roles

6. Complete the following sections to set the configuration:
   - **Name:** Type *VPNProfile*
   - **IPv4 Address Pool:** Type the IP range format that the internal Dynamic Host Configuration Protocol (DHCP) server will use for the new VPN clients.
     For example, 10.30.1.240-10.30.1.245
   - **DNS Settiings:** Select the **Manual DNS Settings** option and then provide the following settings:
     - **Primary DNS:** Type the IP address for the primary DNS. For example, 10.30.1.7
     - **DNS Domain:** Type the DNS Domain. For example, EMS1.hptest.com

- **Roles:** Select **Policy applies to ALL roles**

Click **Save Changes** to save the new configuration.

Figure 11. VPNprofile policy



VPNprofile

* Name: VPNprofile — **Required:** Label to reference this profile.

Description:

IPv4 address assignment

Specify how IPv4 addresses are assigned to clients.

○ **DHCP servers**
Specify the name or IPv4 address for up to 3 DHCP servers
10.30.1.7

DHCP options
Specify any DHCP options that should be sent to the DHCP Server. Enter the option number, option value, and option value type. Option values can be token replaced values.
Note: Please refer to Admin Guide for more details.

☐	Option Number	Option Value	Option Type	
			String	Add

● **IPv4 address pool**
Specify the assignable IPv4 address ranges for this profile, one per line.
Note: Please refer to Admin Guide for details.
10.30.1.240-10.30.1.245

Examples:
10.10.1.1-10.10.5.200
10.10.10.10-100
10.10.10.50

IPv6 address assignment

☐ **Enable IPv6 address assignment to clients**

IPv6 address pool
Specify the assignable IPv6 address ranges for this profile, one per line.
Note: Please refer to Admin Guide for details.

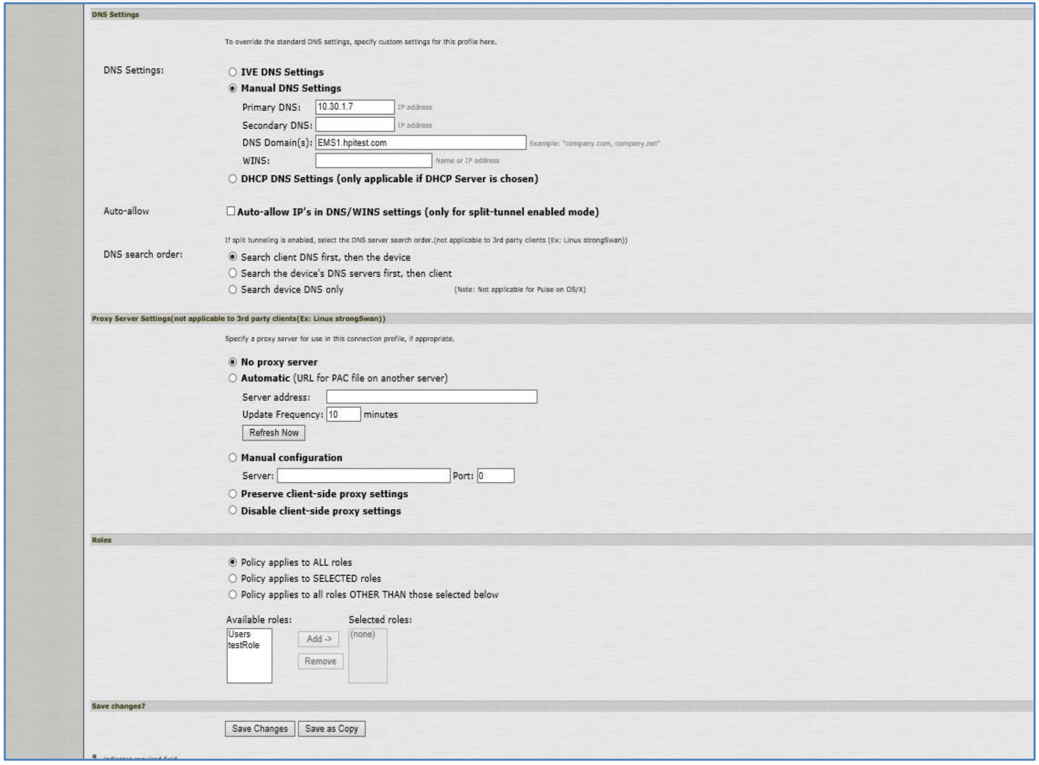
Examples:
2001:DB8::5:100-2001:DB8::5:fff0
2001:DB8::6:0/112
2001:DB8::7:50

Connection Settings

Transport: ● **ESP** (maximize performance)

UDP port:	4500	
ESP to SSL fallback timeout:	15	seconds
Key lifetime (time based):	20	minutes
Key lifetime (bytes transferred):	0	bytes (0 implies no limits)
Replay Protection:	☑	
Compression:	☐	
ESP Transport Only (No SSL fallback, this setting is for the Pulse client only):	☐	
Encryption:	○ **AES128/MD5** (maximize performance) ● **AES128/SHA1** ○ **AES256/MD5** ○ **AES256/SHA1** (maximize security)	

○ **SSL** (maximize compatibility)



DNS Settings

To override the standard DNS settings, specify custom settings for this profile here.

