Implementation Guide for protecting

Cisco VPN 3000 Concentrator

with

BlackShield ID

http:// www.cryptocard.com

Copyright

Trademarks

Additional Information, Assistance, or Comments

CRYPTOCard's technical support specialists can provide assistance when planning and implementing CRYPTOCard in your network. In addition to aiding in the selection of the appropriate authentication products, CRYPTOCard can suggest deployment procedures that provide a smooth, simple transition from existing access control systems and a satisfying experience for network users. We can also help you leverage your existing network equipment and systems to maximize your return on investment.

CRYPTOCard works closely with channel partners to offer worldwide Technical Support services. If you purchased this product through a CRYPTOCard channel partner, please contact your partner directly for support needs.

To contact CRYPTOCard directly:

International Voice: +1-613-599-2441

North America Toll Free: 1-800-307-7042

support@cryptocard.com

For information about obtaining a support contract, see our Support Web page at http://www.cryptocard.com.

Related Documentation

Refer to the Support & Downloads section of the CRYPTOCard website for additional documentation and interoperability guides: http://www.cryptocard.com.

Publication History

Date	Changes	Version
January 26, 2009	Document created	1.0
July 9, 2009	Copyright year updated	1.1

Table of Contents

Overview

By default the Cisco VPN Concentrator requires that a user provide a correct user name and password to successfully logon. This document describes the steps necessary to augment this logon mechanism with strong authentication by adding a requirement to provide a one-time password generated by a CRYPTOCard token using the instructions below.

Applicability

This integration guide is applicable to:

Security Partner Information	
Security Partner	Cisco
Product Name and Version	Cisco Concentrator 3000
Protection Category	Remote Access
Authentication encryption	PAP

CRYPTOCard Server	
Authentication Server	BlackShield ID
Version	Small Business Edition 1.2+ Professional Edition 2.3+

Assumptions

BlackShield ID has been installed and configured and a “Test” user account can be selected in the Assignment Tab.

Operation

When a user attempts to logon using the Cisco VPN client, they will input their user name and input a one-time password generated from their token. Upon valid authentication, the Cisco VPN connection will resume normal logon process flow.

Preparation and Prerequisites

1. Ensure end users can authenticate through the Cisco Concentrator with a static password before configuring the Cisco Concentrator 3000 to use RADIUS authentication.
2. BlackShield Pro server installed and a user account assigned with a CRYPTOCard token.
3. BlackShield Agent for Internet Authentication Service (*IAS*) or Network Policy Server (*NP*S).
4. Cisco ASA Server must be configured as a RADIUS client in Internet Authentication Service (*IAS*) or Network Policy Server (*NP*S).
5. Radius UDP ports are open between the Cisco Concentrator and the BlackShield ID server.

Configuration

Cisco VPN 3000 Concentrator

Configuring the Cisco VPN 3000 Concentrator consists of 3 steps:

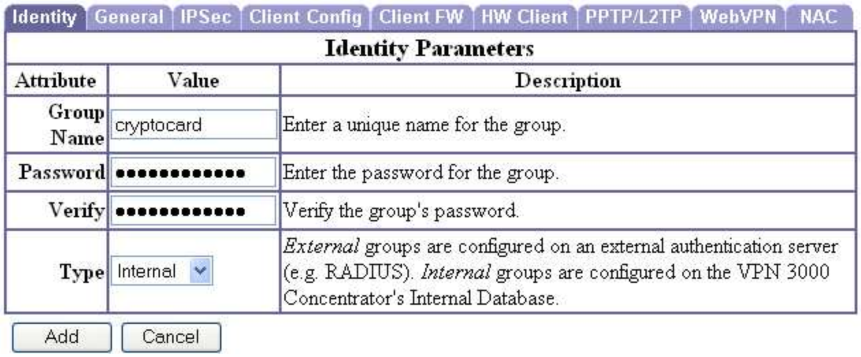
Step 1: Create a CRYPTOCard group

Step 2: Add a RADIUS server

Step 3: Test the Authentication Server

Step 1: Create a CRYPTOCard Group

1. In the VPN configuration manager, select Configuration | User Management | Groups.
2. Click Add Group.
3. Enter a Group Name and Password for the Group. Select Internal as the Type.

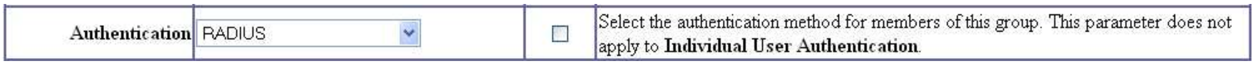


Identity Parameters

Attribute	Value	Description
Group Name	cryptocard	Enter a unique name for the group.
Password	●●●●●●●●●●●●	Enter the password for the group.
Verify	●●●●●●●●●●●●	Verify the group's password.
Type	Internal ▾	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

The internal group name and password is used when configuring the end user VPN client software.

