

VPN Tracker for Mac OS X



How-to:

Interoperability with

NetScreen

Internet Security Appliances

Rev. 4.0

Copyright © 2003-2004 equinux USA Inc. All rights reserved.

1. Introduction

This document describes how VPN Tracker can be used to establish a connection between a Macintosh running Mac OS X and a NetScreen Internet Security Appliance.

The NetScreen is configured as a router connecting a company LAN to the Internet.

This paper is only a supplement to, not a replacement for, the instructions that have been included with your NetScreen. Please be sure to read those instructions and understand them before starting.

All trademarks, product names, company names, logos, screenshots displayed, cited or otherwise indicated on the How-to are the property of their respective owners.

EQUINUX SHALL HAVE ABSOLUTELY NO LIABILITY FOR ANY DIRECT OR INDIRECT, SPECIAL OR OTHER CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE USE OF THE HOW-TO OR ANY CHANGE TO THE ROUTER GENERALLY, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS, OR DATA, EVEN IF EQUINUX HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2. Prerequisites

First you have to make sure that your NetScreen has VPN support built in. Please refer to your NetScreen manual for details.

Furthermore you should use a recent NetScreen fimware version. The latest firmware release for your NetScreen appliance can be obtained from

http://www.NetScreen.com/

For this document, ScreenOS 4.01 and 5.0.0r3.0 has been used.

When using Pre-shared key authentication you need one VPN Tracker Personal Edition license for each Mac connecting to the NetScreen.

VPN Tracker is compatible with Mac OS X 10.2.5+ / 10.3.

3. Connecting to a NetScreen VPN Appliance (single user)

In this example the Mac running VPN Tracker is directly connected to the Internet via a dialup or PPP connection.¹

The NetScreen is configured in NAT mode and has the static WAN IP address 169.1.2.3 and the private LAN IP address 192.168.1.1. The Stations in the LAN behind the NetScreen use 192.168.1.1 as their default gateway and should have a working Internet connection.



Figure 1: VPN Tracker – NetScreen connection diagram

¹ Please note that the connection via a router, which uses Network Address Translation (NAT), only works if the NAT router supports "IPSEC passthrough". Please contact your router's manufacturer for details.

3.1 <u>NetScreen Configuration</u>

The pre-defined VPN Tracker connection type has been created using the default settings for your NetScreen appliance. If you change any of the settings on the NetScreen, you will eventually have to adjust the connection type in VPN Tracker.

Step 1 Create a new User Group:

Go to [Objects -> Users -> Local Groups]. Click "New" to add a goup. Type in an arbritary group name eg. vpntracker-dialup.

000	NetScreen Administration Tools (ns5xt)		0
	Objects > User Groups > Local > Edit	ns5xt	?
NETSOREEN Science Security Sciences NS5XT Home Configuration NS5XT Home Configuration NS5XT Home Configuration NS5XT NS5	Objects > User Groups > Local > Edit Group Name vpstracker-dialap < Croup Members>	ns5xt	
+ Wizards + Help Logout			
Document: Done			0 //.

Figure 2: NetScreen – Create User Group

Step 2 Create a new user:

Go to [Objects -> Users -> Local]. Then add a user (eg. vpntracker@example.net) to the previously created group. Select "IKE User" and "Simple Identity" and type in an IKE Identity eg. your email adress.

000	NetScreen Administrat	ion Tools (ns5xt)	
	Objects > Users > Local > Edit	ns5xi	: ?
O O	NetScreen Administrat Objects > Users > Local > Edit User Name vpstracker@example.ne Status Status IKE User Simple Identity IKE ID Type Use Distinguished Name For ID CN OU Organization Location State Country E-mail Container Authentication User XAuth User IXEN	Auth/IKE/L2TP/XAuth User Auth/IKE/L2TP/XAuth User Disable Number of Multiple Logins with Same ID 1 IKE Identity User Password User Password	
+ Help	L2TP User		
- Logout	L2TP/XAuth Remote Settings IP Pool Primary DNS IP Secondary DNS IP 0.0.0	(Remote IP: 0.0.0.0) Static IP 0.0.0.0 Primary WINS IP 0.0.0.0 Secondary WINS IP 0.0.0.0 OK Cancel	
Document: Done			9 //

Figure 3: NetScreen – Create User

Step 3 Add user to your vpnuser group:

Go to [Objects -> Users -> Local Groups]. Then click on "Edit". Select the user from the list and click on "«".

