The Pulse Secure product that is the subject of this technical documentation consists of (or is intended for use with) Pulse Secure software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.pulsesecure.net/support/eula. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.”
Abbreviated Table of Contents

Table of Contents.................................................................................................................. ii
List of Tables............................................................................................................................. v
About This Guide....................................................................................................................... vi
PART 1 Client-Side Changes...................................................................................................... 1
CHAPTER 1 Environment Variables ......................................................................................... 2
CHAPTER 2 Installers and Setup Programs................................................................................ 3
PART 2 Applications.................................................................................................................. 9
CHAPTER 3 Host Checker.......................................................................................................... 10
CHAPTER 4 Enhanced Endpoint Security .............................................................................. 16
CHAPTER 5 Secure Virtual Workspace..................................................................................... 19
CHAPTER 6 Pulse Secure Collaboration.................................................................................... 20
CHAPTER 7 Windows Secure Application Manager (WSAM).................................................. 24
CHAPTER 8 Java Secure Application Manager (JSAM)............................................................ 31
CHAPTER 9 Network Connect.................................................................................................. 35
CHAPTER 10 Terminal Services Client..................................................................................... 41
CHAPTER 11 Citrix Services Client.......................................................................................... 44
PART 3 Appendices.................................................................................................................. 47
Appendix A Required Permissions........................................................................................... 48
PART 4 Index............................................................................................................................. 53
# Table of Contents

Table of Contents ........................................................................................................... ii

List of Tables ................................................................................................................... v

About This Guide .............................................................................................................. vi

- Document Conventions ................................................................................................. vi
- Requesting Technical Support ....................................................................................... vi
- Self-Help Online Tools and Resources ........................................................................ vii
- Opening a Case with PSGSC ......................................................................................... vii

PART 1 Client-Side Changes ........................................................................................... 1

CHAPTER 1 Environment Variables ................................................................................. 2

- Environment Variable Definitions .................................................................................. 2

CHAPTER 2 Installers and Setup Programs ...................................................................... 3

- Pulse Secure Installer Service ....................................................................................... 3
  - Installer Package File and File Location ................................................................... 3
  - Additional Package Files and File Locations ............................................................. 3
  - Files Remaining After Uninstall ............................................................................... 5
  - Registry Modifications ............................................................................................... 5
  - Log File Location ....................................................................................................... 5
- Pulse Secure Setup ......................................................................................................... 5
  - Installer Package Files ............................................................................................... 5
  - Additional Package Files and File Locations ............................................................. 5
  - Registry Modifications ............................................................................................... 6
  - Log File Location ....................................................................................................... 7

PART 2 Applications ........................................................................................................ 9

CHAPTER 3 Host Checker .................................................................................................. 10

- Host Checker Windows Client ....................................................................................... 10
  - Installer Package Files and File Location ................................................................... 10
  - Additional Installer Package Files and File Locations ............................................... 10
  - Log File Locations ..................................................................................................... 11
- Host Checker Macintosh Clients .................................................................................. 12
  - Application and Additional Files Installed by Host Checker ..................................... 12
  - Files Remaining After Uninstall ............................................................................... 13
  - Log files Installed by Host Checker ........................................................................... 13
- Host Checker Linux Clients ........................................................................................... 14
  - Application and Additional Files Installed by Host Checker ..................................... 14
  - Files Remaining After Uninstall ............................................................................... 14
  - Log Files Installed by Host Checker .......................................................................... 14
- Cache Cleaner ................................................................................................................ 14
  - Files Remaining After Uninstall ............................................................................... 14
  - Registry Modifications ............................................................................................... 15
  - Log File Location ....................................................................................................... 15

CHAPTER 4 Enhanced Endpoint Security ....................................................................... 16
Table of Contents

Chapter 5 Secure Virtual Workspace .......................................................... 19
  Secure Virtual Workspace ........................................................................ 19
  Registry Modifications ........................................................................... 19
  Files Remaining After Uninstall .............................................................. 19

Chapter 6 Pulse Secure Collaboration ......................................................... 20
  Pulse Secure Collaboration Windows Client ............................................ 20
    Installer Package File and File Location ................................................ 20
    Files Remaining After Uninstall ............................................................ 20
    Registry Modifications ......................................................................... 20
    Log File Locations ............................................................................... 21
  Pulse Secure Collaboration Macintosh Clients ........................................ 21
    Application and Additional Files Installed by Pulse Secure Collaboration ... 21
    Files Remaining After Uninstall ............................................................ 21
    Log Files Installed by Pulse Secure Collaboration .................................. 22
  Pulse Secure Collaboration Linux Client .................................................. 22
    Application and Additional Files Installed by Pulse Secure Collaboration ... 22
    Log Files Installed by Pulse Secure Collaboration .................................. 22
  Pulse Secure Collaboration Plug-In .......................................................... 23
    File Location ....................................................................................... 23
    Files Remaining After Uninstall ............................................................ 23
    Registry Modifications ......................................................................... 23

Chapter 7 Windows Secure Application Manager (WSAM) ......................... 24
  Windows Secure Application Manager (WSAM) ....................................... 24
    Installer Package Files and File Locations ............................................. 24
    Additional Files Installed by Package and File Locations ....................... 25
    Files Remaining After Uninstall ............................................................ 25
    Registry Modifications ......................................................................... 26
    Log File Location ............................................................................... 29

Chapter 8 Java Secure Application Manager (JSAM) .................................. 31
  Java Secure Application Manager (JSAM) ................................................. 31
  JSAM Windows Client ............................................................................ 31
    Additional Files Installed by Package and File Locations ....................... 31
    Files Remaining After Uninstall ............................................................ 32
    Registry Modifications ......................................................................... 32
    Log File Locations ............................................................................... 32
  JSAM Macintosh Clients .......................................................................... 33
    Application and Additional Files Installed by JSAM ............................... 33
    Files Remaining After Uninstall ............................................................ 33
    Log Files Installed by JSAM ................................................................. 33
  JSAM Linux Client .................................................................................. 33
    Application and Additional Files Installed by JSAM ............................... 33
    Files Remaining After Uninstall ............................................................ 33
List of Tables

Table1: Notice Icons ........................................................................................................................................... vi
Table2: Windows Secure Application Manager (WSAM) .......................................................................................... 48
Table3: Java Secure Application Manager (JSAM) .................................................................................................. 48
Table4: Network Connect ....................................................................................................................................... 49
Table5: Terminal Services Component .................................................................................................................... 50
Table6: Citrix Terminal Services Component .......................................................................................................... 50
Table7: Host Checker (includes Secure Virtual Workspace) ........................................................................................ 50
Table8: Enhanced Endpoint Security ......................................................................................................................... 51
Table9: Cache Cleaner ............................................................................................................................................... 51
Table10: Pulse Secure Collaboration ......................................................................................................................... 51
About This Guide

- Document Conventions
- Requesting Technical Support

Document Conventions

Table 1 defines notice icons used in this guide.

Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Meaning</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>Informational note</td>
<td>Indicates important features or instructions.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></td>
<td>Caution</td>
<td>Indicates a situation that might result in loss of data or hardware damage.</td>
</tr>
<tr>
<td><img src="image3" alt="Icon" /></td>
<td>Warning</td>
<td>Alerts you to the risk of personal injury or death.</td>
</tr>
<tr>
<td><img src="image4" alt="Icon" /></td>
<td>Laser warning</td>
<td>Alerts you to the risk of personal injury from a laser.</td>
</tr>
<tr>
<td><img src="image5" alt="Icon" /></td>
<td>Tip</td>
<td>Indicates helpful information.</td>
</tr>
<tr>
<td><img src="image6" alt="Icon" /></td>
<td>Best practice</td>
<td>Alerts you to a recommended use or implementation.</td>
</tr>
</tbody>
</table>

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: http://www.juniper.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
- 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 1-888-314-5822 (toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.pulsesecure.net/support.
PART 1 Client-Side Changes

- Environment Variables
- Installers and Setup Programs
CHAPTER 1 Environment Variables

- Environment Variable Definitions

Environment Variable Definitions

The environment variable definitions used in this topic are as follows.

For Windows 2000 and Windows XP:

- `%USERPROFILE% = %SystemDrive%\Documents and Settings\%USERNAME%`
- `%ALLUSERSPROFILE% = %SystemDrive%\Documents and Settings\All User`
- `%APPDATA% = %USERPROFILE%\Application Data`
- `%TEMP% = %USERPROFILE%\Local Settings\Temp`

For Windows Vista, Windows 7 and Windows 8:

- `%USERPROFILE% = %SystemDrive%\Users\%USERNAME%`
- `%APPDATA% = %USERPROFILE%\AppData\Roaming`

For medium and high integrity processes:

- `%TEMP% = %USERPROFILE%\AppData\Local\Temp`

For low integrity processes:

- `%TEMP% = %USERPROFILE%\AppData\Local\Temp\low`

Related Documentation

- Pulse Secure Installer Service
CHAPTER 2 Installers and Setup Programs

- Pulse Secure Installer Service
- Pulse Secure Setup

Pulse Secure Installer Service

When installing a Windows-based Secure Access Service client application on a user’s Windows system, the Pulse Secure Installer Service deploys two files on the client machine:

- JuniperSetupSP1Control.ocx
- AccessServiceComponent.exe (The device auto-starts this service when installing, and, then stops and removes it when uninstalling.)

