Pulse Secure Desktop Client Configuration on Pulse Policy Secure

Supporting Pulse Secure Desktop Client 9.1R9

Product Release	**9.1R9**
Published	**October 2020**
Document Version	**1.0**

Pulse Secure, LLC
2700 Zanker Road,
Suite 200 San Jose
CA 95134

www.pulsesecure.net

END USER LICENSE AGREEMENT

Contents

Preface

Document conventions

The document conventions describe text formatting conventions, command syntax conventions, and important notice formats used in Pulse Secure technical documentation.

Text formatting conventions

Text formatting conventions such as boldface, italic, or Courier font may be used in the flow of the text to highlight specific words or phrases.

Format	Description
bold text	Identifies command names
	Identifies keywords and operands
	Identifies the names of user-manipulated GUI elements
	Identifies text to enter at the GUI
italic text	Identifies emphasis
	Identifies variables
	Identifies document titles
`Courier Font`	Identifies command output
	Identifies command syntax examples

Command syntax conventions

Bold and italic text identify command syntax components. Delimiters and operators define groupings of parameters and their logical relationships.

Convention	Description
bold text	Identifies command names, keywords, and command options.
italic text	Identifies a variable.
[ ]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.

Convention	Description
{ **x** | **y** | **z** }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x | **y**	A vertical bar separates mutually exclusive elements.
< >	Non-printing characters, for example, passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, member[member...].
\	Indicates a "soft" line break in command examples. If a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.
bold text	Identifies command names, keywords, and command options.

Notes and Warnings

Note, Attention, and Caution statements might be used in this document.

Note: A Note provides a tip, guidance, or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates a stronger note, for example, to alert you when traffic might be interrupted or the device might reboot.

CAUTION
A Caution statement alerts you to situations that can be potentially hazardous to you or cause damage to hardware, firmware, software, or data.

Requesting Technical Support

Technical product support is available through the Pulse Secure Global Support Center (PSGSC). If you have a support contract, file a ticket with PSGSC.

- Product warranties—For product warranty information, visit https://support.pulsesecure.net/product-service-policies/

Self-Help Online Tools and Resources

For quick and easy problem resolution, Pulse Secure provides an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://support.pulsesecure.net
- Search for known bugs: https://support.pulsesecure.net
- Find product documentation: https://www.pulsesecure.net/techpubs
- Download the latest versions of software and review release notes: https://support.pulsesecure.net

- Open a case online in the CSC Case Management tool: https://support.pulsesecure.net
- To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://support.pulsesecure.net

For important product notices, technical articles, and to ask advice:

- Search the Pulse Secure Knowledge Center for technical bulletins and security advisories: https://kb.pulsesecure.net
- Ask questions and find solutions at the Pulse Community online forum: https://community.pulsesecure.net

Opening a Case with PSGSC

You can open a case with PSGSC on the Web or by telephone.

- Use the Case Management tool in the PSGSC at https://support.pulsesecure.net.
- Call 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see https://support.pulsesecure.net/support/support-contacts/

Reporting Documentation Issues

To report any errors or inaccuracies in Pulse Secure technical documentation, or to make suggestions for future improvement, contact Pulse Secure Technical Support (https://support.pulsesecure.net). Include a full description of your issue or suggestion and the document(s) to which it relates.

Configuring Pulse Policy Secure

This chapter contains the following sections:

Before You Begin

Before you begin configuring Pulse Secure Desktop Client (Pulse Client), be sure you have already configured your device network settings. Also be sure that you have defined the authentication settings, including the authentication servers and sign-in settings. Authentication Host Checker settings can directly affect a Pulse Client installation because you can define the conditions that an endpoint must meet to be allowed access to protected resources.

Pulse Policy Secure Overview

To enable Pulse Clients to connect to Pulse Policy Secure, you configure the service so that when users request authentication, they are assigned a role based on the role mappings and optional security profile that you create. Access to specific resources is permitted only for users and devices that provide the proper credentials for the realm, that are associated with the appropriate roles, and whose endpoints meet security restrictions. If a user attempts to connect to the network from an endpoint that does not comply with the security restrictions you have defined, the user cannot access the realm or role.

As you plan your configuration, be sure you know how you want to deploy Pulse Client. You can use one or more of the following Pulse Client deployment options:

- Use the defaults or make changes to the Pulse Client default component set and default connection set, and then download and distribute Pulse Client by having users log in to the Pulse Secure server's user Web portal. After the installation is complete, users have all the connections they need to access network resources.
- Create the connections that an endpoint needs for connectivity and services, download the settings file (.pulsepreconfig), and download default Pulse Client installation program. For Windows endpoints you run the Pulse Client installation program by using an msiexec command with the settings file as an option. For OS X endpoints, you run the default installer and then import the pulsepreconfig file using a separate command.
- Distribute Pulse Client with no preconfiguration. You can download the default Pulse Client installation file, and then distribute the file to endpoints using your organization's standard software distribution methods. Because the installer does not contain preconfigured connections, users must define network connections manually. Users can also automatically download a Pulse Secure server's dynamic connection by browsing to and logging into the Pulse Secure server's Web portal. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Secure server and launches Pulse Client from the server's Web interface.

Pulse Policy Secure and Pulse Connect Secure Deployment Options

For Pulse Policy Secure and Pulse Connect Secure, you can deploy all of the connections required for Windows and macOS clients to connect to any Pulse Secure server.

Note: Pulse Secure Client for Mobile Devices is distributed through the app stores.

Pulse Policy Secure and Pulse Connect Secure support the following deployment options:

- **Web install**: Create all of the settings that a Windows or macOS endpoint needs for connectivity and services, and install the software on endpoints that connect to the Pulse Secure server's Web portal. Pulse Secure servers include a default client connection set and client component set. The default settings enable you to deploy Pulse Client to users without creating new connection sets or component sets. The default settings for the client permit dynamic connections and install only the components required for the connection.
- **Default installer**: A default Pulse Client installer package (in .msi format for Windows and .dmg for macOS) is included in the Pulse Secure server software. You can distribute this default installer to endpoints, run it, and then let users create their own connections or have users browse to the Pulse Secure server and authenticate though the server's Web portal to receive the initial configuration and bind the client to the server for future configuration updates. Users can automatically install connections to other Pulse Secure servers (if Pulse Client's configuration allows dynamic connections) by browsing to the user Web portal of a Pulse Secure server where a dynamic connection has been made available. A dynamic connection is a predefined set of connection parameters that enables a client to connect to the host server. If the user is able to log in to the Pulse Secure server's user Web portal and start Pulse Client from the Web interface, the connection parameters are downloaded and installed on Pulse Client. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Secure server and launches Pulse Client from the server's Web interface.
- **Preconfigured installer**: Create the connections that an endpoint needs for connectivity and services, download the settings file (.pulsepreconfig), and download default Pulse Client installation program. For Windows endpoints you run the Pulse Client installation program by using an msiexec command with the settings file as an option. For OS X endpoints, you run the default installer and then import the. pulsepreconfig file using a separate command.

Note: Pulse Secure Client for Mobile Devices uses a different deployment model than Pulse Client for Windows and Pulse Client for Mac endpoints.

SRX Series Gateway Deployment Options

Windows and macOS endpoints can use Pulse Client software to connect to SRX Series gateways that are running a Junos OS release between v10.2 and v12.3, and that have dynamic VPN access enabled and configured. For SRX Series devices running Junos OS Release 10.2 through 10.4, Pulse Client is supported but must be deployed separately. You can download the Pulse Client installer from a Pulse Secure server or the *Pulse Client Licensing and Download Center* in the Pulse Secure Support Portal (my.pulsesecure.net), and install it using local distribution methods such as SMS/SCCM. By using preconfiguration file, you can add preconfigured connections when you install Pulse Client. After installing Pulse Client for Windows or Pulse Client for OS X, users can also create a connection to an SRX gateway. In Junos OS Release 11.1 and later, if Pulse Client does not exist on the client machine, Pulse Client is automatically downloaded and installed when you log into an SRX Series device.

Note: Pulse Client Dynamic VPN functionality is compatible with SRX-Branch (SRX100-SRX650) devices only. SRX-HE (SRX1400-SRX5800 - also called SRX Data Canter) devices do not support Pulse Client Dynamic VPN from either Windows or Mac clients.

Configuring a Role for Pulse Policy Secure

A user role defines session settings and options, personalization settings (user interface customization and bookmarks), and enabled access features (Web, file, application, Telnet/SSH, Terminal Services, network, meeting, and e-mail access). A user role does not specify resource access control or other resource-based options for an individual request. For example, a user role can define whether or not a user can perform Web browsing. However, the individual Web resources that a user may access are defined by the Web resource policies that you configure separately.

To configure a role for Pulse Client endpoints:

1. From the admin console, select **Users > User Roles > New User Role**.
2. Enter a name for the role and, optionally, a description.
3. Click Save Changes. The role configuration tabs appear.
4. Set the following options:

   General > Overview

   - **Options**: Select the "Pulse Secure" check box.

   General > Restrictions

   - **Source IP**: Source IP options allow you to make an assignment to this role dependent on the endpoint's IP address or IP address range. To enable source IP address restrictions, select **Allow or deny users from the following IP addresses**, and then add IP addresses or address ranges. Select **Allow** to allow users to sign in from the specified IP address, or **Deny** to prevent users from signing in from the specified IP address. Then click **Add**. When you are finished making changes, click **Save Changes**.
   - If you add multiple IP addresses, move the highest priority restrictions to the top of the list by selecting the check box next to the IP address, and then clicking the up arrow button. For example, to deny access to all users on a wireless network (10.64.4.100) and allow access to all other network users (0.0.0.0), move the wireless network address (10.64.4.100) to the top of the list and move the (0.0.0.0) network below the wireless network.
   - **Browser**: Browser options allow you to enforce the use of a particular type of browser for Web access to Pulse Policy Secure. Browser options apply only to operations that involve accessing Pulse Policy Secure through its user Web portal, such as acquiring a dynamic connection or installing Pulse Client through a role. Normal connection operations between Pulse Client and Pulse Secure server are not affected by browser restrictions.
   - **Certificate**: Certificate options allow you to require users to sign in from an endpoint that possesses the specified client-side certificate from the proper certificate authority. Before you enable this option, be sure that you have configured the client-side certificate on the Trusted Client CAs page of the admin console.
   - **Host Checker**: Host Checker options allow you to enable Host Checker polices, to choose one or more policies for the role, and specify whether the endpoint must meet all or just one of the selected Host Checker policies. The Host Checker policies that appear as Available Policies must be previously defined as part of the Endpoint Security settings in the Authentication section of the admin console.

   General > Session Options

- **Session lifetime**: Session lifetime options allow you to set timeout values for user sessions. You can change the defaults for the following:
  - **Max. Session Length**: Specify the number of minutes a user session might remain open before ending. During a user session, prior to the expiration of the maximum session length, Pulse Client prompts the user to re-enter authentication credentials, which avoids the problem of terminating the user session without warning.
  - **Heartbeat Interval**: Specify the frequency at which Pulse Client should notify Pulse Connect Secure to keep the session alive. You should ensure that the heartbeat interval of the agent is greater than the Host Checker interval, otherwise performance could be affected. In general, the heartbeat interval should be set to at least 50% more than the Host Checker interval.
  - **Heartbeat Timeout**: Specify the amount of time that Pulse Connect Secure should wait before terminating a session when the endpoint does not send a heartbeat response.
  - **Auth Table Timeout**: Specify a timeout value for the auth table entry to be provisioned as needed. Based on user identity and endpoint status, Pulse Policy Secure assigns the user a set of roles that specify which resources the user can access. The Pulse Secure server pushes the roles associated with each endpoint's source IP address (called auth table entries) to the Infranet Enforcer. The Infranet Enforcer allows traffic between the endpoint and the protected resources based on resource access policies.
  - **Reminder Time**: When the Enable Session Extension feature is enabled, the Reminder Time specifies the number of minutes prior to a session end when the server sends a notice through Pulse Client and notifies the user that the session will end soon.
  - **Use Session/Idle timeout values sent by the primary Radius authentication Server**: The session takes its timeout values from the Radius server Idle-timeout setting.
  - **Enable Session Extension**: You can select the Enable Session Extension check box to allow Pulse Client users to continue a session beyond the maximum session length. If this feature is enabled, users can extend a session through the Pulse Client user interface.
  - **Allow VPN Through Firewall**: Enable this option to allow Infranet Enforcer traffic to act as a heartbeat and keep the session alive.
- **Roaming session**: Roaming allows user sessions to work across source IP addresses. Roaming session options include the following:
  - **Enabled**: Select this option to enable roaming for users mapped to this role. A roaming user session works across source IP addresses, which allows mobile users with dynamic IP addresses to sign in to Pulse Connect Secure from one location and continue working from other locations.
  - **Limit to subnet**: Select this option to limit the roaming session to the local subnet specified in the Netmask box. Users can sign in from one IP address and continue using their sessions with another IP address as long as the new IP address is within the same subnet.
  - **Disabled**: Select this option to disable roaming user sessions for users mapped to this role. Users who sign in from one IP address cannot continue an active Infranet Controller session from another IP address; user sessions are tied to the initial source IP address.

General > UI Options

- The UI options allow you to define options that a user sees after a successful login to the Pulse Policy Secure server by means of a browser.

5. Select the **Agent** tab. The agent is the client program for a user assigned to this role. When a user connects to the system using a Web browser, the user can click a button to download and install the selected agent if it is not already installed on the user's endpoint. Configure the following options.
   - Select **Install Agent** for this role.

     Agent options appear only after you select this check box.
   - Select **Install Pulse Secure**.
6. In the "Session scripts" area, optionally specify a location for the following:

- **Windows: Session start script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client connects with Pulse Policy Secure. For example, you can specify a script that maps network drives on an endpoint to shares on protected resources. The script must be in a location (either local or on the network) that is accessible by the user.
- **Windows: Session end script**: Specify a script (.bat, .cmd, or .exe) to run for users assigned to the role after Pulse Client disconnects from Pulse Policy Secure. For example, you can specify a script that disconnects mapped network drives. If there is no start script defined, or the start script has not been run, the end script does not run. The script must be in a location (either local or on the network) that is accessible by the user.

7. Click **Save Changes**, and then select **Agent > Pulse Secure Settings**.
8. Select a component set that you have created, use the Default component set or select "none". You would select "none" only if you are creating this role to distribute new or updated connections to existing Pulse Client users.
9. Click **Save Changes**.
10. Select **Users > User Realms > Select Realm > Role Mapping > New Rule** to configure role mapping rules that map Pulse Client users to the role you configured.

Related Documentation

- "Pulse Policy Secure Overview"
- "Endpoint Security Monitoring and Management for Pulse Policy Secure"

Pulse Client Connection Set Options for Pulse Policy Secure

A Pulse Client connection set contains network options and allows you to configure specific connection policies for client access to any Pulse Secure server that supports Pulse Client. The following sections describe each of the configuration options for a Pulse Client connection set.

Pulse Client Connection Set Options

The following items apply to all connections in a connection set.

- **Allow saving logon information**: Controls whether the Save Settings check box is available in login dialog boxes in Pulse Client. If you clear this check box, Pulse Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.

Pulse Client can retain learned user settings. These settings are retained securely on the endpoint, evolving as the user connects through different Pulse Secure servers. Pulse Client can save the following settings:

- Certificate acceptance
- Certificate selection
- Realm
- Username and password
- Proxy username and password
- Secondary username and password
- Role

Note: If the authentication server is an ACE server or a RADIUS server and authentication is set to Users authenticate using tokens or one-time passwords, Pulse Client ignores the **Allow saving logon information** option. If the user sees a username and token prompt and the Save settings check box is disabled. Pulse Client supports soft token, hard token, and smart card authentication.

When a user opts to save settings, that information is used for each subsequent connection without prompting. If a setting changes (for example, if a user changes a password), the saved setting is invalid and connection attempts fail. In this case, the user must use the client's Forget Saved Settings feature, which clears all user-saved settings.

- **Allow user connections**: Controls whether connections can be added by the user.
- **Display splash screen**: Clear this check box to hide the Pulse Client splash screen that normally appears when Pulse Client starts.
- **Dynamic certificate trust**: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse Secure server.

  Note: By default, Dynamic certificate trust check box will be unchecked.
- **Dynamic connections**: Allows connections within this connection set to be automatically updated or added to a Pulse Client when the user connects to the Pulse Secure server through the user Web portal, and then clicks the Pulse Secure button. Dynamic connections are created as manual rather than automatic connections, which means that they are run only when the user initiates the connection or the user browses to a Pulse Secure server and launches Pulse Client from the server's Web interface.

