

iPad or iPhone with Junos Pulse and Juniper[®] SSL VPN appliance

Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information	n	
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview	
	Arlington Business Park	
	Theale	
	Reading	
	RG7 4TY	
Andy Kemshall	akemshall@securenvoy.com	



Juniper[®] SSL VPN appliance Integration Guide

This document describes how to setup an iPad or iPhone with the Junos Pulse application connecting to a Juniper® SSL VPN appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

Junos Palse and Juniper® SSL VPN appliance provides - Secure Remote Access to the internal corporate network for iPad's or iPhones.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Juniper®), without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of (your PIN and your Phone to receive the one time passcode)

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration, as does the Juniper[®] SSL VPN appliance. All notes within this integration guide refer to this type of approach.

Note that two configuration options exists, one for Pre-loaded Passcodes including Day Codes, Tmp Codes and Static Codes (Section 1.1 to 3), the other for Real Time Codes (Appendix A to C)

The equipment used for the integration process is listed below:

Juniper Juniper® SSL VPN appliance version 7.0R1

SecurEnvoy

Windows 2003 server SP1 IIS installed with SSL certificate (required for remote administration) Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.4.501

iPad with Junos Pulse



Index

1.0	Pre Reguisites	3
1.1	Configuration of Juniper® for Pre-Loaded Passcodes	4
2.0	Configuration of SecurEnvoy for Pre-Loaded Passcodes	7
3.0	Test Pre-Loaded Codes Logon	8

Appendix A	Configuration of Juniper® for Real Time Authentication	12
Appendix B	Configuration of SecurEnvoy for Real Time Passcodes	15
Appendix C	Test Real Time Codes Logon	17

1.0 Pre Requisites

It is assumed that the Juniper® SSL VPN appliance has been installed and basic configuration carried out. A user can connect by authenticating with their Microsoft AD Domain username and password. (This could be configured for any username and password authentication server)

Securenvoy Security Server has been installed with the Radius service and has a suitable account that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Juniper® SSL VPN appliance(s), additional open ports will be required.

NOTE: Add radius profiles for each Juniper® SSL VPN appliance that requires Two-Factor Authentication.



1.1 Configuration of Juniper® for Pre-Loaded Passcodes

Login to the Juniper® SSL VPN appliance with administrative permissions.

Navigate to "Authentication" "Auth. Servers" select new "Radius Server" and press "New Server" $% \mathcal{S}^{\prime\prime}$



Populate information for the new Radius server (SecurEnvoy) Enter Name, IP address, authentication port and shared secret.

SecurEnvoy recommend to set the timeout settings to at least 10 seconds or greater with a retry of 0.

If redundancy is required, enter details for a second SecurEnvoy Radius server.

Root - Go		Cent	ral Hanager Root	Help Guidance Sign Ou
System Status • Configuration • Network • Clustering •	Auth Servers > SecurEnvoy Settings Users			
IF-MAP Federation	Name:	SecurE	nvoy	Label to reference this server.
Authentication	NAS-Identifier:	192.168	.200.10	Name of the device as known to Radius server
Signing In +	Primary Server			
Endpoint Security * Auth. Servers	Radius Server:	192.168	.100.11	Name or IP address
Administrators	Authentication Port:	1812		
Admin Realms + Admin Roles +	Shared Secret:	•••••	6	
Users	Accounting Port:	1813		Port used for Radius accounting, if applicable
User Realms + User Roles +	NAS-IP-Address:			IP address
Resource Profiles + Resource Policies + Junos Pulse +	Timeout:	10	seconds	
Maintenance	Retries:	0		
System + Import/Export + Push Config +	Users authentica	te using	tokens or one-ti device will send the u	me passwords sec's suthentication method as "token" if you use



Navigate to "Users", "User Realms" and select the user realm for Microsoft AD Domain authentication.