If you plan to use the Pulse Secure Installer MSI package, you will need administrator rights to install onto your client systems. If you plan to use the EXE version, administrator rights is not needed as long as a previous version of the access service component (deployed through, for example, JIS, Pulse, and so forth) is already present.

Installer Package File and File Location

The Secure Access Service loads the installer service files in the following locations:

- C:\Program files\Juniper Networks\Installer Service\AccessServiceComponent.exe (Windows NT/2000/XP)
- C:\WINNT\Downloaded Program Files\JuniperSetupSP1Control.ocx (Windows NT and 2000)
- C:\Windows\Downloaded Program Files\JuniperSetupSP1Control.ocx (Windows XP)

Additional Package Files and File Locations

The Pulse Secure Service installs the following files in C:\WINNT\Downloaded Program Files for Windows NT/2000 and in C:\Windows\Downloaded Program Files for Windows XP/Vista, Windows 7 and Windows 8.

- install.log
- JuniperExt.exe
- JuniperSetup.inf
- JuniperSetupClient.inf
- JuniperSetupClient.ocx
- JuniperSetupClientCtrlUninstaller.exe
- string_de.properties
- string_en.properties
- string_es.properties
- string_fr.properties
- string_ja.properties
- string_ko.properties
- string_zh.properties
- string_zh.cn.properties

The Pulse Secure Installer Service also installs the following files in C:\Program Files\Juniper Networks\Installer Service:

- AccessServiceComponent.x86.exe
- JuniperSetupClientOCX.exe
- JuniperSetupOCX.exe
- x86.Microsoft.VC80.CRT_P.8.0.50727.762.exe
- x86.Microsoft.VC80.CRT_R.8.0.50727.762.exe

The Pulse Secure Installer Service also creates the following files:

- C:\Documents and Settings\All Users\Application Data\Juniper Networks\Logging\debuglog.log (Windows NT/2000/XP)
- C:\Users\Public\Juniper Networks\Logging\debuglog.log (Windows Vista/Windows 7/Windows 8)
- C:\Users\admin\AppData\Roaming\Juniper Networks\Logging\debuglog.log (Windows Vista/Windows 7/Windows 8)

AccessServiceComponent extracts the following files:

- access.ini
- dsAccessService.exe
- dsInstallerService.dll
- dsLogService.dll
- MessageCatalogCommon_DE.txt
- MessageCatalogCommon_EN.txt
- MessageCatalogCommon_ES.txt
- MessageCatalogCommon_FR.txt
- MessageCatalogCommon_JA.txt
- MessageCatalogCommon_KO.txt
CHAPTER 2: Installers and Setup Programs

- MessageCatalogCommon_ZH-CN.txt
- MessageCatalogCommon_ZH.txt
- uninstall.exe

Files Remaining After Uninstall

When the ActiveX control is deleted from within Internet Explorer, it leaves the following files behind:

- C:\Documents and Settings\<user>\Application Data\Juniper Networks\Setup\JuniperSetupCtl.log
- C:\Program Files\Juniper Networks\Installer Service\NeoterisSetupService.log

Registry Modifications

The installer package creates a registry key under
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\JuniperAccessService and
HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks.

Log File Location

The Pulse Secure Installer Service installs the log files in the following location: C:\Program Files\Juniper Networks\Installer Service.

Related Documentation

- Pulse Secure Setup
- Required Rights to Run and Install Applications

Pulse Secure Setup

When a Windows user signs in to the SA Series Appliance, the device attempts to install an ActiveX control (Pulse Secure Setup) on the user’s system. If the device successfully installs Pulse Secure Setup, then the Pulse Secure Setup manages the installation of Windows-based client applications.

Installer Package Files

The SA Series Appliance loads the following installer file.

- JuniperSetupClient.cab

Additional Package Files and File Locations

The Pulse Secure Setup installs the following additional files under C:\WINNT\Downloaded Program Files (Windows XP/2000) or C:\Windows\Downloaded Program Files (Windows Vista, Windows 7 and Windows 8):

- install.log
- JuniperExt.exe
In addition, the following folder is created.

C:\Documents and Settings\username\Application Data\Juniper Networks

If the administrator configures a list of Secure Access Services that the client can trust, this list of Secure Access Services is stored in the following files:

- %ProgramFiles%\Juniper Networks\Whitelist.txt (Windows)
- /usr/local/juniper/whitelist.txt (Macintosh and Linux)

In addition, users can themselves make the decision to trust a Secure Access Service. When the user makes a decision to trust a Secure Access Service, the Secure Access Service is added to the user whitelist. User whitelist files are located in:

- %AppData%\Juniper Networks\Whitelist.txt (Windows)
- ~/Library/Application Support/Juniper Networks/whitelist.txt (Macintosh)
- ~/.juniper_networks/whitelist.txt (Linux)

**Registry Modifications**

For Windows Vista, Windows 7 and Windows 8, the following registry keys are created:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\InternetRegistry\REGISTRY\USER\S-1-5-21-68661237-3255334891-3485583729-1000\SOFTWARE\Juniper Networks
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\{CFE2313F-F5C4-45DCA667-42C339E859FF\}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\AppID\JuniperSetupClient.ocx
CHAPTER 2: Installers and Setup Programs

- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{107AD0CA-8339-40C5-8554-AE361FB31090\}InProcServer32
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{F27237D7-93C8-44C2-AC6E-D6057B9A918F\}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\dsATLSsetupCtrl. JuniperSetupClientCont.1
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Interface\{107AD0CA-8339-40C5-8554-AE361FB31090\}
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{1FEB5880-8108-4CA6-9FF0-BA5191352FCC\}1.0
- HKEY_LOCAL_MACHINE\SOFTWARE\Classes\TypeLib\{1FEB5880-8108-4CA6-9FF0-BA5191352FCC\}1.0.0\win32
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{F27237D7-93C8-44C2-AC6E-D6057B9A918F\}\Contains\Files
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{F27237D7-93C8-44C2-AC6ED057B9A918F\}\Contains\Files\Flags\JuniperExt.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Code Store Database\Distribution Units\{F27237D7-93C8-44C2-AC6ED057B9A918F\}\Contains\Files\Flags\JuniperSetupClient.ocx
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{3EEDF1D3-9D79-4b3e-B8EB-84DB35D7F282\}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Low Rights\ElevationPolicy\{3FB35533-A034-42dc-B051-95F1819F6A9A\}
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ModuleUsage\C:\Windows\Downloaded Program Files\JuniperExt.exe
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ModuleUsage\C:\Windows\Downloaded Program Files\JuniperSetupClient.ocx
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\SharedDLLs
- HKEY_USERS\S-1-5-21-68661237-3255334891-3485583729-1000\Software\Microsoft\Internet Explorer\InternetRegistry\REGISTRY\USER\S-1-5-21-68661237-3255334891-3485583729-1000\SOFTWARE\Juniper Networks

Log File Location

The Pulse Secure Setup installs the log files in the following locations.

For Windows XP and Windows 2000:

- C:\Documents and Settings\All Users\Application Data\Juniper Networks\Logging\debuglog.log
- C:\Documents and Settings\username\Application Data\Juniper Networks\Setup\JuniperSetupControlXP.log (ActiveX logs)

© 2014 by Pulse Secure, LLC. All rights reserved
For Windows Vista, Windows 7 and Windows 8:

- C:\Users\username\AppData\Roaming\Juniper Networks\Logging\debuglog.log
- C:\Users\username\AppData\Local\Temp\Low\JuniperSetupClientControl.log (for ActiveX logs)

For low-integrity processes, such as Internet Explorer 7, the ActiveX installer installs the following log files in C:\Users\username\AppData\Local\Temp\Low:

- JuniperSetupClientCtrl.log
- JuniperSetupDll.log

Related Documentation

- Pulse Secure Installer Service
- Required Rights to Run and Install Applications
PART 2 Applications

- Host Checker
- Enhanced Endpoint Security
- Secure Virtual Workspace
- Pulse Secure Collaboration
- Windows Secure Application Manager (WSAM)
- Java Secure Application Manager (JSAM)
- Network Connect
- Terminal Services Client
- Citrix Services Client
CHAPTER 3 Host Checker

- Host Checker Windows Client
- Host Checker Macintosh Clients
- Host Checker Linux Clients
- Cache Cleaner

Host Checker Windows Client

To run Host Checker, the dsHostCheckerSetup.exe.cab package is downloaded to the user's client. This package is responsible for downloading additional files to the user's system in order to run Host Checker. Host Checker deletes the dsHostCheckerSetup.exe.cab package after installation is complete.

Installer Package Files and File Location

Host Checker installs the following CAB file: %TEMP%\dsHostCheckerSetup.exe.cab

Additional Installer Package Files and File Locations

Host Checker installs the following additional files on the client in C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker:

- CertAuthIMC.dll
- dsHostChecker.exe
- dsHostCheckerProxy.exe
- dsHostCheckerResource_de.dll
- dsHostCheckerResource_en.dll
- dsHostCheckerResource_es.dll
- dsHostCheckerResource_fr.dll
- dsHostCheckerResource_ja.dll
- dsHostCheckerResource_ko.dll
- dsHostCheckerResource_zh.dll
- dsHostCheckerResource_zh_cn.dll
- dsInstallerClient.dll
- dsnisidll.dll
- dsWinClient.dll
In addition, if you implement policies that download or check for third-party software, Host Checker may install additional DLLs in subdirectories of: C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker.

