
CRYPTOCARD Authentication
for Check Point Firewall-1 and VPN-1 NG FP3
Quick Start Guide

Table of Contents

CHANGE HISTORY	II
1. OVERVIEW	1
2. PREREQUISITES	2
3. CONFIGURE CHECK POINT FW-1 AND VPN-1	3
3.1 Configuring a RADIUS port in Check Point™ FireWall-1® / VPN-1®	3
3.2 Defining the RADIUS Workstation in Check Point™ FireWall-1® / VPN-1®	4
3.2.1 Defining the RADIUS Server in FireWall-1/VPN-1â	5
3.2.2 Enabling RADIUS Authentication on FireWall-1â / VPN-1â	6
3.2.3 Configuring the VPN-1â settings & IKE Encryption	7
3.2.4 Creating an Authentication Group (VPN-1â)	8
3.2.5 Adding CRYPTOCARD Users in FireWall-1â / VPN-1â	8
3.2.6 Configuring a Generic User Entry	10
3.2.7 Creating a FireWall-1â / VPN-1â Rule Set	11
4. CONNECT USING SECUREMOTÉ	12
5. CRYPTOCARD AUTHENTICATION PLUG-IN FOR CHECK POINT SECUREMOTÉ CLIENT	13
5.1 Installing CRYPTOCARD EUS	13
5.1.1 Run the EUS installer	13
5.1.2 Select Installation Type	13
5.2 Applying ST-1 or SC-1 token to EUS	13
5.3 SecuRemote™ VPN Plug-in	15
5.4 Installation	15
5.5 SecuRemote™ Authentication	15
6. LOGGING ON TO A WINDOWS DOMAIN WITH CRYPTOLOGON	17
7. TROUBLESHOOTING TIPS	18
7.1 Known Issues	18
7.2 Troubleshooting	18

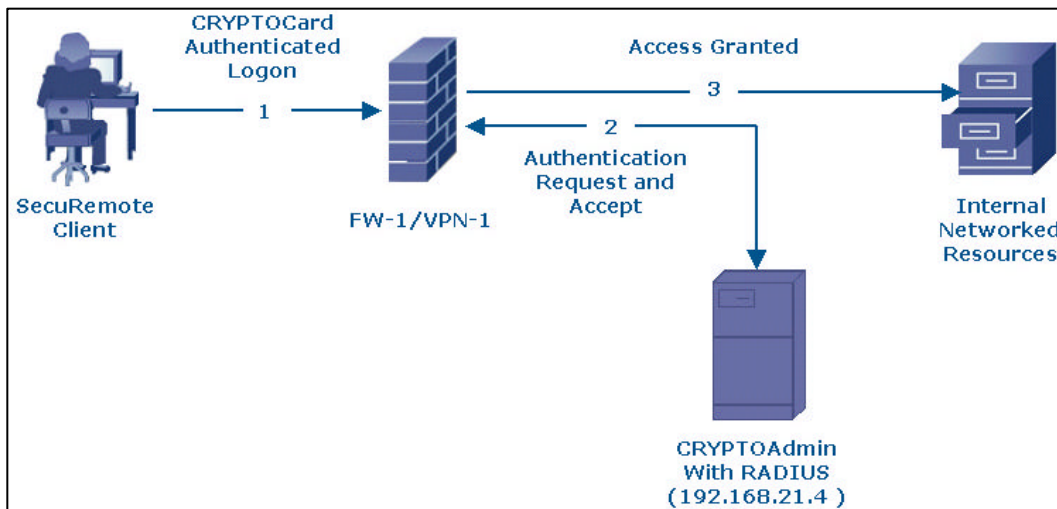
Change History

Issue Date	Changes
2003.02.23	Initial document release for Check Point Firewall-1 / VPN-1 using FP1 or FP2
2001-04-23	Documentation update to reflect configuration changes introduced by Check Point with FP3 Obsoletes Quickstart Guide for FP-1, FP-2. Contact CRYPTOCARD support to obtain a copy if required. Update troubleshooting section for known issues with SAA.

1. Overview

Check Point™ FireWall-1® / VPN-1® with SecuRemote™ can be used to prevent unauthorized access to a network. CRYPTOCARD authentication replaces username and static password with strong two-factor authentication to prevent the use of lost, stolen, shared or easily guessed password to traverse a firewall or establish a tunnel and gain access to protected resources.

The following diagram illustrates the components involved in CRYPTOCARD authentication.



1. End-User responds to the Firewall / VPN logon prompt by entering their logon name and CRYPTOCARD generated One-time Password (OTP). Note that is process can be automated using the SecuRemote Plug-in for CRYPTOCARD ST-1/EUS and SC-1/EUS tokens.
2. The Check Point™ FireWall-1®/ VPN-1® passes the authentication request via RADIUS to the CRYPTOAdmin server. (CRYPTOAdmin can be configured to use easyRADIUS, included with the CRYPTOAdmin distribution, Funk Steel Belted RADIUS, Cisco Secure ACS or Microsoft IAS.). CRYPTOAdmin authenticates the End-user and passes a RADIUS “accept” message back to the Firewall/VPN.
3. Firewall-1/VPN-1 allows the connection to internal resources on receipt of the RADIUS accept message.

The intent of this document is to present the necessary steps to configure Check Point™ FireWall-1® / VPN-1® NG FP3 and SecuRemote™ for use with CRYPTOCARD tokens.