000	NetScreen Administration Tools (ns5xt)		0
	Objects > User Groups > Local > Edit	ns5xt	?
NETSCREEN Scalable Security Solutions			
NSDCT Home Configuration Network Screening Policies VPNs Objects Services Users Local Local Groups External Groups Freedules Group Expressions Certificates Attacks Reports Wizards Help Logout	Group Name vptracker-dialup Group Members> Image: Comparison of the second s		
Document: Done			0 //

Figure 4: NetScreen - User Group settings

Step 4 Create a new Gateway:

- Gateway Name: arbritary Name (e.g. mac-vpntracker)
- Security Level: Compatible
- Remote Gateway Type: **Dialup User**: the previously created User Group
- Preshared Key: your Pre-shared key

Please Note: Every user in the Dialup User Group "vpntracker-dialup" uses the same Pre-shared key. If you don't want to allow this, you must create a separate gateway for every user.

VTNs > Autokey Advanced > Gateway > Edit ns5xt	?
- EN	
Netros Netros Netros Netros Netros Screening Policies Policies VPNs AutoKey KKE AutoKey KKB Screening Policies Dialup User VPNs Vent Status Monitor Status Dialup User Group VPN Groups Monitor Status Objects Reports Wizards Help Logout Logout	_
Document: Done	0

Figure 5: NetScreen – Gateway Settings

Click on the "Advanced" Button and enable "Aggressive Mode". You can leave the other settings at their default value (i.e. NAT-Traversal and all other options should be unchecked).

000	NetScreen Administration Tools (ns5xt)	0
	VPNs > AutoKey Advanced > Gateway > Edit ns5;	xt ?
NETSCREEN NETSCREEN Statistic Statistics NS5XT Home Configuration Network Screening Policies VPNs AutoKey IKE AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal P2 Proposal XAuth Settings VPN Groups Manual Key + L2TP Monitor Status	NetScreen Administration Tools (ns5xt) VPNs > AutoKey Advanced > Gateway > Edit Security Level Predefined Standard O Compatible Basic User Defined Coutom Phase 1 Proposal pre-g2-3des-sha ÷ pre-g2-3des-md5 ÷ Mode (Initiator) O Main (ID Protection) Aggressive Enable NAT-Traversal UDP Checksum Keepalive Frequency O Seconds (0~300 Sec) Heartbeat Hello O Seconds (0~3600 Sec) Reconnect O Seconds (60~9999 Sec) Threshold 3	xt ?
Objects Reports Wizards Help Logout	Local Authentication ● Allow Any User None User Group Allowed Authentication Type CHAP Only External Authentication None Allow Any Ouser Group Allow Any Ouser Group Name User Group Name Allowed Authentication Type CHAP Only Bypass Authentication Vser Name Password Allowed Authentication Type CHAP Only	

Figure 6: NetScreen – Advanced Gateway settings

Step 5 Create a new AutoKey IKE

Go to [VPNs -> Autokey IKE] and click "New". Enter a name and select "Compatible" as Security Level. Choose as "Remote Gateway" the predefined gateway from step 4 (e.g. "mac-vpntracker").

000	NetScreen Administration Tools (ns5xt)		0
	VPNs > AutoKey IKE > Edit	ns5xt	?
 NETSCREEN' Sclable Security Solutions NETSCREEN' Sclable Security Solutions NESSAT Home Configuration Network Screening Policies VPNs AutoKey IKE AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal XAuth Settings VPN Groups Manual Key L2TP Monitor Status Objects Reports Wizards Help Logout 	VPN Name Security Level Standard Compatible Basic Custom Remote Gateway Predefined mac-vpntracker : Create a Simple Gateway Gateway Name Type Static IP Address/Hostname Dialup User User None Dialup User User None Dialup Group Group None Local ID (optional) Preshared Key Use As Seed Basic Outgoing Interface untrust : OK Cacel Advanced	ns5xt	
Document: Done			0 /
bootament. Done			- 11.

