



RSA SecurID Ready Implementation Guide

Last Modified September 20, 2001

1. Partner Information

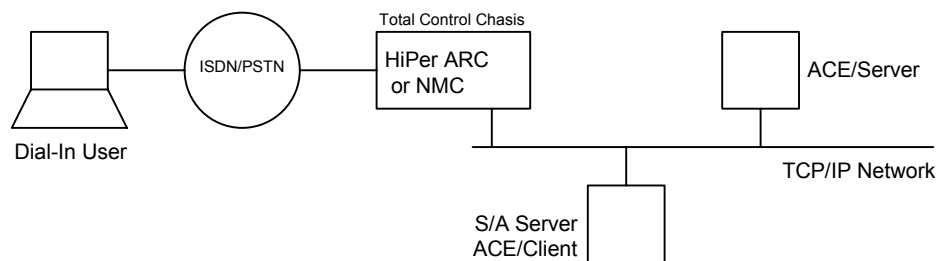
Partner Name	3Com (CommWorks)
Web Site	www.commworks.com
Product Name	Hyper Arc
Version & Platform	4.0.19
Product Description	<p>The Total Control Enterprise Network Hub, containing HiPer ARC and/or NMC cards, can be configured to authenticate dial-in users to any RADIUS server. The 3Com Security/Accounting Server (S/A) is based upon RFC2058, "Remote Authentication Dial In User Service (RADIUS)." 3Com has incorporated support for RSA Security's ACE/Client software into S/A Server.</p> <p>This implementation guide explains how to setup the 3Com Total Control system to have RSA Security's ACE/Server control dial-in user authentication.</p>
Product Category	Remote access

2. Contact Information

	<u>Sales Contact</u>	<u>Support Contact</u>
E-mail		
Phone		
Web	www.commworks.com	www.commworks.com

3. Solution Summary

Feature	Details
Authentication Methods Supported	RADIUS, TACACS+.
ACE/Agent Library Version	N/A
ACE 5 Locking	No
Replica ACE/Server Support	Master/Slave Only
Secondary RADIUS/TACACS+ Server Support	Yes
Location of Node Secret on Client	'None stored'
ACE/Server Agent Host Type	Communication server
SecurID User Specification	Designated users, all users, SecurID as default.
SecurID Protection of Administrators	Yes or No



4. Product Requirements

- *Hardware requirements*

Component Name: Hyper Arc	
3Com	HiPer ARC 4.0.19
3Com	4MEG NMC 5.3.2 [or higher] or 16 MEG NMC 5.2.2 [or higher]

- *Software requirements*

Component Name: Total Control Security/Accounting Server	
Operating System	Version (Patch-level)
HP-UX or Sun Solaris	Version 5.0.6
Windows NT	Version 5.0.7

5. Partner ACE/Agent configuration

Integration with RSA Security's ACE/Client

RSA Security provides an Application Programmer's Interface (API) to its ACE/Client software. By calling ACE/Client API functions, a developer can authenticate a user to the ACE/Server, without invoking a separate authentication dialog. In the Total Control Security/Accounting Server, 3Com includes this type of integration with RSA Security's ACE/Client.