2. Prerequisites

In order to successfully authenticate remote users using CRYPTOCARD tokens, the following items must be properly installed and configured:

- Windows NT Server 4.0 SP6a, Windows 2000 Server, Solaris 2.7, 2.8 or RedHat 7.1 – 8.0 running CRYPTOAdmin Server v.5.32
- Windows NT Server 4.0 SP6a, Windows 2000 Server, Solaris 2.7, 2.8, 2.9 or RedHat 7.2 – 7.3 running Check Point™ FireWall-1® / VPN-1® Version NG FP3 installed and configured.
- A RADIUS Server: easyRADIUS, Funk Steel-Belted Radius 2.27+ or Cisco Secure ACS 3.0+, configured to work with CRYPTOAdmin Server. EasyRADIUS Server, included with the CRYPTOAdmin Server distribution must be installed when using Cisco Secure ACS 3.0+ or if no other RADIUS Server is present.
- Check Point SecuRemote™ NG Client installed and configured.
- An initialized CRYPTOCARD token. An ST-1/EUS software or SC-1/EUS smart card token should be installed if the CRYPTOCARD Authentication Plug-in for SecuRemote will be used, otherwise any token may be used. Refer to the SC-1/EUS and ST-1/EUS Software Token Deployment Guide for token installation instructions.
- The following information is also required.

IP Address of the RADIUS server:	
Port number used by the RADIUS server:	
Shared Secret:	

3. Configure Check Point FW-1 and VPN-1

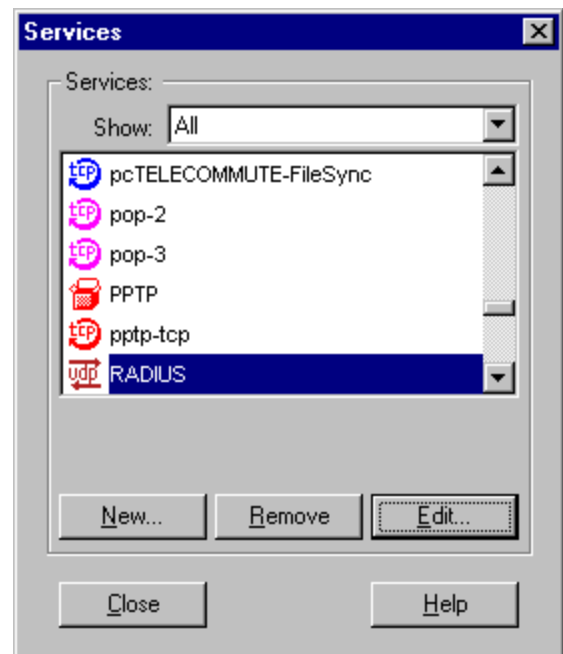
The following steps are required to complete the configuration of the FW-1 and VPN-1.

- Define a RADIUS Workstation
- Define a RADIUS Server
- Configure the RADIUS server port
- Enable RADIUS Authentication.
- Configuring the VPN-1® settings & IKE Encryption
- Create an authentication group.
- Add CRYPTOCARD users in FireWall-1/VPN-1
- Configure the Rule Set.

3.1 Configuring a RADIUS port in Check Point™ FireWall-1® / VPN-1®

Check Point™ FireWall-1 / VPN-1 and the RADIUS Server need to be configured to use the same port so they can exchange RADIUS packets. By default Firewall-1 uses port 1645. The RADIUS standards group has since changed this value to port 1812 as the official RADIUS port. Newer O/S releases have implemented the 1812 port number for RADIUS.

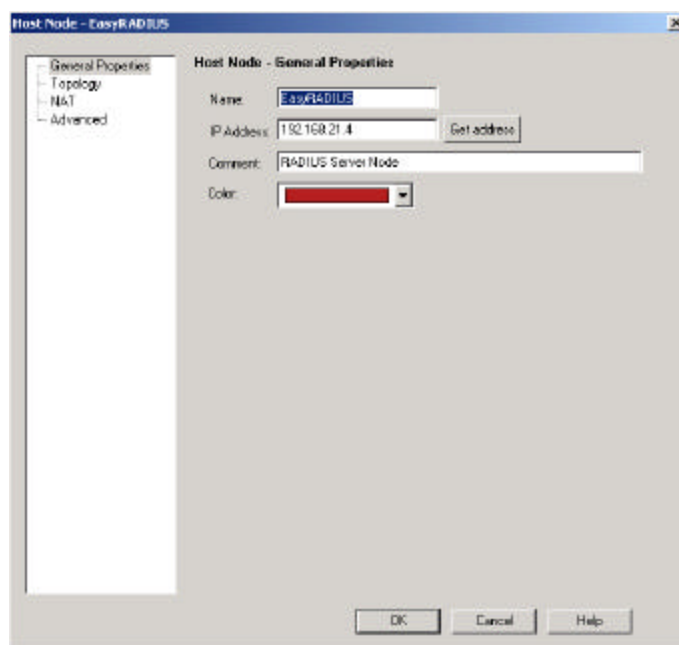
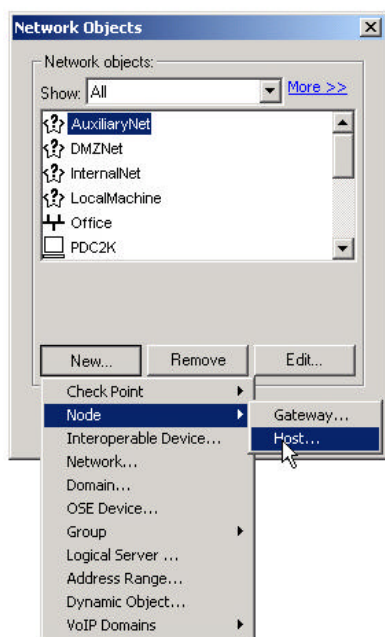
EasyRADIUS, Funk Steel Belted RADIUS, and Cisco Secure ACS will use the RADIUS port listed in the Services file. Please check your \WINNT \ System32 \ drivers \ etc \ services file (On Windows) or /etc/services/ file (On Solaris and RedHat) to determine the RADIUS port you are using for your RADIUS Server. Configure the RADIUS port in FireWall-1 to match the value on the RADIUS Server.