Click the checkbox "Additional authentication server"

Populate information for "Authentication #2" select "Securenvoy" (this is the previously setup Radius authentication server)

Set "Username is" to radial button "predefined as <USER>"

Set "Password is" to radial button "specified by user on sign-in page"

Click checkbox "End session if authentication this server fails"



Navigate to "Authentication" "Signing In" "Sign-in Pages"

Select the sign in page associated with the Microsoft AD Domain authentication, in this example this is the "Default Sign-In Page"

Click the link for "Default Sign-In Page"

Root 👻 Go	Central Manager Root	Help Guidance Sign Out
- System		
Status >	Sianina In	
Configuration +	5	
Network +	Sign-in Policies Sign-in Pages Sign-	in Notifications
Clustering +	Sign in roleices Sign in rages Sign i	in Notifications
Virtual Systems >>		
IF-MAP Federation →	New Page Upload Custom Page:	s Delete
Log/Monitoring >		
- Authentication	Sign-In Page	Type
Signing In 📀 🔸		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
Endpoint Security →	Default Sign-In Page	Standard page
Auth. Servers	Meeting Sign-In Page	Standard Meeting page
272 A 1 2 2 4 1 4		

Enter details for secondary password prompt, in this example "SMS Pass Code" was used

Root - Go	Central I Ro	Manager Oot	Help Guidance Sign O	ut
System Status Configuration Network	Signing In > Default Sign-In Pa	age		
Clustering > Virtual Systems > IF-MAP Federation >	Name: Page Type:	Default Sign-In Page Users/Administrato	Label to reference the sign-in page.	
Log/Monitoring > Authentication	Custom text			
Signing In Endpoint Security Auth. Servers	Welcome message:	Welcome to the		
Administrators Admin Realms Admin Roles	Submit button:	Sign In		
User Realms > User Roles > Resource Profiles > Resource Policies >	Instructions:	Please sign in to b session. davascript is disab This text appears on the ri- can use , >, format the text.	egin your secure script>Note: bled on your ght-hand side of the sign-in page. You , <noscript>, and tags to</noscript>	
Junos Pulse Maintenance System	Username: Password:	Username Password		
Push Config > Archiving > Troubleshooting >	Realm:	Realm	This prompt appears when the sign in page supports more than one realm.	
	Secondary username: Secondary password:	Secondary username SecurEnvoy Passcode		



2.0 Configuration of SecurEnvoy for Pre-Loaded Passcodes

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the "Radius" Button

Enter IP address and Shared secret for each Juniper® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.

Config Radius SecurMail Log V	Log Out
Radius	OK License Expires 1st Jan 2014
Network Access Server ■ 127.0.0.1 ■ 192.168.135.201	NAS IP Address 192.168.135.201 Format xxx.xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Shared Secret password Format xxx.xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx Format xxx.xxx.xxx Format xxx.xxx.xxx Format xxx.xxx Format xxx.xxx Format xxx.xxx Format xxx.xxx Format xxx.xxx Format xxx.xxx Format xxx Format xxx <td< th=""></td<>
	Authenticate Passcode Only (password or pin not required)
	Default Domain dev2.com Only allow this domain
	Only allow users that are in the LDAP group Change Group
	Leave group blank to authenticate all users
	Override customer name in SMS message with Max 20 Leave blank to use default
	Pass Back Data To Radius Client in Attribute 25
	 No information is passed back Password is passed back LDAP group members are passed back (Return distinguished names) User's Distinguished Name
Delete Selected	Update

Click checkbox "Authenticate Passcode Only (password or pin not required)

Click "Update" to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.



2.0 Setup iPad with Junos Pulse

On the iPad, download Junos Pulse from the App Store



Start Junos Pulse and select "Configuration" and "Add new configuration"

Enter Name details Enter the URL to your Juniper SA Box Add Certificate details



Press "Save" Button





3.0 Test iPad Junos Pulse Pre-Loaded Codes Logon

On the iPAD, Start Junos Pulse Application

Select Connect Button

iPad ᅙ		12:25	* 100% 📟
	Juno	s Pulse	
	Configuration	Juniper SA 👂	
	Status	About	K
	XXX		
	Cor	nnect	K
			\langle
			/
	No session	VPN off) 1x

User will enter: UserID in the Username box Microsoft AD Domain password in password box SMS Passcode in the SecurEnvoy Passcode box (received via SMS upon your mobile phone)



	12:56 *	95 % 🗩
Junos Pulse	Connect	
Configuration	Juniper SA 🔸	
JUNIPER.		
Welcome Secure A	to the Access SSL VPN	
Username		
Password		
SecurEnvoy Passcode		
	(Sign In	
No session	VPN off	
m NO SESSION	VPIN OIT 🧐	1x

Once authenticated a new SMS passcode will be sent to the user's mobile phone, ready for the next authentication. The following screen should then be seen.

