

WatchGuard Firebox and MUVPN

Quick Start Guide

Table of Contents

1. PURPOSE	1
1.1 Prerequisites	1
2. CRYPTO-SERVER CONFIGURATION	1
2.1 RadiusProtocol NAS.# keys	2
2.2 Verifying the CRYPTO-Server RADIUS Protocol Settings.....	3
3. CONFIGURING FIREBOX TO USE CRYPTOCARD AUTHENTICATION	4
3.1 MUVPN with CRYPTOCARD.....	4
3.1.1 Performing a MUVPN Connection	5
3.2 Adding CRYPTOCARD Authentication to a Service.....	6
3.2.1 Group-Based Protection.....	6
4. AUTHENTICATED LOGON	7
5. TROUBLESHOOTING TIPS	8

1. Purpose

The intent of this document is to present the necessary steps to configure the WatchGuard Firebox and MUVPN to use CRYPTOCard authentication.

1.1 Prerequisites

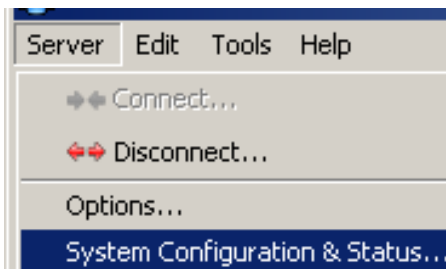
In order to successfully be able to authenticate end-users using CRYPTO-Server, the following items must be properly installed and configured:

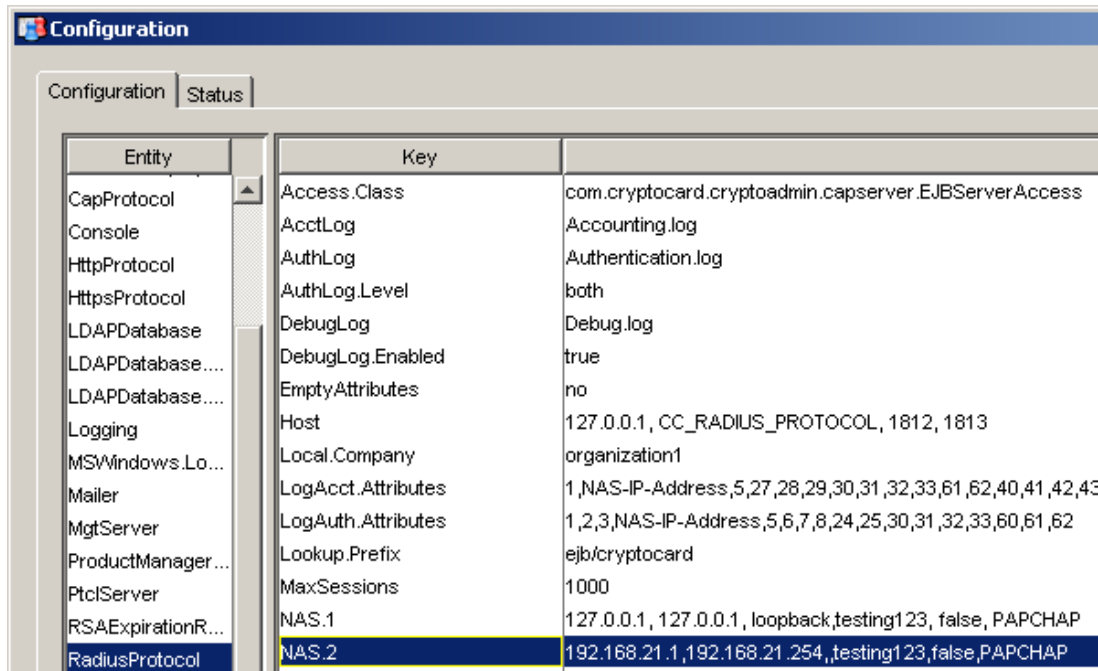
- WatchGuard Firebox installed and configured
- CRYPTO-Server acting as a RADIUS server, or Cisco Secure ACS (version 3.1 or higher), Funk Steel-Belted Radius (version 2.27 or higher) or Microsoft IAS 2003, configured to work with the CRYPTO-Server
- An initialized CRYPTOCard token assigned to a valid CRYPTOCard user
- An End-user client able to connect to the Firebox

2. CRYPTO-Server Configuration

If you wish to use the CRYPTO-Server as your RADIUS server, you must verify that it is configured to accept RADIUS communications from the WatchGuard Firewall.

