

USER GUIDE

WWPass Security for VPN (Juniper VPN)

For WWPass Security Pack 2.4

March 2014

TABLE OF CONTENTS

Chapter 1 — Getting Started	. 3
Introducing WWPass Security for VPN (Juniper VPN)	.4
Related Documentation	.5
Presenting Your PassKey to Your Computer	.6
Need Assistance?	.7
Report a Problem from Dashboard	.7
Chapter 2 — Requirements	. 8
System Requirements	. 8
User Requirements	.9
Chapter 3 — Setup for Administrators	10
Smart Start for Administrators	11
Prepare to Issue Certificates from a CA	12
Guidelines for deploying an Internal Microsoft CA	12
Install a Device Certificate	13
Install a Trusted Client CA Certificate	17
Configure a Certificate Server	19
Configure CRL Checking	21
Set Smart Card Group Policies	22
Chapter 4 — Setup for Users	23
Smart Start for Users	24
Obtain a Certificate	24
Guidelines	24
Obtain a Certificate Via Active Directory Certificate Services	25
Import a Certificate Using the WWPass Dashboard	27
Chapter 5 — Use Your PassKey to Log In	28
Log Into Juniper VPN Using a PassKey	29



CHAPTER 1 — GETTING STARTED

This chapter introduces WWPass® Security for VPN (Juniper VPN)[™] and provides basic information on using a PassKey[™] from WWPass, accessing related documentation, and contacting WWPass Product Support.

Topics In This Chapter

- Introducing WWPass Security for VPN (Juniper VPN)
- Related Documentation
- <u>Presenting Your PassKey to Your Computer</u>
- Need Assistance?



Introducing WWPass Security for VPN (Juniper VPN)

This documentation covers how to set up and use WWPass Security for VPN (Juniper VPN), the WWPass authentication solution for Juniper VPN.



WWPass Security for VPN (Juniper VPN) allows users to log into a Juniper SSL VPN using a PassKey instead of a username and password.

Authentication is certificate-based. An X.509 certificate is associated with each user's PassKey and presented for login via their PassKey. The certificate is stored in WWPass secure cloud storage, where it cannot be stolen.

PassKey authentication provides the strongest protection available for the sensitive business information that can be accessed via an organization's Virtual Private Network.

Click here for information about PassKeys in KeySet help.

Note: WWPass Security for VPN (Juniper VPN) is part of the WWPass Security Pack[™] and is shown in the WWPass Dashboard[™] on Windows computers. The Security Pack allows you to activate a PassKey and use WWPass authentication solutions. Dashboard shows you the solutions included in the Security Pack. Click <u>here</u> to access documentation for the Security Pack.

Related Documentation

This documentation provides information on WWPass Security for VPN (Juniper VPN) for system administrators and end users.

For information on the Security Pack it is part of, click links in the list below. The list includes documentation on installing the Security Pack, on other WWPass solutions in the Security Pack, and on the WWPass KeySets that are used with these solutions for secure authentication.

WWPass KeySets and Key Services	<u>HTML</u>	<u>PDF</u>
WWPass Security Pack		
Installation		
Windows	HTML	<u>PDF</u>
Mac	HTML	<u>PDF</u>
Linux	HTML	<u>PDF</u>
WWPass Dashboard for Security Pack	<u>HTML</u>	<u>PDF</u>
WWPass Solutions for Security Pack		
WWPass Security for Email (Outlook & OWA)	<u>HTML</u>	<u>PDF</u>
Security for Email (Thunderbird)	HTML	<u>PDF</u>
WWPass Security for VPN (Juniper VPN)	HTML	Currently open
Security for VPN (OpenVPN)	<u>HTML</u>	<u>PDF</u>
WWPass Security for Windows Logon	<u>HTML</u>	<u>PDF</u>
WWPass Security for SharePoint	<u>HTML</u>	<u>PDF</u>
Personal Secure Storage		
Windows		<u>PDF</u>
Мас		<u>PDF</u>
Linux		<u>PDF</u>

🛩 wwpass®



Presenting Your PassKey to Your Computer

To use your PassKey, you "present" it to your computer and enter your access code, if prompted for this.

How do you "present" a Key to a computer? This depends on your KeySet type:

- If you have an NFC / USB KeySet, you can place a Key on an NFC reader or insert a Key into a USB Port.
- If you have a USB KeySet, you can insert a Key into a USB port.

Enter the access code for a Key using exactly the same characters and cases (upper or lower) it was created with.

You are given three chances to enter the correct code. If you enter the wrong access code three times in a row, your PassKey is locked for 15 minutes and cannot be used.

You are given three chances to enter the correct code. If you enter the wrong access code three times in a row, your PassKey is locked for 15 minutes and cannot be used.



Need Assistance?

If you encounter a problem or have a question, you can contact WWPass Product Support as follows:

Phone 1-888-WWPASS0 (+1-888-997-2770)

Email support@wwpass.com

Report a Problem from Dashboard

An easy way to report a problem is to email Product Support from the WWPass Dashboard, included in the WWPass Security Pack.

