# Configuring Support for the CiscoSecure Authentication Agent

The CiscoSecure Authentication Agent (CAA) sits on a remote SOHO site client PC or a dial-in client PC served by a host network and provides a user GUI for end users to access and manage their ISDN or dial-in connections to their host network with CiscoSecure ACS for Windows NT or CiscoSecure ACS for UNIX installed.

A network administrator can initially set up a remote (SOHO) router and deliver a custom configuration to a remote user. The remote user simply copies that configuration file to a disk and runs a Windows 95 or Windows NT setup file.

- If set up to support CAA "Single Authentication," the SOHO routing device, upon detecting interesting traffic to the NAS network, will invoke the CAA client to display user login prompts, and then using the user's inputs, set up an ISDN connection between the SOHO and the NAS network.
  - CAA client can also be configured to support user-initiated single-authentication login.
  - Synchronous token card login is supported.
- If the SOHO and NAS devices are set up for CAA "Double Authentication," the two devices carry out an initial authentication to set up a Telnet session, transparent to the SOHO end users.
  - If "Standard Double Authentication" is configured, users can right-click in the lower-right corner of their monitors to display the CAA login prompts and carry out a second authentication on themselves to access specific Internet services, such as FTP, FTP-data, and HTTP.
  - If "Automated Double Authentication" is configured, the CAA login prompt automatically displays itself when the users launch an application requiring access to the host network.
  - Both synchronous and asynchronous token card login is supported through double authentication.
- The CAA also provides a Messaging Service supporting the display of Password Aging messages sent by a CiscoSecure ACS for Windows NT server to dial-in users.

# Features and Supported Platforms

The features of CiscoSecure Authentication Agent have been successfully tested on the platforms identified in Table 1.

***Table 1 CAA Features and Tested Platforms***

| Feature | SOHO or Remote PC Platform | SOHO Router IOS Platform | NAS IOS Platform | CiscoSecure ACS Platform | Token Server (optional) |
|---|---|---|---|---|---|
| Single Authentication | • Windows 95<br>• Windows NT 4.0<br>(Requires latest version of CAA client installed) | • Supported on Cisco 760/770 SOHO routers only<br>• EIOS image 4.2 (6) | • CIOS 12.05 | • CiscoSecure ACS for Windows NT 2.3<br>• CiscoSecure ACS for UNIX 2.3.2 | • Synchronous token authentication |
| Double Authentication | • Windows 95<br>• Windows NT 4.0<br>(Requires latest version of CAA client installed) | CIOS 12.05 | • CIOS 12.05 | • CiscoSecure ACS for Windows NT 2.3<br>• CiscoSecure ACS for UNIX 2.3.2 | • Synchronous token authentication<br>• Asynchronous token authentication |
| Automated Double Authentication | • Windows 95<br>• Windows NT 4.0<br>(Requires latest version of CAA client installed) | CIOS 12.05 | • CIOS 12.05 | • CiscoSecure ACS for Windows NT 2.3<br>• CiscoSecure ACS for UNIX 2.3.2 | • Synchronous token authentication<br>• Asynchronous token authentication |
| Messaging | • Windows 95<br>• Windows NT 4.0<br>(Requires latest version of CAA client installed) | • NA<br>(Dial-in support only) | • CIOS 12.05 | • CiscoSecure ACS for Windows NT 2.3<br>(Supported for the CiscoSecure User Database only) | • NA |

# Obtaining the CiscoSecure Authentication Agent Software

To obtain the CiscoSecure Authentication Agent software:

**Step 1** From a Windows 95 or Windows NT workstation, use your web browser to access the CiscoSecure Software Images site at the following URL:

`http://www.cisco.com/cgi-bin/tablebuild.pl/ciscosecure`

**Step 2** From this site, download the CAA software package, **caaadmin.exe**, to your PC.

**Step 3** From this site, download the CAA installation instructions, **CiscoSecureAA_Install.pdf**, to your PC.

**Step 4** Using the Adobe Acrobat Reader software, follow the instructions in the **CiscoSecureAA_Install.pdf** file to unzip the **caaadmin.exe** package and install the CAA configurator on your PC.

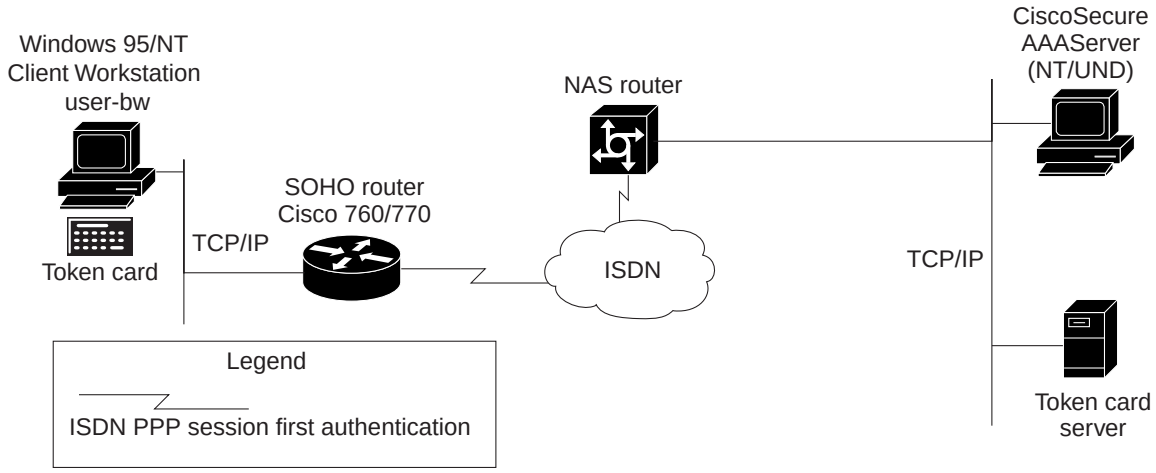
# Single Authentication Setup

Single authentication is supported only for Cisco 760/770 SOHO routers.