Connect to the CRYPTO-Server using the Console, and choose Server -> System Configuration & Status... from the menu.





Entity	Key	Value
CapProtocol	Access.Class	com.cryptocard.cryptoadmin.capservice.EJBServerAccess
Console	AcctLog	Accounting.log
HttpProtocol	AuthLog	Authentication.log
HttpsProtocol	AuthLog.Level	both
LDAPDatabase	DebugLog	Debug.log
LDAPDatabase....	DebugLog.Enabled	true
LDAPDatabase....	EmptyAttributes	no
Logging	Host	127.0.0.1, CC_RADIUS_PROTOCOL, 1812, 1813
MSVWindows.Lo...	Local.Company	organization1
Mailer	LogAcct.Attributes	1,NAS-IP-Address,5,27,28,29,30,31,32,33,61,62,40,41,42,43
MgtServer	LogAuth.Attributes	1,2,3,NAS-IP-Address,5,6,7,8,24,25,30,31,32,33,60,61,62
ProductManager...	Lookup.Prefix	ejb/cryptocard
PtclServer	MaxSessions	1000
RSAExpirationR...	NAS.1	127.0.0.1, 127.0.0.1, loopback,testing123, false, PAPCHAP
RadiusProtocol	NAS.2	192.168.21.1,192.168.21.254,,testing123,false,PAPCHAP

In the "Entity" column choose "RadiusProtocol".

Next look at the "Value" corresponding to the key "NAS.2".

The value of this key defines which RADIUS clients are allowed to connect to the CRYPTO-Server, and the shared secret they must use.

2.1 RadiusProtocol NAS.# keys

By default, the CRYPTO-Server is configured to listen for RADIUS requests over UDP port 1812, from any host on the same subnet, using a shared secret of "testing123". You can manually define as many RADIUS clients as desired by adding NAS.# entries to the CRYPTO-Server configuration.

The syntax of the data for a NAS entry is as follows:

<First IP>, <Last IP>, <Hostname>, <Shared Secret>, <Perform Reverse Lookup?>, <Authentication Protocols>

Where:

<First IP>: The first IP address of the RADIUS client(s) configured in this NAS.# key.

<Last IP>: The last IP address of the RADIUS client(s) configured in this NAS.# key.

If only one IP address is defined by a NAS.# key, the <First IP> and <Last IP> will be the same.

<Hostname>: Only applies in cases where the NAS.# key is for one host. Required for performing reverse lookup.

<Shared Secret>: A string used to encrypt the password being sent between the CRYPTO-Server and the RADIUS client (i.e. the Firebox). You will need to enter the exact same string into the WatchGuard configuration in Section 3 (see below). The <Shared Secret> string can be any combination of numbers, and uppercase and lowercase letters.

<Perform Reverse Lookup?>: An added security feature of the CRYPTO-Server is its ability to verify the authenticity of a RADIUS client by cross-checking its IP address with the Domain Name Server. If this value is set to true, when the CRYPTO-Server receives a RADIUS request from the RADIUS client defined by this NAS.# entry, it sends a request to the DNS using the hostname set in the NAS.# entry. The DNS should respond with the same IP address as configured in the NAS.# entry, otherwise the CRYPTO-Server assumes that the RADIUS packet is coming from some other host posing as the RADIUS client, and ignores the request completely.

<Authentication Protocols>: There are many different authentication protocols that can be used during RADIUS authentication. Common examples are PAP, CHAP,MS-CHAP and EAP. This setting determines which authentication protocols the CRYPTO-Server will allow from a given RADIUS client.