Log File Locations

You can enable or disable client-side logs through the System > Log/Monitoring > Client Logs > Settings tab of the Web console.

When you enable logging, Host Checker adds log files to the following locations:

- C:\Documents and Settings\All Users\Application Data\Juniper Networks\Logging\debuglog.log (Windows XP)
C:\users\username\AppData\Roaming\Juniper Networks\Logging\debuglog.log (Windows Vista, Windows 7 and Windows 8)
C:\Users\Public\Juniper Networks\Logging\debuglog.log (Windows Vista, Windows 7 and Windows 8)

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Host Checker Macintosh Clients
- Host Checker Linux Clients
- Cache Cleaner
- Required Rights to Run and Install Applications

Host Checker Macintosh Clients

The following information applies to Macintosh clients only.

Application and Additional Files Installed by Host Checker

Host Checker downloads the HostCheckerInstaller.osx installer file from the server which installs the following files on the Macintosh client under ~/Library/Application Support/Juniper Networks/HostChecker.app

- Contents/
- Contents/CodeResources
- Contents/Info.plist
- Contents/MacOS/
  - HCIMC.dylib
  - HCIMC.dylib
  - HostChecker
  - HostCheckerServicePS.dylib
  - MessageCatalogTncc_DE.txt
  - MessageCatalogTncc_EN.txt
  - MessageCatalogTncc_ES.txt
  - MessageCatalogTncc_FR.txt
  - MessageCatalogTncc_JA.txt
  - MessageCatalogTncc_KO.txt
  - MessageCatalogTncc_ZH-CN.txt
  - MessageCatalogTncc_ZH.txt
- OPSWAT/
  - UnifiedSDK.ini
  - doSilent.txt
  - libCoreUtils.dylib
  - libImplAntivirus.dylib
  - libImplFirewall.dylib
  - libImplSoftwareProduct.dylib
  - libOesisCore.dylib
  - tables.dat
  - temp/
  - OpswatIMC.dylib
  - hostChecker.dylib
  - libdsWinClientDylib.dylib
  - libhcUtils.dylib
  - tnc_config
- Contents/PkgInfo
- Contents/Resources/
  - AppleScriptCommandDescriptor.sdef
  - DSPACSupport.js
  - English.lproj/
    - InfoPlist.strings
    - MainMenu.nib
- Contents/_CodeSignature/
  - CodeResources
  - Contents/versionInfo.ini

**Files Remaining After Uninstall**

There is no Host Checker uninstall on the Macintosh client.

**Log files Installed by Host Checker**

Host Checker stores the log files in the following location on the Macintosh client:

- ~/Library/Logs/Juniper Networks
- /private/var/log/Juniper Networks/Logging/debuglog.log

**Related Documentation**
Host Checker Linux Clients

The following information applies to Linux clients only.

Application and Additional Files Installed by Host Checker

Host Checker installs $HOME/.juniper_networks/tncc.jar on the Linux client.

Files Remaining After Uninstall

The following files remain on the Linux client after uninstall:

- $HOME/.juniper_networks/dsHCLauncher_linux1.log
- $HOME/.juniper_networks/dsHostChecker_linux1.log

Log Files Installed by Host Checker

Host Checker installs the following log files on Linux systems:

- $HOME/.juniper_networks/dsHCLauncher_linux1.log
- $HOME/.juniper_networks/dsHostChecker_linux1.log

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Host Checker Windows Client
- Host Checker Macintosh Clients
- Cache Cleaner
- Required Rights to Run and Install Applications

Cache Cleaner

Cache Cleaner is installed as part of Host Checker. Host Checker downloads the binary files dSCacheCleaner.dll and dsCCProc.exe.

Files Remaining After Uninstall

None.
Registry Modifications

Cache Cleaner sets the following string registry values in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Juniper_Networks_Cache_Cleaner version number.

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>“Juniper Networks Cache Cleaner version”</td>
</tr>
<tr>
<td>DisplayVersion</td>
<td>the current software version</td>
</tr>
<tr>
<td>Publisher</td>
<td>“Juniper Networks”</td>
</tr>
<tr>
<td>QuietUninstallString</td>
<td>“%APPDATA%\Juniper Networks\Cache Cleaner version\uninstall.exe /S”</td>
</tr>
<tr>
<td>StartupApp</td>
<td>“%APPDATA%\Juniper Networks\Cache Cleaner version\dsCacheCleaner.exe”</td>
</tr>
<tr>
<td>StopApp</td>
<td>“%APPDATA%\Juniper Networks\Cache Cleaner version\dsCacheCleaner.exe”</td>
</tr>
<tr>
<td></td>
<td>-action stop -nodelete 1”</td>
</tr>
<tr>
<td>UninstallString</td>
<td>“%APPDATA%\Juniper Networks\Cache Cleaner version\uninstall.exe”</td>
</tr>
<tr>
<td>URLInfoAbout</td>
<td>“<a href="http://www.juniper.net%E2%80%9D">http://www.juniper.net”</a></td>
</tr>
</tbody>
</table>

Log File Location

You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console. For Windows 2000 and Windows XP, when you enable logging Cache Cleaner adds log files to %ALLUSERSPROFILE%\Application Data\Juniper Networks\Logging\debuglog.log.

For Windows Vista, Windows 7 and Windows 8, Cache Cleaner adds log files to %APPDATA%\Juniper Networks\Logging\debuglog.log.

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Host Checker Windows Client
- Host Checker Macintosh Clients
- Host Checker Linux Clients
- Required Rights to Run and Install Applications
CHAPTER 4 Enhanced Endpoint Security

Enhanced Endpoint Security (EES) requires a two-phase installation process. During the first phase, the EES installer is downloaded and installs Pulse Secure binaries. The second phase downloads the WebRoot SDK installer which installs the WebRoot components and an initial set of malware signatures.

**NOTE:** EES requires you to have administrator privileges in order to install.

EES is a JUNS plug-in and requires JUNS Access Service to be installed on the client system. A JUNS plug-in is a component, such as EES or Host Checker that runs under the Juniper Unified Network Service (a Windows NT service). If JUNS is not already installed, EES automatically installs it. If a JUNS service already installed on the end-user system, EES is installed with limited user privilege.

Installer Package Files and File Location

EES installs the following CAB file: EndpointDefenseInstaller.exe

Additional Installer Package Files and File Locations

EES installs the following additional files on the client in %CommonProgramFiles%\Juniper Networks\Endpoint Defense:

- dsEES.dll
- EndpointDefensePS.dll
- EPD.dep
- install.log (installed when both EES and WebRoot SDK is installed)
- uninstall.exe
- versionInfo.ini
- WRSS.log (installed when both EES and WebRoot SDK is installed)

EES installs the WebRoot SDK in %CommonProgramFiles%\Juniper Networks\Endpoint Defense\WRSSMini and includes the following files and folders. Note that different versions of WebRoot SDK may change the files in this list.

- CoreScan.dll
- dbghelp.dll
- Lockbox.dll
- pcre3.dll
- SSU.exe
- WRSSMini.dll
- ZipTV06.dll
- ztv内阁.dll
- ztvunrar3.dll
- drv/WRSSMini.inf
- drv/amd64/SSFSFD.sys
- drv/amd64/SSIDRV.sys
- drv/amd64/SsiEfr.exe
- drv/i386/SSFSFD.sys
- drv/i386/SSHRMD.sys
- drv/i386/SSIDRV.sys
- drv/i386/SsiEfr.exe
- Masters/inst.const
- Masters/inst.mst
- Masters/Masters.bak
- Masters/masters.const
- Masters/masters.mst

**JUNS Plug-in Registration**

dsEES.dll needs to be registered with JUNS Access Service to run as a plug-in. The JUNS Access Service maintains a record of plug-ins in %CommonProgramFiles%Juniper Networks\JUNS\access.ini. The bolded entries shown below are created by the EES installer.

[Plugins]
InstallerService=C:\Program Files\Common Files\Juniper Networks\JUNS\dsInstallerService.dll
EndpointDefense=C:\Program Files\Common Files\Juniper Networks\Endpoint Defense\dsEES.dll
[InstallerService]
StartType=Auto
[EndpointDefense]
StartType=Auto

If the JUNS plug-in is enabled on the end-user system, you should not expect any other .exe applications running on the end-user system.
If Host Checker is running as a user mode process (dsAccessService.exe is running), EES is loaded into that process.

Registry Modifications

EES sets the following registry values under HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\Host Checker:

<table>
<thead>
<tr>
<th>String</th>
<th>Set To</th>
</tr>
</thead>
<tbody>
<tr>
<td>WebrootInstallPath</td>
<td>The installation directory, for example, &quot;C:\Program Files\Common Files\Juniper Networks\Endpoint Defense&quot;. The actual path is dependent on the CommonProgramFiles variable.</td>
</tr>
<tr>
<td>WebrootInstallVersion</td>
<td>6.5.1.102</td>
</tr>
</tbody>
</table>

Files Remaining After Uninstall

- %CommonProgramFiles%\Juniper Networks\Endpoint Defense\install.log
- %CommonProgramFiles%\Juniper Networks\Endpoint Defense\WRSS.log

Log File Location

EES log messages are included in the Juniper debug log files on the end-user systems.