The email identifies version numbers for your Security Pack and operating system. In addition, current logs for WWPass software are automatically attached to the email.

Logs contain information that can help Product Support troubleshoot any problem you experience. For example, logs contain information such as actions and their times, and services accessed. Actions include PassKey authentication for login, email signing, and email decryption.

Logs are located in Users\username and ProgramData. They should not be changed before they are sent to Product Support.

To report a problem from Dashboard

- 1. Click the mail button in the upper-right corner of Dashboard.
- 2. In the Support window that opens, type a description of the problem you need help with. You can also type a question.
- 3. Enter the email address Product Support should reply to. Also enter your name.
- 4. Click Submit Report to send your report along with the current version of all available logs.

Dear Service Desk,		
I cannot digitally sign my	y email.	
I received a message sa to my computer.	aying my certificate was not available even though my PassKey w	as <mark>presented</mark>
Sincerely,		
End User		
End User		
End User Name (optional)	End User	
End User Name (optional) Email Address (optional)	End User user @email.com	

CHAPTER 2 — REQUIREMENTS

System Requirements

Requirement	Details				
Juniper SA SSL VPN	This provides VPN access to your network. Supported products are Juniper Secure Access SSL VPN Series Appliance versions 7.0R2 through 7.1R1.				
Windows Server and domain-based network	Windows Server 2008 and 2008 R2 (32-bit and 64-bit) are supported. Microsoft Internet Information Services (IIS) should be enabled on Windows Server.				
Internet access	Outbound TCP connections must be allowed from user computers to ports 80 (HTTP) and 443 (HTTPS). Network software and hardware (including routers and firewalls) should not block connections to these ports.				
Certificate Authority	 A Certificate Authority (CA) is needed to issue a Trusted Client CA certificate (root certificate) and client-side certificates for users (see below). Both types of certificates must be issued by the same CA. The CA can be: An internal CA such as the Microsoft Enterprise CA that issues domain-based, self-signed certificates that are trusted within your organization. An external third-party CA such as Comodo. 				
Certificates	 The following certificates are needed for authenticating users into your Juniper VPN: Device certificate—This is installed on your SA Series Appliance and helps to secure network traffic to and from your Secure Access Service using information such as organization name, a copy of your organization's public key, the digital signature of the certificate authority (CA) that issued the certificate, serial number, and expiration date. A device certificate can be requested and imported from the administration console for your SA Series Appliance (e.g., Central Manager). Trusted Client CA certificate—This is installed on your SA Series Appliance and serves as a root certificate. It is used by your Secure Access Service to validate client-side user certificates during login. A Trusted Client CA certificate is obtained from your CA. The Secure Access Service supports X.509 CA certificates in DER and PEM formats. Client-side user certificates—These are associated with user PassKeys and used to authenticate users when they log into your Juniper VPN. User certificates are obtained from your CA. 				



User Requirements

Requirement	Details			
Computer with Windows operating system	 The following versions of Windows are supported: Microsoft Windows 8.1 (32-bit and 64-bit) Microsoft Windows 8 (32-bit and 64-bit) Microsoft Windows 7 (32-bit and 64-bit) Note: Outbound TCP connections must be allowed to ports 80 (HTTP) and 443 (HTTPS). 			
Windows account	A Windows domain account is used for both your Windows network and your Juniper VPN. The Windows account is mapped to the VPN through Microsoft Active Directory.			
Client-side user certificate	This a digital X.509 certificate from the Certificate Authority (CA) used by your organization. It serves as a credential that authenticates your identity when you log into your Juniper VPN with a PassKey.			
Web browser	 The following web browsers are supported: Internet Explorer 8 and later (32-bit and 64-bit) Chrome 20 and later Firefox 14 and later Opera 11 and later 			
WWPass KeySet	This includes the PassKey used for logging into your Juniper VPN. Click here to open KeySet help.			
WWPass Security Pack	This includes software that is needed to activate your PassKey and use WWPass Security for VPN (Juniper VPN). Click here to open Security Pack help.			



CHAPTER 3 — SETUP FOR ADMINISTRATORS

This chapter covers setup for system administrators. It includes information on essential tasks that must be performed before users can authenticate into a Juniper SA SSL VPN using a PassKey.

For information on additional setup, see the appropriate Juniper Secure Access Administration and Installation Guide. For example, refer to Juniper documentation for information on:

- Authentication realms
- Role mapping rules
- Authentication servers
- Authentication policies
- Sign-in URLs
- Adding users to CRLs (certificate revocation lists)

Topics In This Chapter

- Smart Start for Administrators
- Prepare to Issue Certificates from a CA
- Install a Device Certificate
- Install a Trusted Client CA Certificate
- Configure a Certificate Server
- <u>Configure CRL Checking</u>
- Set Smart Card Group Policies

Smart Start for Administrators

This Smart Start is an overview of the main setup steps for system administrators. It provides a road map to follow as you go through the setup process.