Figure 7: NetScreen - AutoKey IKE settings

Click on "Advanced" to check the default settings. Normally it isn't necessary to change anything here.

000	NetScreen Administration Tools (ns5xt)		0
	VPNs > AutoKey IKE > Edit	ns5xt	?
NETSCREEN Statistic Strenthy Statistics NS5XT Home Configuration Network Screening Policies VPNs AutoKey IKE AutoKey Advanced Gateway PI Proposal	NetScreen Administration Tools (ns5xt) VPNs > AutoKey IKE > Edit Security Level Predefined Standard Output Custom Phase 2 Proposal nopfs-esp-3des-sha nopfs-esp-3des-md5 Replay Protection Transport Mode (For L2TP-over-IPSec only) Bind to Tunnel Interface none Tunnel Zone Untrust-Tun	ns5xt	
PI Proposal P2 Proposal VPN Groups VPN Groups L2TP Monitor Status Objects Reports Wizards Help Logout	Proxy-ID - Local IP / Netmask 0.0.0.0 / / Remote IP / Netmask 0.0.0.0 / / Service ANY VPN Group None : Weight 0 VPN Monitor - Source Interface default : Destination IP 0.0.0 Optimized - Rekey Return Cance		
Document: Done			0 //

Figure 8: NetScreen - Advanced AutoKey IKE settings

000	NetScre	en Administration Tools	s (ns5xt)			\bigcirc
	VPNs > AutoKey IKE				ns5xt	?
- AV	List 20 ‡ per page					New
NETSCREEN [*] Scalable Security Solutions		6 -1	5		C	
NS5XT	Name	Gateway	Compatible	Monitor	Configure	
 Home Configuration Network Screening Policies VPNs AutoKey IKE AutoKey Advanced Gateway P1 Proposal P2 Proposal XAuth Settings VPN Groups Manual Key L2TP Monitor Status Objects Wizards Help Logout 	mac-vpntracker	mac-vpntracker	Compatible	Off	Edit Remo	ve
Document: Done						6

After steps 1-5 the IPSec Configuration should look like this:

Figure 9: NetScreen - Auto IKE Summary

Step 6 Create a new Policy

You must now edit the Firewall policies to allow the VPN Tracker Mac to access the local network on the NetScreen side.

To create a new policy, choose "From: Untrust" -> "To: Trust" and press the "New" button:

- Source Address: Address Book -> Dial-Up VPN
- Destination Address: the network behind your Netscreen appliance (e.g. 192.168.1.0/24)
- Action: Tunnel
- Tunnel: the previously created VPN (e.g. mac-vpntracker)
- Position at Top: checked

000	Net	Screen Administration Tools (ns5xt)		0
	Policies (From Untrust To	Trust)	ns5xt	?
- EN				
NETSCREEN Scalable Secarity Solations NS5XT	Name (optional) Source Address	New Address		
+ Configuration + Network + Screening	Destination Address	Address Book Entry Dial-Up VPN Multiple New Address 192.168.0.1 Address Book Entry Any Multiple		
Policies + VPNs + Objects + Reports	Service Application	ANY : Multiple		
Help Logout	Action	Tunnel : Deep Inspection VPN mac-vpntracker :		
		Modify matching bidirectional VPN policy L2TP None		
	Logging Position at Top	 ☑ 		_
		OK Cancel Advanced		
Document: Done				S //.

Figure 10: NetScreen - Policies

3. Connecting to a NetScreen VPN Appliance (single user)

3.2 VPN Tracker configuration

Step 1 Add a new connection with the following options:

- Vendor: "NetScreen"
- Model: your VPN device

e O Connection: New York	
Connection: New York	
Connection Network Authentication Identifiers DNS	
Vendor: Juniper Networks	
Model: Juniper Networks NetScreen-500 Juniper Networks NetScreen-500 Juniper Networks NetScreen-SCT Juniper Networks NetScreen-SXP Image: State of the state of t	
Click the lock to prevent further changes.	
Cancel OK	

Figure 11: VPN Tracker - Connection settings

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. 169.1.2.3)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.255.0).