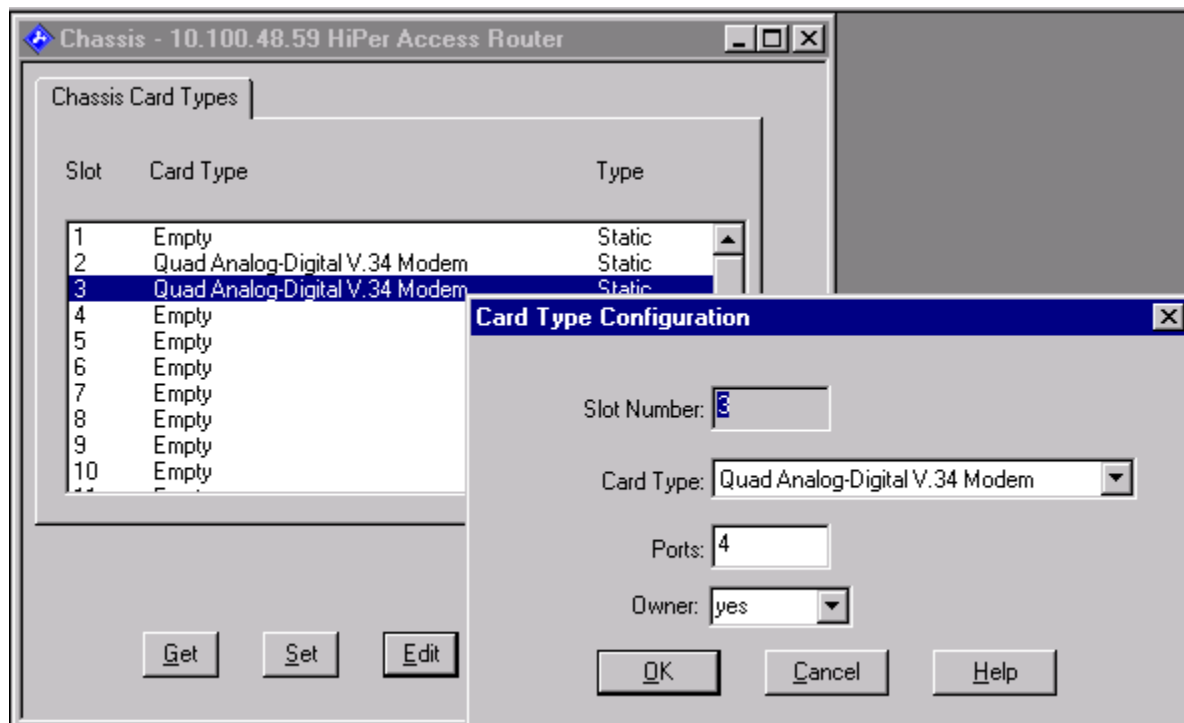
On the Windows NT platform, it is required to install the ACE/Client on the same system running S/A server. On Unix platforms, it is not required to install the ACE/Client, as S/A Unix contains ACE/Client API libraries built-in.

Configuration

HiPer ARC Card

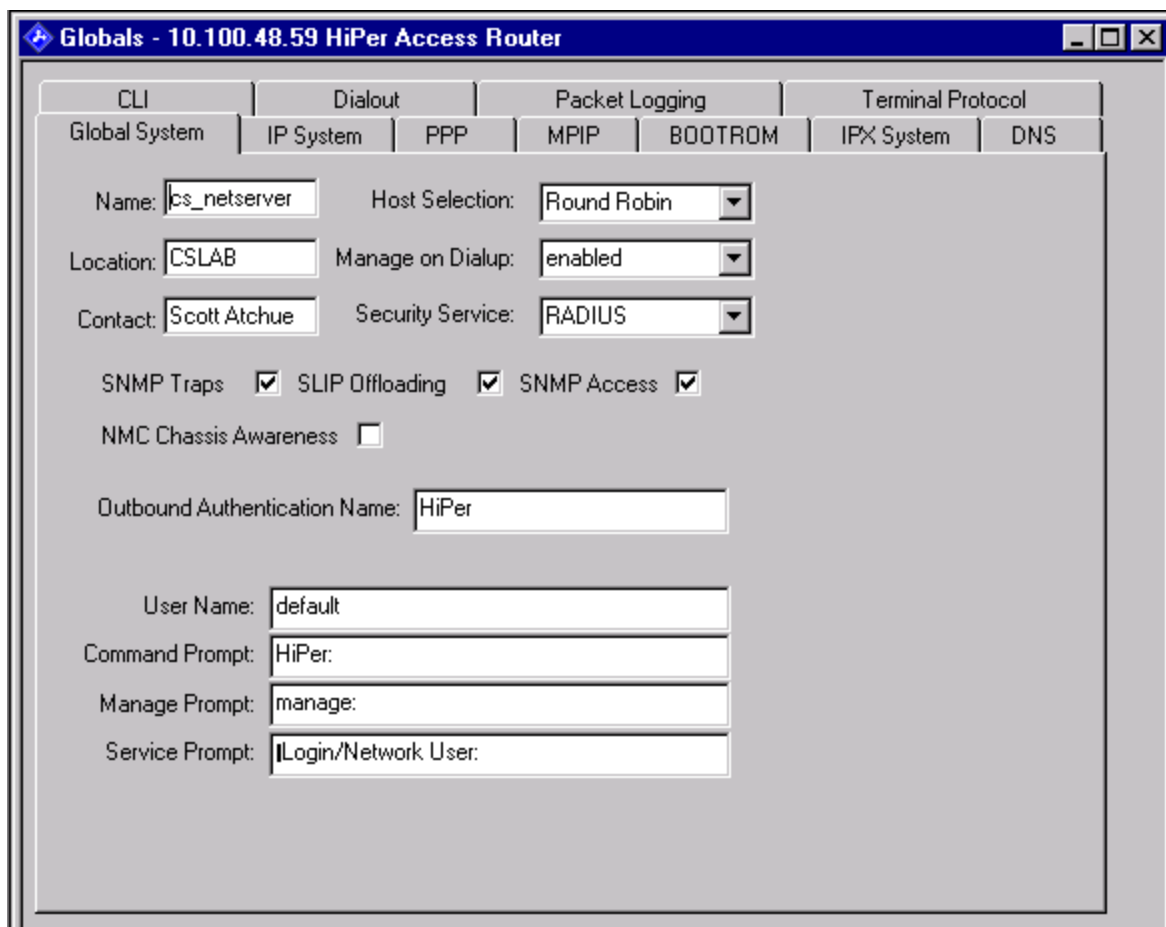
This section explains how to set up the HiPer ARC to communicate with the S/A Server. It assumes that the HiPer ARC is already configured to use the Internet Protocol (IP).