Smart Start

- 1. Prepare for <u>issuing certificates</u> with a CA (Certificate Authority). The CA will generate a Trusted Client CA certificate for your SA Series Appliance and client-side certificates for user PassKeys.
- 2. Install a <u>device certificate</u> on your SA Series appliance using the administration console:
 - a) Obtain a certificate from a CA (Certificate Authority) by creating a CSR (certificate signing request).
 - b) Import the certificate.
- 3. Install a <u>Trusted Client CA certificate</u> on your SA Series Appliance via the administration console.
- 4. Configure a <u>certificate server</u> for authentication.
- 5. Configure <u>CRL checking</u>. This allows the SA Series Appliance to use a CRL (certificate revocation list) to validate user certificates.
- 6. Set <u>Smart Card Group Policies</u> for user computers across your domain. PassKeys use Smart Card technology.
- 7. Set up a PassKey for your own use:
 - a) Install the WWPass Security Pack on your computer. Click here for Security Pack help.
 - b) Obtain and activate a WWPass KeySet. This includes a PassKey. Click <u>here</u> for KeySet help. (If you are currently using another WWPass solution, your KeySet is already activated.)
 - <u>Obtain</u> a certificate for your Juniper VPN and associate it with your PassKey. <u>Present</u> your PassKey to your computer before you begin.

^a wwpass°



Prepare to Issue Certificates from a CA

This topic provides general information on preparing to issue digital X.509 certificates from a Certificate Authority (CA).

A CA is needed to issue a Trusted Client CA certificate (root certificate) for your Secure Series Appliance and client-side certificates for users. The Trusted Client CA certificate is used to validate user certificates. Both types of certificates must be issued by the same CA.

The CA can be:

- An internal CA such as the Microsoft Enterprise CA. This issues domain-based, self-signed certificates that are trusted within your organization. Guidelines are provided below.
- An external third-party CA such as Comodo.

For more information, see Juniper documentation.

Note: The Secure Access Service supports X.509 CA certificates in the DER and PEM formats.

Guidelines for deploying an Internal Microsoft CA

Below are guidelines on setting up to issue domain-based certificates from a Microsoft CA server on your Windows domain. Windows Server 2008 and 2008 R2 are supported.

Users can enroll for certificates via their browsers from Active Directory Certificate Services (included with the Microsoft CA server.)

Basic guidelines are to:

- 1. Select the Active Directory Certificate Services role from Server Manager for Windows Server. Also select the following role services:
 - Certification Authority (issues certificates).
 - Certification Authority Web Enrollment (provides the Active Directory web interface for certificate enrollment).
- Configure the Smart Card Logon template for the CA. The template's default setting for CSP (Cryptographic Service Provider) should be Microsoft Base Smart Card Crypto Provider. (This setting associates a certificate with a user's PassKey.) Users select Smart Card Logon as the Certificate Template when they request a certificate.
- 3. For the Active Directory Domain Controller, make sure:
 - Smart Card authentication is enabled.
 - A Domain Controller certificate is installed. This should be valid for your Active Directory domain.
 - The Domain Controller trusts the CA used to issue X.509 certificates to users.
 - The HTTPS protocol is bound to the IIS server.



Install a Device Certificate

Follow the procedures below to request and install a digital device certificate for your SA Series Appliance:

- The first procedure tells you how to create a CSR (certificate signing request) and send the request to your CA.
- The second procedure tells you how to import the signed certificate to your SA Series Appliance.

Both procedures are performed from the Secure Access Service administration console (e.g., Central Manager). You can skip these procedures if a digital certificate is already installed on your Web servers.

A device certificate helps to secure network traffic to and from your Secure Access Service using information such as your organization name, a copy of your organization's public key, the digital signature of the certificate authority (CA) that issued the certificate, a serial number, and expiration date.

Note: When you create a CSR through the administration console, a private key is created locally that corresponds to the CSR. If you delete the CSR, the private key is also deleted, which prohibits you from installing a signed certificate generated from the CSR.

To create a CSR

1. In the administration console, choose System > Configuration > Certificates > Device Certificates. The Certificates tab of the Configuration page appears.

