



Pulse Connect Secure

Getting Started Guide

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

www.pulsesecure.net

Copyright Notice

This product includes the Envoy SNMP Engine, developed by Epilogue Technology, an Integrated Systems Company. Copyright © 1986-1997, Epilogue Technology Corporation. All rights reserved. This program and its documentation were developed at private expense, and no part of them is in the public domain.

This product includes memory allocation software developed by Mark Moraes, copyright © 1988, 1989, 1993, University of Toronto.

This product includes FreeBSD software developed by the University of California, Berkeley, and its contributors. All of the documentation and software included in the 4.4BSD and 4.4BSD-Lite Releases is copyrighted by the Regents of the University of California. Copyright © 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994. The Regents of the University of California. All rights reserved.

GateD software copyright © 1995, the Regents of the University. All rights reserved. Gate Daemon was originated and developed through release 3.0 by Cornell University and its collaborators. Gated is based on Kirton's EGP, UC Berkeley's routing daemon (routed), and DCN's HELLO routing protocol. Development of Gated has been supported in part by the National Science Foundation. Portions of the GateD software copyright © 1988, Regents of the University of California. All rights reserved. Portions of the GateD software copyright © 1991, D. L. S. Associates.

This product includes software developed by Maker Communications, Inc., copyright © 1996, 1997, Maker Communications, Inc.

Products made or sold by Pulse Secure or components thereof might be covered by one or more of the following patents that are owned by or licensed to Pulse Secure: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

Pulse Secure, the Pulse Secure logo, NetScreen, and ScreenOS are registered trademarks of Pulse Secure, LLC. in the United States and other countries. Pulse and Pulse e are trademarks of Pulse Secure, LLC. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Copyright © 2015 Pulse Secure, LLC. All rights reserved. Printed in the USA.

FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with the instruction manual, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.



Caution: Changes or modifications to this product could void the user's warranty and authority to operate this device and may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

U.S. Government Rights

Commercial software and commercial software documentation: This documentation is commercial computer software documentation and the products (whether hardware or software) covered by this documentation are or contain commercial computer software. Government users are subject to the Pulse Secure, LLC. standard end user license agreement and any applicable provisions of the FAR and its supplements. No further rights are granted.

Products (whether hardware or software) covered by, and information contained in, this documentation are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical, biological weapons end uses or end users, whether direct or indirect, are strictly prohibited. Export or re-export to countries subject to U.S. embargo or to entities identified on US export exclusion lists, including, but not limited to, the denied persons and specially designated national lists, is strictly prohibited.

Disclaimer

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR PULSE SECURE REPRESENTATIVE FOR A COPY.

Contents

About This Guide	5
Objectives	5
Audience	5
Document Conventions	5
Obtaining Documentation	5
Documentation Feedback	5
Requesting Technical Support	5
PART 1	7
Chapter 1	8
Pulse Connect Secure Solution and Traffic	8
Pulse Connect Secure Solution Overview	8
Securing Traffic with Pulse Connect Secure	9
Chapter 2	11
User Authentication	11
Authenticating Users with Existing Servers	11
Chapter 3	12
Resource Intermediation	12
Fine-Tuning Access to Pulse Connect Secure and the Resources It Intermediates	12
Chapter 4	13
Host Checker	13
Protecting Against Infected Computers and Other Security Concerns	13
Chapter 5	14
Redundancy	14
Ensuring Redundancy in the Pulse Connect Secure Environment	14
PART 2	15
Chapter 6	16
Pulse Connect Secure	16
Configuring Pulse Connect Secure	16
PART 3	17
Chapter 7	18
Administrator Settings	18
Default Settings for Administrators	18
Trusted Server List	18

Chapter 8	21
Test Scenario Creation	21
Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices	21
Using the Test Scenario	21
Chapter 9	23
Resource Intermediation	23
Creating a Seamless Integration Between Pulse Connect Secure and the Resources It Intermediates	23
Chapter 10	24
User Access and End-User Interface	24
Enabling Users on a Variety of Computers and Devices to Use Pulse Connect Secure	24
Providing PCS for My International Users	24
Verifying User Accessibility	24
Chapter 11	26
Admin and End-User Interface Customization	26
Making the Pulse Connect Secure Interface Match My Company's Look-and-Feel	26
Customizable Admin and End-User UIs	26
Chapter 12	28
Serial Console	28
Using the Serial Console	28
Rolling Back to a Previous System State Through the Serial Console	29
Resetting a Pulse Connect Secure Device to the Factory Setting Using the Serial Console	29
Performing Common Recovery Tasks with the Serial Console	30
PART 4	32
Index	33

About This Guide

Objectives

The Pulse Connect Secure Getting Started Guide describes how to use the Pulse Secure branding tool to customize the Pulse Secure client interface.



Audience

The Pulse Connect Secure Getting Started Guide is for developers who are responsible for customizing Pulse Secure client software.

Document Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.

Obtaining Documentation

To obtain the most current version of all Pulse Secure technical documentation, see the products documentation page at <https://www.pulsesecure.net/techpubs>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using one of the following methods:

- Document name
- Page number
- Software release version

Requesting Technical Support

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

- Product warranties—For product warranty information, visit <http://www.pulsesecure.net>.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.pulsesecure.net/support>

- Search for known bugs: <http://www.pulsesecure.net/support>
- Find product documentation: <https://www.pulsesecure.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base:
<http://www.pulsesecure.net/support>
- Download the latest versions of software and review release notes:
<http://www.pulsesecure.net/support>
- Search technical bulletins for relevant hardware and software notifications:
<http://www.pulsesecure.net/support>
- Join and participate in the Pulse Secure, LLC Community Forum:
<http://www.pulsesecure.net/support>
- Open a case online in the CSC Case Management tool: <http://www.pulsesecure.net/support>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
<http://www.pulsesecure.net/support>

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 <http://www.pulsesecure.net/support>.
- Call Phone: 1-844 751 7629 (Toll Free, US).

For international or direct-dial options in countries without toll-free numbers, see
<http://www.pulsesecure.net/support>

PART 1

Overview

- **Pulse Connect Secure Solution and Traffic**
- **User Authentication**
- **Resource Intermediation**
- **Host Checker**
- **Redundancy**

Chapter 1

Pulse Connect Secure Solution and Traffic

- **Pulse Connect Secure Solution Overview**
- **Securing Traffic with Pulse Connect Secure**

Pulse Connect Secure Solution Overview

The Pulse Connect Secure enables you to give employees, partners, and customers secure and controlled access to your corporate data and applications including file servers, Web servers, native messaging and e-mail clients, hosted servers, and more from outside your trusted network using just a Web browser.