  If dynamic connections are disabled, and the user logs in through the Web portal of a Pulse Secure server that is not already included in Pulse Client's connection set, then starting Pulse Client from the Web portal does not add a new Pulse Client connection for that Pulse Secure server. If you choose to disable dynamic connections, you can still allow users to manually create connections by enabling **Allow User Connections**.
- **FIPS mode enabled**: Enable FIPS mode communications for all Pulse Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse Client connection is operating in FIPS mode, "FIPS On" appears in the lower corner of the Pulse Client interface. If the Pulse Secure server hardware does not support

FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

Note: Users cannot enable FIPS mode from within Pulse Client. You must create FIPS-enabled connections on the server and deploy them.

- **Wireless suppression**: Disables wireless access when a wired connection is available. If the wired connection is removed, Pulse Client enables the wireless connections with the following properties:
  - Connect even if the network is not broadcasting.
  - Authenticate as computer when computer information is available.
  - Connect when this network is in range.

Note: Wireless suppression occurs only when the wired connection is connected and authorized. If you enable wireless suppression, be sure to also configure a connection that enables the client to connect through a wired connection.

UAC 802.1X Connection Type Options

Use this connection type to define authenticated connectivity to 802.1X devices, wired or wireless. Users cannot create 802.1X connections from the Pulse Client interface. Users see 802.1X connections in the Pulse Client interface only when the connection has been deployed from the server and the specified network is available.

Note: When configuring an 802.1x connection, Pulse Policy Secure will force Pulse Client to connect using Client IP Address of the same family as of the specified Radius Client's IP Family. When you specify Radius Client as IPV6, Pulse Policy Secure will allow Pulse Client to connect only using IPv6 address in 802.1x scenario. Also Pulse Client does not consider link-local IPv6 Addresses to complete an 802.1x Connection in a scenario where it needs an IPv6 address to connect to Pulse Policy Secure. For more information see PPS Admin Guide.

- **Adapter type**: Specifies the type of adapter to use for authentication: wired or wireless.
- **Outer username**: Enables a user to appear to log in anonymously while passing the actual login name (called the inner identity) through an encrypted tunnel. As a result, the user's credentials are secure from eavesdropping, and the user's inner identity is protected. In general, enter “anonymous”, which is the default value. In some cases, you might need to add additional text. For example, if the outer identity is used to route the user's authentication to the proper server, you might be required to use a format such as “anonymous@acme.com”.

Note: If you leave the box blank, the client passes the users or the machine's Windows login name as the outer identity.

- **Scan list**: If you selected wireless as the adapter type, the scan list box is available to specify the SSIDs, including non-broadcast SSIDs, to connect to in priority order. If you leave the list empty, the user can connect to any available wireless network.
- **Support Non-broadcast SSID**: Allows a user to connect to a non-broadcast wireless network from within the Pulse Client interface. Selecting this field enables the following options:
  - **Wireless Security Algorithm**: Specify wireless authentication:

    - WPA
    - WPA2
- **Wireless Security Cipher**: Specify the type of encryption used by the non-broadcast network:
    - TKIP
    - AES

If the non-broadcast SSID options are configured, the Pulse Client connection configuration includes the values and they are used to configure the wireless profile on the endpoint.

Trusted Server List (for UAC 802.1X Connection)

FQDN criteria for 802.1X/EAP server certificates (with wildcard support) can be specified in the Trusted Server List of the PPS admin console. In the name field, you can enter a fully-qualified-domain name (FQDN) that can be either an exact FQDN or an FQDN that begins with a "." and/or can contain wildcards ("*").

Note the Following:

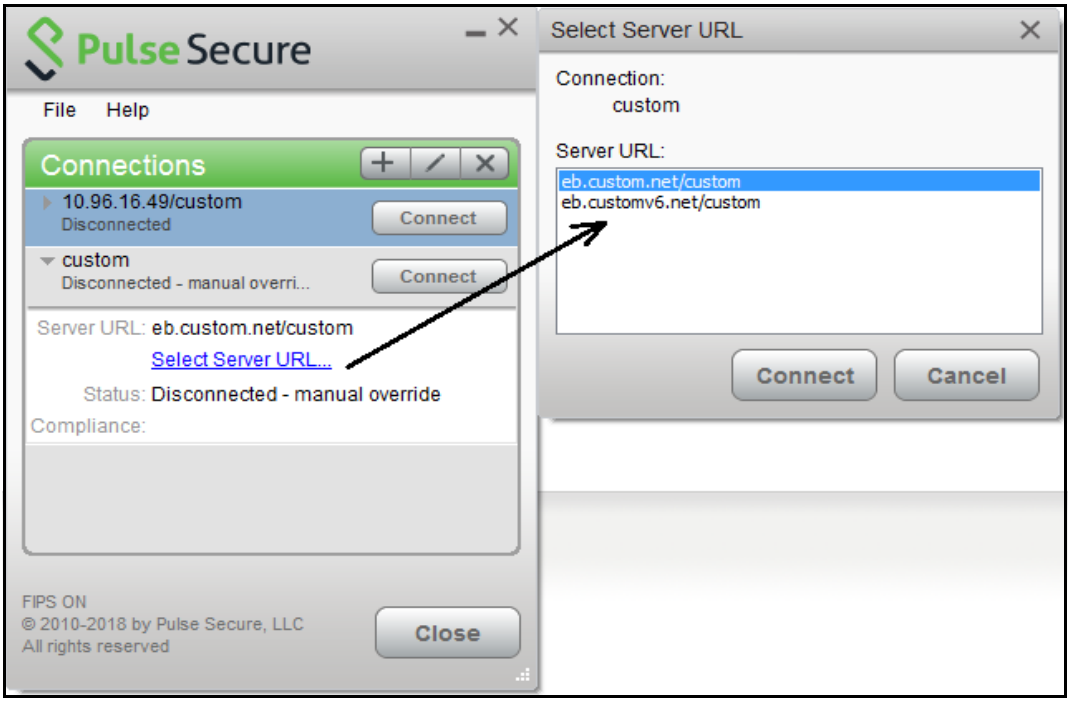
- The "ANY" entry matches any server certificate name.
- An entry that contains "=" requires an exact Subject:DN (Distinguished Name) match.
- An entry that is neither "ANY" nor contains "=" is an FQDN. It can be either an exact value or include wildcards and/or begin with a "." character. This value will be checked against FQDNs in the server's certificate (Subject:DN:CN=..., SAN:DNS=...).
    - An entry that begins with "." will wildcard only the first subdomain (domain component) in the FQDN. For example, " mycompany.com" will match "foo.mycompany.com" but not "foo.bar.mycompany.com". As such, a FQDN beginning with "." is equivalent to the same FQDN beginning with "." (e.g., ".mycompany.com" is equivalent to ".mycompany.com"). Note that this mechanism is more restrictive than what is described in RFC 5280.
    - FQDN may contain at most one wildcard per domain component (DC). For example, "a.mycompany.com" is not allowed and will always result in authentication failure.
    - A wildcard matches 1 or more characters (but not zero characters). For example, "f*r.mycompany.com" will match "foo-bar.mycompany.com" but not "fr.mycompany.com".
    - See RFC 2818 and RFC 6125 for more details and security implications of wildcards.
    - Be careful when mixing wildcard FQDN entries with certificates that contain wildcards in their names. For example, the entry "foo*.mycompany.com" will match a certificate with the name "*bar.mycompany.com".
    - This wildcarding mechanism does not work with server certificates that contain the "?" character in their names. (This is not a common occurrence.)
- You can choose any server certificate's issuing certificate authority (CA) from the drop-down list. It could be the direct issuer or any CA at higher level in the certificate chain, up to the root.

Connect Secure or Policy Secure (L3) Connection Type Options

Use a Connect Secure or Policy Secure (L3) connection for a Layer 3 connection to Pulse Connect Secure or Pulse Policy Secure.

- **Allow user to override connection policy**: Allows a user to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status, suspend/resume a connection to Pulse Connect Secure or shut down Pulse Client.
- **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**: This option must be selected if this connection is for Pulse Policy Secure. If the connection is for Pulse Connect Secure, you can disable this check box and use the connection for accessing Pulse Collaboration meetings only by also selecting Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection.
- **Enable Pulse Collaboration integration on this connection**: This option must be disabled if this connection is for Pulse Policy Secure. If the connection is for Pulse Connect Secure, you can enable this check box and use the connection for accessing Pulse Collaboration meetings.
- **Connect to URL of this server only**: Specifies whether the endpoint connects to this Pulse Secure server exclusively or if it can connect to the any of the servers listed in the list of connection URLs. Disable this check box to enable the List of Connection URLs.
- **List of Connection URLs**: Allows you to specify a list of Pulse Secure servers (Pulse Policy Secure or Pulse Connect Secure) for this connection. Pulse Client attempts to reach each server in the list, in the order listed, until it succeeds. You can specify up to 8 Pulse Secure servers. If you enable the Randomize URL list order check box, Pulse Client ignores the listed order and chooses from the list randomly. If the Pulse Client connection is configured to use a list of Pulse Secure servers, any preferred roles and realms you specify must be applicable to all of those servers. The default behavior is to start with the most recently connected URL first, then try from top of list. The most recently connected URL is saved across reboots. Connections that use machine authentication always use the ordered list of connection URLs. In the case of an interrupted connection, such as temporarily losing the WiFi link, Pulse Client always tries to reconnect to the most recently connected URL. During a credential provider connection attempt, Pulse Client chooses the URL automatically. It does not display a window to let the user choose a URL. Figure 1 shows how the Pulse Client user can select a server from the list of connection URLs.

Figure 1 Pulse Client for Windows with a List of Connection URLs



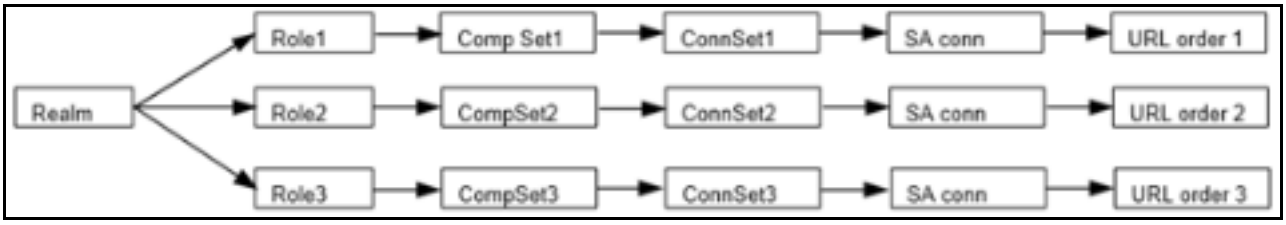
- **Attempt most recently connected URL first**: If you have specified a list of connection URLs, you can select this check box to have Pulse Client always attempt the most recent successful connection. If that connection is not successful, Pulse Client then starts at the top of the list.
- **Randomize URL list order**: If you have specified a list of connection URLs, select this check box to have Pulse Client ignore the order in which the servers are listed. You can select this option to spread the connection load across multiple Pulse Secure servers. If you enabled **Attempt most recently connected URL first**, then Pulse Client attempts that connection first. If that connection attempt fails, Pulse Client chooses randomly from the list for the next connection attempt. During a credential provider connection attempt, Pulse Client chooses the URL automatically. It does not display a window to let the user choose a URL.

Note: IF-MAP federation must be configured to ensure that a suspended session can be resumed to a different URL.

Note: When this feature is used with Pulse Policy Secure, all of the Pulse Secure servers in the list must be configured for failover, so that any one of them can provision the firewall enforcer.

The connection list enables you to support different URL ordering for different users. You can use custom expressions in a realm's role mapping rules to associate different users to different roles. For example, you could use a custom expression that is based on the OU (Organization Unit) when using an LDAP authentication server, (UserDN.OU = "Americas"). Each role is associated with a different Pulse Client connection set, and each Pulse Client connection within the connection set is configured with different URL lists. Figure 2 shows the role mapping for providing different URL lists for different users.

Figure 2 Mapping URL Lists to Users



SRX (for Dynamic VPN) Connection Type Options

Use an SRX connection for a dynamic VPN connection to an SRX Series Services Gateway.

- **Address**: Specifies the IP address of the SRX Series device.
- **Allow user to override connection policy**: Allows users to override the connection policy by manually connecting or disconnecting. Typically, you leave this option selected to make sure that a user can establish a connection under all conditions. If you disable this check box, the user cannot change the endpoint's connection status or shut down Pulse Client.

Pulse Client Connection is Established Options

For all connection types, specify how the connection is established. The options vary according to the type of connection. Automatic connections include machine authentication and credential provider connections. Connections can be established using the following options.

Note: All connections that are configured to start automatically attempt to connect to their target networks at startup time. To avoid multiple connection attempts, be sure that only one connection is configured to start automatically, or configure location awareness rules.

- Modes:
  - **User**: Enables user authentication.
  - **Machine**: Enables machine authentication, which requires that Active Directory is used as the authentication server and that machine credentials are configured in Active Directory. A machine connection is, by default, an automatic connection.
  - **Machine or user**: Enables machine authentication for the initial connection. After user authentication, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored.
- Options:
  - **Connect automatically**: Connections are attempted when the conditions specified in the location awareness rules are true, and disconnected when the conditions are no longer true.
  - **Enable pre-desktop login (Credential provider)**: Enables Pulse Client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse Client connection to the network, login to the endpoint, and login to the domain server.
  - **Reconnect at Session Timeout or Deletion)**: If this option is enabled, user initiated sessions automatically attempt to reconnect upon a session timeout or deletion. If this option is disabled, then user initiated sessions remain disconnected upon a session timeout or deletion.

Pulse Client Connection is Established Examples

The following configurations show how to select the Connection is established options of a Pulse Client connection set for specific user login behavior:

Figure 3 Connect manually

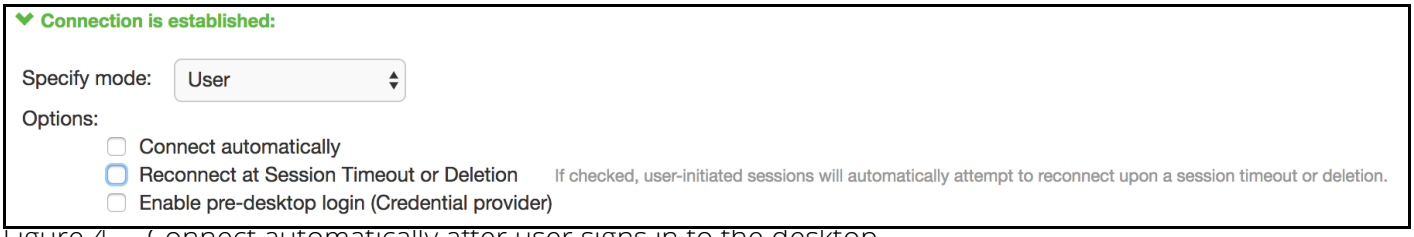


Figure 4 Connect automatically after user signs in to the desktop

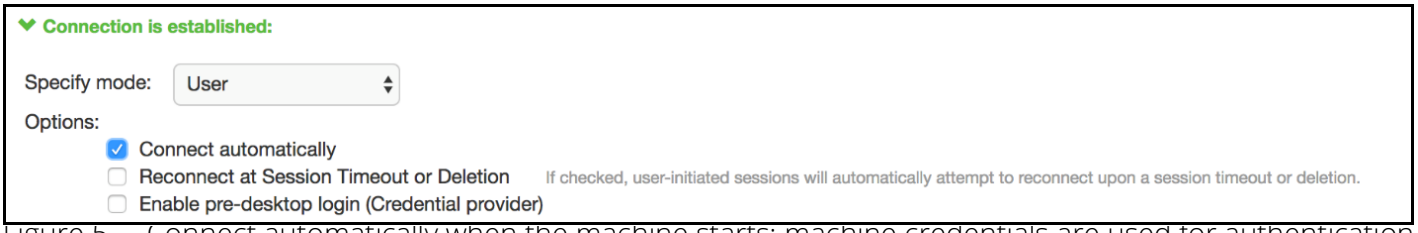
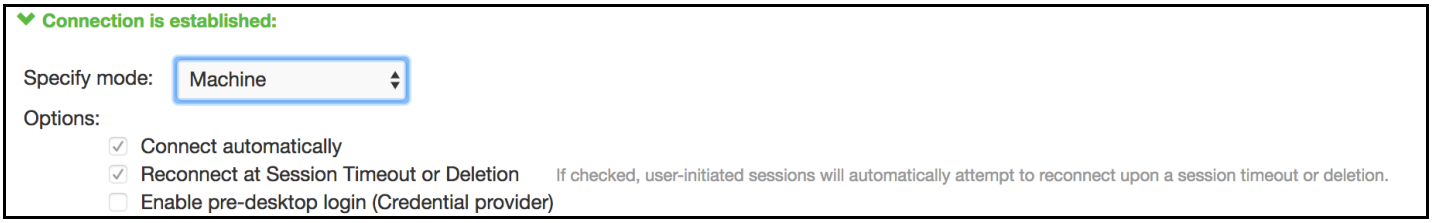