Currently PAP and CHAP are the only available authentication protocols for RADIUS clients.

NOTE: After changing or adding a NAS.# entry, click the “Apply” button.

2.2 Verifying the CRYPTO-Server RADIUS Protocol Settings

The RADIUSProtocol.dbg log¹ on the CRYPTO-Server will include information about its RADIUS configuration. Each time the Protocol Server starts, the following information is logged:

```
Adding IP range 127.0.0.1 to 127.0.0.1 to ACL with reverse lookup set to false
Adding IP range 192.168.21.1 to 192.168.21.254 to ACL with reverse lookup set
to false
RADIUS protocol has established link with EJB server at
jnp://192.168.21.5:1099
RADIUS Receiver Started: listening on port 1812 UDP.
```

¹ See section 5 Troubleshooting Tips for the location of the RADIUSProtocol.dbg file

RADIUS Receiver Started: listening on port 1813 UDP.

This example indicates that the CRYPTO-Server is listening for RADIUS requests on UDP port 1812 (for authentication) and 1813 (for accounting), and RADIUS clients within the IP range of 192.168.21.1 to 192.168.21.254. As well, no reverse lookup is being performed.

3. Configuring Firebox to use CRYPTOCARD Authentication

How you configure the Firebox depends on what type of Firebox authentication you want to direct to the CRYPTO-Server. If you want MUVPN connections to be authenticated by the CRYPTO-Server follow the instructions in section 3.1. To authenticate Firebox Groups using the CRYPTO-Server, follow the instructions in section 3.2.

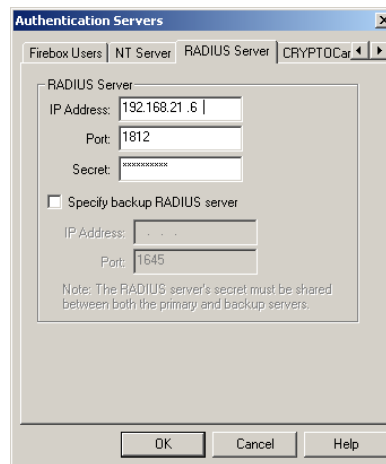
3.1 MUVPN with CRYPTOCARD

WatchGuard MUVPN (Mobile User Virtual Private Networking) clients are able to use CRYPTOCARD tokens to authenticate their VPN connection. The Firebox currently allows MUVPN clients to authenticate to a RADIUS server, such as the CRYPTO-Server, or another RADIUS server configured to work with the CRYPTO-Server.

From the Firebox Policy Manager,

- Select Setup | Authentication Servers
- Select the **RADIUS Server** tab
- Enter the necessary information to allow the WatchGuard Firebox to connect to the CRYPTO-Server.

Click **OK**.



Follow the WatchGuard instructions for setting up MUVPN as usual, but choose RADIUS as the authentication server.

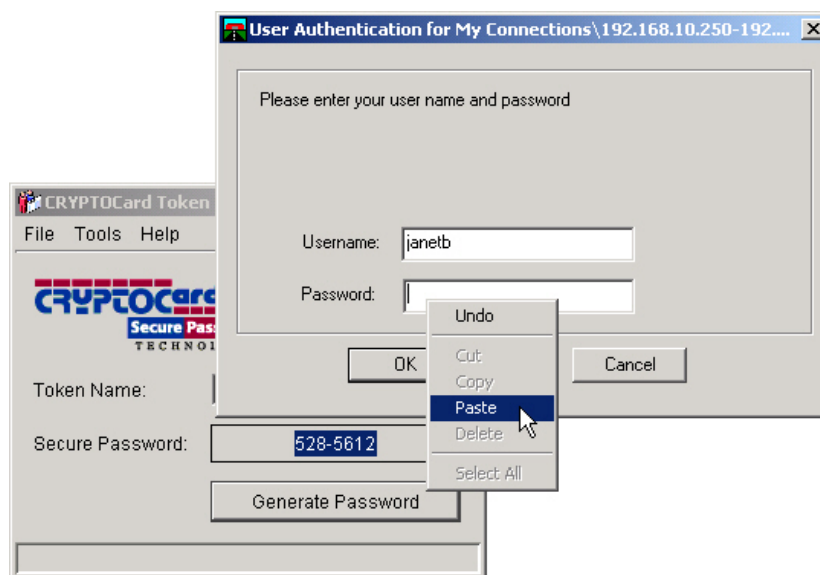
Follow the instructions in section 3.2.1 on setting authorizations on the CRYPTO-Server, so that the desired CRYPTOCARD users return a RADIUS Filter-ID matching the name of the MUVPN group.