Pulse Connect Secure provides robust security by intermediating the data that flows between external users and your company's internal resources. Users gain authenticated access to authorized resources through an extranet session hosted by the appliance.

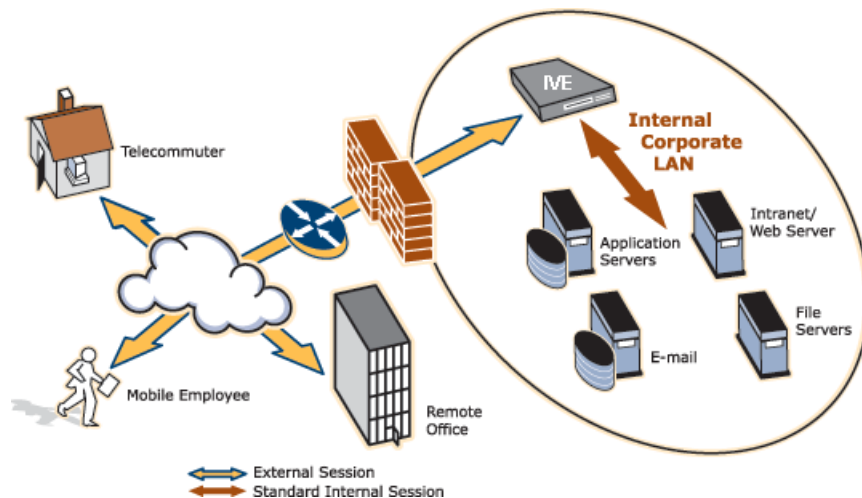
During intermediation, Pulse Connect Secure receives secure requests from the external authenticated users and then makes requests to the internal resources on behalf of those users. By intermediating content in this way, Pulse Connect Secure eliminates the need to deploy extranet toolkits in a traditional DMZ or provision a remote access VPN for employees.

To access the intuitive Pulse Connect Secure home page, your employees, partners, and customers need only a Web browser that supports SSL and an Internet connection. This page provides the window from which your users can securely browse Web or file servers, use HTML-enabled enterprise applications, start the client/server application proxy, begin a Windows, Citrix, or Telnet/SSH terminal session, access corporate e-mail servers, start a secured layer 3 tunnel, or schedule or attend a secure online meeting.



Note: These capabilities depend upon the Pulse Connect Secure product and upgrade options you have purchased.

Figure 1: Pulse Connect Secure Working within a LAN



You can configure Pulse Connect Secure in the following ways:

- Provide users with secure access to a variety of resources. Pulse Connect Secure intermediates access to multiple types of applications and resources such as Web-based enterprise applications, Java applications, file shares, terminal hosts, and other client/server applications such as Microsoft Outlook, Lotus Notes, the Citrix ICA Client, and pcAnywhere. Additionally, administrators can provision an access method that allows full Layer 3 connectivity, providing the same level of access that a user would get if they were on the corporate LAN.
- Fine-tune user access to the appliance, resource types, or individual resources based on factors such as group membership, source IP address, certificate attributes, and endpoint security status. For

instance, you can use dual-factor authentication and client-side digital certificates to authenticate users to Pulse Connect Secure and use LDAP group membership to authorize users to access individual applications.

- Assess the security status of your users' computers by checking for endpoint defense tools such as current antivirus software, firewalls, and security patches. You can then allow or deny users access to the appliance, resource types, or individual resources based on the computer's security status.

Pulse Connect Secure acts as a secure, Application Layer gateway intermediating all requests between the public Internet and internal corporate resources. All requests that enter Pulse Connect Secure are already encrypted by the end user's browser, using SSL/HTTPS 128-bit or 168-bit encryption—unencrypted requests are dropped. Because Pulse Connect Secure provides a robust security layer between the public Internet and internal resources, administrators do not need to constantly manage security policies and patch security vulnerabilities for numerous different application and Web servers deployed in the public-facing DMZ.

Related Documentation

- **Securing Traffic with Pulse Connect Secure**
- **Authenticating Users with Existing Servers**
- **Fine-Tuning Access to Pulse Connect Secure and the Resources It Intermediates**
- **Creating a Seamless Integration Between Pulse Connect Secure and the Resources It Intermediates**
- **Protecting Against Infected Computers and Other Security Concerns**
- **Ensuring Redundancy in the Pulse Connect Secure Environment**
- **Making the Pulse Connect Secure Interface Match My Company's Look-and-Feel**
- **Enabling Users on a Variety of Computers and Devices to Use Pulse Connect Secure**
- **Providing PCS for My International Users**

Securing Traffic with Pulse Connect Secure

Pulse Connect Secure enables you to secure access to a wide variety of applications, servers, and other resources through its remote access mechanisms. Once you have chosen which resource you want to secure, you can then choose the appropriate access mechanism.

For instance, if you want to secure access to Microsoft Outlook, you can use the Secure Application Manager (SAM). The Secure Application Manager intermediates traffic to client/server applications including Microsoft Outlook, Lotus Notes, and Citrix. Or, if you want to secure access to your company Intranet, you can use the Web rewriting feature. This feature uses Pulse Connect Secure's Content Intermediation Engine to intermediate traffic to Web-based applications and Web pages.

Pulse Connect Secure includes remote access mechanisms that intermediate the following types of traffic:

- Web-based traffic, including Web pages and Web-based applications—Use the Web rewriting feature to intermediate this type of content. The Web rewriting feature includes templates that enable you to easily configure access to applications such as Citrix, OWA, Lotus iNotes, and Sharepoint. In addition, you can use the Web rewriting custom configuration option to intermediate traffic from a wide variety of additional Web-based applications and Web pages, including custom-built Web applications.
- Java applets, including Web applications that use Java applets—Use the hosted Java applets feature to intermediate this type of content. This feature enables you to host Java applets and the HTML pages that they reference directly on Pulse Connect Secure rather than maintaining a separate Java server.
- File traffic, including file servers and directories—Use the file rewriting feature to intermediate and dynamically "webify" access to file shares. The file rewriting feature enables you to secure traffic to a variety of Windows and UNIX based servers, directories, and file shares.
- Client/server applications—Use the Secure Application Manager (SAM) feature to intermediate this type of content. SAM comes in two varieties (Windows and Java versions, or WSAM and JSAM). The WSAM and JSAM features include templates that enable you to easily configure access to

applications such as Lotus Notes, Microsoft Outlook, NetBIOS file browsing, and Citrix. In addition, you can use the WSAM and JSAM custom configuration options to intermediate traffic from a wide variety of additional client/server applications and destination networks.