4. Under the IPSec tab, select RADIUS in the Authentication pull-down menu.

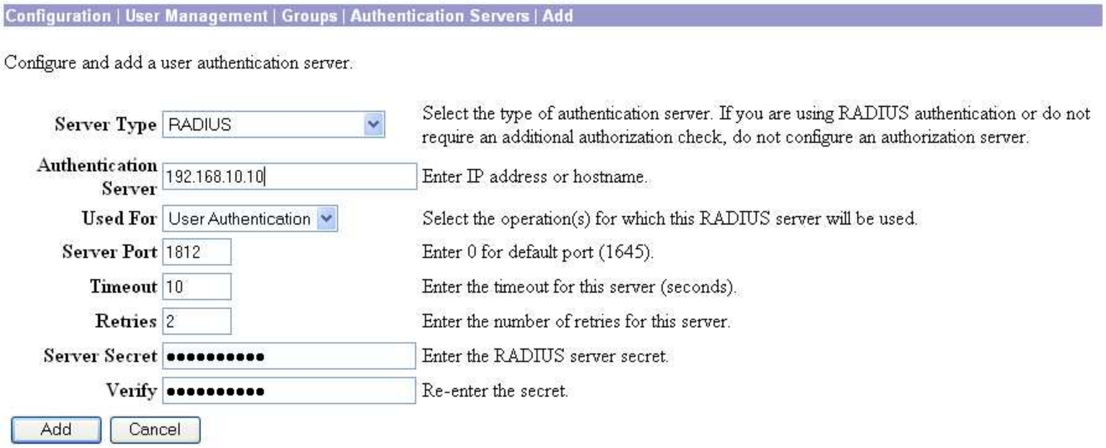


Authentication	RADIUS	☐	Select the authentication method for members of this group. This parameter does not apply to **Individual User Authentication**.

5. Click Add to add this group to the VPN concentrator.
6. Ensure this newly created group has an Address Pool of IP addresses that can be assigned to the VPN client connections. Select the Group and click Address Pools. Then click Add and enter the Range Start, Range End, and Subnet Mask. Apply the change.

Step 2: Add an Authentication Server (RADIUS Server)

1. In the VPN configuration manager, select Configuration | User Management | Groups. Highlight the VPN Group created in Step 4.1 then select Authentication Servers.
2. Click Add to add a new authentication server. Fill in the information for your RADIUS server. Once all the information is entered, click Add.



Configuration | User Management | Groups | Authentication Servers | Add

Configure and add a user authentication server.

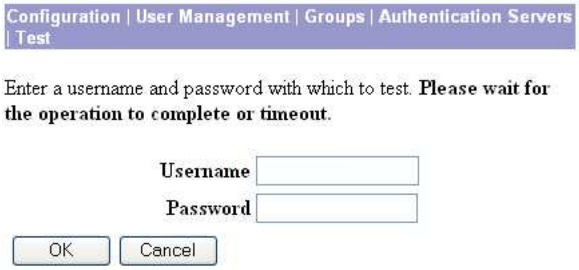
Server Type	RADIUS	Select the type of authentication server. If you are using RADIUS authentication or do not require an additional authorization check, do not configure an authorization server.
Authentication Server	192.168.10.10	Enter IP address or hostname.
Used For	User Authentication	Select the operation(s) for which this RADIUS server will be used.
Server Port	1812	Enter 0 for default port (1645).
Timeout	10	Enter the timeout for this server (seconds).
Retries	2	Enter the number of retries for this server.
Server Secret	●●●●●●●●●●●	Enter the RADIUS server secret.
Verify	●●●●●●●●●●●	Re-enter the secret.

The VPN concentrator must be configured as a client of the RADIUS server. The RADIUS server must have a configuration that matches the one described above to be able to receive authentication requests from the VPN concentrator.

Step 3: Test the Authentication Server

Once the RADIUS server has been added to the VPN concentrator setup, use the internal test mechanism to ensure the VPN concentrator can authenticate using a CRYPTOCard token:

1. In the VPN configuration manager, select Configuration | User Management | Groups. Highlight the VPN Group created in Step 4.1 then select Authentication Servers.
2. Highlight the RADIUS server entry select Test.



Configuration | User Management | Groups | Authentication Servers | Test

Enter a username and password with which to test. **Please wait for the operation to complete or timeout.**

Username

Password

3. Enter the User Name of a CRYPTOCard account, and the CRYPTOCard Password generated by the token assigned to that user. Click OK. If the test fails, refer to Troubleshooting section.