Single Authentication provides a simple Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) using the EIOS image 4.2 (6) or later. Single Authentication is specifically designed for use with the Cisco 770 or 760 routers using the UDP SOHO/Client Packet.

**Note** Only one SOHO-client-to-host-network connection at a time is supported through the SOHO router.

***Figure 1 Single Authentication***




The SOHO router prompts the client workstation user for login input when it detects interesting traffic.

The SOHO router then authenticates with the NAS network using the user's login input.

31525

# Single Authentication Setup Summary

To support CAA single authentication, the following configurations are required:

- Use the CAA Configurator to set up the CAA client for single authentication. See the"CAA Configuration Supporting Single Authentication" section on page 5.
- Set up CiscoSecure group profiles to support single authentication:
  - If using CiscoSecure ACS NT, see the "CiscoSecure ACS NT Configuration Supporting Single Authentication" section on page 5.
  - If using CiscoSecure ACS for UNIX, see the "CiscoSecure ACS UNIX Profile Supporting Single Authentication" section on page 6.
- Configure the SOHO router to support single authentication. See the "Cisco 760/770 SOHO Router Single Authentication Configuration" section on page 6.
- Configure the NAS router to support single authentication. See the "NAS IOS Configuration Supporting Single Authentication" section on page 10.
- If you need to troubleshoot, see the "Single Authentication Setup Tips" section on page 11.

# CAA Configuration Supporting Single Authentication

Use the CAA Configurator to set up the CAA configuration for your remote user PCs.

**Step 1** If you have not already done so, install and run the CAA Configurator as described in the *CiscoSecure Authentication Agent Quick Reference Card*.

**Step 2** While setting up your user files with the CAA Configurator, be sure to enable the following options:

- Simplified ISDN Token Authentication
- Single Authentication

**Step 3** Include the resulting *.caa configuration file on CAA installation disks or in a package and install on your remote users' PCs, again, as described in *CiscoSecure Authentication Agent Quick Reference Card.*

# CiscoSecure ACS NT Configuration Supporting Single Authentication

Configure the following network, group, and user items in the CiscoSecure ACS.

**Step 1** If you have not already done so, follow these steps in the Network Configuration window:

**Note** If the first NAS into which clients dial was set up during CiscoSecure ACS installation, this configuration should already be complete.

- If you are using network device groups (NDGs) click the name of the applicable NDG.
- Add or edit a NAS.
- Enter the name of the NAS.
- Enter the IP address of the NAS.
- Enter the shared secret key of the NAS and CiscoSecure ACS.

**Step 2** Select **TACACS+ (Cisco)** as the security control protocol.

**Step 3** Create an ISDN SOHO group.

**Step 4** Create a standard ISDN user and map the user to the ISDN SOHO group. Configure this user for token authentication if required.

**Note** CAA set up for single authentication supports synchronous token card login only. CAA in single authentication mode does not support asynchronous token card login.

### Alternative Token Card User Setup

If using a token server user database external to CiscoSecure, you can configure the CiscoSecure unkown user policy that instructs CiscoSecure to search the external database to authenticate a token server user:

1. For example, if configuring a Secure ID token card user, you would set up connectivity between the CiscoSecure ACS and the SDI database.
2. Then you would configure CiscoSecure to search the SDI database for profiles of unknown users.
3. Finally, you would create a PPP group for unknown users enabling PPP IP under the TACACS+ setting.

## CiscoSecure ACS UNIX Profile Supporting Single Authentication

If you are using CiscoSecure ACS for UNIX, no particular group membership is required. The following sample user profile supports a token card user login authentication.

```
user=sdi2 {
  profile_id=19
  set server current-failed-logins=0
  profile_cycle=5
  member=accounting
  password=sdi
  default attribute=permit
  default service=permit
  service=shell {
    set autocmd = access-profile
    default attribute = permit
    }
  service = ppp {
    protocol = lcp{
      default attribute=permit
      }
    protocol = multilink {
      default attribute=permit
      }
    protocol=ip {
      default attribute-permit
      }
    }
```

## Cisco 760/770 SOHO Router Single Authentication Configuration

EIOS 4.2(6) or later must be installed on the Cisco 760/770 SOHO router.

Add the following statements to the SET USER LAN section of the configuration file of the Cisco 760//770 device:

```
SET IP ROUTING ON  # Allows for LAN routing
SET IP ADDRESS 200.200.200.1  # Shown here with static LAN IP address
SET IP NETMASK 255.255.255.0  # Shown here with static LAN IP subnet mask
SET IP RIP UPDATE PER  # Sets the IP RIP update to periodic (other options are
                                                    Linkup/Snapshot/Demand/Off)
```

Add the following statements to the configuration file to create a host NAS profile:

```
SET USER 5300
SET PROFILE POWERUUP ACTIVATE
SET 1 NUMBER 95552000
SET 2 NUMBER 95552000
SET PPP TAS DISTRIBUTED
SET PPP TAS CLIENT 0.0.0.0
SET PPP TAS CHAPSECRET LOCAL ON
SET PPP CLIENTNAME 765
SET PPP PASSWORD CLIENT ENCRYPTED 121a0c041104
SET PPP SECRET CLENT ENCRYPTED 05080flc2243
SET PPP PASSWORD HOST ENCRYPTED 101b5a4955
SET PPP SECRET HOST ENCRYPTED 115c4a5547
SET IP ROUTING ON
SET IP ADDRESS 0.0.0.0 # WAN mask
SET IP NETMASK 0.0.0.0
SET IP ROUT DEST 0.0.0.0/0 GATEWAY 0.0.0.0 PROPAGATE OFF COST 1
```

## Sample SOHO Router Single Authentication Configuration

This section includes a Cisco 760/770 sample configuration for single authentication using unnumbered Ethernet (dynamic addressing—IP assigned by the NAS).