JUNIPEr.			
Central Manager			
 System Status Configuration Network Clustering Status a 	Configuration Security Certificates DMI Agent NCP Device Certificates Trusted Client CAs Tru	Sensors Client Types Secure Meet	ang Vintual Desixtops Viser Record Synchronization REv2
IF-MAP Federation Log/Monitoring Authentication Signing In Endpoint Security Auth. Servers	Specify the Device Certificate(s). If you don' Import Certificate & Key Delete	t have a certificate yet, you can create a	a CSR and import the resulting signed certificate. If necessary, you
- Administrators	Certificate issued to	Issued by	Valid Dates
Admin Realms Admin Roles User Realms User Realms User Roles Resource Profiles	iniper.tex.com	tex-CA-CA	Apr 19 17:30:01 2013 GMT to Apr 19 17:30:01 2015 GMT
Resource Policies Junos Pulae	New CSR Delete		

2. Click New CSR. The New Certificate Signing Request page appears.

Configuration >

Common Name: (e.g., secure.company.com)	juniper.company.com
Organization Name: (e.g., Company Inc.)	Company Inc.
Org. Unit Name: (e.g., IT Group)	IT Group
Locality: (e.g., SomeCity)	AnyCity
State (fully spelled out): (e.g., California)	NH
Country (2 letter code): (i.e., US)	US
Email Address:	manager@company.com
Key Length:	● 1024-bit ○ 2048-bit
Please enter some random cl We recommend that you ent	naracters to augment the system's random key generator. er approximately twenty characters.
Random Data:	

3. Enter the required information and click **Create CSR**. The Pending Certificate Signing Request page appears.

Q CSR created successfully	
Your CSR was created successfully. See below for instructions on sending the CSR to a Certificate Authority. The certificate approval process may take several days. When you receive the signed certificate from the Certific	ate Authority, you will need to import the certificate to complete this process.
Configuration > Pending Certificate Signing Request	
CSR Details	
Common Name: juniper.company.com Created: 6/12/2013 9:31:1	
Org. Name: Company Inc. Locality: AnyCity Org. Unit Name: IT Group State: NH Email Address: manage@company.com Country:US Key Size: 1024 bits	
Back to Device Certificates	
Step 1. Send CSR to Certificate Authority for signing	
To send the CSR to a Certificate Authority (CA), you need to copy the encoded text below, including the	BEGIN and END lines, and submit it to the CA in one of the following ways:
 Save the text as a ,cert file and attach it to an email message to the CA Paste the text into an email message to the CA Paste the text into a Veb form provided by the CA 	
Note: Manage the CSR process carefully. If you submit more than one CSR to a CA, you may be billed f	or each CSR.
BEGIN CERTIFICATE REQUEST	
MIIBZTCCAUICAQAwgZgxCzAJBgNVBAYTAIVTNQswCQYDVQQIEwJOSDEQMA4GA1UE BxMHQW55Q210eTERMABGA1UECxMISVQgR3JvdXAxFTATBgNVBAcTDENvbXBhbnxg	
SW5jLjEcMBoGAlUEAxMTanVuaXBlc15jb2lwYW55LmNvbTE1MCAGCSqGS1b3DQEJ ARYTbWFuYWdlckBjb21wYW55LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC	~

4. Follow the instructions shown. These explain what information to send to your CA and how to send it.



5. When you receive the signed certificate from the CA, save the certificate in a location that can be accessed by your administration console. Then import the certificate file using the next procedure.

To import the certificate generated from a CSR

1. In the administration console, choose System > Configuration > Certificates > Device Certificates. The Certificates tab of the Configuration page appears.

Configuration		
Security Certificates DMI Agent NCP 5	ensors Client Types Secure Meeting V	Virtual Desktops User Record Synchronization IKEv2
Device Certificates Trusted Client CAs Truste	Server CAs Code-signing Certificates Clie	ent Auth Certificates
Specify the Device Certificate(s). If you don't h	ave a certificate yet, you can create a CSR a	and import the resulting signed certificate. If necessary, yo
Import Certificate & Key Delete]	
Certificate issued to	Issued by	Valid Dates
juniper.tex.com	tex-CA-CA	Apr 19 17:30:01 2013 GMT to Apr 1 2015 GMT
New CSR Delete		
Certificate Signing Requests		Created
Pending CSR for juniper.company.com	6/12/2013 09:31:01	

2. Under Certificate Signing Requests, click the **Pending CSR** link that corresponds to the signed certificate. The Pending Certificate Signing Request page appears.

CSR	created suc	cessfully		
Your CS	R was creat	ted successfully. Se	e below for instructions on sending the CSR to a Certificate Authority.	
The cert	tificate appr	oval process may t	ake several days. When you receive the signed certificate from the Certific	ate Authority,
Configurat Pend	ing Cer	rtificate Sig	ning Request	
CS	R Details			
Core	mmon Name: ated:	juniper.company.com 6/12/2013 9:31:1	n	
Org Org Em Key), Name:), Unit Name: ail Address: y Size:	Company Inc. IT Group manager@company. 1024 bits	Locality: AnyCity State: NH com Country: US	
Back to (Device Certi	ficates		
Step 1.	Send CSR	to Certificate Au	thority for signing	
	To send th	e CSR to a Certific	ate Authority (CA), you need to copy the encoded text below, including the	e BEGIN and E
	• Sa • Pa • Pa	we the text as a ,ce ste the text into an ste the text into a	ert file and attach it to an email message to the CA email message to the CA Web form provided by the CA	
	Note: Man	age the CSR proce	ss carefully. If you submit more than one CSR to a CA, you may be billed	for each CSR.
	B	EGIN CERTIFI	CATE REQUEST	
	MIIB2T BxMHQW	CCAUICAQAwgZ 55Q210eTERMA	gxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJOSDEQMA4GA1UE 8GA1UECxMISVQgR3JvdXAxFTATBgNVBAoTDENvbXBhbnkg	^
	SW5jLj ARYTbW	EcMBoGA1UEAx FuYWdlckBjb2	MTanVuaXBlci5jb21wYW55LmNvbTE1MCAGCSqGSIb3DQEJ 1wYW55LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC	~