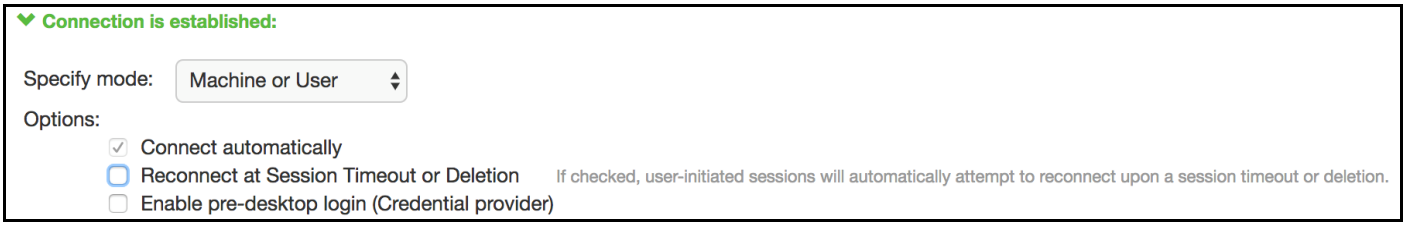
Figure 5 Connect automatically when the machine starts; machine credentials are used for authentication



Note: When you use machine credentials for authentication and no user credentials, Pulse Client cannot perform user-based tasks. The following tasks can be run only when the user is logged in:

- Run session scripts
- Detect or modify proxy settings
- Run automatic Pulse Client upgrade
- Install or upgrade Pulse Client components

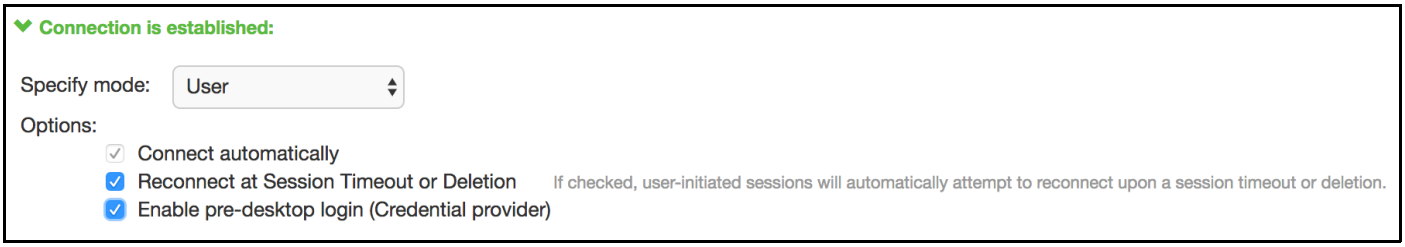
Figure 6 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop



The configuration in Figure 6 enables machine authentication for the initial connection. After the user connects with user credentials, the machine authentication is dropped. When the user logs out, the machine authentication connection is restored. In one typical use case, the machine credentials provide access to one VLAN, and the user credentials provide access to a different VLAN.

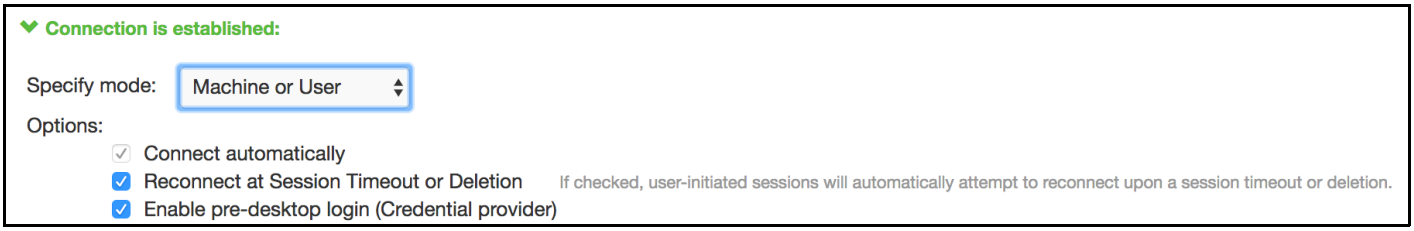
Note: If the machine and user have different roles, each role should map to the same connection set. Otherwise, after the user connects, the existing connection set might be replaced.

Figure 7 Connect automatically at user login



The configuration in Figure 7 enables Pulse Client interaction with the credential provider software on the endpoint. The user credentials are used to establish the authenticated Pulse Client connection to the network, to log in to the endpoint, and to log in to the domain server.

Figure 8 Connect automatically when the machine starts; connection is authenticated again at user login



The configuration in Figure 8 enables Pulse Client interaction with the credential provider software on the endpoint. Machine credentials are used to establish the authenticated Pulse Client connection to the network. When the user provides user credentials, the connection is authenticated again. In one typical use case, the machine credentials provide access to one VLAN, and the user credentials provide access to a different VLAN.

Location Awareness Rules

For Connect Secure or Policy Secure (L3) and SRX connections that are set to have the connection established automatically, you should define location awareness rules that enable an endpoint to connect conditionally. If you do not have location awareness rules defined, Pulse Client attempts to connect with each connection that is defined as an automatic connection until it connects successfully. Location awareness rules allow you to define an intelligent connection scheme. For example, the endpoint connects to Pulse Policy Secure if it is connected to the company intranet, or it connects to Pulse Connect Secure if it is in a remote location.

A Pulse Client connection uses the IP address of a specified interface on the endpoint to determine its network location. Each location awareness rule includes the following settings:

- **Name**: A descriptive name, for example, "corporate-DNS." A name can include letters, numbers, hyphens, and underscores.

- **Action**: The method the connection uses to discover the IP address. Choose one of the following values:
  - **DNS Server**: Allows the endpoint to connect if the endpoint's DNS server on the specified interface is set to one of the specified values. Use the Condition box to specify IP addresses or address ranges.
  - **Resolve Address**: Allows the endpoint to connect if the hostname specified in the DNS Name box can be resolved by the DNS server for the specified interface. If one or more address ranges are specified in the Address Range box, the address must resolve to one of the ranges to satisfy the expression.
  - **Endpoint Address**: Allows the endpoint to connect if the IP address of the specified interface is within a range specified in the IP Address Range box.

Note: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

Machine Connection Preferences

The Machine Connection Preferences appear if you have selected one of the machine authentication options for how the connection is established. Normally Pulse Client presents a selection dialog box if more than one realm or role is available to the user. However, a connection that is established through machine authentication fails if a dialog box is presented during the connection process. To suppress the selection dialogs, either ensure that only one role and realm is available to users, or specify a preferred realm and role for this connection.

- **Preferred Machine Realm**: Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm available for the specified login credentials
- **Preferred Machine Role Set**: Specify the role or the name of rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.

User Connection Preferences

The User Connection Preferences options enable you to specify a realm and role for automatic connections that would otherwise present a selection dialog box to the user. To suppress the selection dialogs, either ensure that only one role and realm is available to users, or specify a preferred realm and role for this connection.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

- **Preferred User Realm**: Specify the realm for this connection that is used when a user logs onto the endpoint. The connection ignores any other realm available for the user's login credentials

If one of the credential provider connection options is enabled, the following options are available:

- **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
- **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

- **Preferred User Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.
- **Select client certificate from machine certificate store**: Enables you to specify the location of the client certificate on a Windows endpoint as part of a Pulse Client connection that verifies the identity of both the machine and the user before establishing a connection. When this check box is selected, the Pulse Client connection looks at client certificates located in the Local Computer personal certificate store. When this check box is not selected, the connection accesses the user certificate store a Windows endpoint. For more information, see "Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure" on page 39.

Related Documentation

- "Machine Authentication for Pulse Policy Secure Overview"
- "Configuring Location Awareness Rules for Pulse Client"
- "Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure"
- "Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection"
- "Creating a Pulse Client Connection Set for Pulse Policy Secure"

Creating a Pulse Client Connection Set for Pulse Policy Secure

A Pulse Client connection (also called a client configuration) set contains network options and allows you to configure specific connection policies for client access to any Pulse Secure server that supports Pulse Client.

To create a Pulse Client configuration:

1. From the admin console, select **Users > Pulse Secure > Connections**.
2. Click **New**.
3. Enter a name and, optionally, a description for this connection set.

Note: You must enter a connection set name before you can create connections.

4. Click **Save Changes**.
5. From the main Pulse Client Connections page, select the connection set.
6. Under Options, select or clear the following check boxes:
   - **Allow saving logon information**: Controls whether the Save Settings check box is available in login credential dialog boxes in Pulse Client. If you clear this check box, Pulse Client always requires users to provide credentials. If you select this check box, users have the option of saving their credentials.
   - **Allow user connections**: Controls whether connections can be added by the user through the Pulse Client interface.
   - **Display splash screen**: Clear this check box to hide the Pulse Client splash screen that normally appears when Pulse Client starts.

- **Dynamic certificate trust**: Determines whether users can opt to trust unknown certificates. If you select this check box, a user can ignore warnings about invalid certificates and connect to the target Pulse Secure server.

  Note: By default, Dynamic certificate trust check box will be unchecked.

- **Dynamic connections**: Allows new connections to be added automatically to Pulse Client when the user connects through the Pulse Secure server's Web portal and then starts Pulse Client through the Web portal interface.
- **FIPS mode enabled**: Enable FIPS mode communications for all Pulse Client connections in the connection set. The Federal Information Processing Standard (FIPS) defines secure communications for the U.S. government. When a Pulse Client connection is operating in FIPS mode, "FIPS On" appears in the lower corner of the Pulse Client interface. If the Pulse Secure server hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

Note: Users cannot enable FIPS mode for connections that are created on the client. You must deploy connections with FIPS mode enabled using a pre-configured connection set with FIPS mode enabled or have users establish a browser session to the FIPS enabled Pulse Secure server.

- **Wireless suppression**: Disables wireless access when a wired connection is available. Wireless suppression occurs only when the wired connection is connected and authorized.

7. Under Connections, click **New** to define a new connection.
8. Enter a name and, optionally, a description for this connection.
9. Select a type for the connection. Type can be any of the following:
   - UAC 802.1X
   - Connect Secure or Policy Secure (L3)
   - SRX
10. 1If you select UAC 802.1X from the type list, enter a value or select or clear the following check boxes:
    - **Adapter type**: Select Wired or Wireless.
    - **Outer username**: Enter the outer username.
    - **Scan list**: If you selected wireless as the adapter type, the scan list box is available to specify the SSIDs, including non-broadcast SSIDs, to connect to in priority order. If you leave the list empty, the user can connect to any available wireless network.
    - **Support Non-broadcast SSID**: Allow users to connect to a non-broadcast wireless network from within the Pulse Client interface.
11. **Wireless Security Algorithm**: Specify the type of wireless security that the client uses to connect to the non-broadcast wireless network:
    - WPA
    - WPA2

12. **Wireless Security Cipher**: Specify the type of encryption that the client uses to communicate with the non-broadcast network:
    - TKIP
    - AES
13. Click **Save Changes**.
14. If you selected "Connect Secure" or "Policy Secure (L3)" for the type, configure the following:
    - **Allow user to override connection policy**

Note: If you disable this check box, the user cannot change the endpoint's connection status or shut down Pulse Client.

- **Enable Pulse Collaboration integration on this connection**
- **Support Remote Access (SSL VPN) or LAN Access (UAC) on this connection**
- **Connect to URL of this server only**: Specifies whether the endpoint connects to this Pulse Secure server exclusively or if it can connect to the any of the servers listed in the list of connection URLs. Disable this check box to enable the List of Connection URLs.
- **List of Connection URLs**: Allows you to specify a list of Pulse Secure servers (Pulse Policy Secure or Pulse Connect Secure) for this connection. Pulse Client attempts to reach each server in the list, in the order listed, until it succeeds. You can specify up to 8 Pulse Secure servers. If you enable the Randomize URL list order check box, Pulse Client ignores the listed order and chooses from the list randomly. If the Pulse Client connection is configured to use a list of Pulse Secure servers, any preferred roles and realms you specify must be applicable to all of those servers.
  - Start with most recently connected URL first, then try from top of list. The most recently connected URL is saved across reboots.
  - Connections that use machine authentication ignore this option and always use the ordered list of connection URLs.
  - In the case of an interrupted connection, such as temporarily losing the WiFi link, Pulse Client always tries to reconnect to the most recently connected URL.
  - During a credential provider connection attempt, Pulse Client chooses the URL automatically. It does not display a window to let the user choose a URL.
- **Randomize URL list order**: If you have specified a list of connection URLs, select this check box to have Pulse Client ignore the order in which the servers are listed. You can select this option to spread the connection load across multiple Pulse Secure servers. If you enabled **Attempt most recently connected URL first**, Pulse Client attempts that connection first. If that connection attempt fails, Pulse Client chooses randomly from the list for the next connection attempt. During a credential provider connection attempt, Pulse Client chooses the URL automatically. It does not display a window to let the user choose a URL.

Note: IF-MAP federation must be configured to ensure that a suspended session can be resumed to a different URL.

Note: When this feature is used with Pulse Policy Secure, all of the Pulse Secure servers in the list must be configured for failover so that any one of them can provision the firewall enforcer.

- **Client Certificate Location**: Enables you to specify the certificate store that Pulse Client accesses for certificate authentication on Windows endpoints. Typically, you would use the default setting, which retrieves the certificate from the user's personal certificate store, and then certificate authentication is controlled by the **Connection is established** option. If you disable this option, the Pulse Client connection uses a machine certificate from the Local Computer Personal certificate store, which enables you to perform machine authentication and user authentication for the Pulse Client connection. If you disable this option, you must also create a sign-in policy and configure authentications servers to perform the user authentication.

15. If you select "SRX", enter the IP address of the SRX device in the Address box and specify whether you want the user to be able to override connection policy.
16. Specify how the connection is established, manually or automatically. These options enable you to configure machine authentication and credential provider authentication.
17. (Optional) You can enable location awareness on automatic connections by creating location awareness rules. Location awareness can force a connection to a particular interface.
18. (Optional) You can set preferred role and realm options for a machine authentication connection.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

19. After you have created the client connection set, create a client component set and select this connection set.

Related Documentation

- "Configuring Location Awareness Rules for Pulse Client"
- "Preferred Realm and Role for Pulse Client Machine Authentication"
- "Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection"

Pulse Client FIPS Mode Overview for Pulse Policy Secure

The United States Federal Information Processing Standard (FIPS) defines security and interoperability requirements for computer systems that are used by the U.S. government. Pulse Client for Windows, Mac, and Linux, support FIPS mode operations when communicating with Pulse Connect Secure and Pulse Client for Windows and Mac support FIPS mode operations when communicating with Pulse Policy Secure. When it is operating in FIPS mode, "FIPS On" appears in the bottom corner of the Pulse Client for Windows and Mac clients.

You enable FIPS mode operations for Pulse Client for Windows when you configure Pulse Client connections on the server. You enable FIPS mode operations for a connection set. That connection set can include any or all of the four types of Pulse Client connections:

- **UAC (802.1X)**: Pulse Client uses FIPS mode cryptography for authentication but it uses default Microsoft cryptography for the WEP/WPA wireless encryption.
- **Connect Secure or Policy Secure (L3)**: FIPS mode cryptography is supported.
- **SRX**: FIPS mode cryptography is not supported.

Note: Users cannot enable FIPS mode for connections that are created on the client. You must deploy connections with FIPS mode enabled using a pre-configured connection set with FIPS mode enabled or have users establish a browser session to the FIPS enabled Pulse Secure server.

Windows Endpoint Requirements

Pulse Client supports FIPS mode on Windows 8.1 and later Windows versions, and on Pulse Mobile Client for iOS and Android for communications with Pulse Connect Secure. FIPS is not supported by Pulse Client for Apple OS X.