- Telnet and SSH terminal emulation sessions—Use the Telnet/SSH feature to intermediate this type of content. This feature enables you to easily configure access to a variety of networked devices that utilize terminal sessions including UNIX servers, networking devices, and other legacy applications.
- Windows Terminal Servers and Citrix server terminal emulation sessions— Use the Terminal Services feature to intermediate this type of content. This feature enables you to easily configure access to Windows Terminal Servers, Citrix MetaFrame Servers, and Citrix Presentation Servers (formerly known as Nfuse servers). You can also use this feature to deliver the terminal services clients directly from Pulse Connect Secure, eliminating the need to use another Web server to host the clients.
- E-mail clients based on the IMAP4, POP3, and SMTP protocols—Use the email client feature to intermediate this type of content. This feature enables you to easily configure access to any corporate mail server based on the IMAP4, POP3, and SMTP protocols, such as Microsoft Exchange Server and Lotus Notes Mail servers.
- All network traffic—Use the VPN Tunneling feature to create a secure, Layer 3 tunnel over the SSL connection, allowing access to any type of application available on the corporate network. This feature enables you to easily connect remote users into your network by tunneling network traffic over port 443, enabling users full access to all of your network resources without configuring access to individual servers, applications, and resources.

Related Documentation

- **[Pulse Connect Secure Solution Overview](#)**

Chapter 2

User Authentication

- **Authenticating Users with Existing Servers**

Authenticating Users with Existing Servers

You can easily configure Pulse Connect Secure to use your company's existing servers to authenticate your end users—Users do not need to learn a new username and password to access the Pulse Connect Secure device. Pulse Connect Secure supports integration with LDAP, RADIUS, NIS, Windows NT Domain, Active Directory, eTrust SiteMinder, SAML, and RSA ACE/Servers.

Or, if you do not want to use one of these standard servers, you can store usernames and credentials directly on Pulse Connect Secure and use Pulse Connect Secure itself as an authentication server. In addition, you can choose to authenticate users based on attributes contained in authentication assertions generated by SAML authorities or client-side certificates. Or, if you do not want to require your users to sign into Pulse Connect Secure, you can use the Pulse Connect Secure anonymous authentication server, which allows users to access the Pulse Connect Secure device without providing a username or password.



Note: Pulse Mobile client supports only one case of dual-factor authentication, where the client certificate is the primary and local auth is the secondary.

Related Documentation

- **Pulse Connect Secure Solution Overview**

Chapter 3

Resource Intermediation

- **Fine-Tuning Access to Pulse Connect Secure and the Resources It Intermediates**

Fine-Tuning Access to Pulse Connect Secure and the Resources It Intermediates

In addition to using authentication servers to control access to Pulse Connect Secure, you can control access to Pulse Connect Secure and the resources it intermediates using a variety of additional client-side checks. Pulse Connect Secure enables you to create a multilayered approach to protect Pulse Connect Secure and your resources:

1. First, you can perform preauthentication checks that control user access to the Pulse Connect Secure sign-in page. For instance, you might configure Pulse Connect Secure to check whether or not the user's computer is running a particular version of Norton Antivirus. If it is not running, you can determine that the user's computer is unsecure and disable access to the Pulse Connect Secure sign-in page until the user has updated the computer's antivirus software.
2. Once a user has successfully accessed the Pulse Connect Secure sign-in page, you can perform realm-level checks to determine whether he can access the Pulse Connect Secure end-user home page. The most common realm-level check is performed by an authentication server. (The server determines whether the user enters a valid username and password.) You can perform other types of realm-level checks, however, such as checking that the user's IP address is in your network or that the user is using the Web browser type that you specify.

If a user passes the realm-level checks that you specify, the user can access the Pulse Connect Secure end-user home page. Otherwise, Pulse Connect Secure does not enable the user to sign in, or Pulse Connect Secure displays a "stripped down" version of the home page that you create. Generally, this stripped down version contains significantly less functionality than is available to your standard users because the user has not passed all of your authentication criteria. Pulse Connect Secure provides extremely flexible policy definitions, enabling you to dynamically alter end-user resource access based on corporate security policies.

3. After Pulse Connect Secure successfully assigns a user to a realm, the appliance maps the user to a role based on your selection criteria. A role specifies which access mechanisms a selected group of users can access. It also controls session and UI options for that group of users. You can use a wide variety of criteria to map users to roles. For instance, you can map users to different roles based on endpoint security checks or on attributes obtained from an LDAP server or client-side certificate.
4. In most cases, a user's role assignments control which individual resources the user can access. For instance, you might configure access to your company's Intranet page using a Web resource profile and then specify that all members of the Employees role can access that resource.

However, you can choose to further fine-tune access to individual resources. For instance, you may enable members of the Employees role to access your company's Intranet (as described earlier), but add a resource policy detailed rule that requires users to meet additional criteria to access the resource. For example, you may require users to be members of the Employees role and to sign into Pulse Connect Secure during business hours to access your company Intranet.

Related Documentation

- **Pulse Connect Secure Solution Overview**

Chapter 4

Host Checker

- **Protecting Against Infected Computers and Other Security Concerns**

Protecting Against Infected Computers and Other Security Concerns

Pulse Connect Secure enables you to protect against viruses, attacks, and other security concerns using the Host Checker feature. Host Checker performs security checks on the clients that connect to Pulse Connect Secure. For instance, you can use Host Checker to verify that end-user systems contain up-to-date antivirus software, firewalls, critical software hotfixes, and other applications that protect your users' computers. You can then enable or deny users access to the Pulse Connect Secure sign-in pages, realms, roles, and resources based on the results that Host Checker returns. Or, you can display remediation instructions to users so they can bring their computers into compliance.

You can also use Host Checker to create a protected workspace on clients running Windows 2000 or Windows XP. Through Host Checker, you can enable the Secure Virtual Workspace (SVW) feature to create a protected workspace on the client desktop, ensuring that any end user signing in to your intranet must perform all interactions within a completely protected environment. Secure Virtual Workspace encrypts information that applications write to disk or the registry and then destroys all information pertaining to itself or Pulse Connect Secure session when the session is complete.