Cisco VPN Client Configuration

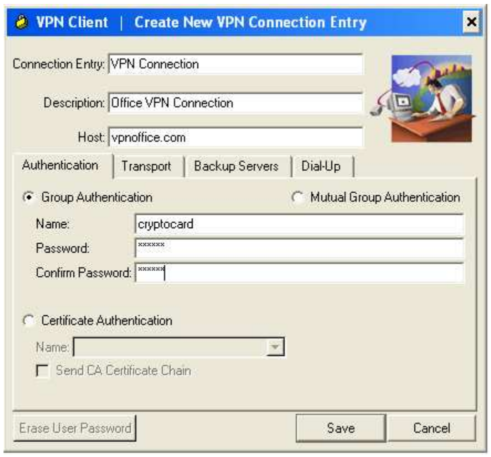
You must configure the VPN client software to enable the end user to connect to the IPSec group. There are 2 steps to configuring the Cisco VPN Client:

Step 1: Create a new VPN connection

Step 2: Connect using the Cisco VPN client

Step 1 - Create a new VPN connection

From the Cisco VPN Client software, click New to create a new connection entry. Fill in the information for the connection entry, using the group name and password specified in section titled '**Create a CRYPTOCard group**'.



VPN Client | Create New VPN Connection Entry

Connection Entry: VPN Connection

Description: Office VPN Connection

Host: vpnoffice.com

● Group Authentication ○ Mutual Group Authentication

Name: cryptocard

Password: ******

Confirm Password: ******

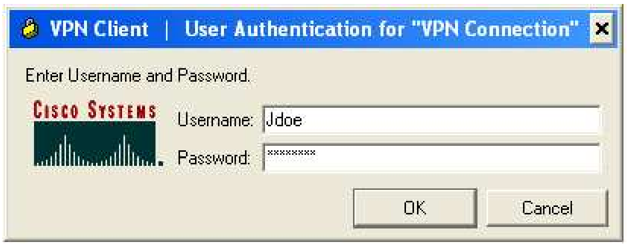
○ Certificate Authentication

Name:

□ Send CA Certificate Chain

Step 2 - Connect using the Cisco VPN client

1. Once the VPN client software has been configured correctly, the end user should be able to connect to the concentrator using their CRYPTOCard token. Choose the connection entry created and click Connect.
2. Once the group information has been passed to (and accepted by) the VPN Concentrator, a dialog box will open requesting a Username and Password. Enter the CRYPTOCard Username. Generate a one-time password from the CRYPTOCard token and enter your PIN followed by the one-time password in the Password field (depending on whether you have configured it to require Server-Side PIN). Click OK.



Enter Username and Password.

Username: Jdoe

Password: ********

3. Once the concentrator has verified the username and password with the CRYPTO-Server database, the connection will be established.

Troubleshooting

When troubleshooting issues with setting up RADIUS authentication on a Cisco VPN concentrator it may be helpful to refer to the log files on the VPN concentrator. Refer to Cisco documentation for details about the VPN concentrator logging facility.

All logging information for Internet Authentication Service (IAS) or Network Policy Server (NPS) can be found in the Event Viewer.

All logging information for the BlackShield IAS\NPS agent can be found in the \Program Files\CRYPTOCard\BlackShield ID\IAS Agent\log directory.

All logging information on the BlackShield ID Pro server can be found in the Snapshot Tab of the management console.

The following is an explanation of the logging messages that may appear in the event viewer for the Internet Authentication Service (IAS) or Network Policy Server (NPS) RADIUS Server.

Error Message:	Packet DROPPED: A RADIUS message was received from an invalid RADIUS client.
Solution:	Verify a RADIUS client entry exists on the RADIUS server.

Error Message:	Authentication Rejected: Unspecified
Solution:	This will occur when one or more of the following conditions occur: • The username does not correspond to a user on the BlackShield Server. • The CRYPTOCard password does not match any tokens for that user. • The shared secret entered in Cisco Secure ACS does not match the shared secret on the RADIUS server

Error Message:	Authentication Rejected: The request was rejected by a third-party extension DLL file.
Solution:	This will occur when one or more of the following conditions occur: • The BlackShield Agent for IAS\NPS cannot contact the BlackShield Server. • The Pre-Authentication Rules on the BlackShield server do not allow incoming requests from the BlackShield Agent for IAS\NPS. • The BlackShield Agent for IAS\NPS Keyfile does not match the Keyfile stored on the BlackShield Server. • The username does not correspond to a user on the BlackShield Server • The CRYPTOCard password does not match any tokens for that user.

Further Information

For further information, please visit http://www.cryptocard.com