**Note** Required or recommended statements are in bold type, all others are system defaults that do not require changes. TAS stands for Token Access Support.

```
765> upload
CD
SET SCREENLENGTH 20
SET COUNTRYGROUP 1
SET LAN MODE ANY
SET WAN MODE ONLY
SET AGE OFF
SET MULTIDESTINATION ON
SET SWITCH NI-1            # Carrier switch type
SET 1 SPID 714666120400    # Spid for B1 provided by Carrier
SET 1 DIRECTORYNUMBER 6661204    # The local number for B1
SET 2 SPID 714666120500   # Spid for B2 provided by Carrier
SET 2 DIRECTORYNUMBER 6661205    # The local number for B2
SET AUTODETECTION OFF
SET CONFERENCE 60
SET TRANSFER 61
SET 1 DELAY 30
SET 2 DELAY 30
SET BRIDGING ON
SET LEARN ON
SET PASSTHRU OFF
SET SPEED AUTO
SET PLAN NORMAL
SET 1 AUTO ON
SET 2 AUTO ON
SET 1 NUMBER
SET 2 NUMBER
SET 1 BACKUPNUMBER
SET 2 BACKUPNUMBER
SET 1 RINGBACK
SET 2 RINGBACK
SET 1 CLIVALIDATENUMBER
```

```
SET 2 CLIVALIDATENUMBER
SET CLICALLBACK OFF
SET CLIAUTHENTICATION OFF
SET SYSTEMNAME 765
LOG CALLS TIME VERBOSE
SET UNICASTFILTER OFF
DEMAND 1 THRESHOLD 0
DEMAND 2 THRESHOLD 48
DEMAND 1 DURATION 1
DEMAND 2 DURATION 1
DEMAND 1 SOURCE LAN
DEMAND 2 SOURCE BOTH
TIMEOUT 1 THRESHOLD 0
TIMEOUT 2 THRESHOLD 48
TIMEOUT 1 DURATION 0
TIMEOUT 2 DURATION 0
TIMEOUT 1 SOURCE LAN
TIMEOUT 2 SOURCE BOTH
SET REMOTEACCESS PROTECTED
SET LOCALACCESS ON
SET CLICKSTART ON
SET LOGOUT 5
SET CALLERID OFF
SET PPP AUTHENTICATION IN PAP
SET PPP CHAP REFUSE NONE
SET PPP AUTHENTICATION OUT NONE
SET PPP TAS CLIENT 0.0.0.0  # copied here automatically when set at NAS profile
SET PPP TAS CHAP SECRET LOCAL ON  # copied here automatically when set at NAS profile
SET PPP PASSWORD CLIENT ENCRYPTED 045802150c2e  # copied here automatically when set
                                                  at NAS profile
SET PPP SECRET CLIENT ENCRYPTED 13061e010803  # copied here automatically when set
                                                at NAS profile

SET PPP CALLBACK REQUEST OFF
SET PPP CALLBACK REPLY OFF
SET PPP NEGOTIATION INTEGRITY 10
SET PPP NEGOTIATION COUNT 10
SET PPP NEGOTIATION RETRY 3000
SET PPP TERMREQ COUNT 2
SET PPP MULTILINK ON
SET COMPRESSION STAC
SET PPP BACP ON
SET PPP ADDRESS NEGOTIATION LOCAL OFF
SET IP PAT UDPTIMEOUT 5
SET IP PAT TCPTIMEOUT 30
SET CALLDURATION 0
SET SNMP CONTACT ""
SET SNMP LOCATION ""
SET SNMP TRAP COLDSTART OFF
SET SNMP TRAP WARMSTART OFF
SET SNMP TRAP LINKDOWN OFF
SET SNMP TRAP LINKUP OFF
SET SNMP TRAP AUTHENTICATIONFAIL OFF
SET DHCP OFF
SET DHCP DOMAIN
SET DHCP NETBIOS_SCOPE
SET VOICEPRIORITY INCOMING INTERFACE PHONE1 ALWAYS
SET VOICEPRIORITY OUTGOING INTERFACE PHONE1 ALWAYS
SET CALLWAITING INTERFACE PHONE1 ON
SET VOICEPRIORITY INCOMING INTERFACE PHONE2 ALWAYS
SET VOICEPRIORITY OUTGOING INTERFACE PHONE2 ALWAYS
SET CALLWAITING INTERFACE PHONE2 ON
```

```
SET CALLTIME VOICE INCOMING OFF
SET CALLTIME VOICE OUTGOING OFF
SET CALLTIME DATA INCOMING OFF
SET CALLTIME DATA OUTGOING OFF
SET USER LAN
SET IP ROUTING ON  # Allows for LAN routing
SET IP ADDRESS 200.200.200.1  # Shown here with static LAN IP address
SET IP NETMASK 255.255.255.0  # Shown here with static LAN IP subnet mask
SET IP FRAMING ETHERNET_II
SET IP PROPAGATE ON
SET IP COST 1
SET IP RIP RECEIVE V1
SET IP RIP UPDATE PER  # Sets the IP RIP update to periodic (other options are
                                        Linkup/Snapshot/Demand/Off)
SET IP RIP VERSION 1
SET USER Internal
SET IP FRAMING ETHERNET_II
SET USER Standard
SET PROFILE ID 000000000000
SET PROFILE POWERUP ACTIVATE
SET PROFILE DISCONNECT KEEP
SET IP ROUTING ON
SET IP ADDRESS 0.0.0.0
SET IP NETMASK 0.0.0.0
SET IP FRAMING NONE
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1
SET USER 5300  # first create a Host NAS profile (i.e. 5200)
SET PROFILE ID 000000000000
SET PROFILE POWERUP ACTIVATE  # Use the SEt ACtive
SET PROFILE DISCONNECT KEEP
SET BRIDGING OFF
SET 1 NUMBER 96502000  # NAS host tel. No. to be called on B1
SET 2 NUMBER 96502000  # NAS host tel. No. to be called on B2
DEMAND 2 THRESHOLD 32
DEMAND 2 DURATION 5
TIMEOUT 1 DURATION 360
TIMEOUT 2 DURATION 360
SET PPP TAS DISTRIBUTED  # Single Authen. where each PC is individually authenticated
SET PPP TAS CLIENT 0.0.0.0  # In a Distributed Mode the Cisco Authentication
                              Agent Client will send the SEt PPp TAS Client
                              command along with the IP address of the actual PC
                              with the interesting traffic. This address will
                              change based PC that is sending the interesting
                              traffic.
SET PPP TAS CHAPSECRET LOCAL ON  # CHAPSECRET must be set to On
SET PPP CLIENTNAME 765  # Helpful to identify the SOHO when calling the NAS
SET PPP PASSWORD CLIENT ENCRYPTED 121a0c041104  # PAP authen. sent to the NAS
SET PPP SECRET CLIENT ENCRYPTED 05080f1c2243  # CHAP authentication sent to the NAS
SET PPP PASSWORD HOST ENCRYPTED 101b5a4955  # PAP authentication from the NAS
SET PPP SECRET HOST ENCRYPTED 115c4a5547  # CHAP authentication from the NAS
SET IP ROUTING ON  # Allows for WAN routing
SET IP ADDRESS 0.0.0.0  # Shown here with dynamic WAN IP addressing
SET IP NETMASK 0.0.0.0  # Shown here with dynamic WAN subnet IP mask
SET IP FRAMING NONE
SET IP RIP RECEIVE V1
SET IP RIP UPDATE OFF
SET IP RIP VERSION 1
SET IP ROUTE DEST 0.0.0.0/0 GATEWAY 0.0.0.0 PROPAGATE OFF COST 1  # IP route
                                                                    to NAS
CD
LOGOUT
765>
```