You can also secure your network from hostile outside intrusion by integrating your Pulse Connect Secure with a Juniper Networks Intrusion Detection and Prevention (IDP) sensor. You can use IDP devices to detect and block most network worms based on software vulnerabilities, non-file-based Trojan horses, the effects of Spyware, Adware, and Key Loggers, many types of malware, and zero day attacks through the use of anomaly detection.

Related Documentation

- **Pulse Connect Secure Solution Overview**

Chapter 5

Redundancy

- **Ensuring Redundancy in the Pulse Connect Secure Environment**

Ensuring Redundancy in the Pulse Connect Secure Environment

You can ensure redundancy in your Pulse Connect Secure environment using the clustering feature. With this feature, you can deploy two or more appliances as a cluster, ensuring no user downtime in the rare event of failure and stateful peering that synchronizes user settings, system settings, and user session data.

These appliances support active/passive or active/active configurations across a LAN. In Active/Passive mode, one Pulse Connect Secure device actively serves user requests while the other Pulse Connect Secure device runs passively in the background to synchronize state data. If the active Pulse Connect Secure device goes offline, the passive Pulse Connect Secure device automatically starts servicing user requests. In active/active mode, all the machines in the cluster actively handle user requests sent by an external load balancer. The load balancer hosts the cluster VIP and routes user requests to Pulse Connect Secure defined in its cluster group based on source-IP routing. If a Pulse Connect Secure device goes offline, the load balancer adjusts the load on the other active Pulse Connect Secure device.



Note: WAN clustering is not supported on the Pulse Secure Gateways, except as it relates to campus networks. In a well-connected campus network, where the connectivity is more LAN-like than WAN-like, the Pulse Secure Gateways can be clustered in separate buildings.

Related Documentation

- **Pulse Connect Secure Solution Overview**

PART 2

Configuration

- **Pulse Connect Secure**

Chapter 6

Pulse Connect Secure

- **Configuring Pulse Connect Secure**

Configuring Pulse Connect Secure

To enable users to start using Pulse Connect Secure, you must complete the following basic steps:

1. Plug in the appliance, connect it to your network, and configure its initial system and network settings.
2. After you connect the Pulse Connect Secure device to your network, you need to set the system date and time, upgrade to the latest service package, and install your product licenses. When you first sign into the admin console, Pulse Connect Secure displays an initial configuration task guide that quickly walks you through this process.
3. After you install your product licenses, you need to set up your access management framework to enable your users to authenticate and access resources. Configuration steps include:
 - a. Define an authentication server that verifies the names and passwords of your users.
 - b. Create user roles that enable access mechanisms, session options, and UI options for user groups.
 - c. Create a user authentication realm that specifies the conditions that users must meet to sign into Pulse Connect Secure.
 - d. Define a sign-in policy that specifies the URL that users must access to sign into Pulse Connect Secure and the page that they see when they sign in.
 - e. Create resource profiles that control access to resources, specify which user roles can access them, and include bookmarks that link to the resources.

Pulse Connect Secure includes a task guide in its admin console that quickly walks you through this process. To access this task guide, click the Guidance link located in the upper right corner of the admin console. Then, under Recommended Task Guides, select Base Configuration. Once you have completed these basic steps, your Pulse Connect Secure is ready for use. You can start using it as is, or configure additional advanced features such as endpoint defense and clustering.

Related Documentation

- **Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices**

PART 3

Administration

- **Administrator Settings**
- **Test Scenario Creation**
- **Resource Intermediation**
- **User Access and End-User Interface**
- **Admin and End-User Interface Customization**
- **Serial Console**

Chapter 7

Administrator Settings

- **Default Settings for Administrators**
- **Trusted Server List**

Default Settings for Administrators

Just like for users, Pulse Connect Secure provides default settings that enable you to quickly configure accounts for administrators. This list summarizes the system default settings for administrators:

- **Administrator roles**—There are two built-in administrator roles.
 - **Administrators** — This built-in role permits administrators to manage all aspects of Pulse Connect Secure. The administrator user you create through the serial console is mapped to this role.
 - **Read-Only Administrators** — This built-in role permits users mapped to the role to view (but not configure) all Pulse Connect Secure settings. You need to map administrators to this role if you want to restrict their access.
- **Administrators local authentication server** — The Administrators local authentication server is an a Pulse Connect Secure database that stores administrator accounts. You create the first administrator account in this server through the serial console. (Pulse Connect Secure adds all administrator accounts created through the serial console to this server.) You cannot delete this local server.
- **Admin Users authentication realm** — The Admin Users authentication realm uses the default Administrators local authentication server, an authentication policy that requires a minimum password length of four characters, no directory server, and one role mapping rule that maps all users who sign in to the Admin Users realm to the Administrators role. The administrator account you create through the serial console is part of the Admin Users realm.
- ***/admin sign-in policy** — The default administrator sign-in policy (*/admin) specifies that when a user enters the URL to Pulse Connect Secure followed by /admin, Pulse Connect Secure displays the default sign-in page for administrators. This policy also requires the administrator to select an authentication realm (if more than one realm exists). The */admin sign-in policy is configured to apply to the Admin Users authentication realm, therefore this sign-in policy applies to the administrator account you create through the serial console.

Related Documentation

- **Defining a User Role**

Trusted Server List

The Pulse Connect Secure uses two mechanisms to install and launch client software from a web browser:

- ActiveX controls (available only for Windows/IE)
- Java applets

With both mechanisms, the user is prompted to trust ActiveX controls and Java applets they have not run before. Inherent problems with these types of mechanisms are:

- When the user trusts an ActiveX control that control is trusted forever.
- When trusting a Java applet, users are trusting all code that is signed by the exact same code signing certificate.

To address the above, administrators can create a text file (called a whitelist) that contains a list of trusted Pulse Connect Secures, fully qualified domain names or IP addresses, one per line. Administrators can configure two types of whitelists:

- **Admin whitelist**—The admin whitelist file can be modified only by the endpoint administrator. The administrator must use SMS or other mechanism to copy the admin whitelist file to the end-user's

system. Admin whitelist files are located in:

%ProgramFiles%\Pulse Secure\Whitelist.txt (Windows)

/usr/local/pulse/whitelist.txt (Macintosh and Linux)

- User whitelist—Users can themselves make the decision to trust a Pulse Connect Secure. When the user makes a decision to trust Pulse Connect Secure, the Pulse Connect Secure gets added to the user whitelist. User whitelist files are located in:

%AppData%\Pulse Secure\Whitelist.txt (Windows)

~/Library/Application Support/Pulse Secure/whitelist.txt (Macintosh)

~/.pulse_secure/whitelist.txt (Linux)



Note: The trusted server list feature is for applications launched from a browser window. It does not apply to applications launched from the command-line or other means.