3.2 Defining the RADIUS Workstation in Check Point™ FireWall-1® / VPN-1®

On the machine with Check Point™ FireWall-1® / VPN-1®, define the IP address of the RADIUS Server. This should be on the system that CRYPTOAdmin and easyRADIUS was installed on, in this case the IP is 192.168.21.4

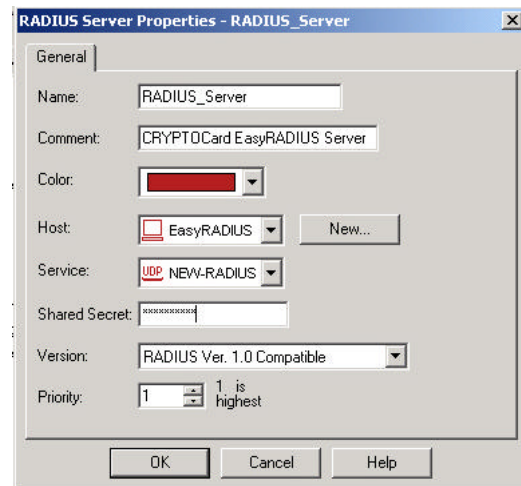
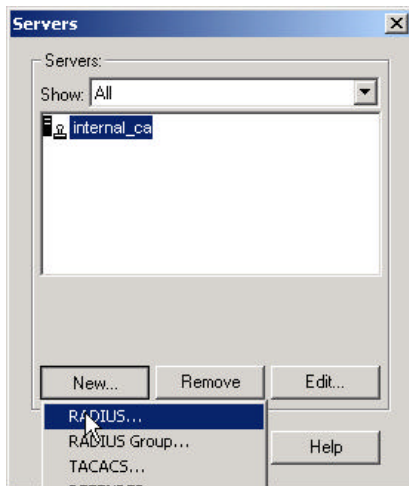
From the Check Point™ SmartDashboard, select Network Objects from the Manage Menu. Click New, select Node, and then click Host. Under General Properties, enter the Host Node Properties: Name, IP Address of RADIUS Server, Comment, and Color. Click OK then Close.



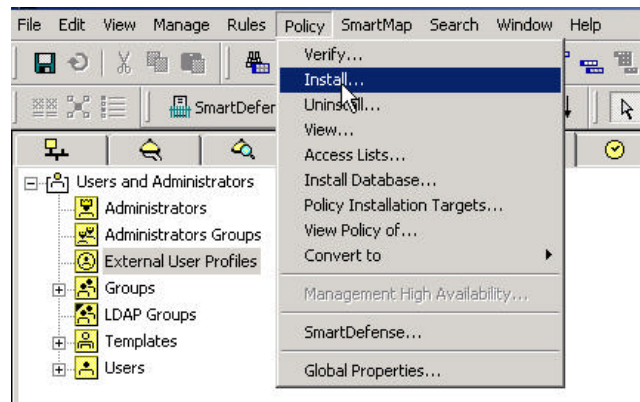
3.2.1 Defining the RADIUS Server in FireWall-1/VPN-1

From the system running Check Point™ FireWall-1® / VPN-1®, you need to define the machine which has your RADIUS Server installed on it. From the Check Point™ SmartDashboard, open the Manage Menu and choose Servers. In the Servers window, click New, then select RADIUS

Define your RADIUS Server Properties: Name, Comment, Color, Host (this should be the Host Node you defined in the previous section), Service (NEW-RADIUS should be selected if the RADIUS server is using port 1812), Shared Secret, and Version. Click OK, and then Close.



Click the Policy menu then choose Install.



The Shared Secret entered above must match the Shared Secret that is defined on the actual RADIUS server. For easyRADIUS, the default Shared Secret is 'testing123' without the

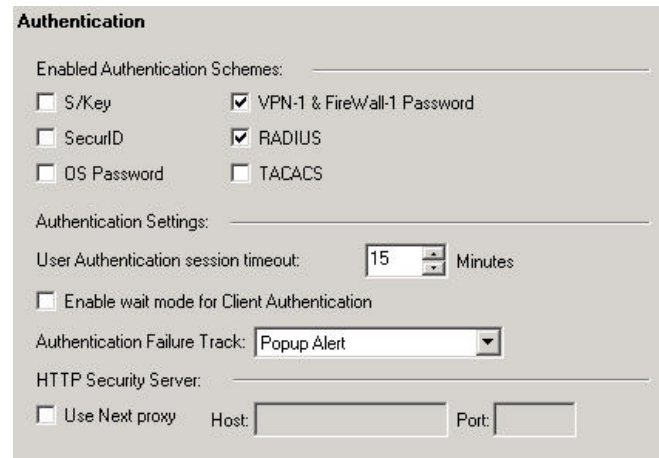
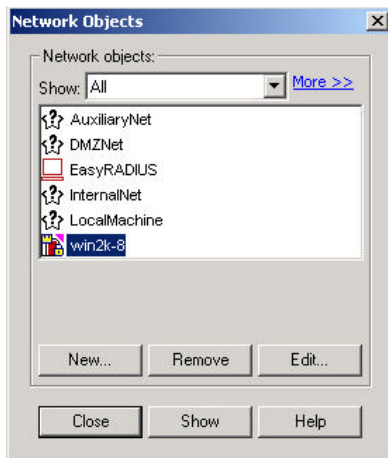
quotes. This is defined in the **clients** file located in /etc/cryptocard directory (Solaris and RedHat) or the \Program Files\CRYPTOCARD\CRYPTOAdmin\Server directory (Windows).

When choosing your RADIUS protocol version, you can select either RADIUS Version 1.0 or RADIUS Version 2.0. Both will work with easyRADIUS.