To support client certificate private key operations on Windows, the security policy on the Windows endpoint must have FIPS enabled. To verify that FIPS is enabled, use the Microsoft Management Console (MMC). Make sure that the Group Policy Snap-in is installed, and then open the following item:

Local Computer Policy > Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options

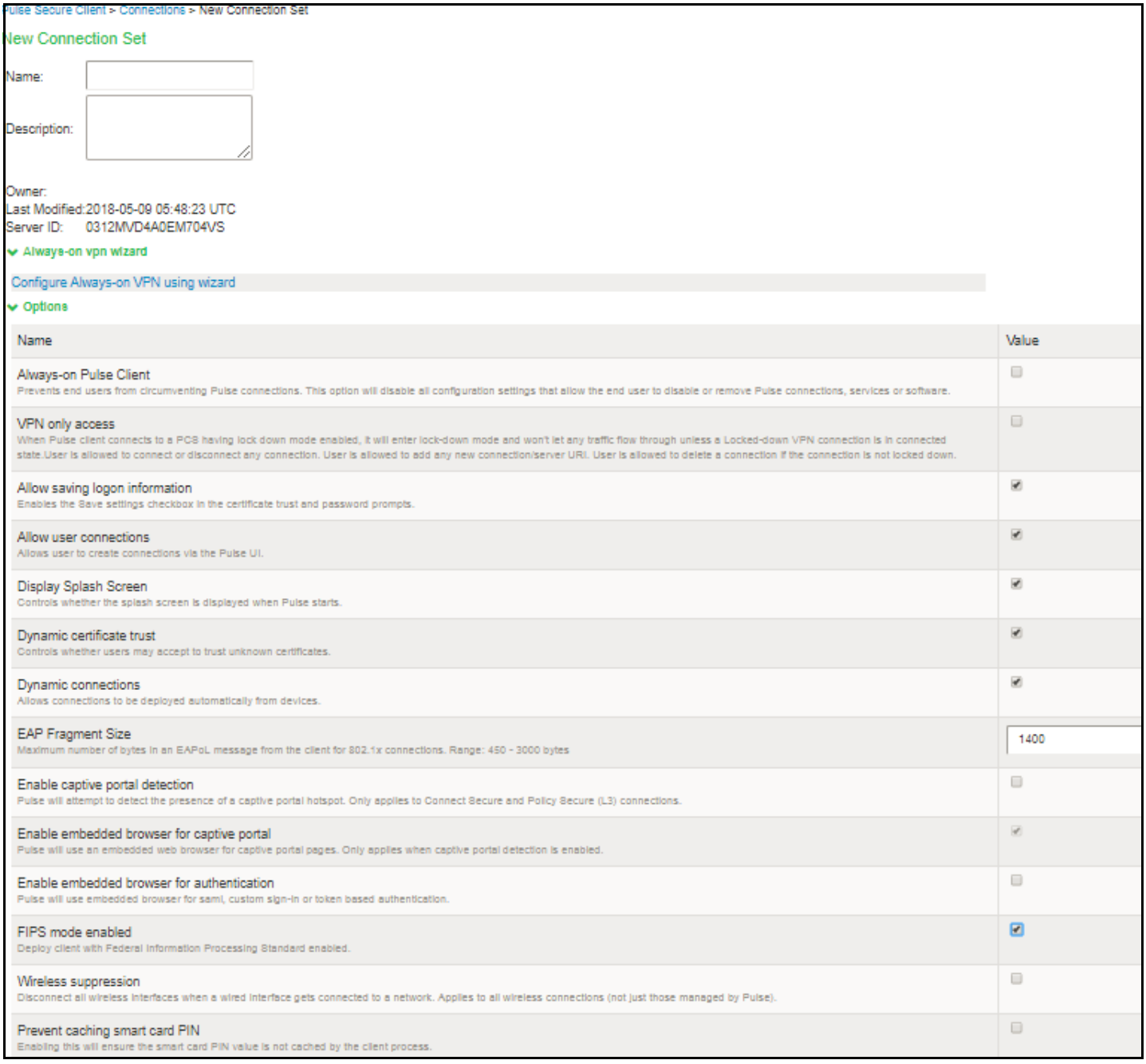
Scroll through the Policy list and make sure that the following policy is enabled:

"System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing"

Configuration Overview

Pulse Client includes all components required for FIPS mode communications. You enable the Pulse Secure server for FIPS mode operations as part of the System SSL Options (**System > Configuration > Security > SSL Options**). To enable FIPS mode communications for Pulse Client for Windows, deploy one or more Pulse Client connections to the client that are FIPS enabled. Figure 9 shows the check box in the Pulse Client connection set configuration screen that enables FIPS mode operations for all connections in the connection set.

Figure 9 Enabling FIPS Mode for Pulse Client Connections



Note: If the Pulse Secure server hardware does not support FIPS mode operations, FIPS mode configuration options are not present in the admin console interface. FIPS mode operations are supported on PSA-V Series Pulse Secure Gateways and some SA series appliances. The device must be running Pulse Policy Secure R5.0 or later or Pulse Connect Secure R8.0 or later.

Related Documentation

- "Creating a Pulse Client Connection Set for Pulse Policy Secure"

Securing the Connection State on Pulse Client

To disable user interaction with Pulse Client connections on the endpoint, you can configure Pulse Client Connections so that when they are deployed to the endpoint, users cannot shut down a connection, suspend or resume a connection, or shut down Pulse Client. Disabling user interaction with Pulse Client enables the administrator to control how endpoints connect to the network without allowing the user to override administrative control. For example, if you use machine authentication, the connection from endpoint to server is established automatically. By locking down the Pulse Client endpoint, users cannot change their connection.

To secure the Pulse Client endpoint:

1. Click **Users > Pulse Secure Connections**.
2. Edit or create a new connection.
3. Disable the check box labeled "Allow user" to override connection policy.

Related Documentation

- "Pulse Client Connection Set Options for Pulse Policy Secure"
- "Endpoint Security Monitoring and Management for Pulse Policy Secure"
- "Machine Authentication for Pulse Policy Secure Overview"

Machine Authentication for Pulse Policy Secure Overview

Machine authentication uses machine credentials (machine name and password or machine certificate) to authenticate the endpoint. You can enable machine authentication for Pulse Policy Secure as part of a Pulse Client Connection and distribute the connection to endpoints through the normal Pulse Client distribution methods. You enable machine authentication support on a Pulse Client connection, either Layer 2 or Layer 3.

The following describes the requirements for a machine authentication environment:

- The authentication server used by the Pulse Client connection must be Active Directory/Windows NT for machine name/password authentication or a certificate server for machine certificate authentication.
- The endpoint must be a member of a Windows domain, and the machine credentials must be defined in Active Directory.
- The Pulse Client connection must be configured so that no prompts are presented during the login process. For example, prompts for realm or role selection or for a server certificate trust prompt cause the connection to fail. You can specify a preferred role and realm for the connection, which eliminates realm and role selection dialogs.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

- For machine certificate authentication, the domain workstation login certificate must be issued by the domain certificate authority. The root certificate must be in the Machine Trusted Certificate store instead of the certificate store for a particular user.

Pulse Client supports the following machine authentication types:

- **machine-only**: The connection is established using machine credentials when no user is logged in. The connection is maintained after user login.
- **user-after-desktop**: The connection is established using machine credentials when no user is logged in. After user login, the machine connection is disconnected. Once the user logs out, the user connection is disconnected and the machine connection is reestablished.

Related Documentation

- "Preferred Realm and Role for Pulse Client Machine Authentication"
- "Configuring Machine-Only Machine Authentication for a Pulse Client Connection"
- "Configuring User-After-Desktop Machine Authentication for a Pulse Client Connection"
- "Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure"
- "Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection"

Configuring Machine-Only Machine Authentication for a Pulse Client Connection

When a Pulse Client connection is configured for machine-only machine authentication, the Pulse Client connection is established using machine credentials when no user is logged in. The connection is maintained after user login.

To enable a Pulse Client connection for machine-only machine authentication:

1. Click **Users > Pulse Secure > Connections** and create or select a connection set.
2. Create or edit a connection. For the connection type, you can select either UAC (802.1X) for a Layer 2 connection or Connect Secure or Policy Secure (L3) for a Layer 3 connection.
3. Under Connection is established, for the mode select **Machine**.

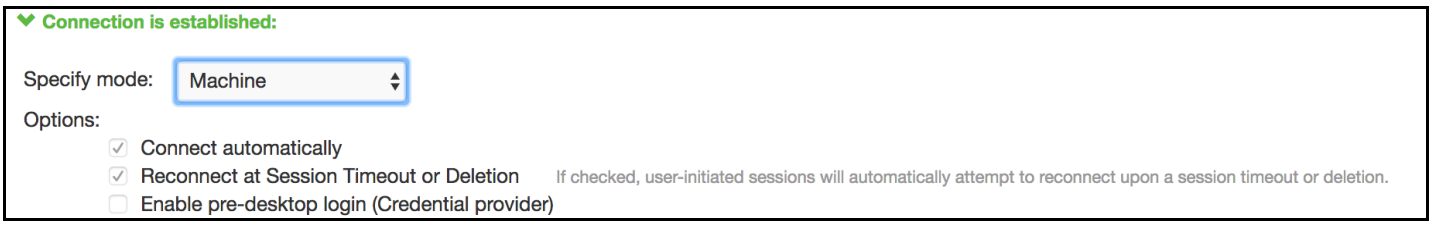
Machine credentials are used to connect to the Pulse Secure server when the endpoint is started, before a user logs in. The connection is maintained when a user logs in, logs out, or switches to a different login.

Note: When you use machine credentials for authentication and no user credentials, Pulse Client cannot perform user-based tasks. The following tasks can be run only when the user is logged in:

- Run session scripts
- Detect or modify proxy settings
- Run automatic Pulse Client upgrade
- Install or upgrade Pulse Client components

4. Select the **Connect automatically** check box.

Figure 10 Connect automatically when the machine starts; machine credentials are used for authentication



5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type "ANY" as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
6. Specify **Realm and Role Preferences** to suppress realm or role selection dialogs during the login process:
   - **Preferred Machine Realm**: Specify the realm for this connection. The connection ignores any other realm that is available for the specific login credentials.
   - **Preferred Machine Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name must be a member of the preferred machine realm.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

Related Documentation

- "Machine Authentication for Pulse Policy Secure Overview"
- "Credential Provider Authentication for Pulse Policy Secure Overview"
- "Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection"

Configuring User-After-Desktop Machine Authentication for a Pulse Client Connection

When a Pulse Client connection is configured for user-after-desktop machine authentication, the connection is established using machine credentials when no user is logged in. After user login, the machine connection is disconnected. Once the user logs out, user connection is disconnected and machine connection is reestablished.

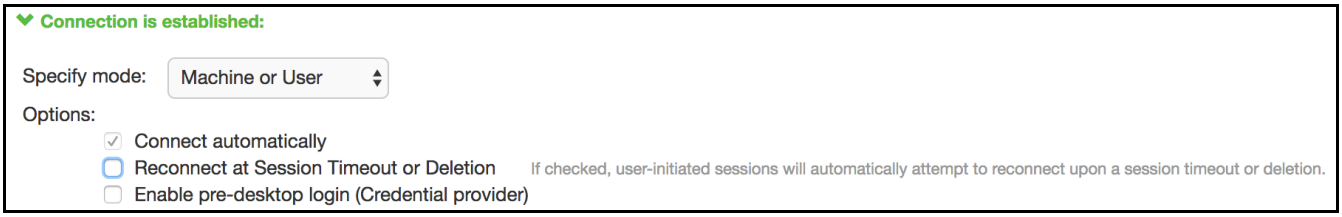
To enable a Pulse Client connection for user-after-desktop machine authentication:

1. Click **Users > Pulse Secure > Connections**, and then create or select a connection set.
2. Create or edit a connection. For the connection type, you can select either UAC (802.1X) for a Layer 2 connection or Connect Secure or Policy Secure (L3) for a Layer 3 connection.
3. Under Connection is established, for mode, select **Machine** or **User**.

Machine credentials are used to connect to the Pulse Secure server when the endpoint is started, before a user logs in. When a user logs in, the machine authentication connection is dropped, and the user login is used instead. When the user logs out, the machine connection is reestablished.

4. Select the **Connect automatically** check box.

   Figure 11 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop



5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type ANY as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.

6. Specify Realm and Role Preferences to suppress realm or role selection dialogs during the login process for both machine and user logins:

   - **Preferred Machine Realm**: Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm that is available for the specific login credentials.
   - **Preferred Machine Role Set**: Specify the role or the name of a rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.
   - **Preferred User Realm**: Specify the realm that for this connection that is used when a user logs into the endpoint. The connection ignores any other realm that is available for the user's login credentials.
   - **Preferred User Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

Related Documentation

- "Machine Authentication for Pulse Policy Secure Overview"
- "Credential Provider Authentication for Pulse Policy Secure Overview"
- "Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection"

Preferred Realm and Role for Pulse Client Machine Authentication

When a Pulse Client Connection is configured to use machine authentication, any prompts that occur during the login process cause the connection to fail. For example, if the Pulse Secure server authentication policy allows a user to select a realm or a role during the login process, Pulse Client presents a dialog box to the user and prompts for the realm or role selection. To avoid failed connections caused by prompts during machine authentication, you can specify a preferred role and realm for a Pulse Client connection.

Note: Realm and role prompts are not the only prompts that are possible during the login process. If the Pulse Client connection has the Dynamic Certificate Trust option enabled and there is an issue with the server certificate, Pulse Client asks the user if it is OK to proceed. That certificate prompt causes a machine connection to fail. Note that the prompt for upgrading Pulse Client software is presented after the user connection is established, and it will not affect a machine authentication connection.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, any preferred roles and realms you specify must be applicable to all of those servers.

For a Pulse Client connection that is used for machine authentication, you do not need to specify the preferred role if either of the following conditions is true:

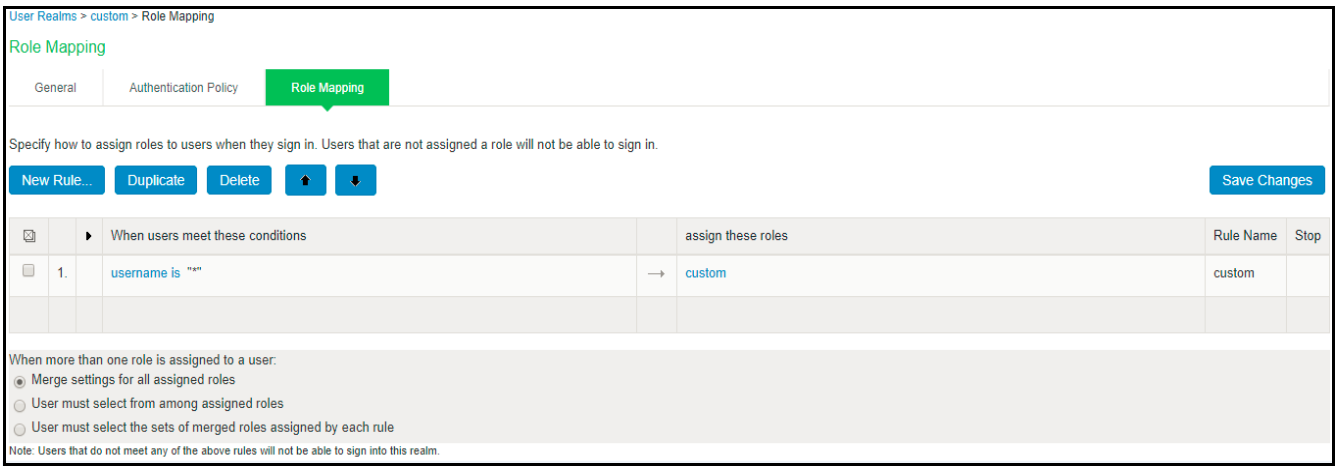
- Users are mapped to only one role.
- Users are mapped to more than one role, but the realm's role mapping properties are set to merge settings for all assigned roles.

For a Pulse Client connection that is used for machine authentication, you must specify the preferred realm if the authentication sign-in policy allows the user to select a realm. If that realm maps to only one role, you do not need to specify the role.

For a Pulse Client connection that is used for machine authentication, you must specify the preferred role if either of the following conditions is true:

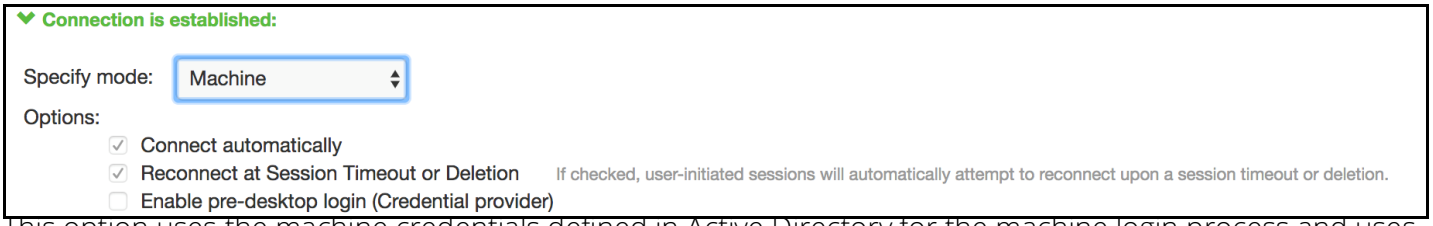
- The realm that the user connects to maps to more than one role and the realm's role mapping properties are set to require that the user must select a role. The preferred role set must be the name of a role assigned in that realm.
- The realm that the user connects to maps to more than one role, and the realm's role mapping properties are defined by role mapping rules. You specify the preferred role by specifying the name of a rule that assigns the role set. Figure 12 shows a role mapping rule with the rule name highlighted.

Figure 12 Pulse Client Role Mapping Rule



To identify the connection as a machine authentication connection, you specify how the connection is established using one of the configurations shown in Figure 13 and Figure 14.

