

Cisco Secure ACS 3.0+

Quick Start Guide



# Table of Contents

**OVERVIEW ..... 1**

CONFIGURING THE EXTERNAL USER DATABASE ..... 1

SETTING THE UNKNOWN USER POLICY ..... 3

MAPPING CRYPTOCARD USERS TO A CISCO SECURE GROUP..... 3

CRYPTO-SERVER CONFIGURATION ..... 4

RADIUSPROTOCOL NAS.# KEYS..... 5

VERIFYING THE CRYPTO-SERVER RADIUS PROTOCOL SETTINGS..... 6

**TROUBLESHOOTING TIPS ..... 7**

TOKEN CACHING ..... 7

CISCO SECURE LOGGING MESSAGES ..... 7

“CS USER UNKNOWN” ..... 7

“EXTERNAL DB AUTH FAILED” ..... 7

“EXTERNAL DB NOT OPERATIONAL” ..... 7

CISCOSECURE ACS 3.1 CRASHES ..... 8

CHANGING THE RADIUS PORT USED BY CRYPTO-SERVER ..... 8

## Overview

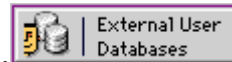
Cisco Secure version 3.0+ connects to the CRYPTO-Server using the RADIUS authentication protocol. This means that the CRYPTO-Server may run on the same machine as ACS, or on a separate machine, and that the CRYPTO-Server must be listening for RADIUS communication.


The following information is required during configuration:

IP Address of the ACS server:	
IP Address of CRYPTO-Server:	
Port number used by CRYPTO-Server for RADIUS communication:	
RADIUS Shared Secret:	


### Configuring the External User Database

From the Cisco Secure ACS administrator select External User Databases.



Then click on Database Configuration.  [Database Configuration](#)

Next select CRYPTOCARD Token Server. [CryptoCard Token Server](#) or RADIUS Server.

**Create a new External Database Configuration** 

Enter a name for the new configuration for CryptoCard Token Server

Choose Create New Configuration.

**CryptoCard Token Server Configuration.**

**RADIUS Configuration**

Primary Server Name/IP:	<input type="text"/>
Secondary Server Name/IP:	<input type="text"/>
Shared Secret:	<input type="text"/>
Authentication Port:	<input type="text" value="1812"/>
Timeout (seconds):	<input type="text" value="10"/>
Retries:	<input type="text" value="3"/>
Failback Retry Delay (minutes):	<input type="text" value="5"/>

Submit the default name for the configuration.

Select Configure.

Enter the IP address or host name of the primary CRYPTO-Server.

[OPTIONAL] Enter the IP address or host name of the secondary CRYPTO-Server.

Enter the shared secret as configured on the CRYPTO-Server(s).

Verify that the correct port for RADIUS communication from the CRYPTO-Server is entered.

---

**NOTE:** If Cisco Secure and CRYPTO-Server are installed on the same server, the CRYPTO-Server RADIUS protocol must be manually configured to use an available port. This is because Cisco Secure will already lock ports 1645, 1646, 1812 and 1813 (defaults) for its RADIUS server. To change the port that CRYPTO-Server uses, refer to the Troubleshooting section at the end of this document.

---

Enter the timeout for communications between ACS and CRYPTO-Server.

Enter the number of retries ACS should make before trying the secondary CRYPTO-Server.

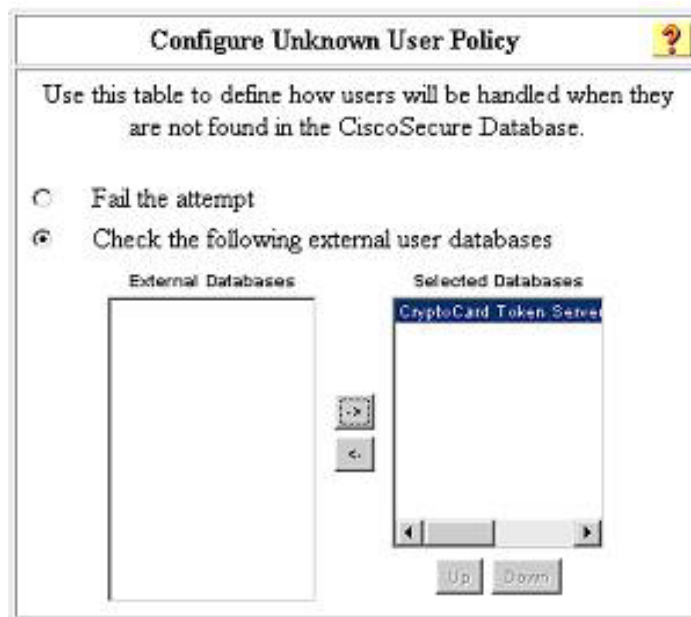
Enter the delay that ACS should wait before trying to communicate with a non-responsive primary CRYPTO-Server again, as the "Failback Retry Delay".