# NAS IOS Configuration Supporting Single Authentication

The following sample NAS configuration supports CAA single authentication:

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 5300-51
!
boot system flash c5300-j-mz.120-5.T1.bin
aaa new-model   # use the new AAA reference model
aaa authentication login default local group tacacs+ # authenticate login (telnet) users
using tacacs+
aaa authentication ppp default local group tacacs+  # authenticate ppp (dialup) users
using tacacs+
aaa authorization exec default group tacacs+  # authorize exec services using tacacs+
aaa authorization network default local group tacacs+  # authorize network services using
tacacs+
enable password cisco
!
spe 1/0 1/7
 firmware location system:/ucode/mica_port_firmware
!
!
resource-pool disable
!
!
ip subnet-zero
no ip domain-lookup
!
virtual-profile virtual-template 1 * enable virtual-profile by virtual interface template
isdn switch-type primary-5ess
cns event-service server
!
!
controller T1 0
!
controller T1 1
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
!
controller T1 3
!
process-max-time 200
!
interface Ethernet0
 no ip address
 no ip directed-broadcast
!
interface Virtual-Template1 # needed to download the acl to the port
 ip unnumbered FastEthernet0
 no ip directed-broadcast
 ppp authentication chap # use chap to authenticate ppp connection
!
```

```
interface Serial1:23
 ip unnumbered Ethernet0
 no ip directed-broadcast
  encapsulation ppp
 no ip route-cache
 dialer-group 1 # configure an interface to belong to a specific dialing group
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no fair-queue
 ppp authentication chap # use chap to authenticate ppp connection
!
interface FastEthernet0
 ip address 10.22.2.51 255.255.255.0
 no ip directed-broadcast
!
router rip
network 10.0.0.0
!
ip classless
ip route 192.168.22.0 255.255.255.0 192.168.22.80
ip route 192.168.22.70 255.255.255.255 Serial1:23
ip route 192.168.22.80 255.255.255.255 Serial1:23
no ip http server
!
!
dialer-list 1 protocol ip permit
!
tacacs-server host 10.22.2.1
tacacs-server key cisco54321
!
line con 0
 transport input none
line 1 48
 transport preferred all
line aux 0
line vty 0 4
 exec-timeout 0 0
 password cisco
!
end
```

# Single Authentication Setup Tips

To ensure correct operation of single authentication, verify the following:

- Ping the NAS from the Cisco 760/770 device to verify that it is reachable.
- Verify that the Cisco 760/770 device is using Cisco EIOS image 4.2(6) or later.
- Verify that the user is correctly defined within the CiscoSecure database.
- Verify the ISDN connection from the SOHO router to the NAS router is operating correctly by executing a test call on the Cisco 760/770 device or a ping test on the Cisco NAS device.
- Verify that the NAS is configured correctly and the ISDN connection, carrier ISDN lines, network interface cards (NICs), and cables are connected and operating successfully.

# Double Authentication and Automated Double Authentication Setup

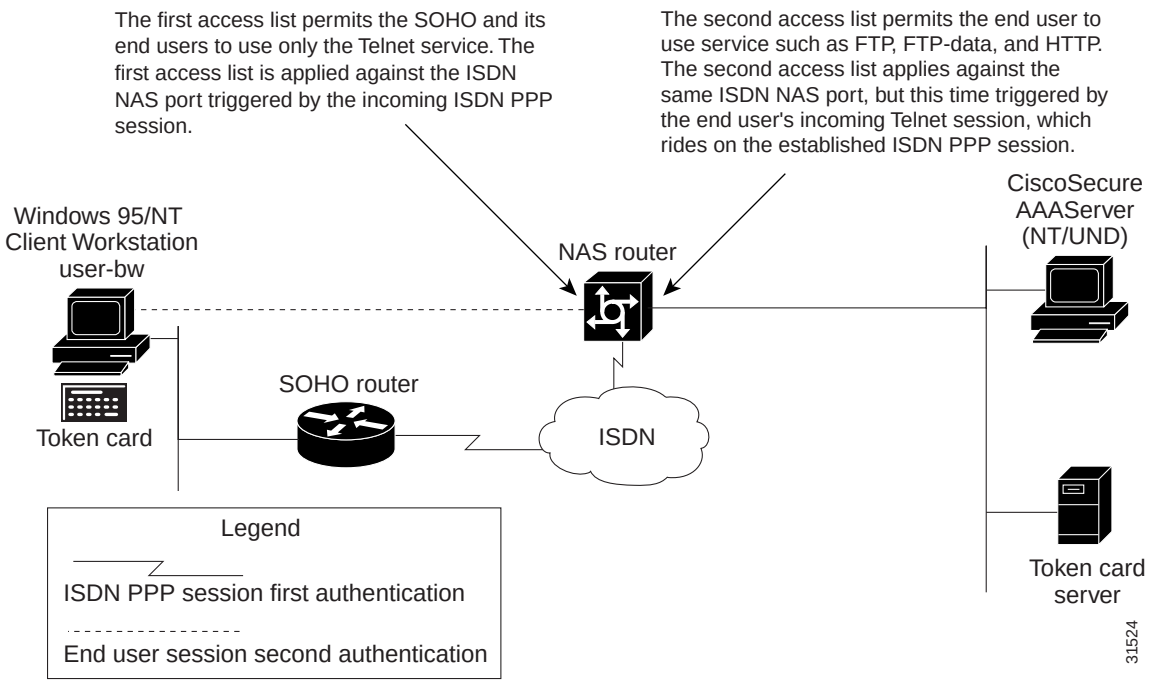
Supporting CAA double authentication requires that the CiscoSecure ACS administrator set up a first and second authentication group. The first authentication group consists of the SOHO routers, and the second authentication group consists of the SOHO end users.

Double authentication consists of a two-part authentication challenge:

- In the first authentication challenge, CHAP (or PAP) authenticates the SOHO device and allows the SOHO's ISDN connection to be established with the NAS. Then PPP negotiates with AAA to authorize the SOHO to access the NAS network. The first challenge triggers the first access control list (ACL) to be downloaded from CiscoSecure ACS and applied against the ISDN port on the NAS to which the SOHO is connected. The ACL assigns the SOHO device and its end users restricted Telnet access to the target NAS only for the purpose of carrying out the second authentication.
- The second authentication challenge proceeds over Telnet directly between the user and the NAS network. Authentication is implemented in either a standard or automated way:
  - In the standard double authentication implementation, SOHO CAA users right-click their mouse button to display the CAA client Connect option and carry out user authentication with the NAS, CiscoSecure ACS, and optional token server. CiscoSecure authorizes any additional access to the network based on each user's second authentication group profile and that user's individual profile. When authorization is complete, the users have been double-authenticated.
  - In the automated double authentication implementation, the users do not initiate the second authentication. Instead, as users access applications that require network services, the host NAS, on receiving interesting traffic, signals the CAA client to automatically display a login box for the user to fill-in. Based on the second authentication group profile and the user's individual profile, the NAS either grants or denies the user access to the requested service. When authorization is complete, the users have been double-authenticated.

Some token cards require you to implement double authentication with an ISDN connection. See your token card documentation to determine if your particular card requires this feature.

***Figure 2 Double Authentication***




# Double Authentication and Automated Double Authentication Setup Summary

To support double authentication the following configurations are required:

- Use the CAA Configurator to set up the CAA client for double authentication. See the "CAA Configuration Supporting Double Authentication and Automated Double Authentication" section on page 14.
- Set up CiscoSecure group profiles to support double authentication:
  - If using CiscoSecure ACS NT, see the "CiscoSecure ACS for Windows NT Configuration Supporting Double Authentication and Automated Double Authentication" section on page 15.
  - If using CiscoSecure ACS for UNIX, see the "CiscoSecure ACS UNIX Profiles Supporting Double Authentication and Automated Double Authentication" section on page 16.
- Configure the SOHO router to support double authentication. See the "SOHO Router Configuration Supporting CAA Double Authentication and Automated Double Authentication" section on page 18.
- Configure the NAS router to support double authentication:
  - See the "NAS Configuration Supporting CAA Double Authentication and Automated Double Authentication" section on page 20.
  - or see the "Double Authentication Setup Tips" section on page 22.
- If you need to troubleshoot, see the "Double Authentication Setup Tips" section on page 22.

# CAA Configuration Supporting Double Authentication and Automated Double Authentication

Use the CAA Configurator to set up the CAA configuration for your remote user PCs.

**Step 1** If you have not already done so, install and run the CAA Configurator as described in the *CiscoSecure Authentication Agent Quick Reference Card*.

**Step 2** While setting up your user files with the CAA Configurator, be sure to specify or enable the following options:

- Simplified ISDN Token Authentication
- Double Authentication
- Synchronous or Asynchronous token card authentication (if applicable)
- IP Address of Destination (if configuring user-initiated calls)
- Customized CAA prompt strings, if necessary in the CAA Configurator “Prompts” dialog
- In the CAA Configurator “Authentication” dialog, the appropriate prompt strings to expect from the NAS or token server and the appropriate automated response strings (if any) to pass back to NAS or token server:
  - For example, the sample Authentication dialog configuration in Table 1 supports a synchronous token login scenario where (1) the NAS sends a “Username:” or “Login:” string to prompt for username; (2) the NAS sends the “Password:” string to prompt for password; and (3) The NAS sends an Telnet session prompt, for which “%d” cancels any user response requirement; (4) the token server sends a the “Enter PASSCODE:” or “Pass Code:” string to prompt for the OTP, which the user enters from his or her token card.

    The PIN prompt is issued in a separate operation, when the user is changing the PIN ID number.

***Table 2 Authentication Settings Supporting a Synchronous Token Login***

| Authentication Data | Wait for: | Respond with: |
|---|---|---|
| Username | Username:\| Login: | |
| Token | Enter PASSCODE:\| Pass Code: | |
| Password | Password: | |
| PIN | New Pin required:\|PIN = | |
| Other | as5300> | %d |
| Other | NAS> | exit |

– The Authentication dialog configuration in Table 2 supports an asynchronous token login scenario where (1) the NAS sends a “Username” or “Login” string to prompt for username; and (2) the Token server sends a “Challenge” string, to which the user does not respond directly, but enters into his or her token card, and a “Response:” or “Enter Response:” string, to which the user responds with the response string generated by his or her token card.

***Table 3 Authentication Settings Supporting an Asynchronous Login***

| Authentication Data | Wait for: | Respond with: |
|---|---|---|
| Username | Username:\| Login: | |
| Token | Response:\| Enter Response: | |
| Password | | |
| PIN | | |
| Other | Challenge | %d |
| Other | NAS> | exit |

**Step 3** Include the resulting *.caa configuration file on CAA installation disks or in a package and install on your remote users’ PCs, as described in *CiscoSecure Authentication Agent Quick Reference Card.*

# CiscoSecure ACS for Windows NT Configuration Supporting Double Authentication and Automated Double Authentication

If using CiscoSecure ACS NT, define the access control lists (ACLs) and network access privileges of the SOHO users on CiscoSecure ACS.

## Network Configuration

Follow these steps in the Network Configuration window:

**Note** If the first NAS into which clients dial was set up during CiscoSecure ACS installation, this configuration should already be complete.

**Step 1** If you are using network device groups (NDGs), click the name of the applicable NDG.

**Step 2** Add or edit a NAS.

**Step 3** Enter the name of the NAS.

**Step 4** Enter the IP address of the NAS.

**Step 5** Enter the shared secret key of the NAS and CiscoSecure ACS.

**Step 6** Select **TACACS+ (Cisco)** as the security control protocol.

### External User Databases Configuration

Configure the database for the token card you are using. See the CiscoSecure documentation for details.

### Group Setup

Add an ISDN SOHO group. The following TACACS+ statements must be included in the double-authentication user's or group's profile. Users on the same SOHO 802.3 segment inherit the capabilities and limitations of the first session established.

**Step 1** Add a first authentication group for the Cisco SOHO device.

**Step 2** In the Custom Attributes section, assign PPP/IP to the group by adding the following statements:

```
inacl #3=permit tcp any any eq telnet
inacl #4=permit tcp any any established
```

Make sure **PPP LCP** and **ppp multilink** are checked.

**Step 3** Add the SOHO device to the first authentication group and assign it a standard CHAP password.

**Step 4** Add a second authentication group, which will include the actual users.

**Step 5** In the Custom Attributes section, assign PPP/IP to the group by adding the following statement:

```
inacl #5=permit tcp any any
```

Make sure PPP LCP, Shell (exec) and AutoCommand are checked. AutoCommand is defined for the access profile only at the per-user level.

**Step 6** Map the CHAP password user or token card user to the second authentication group.

### User Setup

Add or edit a user.

## CiscoSecure ACS UNIX Profiles Supporting Double Authentication and Automated Double Authentication

For CiscoSecure ACS for UNIX, you also set up first authentication group and second authentication group profiles, but insert the access list statements supporting CAA double authentication in the user profiles.

The following sample user profiles, used in conjunction with the sample Cisco 800 SOHO router and Cisco 3640 NAS router configurations in the two previous sections, support the double authentication process of the CAA.

## User Profile in the First Authentication Group

In the 800-1 user profile, below, a Cisco 800 SOHO router is defined as a user on the CiscoSecure ACS and mapped to the first-authen group. The initial SOHO-to-NAS-router authentication is carried out against this profile.

```
user = 800-1{
  profile_id = 21
  profile_cycle = 1
  member = first-authen
  password = chap "********"
  password = clear "********"
  service=ppp {
    default attribute=permit
    protocol=ip {
      set inacl#3="permit tcp any any eq telnet"
      set inacl#5="permit tcp any any established"
      default attribute=permit
      }
    protocol=lcp {
      default attribute=permit
      }
    protocol=multilink {
      default attribute=permit
      }
    }
  service=shell {
    default cmd=permit
    default attribute=permit
    }
  }
```

## User Profile in the Second Authentication Group

In the sdi2 user profile, below, an end user with IP permission is defined as a user on the CiscoSecure ACS for UNIX server and mapped to the second-authen group. The secondary per-service request authentications are carried out against this profile.

```
user = sdi2{
  profile_id = 19
  set server current-failed-logins = 0
  profile_cycle = 15
  member = second-authen
  password = sdi
  default attribute=permit
  default service=permit
  service=shell {
    set autocmd=access-profile
    default attribute=permit
    }
  service=ppp {
    protocol=lcp {
      default attribute=permit
      }
    protocol=multilink {
      default attribute=permit
      }
    protocol=ip {
      set inacl#8="permit ip any any"
      default attribute=permit
      }
    }
  }
```

# SOHO Router Configuration Supporting CAA Double Authentication and Automated Double Authentication

The following commands, entered in the configuration file of a Cisco 800 SOHO router, support a double authentication process with a Cisco 3640 NAS router.

**Note** In the following sample, AAA required or recommended statements are in bold type. Statements with comments (preceded by #) are recommended to be added during the initial NAS configuration.