00	Connection: New York
	Connection: New York
Connec	tion Network Authentication Identifiers DNS
	Topology: Host to Network
	Network Port: Automatic
VPN Gate	eway Address: 169.1.2.3
1	Local Address: optional
Remote N	letwork/Mask: 192.168.1.0 / 255.255.255.0 +
Click the I	lock to prevent further changes.

Figure 12: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.²

² For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the NetScreen configuration.
- Enable XAUTH if the corresponding option is enabled on the NetScreen.

00	Connection: New York
	Pre-shared key: presharedkey
Co	C Enter key when establishing connection DNS The key will not be saved on disk.
í í	Cancel OK
	Enable Extended Authentication (XAUTH)
Click	the lock to prevent further changes.
	Revert Save

Figure 13: VPN Tracker - Authentication settings

Step 4 Identifier Settings:

- Local Identifier: your identity you've supplied in figure 2 in section 3.1 (e.g. vpntracker@equinux.com)
- Remote Identifier: Remote endpoint IP address.

⊜ ⊖ ⊖ C	onnection: New York		
Connection:	New York		
Connection Networ	k Authentication	Identifiers	DNS
Local Identifier: Remote Identifier:	 Local endpoint IP Own certificate vpntracker@equi Remote endpoint Remote certificate Verify remote ide 	address nux.cc Email IP address e ntifier	
Click the lock to prevent	urther changes.	Revert	Save

Figure 14: VPN Tracker - Identifier settings

Step 5 Save the connection and Click "Start IPsec" in the VPN Tracker main window.

You're done. After 10-20 seconds the red status indicator for the connection should change to green, which means you're securely connected to the NetScreen. After IPsec has been started, you may quit VPN Tracker. The IPsec service will keep running.

Now to test your connection simply ping a host in the NetScreen network from the dialed-in Mac in the "Terminal" utility:

ping 192.168.1.10

4. Connecting to a NetScreen VPN Appliance (multiple users)

In order to authenticate multiple clients with different credentials, we recommend using XAuth for user authentication. To assign virtual IP addresses by the NetScreen appliance, Mode-Config will be used.

Step 1 Please refer to step 1 in section 3.2.

Step 2 Create new users:

Go to [Objects -> Users -> Local]. Then add a user (eg. vpntracker@example.net) to the previously created group. Select **"IKE User"** and **"Simple Identity"** and type in an IKE Identity eg. your email adress. Additionally, check the **"XAuth User"** box and enter a password for the user. Repeat this step for all your users.

00	NetScreen Adm	inistration Tools (ns5xt)		0
Ођ	ects > Users > Local > Edit		ns5xt	?
NETSCREEN* Scalable Security Solutions		uth/IKE/J2TP/XAuth liser		
- <u>Home</u>	User Name vpntracker	Groups: vpntracker-dialup		
+ <u>Configuration</u>	Status 💿 Enable	O Disable		
+ Screening	V IKE User	Number of Multiple Logins with Same ID		
- Policies	Simple Identity			
- <u>VPNs</u>	IKE ID Type AUTO	IKE Identity vpntracker@equinux.com		
- AutoKey Advanced	O Use Distinguished Name For ID			
- Gateway	CN			
P1 Proposal	ou			
- XAuth Settings	Organization			
VPN Groups	Location			
<u>Manual Key</u>	State			
- Monitor Status	Country			
= <u>Objects</u>	E-mail			
+ Addresses	Container			
- Users		liter Decimord ******		
<u> Local</u>	Authentication User	Confirm Password ******		
- Local Groups	VAUTO USer	Commit Password		
– IP Pools				
Schedules	L2TP/XAuth Remote Settings	(Remote IP: 0.0.0.0)		
<u>Group Expressions</u>	IP Pool None 🔻	Static IP 0.0.0.0	_	
+ Attacks	Primary DNS IP 0.0.0	Primary WINS IP 0.0.0.0	_	
+ Reports	Secondary DNS IP 0.0.00	Secondary WINS IP 0.0.0.0		
+ <u>Wizards</u>				-
Logout		OK		

Figure 15: NetScreen - XAuth User settings

Step 3 Add users to your vpnuser group:

Go to [Objects -> Users -> Local Groups]. Then click on "Edit". Select the users from the list and click on "«", in order to add them to your group.