Administrator and User Configuration

The following is a snippet of a whitelist file:

qa.pulsesecure.net

dev1.pulsesecure.net

66.129.224.48



Note: Whitelist files are not deleted when the Pulse Connect Secure software is removed.

There are two modes of enforcement:

- Allow Admin List Only—When software launches from the Pulse Connect Secure that is not in the administrator whitelist, the launch fails and the user receives the error message “You are not allowed to launch software downloaded from <server>. Contact your system administrator for assistance.” If the Pulse Connect Secure is in the administrator whitelist, the launch proceeds as requested.
- Prompt—When software launches from Pulse Connect Secure that is not in the administrator whitelist or the user whitelist, the user is prompted if they want to launch the software with the message “Do you want to download, install and/or execute software from the following server”. If the user declines, the launch fails. If the user accepts, the launch proceeds. The user also has the option to automatically add the Pulse Connect Secure to the user whitelist file by selecting one of the following options from the message window:
 - Always —Add the server to the user whitelist file and download, install or launch the software
 - Yes—Download, install or launch the software but don’t add the server to the user whitelist file
 - No—Don’t download, install or launch software and don’t add the server to the user whitelist file

If the first line of the whitelist file contains “AllowAdminListOnly” (case insensitive) then Allow Admin List Only enforcement mode is used. Otherwise, prompt mode enforcement is used.

A snippet of a whitelist file using Allow Admin List Only enforcement is shown here:

AllowAdminListOnly

qa.pulsesecure.net

dev1.pulsesecure.net

66.129.224.48



Note: Prompt enforcement is the default mode when you upgrade your Pulse Connect Secure software to the latest revision.

To add clusters to the whitelist file:

- For Active/Passive clusters enter the VIP in the whitelist.
- For Active/Active clusters enter the load balancer hostname in the whitelist.

White List Flow Chart

The following steps outline the process for determining whether to launch the software.

1. If the URL of the page initiating the launch does not begin with https, abort the launch and notify the user.
2. Else if the admin whitelist exists,
 - If the origin site is listed in the whitelist, proceed with the launch.
 - If the origin site is not in the whitelist and the whitelist starts with “AllowAdminListOnly”, abort the launch and notify the user.
3. Else if the user whitelist exists,
 - If the origin site is in the user whitelist, proceed with the launch.
4. Prompt the user if they trust the origin site.
5. If the user agrees to trust the origin:
 - If they select Always then add the server to user whitelist file.
 - Proceed with the launch.
6. Abort the launch.

Related Documentation

- **Uploading Java Applets to Secure Access**

Chapter 8

Test Scenario Creation

- **Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices**
- **Using the Test Scenario**

Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices

Pulse Connect Secure provides a flexible access management system that makes it easy to customize a user's remote access experience through the use of roles, resource policies, authentication servers, authentication realms, and sign-in policies. To enable you to quickly begin working with these entities, Pulse Connect Secure ships with system defaults for each. You can create each access management entity by performing the following tasks:

- Define a user role
- Define a resource policy
- Define an authentication server
- Define an authentication realm
- Define a sign-in policy

Pulse Connect Secure supports two types of users:

- **Administrators**—An administrator is a person who may view or modify Pulse Connect Secure configuration settings. You create the first administrator account through the serial console.
- **Users**—A user is a person who uses Pulse Connect Secure to gain access to corporate resources as configured by an administrator.

Related Documentation

- **Verifying User Accessibility**
- **Defining a User Role**
- **Defining a Resource Profile**
- **Defining an Authentication Server**
- **Defining an Authentication Realm**
- **Defining a Sign-In Policy**
- **Using the Test Scenario**

Using the Test Scenario

The test scenario enables you to do the following tasks:

- Access the user console using the modified default sign-in policy.
- Sign in as the user created in the Test Server to map to the Test Realm.
- Test your Web browsing capabilities, which are dependent upon the proper configuration of Test Role and Test Web Access.

To use the test scenario:

1. In a browser, enter the machine's URL followed by /test to access the user sign-in page. The URL is in the format: https://a.b.c.d/test, where a.b.c.d is the machine IP address you entered in the serial console during initial configuration.
2. Click **Yes** when prompted with the security alert to proceed without a signed certificate. If the user sign-in page appears, you have successfully connected to your Pulse Connect Secure device.



Note: If you performed the optional configuration steps in “Defining a Sign-In Policy”, the header color is red.

3. Enter the username and password you created for the user account in Test Server, type Test Realm in the Realm box, and then click **Sign In** to access the Pulse Connect Secure home page for users.

Pulse Connect Secure forwards the credentials to Test Realm, which is configured to use Test Server. Upon successful verification by this authentication server, Pulse Connect Secure processes the role mapping rule defined for Test Realm, which maps testuser2 to Test Role. Test Role enables Web browsing for users.
4. In the browser Address box, enter the URL to your corporate Web site and click **Browse**. Pulse Connect Secure opens the Web page in the same browser window, so to return to the Pulse Connect Secure home page, click the center icon in the browsing toolbar that appears on the target Web page.
5. On the Pulse Connect Secure home page, type www.google.com and click **Browse**. Pulse Connect Secure displays an error message, because the Test Web Access resource policy denies access to this site for users mapped to Test Role.
6. Return to the Pulse Connect Secure home page, click **Sign Out**, and then return to the user sign-in page.
7. Enter the credentials for testuser1, specify the Users realm, and then click **Sign In**.
8. On the Pulse Connect Secure home page, type www.google.com and click **Browse**. Pulse Connect Secure opens the Web page in the same browser window.
9. The test scenario demonstrates the basic Pulse Connect Secure management mechanisms. You can create very sophisticated role mapping rules and resource policies that control user access depending on factors such as a realm’s authentication policy, a user’s group membership, and other variables. To learn more about Pulse Connect Secure management, we recommend that you take a few minutes to review the online Help to familiarize yourself with its contents.