	13.35		4.91
J	unos Puls	e	
Configuratio	'n	Juniper SA ゝ	
			<
			<
			<
Status		About	2
	Diagonal		
	Disconneci		1
equiplab\graes	ide	VPN on 🗧	Э



Appendix A Configuration of Juniper® for Real Time Authentication

Login to the Juniper® SSL VPN appliance with administrative permissions.

Navigate to "Authentication" "Auth Servers" select new "Radius Server"



Populate information for the new Radius server (SecurEnvoy)

Enter Name, IP address, authentication port and shared secret.

SecurEnvoy recommend you set the timeout settings to at least 10 seconds or greater with a retry of 0.

If redundancy is required, enter details for a second SecurEnvoy Radius server.

Root - Go		Central	Manager	Help Guidance Sign Out
Status · · · · · · · · · · · · · · · · · · ·	Auth Bervers > SecurEnvoy Settings Users			
IF-MAP Federation +	Name:	SecurEnvo	y	Label to reference this server.
- Authentication	NAS-Identifier:	192.168.20	00.10	Name of the device as known to Radius server
Signing In +	Primary Server			
Auth. Servers	Radius Server:	192.168.10	00.11	Name or IP address
- Administrators	Authentication Port:	1812		
Admin Realms + Admin Roles +	Shared Secret:			
- Users	Accounting Port:	1813		Port used for Radius accounting, if applicable
User Realms + User Roles +	NAS-IP-Address:			IP address
Resource Profiles + Resource Policies + Junos Pulse +	Timeout:	10 s	econds	
- Maintenance	Retries:	0		
System + Import/Export + Push Config +	Users authentica	te using t	okens or one-ti	me passwords user's suthentication method as "token" if you use