- WebRoot debug logs are located in <%%AllUsersProfile%\Application Data\Webroot\WRSSMini\Logs>. Only the last three logs are saved to conserve disk space.
- WebRoot memory dumps are also located in <%%AllUsersProfile%\Application Data\Webroot\WRSSMini\Logs>.

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Required Rights to Run and Install Applications
CHAPTER 5 Secure Virtual Workspace

- Secure Virtual Workspace

**Secure Virtual Workspace**

To run Secure Virtual Workspace (SVW), Host Checker downloads neoSVWData.zip and neoSVWDlls.zip. Then Host Checker unzips the following files onto the client computer under C:\Documents and Settings\username\Application Data\Juniper Networks\Host Checker\policy_number:

- wallpaper.bmp
- dsjvd.dll
- dsjvdsvc.dll
- dsmonitor.dll
- dsVdeskPackage.dll
- dsjvd64.dll (64-bit SVW only)
- dsmonitor64.dll (64-bit SVW only)

Host Checker deletes neoSVWData.zip and neoSVWDlls.zip after unzipping the files.

**Registry Modifications**

SVW creates the key HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\VDesk.

**Files Remaining After Uninstall**

None. Host Checker uninstalls SVW as part of the Host Checker uninstallation process.

**Related Documentation**

- Pulse Secure Installer Service
- Pulse Secure Setup
- Required Rights to Run and Install Applications
CHAPTER 6 Pulse Secure Collaboration

- Pulse Secure Collaboration Windows Client
- Pulse Secure Collaboration Macintosh Clients
- Pulse Secure Collaboration Linux Client
- Pulse Secure Collaboration Plug-In

Pulse Secure Collaboration Windows Client

To execute the Windows version of Pulse Secure Collaboration, Secure Access Service downloads the neoCBoxSetup.exe package to the user's computer.

Installer Package File and File Location

Pulse Secure Collaboration installs the neoCBoxSetup.exe file on the Windows client in
C:\Documents and Settings\username\Local Settings\Temp\neoCBoxSetup.exe

Additional Files Installed by Package and File Locations

- With an Active-X based install, Pulse Secure Collaboration installs additional files in:
  - (Windows NT/2000/XP) C:\Documents and Settings\username\Application Data\Juniper Networks\Junos Pulse Collaboration version_number
  - (Windows Vista, Windows 7 and Windows 8) C:\Users\username\AppData\Roaming\Juniper Networks\Junos Pulse Collaboration version_number

The Pulse Secure Collaboration installer also contains the Access Services installer when run on a Windows Vista, Windows 7 or Windows 8 system.

See the Pulse Secure Collaboration directory for a complete list of files.

Files Remaining After Uninstall

After Pulse Secure Collaboration uninstalls, the cbox_cfg.ini and cbox_cfg.txt files (for the Java client) and the installer logs remain on the client.

Registry Modifications

Pulse Secure Collaboration sets the following registry values:

<table>
<thead>
<tr>
<th>String</th>
<th>Set in</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>HKEY_CURRENT_USER\Software\Juniper Networks\Junos Pulse Collaboration version_number level</td>
</tr>
<tr>
<td></td>
<td>HKLM\Software\Juniper Networks\Logging\Level</td>
</tr>
</tbody>
</table>
Log File Locations

You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console.

**NOTE:** The maximum file size for each of the Pulse Secure Collaboration log files is 10 MB.

When you enable logging, Pulse Secure Collaboration adds log files to the following locations for Windows XP:

- C:\Documents and Settings\All Users\Application Data\Juniper Networks\Logging\debuglog.log
- C:\Documents and Settings\username\Application Data\Juniper Networks\Logging\debuglog.log

When you enable logging, Pulse Secure Collaboration adds log files to the following locations for Windows Vista, Windows 7 and Windows 8:

- C:\Users\Public\Juniper Networks\Logging\debuglog.log
- C:\Users\username\AppData\Roaming\Juniper Networks\Logging\debuglog.log

**Related Documentation**

- Pulse Secure Installer Service
- Pulse Secure Setup
- Pulse Secure Collaboration Macintosh Clients
- Pulse Secure Collaboration Linux Client
- Pulse Secure Collaboration Plug-In
- Required Rights to Run and Install Applications

**Pulse Secure Collaboration Macintosh Clients**

The following information applies to Macintosh clients only.

**Application and Additional Files Installed by Pulse Secure Collaboration**

Pulse Secure Collaboration installs the following files on the Macintosh client:

- ~/Library/Application Support/Juniper Networks/meetingAppMac.jar
- ~/Library/Application Support/Juniper Networks/cbox_cfg.txt
- ~/Library/Application Support/Juniper Networks/meeting.icns

**Files Remaining After Uninstall**

There is no Pulse Secure Collaboration uninstall on the Macintosh client.
Log Files Installed by Pulse Secure Collaboration

Pulse Secure Collaboration installs log files in the following locations on the Macintosh client:

- ~/Library/Logs/Juniper Networks/dsCboxLauncher_mac.log, where x is 0 or 1.
- ~/Library/Logs/Juniper Networks/dsCboxUI_mac.log, where x is 0 or 1.
- ~/Library/Logs/Juniper Networks/dsCboxUISummary_mac.log, where x is 0 or 1.
- ~/Library/Logs/Juniper Networks/MacPresenter.log.

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Pulse Secure Collaboration Windows Client
- Pulse Secure Collaboration Linux Client
- Pulse Secure Collaboration Plug-In
- Required Rights to Run and Install Applications

Pulse Secure Collaboration Linux Client

The following information applies to Linux clients only.

Application and Additional Files Installed by Pulse Secure Collaboration

Pulse Secure Collaboration installs the following files on the Linux client:

- ~/.juniper_networks/meetingAppSun.jar
- ~/.juniper_networks/libSMJNIWinLinux.so

Log Files Installed by Pulse Secure Collaboration

Pulse Secure Collaboration installs log files in the following locations on the Linux client:

- ~/.juniper_networks/LinuxPresenter_x.log where x is 0 or 1.
- ~/.juniper_networks/dsCboxUISummary_linux.x.log where x is 0 or 1.
- ~/.juniper_networks/dsCboxUI_linux.x.log where x is 0 or 1.
- ~/.juniper_networks/dsCboxLauncher_linux.x.log where x is 0 or 1.

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Pulse Secure Collaboration Windows Client
- Pulse Secure Collaboration Macintosh Clients
- Pulse Secure Collaboration Plug-In
Pulse Secure Collaboration Plug-In

To run the Pulse Secure Collaboration plug-in, the Secure Access Service downloads the Pulse Secure Collaboration plug-in to the user’s client.

File Location

The Pulse Secure Collaboration plug-in is installed on the Windows client in \Documents and Settings\user\Application Data\Juniper Networks\Pulse Secure Collaboration Plugin

Files Remaining After Uninstall

After the Pulse Secure Collaboration plug-in is uninstalled, the SecureMeetingOutlook.log file remains on the client.

Registry Modifications

<table>
<thead>
<tr>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
</tr>
</tbody>
</table>

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Pulse Secure Collaboration Windows Client
- Pulse Secure Collaboration Macintosh Clients
- Pulse Secure Collaboration Linux Client
- Required Rights to Run and Install Applications
CHAPTER 7 Windows Secure Application Manager (WSAM)

Windows Secure Application Manager (WSAM)

An administrator can use the Pulse Secure Installer Service to download, install, upgrade, and run client-side applications on client systems without requiring administrator privileges. With this approach, it is not necessary for the end-user to, for example, manually download the WSAM installer.

An administrator can choose to download a “stand-alone” installer to a client’s system for installing WSAM from a command line, batch file or Windows service. In this case, the administrator should install WSAM on the client as the end-user may not have the appropriate permissions.