000	http://192.168.13.101 - NetScreen Administration Tools (ns5xt)		0
- EN	Objects > User Groups > Local > Edit	ns5xt	?
NETSCREEN Salak Strain Statist NSSOT Home Configuration NSSOT Screening Policies NYPS AutoKey IKE AutoKey IKE Auto	Group Name vptracker-dialup vptracker vptracker2 vptracker3 vptracker3 vet vet M Cancel		
– <u>Logovi</u>			//

Figure 16: NetScreen - User Group settings

Step 4 Create a new Gateway:

- Gateway Name: arbritary Name (e.g. mac-vpntracker)
- Security Level: Compatible
- Remote Gateway Type: **Dialup User**: the previously created User Group
- Preshared Key: your Pre-shared key

000	NetScreen Administration Tools (ns5xt)		\odot
	VPNs > AutoKey Advanced > Gateway > Edit	ns5xt	?
Scaleble Security Solutions NS5XT	Gateway Name mac-vpntnacker Security Level O Standard O Compatible O Basic O Custom		
Configuration Configuration Network Screening Policies VPNs AutoKey IKE AutoKey Advanced	Remote Gateway Type IP Address IP Address/Hostname Dynamic IP Address Peer ID Dialup User User Image: None Dialup User Group Group Vpntracker-dialup		
Gateway P1 Proposal P2 Proposal XAuth Settings VPN Groups	Preshared Key ••••••• Use As Seed Local ID (optional) Outgoing Interface untrust :		
Manual Rey L2TP Monitor Status Objects Reports Wizards	OK Cancel Advanced		
▪ Help - Logout			
Document: Done			0 //

Figure 17: NetScreen – Gateway Settings

Advanced Gateway Settings:

- Security Level (Predefined): Compatible
- Mode (Initiator): Aggressive
- NAT-Traversal: Enabled
- XAuth Server: Enabled
 - Local Authentication: User Group (select your VPN user group here)

00	http://192.168.13.101 - NetScreen Administration Tools (ns5xt)	0
	VPNS > Autokey Auvanceo > Gateway > Edit nS5xt	?
NET S CREEN Sidely Story NSSXT Home Configuration Network Screening Polities VPNs AutoKey Atke AutoKey Advanced Gateway P. Proposal VPNs AutoKey Advanced Gateway P. Proposal XAuth Settings VPN Groups Manual Key Monitor Status Objects Reports	Security Level Predefined Standard Compatible Basic User Defined Custom Phase 1 Proposal pre-g2-3des-sha pre-g2-3des-md5 pre-g2-des-sha pre-g2-des-md5 pre-g2-des-sha pre-g2-des-md5 pre-g2-des-gameted gameted g	
+ <u>Wizards</u> + <u>Help</u>	Allow Any	
Logout_	© User Group Vpntracker-dialup ▼	
	Allowed Authentication Type CHAP Only External Authentication CHAP Only CHAP Only CHAP Only Query Remote Setting Query Remote Seting Query Remote Setting Query Remote S	
	O Bypass Authentication	
	User Name Password	
	Allowed Authentication Type CHAP Only	
	Preferred Certificate(optional)	
	Peer CA All	
	Peer Type X509-SIG V	_
	Use Distinguished Name for Peer ID CN	U
	OU Organization	
	Location	Ļ
	State	1

Figure 18: NetScreen - Advanced Gateway settings

Step 5 IP Pool settings:

Please create an IP pool with IP addresses that should get assigned to the VPN clients. This could be addresses from the local network or any other (private) network.