Start the HiPer Access Router Manager. Select Tables – Chassis Configuration. Highlight the modem card that you want the HyperArc to use, and select edit. Change the owner pull down box to yes.



Configure the HiPer ARC to use RADIUS authentication.

1. Go to Tables – Globals. Set the Security Service to RADIUS.



Globals - 10.100.48.59 HiPer Access Router

CLI | Dialout | Packet Logging | Terminal Protocol

Global System | IP System | PPP | MPIP | BOOTROM | IPX System | DNS

Name: Host Selection:

Location: Manage on Dialup:

Contact: Security Service:

SNMP Traps ☒ SLIP Offloading ☒ SNMP Access ☒

NMC Chassis Awareness ☐

Outbound Authentication Name:

User Name:

Command Prompt:

Manage Prompt:

Service Prompt:

2. Go to Tables - AAA.
3. Select the RADIUS TAB.
4. Enter The Primary Server IP address, the Source Port and Primary Secret of your RADIUS server.
You can also set the Alternate Server and Tertiary Server IP address, Source Port and Primary Secret for any backup RADIUS Servers you want to use.

The screenshot shows the configuration window for a HiPer Access Router at IP 10.100.48.59. The 'RADIUS' tab is selected. The 'Security' section includes fields for Primary, Alternate, and Tertiary Servers, Source, Primary, Alternate, and Tertiary Ports (all set to 1645), Timeout (30), Max Retries (10), Authentication (RoundRobin), and Attribute Style (Standard). There are buttons for Primary, Alternate, and Tertiary Secret keys. The 'Accounting' section includes IP Addresses (Primary, Alternate, First Backup, Second Backup, Alt. First Backup, Alt. Second Backup), Ports (Primary, Source, Alternate, First Backup, Second Backup, Alt. First Backup, Alt. Second Backup, all set to 1646), and Secret keys (Primary, Alternate, First Backup, Second Backup, Alt. First Backup, Alt. Second Backup). Checkboxes for 'Enable Acctg', 'Enable Interval', and 'Enable Primary Accounting' are present. Start Time is set to 'Connection' and Timeout is 60. Interval is 240.

5. Save the Configuration

NMC Card

The NMC contains no user tables of its own and must forward all authentication requests to a RADIUS server. This section explains how to set up an NMC to communicate with a S/A Server. It assumes that the NMC is already configured to use IP.

NOTE: You will need to access the NMC's console interface through the NMC's WAN port in order to execute the commands in this section.

Tell the NMC the RADIUS secret of the S/A Server.

1. From the Main Menu, enter 1 to access the **Configuration** screen.
2. From the Configuration screen, enter 7 to specify a RADIUS Security Secret Key. You can enter a key with as many as 64 characters.
3. From the Configuration screen, enter 9 to Save Configuration to Non-Volatile Memory.
4. Exit the console interface.

Tell the NMC the I.P. address of the S/A Server. This must be done using SNMP. You can use the Total Control Manager or any other SNMP application which understands Management Information Bases (MIBs).