Installer Package Files and File Locations

WSAM downloads its package files to the following locations:

- Windows 2000 and Windows XP (32- and 64-bit):
  C:\Documents and Settings\username\Local Settings\Temp\samsetupnt.exe
- Windows Vista, Windows 7 and Windows 8 (32- & 64-bit):
  \Users\username\AppData\Local\Temp
- Windows Mobile 6.0 Pocket PC/6.0 Classic/6.0 Professional:
  \My Documents\WSAMInstARM.cab
- Windows Mobile 5.0 Smartphone/6.0 Standard:
  \My Document\WSAMInstARMSP.cab

**NOTE:** You may choose to use a WSAM standalone installer or scriptable installer instead of the standard Web installers already mentioned. If you do, the installers are located where you save them, which may not be the same directories listed here. The filenames for these downloadable installers are:

- WSAMInstNt.exe—WSAM standalone installer for Windows 2000/XP/Vista/Windows7 (including 32- & 64-bit) systems
- WSAMInstARM.cab—WSAM standalone installer for Windows Mobile 5.0 PocketPC/6.0 Classic/6.0 Professional
- WSAMInstARMSP.cab—WSAM standalone installer for Windows Mobile 5.0 Smartphone/6.0 Standard
Additional Files Installed by Package and File Locations

For Windows XP, Windows Vista, Windows 7 and Windows 8, WSAM installs the following additional files on the client in C:\Program Files\Juniper Networks\Secure Application Manager or C:\Program Files (x86)\Juniper Networks\Secure Application Manager for 64-bit Windows operating systems:

- dsSamProxy.exe
- dsSamResource_DE.dll
- dsSamResource_EN.dll
- dsSamResource_ES.dll
- dsSamResource_FR.dll
- dsSamResource_JA.dll
- dsSamResource_KO.dll
- dsSamResource_ZH.dll
- dsSamResource_ZH_CN.dll
- dsSamUI.exe
- dsWinClient.dll
- dsWinClientResource_DE.dll
- dsWinClientResource_EN.dll
- dsWinClientResource_ES.dll
- dsWinClientResource_FR.dll
- dsWinClientResource_JA.dll
- dsWinClientResource_KO.dll
- dsWinClientResource_ZH.dll
- dsWinClientResource_ZH_CN.dll
- gaptbar.dll
- install.log
- Microsoft.VC80.CRT/Microsoft.VC80.CRT.manifest
- Microsoft.VC80.CRT/msvcp80.dll
- Microsoft.VC80.CRT/msvcr80.dll
- pending.reboot
- samclean.exe
- samdiagEx.dll (Windows 2000/XP/Vista/Windows 7/Windows 8 only)
- samlauncher.exe
- SAMNB.dll (Windows 2000/XP/Vista/Windows 7/Windows 8 only)
- UninstallSAM.exe
- versionInfo.ini

On Windows 2000, XP, Vista, Windows 7 and Windows 8 systems, WSAM also installs a TDI driver (neofltr_release_number_build_number.sys) in $SystemRoot\system32\drivers.

For Windows mobile, WSAM installs the following additional files on the client in \Program Files\Juniper Networks\WSAM:

<table>
<thead>
<tr>
<th>File</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>dsSamProxy.exe</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>gapsp.dll</td>
<td>Windows</td>
</tr>
<tr>
<td>SamResource_DE.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_EN.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_ES.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_FR.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_JA.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_KO.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_ZH.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamResource_ZH_CN.dll</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
<tr>
<td>SamUI.exe</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
</tbody>
</table>

**Files Remaining After Uninstall**

After WSAM uninstalls, the following files remain on the Windows XP/2000/Vista, Windows 7 and Windows 8 client:

- Microsoft.VC80.CRT\Microsoft.VC80.CRT.manifest
- Microsoft.VC80.CRT\msvcp80.dll
- Microsoft.VC80.CRT\msvcr80.dll
- pending.reboot
- samclean.exe

**Registry Modifications**

WSAM sets the following registry values for the installation, uninstallation, current version, TDI driver for Windows 2000, XP, Vista, Windows 7 and Windows 8 only, and miscellaneous:

**Installation Values**

For Windows XP, Windows Vista, Windows 7 and Windows 8, WSAM sets the following installation values in HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\Secure Application Manager:
## CHAPTER 7: Windows Secure Application Manager (WSAM)

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallPath</td>
<td>C:\Program Files\Juniper Networks\Secure Application Manager</td>
</tr>
<tr>
<td>Language</td>
<td>EN (or appropriate language value)</td>
</tr>
</tbody>
</table>

For Windows Mobile, WSAM sets the following installation values:

- In `HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\WSAM`:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>AutoStart</td>
<td>0 or 1</td>
</tr>
<tr>
<td>ProductVersion</td>
<td>&lt;version number&gt;&lt;build number&gt;</td>
</tr>
<tr>
<td>ProductName</td>
<td>WSAM</td>
</tr>
</tbody>
</table>

- `HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\WSAM\Config`:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>Url1</td>
<td>???</td>
</tr>
</tbody>
</table>

- `HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\WSAM\Log`:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>LoggingApps</td>
<td>iexplore.exe; tmail.exe</td>
</tr>
<tr>
<td>LogLevel</td>
<td>3</td>
</tr>
<tr>
<td>ProductLocation</td>
<td>\Program Files\Juniper Networks\WSAM</td>
</tr>
</tbody>
</table>

Uninstallation Values

WSAM sets the following uninstall values in

- `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Neoteris_Secure_Application_Manager\Commands for Windows 2000, XP, Windows Vista, Windows 7 and Windows 8.`

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DelRV</td>
<td>&quot;C:\Program Files\Juniper Networks\Secure Application Manager\samnb.dll&quot;, SFS_DeleteRebootValue</td>
</tr>
</tbody>
</table>
Secure Access Service Client - Side Changes Guide

WSAM also sets the following locations:

- HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Secure Application Manager\SessionEstablishTasks
- HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Secure Application Manager\SessionCleanupTasks
- HKEY_CURRENT_USER\SOFTWARE\Juniper Networks\Secure Application Manager\EnableLogSvr (Set to 0 or 1, depending on server side log setting)

**Current Version Values**

WSAM sets the following uninstall and version information values in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\Neteiris_Secure_Application_Manager:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>“Juniper Networks Secure Application Manager”</td>
</tr>
<tr>
<td>DisplayVersion</td>
<td>&lt;version number&gt;-&lt;build number&gt;</td>
</tr>
<tr>
<td>Publisher</td>
<td>Juniper Networks</td>
</tr>
<tr>
<td>QuietUninstallString</td>
<td>C:\Program Files\Juniper Networks\Secure Application Manager\UninstallSAM.exe</td>
</tr>
<tr>
<td>StartupApp</td>
<td>C:\Program Files\Juniper Networks\Secure Application Manager\dsSamProxy.exe</td>
</tr>
<tr>
<td>UninstallString</td>
<td>C:\Program Files\Juniper Networks\Secure Application Manager\UninstallSAM.exe</td>
</tr>
<tr>
<td>URLInfoAbout</td>
<td><a href="http://www.juniper.net/products/ssl">http://www.juniper.net/products/ssl</a></td>
</tr>
</tbody>
</table>

In addition, WSAM sets the following version values:

<table>
<thead>
<tr>
<th>Location</th>
<th>Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ Zones\1</td>
<td>1A00 to: 1</td>
</tr>
<tr>
<td>HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ Zones\1</td>
<td>1A00 to: 1</td>
</tr>
</tbody>
</table>

**TDI Driver Values (Windows 2000/XP/Vista/Windows 7/Windows 8 Only)**

XP systems in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NEOFLTR_releaseNumber_buildNumber:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>DisplayName</td>
<td>Juniper Networks TDI Filter Driver (NEOFLTR_releaseNumber_buildNumber)</td>
</tr>
</tbody>
</table>
WSAM sets the following values in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NEOFLTR_releaseNumber_buildNumber\Enum:

<table>
<thead>
<tr>
<th>String</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>0</td>
<td>Root\LEGACY_NEOFLTR_releaseNumber_buildNumber\0 000</td>
</tr>
<tr>
<td>DWord</td>
<td>Count</td>
<td>0x00000001</td>
</tr>
<tr>
<td>Dword</td>
<td>NextInstance</td>
<td>0x00000001</td>
</tr>
</tbody>
</table>

WSAM sets the following value in HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters:

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>IrpStackSize</td>
<td>Applicable TDI Irp stack size, if required</td>
</tr>
</tbody>
</table>

**Miscellaneous**

WSAM sets the following miscellaneous registry values:

- String: IntranetAuthOptions is set in HKEY_LOCAL_MACHINE\SOFTWARE\Neoteris\Secure Application Manager\Backup and HKEY_CURRENT_USER\SOFTWARE\Neoteris\Secure Application Manager\Backup.

**Log File Location**

You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console. When you enable logging, WSAM adds log files to the following location:

For Windows 2000/XP:

- C:\Documents and Settings\All Users \Application Data\Juniper Networks\Secure Application Manager
- C:\Documents and Settings\All Users \Application Data\Juniper Networks\Logging

For Windows Vista, Windows 7 and Windows 8:

- C:\Users\username\AppData\Roaming\Juniper Networks\Secure Application Manager
- C:\Users\username\AppData\Roaming\Juniper Networks\Logging

WSAM also adds an installation log file to the C:\Program Files\Juniper Networks\Secure Application Manager directory.

For Windows Mobile 5 users, WSAM adds log files to the \Program Files\Juniper Networks\WSAM\Log directory.

**Related Documentation**

- Pulse Secure Installer Service
- Pulse Secure Setup
- Required Rights to Run and Install Applications
CHAPTER 8 Java Secure Application Manager (JSAM)

- Java Secure Application Manager (JSAM)
- JSAM Windows Client
- JSAM Macintosh Clients
- JSAM Linux Client

Java Secure Application Manager (JSAM)

To run JSAM, the Secure Access Service launches an applet on the user’s client. This applet handles downloading additional files to the user’s system in order to run JSAM.

In addition, JSAM modifies the hosts file if you choose Automatic host-mapping under Users > User Roles > Role > SAM > Options > Java SAM Options.

Related Documentation
- Pulse Secure Installer Service
- Pulse Secure Setup
- JSAM Windows Client
- JSAM Macintosh Clients
- JSAM Linux Client
- Required Rights to Run and Install Applications

JSAM Windows Client

The following information applies to Windows clients only.