Figure 13 Connect automatically when the machine starts; machine credentials are used for authentication



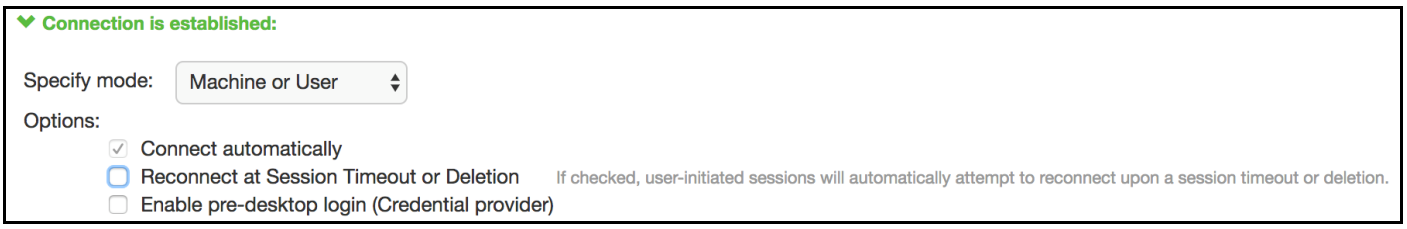
This option uses the machine credentials defined in Active Directory for the machine login process and uses the same credentials for user login. When you select this option, the Realm and Role Set Preferences settings enable you to specify the following options:

- **Preferred Machine Realm**: Type the realm name that maps to the role you want to assign.
- **Preferred Machine Role Set**: Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Alternatively, you can specify the name of a role mapping rule that assigns the role set.

Note: When you use machine credentials for authentication and no user credentials, Pulse Client cannot perform user based tasks. The following tasks can be run only when the user is logged in:

- Run session scripts
- Detect or modify proxy settings
- Run automatic Pulse Client upgrade
- Install or upgrade Pulse Client components

Figure 14 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop



This option uses the Active Directory machine credentials for the machine login process. When machine login is complete, Pulse Client drops that connection and then uses the user credentials for user login. When you select this option, the Realm and Role Set Preferences enable you to specify the following options:

- **Preferred Machine Realm**: Type the realm name that maps to the role you want to assign.
- **Preferred Machine Role Set**: Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Alternatively, you can specify the name of a role mapping rule that assigns the role set.
- **Preferred User Realm**: Type the realm name that maps to the role you want to assign.
- **Preferred User Role Set**: Type the name of the role. The role must be one that is identified in the realm's role mapping properties. Alternatively, you can specify the name of a role mapping rule that assigns the role set.

Related Documentation

- "Machine Authentication for Pulse Policy Secure Overview"

Remote Desktop Protocol Compatibility with a Pulse Client 802.1X Machine Authentication Connection

If you want to use Remote Desktop Protocol (RDP) to access an endpoint over a Pulse Client 802.1X connection, machine authentication is required. Because of a Microsoft OS limitation, an RDP connection attempt over a user-only 802.1X authenticated connection will fail. To support RDP connectivity over an authenticated 802.1X connection, you must have a machine-only connection or a machine-then-user connection. In the case of a machine-then-user connection, when you use RDP to connect to a machine over an 802.1X connection that is connected as user, the connection transitions the 802.1X connection to a machine connection. If you subsequently log into the machine directly, it transitions back to a user connection.

To access the endpoint using RDP, you must define the connection to be established using one of the following Pulse Client configurations:

Figure 15 Connect automatically when the machine starts; machine credentials are used for authentication

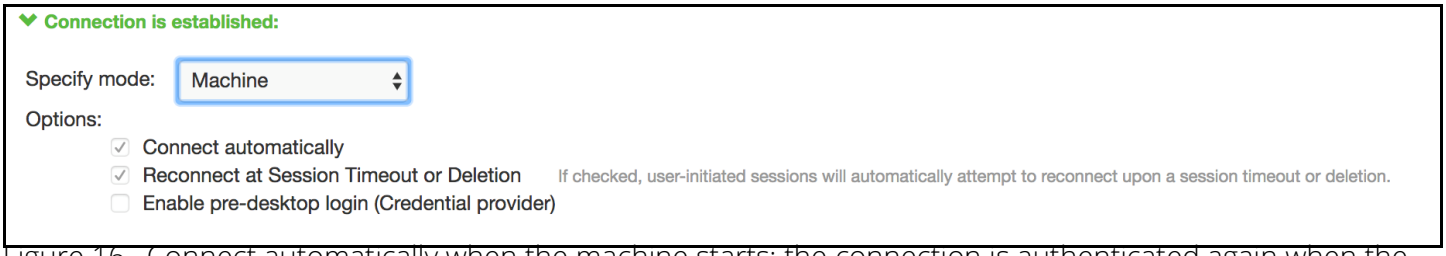
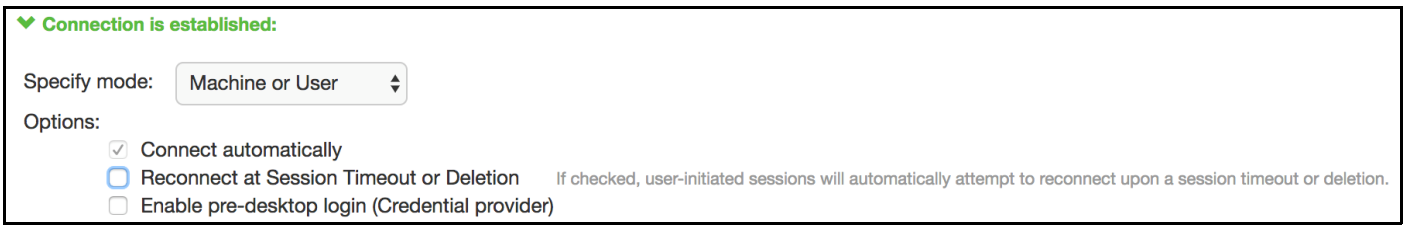


Figure 16 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop



Related Documentation

- "Machine Authentication for Pulse Policy Secure Overview"

Credential Provider Authentication for Pulse Policy Secure Overview

When Microsoft introduced Windows Vista, it moved away from a login integration interface based on Graphical Identification and Authentication (GINA) in favor of credential provider authentication. Pulse Client credential provider integration enables connectivity to a network that is required for the user to log into the Windows domain. For example, the domain controller might reside behind a firewall and the endpoint uses credential provider login to connect to Pulse Policy Secure prior to domain login. Pulse Client integrates with Microsoft credential providers to enable password-based login and smart card login. Pulse Client connections also support an option that allows a user to use either a smartcard or a password to log in. Credential provider login is supported on Windows 8.1 and later Windows platforms.

You can use the Pulse Client support for credential provider authentication to provide single sign-on capabilities. Pulse Client establishes a connection to the network and then uses the same credentials to log in to the Windows domain.

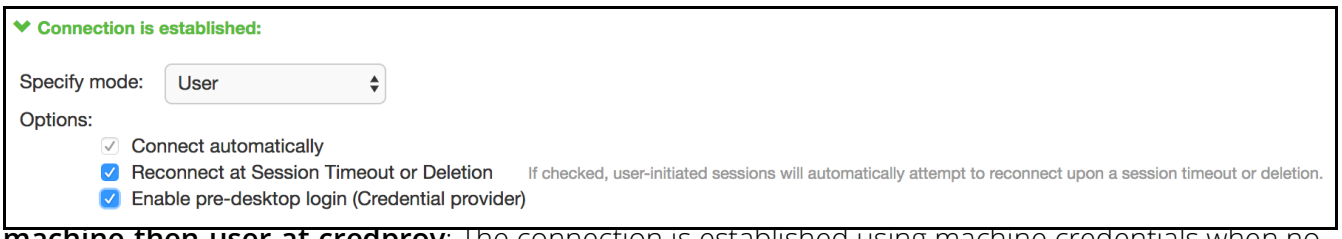
You enable credential provider support on a Pulse Client connection. After the connection has been downloaded to the endpoint through the normal Pulse Client distribution methods, Pulse Client annotates the credential provider tile that appears on the user login screen by adding a Pulse Secure icon in the lower right corner of the tile. When the user initiates the login process, Pulse Client establishes the connection.

Note: A connection attempt to a Pulse Secure server fails if the connection uses Host Checker and Host Checker is installed in a non-default appdata folder. Host Checker is installed

Pulse Client supports the following credential provider types:

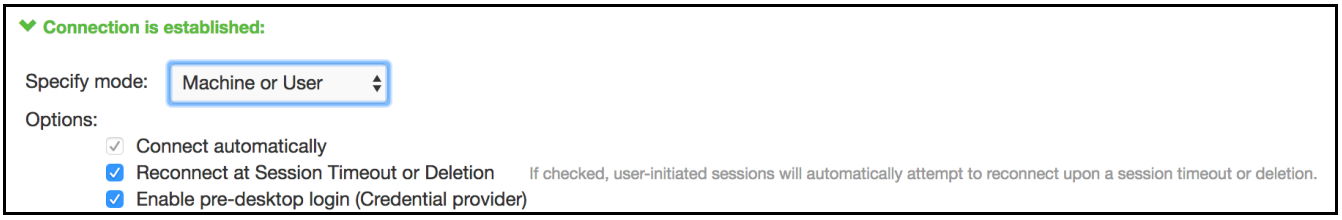
- **user-at-credprov**: The connection is established before the user login using credentials collected at the selected credential tile, which provides single-sign-on functionality. The connection is maintained as an active connection on the user's desktop. To enable user-at-credprov authentication, use the Pulse Client connection configuration shown in Figure 17.

Figure 17 Connect automatically at user login



- **machine-then-user-at-credprov**: The connection is established using machine credentials when no user is logged in. When a user clicks a login tile and provides user credentials, the machine connection is disconnected and a new connection is established. When the user logs out, the user connection is disconnected and the machine connection is reestablished. In one typical machine-then-user-at-credprov implementation, the machine connection and the user connection are mapped to different VLANs. To enable machine-then-user-at-credprov authentication, use the Pulse Client connection configuration shown in Figure 18.

Figure 18 Connect automatically when the machine starts; connection is authenticated again at user login



Pulse Client credential provider support usage notes:

- If the endpoint includes more than one Pulse Client Layer 2 connection, Windows determines which connection to use:

  1. If a network cable is attached to the endpoint, Layer 2 wired connections are attempted, and then wireless connections. If more than one wireless network is available, the order is determined by the scan list specified as a Pulse Client connection option.

  2. After all Layer 2 options are attempted, Pulse Client runs location awareness rules to find one or more eligible Layer 3 connections that are configured for credential provider login. If more than one Layer 3 connection is found, Pulse Client prompts the user to select a connection. A user can cancel the network connection attempt by clicking the cancel button.

  3. After Pulse Client evaluates all configured connection options, Pulse Client returns control to Windows, which enables the user login operation.

- For connections that use user credentials, you can configure the Pulse Client connection so that prompts are presented during the login process, for example, prompts for realm or role selection or a server certificate trust prompt. For connections that use machine credentials, Pulse Client prompts cause the connection to fail because there is no interface to allow a response to the prompts. You can suppress any potential realm and role choice by specifying a preferred realm and role for the connection.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

- Pulse Client upgrade notifications and actions are disabled during credential provider login and postponed until the user connection is established. Host Checker remediation notifications are displayed.
- To allow users to log in using either a smart card or a password, you can create different authentication realms for each use case and then specify the Preferred Smartcard Logon Realm and Preferred Password Logon Realm as part of the connection properties.
- A credIf the client machine has non-default value for the %appdata% environment variable, then login usingHost Checker are enabled and client machine has non default value for %appdata% then login using GINA fails

  appdata is a user environment variable as well. Here user modifies the appdata of user. Credential provider runs in system user context and no user is logged in that time. User appdata details are stored in HKEY_CURRENT_USER registry. Since no user is logged in current HKEY_CURRENT_USER will be of system user. So credential provider uses a logic to form the default appdata path of user. This logic will work when default path is modified.

Related Documentation

- "Configuring Location Awareness Rules for Pulse Client"

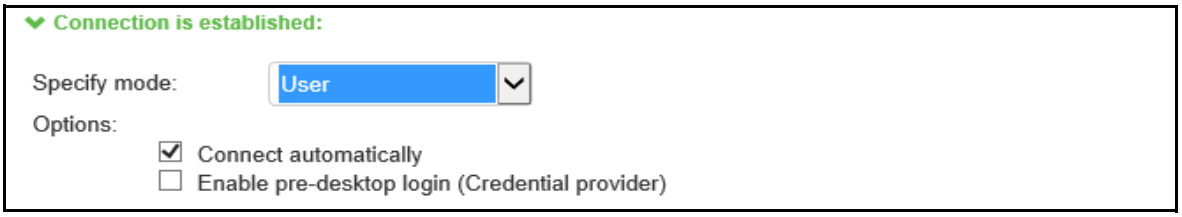
Configuring User-at-Credprov Credential Provider Authentication for a Pulse Client Connection

With a user-at-credprov connection, the Pulse Client connection establishes the connection before user login using credentials collected at the selected credential tile, which provides single sign-on functionality. The connection is maintained as an active connection on the user's desktop.

To enable user-at-credprov credential provider support for a Pulse Client connection:

1. Create a Pulse Client connection set for the role (**Users > Pulse Secure > Connections**), and then create a new Pulse Client connection. You can select either a Layer 3 connection type, Connect Secure or Policy Secure (L3), or a Layer 3 connection type, UAC (802.1X).
2. In the Connection is established section, select "User" for the mode.
3. Under Options, select the "Connect automatically" and the "Enable pre-desktop login (Credential provider)" check boxes.

   Figure 19 Connect automatically at user login



4. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type ANY as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
5. Specify Realm and Role Preferences to suppress realm or role selection dialogs during the login process:
   - **Preferred User Realm**: Specify the realm for this connection. The connection ignores any other realm that is available for the specific login credentials.

   The following options enable you to allow the user to login using a smart card or a password:
   - **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
   - **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

- **Preferred User Role Set**: Specify the preferred role or the name of the rule for the role set to be used for user authentication. The role or rule name must be a member of the preferred user realm.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

Related Documentation

- "Credential Provider Authentication for Pulse Policy Secure Overview"
- "Configuring a Pulse Client Credential Provider Connection for Password or Smart Card Login"

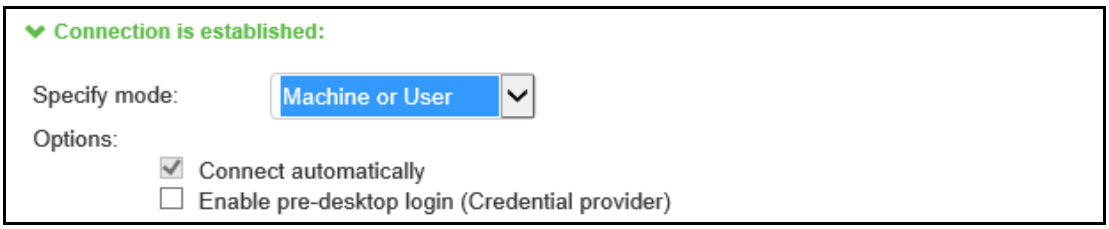
Configuring Machine-Then-User-at-Credprov Credential Provider Authentication for a Pulse Client Connection

With a machine-then-user-at-credprov connection, Pulse Client establishes the connection using machine credentials when no user is logged in. When a user clicks a login tile and provides user credentials, the machine connection is disconnected, and a new connection is established. When the user logs out, the user connection is disconnected, and the machine connection is reestablished. In one typical machine-then-user-at-credprov implementation, the machine connection and the user connection are mapped to different VLANs.

To enable machine-then-user-at-credprov credential provider support for a Pulse Client connection:

1. Create a Pulse Client connection set for the role (**Users > Pulse Secure > Connections**), and then create a new Pulse Client connection. You can select either a Layer 3 connection type, Connect Secure or Policy Secure (L3), or a Layer 2 connection type, Policy Secure (802.1X).
2. In the Connection is established section, select "Machine or User" for the mode.
3. Under Options, select the **Connect automatically** check box.

Figure 20 Connect automatically when the machine starts. Connection is authenticated again at user login



4. In the Connection is established section, select one of the following options:
5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type ANY as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
6. Specify "Realm and Role Preferences" to suppress realm or role selection dialogs during the login process for both machine and user logins:
   - **Preferred Machine Realm**: Specify the realm that this connection uses when establishing the machine connection. The connection ignores any other realm that is available for the specific login credentials.
   - **Preferred Machine Role Set**: Specify the role or the name of the rule for the role set that this connection uses when establishing the machine connection. The role or rule name used must be a member of the preferred machine realm.
   - **Preferred User Realm**: Specify the realm that for this connection that is used when a user logs in to the endpoint. The connection ignores any other realm that is available for the user's login credentials.

The following options enable you to allow the user to log in using a smart card or a password:

- **Preferred Smartcard Logon Realm**: Preferred realm to be used when user logs in with a smart card.
- **Preferred Password Logon Realm**: Preferred realm to be used when user logs in with a password.