3. Under Import Signed Certificate, browse to the certificate file you received from the CA. Then click **Import**.

Step 2.	Import signed certificate When you receive the signed certificate file from the CA, select it below and click Import. This will add the signed certificate and remove this pending CSR					
	Signed certificate:	Browse				
	Import					



Install a Trusted Client CA Certificate

Follow the steps below to install a Trusted Client CA certificate on your SA Series Appliance. All steps are performed from the Secure Access Service administration console (e.g., Central Manager).

The Secure Access Service uses the Trusted Client CA certificate to validate user certificates during login. It checks to make sure a user certificate is not expired or corrupt and that it is signed by your CA.

Before you begin, obtain a Trusted Client CA certificate from your CA. The certificate must be available for upload in step 3 below.

The Secure Access Service supports X.509 CA certificates in DER and PEM formats.

Note: In addition to installing a CA certificate on your SA Series Appliance, you need to enable authentication by configuring a <u>certificate server</u>.

To install a CA certificate on the SA Series Appliance

1. In the administration console, choose System > Configuration > Certificates > Trusted Client CAs. The Certificates tab for the Configuration page appears.

JUNIPEr.					·
Central Manager					Help Guidance Sign Out
Configuration	Configuration				
Network Clustering IF-MAP Federation	Security Certificates D Device Certificates Trusted C	MI Agent NCP Se lient CAs Trusted Ser	ensors Client Type ver CAs Code-signin	s Secure Meeting Virtual Des g Certificates Client Auth Certificates	ktops User Record Synchronization IKEv2
Log/Monitoring (Authentication Signing In Endpoint Security (Users can be required to pre certificate authorities.	esent valid client-side	e certificates to sigr	n in (see the realm-specific <u>Certif</u>	icate Authentication Policy page). Specify trusted
Auth. Servers	Auto-import options	Import CA Certifi	cate Delete		
Admin Realms + Admin Roles +	Trusted Client CA		Trusted for client authentication?	Valid dates	Status checking
- Users	tex-CA-CA		Yes	2013/04/19 - 2018/04/19	Use CRLs

2. Click Import CA Certificate. The Import Trusted Client CA page appears.

File Edit View F	avorites Tools Help 🗮 🕶 Page = Safety = Tools = 😥 =	
JUNIPEr.		^
Central Manager		Help Guidance Sign Out
Status Status Configuration Network	Configuration > Trusted Client CAs > Import Trusted Client CA	
Clustering	Certificate file	
IF-MAD Federation	Import from: Browse	
Signing In Endpoint Security Auth. Servers	Import Trusted Client CA?	

- 3. Browse to the CA certificate you want to import, select it, and click **Open**.
- 4. From the Import Trusted Client CA page, click **Import Certificate**. The Trusted Client CA page appears.

 In the Client Certificate Status checking section, select Use CRLs as the certificate validation method. This tells the SA Series Appliance to use a CRL (Certificate Revocation List) to validate user certificates.



6. Uncheck the **Verify Trusted Client CA** option if you do not want the SA Series Appliance to validate the CRL from which the certificate is issued.



7. Select the **Trusted for Client Authentication** flag. This tells the SA Series Appliance to trust the CA certificate when authenticating user certificates.



8. Make sure the **Participate in Client Certificate Negotiation** flag is selected (the default setting). This tells the SA Series Appliance to send a list of trusted client CAs to user browsers for certificate selection. (This flag is disabled when the **Trusted for Client Authentication** flag is disabled.)

Participate in Client Certificate Negotiation	
Indicating whether this CA will be sent to the browser for client certificate selection CA chain of the certificate should be deselected.	. To stop a client certificate

9. Click Save Changes.

e wwpass°



Configure a Certificate Server

Follow the steps below to enable authentication by creating a certificate server on the SA Series Appliance. All steps are performed from the Secure Access Service administration console (e.g., Central Manager).

A certificate server is a type of local authentication server. It allows you to authenticate users based on certificate attributes and can be used instead of a standard authentication server (such as LDAP or RADIUS).