Additional Files Installed by Package and File Locations

For Windows 2000/XP, JSAM installs additional files in: C:\Documents and Settings\username\Application Data\Juniper Networks\Java Secure Application Manager

For Windows Vista, Windows 7 and Windows 8:

- If UAC is disabled, JSAM installs C:\Users\username\AppData\Roaming\Juniper Networks\jsamtool.exe.
- If UAC is enabled, JSAM installs C:\Users\username \AppData\Local\Temp\Low\Juniper Networks\Java Secure Application Manager\jsamtool.exe.
Files Remaining After Uninstall

For Windows 2000/XP, after JSAM uninstalls, only the log files remain on the client.

For Windows Vista, Windows 7 and Windows 8, after JSAM uninstalls, files in C:\Users \username\AppData\Local\Temp\Low\Juniper Networks\Java Secure Application Manager remain.

Registry Modifications

JSAM sets the following registry values:

- If you configure a standard NetBIOS application through JSAM, or you configure a custom application on port 137, 138, or 139, JSAM makes the following registry key modification on Windows XP machines (Administrator privileges required):
  SMBDeviceEnabled=dword:00000000 is set in the registry location:
  HK\EY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters

- If you enable Outlook 5.5, 2000, or 2002 (Administrator privileges required), JSAM adds
  HK\EY_LOCAL_MACHINE\Software\Microsoft\Exchange\Exchange Provider\Rpc_Binding_Order to the registry.
  (The second entry for this registry key is changed to ncacn_http.)

  The original value of this setting is:
  ncalrpc,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp

  After JSAM is initially used, the value of this setting is:
  ncalrpc,ncacn_http,ncacn_ip_tcp,ncacn_spx,ncacn_np,netbios,ncacn_vns_spp

- If you disable the Skip Web Proxy Registry Check option under Users > User Roles > Role > SAM > Options > Java SAM Options (User read access required), JSAM reads:
  HK\EY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\ProxyEnable

Log File Locations

You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console.

For Windows 2000/XP, when you enable logging, JSAM adds C:\Documents and Settings\username\Application Data\Juniper Networks\Java Secure Application Manager\dsJSAM_win0.log and dsJSAM_win1.log

For Windows Vista, Windows 7 and Windows 8, when you enable logging, JSAM adds C:\Users\username\AppData\Local\Temp\Low\Juniper Networks\Java Secure Application Manager\jsamtool.log and dsJSAM_win1.log.

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- JSAM Macintosh Clients
- JSAM Linux Client
• Required Rights to Run and Install Applications

JSAM Macintosh Clients

The following information applies to Macintosh clients only.

Application and Additional Files Installed by JSAM

JSAM installs the following files on the Macintosh client:

- ~/Library/Application Support/Juniper Networks/NeoterisMac.jar
- ~/Library/Java/Extensions/libJNPRAuthKit.jnilib
- ~/Library/Application Support/Juniper Networks/jsam.icns
- ~/Library/Application Support/Juniper Networks/logo.gif

Files Remaining After Uninstall

The following file remains on the Macintosh client after uninstall: ~/Library/Logs/Juniper Networks/Java Secure Application Manager

Log Files Installed by JSAM

JSAM installs log files in the following location on the Macintosh client: ~/Library/Logs/Juniper Networks/Java Secure Application Manager

Related Documentation

• Pulse Secure Installer Service
• Pulse Secure Setup
• JSAM Windows Client
• JSAM Linux Client
• Required Rights to Run and Install Applications

JSAM Linux Client

The following information applies to Linux clients only.

Application and Additional Files Installed by JSAM

JSAM does not install any application files on the Linux client.

Files Remaining After Uninstall

The only files that remain on the Linux client after uninstall are the log files.

Log Files Installed by JSAM

JSAM adds log files to the ~/.juniper_networks directory.

Related Documentation
- Pulse Secure Installer Service
- Pulse Secure Setup
- JSAM Windows Client
- JSAM Macintosh Clients
- Required Rights to Run and Install Applications
CHAPTER 9 Network Connect

- Network Connect and GINA Windows Client
- Network Connect Linux Client
- Network Connect Macintosh Clients

Network Connect and GINA Windows Client

To run Network Connect and Graphical Identification and Authorization (GINA), the Secure Access Service downloads the NcSetup.exe.cab package to the user’s Windows client. This package is responsible for downloading additional files to the user’s system in order to run Network Connect and GINA.

Installer Package Files and File Locations

- C:\Documents and Settings\username\Local Settings\Temp\neoNCsetup.exe.cab (Windows 2000/XP)
- C:\Users\username\AppData\Local\Temp\neoNCSetup.exe (Windows Vista, Windows 7 and Windows 8)
- For FIPS compliant systems, the following additional packages are downloaded:
  - C:\Documents and Settings\username\Application Data\Juniper Networks\Setup Client\neoFIPSSetup_6.5.x.xxxxx.exe (Windows 2000/XP)
  - C:\Users\username\AppData\Roaming\Juniper Networks\Setup Client\neoFIPSSetup_6.5.x.xxxxx.exe (Windows Vista, Windows 7 and Windows 8)

Additional Files Installed by Package and File Locations

On Windows 2000, XP, Windows Vista, Windows 7 and Windows 8, Network Connect installs the following additional files on the client in the following locations. The following files are installed in C:\Program Files\Juniper Networks\Network Connect version_number:

- dsNcAdmin.dll
- dsNetworkConnect.exe
- dsNcDiag.dll
- versionInfo.ini
- dsNcGina.dll
- dsNCGINACOMPATIBLE.txt
- dsNCResource_EN.dll
- dsNCResource_DE.dll
Network Connect also installs the following files:

- C:\Program Files\Juniper Networks\Common Files\dsNcService.exe
- C:\Program Files\Juniper Networks\Common Files\odFips2.dll (FIPS only)
- C:\Program Files\Juniper Networks\Common Files\odFips2.dll.icv (FIPS only)
- C:\Program Files\Juniper Networks\Common Files\salib_OSSL.dll (FIPS only)
- C:\<WINDIR>\system32\drivers\dsNcAdpt.sys
- C:\<WINDIR>\system32\dsGinaLoader.dll (Windows 2000 and Windows XP)

For Windows Vista, Windows 7 and Windows 8, Network Connect also installs the following files:

- %windows%\system32\dsNCCredProv.dll
- %windows%\system32\dsNcSmartCardProv.dll

Files Remaining After Uninstall

After Network Connect uninstalls, the following files remain on the client:

- dsGinaLoader.dll
If only one Network Connect installation is present on the client, this file is removed after you reboot. If there are multiple versions of Network Connect installed on the client, this file remains on the client.

- C:\Program Files\Juniper Networks\Common Files\Config.ini

### Registry Modifications

Additionally, if GINA is enabled in the Admin Web console, Network Connect sets following string registry value in HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon (Windows 2000 and Windows XP only):

<table>
<thead>
<tr>
<th>String</th>
<th>Set to</th>
</tr>
</thead>
<tbody>
<tr>
<td>GinaDLL</td>
<td>&quot;dsGinaLoader.dll&quot;</td>
</tr>
</tbody>
</table>

Network Connect creates the following keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Juniper Networks\Network Connect version_number
- HKEY_CURRENT_USER\Software\Juniper Networks\Network Connect version_number
- (Windows Vista, Windows 7 and Windows 8 only) HKEY_LOCAL_MACHINE
  "SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{9f4a51de-92b1-483a-b717-dd7d3bb7d3db}"
- (Windows Vista, Windows 7 and Windows 8 only) HKEY_CLASSES_ROOT
  "CLSID\{9f4a51de-92b1-483a-b717-dd7d3bb7d3db}"
- (Windows Vista, Windows 7 and Windows 8 only) HKEY_LOCAL_MACHINE
  "SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP Providers\{60442b50-aac2-4db7-b9b0-813d2107287d}"
- (Windows Vista, Windows 7 and Windows 8 only) HKEY_CLASSES_ROOT
  "CLSID\{60442b50-aac2-4db7-b9b0-813d2107287d}"

### Log File Location

You can enable or disable client-side logs by clicking **System > Log/Monitoring > Client Logs > Settings** in the Web console.

When you enable logging, Network Connect adds log files to the following location:

For Windows 2000/XP:
C:\Documents and Settings\All Users\Application Data\Juniper Networks\logging\debuglog.log

For Windows Vista, Windows 7 and Windows 8: C:\Users\username\AppData\roaming\Juniper Networks\logging\debuglog.log and C:\Users\public\Juniper Networks\logging\debuglog.log

### Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Network Connect Linux Client
- Network Connect Macintosh Clients
Required Rights to Run and Install Applications

Network Connect Linux Client

The following information applies to Linux clients only.

Application and Additional Files Installed by Network Connect

Network Connect installs the following files on the Linux client:

- ~/.juniper_networks/ncLinuxApp.jar
- ~/.juniper_networks/network_connect/installNC.sh
- ~/.juniper_networks/network_connect/libncui.so
- ~/.juniper_networks/network_connect/missing.info
- ~/.juniper_networks/network_connect/ncdiag
- ~/.juniper_networks/network_connect/NC.jar
- ~/.juniper_networks/network_connect/ncsvc
- ~/.juniper_networks/network_connect/version.txt
- ~/.juniper_networks/network_connect/xlaunchNC.sh

Files Remaining After Uninstall

No files remain on the Linux client after uninstall, but the ~/.juniper_networks/network_connect/ directory does remain.