Note: Be sure that the authentication realms you specify exist, and that they support the appropriate login credential option.

- **Preferred User Role Set**: Specify the preferred role or the name of rule for the role set to be used for user authentication. The role or rule name used must be a member of the preferred user realm.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

7. Optionally, specify pre-login preferences:
   - **Pre-login maximum delay**: The time period (in seconds) that a Windows client waits for an 802.1X connection to succeed during the login attempt. The range is 1 to 120 seconds.
   - **Pre-login user based virtual LAN**: If you are using VLANs for the machine login, you can enable this check box to allow the system to make the VLAN change.

8. Click **Save Changes**, and then distribute the Pulse Client connection to Pulse Client endpoints.

Related Documentation

- "Credential Provider Authentication for Pulse Policy Secure Overview"
- "Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure"
- "Configuring a Pulse Client Credential Provider Connection for Password or Smart Card Login"

Configuring a Pulse Client Credential Provider Connection for Password or Smart Card Login

If you allow a user to log in with a smart card or with a username/password, then you can have the Pulse Client Credential provider automatically authenticate the user based on the login method. The Pulse Client user sees two different credential provider tiles for the Pulse Client connection, one for smart card authentication and one for username/password authentication. Credential provider tiles that launch a Pulse Client connection include a Pulse Secure logo (see Figure 21). The Pulse Client connection determines which realm to use through preferred realm settings that you specify as part of the Pulse Client connection preferences. If the connection succeeds, the login type is saved so that, if re-authentication is needed (for example, if the connection times out), the same login type is used.

Figure 21 Pulse Client Credential Provider Tiles

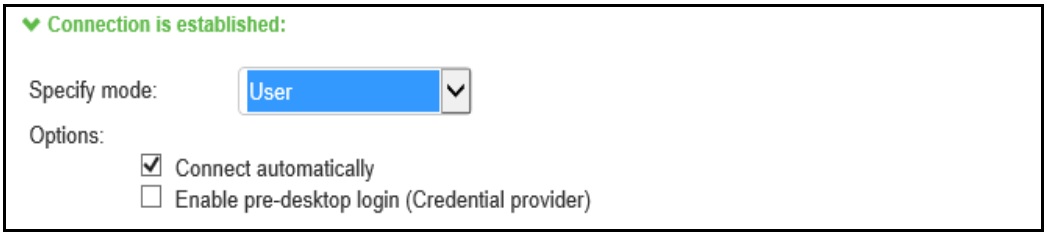
Before you begin:

- Before you deploy a connection that uses this feature, make sure that you have created all the authentication realms that are required. You need one realm for smart card authentication and a different one for user name/password authentication. Both realms can be mapped to the same role, or you can use different roles. In either case you include a remediation role for endpoints that do not pass Host Checker evaluation. If you use machine authentication for a connection (machine-then-user-at-credprov), you need an authentication realm for the machine.
- Make sure that all of the realms that are used in the Pulse Client connection are included in the sign-in policy.
- The authentication realms on the Pulse Secure server must be configured so that the Preferred Pre-login Smartcard Realm uses certificate authentication and the Preferred Pre-login Password Realm uses username/password authentication.

The following procedure summarizes the steps to create a Pulse Client Connection that uses credential provider authentication, and allows the user to choose either smart card login or username/password login. Table 1 describes the configuration options:

1. Click **Users > Pulse Secure > Connections** and create or select a connection set.
2. Create or edit a connection. For connection type, you can select either "UAC (802.1X)" for a Layer 2 connection or "Connect Secure" or "Policy Secure (L3)" for a Layer 3 connection. The "SRX connection" type does not support credential provider authentication.
3. For the Connection is established option, choose one of the credential configuration options shown in Figure 22 and Figure 23.

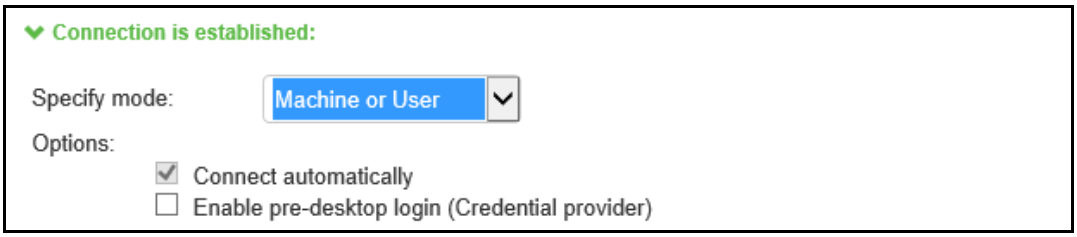
   Figure 22 Connect automatically after user signs in to the desktop

   The user credentials are used to establish the authenticated Pulse Client connection to the network, log in to the endpoint, and log in to the domain server.

   Select **User** as the mode. Under options, select **Connect automatically**.

   Figure 23 Connect automatically when the machine starts; the connection is authenticated again when the user signs in to the desktop

   Machine credentials are used to establish the authenticated Pulse Client connection to the network using the specified Machine Connection Preferences or Pre-login Connection Preferences. When the user provides user credentials, the connection is authenticated again.

   Select **Machine or User** as the mode. Under options, select **Connect automatically**.

4. For Connect Secure or Policy Secure (L3) connections that are set to have the connection established automatically, you can define location awareness rules that enable an endpoint to connect conditionally.
5. For a Layer 2 connection that uses machine certificate authentication, make sure that the connection has an entry in the Trusted Server List. To allow any server certificate, type "ANY" as the Server certificate DN. To allow only one server certificate, specify the server certificate's full DN, for example, C=US; ST=NH; L=Kingston; O=My Company; OU=Engineering; CN=c4k1.stnh.mycompany.net; E=ausername@mycompany.com.
6. For the desired connection behavior, set the connection preferences as described in Table 1.

Note: If the Pulse Client connection is configured to use a list of Pulse Secure servers, the preferred roles and realms you specify must be applicable to all of those servers.

Table 1 Configuration Options for Credential Provider Login

Pulse Client Credential Provider Login Behavior	Connection is established	User Connection Preferences	Pre-Login Connection Preferences	Machine Connection Preferences
At user login, the user can choose from two credential provider tiles: smart card login or username/ password login. The credentials are then used to connect to the network, login to the endpoint, and login to the domain server.	Automatically at user login	Preferred User Realm and Preferred User Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.	Enables Pulse Client credential provider tiles. The realm name appears on each tile. You must specify values for both of the following options: • **Preferred Pre-login Password Realm**: The authentication realm that provides username/ password authentication. • **Preferred Pre-login Smartcard Realm**: The authentication realm that provides smartcard authentication.	Not available.

Pulse Client Credential Provider Login Behavior	Connection is established	User Connection Preferences	Pre-Login Connection Preferences	Machine Connection Preferences
At machine login and at user login, the user can choose from two credential provider tiles: smart card login or username/ password login.	Automatically when machine starts. Connection is authenticated again at user login.		Enables Pulse Client credential provider tiles. The realm name appears on each tile. • **Preferred Pre-login Password Realm**: The authentication realm that provides username/ password authentication. • **Preferred Pre-login Smartcard Realm**: The authentication realm that provides smartcard authentication.	Preferred Machine Realm and Preferred Machine Role Set are not available if you specify values for Preferred Pre-login Password Realm Preferred Pre-login Smartcard Realm.

Related Documentation

- "Configuring Location Awareness Rules for Pulse Client"
- "Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure"

Machine and User Authentication Through a Pulse Client Connection for Pulse Policy Secure

Pulse Client supports certificate authentication for establishing Layer 2 and Layer 3 connections. On Windows endpoints, a Pulse Client connection accesses client certificates located in the Local Computer personal certificate store to provide machine authentication, or user certificates located in a user's personal certificate store or on a smart card for user authentication. A Pulse Client connection can access certificates from only one location. For information on machine authentication, see "Machine Authentication for Pulse Policy Secure Overview" on page 24.

You can create a Pulse Client connection that uses System Local, Active Directory, or RSA ACE server authentication to verify the user and a certificate to verify machine identity before establishing a connection. To do so, you must first enable an option for the Pulse Client connection that allows the connection to check the client certificates located in the Local Computer personal certificate store. The option, Select client certificate from machine certificate store, is part of the User Connection Preferences of a Pulse Client

connection. User authentication is accomplished through realm authentication. Machine authentication is accomplished as part of a realm certificate restriction, because the Pulse Client connection uses the machine certificate. If the certificate store holds more than one valid certificate for the connection, Pulse Client opens a dialog box that prompts the user to select a certificate.

The following list summarizes the steps to configure a Pulse Client connection on a Windows endpoint that authenticates both the user and the machine. For detailed procedures on how to perform each configuration task, see the links at "Related Documentation" on page 40.

- Install a machine authentication certificate in the Local Computer personal certificate store of the Windows endpoint and configure the Pulse Secure server certificate server.
- Create a Pulse Client connection for the target Pulse Secure server. The connection type can be UAC (802.1X) or Connect Secure or Policy Secure (L3). The Connection is established option is typically set to Manually by the user or Automatically at user login.
- In the User Connection Preferences section of the connection properties, click the check box labeled **Select client certificate from machine certificate store**. This option enables the Pulse Client connection to perform the machine authentication as part of the Pulse Client connection attempt.
- Create a sign-in policy on the Pulse Secure server that specifies a user realm. The realm authentication server can be a System Local, Active Directory, or RSA ACE server.
- Configure a certificate restriction on the realm to enable the Pulse Secure server to request a client certificate. Be sure to enable the option labeled Only allow users with a client-side certificate signed by Trusted Client CAs to sign in. Because the Pulse Client connection is configured to use the machine certificate, the user authentication takes place by means of the realm certificate restriction.

Related Documentation

- "Using Device Certificates"

Configuring Location Awareness Rules for Pulse Client

The location awareness feature enables Pulse Client to recognize its location and then make the correct connection. For example, you can define rules so that a Pulse Client that is started in a remote location automatically establishes a VPN connection to Pulse Connect Secure, and then that same client automatically connects to Pulse Policy Secure when it is started in the corporate office. If Pulse Client detects that it is connected to the corporate LAN and it already has a VPN connection (for example, the VPN connection was suspended when the computer was put into hibernation), it first discovers that the VPN location awareness rules are no longer true, disconnects that VPN connection, and then evaluates the location awareness rules for the other configured connections.

Location awareness relies on rules you define for each Pulse Client connection. If the conditions specified in the rules resolve to TRUE, Pulse Client attempts to make the connection. If the conditions specified in the rules do not resolve to TRUE, Pulse Client tries the next connection. To set up the location awareness rules that select among many connections, you must define location awareness rules for each connection. Each location awareness rule is based on the endpoint's ability to reach an IP address or resolve a DNS name over a specified network interface.

The following location awareness example includes two connections. Each connection is configured to connect to only one target server. The first connection is a Pulse Policy Secure connection that resolves to TRUE when the endpoint is connected to the corporate LAN. The second connection is a Pulse Connect Secure connection that resolves to TRUE when the endpoint is located in a remote location. If Pulse Client detects that it is connected to the corporate LAN and it already has a VPN connection, it disconnects that VPN connection.

Pulse Policy Secure connection

```
If the DNS server that is reachable on the endpoint's physical network interface is one of
your organization's internal DNS servers, then establish the connection.
```

Pulse Connect Secure connection

```
If the DNS server that is reachable on the endpoint's physical network interface is not one
of your organization's internal DNS servers, and the DNS name of your Pulse Connect Secure
device resolves to the external facing IP address of the Pulse Connect Secure device, then
establish the connection.
```

Note: Connections can be set to manual, automatic, or controlled by location awareness rules. When the user logs in, Pulse Client attempts every connection in its connections list that is set to automatic or controlled by location awareness rules.

Note: To create a negative location awareness rule, you first create the positive state and then use rule requirement logic to use the rule as a negative condition.

To configure location awareness rules:

1. If you have not already done so, create a connection or open an existing connection.

   You can configure location awareness rules for SRX connections and Connect Secure or Policy Secure (L3) connections. Location awareness rules do not apply to UAC (802.1X) connections.

2. Click the Mode list, and then select one of the options: **User**, **Machine**, or **Machine or user**.

3. If you selected **User** as the Mode, Under Options, select **Connect automatically**. If you selected **Machine** or **Machine or User**, **Connect automatically** is enabled by default.

4. Under Location awareness rules, click **New**.

   Alternatively, you can select the check box next to an existing rule, and then click **Duplicate** to create a new rule that is based on an existing rule.

5. Specify a name and description for the rule.

6. In the Action list, select one of the following:

   - **DNS server**: Connect if the DNS server associated with the endpoint's network properties is (or is not) set to a certain value or set of values. Specify the DNS server IP address in the IP address box. Also specify a network interface on which the condition must be satisfied:
     - **Physical**: The condition must be satisfied on the physical interfaces on the endpoint.
     - **Pulse Secure**: The condition must be satisfied on the virtual interface that Pulse Client creates when it establishes a connection.
     - **Any**: Use any interface.

- **Resolve address**: Connect if the configured hostname or set of hostnames is (or is not) resolvable by the endpoint to a particular IP address. Specify the hostname in the DNS name box and the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

Note: Pulse Client evaluates IP and DNS policies on network interface changes. DNS lookups occur on DNS configuration changes or when the time-to-live setting (10 minutes) expires for a particular host record. If Pulse Client cannot resolve the host for any reason, it polls the configured DNS server list every 30 seconds. If the host had been resolved successfully previously and the time-to-live timer has not expired, the polling continues until the timer expires. If the host had not been resolved successfully previously, the resolution attempt fails immediately.

- **Endpoint Address**: Connect if a network adapter on the endpoint has an IP address that falls within or outside of a range or a set of ranges. Specify the IP address or addresses in the IP address box. Also specify a network interface on which the condition must be satisfied.

7. Click **Save Changes**.

   After you create the rule or rules, you must enable each rule you want to use for the connection. To enable a negative form of a rule, use a custom version of the rule. To enable location awareness rules:

8. In the list of connection awareness rules for a connection, select the check box next to each rule you want to enable.
9. To specify how to enforce the selected location awareness rules, select one of the following options:
   - **All of the above rules**: The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied.
   - **Any of the above rules**: The condition is TRUE and the connection is attempted when any select location awareness rule is satisfied.
   - **Custom**: The condition is TRUE and the connection is attempted only when all selected location awareness rules are satisfied according to the Boolean logic you specify in the Custom box. Use the Boolean condition to specify a negative location rule. For example, connect to Pulse Connect Secure when Rule-1 is false and Rule-2 is true. The Boolean logic in the custom box would be: "NOT Rule-1 AND Rule-2". The accepted Boolean operators are AND, OR, NOT, and the use of ( ).
10. 1Click **Save Changes**.

Pulse Policy Secure Component Set Options

A Pulse Client component set includes specific software components that provide Pulse Client connectivity and services.

Note: Pulse Client component set options affect Web-based installations only.

Component set options include the following choices:

- **All components**: Supports all Pulse Client connection types. Use the **All components** option when you want client endpoints to be able to connect to all supported Pulse Secure servers.
- **No components**: Updates existing Pulse Client configurations, for example, to add a new connection. Do not use this option for a new installation.

Creating a Pulse Client Component Set for Pulse Policy Secure

A Pulse Client component set includes specific software components that provide Pulse Client connectivity and services.

Note: Pulse Client component set options affect Web-based installations only.

To create a client component set:

1. From the admin console, select **Users > Pulse Secure > Components**.
2. Click **New** to create a new component set.
3. If you have not yet created a client connection set, select **Users > Pulse Secure > Connections** and create a new connection set. Or you can use the default client configuration, which permits dynamic connections, supports the outer username anonymous, and allows the client to automatically connect to Pulse Policy Secure or Pulse Connect Secure.
4. Specify a name for the client component set.
5. (Optional) Enter a description for this client component set.
6. Select a connection set that you have created, or use the default connection set.
7. For Pulse Client components, select one of the following options:
   - **All components**: Supports all Pulse Client connection types.
   - **No components**: Updates existing Pulse Client configurations, for example, to add a new connection. Do not use this setting for a new installation.
8. Click **Save Changes**.
9. After you create a component set, distribute the client to users through a role. When users access the role, the installer automatically downloads to the endpoint. The installer components and connections are applied to the endpoint client.

   If client connections associated with the component set for a role are changed even though the list of components has not, the existing configuration on the endpoint is replaced immediately if the endpoint is currently connected, or the next time the endpoint connects.

   If a user is assigned to multiple roles and the roles include different component sets, the first role in an endpoint's list of roles is the one that determines which client (component set) is deployed.

Endpoint Security Monitoring and Management for Pulse Policy Secure

You can configure Host Checker policies that verify the endpoint's operating system service pack, software version, or desktop application patch version compliance. Host Checker uses a list of the most current patch versions from the vendor for predefined rules in the Host Checker policy. Host Checker does not scan for non-security patches. Host Checker runs on Windows (Including Windows RT and Windows Phone) endpoints, Apple OS X and iOS endpoints, and on Google Android endpoints. The supported Host Checker features vary on each platform.