## Setting the Unknown User Policy

The Unknown User Policy in Cisco Secure can be used to automatically add CRYPTOCARD users to the ACS database.

The rules of this policy are used by ACS to determine what to do when an authentication request comes in for a username that is not found in the Cisco Secure database.

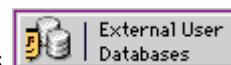
If the policy states that the CRYPTO-Server should be checked, then the username will be forwarded to CRYPTOCARD for authentication. The username will only be added to the Cisco Secure database after the user has succeeded in authenticating to the CRYPTO-Server.



## Mapping CRYPTOCARD Users to a Cisco Secure Group

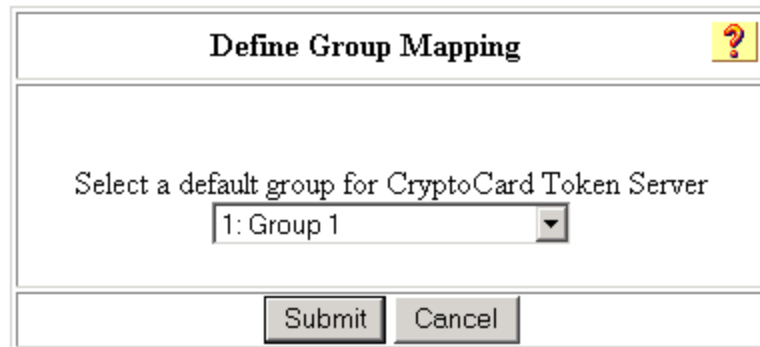
The Database Group Mappings setting determines what group to create new CRYPTOCARD users in, if the Unknown User Policy is configured to check the CRYPTOCARD Token Server.

From the Cisco Secure ACS administrator select External User Databases.



Then click on Database Group Mappings.  [Database Group Mappings](#)

Select the CRYPTO-Server [CryptoCard Token Server](#) or RADIUS Server.



Choose the desired default group.

### CRYPTO-Server Configuration

You may need to configure the CRYPTO-Server to accept RADIUS communication from the Cisco Secure ACS host.

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



Entity	Key	
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....	Empty.Attributes	no
Logging	Host	127.0.0.1, CC_RADIUS_PROTOCOL, 1812, 1813
MSWindows.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
RSASessionR...	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.

### RadiusProtocol NAS.# keys

By default, the CRYPTO-Server is configured to listen for RADIUS requests 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 CRYPTOServer and the RADIUS client (i.e. Cisco ACS). You will need to enter the exact same string into Cisco ACS in the "Configuring the External User Database" section above. 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.**

---

### Verifying the CRYPTO-Server RADIUS Protocol Settings

The RADIUSProtocol.dbg<sup>1</sup> log 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.
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.

---

<sup>1</sup> On Windows this file is located under Program Files\CRYPTOCARD\CRYPTO-Server\bin

## Troubleshooting Tips

### Token Caching

If token caching fails with Cisco Secure 3.0, verify the registry on the ACS server:

HKLM\SW\Cisco\CiscoAAAv3.0\Authenticators\Libraries\13\

REG\_DWORD "Properties" should be 0x10d (269 decimal)

Then restart the CSAdmin and CSauth services.

### Cisco Secure logging messages

The following is an explanation of the logging messages in the "Failed Attempts" log file in Cisco Secure ACS:

#### "CS user unknown"

Cisco Secure logs this message when it receives a username that is not in the local database.