When you configure Pulse Connect Secure for your enterprise, we recommend that you perform user access configuration. Before you make your Pulse Connect Secure available from external locations, we recommend that you import a signed digital certificate from a trusted certificate authority (CA).

Related Documentation

- [Verifying User Accessibility](#)
- [Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices](#)
- [About Multi-Language Support for the Pulse Connect Secure](#)
- [Defining a User Role](#)
- [Defining a Resource Profile](#)
- [Defining an Authentication Server](#)
- [Defining an Authentication Realm](#)
- [Defining a Sign-In Policy](#)

Chapter 9

Resource Intermediation

- **Creating a Seamless Integration Between Pulse Connect Secure and the Resources It Intermediates**

Creating a Seamless Integration Between Pulse Connect Secure and the Resources It Intermediates

In a typical Pulse Connect Secure configuration, you could add bookmarks directly to the Pulse Connect Secure end-user home page. These bookmarks are links to the resources that you configure Pulse Connect Secure to intermediate. Adding these bookmarks enables users to sign into a single place (Pulse Connect Secure) and find a consolidated list of all of the resources available to them.

Within this typical configuration, you can streamline the integration between Pulse Connect Secure and the intermediated resources by enabling single sign-on (SSO). SSO is a process that allows preauthenticated Pulse Connect Secure users to access other applications or resources that are protected by another access management system without having to re-enter their credentials. During Pulse Connect Secure configuration, you can enable SSO by specifying user credentials that you want the Pulse Connect Secure to pass to the intermediated resources.

Or, if you do not want to centralize user resources on the Pulse Connect Secure end-user home page, you could create links to the Pulse Connect Secure-intermediated resources from another Web page. For instance, you can configure bookmarks on Pulse Connect Secure, and then add links to those bookmarks from your company's Intranet. Your users can then sign into your company Intranet and click the links there to access the intermediated resources without going through the Pulse Connect Secure home page. As with standard Pulse Connect Secure bookmarks, you can enable SSO for these external links.

Related Documentation

- **Pulse Connect Secure Solution Overview**
- **About Single Sign-On**

Chapter 10

User Access and End-User Interface

- **Enabling Users on a Variety of Computers and Devices to Use Pulse Connect Secure**
- **Providing PCS for My International Users**
- **Verifying User Accessibility**

Enabling Users on a Variety of Computers and Devices to Use Pulse Connect Secure

In addition to allowing users to access Pulse Connect Secure from standard workstations and kiosks running Windows, Macintosh, and Linux operating systems, end users can access Pulse Connect Secure from connected PDAs, handhelds and smart phones such as i-mode and Pocket PC. When a user connects from a PDA or handheld device, Pulse Connect Secure determines which pages and functionality to display based on settings that you configure.

For more information about specifying which pages Pulse Connect Secure displays to different devices, see the Pulse Connect Secure supported platforms document available on the Pulse Secure Customer Support Center website.

Related Documentation

- **Pulse Connect Secure Solution Overview**
- **Handheld Devices and PDAs**

Providing PCS for My International Users

Pulse Connect Secure supports English (US), French, German, Spanish, Simplified Chinese, Traditional Chinese, Japanese, and Korean. When your users sign into Pulse Connect Secure, it automatically detects the correct language to display based on the user's Web browser setting. Or, you can use end-user localization and custom sign-in pages options to manually specify the language that you want to display to your end users.

Related Documentation

- **Pulse Connect Secure Solution Overview**
- **About Multi-Language Support for the Pulse Connect Secure**

Verifying User Accessibility

You can easily create a user account in the system authentication server for use in verifying user accessibility to your Pulse Connect Secure device. After creating the account through the admin console, sign in as the user on the Pulse Connect Secure user sign-in page.

To verify user accessibility:

1. From the admin console, choose **Authentication > Auth. Servers**.
2. Select the **System Local** link.
3. Select the **Users** tab.
4. Click **New**.
5. Type testuser1 as the username and enter a password, and then click **Save Changes**. Pulse Connect Secure creates the testuser1 account.
6. Use another browser window to enter the machine's URL to access the user sign-in page. The URL is in the format: https://a.b.c.d, where a.b.c.d is the machine IP address you entered in the serial console when you initially configured your Pulse Connect Secure.
7. Click **Yes** when prompted with the security alert to proceed without a signed certificate. The user sign-in

page appears, indicating that you have successfully connected to your Pulse Connect Secure.

8. Enter the username and password you created for the user account and then click **Sign In** to access the Pulse Connect Secure home page for users.
9. Enter the URL to an internal Web server in the Address box and click **Browse**. Pulse Connect Secure opens the Web page in the same browser window, so to return to the Pulse Connect Secure home page, click the center button on the toolbar that appears on the target Web page.
10. Enter the URL to your external corporate site on the Pulse Connect Secure home page, and click **Browse**. Pulse Connect Secure opens the Web page in the same browser window, so use the button on the toolbar to return to the Pulse Connect Secure home page.
11. Click **Browsing > Windows Files** on the Pulse Connect Secure home page to browse through available Windows file shares or **Browsing > UNIX/NFS Files** to browse through available UNIX NFS file shares.

Related Documentation

- **[Creating a Test Scenario to Learn Pulse Connect Secure Concepts and Best Practices](#)**
- **[Defining a User Role](#)**
- **[Defining a Resource Profile](#)**
- **[Defining an Authentication Server](#)**
- **[Defining an Authentication Realm](#)**
- **[Defining a Sign-In Policy](#)**
- **[Using the Test Scenario](#)**

Chapter 11

Admin and End-User Interface Customization

- **Making the Pulse Connect Secure Interface Match My Company's Look-and-Feel**
- **Customizable Admin and End-User UIs**

Making the Pulse Connect Secure Interface Match My Company's Look-and-Feel

Pulse Connect Secure enables you to customize a variety of elements in the end-user interface. Using these customization features, you can update the look-and-feel of the Pulse Connect Secure end-user console so it will resemble one of your standard company Web pages or applications.

For instance, you can easily customize the headers, background colors, and logos that Pulse Connect Secure displays in the sign-in page and end-user console to match your company's style. You can also easily customize the order in which Pulse Connect Secure displays bookmarks and the help system that Pulse Connect Secure displays to users.

Or, if you do not want to display the Pulse Connect Secure end-user home page to users (either in standard or customized form), you can choose to redirect users to a different page (such as your company Intranet) when users first sign into the Pulse Connect Secure console. If you choose to use this option, you may want to add links to your Pulse Connect Secure bookmarks on the new page.