Note: Pulse Policy Secure releases 5.1 and later do not support custom patch assessment rules. The OPSWAT patch solution provides support for patch information monitoring and deployment. Host Checker downloads the OPSWAT SDK and uses it to detect the installed patch management software and the patch status (the list of missing patches as reported by the patch management software). To enable the patch management software to evaluate the patch status of the client machine, the administrator must configure a patch management policy to use for evaluating the patch status of endpoints.

Note: If a realm has a Host Checker policy enabled that is for desktop clients, and a mobile device user employs a browser on the mobile device to connect to the Web portal, the login is denied because the desktop Host Checker program is not compatible with the mobile client OS. If Pulse Mobile Client users are mapped to multiple roles, the login operation assigns them to a role where Host Checker is not enabled if possible. If all the roles have Host Checker enabled, the mobile users will not be allowed to login from the browser. You can create and enable Host Checker policies that are specific to each mobile operating system and then Host Checker runs when Pulse Client connects to the server.

Pulse Policy Secure and Host Checker manage the flow of information between the corresponding pairs of TNC-based integrity measurement collectors (IMCs) and integrity measurement verifiers (IMVs). IMCs are software modules that run on the host and collect information such as antivirus, antispyware, patch management, firewall, and other configuration and security information about the host. IMVs are software modules that run on Pulse Connect Secure and verify a particular aspect of a host's integrity. Each IMV works with the corresponding IMC on the Pulse Client endpoint to verify that the endpoint meets the Host Checker rules. IMCs scan the endpoint frequently for changes in security status. For example, if the user turns off virus checking, the IMC can detect this and then trigger a new check to make sure the modified system complies with the requirements of the Host Checker policy. You can configure Host Checker to monitor third-party IMCs installed on client computers by using third-party IMVs that are installed on a remote IMV server.

You obtain the most current patch version information from a Pulse Secure staging site. You can manually download and import the list into the Pulse Secure gateway, or you can automatically import the list from the Pulse Secure staging site or your own staging site at a specified interval.

Monitoring is based on one or more specified products or on specific patches, though not in the same policy. For example, you could check for Internet Explorer Version 7 with one policy, and Patch MSOO-039: SSL Certificate Validation Vulnerabilities with a second policy. Then, apply both policies to endpoints at the role or realm level to ensure that the user has the latest browser version with a specific patch. In addition, for Microsoft products, you can specify the severity level of patches that you want to ignore. For example, you could ignore low or moderate threats.

When you deploy Pulse Client, Host Checker is included with the installer. You can invoke Host Checker at the role level or the realm level to specify access requirements for endpoints seeking authentication. Host Checker policies that are implemented at the realm level occur before the user is authenticated. Host Checker policies at the role level are implemented after authentication but before the user is permitted to access protected resources. When an endpoint first connects to Pulse Connect Secure, the latest version of the IMC downloaded to the host computer. The initial check takes about 10-20 seconds to run. Outdated IMC files are automatically updated at subsequent checks.

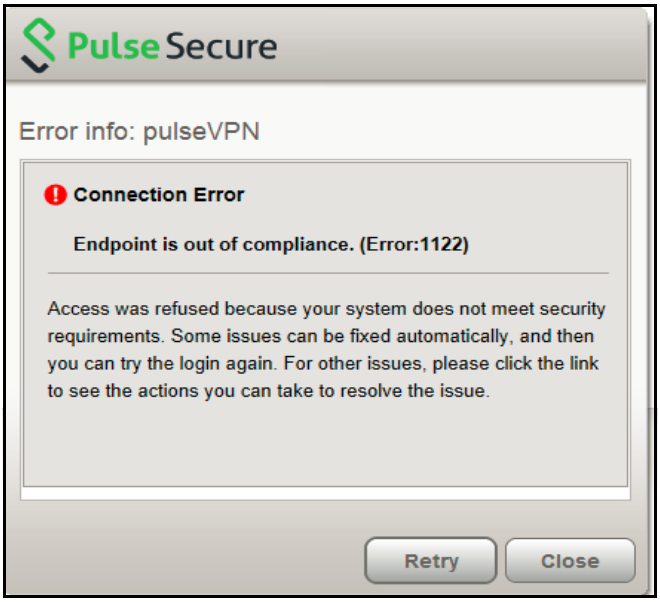
Note: The first time an endpoint connects to a Pulse Connect Secure that has a patch assessment policy, if the connection is a Layer 2 connection, the IMC cannot download. In this case, you should configure a remediation role that displays instructions to direct the user to retry with a Layer 3 connection or to contact the administrator.

Remediation Options

Host Checker can identify issues on an endpoint. However, Host Checker and Pulse Connect Secure cannot resolve issues, that is, perform remediation tasks, on non-compliant endpoints. To repair those issues Pulse Connect Secure supports the following remediation options:

- **Instructions to the user**: The Pulse Connect Secure can send a message to the user describing the non-compliant patches or software and a link to where the user can obtain the required software. Figure 24 shows a typical Pulse Client remediation message.

  Figure 24 Pulse Client Remediation Instructions



- **Initiate SMS/SCCM remediation**: For remediation using Microsoft System Center Configuration Manager (ConfigMgr or SCCM), formerly Systems Management Server (SMS), a preinstalled SMS/SCCM client on the endpoint is triggered by Host Checker to get patches from a preconfigured SMS/SCCM server. This mechanism installs only those patches that are published on the SMS/SCCM server.

Related Documentation

- "Issuing a Remediation Message with Pulse Policy Secure"
- "Using SMS/SCCM Remediation with Pulse Policy Secure"
- "Patch Management Info Monitoring and Patch Deployment"

Issuing a Remediation Message with Pulse Policy Secure

If a Host Checker policy finds that an endpoint is not in compliance, Host Checker can display a message through the Pulse Client interface that includes custom instructions and reason strings on how to bring the endpoint into conformance. The user must perform the steps described in the message before the endpoint is allowed to access protected resources.

To enable a remediation message for a Host Checker policy:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to create a new Host Checker policy.

   For detailed information about Host Checker Rule Settings, see the Pulse Policy Secure documentation at the Pulse Secure website (www.pulsesecure.net).
3. As part of the Host Checker Policy, select **Enable Custom Instructions**.

   When you select this option, a text box appears. Enter the instructions to display to the user on the Host Checker remediation page. You can use the following HTML tags to format text and to add links to resources such as policy servers or web sites: <i>, <b>,
, <font>, and <a href>. For example:

```
You do not have the latest signature files.

<a href="www.example.com">Click here to download the latest signature files.</a>
```

4. Optionally, select **Send reason strings**. Select this option to display a message to users (called a reason string) that is returned by Host Checker or IMV and that explains why the client machine does not meet the Host Checker policy requirements. Reason strings describe to users what the IMV is checking on the client machine. This option applies to predefined rules, to custom rules, and to third-party IMVs that use extensions in the Pulse Secure TNC SDK.
5. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse Client users.

Related Documentation

- "Endpoint Security Monitoring and Management for Pulse Policy Secure"
- "Using SMS/SCCM Remediation with Pulse Policy Secure"

Using SMS/SCCM Remediation with Pulse Policy Secure

Pulse Client supports the SMS/SCCM download method for patch deployment. If the Pulse Policy Secure is configured for the SMS/SCCM method for patch deployment, the Pulse Client endpoint must have the SMS/SCCM client already installed on the endpoint, otherwise remediation fails.

Endpoints configured with SMS/SCCM for software management typically poll the server for updates every fifteen minutes or longer. In a worst-case scenario, clients that are not in compliance with existing Host Checker software requirements might have to wait until the next update interval to login. Using the SMS/SCCM download method, you can force the client to initiate the software update immediately after the patch assessment check. If a user attempts to log in, and the endpoint does not have a required software version for compliance with a Host Checker patch assessment policy, Host Checker immediately notifies the client to poll the server for an immediate update. The client receives notification that an SMS/SCCM update has started.

To configure SMS/SCCM to update the client when notified, set the advertisement time on the SMS/SCCM to As soon as possible.

You assign clients to a particular group or collection on the SMS/SCCM server and then server can advertise patches for that collection. You can configure roles on the Pulse Policy Secure that correspond to collections and SMS/SCCM can send the appropriate patches for a particular role.

You must have the SMS/SCCM client installed and configured correctly on endpoints, and the SMS/SCCM server must be reachable. In a Layer 2 network, Host Checker is performed before the endpoint is connected to the network. Host Checker can obtain the IP address of the SMS/SCCM server configured for the client. If the endpoint is out of compliance and remediation is necessary, Host Checker pings the server IP address every 15 seconds until the server can be notified to update the client.

You should inform users of the expected behavior if this feature is enabled, as there is no notification to the user until the SMS/SCCM sends back the advertisement.

To enable SMS/SCCM assessment and remediation:

1. In the admin console, select **Authentication > Endpoint Security > Host Checker**.
2. In the Policies section, click **New** to create a new Host Checker policy.
3. Under Patch Remediation Options, select **SMS/SCCM Patch Deployment**.
4. Click **Save Changes**.

Be sure to include the Host Checker policy in the realm or role you configure for Pulse Client users.

Related Documentation

- "Endpoint Security Monitoring and Management for Pulse Policy Secure"
- "Issuing a Remediation Message with Pulse Policy Secure"

Patch Management Info Monitoring and Patch Deployment

Configuration and Migration Options for Deprecated Custom: Patch Assessment Rules

With Release 8.1/5.1, the OPSWAT patch solution provides support for patch information monitoring and deployment. Host Checker downloads the OPSWAT SDK and uses it to detect the installed patch management software and the patch status (the list of missing patches as reported by the patch management software). To enable the patch management software to evaluate the patch status of the client machine, the administrator must configure a patch management policy to use for evaluating the patch status of endpoints.

Custom patch assessment rules are not supported beginning in Release 8.1/5.1. The existing patch management rules will be converted to dummy rules during the migration. You can delete the existing rules or convert them to predefined: patch management rules.

To delete the custom patch assessment rules.

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Select the check box to back up the configuration and the XML file that contains Host Checker, realms, and role details.

   Figure 25 shows the configuration page for Host Checker.
3. Under Delete deprecated Custom: Patch Assessment rules, select **Delete**.

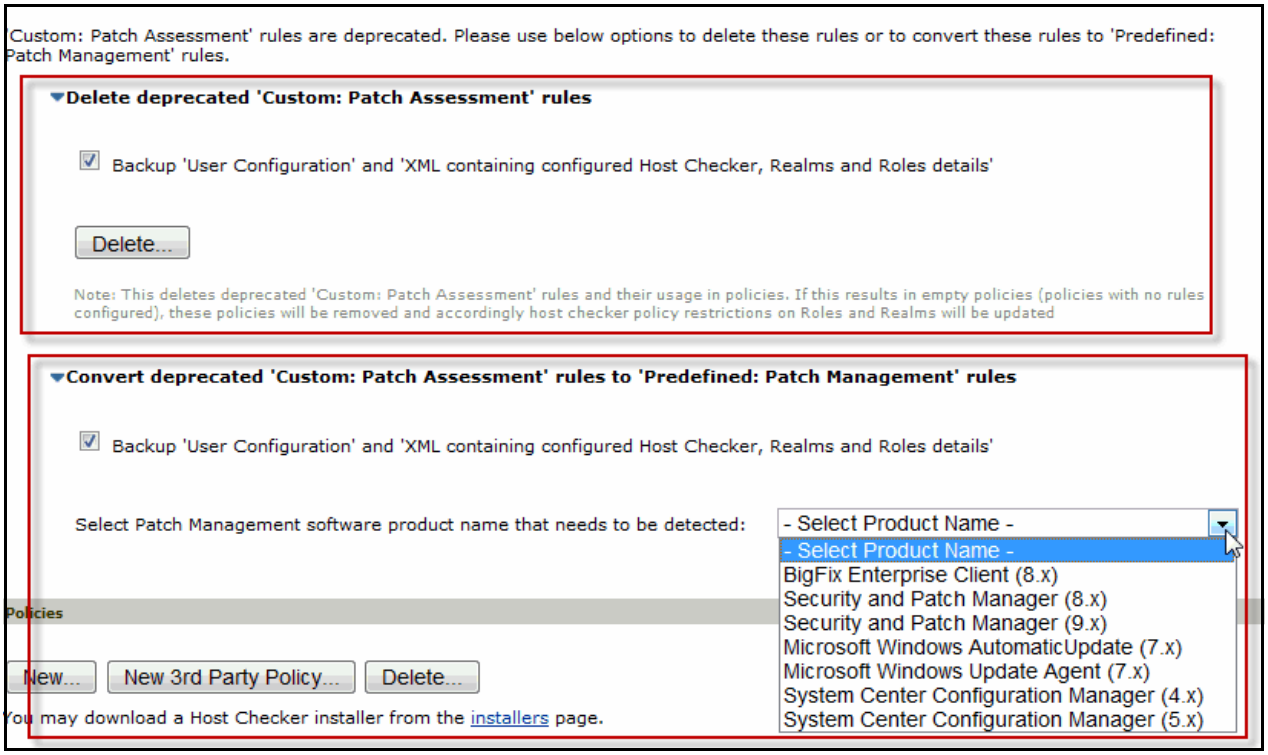
The Result:

Displays a confirmation page with the list of deprecated Custom:Patch Assessment rules and the policies in which they are configured. It also lists the Rule Expression for the respective policies which will be changed and the list of policies that becomes empty because of deletion of above rules. You need to click on Confirm if you want to continue deletion of deprecated rules, otherwise click on Cancel.

To convert the existing Shavlik rules to Opswat rules:

1. Select **Authentication > Endpoint Security > Host Checker**.
2. Select the check box to back up the configuration and the XML file that contains Host Checker, realms, and role details.Figure 25 shows the configuration page for Host Checker.

   Figure 25 Delete or Convert the Deprecated Patch Assessment Rules



3. Select the patch management software that you will use to convert custom patch assessment rules to predefined patch management rules and then click on convert.

Note: Convert button appears only after selecting the Patch management Software. If you select convert you can see the confirmation page which lists the deprecated Custom:Patch Assessment rules and the policies in which they are configured. It also lists the Rule Expression for the respective policies which will be changed. Click Confirm to continue replacement of deprecated Custom:Patch Assessment rules with Predefined: Patch Management rules, otherwise click Cancel.

Using a System Management Server

You can use a System Management Server (SMS) to provide a method for automatic updates to non-compliant software. From Release 8.1/5.1, only SMS/SCCM patch remediation is supported. You can enable SMS/SCCM patch remediation in the Predefined patch management policy page. The client machine must have the SCCM client installed and must be communicating to the SCCM server.

Pushing Pulse Client Configurations Between Pulse Secure servers of the Same Type

You can use the Push Configuration feature to centrally manage Pulse Client Connections, components, and uploaded Pulse Client packages. The Push Configuration feature enables you to copy all configuration settings or selected configuration settings from one Pulse Secure server to another Pulse Secure server of the same type, for example, from one Pulse Connect Secure server to another Pulse Connect Secure server.

The following notes apply to pushing configurations:

- You can push to a single Pulse Secure server or to multiple Pulse Secure servers in one operation. You can push up to 8 targets per push operation. You can run up to 25 push operations simultaneously. The maximum number of targets is 200. If a push to a target Pulse Secure server fails, the operation proceeds to the next target until all identified targets are updated. The results page displays the status and any problems encountered during the process.
- You can push to a Pulse Secure server that is a member of a cluster as long as the target Pulse Secure server is not a member of the same cluster as the source.
- Target Pulse Secure servers can refuse pushed configuration settings. The default is to accept.
- After an update, the target Pulse Secure server restarts its services. Brief interruptions might occur while the service restarts. We recommend that you push to targets when they are idle or when you can accommodate brief interruptions.
- Target Pulse Secure servers do not display a warning message when they receive a pushed configuration.
- The target Pulse Secure server automatically logs out administrators during the push process.
- The source and target Pulse Secure servers must have the same build version and number.
- The administrator account on the source Pulse Secure server must sign in to the target Pulse Secure server without any human intervention. For example, you cannot have dynamic credentials or multiple roles that are not merged as these both require manual interaction.

Before you use Push Configuration, you must configure your system according to the following conditions:

- You must map to the Administrators role, thereby creating a "super administrator" with full administration privileges. Modify **Authentication > Auth Servers > Administrator Server > Users** settings to add yourself to the Administrators role.
- The target Pulse Secure server administrator account must use static password authentication or two-factor tokens that do not use challenge/response type authentication. For example, certificates, Soft ID, and Defender Authentication are not supported. Modify **Administrators > Admin Realms > [Administrator Realm] > General** settings to select the proper authentication server for the administrator realm.