If the username exists in the CRYPTO-Server user database, the Unknown User Policy in Cisco Secure has not been configured properly to search the CRYPTO-Server database. See the "Setting the Unknown User Policy" section of this document.

#### "External DB auth failed"

Cisco Secure logs this message when it receives an incorrect password for a given CRYPTOCARD token user. Use the CRYPTO-Console, or the RadTest command line utility in the Cisco Secure "Utils" directory to verify that the token is working correctly.

#### "External DB not operational"

If a Cisco Secure 3.0+ server logs this message, it indicates that ACS was unable to connect to the CRYPTO-Server as configured in the CRYPTOCARD Token Server Configuration in ACS. Check the RADIUSProtocol.dbg<sup>2</sup> log file on the CRYPTO-Server to determine if RADIUS requests are reaching the CRYPTO-Server.

---

<sup>2</sup> On Windows this file is located under Program Files\CRYPTOCARD\CRYPTO-Server\bin

## CiscoSecure ACS 3.1 Crashes

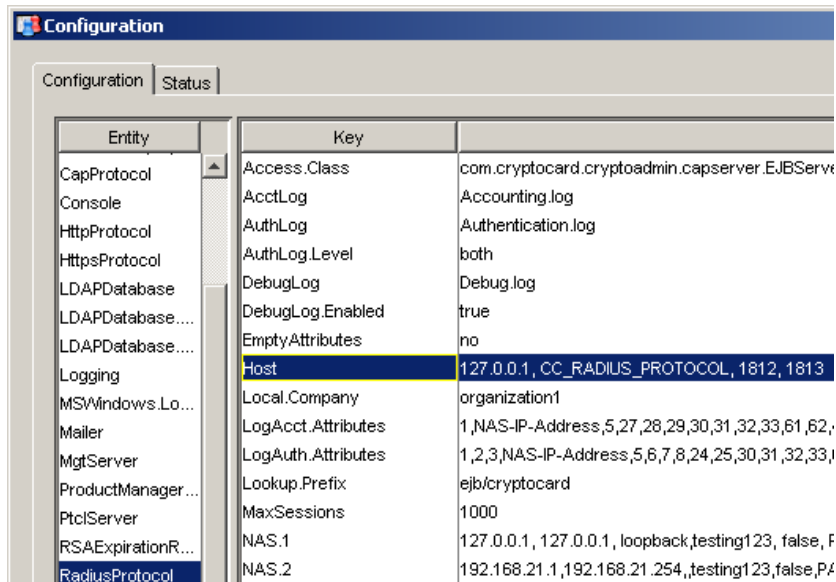
ACS crashes after incorrect passwords or blank passwords when responding to requests from NAS devices using TACACS+.

Solution: In order to avoid this issue when using Tacacs+ ACS must be set with the following setting:

"From Token Server (async tokens only)" must be checked and a value must be entered in the "Password:" field (any value would do). It is located in "TACACS+ Shell Configuration" under "CryptoCard Token Server Configuration" settings under External User Database ---> Database Configuration ---> CryptoCard Token Server.

## Changing the RADIUS Port Used by CRYPTO-Server

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.EJBServ
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,
MgtServer	LogAuth.Attributes	1,2,3,NAS-IP-Address,5,6,7,8,24,25,30,31,32,33,
ProductManager...	Lookup.Prefix	ejb/cryptocard
PtcServer	MaxSessions	1000
RSAExpirationR...	NAS.1	127.0.0.1, 127.0.0.1, loopback,testing123, false, F
RadiusProtocol	NAS.2	192.168.21.1,192.168.21.254,testing123,false,Pf

The value of the "Host" key for the RadiusProtocol entity determines what ports the CRYPTO-Server uses for RADIUS communication. By default, the ports are 1812 for authentication and 1813 for accounting.

For example, changing this value to "**127.0.0.1, CC\_RADIUS\_PROTOCOL, 1900, 1901**" will result in the CRYPTO-Server using port 1900 for RADIUS authentication, and 1901 for RADIUS accounting.

---

**NOTE: After changing the Host entry, click the "Apply" button.**

---

If you encounter a problem that cannot be solved using the tips above, contact [support@cryptocard.com](mailto: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.