To configure a certificate server

1. In the administration console, choose Authentication > Auth. Servers. The Authentication Servers page appears.

File Edit View Fa	vorites Tools Help ĝi ▼ Page ▼ Safety ▼ Tools ▼ 🕢 ▼	
JUNIPEr.		
Central Manager		
Status Configuration Network Clustering TF-MAP Federation Log/Monitoring	Authentication Servers	Delete
- Authentication	Authentication/Authorization Servers	Туре
Signing In +	Administrators	Local Authentication
Auth. Servers	ca.tex.com	Certificate Server
- Administrators	System Local	Local Authentication
Admin Realms	🗆 test	Certificate Server
- Users	test2	Certificate Server

2. Select Certificate Server from the **New** list. Then click **New Server**. The New Certificate Server page appears.

File Edit View	Far	vorites Tools Help s + Page + Safety + To	ols • 😥 •
JUNIPEr.			
Central Manager			
System		A REPORT OF THE REPORT OF	
Status		Auth Servers >	
Configuration		New Certificat	e Server
Network			
Clustering			
IF-MAP Federatio	n »	Mamou	ExtDanakard anin
Log/Monitoring		Name;	[of Passive y Login
- Authentication		User Name Template:	<certdn.cn></certdn.cn>

3. Enter a name to identify the server instance. The name can contain variables for substitution, for example, <certAttr.serialNumber> or <certAttr.altName.xxx>.

- In the User Name Template field, specify how the SA should construct a username. You can use a combination of plain text and certificate variables in angle brackets, for example, <certAttr.serialNumber> or <certAttr.altName.xxx>>.
- 5. Click Save Changes.
- 6. Specify which user realms should use the certificate server for authentication. To do this:
 - a. Choose Users > User Realms or Administrators > Admin Realms. The Authentication Realms page for users or administrators appears.

User Authent	ication Realms		
View: Overview	✓ for all realms	✓ Update	
New Duplicate.			
Authentication P	tealm		Servers
Users			Primary: ForPassKeyLogin

b. Click **Users** from User Authentication Realms. Click **Admin Users** from Administrator Authentication Realms. The General tab of the Users or Admin Users page appears.

User Authentication Realms > Users		
General Authentication Poli	cy Role Mapping	
Name:	Users	Label to reference this realm
Description:	Default authentication realm for users	
	U When editing, start on the Rol	e Mapping page
Servers		
Specify the servers to use for authe	ntication and authorization. To create or manage ser	vers, see the <u>Servers</u> page.
Authentication:	ForPassKeyLogin 🗸	Specify the server to use for authenticating users.
Directory/Attribute:	None 🗸	Specify the server to use for authorization.
Accounting:	None 🗸	Specify the server to use for Radius accounting.

- c. Select the certificate server from the Authentication list in the General tab.
- d. Click Save Changes.
- 7. Associate the user realms with sign-in URLs using settings in the Authentication > Signing In > Signin Policies page.

🛩 wwpass°



Configure CRL Checking

Follow the steps below to configure CRL checking. This allows the SA Series Appliance to use a CRL (certificate revocation list) to validate user certificates. All steps are performed from the Secure Access Service administration console (e.g., Central Manager).

Configuration settings tell the SA Series Appliance where to find the CRL and how often to download it. The CRL should be downloaded frequently enough to ensure that certificate validation is based on current information.

To configure CRL checking

1. In the administration console, choose System > Configuration > Certificates > Trusted Client CAs. The Configuration page appears.

JUNIPEr.					
Central Manager					Help
Configuration	Configuration				
Network Clustering IF-MAP Federation	Security Certificates D Device Certificates Trusted C	MI Agent NCP Sensors	Client Types S	cure Meeting Virtual Desktops I kates Client Auth Certificates	Jser Record Synchronization KEv2
Log/Monitoring Authentication Signing In Endpoint Security	Users can be required to pre authorities.	sent valid client-side cert	ificates to sign in (s	ee the realm-specific <u>Certificate Aut</u>	hentication Policy page). Specify trusti
Auth. Servers	Auto-import options	Import CA Certificate	Delete		
Admin Realms Admin Roles	C Trusted Client CA	1	rusted for client authentication?	Valid dates	Status checking
- Users	E tex-CA-CA	1	/es	2013/04/19 - 2018/04/19	Use CRLs
User Roles	AddTrust External C	A Root	/es	2000/05/30 - 2020/05/30	Use CRLs

2. Click the link for your CA certificate. This should be the Trusted Client CA certificate installed on the SA Series Appliance. The Trusted Client CA page appears.

JUNIPER.		
Central Manager		
- System		
Status		Configuration > Trusted Client CAs >
Configuration	1.	Trusted Client CA
Network	-	Trusted cheft en
Clustering		Certificate
IF-MAP Federation		
Log/Monitoring		Issued To: AddTrust External CA Root
- Authentication		Issued By: AddTrust External CA Root
Signing In	1.	Valid Dates May 20 10,49,29 2000 GMT - May 20 10,49,29 2020 GMT
Endpoint Security		Valid Dates: May 30 10140130 2000 GMT + May 30 10140130 2020 GMT
Auth. Servers		Details: Cther Certificate Details
- Administrators		
Admin Realms		Renew Certificate
Admin Roles		

3. Click CRL Checking Options at the bottom of the page. CRL Checking Options appear.



Set Smart Card Group Policies

This topic covers the Smart Card Group Policies that should be set for computers on your Windows domain using a method such as the Group Policy Object Editor. PassKey authentication uses Smart Card technology.