1. Set the object `nmCHsSecuritySrvrAddr` to the IP address of the S/A Server.
2. Verify the object `nmCHsSecuritySrvrPort` is set to **1645**, the default UDP port used by the S/A Server.

Unix

Total Control Security/Accounting Server

Tell the S/A Server about each user that needs to be passed to the ACE/Client for authentication. The following line from the **users.txt** file defines a SecurID user:

```
auser = 1,upt1,upassg0,11/1/1998,,,0,,,,,,,,,,,,,
```

In this example, the “1” after the “=” tells the S/A Server that user auser should be authenticated by the ACE/Server. Refer to your S/A Server documentation for other user configurable options.

In the **radserv.cfg** file, set the following parameter to “1” to enable the ACE/Server as an authentication method:

```
ACE$Challenge_Support = 1
```

In the **clients.txt** file, tell S/A Server the IP address and the secret of the NETServer or NMC:

```
123.123.12.10 = somethingcryptic
```

ACE/Client for Unix

In order for S/A Server to communicate [via ACE/Client API function calls] with the ACE/Server Master and Slave systems, it must have available to it a copy of the ACE/Server's **sdconf.rec** file. This file is located in your <pathname>/ace/data directory on the system running the ACE/Server software.

Place the sdconf.rec file in the /var/ace directory on the system running S/A Server. If you are unable to locate the /var/ace directory, you'll need to create one. S/A Server is configured to look for the sdconf.rec in this directory only.

Windows NT

Total Control Security/Accounting Server

Using the Total Control S/A Server Manager, you will need to define users and RADIUS clients. This section assumes you have already installed this application.

Define SecurID users in the Security and Accounting Server Microsoft Access database. This is done in the **User Setup** screens:

1. In the User Name field, type the name of a user you would like to add to the database.
2. Set this user's authentication method to SecurID.

User Configuration

Find... New Delete Browse Users Done

Username: ACE

General NMC NETServer V3.x HiPer ARC/SuperStack II/NETServer 8/16 V4 NETBuilder II

Template: FRAMED-PPP Authentication: SecurID

Failed Logins: 0

Deny Access: ☐

Dial In Restrictions

Check Port Number? ☐ Port Number Name List:

Check DNIS? ☐ DNIS Restriction List:

Check ANI? ☐ ANI Restriction List:

Maximum number of concurrent Sessions: 0

Tunnel Name: Tunnel Setup Request: ☐

Hosts via DNS: Interim Accounting Interval: 0

3. Select The HiPer Arc tab and configure the method used to obtain IP addresses for Remote users.

The image shows a 'User Configuration' dialog box with a blue title bar and standard window controls. The top menu bar includes buttons for navigation (back, forward, find), 'New', 'Delete', 'Browse Users', and 'Done'. The 'Username' field is set to 'ACE'. Below this, a tabbed interface shows 'General', 'NMC', 'NETServer V3.x', 'HiPer ARC/SuperStack II/NETServer 8/16 V4' (selected), and 'NETBuilder II'. The 'Service Type' is 'Framed'. A 'Clear' button and a 'DNIS ReAuthentication' checkbox are present. A note indicates that DNIS ReAuthentication 'Indicates second-level authentication'. The 'IP Address' is set to '255.255.255.254' with a dropdown arrow. A tooltip explains: 'The IP address for the user. (select 'Assigned' or 'Negotiated' to have the NAS decide this value, or use Pool Name below)'. The 'Protocol' is 'PPP' with a dropdown arrow. A tooltip explains: 'The protocol used for the connection. (Default=PPP)'. The 'Framed MTU' field is empty. A tooltip explains: 'Maximum Transmission Unit. (For PPP, 100-1514, SLIP, 100-1006. Default=1514)'. The 'Compression' dropdown is also empty. A tooltip explains: 'Header compression used'. The 'Pool Name' is 'scottpool'. A tooltip explains: 'Use this pool name, defined on the NAS, to assign an IP address. This overrides the above IP address.' On the right side, there is a vertical stack of buttons: 'PPP', 'Timeouts', 'Callback', 'Routing', 'IPX', 'Scripts', 'Filters', 'Appletalk', and 'Misc.'