- Do not configure the administrator account in a way that requires the administrator to select a role to sign in to the target Pulse Secure server. For example, do not map a single user to multiple roles, including the Push Configuration administrator role, and then fail to merge those roles. We recommend creating an account exclusively for Push Configuration administrators to guarantee that the administrator does not need to choose a role during the sign-in process and to clearly distinguish the actions of Push Configuration administrators in your log files. Use the **Administrators > Admin Realms > [Administrator Realm] > Role Mapping** settings to set the appropriate role-mapping rules.

To push Pulse Client configurations from one Pulse Secure server to other Pulse Secure servers of the same type:

1. If you have not already done so, define the targets by selecting **Maintenance > Push Config > Targets**.
2. From the admin console, select **Maintenance > Push Config > Push Configuration**.
3. In the What to push box, select **Selected configuration** to display the configuration categories.
4. Scroll down the list and expand the item labeled "Pulse Secure".
5. Select the **Select All Configurations** check box to push all Pulse Client configurations on this Pulse Secure server. Or chose none, all, or selected items from the following categories:
   - **Pulse Secure Connections**: Connection sets and connections.
   - **Pulse Secure Components**: Component sets.
   - **Pulse Secure Versions**: Pulse Client packages that were uploaded to the Pulse Secure server.
6. Add the targets to the **Selected Targets** box.
7. Click **Push Configuration**.

Related Documentation

- "Enabling or Disabling Automatic Upgrades of Pulse Client"

Enabling or Disabling Automatic Upgrades of Pulse Client

After you deploy Pulse Client software to endpoints, software updates occur automatically. If you upgrade the Pulse Client configuration on your Pulse Secure server, updated software components are pushed to a client the next time it connects.

Note: If you configure Pulse Client to make 802.1X based connections, a reboot might be required on Windows endpoints when Pulse Client is upgraded.

Note: A bound endpoint receives connection set options and connections from its binding server, but it can have its Pulse Client software upgraded from any Pulse Secure server that has the automatic upgrade option enabled. During a client software upgrade the client loses connectivity temporarily.

Pulse Client software upgrades are enabled by default. To change the behavior of Pulse Client upgrades:

1. From the admin console, select **Maintenance > System > Options**.
2. Set or clear the **Enable automatic upgrade of Pulse Secure Clients** check box.

3. Click **Save Changes**.

Related Documentation

- "Upgrading Pulse Client"

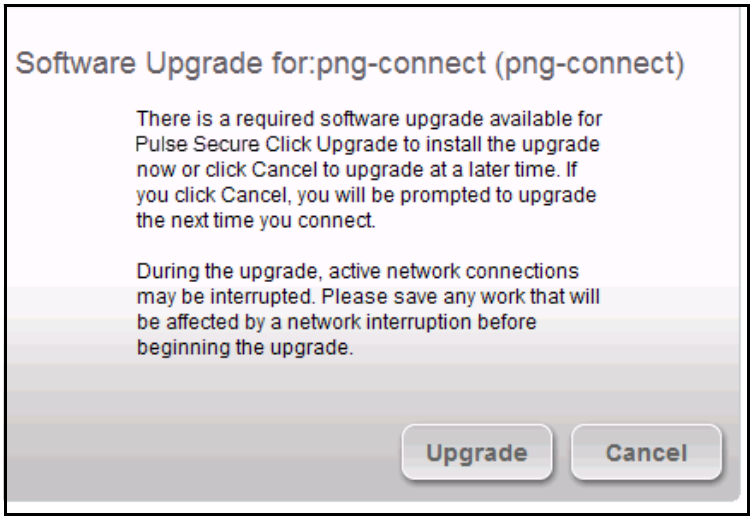
Upgrading Pulse Client

The software image for each supported Pulse Secure server includes a Pulse Client software package. When a newer version of Pulse Client is available, you can upload the new software to the Pulse Secure server. You can have more than one version of Pulse Client on a Pulse Secure server but only one Pulse Client package can be active. If you activate a new version of Pulse Client, and if the Pulse Secure server's automatic upgrade option is enabled, connected Pulse Clients display an upgrade prompt to the user. The user can choose to install the upgrade or cancel the operation. If a user cancels, the upgrade prompt appears each time the client connects to the server. During a client software upgrade Pulse Client loses connectivity temporarily.

Note: The automatic update feature is supported on Pulse Connect Secure and Pulse Policy Secure servers only. SRX gateways do not support automatic Pulse Client software updates.

Note: If you configure Pulse Client to make 802.1X based connections, a reboot might be required on Windows endpoints when Pulse Client is upgraded.

Figure 26 Pulse Client Upgrade Message



After you have staged the new Pulse Client software package in a location accessible to the Pulse Secure server, use the following procedure to upload the software to the Pulse Secure server:

1. In the device admin console, select **Users > Pulse Secure > Components**.
2. In the section labeled "Manage Pulse Secure Client Versions", click **Browse**, and then select the software package.
3. Click **Upload**.

Only one Pulse Client software package can be active at a time. After you upload a new package, you need to enable it.

To enable a Pulse Client package as the default:

1. In the admin console, select **Users > Pulse Secure > Components**.
2. In the section labeled "Manage Pulse Secure Client Versions", select the radio button next to a version, and then click **Activate**.

Related Documentation

- "Enabling or Disabling Automatic Upgrades of Pulse Client"

Using Device Certificates

This topic describes how to use device certificates. It includes the following information:

- "Understanding Device Certificates"
- "Understanding Self-Signed Certificates"
- "Importing a Device Certificate and Private Key"
- "Creating a Certificate Signing Request"
- "Importing a Signed Certificate Created from a CSR"
- "Understanding Intermediate Certificates"
- "Importing Intermediate CA Certificates"
- "Importing a Renewed Certificate That Uses the Existing Private Key"
- "Downloading a Device Certificate"
- "Using Device Certificates with Virtual Ports"

Understanding Device Certificates

A device certificate helps to secure network traffic to and from the Pulse Client service using elements such as your company name, a copy of your company's public key, the digital signature of the Certificate Authority (CA) that issued the certificate, a serial number, and an expiration date. The system also uses device certificates for secure communications with the Infranet Enforcer.

When receiving encrypted data from the system, the client's browser first verifies whether the device certificate is valid and whether the user trusts the CA that issued the certificate. If the user has not already indicated that they trust the certificate issuer, the Web browser prompts the user to accept or install the certificate.

The system supports X.509 device certificates in DER and PEM encode formats (file extensions include .cer, .crt, .der, and .pem) as well as PKCS #12 (file extensions include .pfx and .p12). The system also supports the following features:

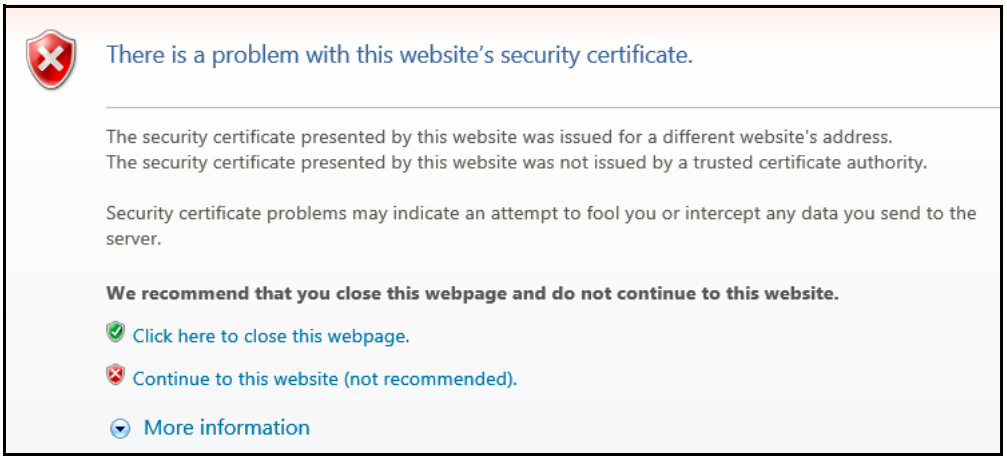
- Intermediate device CA certificates: Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate.
- Multiple device certificates: When using multiple device certificates, each certificate handles validation for a separate hostname or fully qualified domain name (FQDN) and can be issued by a different CA.

Note: Beginning with Connect Secure system software release 7.2, you can assign device certificates to the Connect Secure VLAN interfaces.

Understanding Self-Signed Certificates

When you initialize the system with the serial console, the system creates a self-signed certificate that enables you to immediately begin setting up the system. Users are prompted with a security alert each time they sign in because the certificate is not issued by a trusted CA. Figure 27 shows the security alert.

Figure 27 Security Alert When the Device Certificate Is Not Issued by a Trusted CA



Before promoting the system to production use, we recommend you replace the self-signed certificate with a certificate issued by a trusted CA.

Note: In Policy Secure deployments with ScreenOS Enforcers, you must use a CA-signed device certificate. If you use a self-signed certificate, the ScreenOS Enforcer does not allow a connection. Import a CA-signed device certificate into the Policy Secure and then import the certificate of the CA that signed the device certificate into the ScreenOS Enforcer.

Importing a Device Certificate and Private Key

The system uses certificates to verify itself to other network devices. A digital certificate is an electronic means of verifying your identity through a trusted third party, known as a Certificate Authority (CA). Your company might use its own enterprise CA server, or it might use a reputable third-party CA

To import an enterprise root server certificate and private key:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click **Import Certificate & Key** to display the configuration page.
3. Use one of the following options to complete the import procedure:
   - **If certificate file includes private key**: When the certificate and key are contained in one file.
   - **If certificate and private key are separate files**: When the certificate and key are in separate files.

- **Import via System Configuration file**: When the certificate and key are contained in a system configuration file. With this option, the system imports all of the certificates specified (including private keys and pending CSRs, but not the corresponding port mappings).

In the appropriate form, browse to the certificate and key files. If the file is encrypted, enter the password key.

4. Click **Import**.

Note: The Import Certificate and Key button is disabled on FIPS hardware platforms because importing private keys is not allowed. On a FIPS hardware platform, you must create a CSR and then import a signed certificate from the CA.

Creating a Certificate Signing Request

If your company does not own a digital certificate for its Web servers, you can create a certificate signing request (CSR) and then send the request to a CA for processing. When you create a CSR, a private key is created locally that corresponds to the CSR. If you delete the CSR at any point, this file is also deleted, prohibiting you from installing a signed certificate generated from the CSR.

To create a certificate signing request:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click **New CSR** to display the configuration page.
3. Complete the required information and click **Create CSR**.
4. Follow the on-screen instructions, which explain what information to send to the CA and how to send it.

When you submit a CSR to a CA authority, you might be asked to specify either the type of Web server on which the certificate was created or the type of Web server the certificate is for. Select "apache" (if more than one option with apache is available, select "any"). If you are prompted for the certificate format to download, select the standard format.

Do not send more than one CSR to a CA at one time. Doing so can result in duplicate charges.

Note: To view details of any pending requests that you previously submitted, click the Certificate Signing Request Details link.

Importing a Signed Certificate Created from a CSR

When you receive the signed certificate from the CA, import it.

To import a signed device certificate created from a CSR:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Under Certificate Signing Requests, click the **Pending CSR** link that corresponds to the signed certificate.
3. Under Import signed certificate, browse and select the certificate file you received from the CA, and then click **Import**.

Understanding Intermediate Certificates

Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate. The root certificate is issued by a root CA and is self-signed. Each intermediate certificate is issued by the certificate preceding it in the chain.

To use chained certificates in your deployment, you must ensure that the server (Policy Secure or Connect Secure) and client (Web browser) together contain the entire certificate chain. For example, you can secure traffic using a chain that stems from a VeriSign root certificate. If your users' browsers come preloaded with VeriSign root certificates, you need to install only the lower-level certificates in the chain. When your users sign in, the system presents any required certificates within the chain to the browser to secure the transaction. The system creates the proper links in the chain using the root certificate's IssuerDN. If the system and browser together do not contain the entire chain, the user's browser does not recognize or trust the device certificate because it is issued by another certificate instead of by a trusted CA.

You can upload one or more intermediate CAs in a PEM file. The entire chain must be sent to the client in descending order, starting with the root certificate.

Within a certificate hierarchy, one or more intermediate certificates are branched off a single root certificate. The root certificate is issued by a root CA and is self-signed. Each intermediate certificate is issued by the certificate preceding it in the chain.

To use chained certificates in your deployment, you must install the appropriate client-side certificates in each user's Web browser and then upload the corresponding CA certificates to the Pulse Client Service Intermediate CA store. Use one of the following methods to upload the certificate chain:

- Import the entire certificate chain in one file. The file must contain the root certificate and any sub certificates whose parents are in the file or already imported. You can include certificates in any order in the import file.
- Import the certificates one at a time in descending order. You must install the root certificate first, and then install the remaining chained certificates in descending order.

If you follow one of these methods, the system automatically chains the certificates together in the correct order and displays them hierarchically in the admin console.

Note: If you install multiple certificates in a user's Web browser, the browser prompts the user to choose which certificate to use when signing in.

Importing Intermediate CA Certificates

To import an intermediate CA certificate:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click the **Intermediate Device CAs** link to display the management page.
3. Click **Import CA certificate**.
4. Browse to the certificate file, select it, and click **Import Certificate** to complete the import operation.

Importing a Renewed Certificate That Uses the Existing Private Key

You can renew a device certificate in two ways:

- **Submit a new CSR to a CA**: This process is more secure because the CA generates a new certificate and private key and retires the older private key. To use this renewal method, you must first create a CSR through the admin console.
- **Request renewal based on the CSR previously submitted to the CA**: This process is less secure, because the CA generates a certificate that uses the existing private key.

When you order a renewed certificate, you must either resubmit your original CSR or ensure that the CA has a record of the CSR that you submitted for your current certificate.

To import a renewed device certificate that uses the existing private key:

1. Follow your CA's instructions for renewing a certificate that you previously purchased through them. Be sure to specify the same information you used in the original CSR. Your CA uses this information to create a new certificate that corresponds to the existing key.

Note: Even though you specify the same information used in the original CSR, your root CA might have different serial numbers and keys from the original. You might need to support both new client and old client certificates during the transition period, which also requires that you maintain two root CA certificates (your existing certificate and the renewed certificate), at least temporarily.

2. Select **System > Configuration > Certificates > Device Certificates**.
3. Click the link that corresponds to the certificate you want to renew.
4. Click **Renew Certificate** to display the page.
5. In the Renew the Certificate form, browse to the renewed certificate file, enter the password for the certificate key, and click **Import**.

Downloading a Device Certificate

You download the device certificate to your local host so that you can import it into other network devices as needed.

To download a device certificate:

1. Select **System > Configuration > Certificates > Device Certificates**.
2. Click the link of the device certificate you want to download to display the configuration page.
3. Click the **Download** link.
4. Save the file to the desired location.

Using Device Certificates with Virtual Ports

Virtual ports can be used to create multiple fully qualified domain names for user sign-in.

When a user tries to sign in using the IP address defined in a virtual port, the system uses the certificate associated with the virtual port to initiate the SSL transaction and for NetScreen Address Change Notification (NACN) communications with the Infranet Enforcer.

You must associate the signed certificate with the port that is connected to the Infranet Enforcer. You can use the same port and certificate for OAC or Pulse Client. Or, you can import other signed certificates and associate them with ports connected to OAC.

You can implement digital certificate security with virtual ports in either of the following ways:

- **Associate all hostnames with a single certificate**: With this method, you use a single wildcard certificate to validate the identity of all system hostnames, regardless of which hostname is used to sign into. A wildcard certificate includes a variable element in the domain name, making it possible for users who sign in from multiple hosts to map to the "same" domain. For example, if you create a wildcard certificate for *.yourcompany.com, the system uses the same certificate to validate its identity to users who sign in to employees.yourcompany.com as it does to users who sign into partners.yourcompany.com.
- **Associate each hostname with its own certificate**: With this method, you associate different hostnames with different certificates. Create a virtual port for each hostname. A virtual port activates an IP alias on a physical port. For example, you can create two virtual ports on a single appliance, mapping the first virtual port to the IP address 10.10.10.1 (sales.yourcompany.com) and the second virtual port to the IP address 10.10.10.2 (partners.yourcompany.com). Then you can associate each of these virtual ports with its own certificate, ensuring that users authenticate through different certificates.

To associate certificates with virtual ports:

1. Create the virtual ports.
2. Import the device certificates.
3. Associate the device certificates with the virtual ports:
    1. Select **System > Configuration > Certificates > Device Certificates**.
    2. Click the link of the device certificate you want to configure to display the configuration page.
    3. Use the controls in the "Present certificate on these ports" section to associate ports with the certificate.

Note: You can assign only one device certificate to the Management Port. If you assign a certificate other than the default device certificate to the Management Port, the default device certificate is automatically deselected as the default. If you do not select a device certificate for the Management Port, the system uses the default device certificate that is presented on the Internal port. You cannot assign certificates to Management Port VIPs.