Central Manager - Auth Servers Backup Server (required only if Backup server exists) Radius Server: Name or IP address Authentication Port: Shared Secret: Accounting Port: Port used for Radius accounting, if applicable Radius accounting User-Name: CUSER> (<realm>)(<role sep=")</td"> Template for reporting user identity to Radius server The template can contain textual characters as well as variables for substitution, Variables should be enclosed in angle brackets like this <variables. a="" all="" click="" here="" list="" of="" td="" to="" variables.<="" view=""> Examples: <user> <user> <user> The user's login name <realm> <realm> <user> The user's login name <realm> <user> <user> The user's login name <realm> <user> <user> The user's login name <realm> <user> <user> <user> <user> <user> <user> <</user></user></user></user></user></user></realm></user></user></realm></user></user></realm></user></realm></realm></user></user></user></variables.></role></realm>	🛠 🌈 Central	Manager - Auth Servers				D Doco -	
Backup Server (required only if Backup server exists) Radius Server: Radius Server: Radius Server: Radius Port: Radius accounting Port: Port used for Radius accounting, if applicable Radius accounting User-Name: User-Name: VUSER>(<realm>](<role <variable="" angle="" as="" be="" brackets="" can="" characters="" contain="" enclosed="" for="" identity="" in="" like="" radius="" reporting="" sep="Template" server="" should="" substitution.="" template="" textual="" the="" this="" to="" user="" variables="" well="">. Click here to view a list of all variables. Examples: USER> The user's login name <realm> The user's sign-in realm <role sep=",">Time interval to send an interim update to the accounting enver (MDLE) The first role amongst multiple roles assigned to the user <role> The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The instrume to send an interim update to the accounting server (MDLE) The first role amongst multiple roles assigned to the user (MDLE) The instrume to send an interim update to the accounting server (MDLE) The instrume to send an interim update to the accounting server (MDLE) The instrume to send an interim update to the accounting server (MDLE) The instrume to send an interim update to the accounting server (MDLE) The instrume to send an interim update to the accounting server (MDLE) The instrume to send an interim update t</role></role></realm></role></realm>		Backup Server (reg					(O) Tools
Radius Server: Name or IP address Authentication Port:			uired only if Backup server exists)				
Authentication Port: Shared Secret: Accounting Port: Port used for Radius accounting, if applicable Radius accounting User-Name: USER>(<realm>)[<role li="" login="" name<="" s="" sep=" Template for reporting user identity to Radius enclosed in angle brackets like this <variables. Click here to view a list of all variables. Examples: <USER>: <US</td><td></td><td>Radius Server:</td><td>Name</td><td>or IP address</td><td></td><td></td><td></td></tr><tr><td>Shared Secret: Accounting Port: Port used for Radius accounting, if applicable Radius accounting User-Name: CUSER>(<REALM>)[<ROLE SEP=] Template for reporting user identity to Radius server The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click here to view a list of all variables. Examples: CUSER> The user"> <role sep="">The list of ","-separated roles assigned to the user</role> ROLE SEP="">Time interval to send an interim update to the accounting server (min: 15 minutes) Custom Radius Authentication Rules If received packet Type Attributes Type Attributes Take action Type Attributes Type Take action Type Attributes Type Type Type Type <u< td=""><td></td><td>Authentication P</td><td>ort:</td><td></td><td></td><td></td><td></td></u<></role></realm>		Authentication P	ort:				
Accounting Port: Port used for Radius accounting, if applicable Radius accounting User-Name: CUSER>(<realm>)[<role sep=")</td"> Template for reporting user identity to Radius server The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click here to view a list of all variables. Examples: <user> The user's login name <role sep=",">< The user's login name</role></user></variable></role></realm>		Shared Secret:					
Radius accounting User-Name: _{USER>(<realm>)[<role <user="" login="" name="" s="" sep="]</td> Template for reporting user identity to Radius server The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click here to view a list of all variables. Examples: <USER> The user"> The user's login name <reln> The user's login name <role> The first role amongst multiple roles assigned to the user Interim Update Interval: minutes Custom Radius Authentication Rules New Radius Rule If received packet Take action If received packet Take action</role></reln></role></realm>		Accounting Port:	Port u	sed for Radius a	accounting, if applicable		
User-Name: USER>(<realm>)(<role li="" login="" name<="" s="" sep=" Template for reporting user identity to Radius server The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variables. Click here to view a list of all variables. Examples: USER> USER> USER> The user"> REALM> The user's login name REALM> The user's sign-in realm ROLE SEP=",">The list of ","-separated roles assigned to the user ROLE SEP=",">Time interval to send an interim update to the accounting server (min: 15 minutes) Custom Radius Authentication Rules If received packet Type Attributes </role></realm>		Radius accounting					
The template can contain textual characters as well as variables for substitution. Variables should be enclosed in angle brackets like this <variable>. Click here to view a list of all variables. Examples: <user> The user's login name <realm> The user's sign-in realm <role sep=",">The list of ","-separated roles assigned to the user <role sep=",">The first role amongst multiple roles assigned to the user <role> The first role amongst multiple roles assigned to the user (min: 15 minutes) Custom Radius Authentication Rules If received packet Type Attributes</role></role></role></realm></user></variable>		User-Name:	<user>(<realm>)[<role< td=""><td>E SEP='</td><td>Template for repor server</td><td>ting user identity to Rad</td><td>dius</td></role<></realm></user>	E SEP='	Template for repor server	ting user identity to Rad	dius
Examples: USER> The user's login name <realm> The user's sign-in realm <role sep=",">The list of ","-separated roles assigned to the user <role> The first role amongst multiple roles assigned to the user <role> The first role amongst multiple roles assigned to the user (min: 15 minutes) Time interval to send an interim update to the accounting server (min: 15 minutes) Custom Radius Authentication Rules New Radius Rule Delete</role></role></role></realm>			The template can contain text	tual characters a	s well as variables for su	bstitution. Variables sho	ould be
Interim Update Interval: minutes Time interval to send an interim update to the accounting server (min: 15 minutes, max: 1440 minutes) Custom Radius Authentication Rules New Radius Rule Delete			<user> The user's id <realm> The user's si <role sep=","> The list of ", <role> The first role</role></role></realm></user>	ogin name ign-in realm "-separated role amongst multij	es assigned to the user ple roles assigned to the	user	
Custom Radius Authentication Rules If received packet Take action Type Attributes		Interim Update Ir	nterval: minutes		Time interval to se accounting server (min: 15 minutes,	nd an interim update to max: 1440 minutes)	o the
New Radius Rule Delete If received packet Take action Type Attributes		Custom Radius Auth	hentication Rules				
If received packet Take action Image: Type Attributes					New Radius Rule	Delete 1	F
Type Attributes		If received	packet	Take ad	ction		
		🖾 Туре	Attributes				