The policies and required settings are as follows:

- Smart Card service—Startup type for this should be Automatic. In addition, the service should be started. If this service is stopped on a user computer, the computer will not be able to read the user's PassKey. The Smart Card service is shown as SCardSvr in Windows Task Manager.
- **Smart Card Removal Policy Service**—Startup type for this should be automatic. The Smart Card Removal Policy service is shown as SCPolicySvc in Windows Task Manager.



CHAPTER 4 — SETUP FOR USERS

This chapter covers setup for users. It includes information on essential tasks that must be performed before you can log into your Juniper VPN using your PassKey.

Topics In This Chapter

- Smart Start for Users
- Obtain a Certificate
- Import a Certificate Using the WWPass Dashboard

Smart Start for Users

This Smart Start is an overview of the main setup steps for users. It provides a road map to follow as you go through the setup process.

Smart Start

- 1. Install the WWPass Security Pack on your computer. Click here for Security Pack help.
- 2. Obtain and activate a WWPass KeySet. This includes a PassKey. Click here for KeySet help.

Note: If you are currently using another WWPass solution, your KeySet is already activated.

3. <u>Obtain</u> a certificate for your Juniper VPN and associate it with your PassKey. <u>Present</u> your PassKey to your computer before you begin.

Obtain a Certificate

Ask a system administrator how to obtain a certificate and associate it with your PassKey. The certificate serves as a credential that proves your identity when you log into your Juniper VPN.

A common way to obtain certificates is with Microsoft Active Directory Certificate Services. Click <u>here</u> to see example steps.

If your certificate is available in a file, you can <u>import</u> it to your PassKey using the WWPass Dashboard, which is installed as part of the WWPass Security Pack.

Guidelines

Whatever method you use to obtain a certificate, follow these guidelines to ensure the certificate is associated with your PassKey:

- When you obtain a certificate, select the following as the CSP: **Microsoft Base Smart Card Crypto Provider**. (CSP stands for Cryptographic Service Provider.)
- Before you obtain the certificate, present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.

^a wwpass°



Obtain a Certificate Via Active Directory Certificate Services

The steps below provide an example of how to obtain a certificate via Microsoft Active Directory Certificate Services. Steps at your company might be different.

Note: If the "root certificate" for your Juniper VPN is not trusted by your computer, Active Directory indicates this and provides a link that lets you install the root CA on your computer.

To obtain a certificate via Active Directory

- 1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port. This ensures your certificate is associated with your Passkey.
- 2. Open a web browser from your computer and go to Active Directory Certificate Services using the URL provided by a system administrator, for example: https://pki.companyname.net/certsrv
- 3. From the CA Welcome page, click **Request a certificate**.

Microsoft Active Deschry Certificate Services - VWPbase Corporation Intermediate CA	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail clent, or other program. By using a certificate, you can venify your identity to people you communicate with over the v sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.	Neb,
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.	
For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.	
Select a task: Request agentificate View the Sultus of a pending certificate request Download a CA certificate chain, or CRL	

4. From the Advanced Certificate Request page, click Create and submit a request to this CA.

Microsoft Active Directory Certificate Services - WWPass Corporation Intermediate CA

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit agrequest to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Options are displayed.

Certificate Temp	late:	
	WWPass Sma	artcard Logon 💌
Key Options:		Lis"
	Create new	key set 💿 Use existing key set
CSP	Microsoft Base	e Smart Card Crypto Provider 💌
001	@ Exchange	
Key Usage:	Exchange	
Key Usage: Key Size:	Exchange Min: Max:	2048 (common key sizes: <u>2048</u>)
Key Usage: Key Size:	Exchange Min: Max: Automatic k	2048 (common key sizes: <u>2048</u>) 2048 (common key sizes: <u>2048</u>) key container name



- 5. Select options and submit your certificate request as follows:
 - a) Select the Smartcard Logon template from the Certificate Template list.
 - b) Select **Microsoft Base Smart Card Crypto Provider** from the **CSP** list. This setting associates the certificate with your PassKey.

Key Options:		
	Create new key set	OUse existing key set
CSP:	Microsoft Base Smart C	ard Crypto Provider
		3

- c) Select **Create new key set** and clear the checkbox for **Mark keys as exportable**. Select other settings based on instructions from an administrator.
- d) Click Submit to request a certificate. After your request is "generated", enter access code for your PassKey in the prompt that appears:
 - If certificate requests are automatically approved, your certificate is associated with your PassKey right away. You can now use your PassKey to log into your Juniper VPN.
 - If certificate requests are explicitly approved, the Certificate Pending page appears with your Request ID and instructions. Go to the next step.