If you want to further customize the Pulse Connect Secure sign-in page, you can use the Pulse Connect Secure's custom sign-in pages feature. Unlike the standard customization options that you can configure through the Pulse Connect Secure admin console, the custom sign-in pages feature does not limit the number of customizations you can make to your pages. Using this feature, you can use an HTML editor to develop a sign-in page that exactly matches your specifications.

Related Documentation

- **Pulse Connect Secure Solution Overview**
- **Creating a Seamless Integration Between Pulse Connect Secure and the Resources It Intermediates**
- **Customizable Admin and End-User UIs**

Customizable Admin and End-User UIs

The Pulse Connect Secure enables you to customize a variety of elements in both the admin console and the end-user interface. This section contains information about which elements you can customize and where you can find the appropriate configuration options.

The Pulse Connect Secure enables you to customize the look and feel of the following user interface elements in the admin console:

- **Sign-in pages (default and custom)**—You can customize the page that administrators see when they sign into the admin console using settings in the Authentication > Signing In > Sign-in Pages page. Using settings in this page, you can create welcome messages, sign out messages and other instructions; control page headers; customize select error messages; and create a link to a custom help page within the default Pulse Connect Secure sign-in page. Or, you can upload your own custom sign-in page to the Pulse Connect Secure.
- **UI look and feel**—You can customize the header, background color, and logo displayed in the admin console using settings in the Administrators > Admin Roles > Select Role > General > UI Options page. You can also use settings in this page to enable or disable the “fly out” hierarchical menus that appear when you mouse over one of the menus in the left panel of the admin console.
- **System utilization graphs**—You can choose which system utilization graphs the Pulse Connect Secure displays on the opening page of the admin console using settings in the System > Status > Overview page. You can also use settings in this page to fine-tune the look and data within each of the graphs.
- **Show auto-allow options**—You can show or hide the auto-allow option from yourself or other

administrators who create new bookmarks for roles using settings in the Maintenance > System > Options page.

- **User role views**—You can use customization options on the Users > User Roles page to quickly view the settings that are associated with a specific role or set of roles.
- **User realm views**—You can use customization options on the Users > User Realms page to quickly view the settings that are associated with a specific user realm or set of user realms.
- **Resource policy views**—You can limit which resource policies the Pulse Connect Secure displays on any given resource policy page based on user roles. For instance, you can configure the Users > Resource Policies > Web page of the admin console to only display those resource policies that are assigned to the “Sales” user role. You can customize these using settings in the Users > Resource Policies > Select Policy Type page of the admin console.
- **Web resource policy views**—You can limit which Web resource policy configuration pages the Pulse Connect Secure displays using settings in Users > Resource Policies > Web > Policy Type of the admin console.
- **Administrator roles**—You can delegate select responsibilities to other administrators using settings in the Administrators > Admin Roles section of the admin console. In doing so, you can restrict the visibility of certain options and capabilities to those other administrators.

Customizable End-User Interface Elements Overview

The Pulse Connect Secure enables you to customize the look and feel of the following elements in the end-user interface:

Sign-in pages (default and custom)—You can customize the page that users see when they sign into the admin console using settings in the Authentication > Signing In > Sign-in Pages page. Using settings in this page, you can create welcome messages, sign out messages and other instructions; control page headers; customize select error messages; and create a link to a custom help page within the default Pulse Connect Secure sign-in page. Or, you can upload your own custom sign-in page to the Pulse Connect Secure.

UI look and feel—You can customize the header, background color, and logo displayed in the admin console using settings in the Users > User Roles > Select Role > General > UI Options page. You can also use settings in this page to specify the first page the users see after they sign into the Pulse Connect Secure, the order in which the Pulse Connect Secure displays bookmarks, the help system that the Pulse Connect Secure displays to users, and various toolbar settings.

Default messages and UI look and feel—You can specify what the default look and feel should be for all user roles using settings in Users > User Roles > [Default Options] pages of the admin console. You can also use settings in these pages to define the default errors that users see when they try to access a blocked site, SSO fails, or SSL is disabled.

Chapter 12

Serial Console

- **Using the Serial Console**
- **Rolling Back to a Previous System State Through the Serial Console**
- **Resetting a Pulse Connect Secure Device to the Factory Setting Using the Serial Console**
- **Performing Common Recovery Tasks with the Serial Console**

Using the Serial Console

The serial console provides a limited set of powerful capabilities to help you manage your Pulse Connect Secure, and is available through your operating system's command window.

Before performing any tasks through the Pulse Connect Secure's serial console, you need to connect to the console using a terminal console or laptop.

To connect to a Pulse Connect Secure's serial console:

1. Plug a null modem crossover cable from a console terminal or laptop into the Pulse Connect Secure. This cable is provided in the product box. Do not use a straight serial cable.
2. Configure a terminal emulation utility, such as HyperTerminal, to use these serial connection parameters:
 - 9600 bits per second
 - 8-bit No Parity (8N1)
 - 1 Stop Bit
 - No flow control
3. Press Enter until the Pulse Connect Secure serial console appears.



Note: If you are running a FIPS system and are connecting to the serial console for the first time, you must also set the mode switch on the cryptographic module to I (initialization mode).

If you are using a non-FIPS platform, your serial console will look similar to this:

Please choose from among the following options:

1. Network Settings and Tools
2. Create admin username and password
3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL
9. Toggle SSL HW Acceleration (system will reboot when this setting is modified): on

If you are using a FIPS platform, your serial console will look similar to this:

Please choose from among the following options:

1. Network Settings and Tools
2. Create admin username and password

3. Display log/status
4. System Operations
5. Toggle password protection for the console (Off)
6. Create a Super Admin session.
7. System Maintenance
8. Reset allowed encryption strength for SSL
9. FIPS options

Related Documentation

- **Rolling Back to a Previous System State Through the Serial Console**
- **Resetting a Pulse Connect Secure Device to the Factory Setting Using the Serial Console**
- **Performing Common Recovery Tasks with the Serial Console**

Rolling Back to a Previous System State Through the Serial Console

If you cannot access the admin console, connect to the serial console to perform a system rollback to the previous system state.

If you have not yet performed a Pulse Connect Secure OS service package upgrade, there is no previous state to roll back to and this option is not available. If you have performed a Pulse Connect Secure OS service package upgrade, any system and user configuration data created after the upgrade is lost unless you export the most current configuration files before rolling back the system and then import them afterwards.