Log Files Installed by Network Connect

Network Connect installs the following log files on Linux systems:

- ~/.juniper_networks/network_connect/installnc.log
- ~/.juniper_networks/network_connect/ncsvc.log
- ~/.juniper_networks/network_connect/ncuijava.log
- ~/.juniper_networks/network_connect/ncui.log

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Network Connect and GINA Windows Client
- Network Connect Macintosh Clients
- Required Rights to Run and Install Applications
Network Connect Macintosh Clients

The following information applies to Macintosh clients only.

Application and Additional Files Installed by Network Connect

Network Connect installs the following files on the Macintosh client:

- /Applications/Network Connect.app
- /usr/local/juniper/nc/version/ncproxyd
- /usr/local/juniper/nc/version/nctun[_tiger].kext
- ~/Library/Internet Plug-Ins/net.juniper.DSSafariExtensions.plugin
- ~/Library/Application Support/Juniper Networks/
  NetworkConnectMac_de.jar
  NetworkConnectMac_en.jar
  NetworkConnectMac_es.jar
  NetworkConnectMac_fr.jar
  NetworkConnectMac_ja.jar
  NetworkConnectMac_ko.jar
  NetworkConnectMac_zh.jar
  NetworkConnectMac_zh-cn.jar
  ~/Library/Application Support/Juniper Networks/
  NetworkConnectMac_ppc.jar (PowerPC-based Macintoshes)
  NetworkConnectMac_i386.jar (Intel-based Macintoshes)
  ~/Library/Java/Extensions/libJNPRAuthKit.jnilib
  /usr/local/juniper/nc/install/NCJarVerify.jar
  /usr/local/juniper/nc/install/installer.common
  /usr/local/juniper/nc/install/ncinstallhelper
  /usr/local/juniper/nc/install/fwk_reference_tool
  /usr/local/juniper/nc/install/uninstall_nc.sh
  /usr/local/juniper/nc/install/version

Files Remaining After Uninstall

The following files remaining on the Macintosh client after uninstall:

- All files in ~/Library/Logs/Juniper Networks/Network Connect
- /usr/local/juniper/nc/install/NCJarVerify.jar
- /usr/local/juniper/nc/install/installer.common
- /usr/local/juniper/nc/install/ncinstallhelper
- /usr/local/juniper/nc/install/fwk_reference_tool
- /usr/local/juniper/nc/install/uninstall_nc.sh

**Log Files Installed by Network Connect**

Network Connect stores the log files in the following location on the Macintosh client:

~/Library/Logs/Juniper Networks/Network Connect.

**Related Documentation**

- Pulse Secure Installer Service
- Pulse Secure Setup
- Network Connect and GINA Windows Client
- Network Connect Linux Client
- Required Rights to Run and Install Applications
CHAPTER 10 Terminal Services Client

- Juniper Terminal Services Client

Juniper Terminal Services Client

To run Juniper Terminal Services Client, the Secure Access Service downloads the Neotermservsetup.exe file (or the NeotermservsetupNT.exe file for Windows 2000 and earlier) to the user’s client. This package is responsible for downloading additional files to the user’s system in order to execute Terminal Services.

Installer Package Files and File Locations

The Secure Access Service downloads Neotermservsetup.exe (or NeotermservsetupNT.exe for Windows 2000 and earlier) to the user’s %Temp% directory and deletes it once the installation is complete.

Additional Files Installed by Package and File Locations

The Juniper Terminal Services Client installs additional Juniper proxy files in %APPDATA%\Juniper Networks\Juniper Terminal Services Client on the client:

The Juniper Terminal Services Client installs the following Juniper proxy files on the client:

- dsTermServ.exe
- dsTermServDt.dll
- dsTermServProxy.dll
- dsTermServResource_DE.dll
- dsTermServResource_en.dll
- dsTermServResource_ES.dll
- dsTermServResource_FR.dll
- dsTermServResource_JA.dll
- dsTermServResource_KO.dll
- dsTermServResource_ZH.dll
- dsTermServResource_ZH_CN.dll
- dsWinClient.dll
- dsWinClientResource_DE.dll
- dsWinClientResource_EN.dll
- dsWinClientResource_ES.dll
- dsWinClientResource_FR.dll
- dsWinClientResource_JA.dll
- dsWinClientResource_KO.dll
- dsWinClientResource_ZH.dll
- dsWinClientResource_ZH_CN.dll
- uninstall.exe
- versionInfo.ini

The Juniper Terminal Services Client installs the following files in `%APPDATA%\Juniper Networks\Juniper Terminal Services Client\Microsoft.VC80.CRT`:

- Microsoft.VC80.CRT.manifest
- msvcp80.dll
- msvcr80.dll

**Files Remaining After Uninstall**

None

**Registry Modifications**

The Juniper Terminal Services Client adds the following registry values under the registry key, `HKEY_CURRENT_USER\Software\Juniper Networks\Juniper Terminal Services Client`.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SZ</td>
<td>InstallPath</td>
<td><code>%APPDATA%\Juniper Networks\Juniper Terminal Services Client</code></td>
</tr>
<tr>
<td>REG_SZ</td>
<td>Language</td>
<td><code>user_locale</code>. The default is en.</td>
</tr>
</tbody>
</table>

Juniper Terminal Services Client sets the following string registry values in `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Juniper_Term_Services`.

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>DisplayName</td>
<td>“Juniper Terminal Services Client”</td>
</tr>
<tr>
<td>String</td>
<td>DisplayVersion</td>
<td>Set to the current software version</td>
</tr>
<tr>
<td>String</td>
<td>Publisher</td>
<td>“Juniper Networks”</td>
</tr>
<tr>
<td>String</td>
<td>QuietUninstallString</td>
<td>“%APPDATA%\Juniper Networks\Juniper Terminal Services Client\uninstall.exe” /S</td>
</tr>
<tr>
<td>String</td>
<td>StartupApp</td>
<td>“%APPDATA%\Juniper Networks\Juniper Terminal Services Client\dsTermServ.exe”</td>
</tr>
<tr>
<td>String</td>
<td>StopApp</td>
<td>“%APPDATA%\Juniper Networks\Juniper Terminal Services Client\dsTermServ.exe” – stop</td>
</tr>
<tr>
<td>String</td>
<td>UninstallString</td>
<td>“%APPDATA%\Juniper Networks\Juniper Terminal Services Client\uninstall.exe”</td>
</tr>
</tbody>
</table>
Log File Location

You can enable or disable client-side logs by clicking System > Log/Monitoring > Client Logs > Settings in the Web console.

When you enable logging, the Juniper Terminal Services Client adds the debuglog.log file to the following locations:

For Windows 2000/XP: %ALLUSERSPROFILE%\Application Data\Juniper Networks\Juniper Terminal Services Client

For Windows Vista, Windows 7 and Windows 8: %APPDATA%\Juniper Networks\Juniper Terminal Services Client

Related Documentation

- Pulse Secure Installer Service
- Pulse Secure Setup
- Required Rights to Run and Install Applications
CHAPTER 11 Citrix Services Client

Pulse Secure Citrix Services Client

To execute the Pulse Secure Citrix Services Client, the Secure Access Service downloads neoCitrixServSetup.exe to the user’s client. This executable downloads additional files to the user’s system.

Installer Package Files and File Locations

The Secure Access Service downloads NeoCitrixsrvsetup.exe to the user’s %Temp% directory and deletes it once the installation is complete.

Additional Files Installed by Package and File Locations

The Pulse Secure Citrix Services Client installs the following Juniper proxy files on the client in %APPDATA%\Juniper Networks\ Pulse Secure Citrix Services Client.

For administrators, Citrix client files are also installed to %ProgramFiles%\Citrix where %ProgramFiles% = %SystemDrive%\Program Files.