3.1.1 Performing a MUVPN Connection

Now that the MUVPN profile has been created, it may be distributed to the client systems to allow clients to form a VPN connection to the Firebox.

If using CRYPTOCard software, smart card, or USB dongle tokens: When the MUVPN client prompts for a username and password, launch the CRYPTOCard Authenticator, click on Generate Password, enter the token PIN, and enter the CRYPTOCard username and one-time password into the MUVPN prompt.

If using CRYPTOCard hardware tokens (RB, KT, or SecurID): When the MUVPN prompts the end-user for a username and password, enter the CRYPTOCard username and one-time password² into the MUVPN prompt.

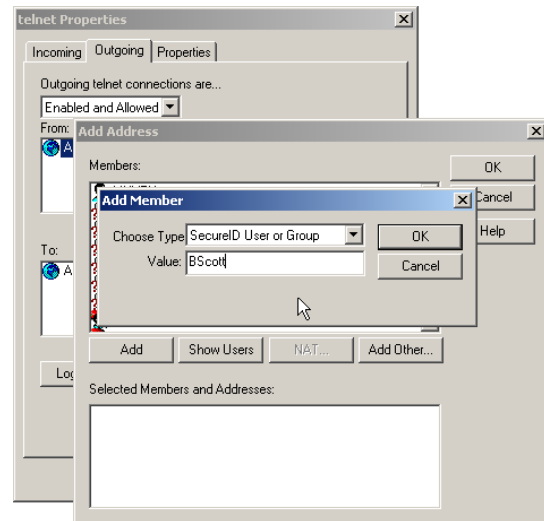


² In some cases this may include a PIN and the response from the users token

3.2 Adding CRYPTOCARD Authentication to a Service

To protect a service/port with CRYPTOCARD authentication, select the rule for that service/port and choose the incoming or outgoing tab, depending on the rule. Then select Add Other...

- From the dropdown, choose SecurID User or Group.
- In the Value field, enter a CRYPTOCARD username or a groupname.

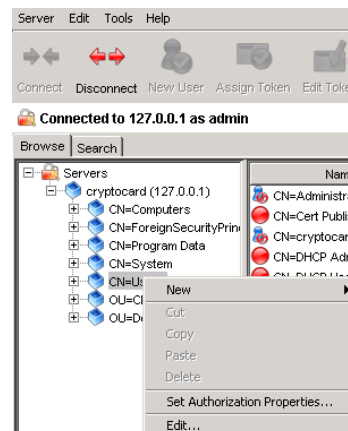


3.2.1 Group-Based Protection

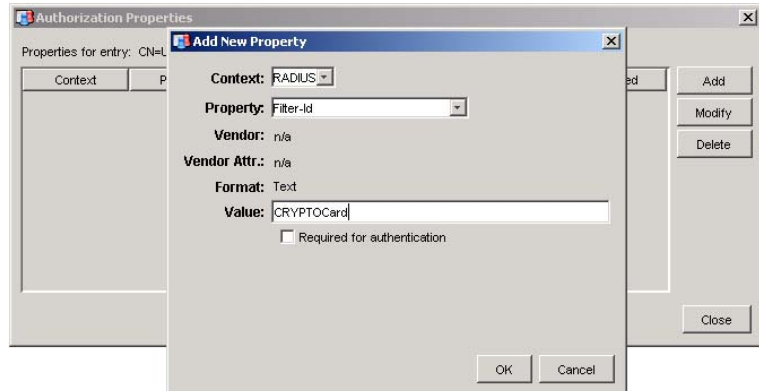
Instead of adding each individual user to a service on the Firebox, you can protect a service based on group membership. Then each CRYPTOCARD user who is a member of that group will automatically be incorporated into that Firebox service rule.