DNS Settings:
○ **IVE DNS Settings**
● **Manual DNS Settings**
Primary DNS: 10.30.1.7 IP address
Secondary DNS: IP address
DNS Domain(s): EMS1.hpitest.com Example: "company.com, company.net"
WINS: Name or IP address
○ **DHCP DNS Settings (only applicable if DHCP Server is chosen)**

Auto-allow ☐ **Auto-allow IP's in DNS/WINS settings (only for split-tunnel enabled mode)**

If split tunneling is enabled, select the DNS server search order.(not applicable to 3rd party clients (Ex: Linux strongSwan))

DNS search order:
● Search client DNS first, then the device
○ Search the device's DNS servers first, then client
○ Search device DNS only (Note: Not applicable for Pulse on OS/X)

Proxy Server Settings(not applicable to 3rd party clients(Ex: Linux strongSwan))

Specify a proxy server for use in this connection profile, if appropriate.

● **No proxy server**
○ **Automatic** (URL for PAC file on another server)
Server address:
Update Frequency: 10 minutes
○ **Manual configuration**
Server: Port: 0
○ **Preserve client-side proxy settings**
○ **Disable client-side proxy settings**

Roles

● Policy applies to ALL roles
○ Policy applies to SELECTED roles
○ Policy applies to all roles OTHER THAN those selected below

Available roles:
Users
testRole

Selected roles:
(none)

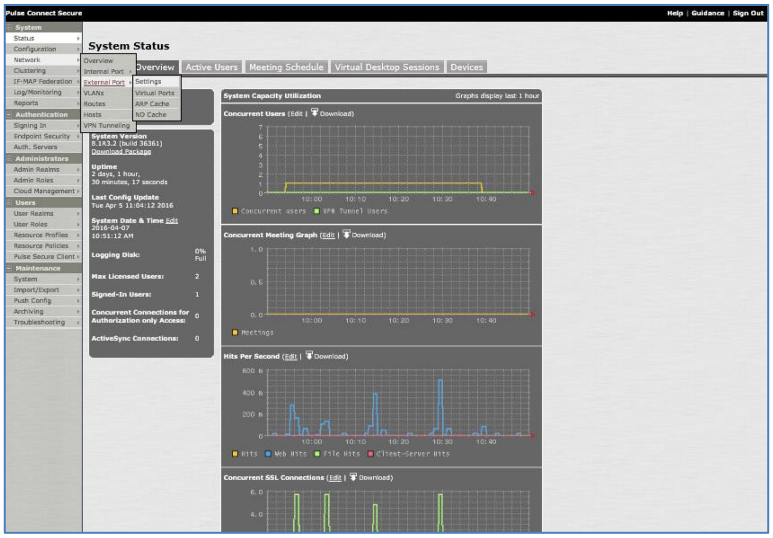
Save changes?

Configure the external port

Follow these steps to enable the external port:

1. On the **System Status** page, in the left pane, select **Network**, and then click the **External Port** tab.

Figure 12. External Port



System Status

System Version
8.1R3.2 (build 36361)
Download Package

Uptime
2 days, 1 hour,
30 minutes, 17 seconds

Last Config Update
Tue Apr 5 11:04:12 2016

System Date & Time Edit
2016-04-07
10:51:12 AM

Logging Disk: 0% Full

Max Licensed Users: 2

Signed-In Users: 1

Concurrent Connections for Authorization only Access: 0

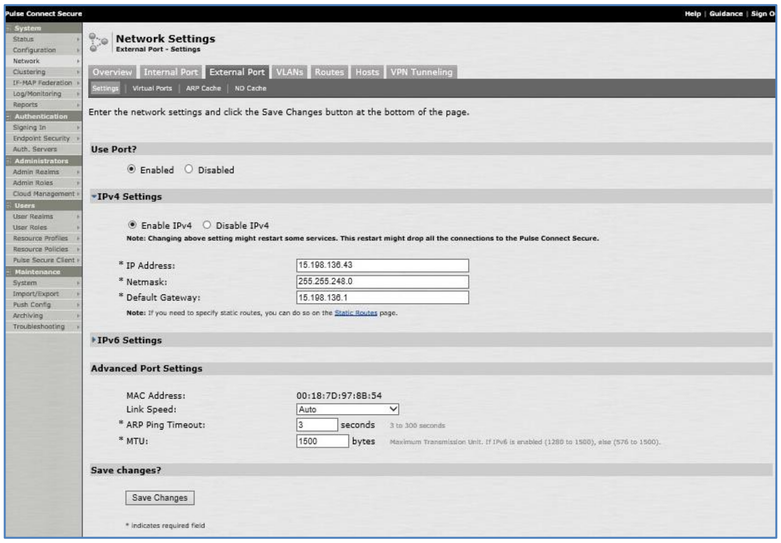
ActiveSync Connections: 0

2. On the **Network Settings** page, in the **Use Port?** section, select the **Enabled** option.

3. Complete the **IPv4 Settings** section.

4. Click **Save Changes** to save the configuration.

Figure 13. Network Settings



Network Settings
External Port - Settings

Enter the network settings and click the Save Changes button at the bottom of the page.

Use Port?

● Enabled ○ Disabled

IPv4 Settings

● Enable IPv4 ○ Disable IPv4

Note: Changing above setting might restart some services. This restart might drop all the connections to the Pulse Connect Secure.

* IP Address: 15.198.136.43
* Netmask: 255.255.248.0
* Default Gateway: 15.198.136.1

Note: If you need to specify static routes, you can do so on the Static Routes page.

IPv6 Settings

Advanced Port Settings

MAC Address: 00:18:7D:97:8B:54
Link Speed: Auto
* ARP Ping Timeout: 3 seconds 3 to 300 seconds
* MTU: 1500 bytes Maximum Transmission Unit. If IPv6 is enabled (1280 to 1500), else (576 to 1500).

Save changes?

* indicates required field