- dsCitrixConnector.dll
- dsCitrixProxy.exe
- dsCitrixProxyResource_DE.dll
- dsCitrixProxyResource_en.dll
- dsCitrixProxyResource_ES.dll
- dsCitrixProxyResource_FR.dll
- dsCitrixProxyResource_JA.dll
- dsCitrixProxyResource_KO.dll
- dsCitrixProxyResource_ZH.dll
- dsCitrixProxyResource_ZH_CN.dll
- dsWinClient.dll
- dsWinClientResource_DE.dll
- dsWinClientResource_EN.dll
- dsWinClientResource_ES.dll
- dsWinClientResource_FR.dll
- dsWinClientResource_JA.dll
• dsWinClientResource_KO.dll
• dsWinClientResource_ZH.dll
• dsWinClientResource_ZH_CN.dll
• uninstall.exe
• versionInfo.ini

Pulse Secure Citrix Services Client also installs the following files in %APPDATA%\Juniper Networks\Juniper Citrix Services Client \Microsoft.VC80.CRT:

• Microsoft.VC80.CRT.manifest
• msvcp80.dll
• msvcr80.dll

Files Remaining After Uninstall

None

Registry Modifications

The Pulse Secure Citrix Services client adds the following registry value under HKEY_CURRENT_USER\Software\Juniper Networks\Juniper Citrix Services Client:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>REG_SZ</td>
<td>Language</td>
<td>user locale. The default is en.</td>
</tr>
</tbody>
</table>

The Pulse Secure Citrix Services Client also sets the following registry values in HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Uninstall\Juniper_Citrix_Services:

<table>
<thead>
<tr>
<th>Type</th>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>String</td>
<td>DisplayName</td>
<td>&quot;Juniper Citrix Services Client&quot;</td>
</tr>
<tr>
<td>String</td>
<td>DisplayVersion</td>
<td>Set to the current software version</td>
</tr>
<tr>
<td>String</td>
<td>Publisher</td>
<td>&quot;Juniper Networks&quot;</td>
</tr>
<tr>
<td>String</td>
<td>QuietUninstallString</td>
<td>&quot;%APPDATA%\Juniper Networks\Juniper Citrix Services Client\uninstall.exe&quot; /S</td>
</tr>
<tr>
<td>String</td>
<td>StartupApp</td>
<td>&quot;%APPDATA%\Juniper Networks\Juniper Citrix Services Client\dsCitrixProxy.exe&quot;</td>
</tr>
<tr>
<td>String</td>
<td>StopApp</td>
<td>&quot;%APPDATA%\Juniper Networks\Juniper Citrix Services Client\dsCitrixProxy.exe&quot; –stop</td>
</tr>
<tr>
<td>String</td>
<td>UninstallString</td>
<td>&quot;%APPDATA%\Juniper Networks\Juniper Citrix Services Client\uninstall.exe&quot;</td>
</tr>
<tr>
<td>String</td>
<td>URLInfoAbout</td>
<td><a href="http://www.juniper.net">http://www.juniper.net</a></td>
</tr>
</tbody>
</table>
Log File Location

You can enable or disable client-side logs by clicking **System > Log/Monitoring > Client Logs > Settings** in the Web console. When you enable logging, the Pulse Secure Citrix Services Client adds the dsCitrixServ.log file to the following location:

For Windows 2000/XP:
\Documents and Settings\username\Application Data\Juniper Networks\Juniper Citrix Services Client

For Windows Vista, Windows 7 and Windows 8:
\Users\username\AppData\Roaming\Juniper Networks\Juniper Citrix Services Client

Related Documentation

- Juniper Networks Installer Service
- Juniper Networks Setup
- Required Rights to Run and Install Applications
PART 3 Appendices

- Required Permissions
Appendix A Required Permissions

- Required Rights to Run and Install Applications

Required Rights to Run and Install Applications

The following tables outline the rights that are required to install and run the following Secure Access Service client-side components using the Secure Access Service’s ActiveX, ActiveX installer service, and Java mechanisms.

Where applicable, the tables contain links to topics that describe in further detail the components that the Secure Access Service uses to install and run its client-side applications.

Table 2: Windows Secure Application Manager (WSAM)

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX: Installer Service</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Admin</td>
<td>Not Applicable</td>
</tr>
<tr>
<td>Run</td>
<td>Standard User</td>
<td>Standard User</td>
<td>Standard User</td>
<td>Not Applicable</td>
</tr>
</tbody>
</table>

NOTE:
- Restricted users can perform the initial installation of WSAM with the installer service only if they start the installation by clicking the WSAM link in the user’s portal page.
- The ActiveX installer requires users to reboot their systems after an installation or upgrade (Windows Mobile only).
- Users must have ActiveX components or Java enabled through their browsers to use the WSAM installers.

Table 3: Java Secure Application Manager (JSAM)

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX: Installer Service</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>JSAM</td>
<td>Not Applicable</td>
<td>Not Applicable</td>
<td>Restricted, Power User, or Admin</td>
<td>User</td>
</tr>
</tbody>
</table>

JSAM with Host File Modification
NOTE:

- **JSAM Windows XP/2000:**
  - Automatic host mapping: you must have the rights to run regedit.exe in "read-only" mode, and the rights to modify the hosts file.
  - Outlook and NetBIOS applications: you must have the rights to run regedit.exe in "read/write" mode.
- **JSAM Windows Vista, Windows 7 and Windows 8:**
  - Automatic host mapping: you must have the rights to install jsamtool.exe on the system and run it.
  - Outlook and NetBIOS applications: you must have the rights to install jsamtool.exe on the system and run it.
- **JSAM Mac OS X:**
  - Automatic host mapping: you must provide the administrator password when JSAM prompts for it at launch.
  - Any applications that listen on ports below 1024: you must provide the administrator password when JSAM prompts for it at launch.
- **JSAM Linux:**
  - Automatic host mapping: you must be the root user.
  - Any applications that listen on ports below 1024: you must be the root user.

### Table 4: Network Connect

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install’</td>
<td>Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Admin</td>
<td>Admin*</td>
<td>“Network Connect Macintosh Clients”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Network Connect Linux Client”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Network Connect and GINA Windows Client”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Network Connect Linux Client”</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>“Network Connect and GINA Windows Client”</td>
</tr>
</tbody>
</table>

NOTE:

- Restricted users can perform the initial installation of Network Connect with the installer service only if they start the installation by clicking the Network Connect link in the user's portal page.
- (Mac only) When Network Connect is first installed (before ncinstallhelper exists on the system), you must provide the administrator password when prompted during the installation. On subsequent launches no special privileges are required.
- When the installer service is running, uninstalling Network Connect as a restricted user should be done from the user browser’s preference page.

* Linux also requires Admin rights to upgrade or downgrade Network Connect. Macintosh does not have this restriction.
Table 5: Terminal Services Component

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Juniper Terminal Services Client&quot;</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Juniper Terminal Services Client&quot;</td>
</tr>
</tbody>
</table>

Table 6: Citrix Terminal Services Component

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>Citrix Client</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>Power User or Admin</td>
<td>&quot;Pulse Secure Citrix Services Client&quot;</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>Restricted, Power User, or Admin</td>
<td>&quot;Pulse Secure Citrix Services Client&quot;</td>
</tr>
</tbody>
</table>

Table 7: Host Checker (includes Secure Virtual Workspace)

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Host Checker Linux Clients&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;Host Checker Macintosh Clients&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;Host Checker Windows Client&quot;</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Host Checker Linux Clients&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;Host Checker Macintosh Clients&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>&quot;Host Checker Windows Client&quot;</td>
</tr>
</tbody>
</table>

**NOTE:** If you implement SVW through Host Checker, note that restricted users, power users, and admins all have adequate rights to install and run SVW.
### Table 8: Enhanced Endpoint Security

<table>
<thead>
<tr>
<th>Action</th>
<th>EES on Windows without installer service</th>
<th>EES on Windows with installer service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Power User, Admin</td>
<td>Restricted, Power User, or Admin</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
</tr>
</tbody>
</table>

### Table 9: Cache Cleaner

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Cache Cleaner&quot;</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Cache Cleaner&quot;</td>
</tr>
</tbody>
</table>

### Table 10: Pulse Secure Collaboration

<table>
<thead>
<tr>
<th>Client/Action</th>
<th>ActiveX Windows</th>
<th>ActiveX: Installer Service Windows</th>
<th>Java Windows</th>
<th>Java Mac/Linux</th>
<th>More Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pulse Secure Collaboration: Win32</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Pulse Secure Collaboration Windows Client&quot;</td>
</tr>
<tr>
<td>Run</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>Restricted, Power User, or Admin</td>
<td>Not Applicable</td>
<td>&quot;Pulse Secure Collaboration Windows Client&quot;</td>
</tr>
</tbody>
</table>

| **Pulse Secure Collaboration: Java** | | | | | |
| Install (see Note below) | Restricted, Power User, or Admin | Not Applicable | Restricted, Power User, or Admin | User | "Pulse Secure Collaboration Windows Client" |
      | | | | | "Pulse Secure Collaboration Linux Client" |
      | | | | | "Pulse Secure Collaboration Macintosh Clients" |
Run | Restricted, Power User, or Admin | Not Applicable | Restricted, Power User, or Admin | User | “Pulse Secure Collaboration Windows Client”
|---------------------------------|--------------|----------------|------|----------------------------------|
| “Pulse Secure Collaboration Linux Client”
| “Pulse Secure Collaboration Macintosh Clients”

Junos Pulse Collaboration: Outlook Plug-in

| Install | Power User, or Admin | Not Applicable | Power User, or Admin | Not Applicable | “Pulse Secure Collaboration Plug-In”
|---------|----------------------|--------------|----------------------|--------------|
| Run     | Restricted, Power User, or Admin | Not Applicable | Restricted, Power User, or Admin | Not Applicable | “Pulse Secure Collaboration Plug-In”

NOTE: On Windows Vista, Windows 7 and Windows 8, if Pulse Secure Collaboration is installed with restricted user privilege, remote control of high privilege processes (such as regedit and so forth) is not available.

Pulse Secure Collaboration requires the end-user to have admin privileges in order to install the client software on Windows Vista and later operating systems. If JIS is installed on the end-user’s system, JIS installs the Pulse Secure Collaboration client and user admin privilege is not required. If JIS is not installed and the user does not have admin privilege, the client software is installed with limited features.

Related Documentation

- Juniper Networks Installer Service
- Juniper Networks Setup
PART 4 Index

C

customer support ..................
contacting PSGSC ..........

S

support, technical See technical support

T

technical support
contacting PSGSC ..........