3.2.2 Enabling RADIUS Authentication on FireWall-1 / VPN-1

From the Check Point™ SmartDashboard, go to the Manage Menu and choose Network Objects. Select the FireWall-1® / VPN-1® object (in this case it's win2k-8) and click Edit.

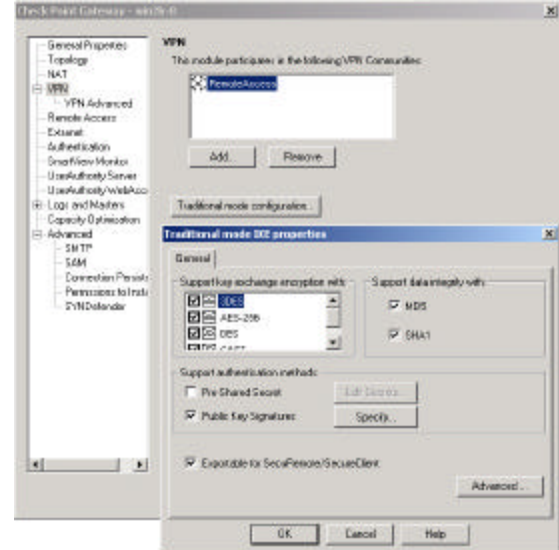
Under General Properties, select Authentication then verify the boxes to the left of VPN-1® & FireWall-1® Password and RADIUS are checked.



3.2.3 Configuring the VPN-1â settings & IKE Encryption

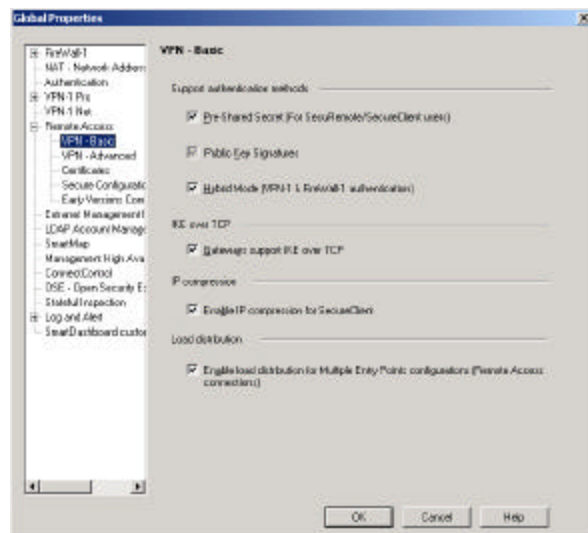
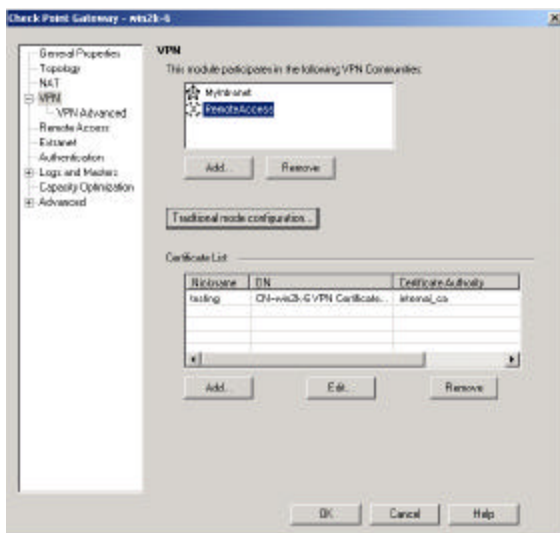
The following steps allow the SecuRemote™ end-users to download the VPN-1® topology from the FireWall, and to encrypt connections to the Inside network.

From the FireWall-1® / VPN-1® network object, under General Properties choose VPN then select your VPN Community (RemoteAccess), click Traditional mode configuration. Make sure to place a check in the box next to 'Exportable for SecuRemote/SecureClient'.



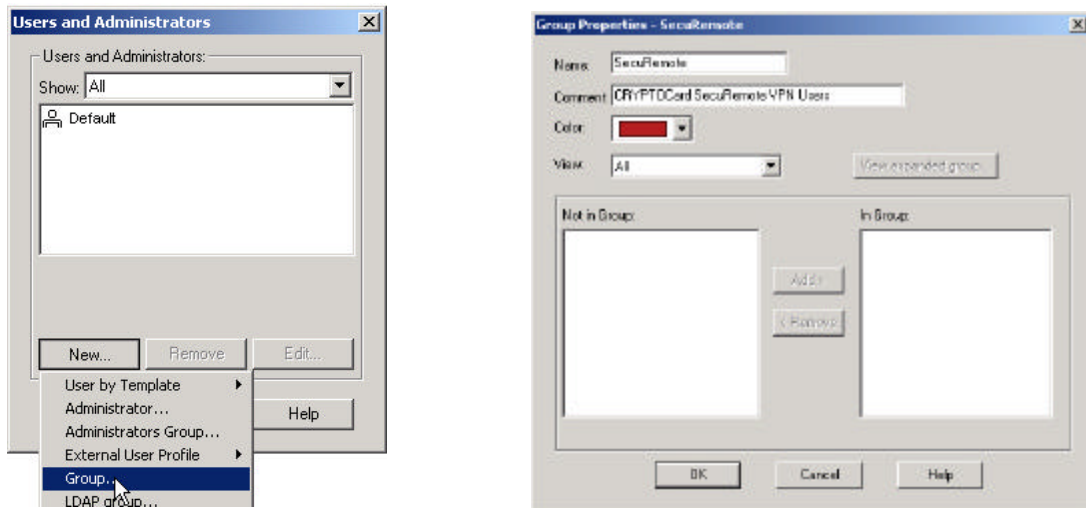
Note: If the FireWall-1â is in the Remote Access community already then this check box is checked and cannot be unchecked.