The group name set on the Firebox in the steps above does not correspond literally to a group name on the CRYPTO-Server, but rather to an authorization property set for a token, user or container of users on the CRYPTO-Server.

To add an authorization on the CRYPTO-Server, from the Console, right-click on the token, user, or container that you wish to add an authorization to, and choose Set Authorization Properties...



From the Authorization Properties window, choose Add, and enter the configuration for a RADIUS Filter-ID property. The value of the Filter-ID property must exactly match the Group name you configured on the Firebox.

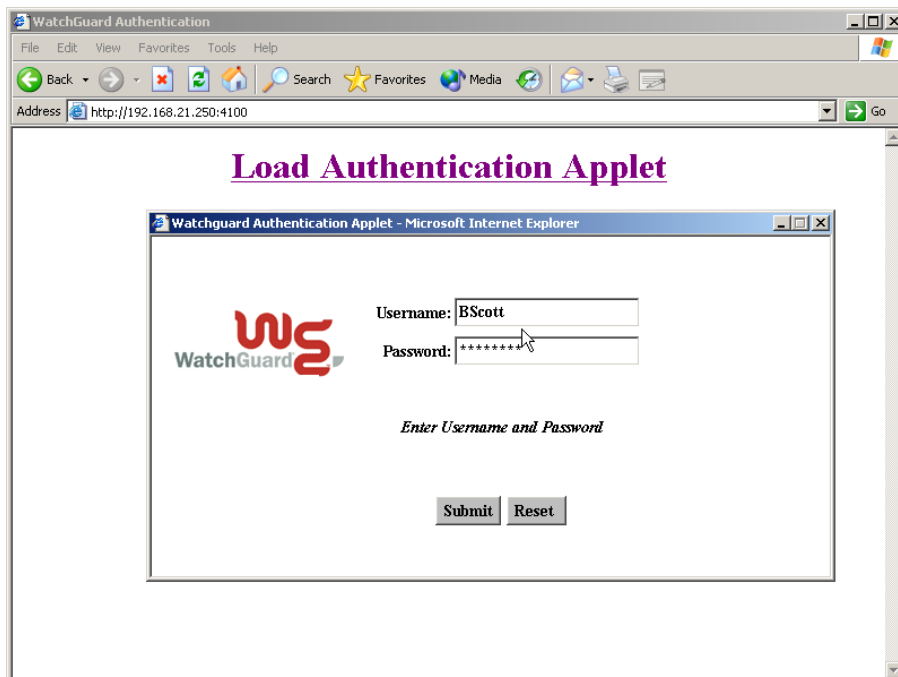


4. Authenticated Logon

In order to authenticate, users must connect to the Firebox using a Java-enabled Web browser to this URL:

http://[Firebox IP here]:4100

This loads a Java applet with prompts for a username, and response.



- Enter a CRYPTOCard username, and a response, and click Submit

The user is then authenticated, and as long as the applet window remains open, the user will be able to access the protected services from that same computer.

5. Troubleshooting Tips

Use the Firebox Traffic Monitor to monitor the authentication process, as it may give indications as to where the authentication is failing.

The CRYPTO-Server stores a log of all RADIUS traffic in

C:\Program Files\CRYPTOCARD\CRYPTO-Server\bin\RADIUSProtocol.dbg

Messages in this log may help pinpoint the source of the problem.

If you are using a Third Party RADIUS server, please refer to its troubleshooting documentation.

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.