```
!
version 12.0
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname 800-1
```

```
!
enable password cisco
username 3640-32 password 0 cisco
!
no ip subnet-zero
!
no ip domain-lookup
isdn switch-type basic-ni  #  define isdn switch type as specified by the
                              telco
!
interface Ethernet0
 ip address 192.168.22.80 255.255.255.0
 ip directed-broadcast
!
interface BRI0
 ip unnumbered Ethernet0
 no ip directed-broadcast
 encapsulation ppp
 dialer map ip 10.22.2.32 name 3640-32 98883401  #  dialer map needed to
                                                    initiate a call to the 3640
dialer load-threshold 1 either  #    configure bandwidth on demand
dialer hold-queue 50
  dialer-group 1   #   configure an interface to belong to a specific
                       dialing group
 isdn switch-type basic-ni
 isdn spid1 949888310100
 isdn spid2 949888310200
 no cdp enable
 ppp authentication chap  #   use chap to authenticate ppp connection
 ppp multilink
 hold-queue 75 in
!
ip classless
ip route 10.22.2.0 255.255.255.0 10.22.2.32
ip route 10.22.2.32 255.255.255.255 BRI0
!
dialer-list 1 protocol ip permit  #  ip traffic is permitted to initiate dial
                                     on demand connection!
line con 0
 exec-timeout 0 0
 transport input none
 stopbits 1
line vty 0 4
 exec-timeout 0 0
 password cisco
 login
!
end
```

# NAS Configuration Supporting CAA Double Authentication and Automated Double Authentication

The following commands, added to the configuration file of a Cisco 3640 NAS device, support the double authentication process.

**Note** To support automated double authentication: Insert the **ip trigger-authentication** statement in the global configuration and in the statement defining the ISDN interface you will be using for Automated Double Authentication.

**Note** AAA required or recommended statements are in bold type. Statements with comments (preceded by #) are recommended to be added during the initial NAS configuration. The term "list-name," used below in the command description, is any character string (a name) used to represent a particular list of authentication method(s) to use for a that login type.

```
version 12.05
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname c3640
!
aaa new-model # use the new AAA reference model
aaa authentication login default tacacs+ # authenticate login (telnet) users using
tacacs+
aaa authentication ppp default tacacs+ # authenticate ppp (dialup) users using tacacs+
aaa authorization exec default tacacs+ # authorize exec services using tacacs+
aaa authorization network default tacacs+ # authorize network services using tacacs+
enable password cisco
!
username c800 password 0 cisco
ip subnet-zero
no ip domain-lookup
ip trigger-authentication timeout 90 port 7500 # automated ACL trigger, time in sec's,
udp port 7500
virtual-profile virtual-template 1 # enable virtual-profile by virtual interface template
isdn switch-type basic-5ess
!
!
!
interface Ethernet0/0
ip address 10.22.2.36 255.255.255.0
no ip directed-broadcast
!
interface Serial0/0
no ip address
no ip directed-broadcast
no ip mroute-cache
shutdown
!
interface Ethernet0/1
no ip address
shutdown
no ip directed-broadcast
```