In the VPN section under General Properties verify that a Certificate exists in the Certificate List. Verify that Hybrid Mode Authentication has been enabled. Select Policy, Global Policy, Remote Access, VPN – Basic. Under Support authentication methods verify that Hybrid Mode has been checkmarked.



3.2.4 Creating an Authentication Group (VPN-1®)

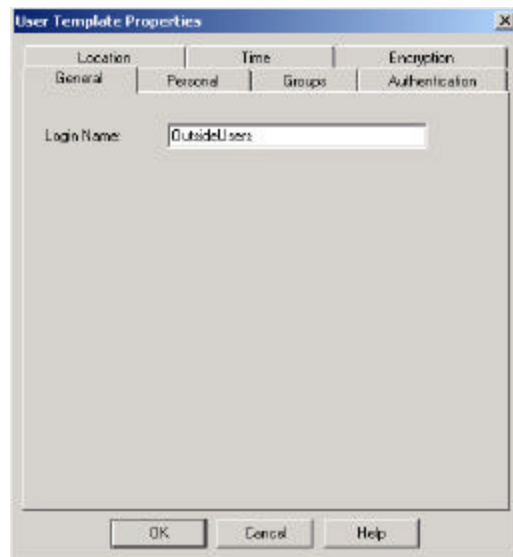
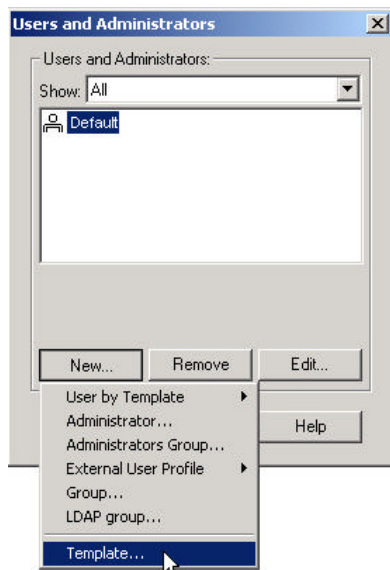
From the Manage Menu, select Users and Administrators then click New and select Group. This group will be used to reference all users being authenticated by a CRYPTOAdmin Server. In the Group Properties box enter the: Name, Comment, and Colour for the group. Click OK.



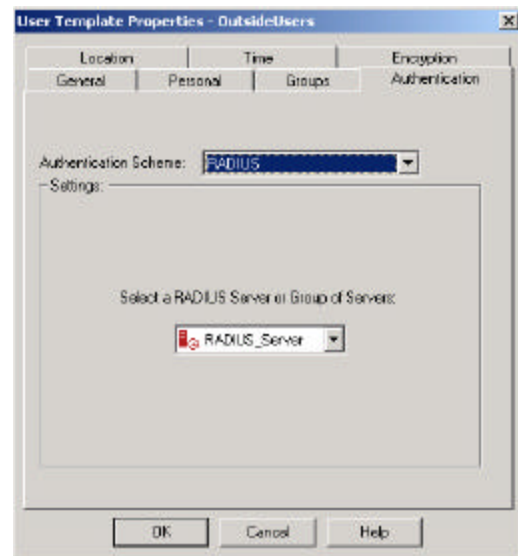
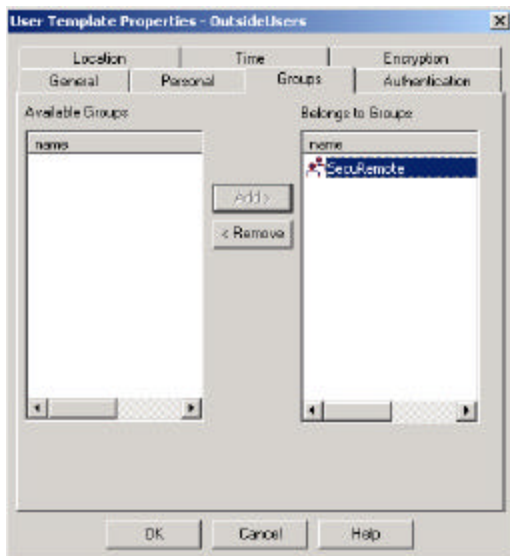
3.2.5 Adding CRYPTOCARD Users in FireWall-1® / VPN-1®

CRYPTOCARD token users can be configured to user RADIUS authentication in two methods on FireWall-1® / VPN-1®. Each CRYPTOCARD token user can be added to the FireWall-1® / VPN-1® database individually, or a generic user entry can be configured. Use the method that best meets your network authentication requirements.

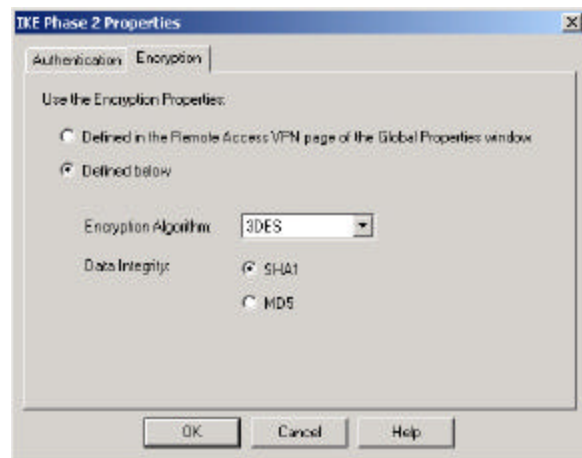
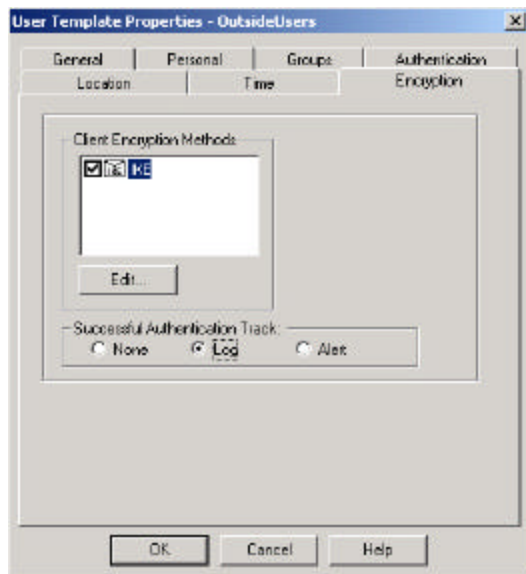
In the Check Point SmartDashboard, select Users and Administrators from the Manage Menu. Click New, then Template. In the User Template Properties dialog box, under the General Tab, define the Login Name. Click the Personal Tab to define the Expiration Date, Comment, and Color.