Security/Accounting Server - User Setup

Define RADIUS clients in the Security and Accounting Server Microsoft Access database. This is done in the **Server Setup** screens:

1. Select the RADIUS Clients Tab
2. In the I.P. address field, type the I.P. address of the HiPer ARC.
3. In the RADIUS port field of the RADIUS clients table, type the RADIUS PORT.
4. In the RADIUS secret field of the RADIUS clients table, type the RADIUS secret of the HiPer ARC.
5. In the Type field of the RADIUS clients table, select the 3Com Hiper, NetServer 8/16

System Settings

RESTART THE S/A SERVER TO ACTIVATE ANY CHANGES MADE HERE

Security | Accounting | **RADIUS Clients** | Passwords | Advanced Functions

	IP	Port	Secret	Type
▶	10.100.48.59	1645	*****	3Com HiPer, NETServer 8/1
	10.100.48.46	1645	*****	Generic RADIUS
	127.0.0.1	1645	*****	3Com HiPer, NETServer 8/1
	127.0.0.1	1646	*****	3Com SA Server
*		1645		Generic RADIUS

Enter the IP address, UDP port, secret, and type of every machine and server that is allowed to communicate with this server. Failing to enter approved RADIUS clients will result in security breach notifications on every message from the unlisted clients

To prevent encryption of accounting server messages, specify no secret for the accounting server.

Done

You may specify a Default User profile to be applied to all users who cannot be found in the Security and Accounting Server database. All attributes of this profile will be applied to such users, including the authentication method.

1. From the Default User pulldown menu, choose the name of an existing user to be the Default User.

System Settings

RESTART THE S/A SERVER TO ACTIVATE ANY CHANGES MADE HERE

Security | Accounting | RADIUS Clients | Passwords | Advanced Functions

RADIUS Security Service Name: Typically 'radius', this is the name from the SERVICES file of the RADIUS security service

Default Username: If not empty, this name will be the source of settings for a user that isn't in the database.

Default Menu Prompt: The default menu prompt used if no user specific menu prompt is found.

Check Dial In Restrictions? ☐ This causes users to have their ANI, DNIS, or port number validated. Specific restrictions must be entered on the user's form for this to work.

Enable Session Limiting? ☐ This enables concurrent session limiting in the server.

Maximum DNS Hosts: The maximum number of IP addresses to be used from a DNS host lookup.

Done

Security/Accounting Server - Server Setup

ACE/Client for Windows NT

The ACE/Client for Windows NT must be installed on the same system running the Windows S/A Server. The ACE/Client must be configured for Local Access Security in order for S/A Server to communicate [via ACE/Client API function calls] with the ACE/Server Master and Slave systems.

6. Certification Checklist

Date Tested: September 20, 2001

Product	Tested Version
ACE/Server	5.0
ACE/Agent	4.4
Hyper Arc	4.0.19

Test	ACE	RADIUS
1st time auth. (node secret creation)	<input type="text"/>	<input type="text" value="N/A"/>
New PIN mode:		
System-generated		
Non-PINPAD token	<input type="text"/>	<input type="text" value="P"/>
PINPAD token	<input type="text"/>	<input type="text"/>
User-defined (4-8 alphanumeric)		
Non-PINPAD token	<input type="text"/>	<input type="text" value="P"/>
Password	<input type="text"/>	<input type="text" value="P"/>
User-defined (5-7 numeric)		
Non-PINPAD token	<input type="text"/>	<input type="text" value="P"/>
PINPAD token	<input type="text"/>	<input type="text"/>
SoftID token	<input type="text"/>	<input type="text"/>
Deny 4 digit PIN	<input type="text"/>	<input type="text" value="P"/>
Deny Alphanumeric	<input type="text"/>	<input type="text" value="P"/>
User-selectable		
Non-PINPAD token	<input type="text"/>	<input type="text" value="P"/>
PINPAD token	<input type="text"/>	<input type="text"/>
PASSCODE		
16 Digit PASSCODE	<input type="text"/>	<input type="text" value="P"/>
4 Digit Password	<input type="text"/>	<input type="text" value="P"/>
Next Tokencode mode		
Non-PINPAD token	<input type="text"/>	<input type="text" value="P"/>
PINPAD token	<input type="text"/>	<input type="text"/>
Replica Servers	<input type="text"/>	<input type="text" value="N/A"/>
User Lock Test (ACE Lock Function)	<input type="text"/>	<input type="text" value="N/A"/>
No ACE/Server	<input type="text"/>	<input type="text" value="P"/>

Init

*P=Pass or Yes F=Fail N/A=Non-available function

7. Known Issues