000	http://192.168.13.101 - NetScree	n Administration Tools (ns5xt)		0
-X-N	Objects > 1P Pools > Edit		ns5xt <mark>?</mark>	
NETSCREEN* Scalable Security Solutions				
NS5XT	IP Pool Name	vpnpool		
+ <u>Configuration</u> + <u>Network</u>	Start IP End IP	10.0.1.10		
+ <u>Screening</u> - <u>Policies</u> - <u>VPNs</u>		OK Cancel		
 <u>AutoKey IKE</u> <u>AutoKey Advanced</u> Gateway 				
<u>P1 Proposal</u> <u>P2 Proposal</u>				
<u>VPN Groups</u> <u>Manual Key</u>				
<u>L2TP</u> <u>Monitor Status</u> Objects				
Addresses Services				
<u>- IP Pools</u> <u>Schedules</u>				
<u>Group Expressions</u> <u>Certificates</u>				
+ <u>Reports</u> + <u>Wizards</u>				
+ <u>Help</u> _ <u>Logout</u>				

Figure 19: NetScreen - IP Pool settings

Step 6 XAuth Settings:

- IP Pool Name: a previously defined IP Pool (e.g. **vpnpool**)
- DNS Primary Server IP: your local primary DNS Server (e.g **192.168.1.1**)
- DNS Secondary Server IP: optional

	NetScreen Administration Tools (n	ns5xt)
	VPNs > AutoKey Advanced > XAuth Settings	ns5xt ?
NETSCREEN [®] Scoloble Security Solutions NS5XT	Reserve Private IP for XAuth User	480 Minutes
- <u>Home</u> + Configuration	Default Authentication Server	Local
+ Network	Query Client Settings on Default Server	
+ <u>Screening</u> <u>Policies</u> VPN-	СНАР	<u> </u>
AutoKey IKE AutoKey Advanced	IP Pool Name	vpnpool 🔻
- <u>Gateway</u> Pl Proposal	DNS Primary Server IP	192.168.1.1
<u>P2 Proposal</u>	DNS Secondary Server IP	192.168.1.2
<u>VPN Groups</u>	WINS Primary Server IP	0.0.0.0
- <u>Manual Key</u>	WINS Secondary Server IP	0.0.0.0
Monitor Status		
 Objects Addresses 		Apply Cancel
+ <u>Services</u>		
<u>Users</u> IP Pools		
- <u>Schedules</u>		
- <u>Certificates</u>		
<u>Attacks</u>		
+ <u>Wizards</u>		
• <u>Help</u>		
Logout		

Figure 20: NetScreen - Advanced Gateway settings

Step 7-8 Please refer to steps 5-6 in chapter 3.2.

4.1 VPN Tracker Configuration

Step 1 Add a new connection with the following options:

- Vendor: "NetScreen"
- Model: your VPN device
- Client Provisioning (Mode Config): Enabled

0 0	Connection: New York
	Connection: New York
Conne	ection Network Authentication Identifiers DNS
	Vendor: Juniper Networks
Con	Model: Juniper Networks NetScreen-50 Juniper Networks NetScreen-500 Juniper Networks NetScreen-5CT Juniper Networks NetScreen-5XP Image: State of the state of t
Click th	e lock to prevent further changes.
Ŭ	Cancel OK

Figure 21: VPN Tracker - Connection setting

Step 2 Change your Network Settings:

- VPN Server Address: public IP address of your VPN Gateway (e.g. 169.1.2.3)
- Remote Network/Mask: network address and netmask of the remote network (eg. 192.168.1.0/255.255.25.0).

00	Con	nection: New Yorl	<
Co	nnection: N	lew York	
Connection	Network	Authentication	Identifiers DNS
т	opology:	Host to Network	•
Netw	ork Port:	Automatic	•
VPN Gateway	Address: 1	69.1.2.3	
Local	Address:		optional
Remote Netwo	rk/Mask: 1	92.168.1.0	/ 255.255.255.0 +
Click the lock to	prevent furt	ther changes.	
0		(Revert Save

Figure 22: VPN Tracker – Network settings

Please note: In order to access multiple remote networks simultaneously, just add them by pressing the Plus-button.³

³ For this step VPN Tracker Professional Edition is needed.

Step 3 Change your Authentication Settings:

- Pre-shared key: the same Pre-shared key as in the NetScreen configuration.
- Enable Extendended Authentication (XAUTH): Enabled

000	Connection: New York
Co	 Pre-shared key: secretkey Hide typing Enter key when establishing connection The key will not be saved on disk. Cancel OK MS <l< th=""></l<>
Click t	he lock to prevent further changes.

Figure 23: VPN Tracker - Authentication settings

Step 4–5 Please refer to steps 4-5 in chapter 3.2.