Scroll to bottom and select "New Radius Rule" button as shown below.

Select Radius Attribute "Reply-Message(18)" Select Operand "matches the expression" Set Value to "Enter Your 6 Digit Passcode"

Note this value MUST match the setting in the SecurEnvoy GUI Config setting "SMS Delivery Mode" Prompt:

Config Radius SecurMail Log V	iewer Users Reporting Help Log Out
Config	License Expires 1st Jan 2014
Licence Upgrade	SMS Delivery Mode
Pin Management	
Day Code	Z Enable Real Time Prorton Enter Your 6 Digit Passcode
SMS Delivery	
Mobile Number	Default (new users have real time set by default)
Direct Password Control	
Tmp Static Code	
Account Lockout	
Passcodes in SMS	
Email Settings	Update
GUI Settings	



Press the "ADD" b	outton to	add	this	rule
-------------------	-----------	-----	------	------

Select Show GENERIC LOGIC Page

Press "Save Changes"

Press "Close"

Root 👻 Go	Centr	al Manage r Root	Help Guidance Sign Out
– System			
Status >	Auth Servers > SecurEnvoy >		
Configuration +	Add Custom Radius Rule	e	
Network +			
Clustering +			
Virtual Systems >>	SecurEnvoy Deal Time		
IF-MAP Federation →	Name: SecurEnvoy Real Time		
Log/Monitoring >			
 Authentication 	If received Radius Response Packet		
Signing In 🔶			
Endpoint Security >	Deserves Desket Tursey Access Ch	allenge =	
Auth. Servers	Response Packet Type: Access of	lallelige +	
- Administrators			
Admin Realms 🔹 🕨	Attribute criteria:		
Admin Roles >>	Radius Attribute	Operand	Value
- Users			
User Realms →	Reply-Message (18)	matches the expression -	Enter Your 6 Digit Passco Add
User Roles >>			
Resource Profiles >	These Aslas asking		
Resource Policies >	Then take action		
Junos Pulse >>			
- Maintenance	show New Pin page		
System +			
Import/Export >			
Push Config >	Show Next Token page		
Archiving >			
Troubleshooting >			
	Show Generic Login page		

Click "Save changes" to submit all configuration parameters

Navigate to "Users", "User Realms" and select the realm configured for SecurEnvoy Populate information for "Servers" (this is the previously setup Radius authentication server)

Additional authentication server is not required.