Microsoft Active Directory Certificate Services - WWPass Corporation Intermediate CA

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

Your Request Id is 839.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with this web browser within 10 days to retrieve your certificate

6. Return to Active Directory Certificate Services to check the status of your request. Click **View the** status of a pending certificate request.

Use this Web site to request a certificate for your Web browser, e-mail client, or othe sign and encrypt messages, and, depending upon the type of certificate you request	er program. By using a certificate, you can verify your identity to people you communicate with over the Web t, perform other security tasks.
You can also use this Web site to download a certificate authority (CA) certificate, o	ertificate chain, or certificate revocation list (CRL), or to view the status of a pending request.
For more information about Active Directory Certificate Services, see Active Directory	ory Certificate Services Documentation
Select a task: Request a certificate View the status of a pending certificate request Dowinoad a CA certificate, certificate totin or CRL	

Microsoft Active Directory Certificate Services - WWPass Corporation Intermediate CA

View the Status of a Pending Certificate Request

Select the certificate request you want to view: (Thursday October 1 2012 12:47:04 PM) 7. When "Certificate Issued" is shown as the status, click **Install this certificate**. Then enter the access code for your PassKey in the prompt that appears. Your certificate is associated with your PassKey. You can now use your PassKey to log into your Juniper VPN.

Microsoft Active Directory Certificate Services - WWPass Corporation Intermediate CA				
Certific	ate Issued			
The cert	ificate you requested was issued to you.			
E	Install this certificate			
Save	response			

Import a Certificate Using the WWPass Dashboard

If your VPN certificate is in a file, follow the steps below to import the certificate to your PassKey using the WWPass Dashboard.

To import a certificate using Dashboard

- 1. <u>Present</u> your PassKey to your computer. This ensures that the certificate is associated with your PassKey.
- 2. Open Dashboard using the Key icon Gerin the system tray.
- 3. In the Certificates tab, click the **Import a new certificate** ¹⁶ button.

WWPass Solutions Certificates	Key Status Advanced			
Available Certifica	ates		Import a new certificate والم	
Certificate Name		Issued By	Expire Date	Delete
Karen Barnes		WWPass Corporation Intermediate CA	17-May-2015	1
Warren Barmers		COMODO Client Authentication and Secure Email CA	17-May-2014	m

- 4. From the Open Certificate window, locate the certificate file. Look for an extension of .pfx or .p12. Select the file and click
- 5. If prompted for the password used to encrypt the certificate file, enter the password and click
- Enter the access code for your PassKey and click

^{_}wwpass°



CHAPTER 5 — USE YOUR PASSKEY TO LOG IN

This chapter covers using your PassKey to log into your Juniper VPN.

Topics In This Chapter

• Log Into Juniper VPN Using a PassKey



Log Into Juniper VPN Using a PassKey

Follow the steps below to use your PassKey to securely log into your Juniper VPN via a web browser.

A **Important:** After you log out, be sure to remove your PassKey from your computer and close your Web browser. If you do not close your browser, other users may be able to access certificate-protected resources.

To log into Juniper VPN using your PassKey

- 1. Present your PassKey to your computer by placing it on an NFC reader or inserting it into a USB port.
- 2. Open a Web browser from your computer and connect to your organization's Juniper VPN using the sign-in URL provided by a system administrator.
- 3. If prompted to select a certificate, click on your Juniper VPN certificate in the list that appears. Then click OK. (The name of the certificate might include "Juniper VPN" or "VPN".)
- 4. When prompted, enter the access code for your PassKey and click . The welcome page for your Juniper VPN appears.
- Under CRL Distribution Points (CDP), select Manually configured CDP. This tells the SA Series Appliance to access the CRL from the CDP (CRL distribution point) specified in the next step. A CDP is a location on an LDAP server or web server where a CA publishes CRLs.

CRL Distribu	tion Points (CDP)	
Usei	Manually configured CDP	~

- 6. Enter the URL of your primary CDP and a backup CDP (backup is optional):
 - For an LDAP server, use the syntax: ldap://Server/BaseDN?attribute?Scope?Filter
 - For a web server, enter the complete path to the CRL object. For example: http://domain.com/CertEnroll/CompanyName%20CA%20Server.crl

Primary Cl	9P	
CDP URL:	http://calias.com/office.calca.cal	

7. In the **CRL Download Frequency** field, specify how often the SA Series Appliance should download the CRL from the CDP. The interval can be from 1 hour to 9999 hours.

Options		
CRL Download Frequency:	1	hours (1-9999)

8. Click Save Changes.



Copyright © 2014 WWPass Corp.[®] All rights reserved. WWPass | 1155 Elm Street, Manchester, NH 03110 | Tel: +1.603.836.4932 or +1.888.997.2771 | <u>www.wwpass.com</u>