To roll back to the previous Pulse Connect Secure OS service package:

1. Connect to your Pulse Connect Secure's serial console.
2. In a browser window, sign in to the admin console.
3. Select **Maintenance > System > Platform**.
4. Click **Reboot Now** and then go back to the console utility window. The window displays a message that the system is restarting.
5. After several moments, you are prompted to hit the Tab key for options. Press the Tab key, and when prompted for the configuration to load, type rollback and then press the **Enter** key.

After clicking Reboot Now on the **Maintenance > System > Platform** page, the server's rollback status is output to the screen, and when complete, you are prompted to hit the Return key (Enter) to modify system settings, which returns you to the initial setup options. When you are finished entering data, simply close the utility window.

If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded and you'll need to go back to the admin console and click Reboot Now to start the process again. If you have already performed a system rollback, the rollback option is not available again until you upgrade the Pulse Connect Secure OS service package again.

Related Documentation

- **Using the Serial Console**

Resetting a Pulse Connect Secure Device to the Factory Setting Using the Serial Console

In rare cases, you may need to reset your Pulse Connect Secure to its original factory settings. Before performing this advanced system recovery option, please contact Pulse Secure (<http://www.pulsesecure.net/support>). If possible, export the most current system and user configuration data before performing a factory reset.

To perform a factory-reset:

1. Connect to the serial console.
2. In a browser window, sign in to the admin console.
3. Select **Maintenance > System > Platform**.
4. Click **Reboot** and then go back to the console utility window. The window displays a message that the system is restarting.
5. After several moments, you are prompted to hit the Tab key for options. Press the Tab key, and when prompted for the configuration to load, type factory-reset and then press the Enter key.

If you wait more than 5 seconds to enter your choice, the current system configuration is automatically loaded and you'll need to go back to the admin console and click Reboot Now to start the process again.

6. When you are prompted to confirm performing a factory-reset, type proceed and then press Enter.

The system begins the process of resetting the machine to its original settings and outputs several screens of data. After several minutes, you are prompted to hit the Tab key to choose configuration choices.

7. When prompted to hit the Tab key, either:

- Wait for the default selection (current) to automatically start, or
- Press **Tab**, type current, and then press **Enter**.

You are then prompted to enter the initial machine configuration settings. For details on how to proceed, see the Getting Started Guide provided in the product packaging or on the Pulse Secure Support site.

After completing the initialization process, you may upgrade to the latest Pulse Connect Secure OS service package and import saved system and user configuration files to return to the last good working state of your machine.

You might receive errors from the Pulse Connect Secure during the initial setup or on a factory reset. Before the Pulse Connect Secure starts services it monitors the network port for a maximum of 120 seconds. The Pulse Connect Secure checks the link status and performs an ARPing on the default gateway. If there is a problem, after 5 seconds, the Pulse Connect Secure displays a message on the serial console that starts with NIC:..... If the link recovers within 120 seconds, the startup process continues. If the link does not recover, the following message appears:

```
Internal NIC: .....[Down code=0x1]
```

Two codes can appear:

- 0x1 means that the interface link status reported by the NIC remains off (for example, a disconnected cable or a cable in the wrong port).
- 0x2 means that the gateway is unreachable. The Pulse Connect Secure boots but is not reachable from IP addresses bound to that network port.

Related Documentation

- **Using the Serial Console**

Performing Common Recovery Tasks with the Serial Console

If you forget your Pulse Connect Secure administrator username and/or password, lock yourself out of your machine due to configuration errors, or change the Pulse Connect Secure IP address and can no longer reach the machine, you can modify the machine settings through the serial console. Connect the serial cable and then choose the appropriate configuration task.

- **Network Settings and Tools**—Enables you to change standard network settings; print a routing table; print or clear an ARP cache; ping another server, trace a route to a server, remove static routes, and add an ARP entry.

Create admin username and password—Enables you to create a new superadministrator account.

- Display log/status—Enables you to display system configuration, user logs, or administrator access logs through the serial console. Note that must enter “q” to return to serial console options after viewing the logs.
- System Operations—Enables you to reboot, shutdown, restart, rollback, or factory reset the Pulse Connect Secure appliance without using the admin console.
- Toggle password protection for the console—Enables you to password protect the serial console. When you toggle this option to “on,” only superadministrators are allowed access.
- Create a Super Admin session—Enables you to create a recovery session to the admin console, even if you have configured the Pulse Connect Secure to block access to all administrators. When you select this option, the appliance generates a temporary token that is valid for 3 minutes. Enter the following URL into a browser window:

<https://<SA-Series-host>/dana-na/auth/recover.cgi>

Then, enter the temporary token when prompted in order to sign into the admin console.

- When you choose this option, the Pulse Connect Secure blocks any additional administrators from signing in to the admin console until you sign in to the specified URL and initiate a session using your token. The appliance blocks additional sign-in attempts so that you can fix any configuration problems that the Pulse Connect Secure may have encountered without conflicting with another session.
- System Maintenance—Enables you to take a system snapshot without using the admin console or perform remote debugging.

When you select system snapshot, the Pulse Connect Secure takes the snapshot immediately. You can then send the snapshot file, by way of SCP, to a remote system. The system prompts you for the destination server port, user ID, password, and the destination path to the remote directory.

If you choose not to send the snapshot file to a remote system, the Pulse Connect Secure saves the file locally. The next time you log in to the admin console, the System Snapshot tab contains a link to the snapshot file.

- Reset allowed encryption strength for SSL—
- FIPS Options (for FIPS devices only)—Enables you to create additional administrator cards for a security world. See the following section for details.



Note: If you are running a FIPS device and you press the clear switch on the cryptographic module, set the cryptographic module’s mode switch to O (operational mode) and restart the system. You do not need to access the serial console for recovery.

Related Documentation

- **Using the Serial Console**

PART 4

Index

- **Index**

Index

A

administrator

super administrator account, creating.....30

ARP

command.....30

C

customer support5

contacting JTAC.....6

D

documentation

comments on.....5

N

network settings

configuring..... 30

P

Ping command30

S

SCP, system snapshot..... 30

serial console, using for system tasks.....28

snapshots, creating.....30

super administrator account, creating..... 30

support, technical See technical support

T

technical support

contacting JTAC.....5

traceroute command.....30