🜈 Central Manager - l	User Realms - Windows Internet Explorer	×			
🕒 🗸 🖉 🕞 https	s://192.168.135.201/dana-admin/realm/policyrealm.cgi?selectRealm=1&rez 🔽 😵 Certificate Error 🛛 🚱 🗙 Google 🔎				
<u>File E</u> dit <u>V</u> iew F <u>a</u> v	vorites <u>T</u> ools <u>H</u> elp				
Google 8 -	🔄 Search 🖗 🖉 🐔 🧭 🥙 🌮 🔤 🛪 🗔 🛠 Bookmarks 🔹 💁 Find 🔹 🏰 Check 🔹 🔌 🔩 🐇 Gign In	•			
😪 🎄 🏾 🄏 Central M	Manager - User Realms 🍈 🔹 🗟 👻 📴 Page 👻 🎯 Tools 👻	»			
Configuration >	Securenvoy				
Network >					
Clustering +	General Authentication Policy Role Mapping				
Virtual Systems >					
- Authentication	Name: Securenvoy Label to reference this realm				
Endpoint Security >	Description.				
Auth. Servers	*				
- Administrators					
Admin Realms →					
Admin Roles →	When editing, start on the Kole Mapping page				
- Users					
User Realms →	Servers				
User Roles Resource Profiles					
Resource Policies >	Specify the servers to use for authentication and authonization. To create or manage servers, see the <u>servers</u> page.				
- Maintenance	Authentication: Securenvoy Specify the server to use for authenticating users.				
System >	Directory/Attribute: Same as above Specify the server to use for authorization.				
Push Config >					
Archiving >	Accounting: None Specify the server to use for Radius accounting.				
Troubleshooting >					
	Additional authentication server				
	Dynamic policy evaluation				
	Other Settings				
	Authentication Policy: Password restrictions				
	Kole Mapping: 1 Rule				
	Save changes?	-			
,		-			

Save Changes

Appendix B Configuration of SecurEnvoy for Real Time Passcodes

To help facilitate an easy to use environment, SecurEnvoy can be set up to use the existing Windows password as the PIN component. SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

Click the **"Radius"** Button

Enter IP address and Shared secret for each Juniper® SSL VPN appliance that wishes to use **SecurEnvoy** Two-Factor authentication.



Config Radius SecurMail Log V	ewer Users Reporting Help Log Out
Radius	OK License Expires 1st Jan 2014
Network Access Server ■ <u>127.0.0.1</u> ■ <u>192.168.135.201</u>	NAS IP Address 192.168.135.201 Format xxx.xxx.xxx.xxx or default for undefined IP's Shared Secret password Format xxx.xxx.xxx.xxx Format xxx.xxx.xxx Format xxx.xxx <
	Authenticate Passcode Only (password or pin not required)
	Default Domain dev2.com - Only allow this domain
	Only allow users that are in the LDAP group Change Group
	Leave group blank to authenticate all users
	Override customer name in SMS message with Max 20
	Leave blank to use default
	Pass Back Data To Radius Client in Attribute 25
	 No information is passed back Password is passed back
	 LDAP group members are passed back (Return distinguished names) User's Distinguished Name
Delete Selected	Update

Do ${\bf NOT}$ click the checkbox "Authenticate Passcode Only"

Click **"Update"** to confirm settings.

Click **"Logout"** when finished. This will log out of the Administrative session.



Appendix C Test iPad Junos Pulse Real Time Codes Logon

On the iPAD, Start Junos Pulse Application

Sciece connect Dutton

Junos Pulse				
Configuration	Juniper SA 👂			
Status	About			
XXX	XXX			
Connect				
No session	VPN off 🕣			

User will enter: UserID in the Username box Microsoft AD Domain password in password box

(•		14:22		* 859
J	unos Pulse	Connec	i	
C	Configuratio	n	Juniper SA	>
JL				
	Welcome Secure	e to the Access	SSL VPN	
	Username Password	Sign In		Pli sig to be yo se se
*	No session		VPN of	f -Э



You will be sent a real time passcode to your phone, enter this 6 digit code at the Response: prompt.

Note: the Juniper Generic Login page can be customised to change this pages text and prompt, see Juniper's guide on customising web templates.

19.22	, co -,, e ,
Junos Pulse Connect	
Configuration Juniper SA >	
JUNIPEC.	
Welcome to the	
Secure Access SSL VPN	
Challenge / Response	
Challenge: Enter Your 6 Digit Passcode	
Enter the challenge string above into your token, and then enter the one-time response in the field below.	
Response:	
Sign In Cancel	
No session VPN off -	1x

After authentication you should see the following

	13:35	5	* 9
	Junos	Pulse	
Config	guration	Juniper SA	>
			X
(×
	Intranet		
	Status	About	
	Discor	nnect	
\times	XX	XX	X
矌 equip	lab\graeside	VPN on	-9