Click on the Groups Tab. Select the SecuRemote group created previously and click the Add button. Click on the Authentication Tab and define the Authentication Scheme as RADIUS, and select the RADIUS Server you just created in the previous section.

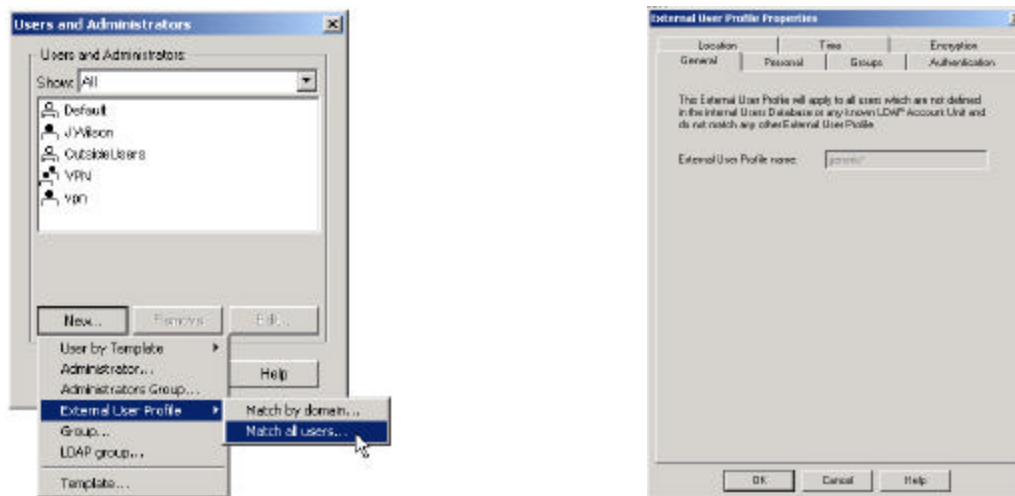


Click the Location Tab and Time Tab to define these settings as per your network security policy. Select the Encryption Tab and check the box to the left of 'IKE'. Click the Edit button to configure the IKE Encryption settings. Select the Encryption Tab to validate the Encryption Algorithm. Click the Install button to add the user to the FireWall-1® user database. Close the Users and Administrators dialog box.

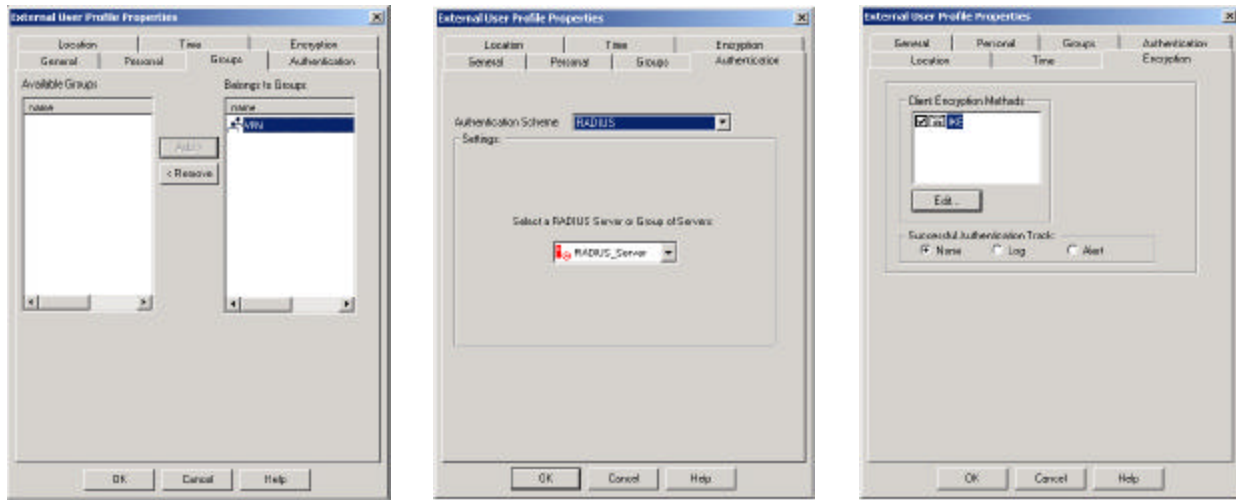


3.2.6 Configuring a Generic User Entry

From the Users and Administrators window, click New, External User Profile then choose Match all users.



In the External User Profile Properties window, select the VPN tab then add the appropriate Group. On the Authentication tab choose RADIUS as the Authentication Scheme then select the RADIUS Server. Select the Encryption tab and place a checkmark in IKE.



3.2.7 Creating a FireWall-1 / VPN-1 Rule Set

Below is an example of two simple rule sets that will require users to authenticate with CRYPTOCARD tokens. Configure the rule sets as per your network requirements.

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON
1	external@Any	* Any	* Any	TCP http TCP ftp TCP telnet	User Auth	Log	Gateways
2	SecuRemote@Al	* Any	* Any	TCP ftp TCP http TCP telnet	Client Auth	Log	Gateways

- The first rule states that anyone in the group External are required to be 'Authenticated' to be able to use HTTP, FTP, or Telnet. Authentication may be via RADIUS or FireWall-1's internal database.
- The second rule has the SecuRemote group that contains users configured to use RADIUS as their authentication method when using the FTP, HTTP, or Telnet services.

Once you have established your rules connect to the service using a CRYPTOCARD Token username and response generated from your token.

4. Connect using SecuRemote™

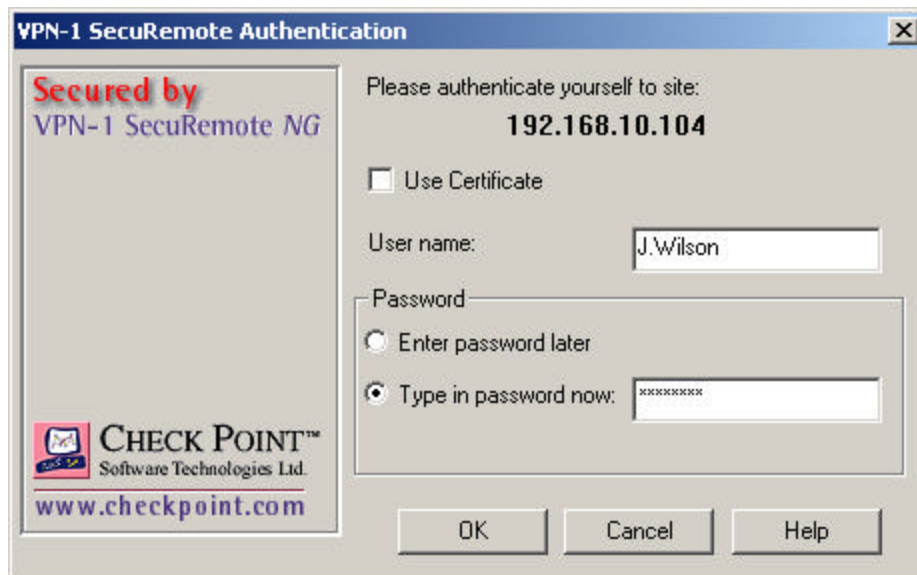
After installing SecuRemote™ /Secure Client™ and configuring it to connect to the VPN-1® / FW-1® gateway, the End-user will be able to connect to the gateway using their CRYPTOCARD token.

Using the connection configured above, connect to the VPN concentrator.

Enter the CRYPTOCARD token username.

Generate a One-Time-Password from the CRYPTOCARD token.

Enter that One-Time-Password in the password field, and click OK.



Once the VPN-1® / FW-1® gateway has verified the username and password with the CRYPTOAdmin database, the secure tunnel will be established.

5. CRYPTOCARD Authentication Plug-in for Check Point SecurRemote Client

CRYPTOCARD authentication includes a Plug-in for Check Point SecurRemote Clients that automates the authentication and logon process for End-users with ST-1/EUS software or SC-1/EUS smart card tokens for a “One-PIN-and-You’re-In” logon experience.

5.1 Installing CRYPTOCARD EUS

5.1.1 Run the EUS installer

- ? For Windows: CRYPTOCARD_EUS_for_Windows.exe
- ? For Linux: CRYPTOCARD_EUS_for_Linux.bin
- ? For Solaris: CRYPTOCARD_EUS_for_Solaris.bin

5.1.2 Select Installation Type

Typical – this mode installs the EUS in default directories and enables EUS management functions for administrators.

Custom – this mode installs the EUS in selected directories and allows EUS management to be enabled for end-users if the option box is selected.

For more information refer to the SC-1/EUS and ST-1/EUS Software Token Deployment Guide.

5.2 Applying ST-1 or SC-1 token to EUS

Locate initialization file on local machine. For all operating systems:

ST-1 initialization file has a .tok extension

Name	Size	Type
J.Wilson.tok	1 KB	CRYPTOCARD Token
L.Mahon.sc	1 KB	CRYPTOCARD Token

SC-1 initialization file has a .SC extension

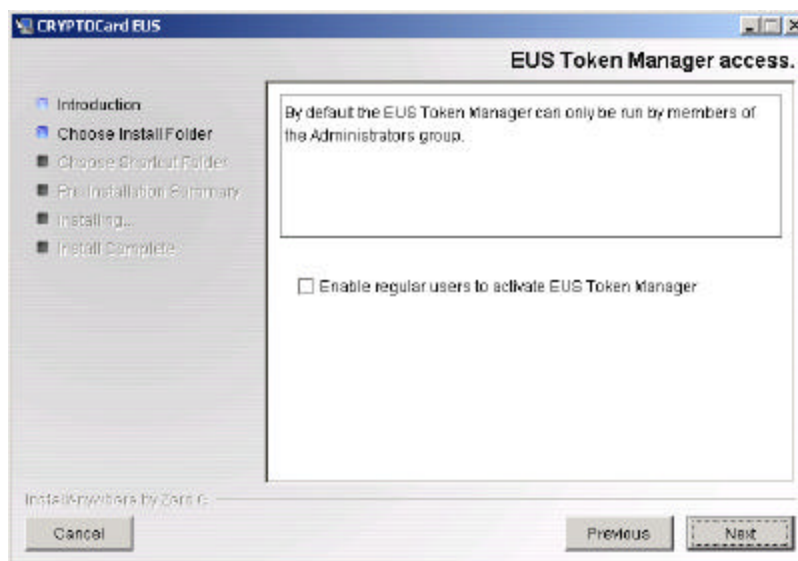
Name	Size	Type
J.Wilson.tok	1 KB	CRYPTOCARD Token
L.Mahon.sc	1 KB	CRYPTOCARD Token

For Windows:

ST-1: Double click on the initialization file. This will start the "Activate Token Wizard"

SC-1: Insert smart card into reader. Double click on the initialization file. This will start the "Activate Token Wizard"

For Linux and Solaris:



ST-1: In a console window type authenticator <token name>.tok.

Complete installation by entering the initial deployment PIN



EUS: The installation is successful when the CRYPTOCARD Token Authenticator appears and the applied token is displayed in the "Token Name" drop down.

The token is now ready for use in manual authentication mode. Plug-ins and agents for VPN, dialer, web server or Windows domain logon automated authentication can now be installed.

5.3 SecuRemote™ VPN Plug-in

The Plug-in for SecuRemote™ simplifies the authentication process for end-users while providing the full benefits of one-time passwords and strong user authentication. During VPN logon the end-user is prompted for the secret security PIN, allowing the Plug-in and EUS to complete the authentication process without further user involvement.

5.4 Installation

Install the VPN Plug-in by running: CRYPTOPlugin_for_SecuRemote.exe.

5.5 SecuRemote™ Authentication

Once the CRYPTOCARD VPN Plug-in is installed, creating the VPN tunnel becomes a simple one-step process for the end-user.

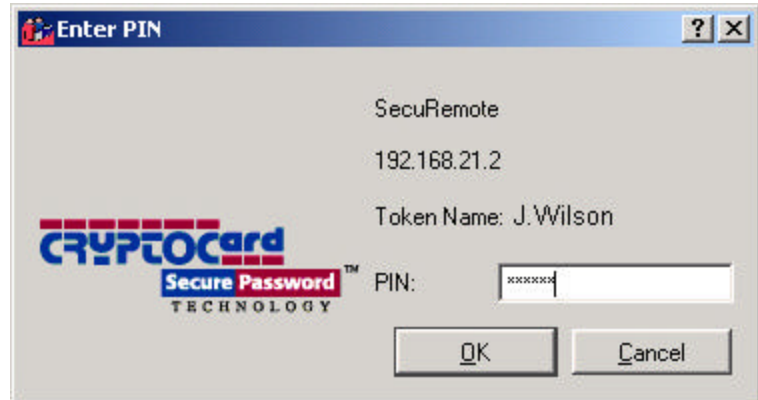
When the end-user clicks "connect" on the SecuRemote™ icon in the system tray, or when SecuRemote™ automatically launches, the end-user is prompted for the token name and PIN to enable their token. Check Point VPN-1 authentication

Click on the SecuRemote icon to launch the VPN Client

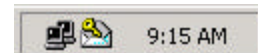


On computers with more than one EUS token, select the token to be used for authentication from the Token Name drop down.

Enter secret security PIN to enable token.



SecuRemote connection will appear in the system tray.



6. Logging on to a Windows Domain with CRYPTOLogon

CRYPTOLogon can be used to prevent unauthorized users from logging on to a Microsoft Windows Domain or a local computer account. Laptop computer users often need to be able to authenticate to a local domain when they are at the office, and log on to a remote domain when they are away from the office. Refer to the CRYPTOLogon Agent for Windows Domain Authentication Deployment Guide for installation and application of CRYPTOLogon Agent. Access to the remote office is made available to these laptop users over a secure VPN tunnel.

CRYPTOLogon can be used in this scenario in the following manner:

Enter the CRYPTOCard secret security PIN to unlock the desktop.



Enter the Windows logon information to connect to the domain



Initiate the VPN tunnel. Once the VPN tunnel is established, the user can browse the network, and has access to mapped drives as if they were connected to the network locally.



7. Troubleshooting Tips

7.1 Known Issues

The CRYPTOCARD SecuRemote Plug-in included with CRYPTOAdmin distributions V.28 and earlier uses CheckPoint's SecuRemote Authentication API (SAA) version 1. SAA v1 suffers from an issue where the wrong authentication dialog box is called on 'Set Password' resulting in an inconsistent user experience and a potential for the Response API to be called out of context. Authentication requests will succeed however an unnecessary authentication dialogue box may appear after a successful authentication. This issue has been corrected by CheckPoint in SAA v2. CRYPTOCARD will be incorporating the newer version of SAA in it's next maintenance release"

7.2 Troubleshooting

If you are experiencing continuous authentication failures, and would like to monitor the easyRADIUS or CRYPTOAdmin services in real-time, run the CRYPTOAdmin service and easyRADIUS service in the foreground.

On Windows:

- From the Services icon in the Control Panel stop both the CRYPTOAdmin and easyRADIUS services.
- Open a Command Prompt and go to the \ Program Files \ CRYPTOCARD \ CRYPTOAdmin \ Server directory. Enter the command **radiusd -sfxxyz -l stdout** without the quotes. The screen should display the message 'Ready to process requests.'
- This will send all output to the screen. This allows you to see in real-time all activity occurring on the RADIUS Server.

On RedHat:

From a console type **/etc/rc.d/init.d/radiusd stop**. Then type **/etc/rc.d/init.d/radiusd start debug**. The screen should display the message 'Ready to process requests.'

On Solaris:

From a console type **/etc/init.d/radiusd stop**. Then type **/etc/init.d/radiusd start debug**. The screen should display the message 'Ready to process requests.'

If you are using easyRADIUS for your RADIUS Server, you must have DNS configured properly or have an updated hosts file on the easyRADIUS Server that lists both interfaces of the FireWall-1/VPN-1 system.

If you encounter a problem that cannot be solved using the tips above, contact support@cryptocard.com or call us at (800) 307-7042 or +1-613-599-2441, Monday through Friday 8:30 am to 5:00 pm EST.