```
!
interface BRI1/0
no ip address
no ip directed-broadcast
shutdown
isdn switch-type basic-5ess
!
interface BRI1/1
 ip address 10.15.2.36 255.255.255.0
 no ip directed-broadcast
 ip trigger-authentication # automated ACL trigger
 encapsulation ppp
 no ip mroute-cache
 dialer map ip 10.15.2.40 name c800 speed 56 7372850 # dialer map needed to initiate a
                                                       call to the 800
 dialer-group 1 # configure an interface to belong to a specific dialing group
 isdn switch-type basic-5ess
 isdn spid1 0173728520
 no peer default ip address
 no cdp enable
 ppp authentication chap # use chap to authenticate ppp connection
 ppp multilink
!
interface BRI1/2
 no ip address
 no ip directed-broadcast
 shutdown
 isdn switch-type basic-5ess
!
interface BRI1/3
 no ip address
 no ip directed-broadcast
 shutdown
 isdn switch-type basic-5ess
!
interface Virtual-Template1 # needed to download the acl to the port
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 peer default ip address pool pool1 # pointer to ip pool range for dynamic ip
 ppp authentication chap # use chap to authenticate ppp connection
!
router eigrp 100
network 10.0.0.0
!
ip local pool pool1 10.14.1.101 10.14.1.110 # ip pool range for dynamic ip
no ip classless
ip route 10.0.0.0 255.0.0.0 10.15.2.40
!
!
logging buffered 4096 debugging
dialer-list 1 protocol ip permit
tacacs-server host 10.22.2.92
tacacs-server key cisco54321
!
line con 0
exec-timeout 0 0
transport input none
line aux 0
line vty 0 4
exec-timeout 0 0
password cisco
end
```

# Double Authentication Setup Tips

Consider the following:

- Double-check the access-list service types you are permitting or denying for the double authentication group or users; for example, if you define FTP service, make sure you also define FTP-data for HTTP service for web browsing.
- Several debug tools are available for Cisco IOS AAA Double Authentication, including **debug aaa authen**, **debug aaa author**, **debug aaa per-user**, **debug ppp authen**, and **debug vtem**. Automated double authentication processes can be examined using **debug ip-trigger authen**.
- Ping the NAS from the Cisco 800 device to verify connectivity.
- Verify the NAS is using Cisco IOS Release 12.05 or later.
- Verify that the user is correctly defined within the CiscoSecure database.
- Verify the ISDN connection from the SOHO to the LAN is operating correctly by doing a test call on the Cisco 800 device.
- Verify that the CAA is actively running in the background on the user workstation. If it is running, the CAA icon appears in the Active Icon tray at the lower right of the screen.
- Verify the NAS device is configured correctly and the ISDN connection, carrier ISDN lines, NICs, and cables are connected and operating correctly.
- Check the PPP negotiation on the Cisco 800 device by entering **diag PPP on**. To turn the diagnostics off, enter **diag PPP off**.
- To troubleshoot the CAA client:
  - Specify the parameters listed in Table 4 in the [debug] section of the *.caa file and restart the CAA client.

***Table 4 *.caa file [debug] section parameters***

| [Debug] Parameter and Value | Descripton[1] |
|---|---|
| Uam = 0 | no debug |
| Uam = 1 | debug level 1 |
| Uam = 2 | Packet dump |
| Telnet = 0 | No debug |
| Telnet = 1 | Log Telnet senda and receive messages between the PC and the NAS. |
| Telnet = 2 | Log Telnet negotiation options messages between the PC and the NAS. |
| Status= 0 | No debug |
| Status= 1 | LogTelnetsend/receivemessagesbetweenthePCandtheNAS. |
| Status= 2 | Log Telnet negotiation options messages between the PC and the NAS. |
| Status= 4 | Log ISDN line commands and data. |

1. Combinations of options can be added together. For example, Status=5 logs both Telnet send/receive messages and ISDN line commands and data.

To view the debug output, exit the CAA Client and open the log.txt file in the CAA Desktop Folder.

# CiscoSecure Authentication Agent Messaging Service

The CAA also provides a Messaging Service supporting the display of Password Aging messages sent by a CiscoSecure ACS for Windows NT server to dial-up users.

The CAA notifies users that their password is aging, and requires them to change the password before it has completely aged (expired). Using the CAA client, users can also change their password prior to receiving the notice.

**Note** CAA Messaging support requires that CiscoSecure ACS for Windows NT be configured to use the CiscoSecure User Database. CAA Messaging is not supported for CiscoSecure ACS for Windows NT installations using the Windows NT User Database.

## CAA Messaging Setup Summary

To support CAA messaging, the following configurations are required.

- On the Windows 95 or Windows NT platform, configure the Dia-Up Network Service. See the "Configuring Microsoft's Dial-Up Networking (DUN) User with Server Assigned IP" section on page 23.
- Use the CAA Configurator to Set up CAA for messaging. See the "CAA Configuration Supporting Messaging" section on page 26.
- Set up a group to receive the password aging messaging. See the "CiscoSecure ACS for Windows NT Sample Group Profile for Messaging Service" section on page 26.
- Set up the NAS to accommodate messaging. See the "NAS Sample Messaging Configuration" section on page 28.
- If you need to troubleshoot, see the "CAA Messaging Service Tips" section on page 31.

## Configuring Microsoft's Dial-Up Networking (DUN) User with Server Assigned IP

### Windows 95 DUN Setup

In Windows 95, set up Dial-Up Networking as follows:

**Step 1** Click the Windows 95 **Start** button and select the **Settings > Control Panel > Add/Remove Programs** options and icons.

**Step 2** Click the **Windows Setup** tab.

**Step 3** Click **Communications**.

To select only one or two of the four options available, or just to verify your choices click **Details…**

You should see four options:

- Dial-Up Networking
- Direct Cable Connection
- HyperTerminal
- Phone Dialer

**Step 4** Click the box for **Dial-Up Networking** and click **OK**.

You are returned to the Windows Setup display.

**Step 5** Click **OK** again.

You might be required to reboot.

**Step 6** Next, select the desired communications application and continue as usual. Please refer to Windows Help for any potential symptoms that might occur while running Dial-Up Networking.

**Step 7** Click **Start,** then click on **Accessories** to locate the Dial-Up Networking Group.

**Step 8** Launch the Dial-Up Networking Application.

**Step 9** Enter a name for the New Connection.

**Step 10** Enter the correct modem for the communications port you will be using and select **Next**.

**Step 11** Enter the telephone number of the remote host NAS you are calling.

**Step 12** Give the connection a name.

**Step 13** Locate and right-click the newly created Dial-Up Networking profile to view the popup menu, and select **Properties**.

**Step 14** Click **Configure** for the three advanced options:

- General Tab—To set the maximum speed (to set the baud) and speaker volume
- Connection Tab—To set the bps, data bits, parity, and stop bits
- Option Tab—To set Connection Control, Dial Control, or Status Control

**Step 15** Enter the telephone number, area code, and country code (if needed) for the remote host (such as, the ISP you are calling). You might also need a 9 or an 8 to place an outgoing call.

**Step 16** Select the Server Type.

Leave type of Dial-Up Server as the default (PPP:Windows, Windows NT 3.5, Internet).

**Step 17** Right-click on your new DUN icon. Click **Properties**.

**Step 18** Click **Configure** to:

- Leave the protocol as PPP and under the TCP/IP settings option, check Server Assigned IP address if the NAS is providing an IP address or enter a preassigned static address IP address.
- Log on to Network and Software Compression enabled.
- If using CHAP, enable **Require encrypted password**. Verify that you have CHAP defined on the NAS and ACS if using this option.

**Step 19** Select **Dial** to make the connection.

With the password aging option turned on the CiscoSecure ACS for Windows NT server, you will receive a greeting message, and a message indicating how long the password will be active and when you last logged in.

**Step 20** If your password is in the "Warning Period" or "Grace Period" you are prompted to change it. If you fail to change your password by the final date, your password will expire and will need to administratively reset.

## Windows NT DUN Setup

In Windows NT 4.0, set up messaging as follows:

**Note** Dial-Up Networking is a default application is added during your Microsoft NT workstation or server installation if RAS is added.

**Step 1** Click **Start**.

**Step 2** Click **Accessories**.

**Step 3** Click **Dial-Up Networking**.

**Step 4** Click **New**. Enter the name for your new phonebook entry.

**Step 5** Click the Server options that apply (for example, I am calling the Internet).

**Step 6** Click the modem to use.

**Step 7** Enter the telephone number, area code, and country code (if needed) for the remote host (for example, the ISP you are calling). Now you should see the message "that's it."

**Step 8** For advanced settings, click **Dial-Up Networking** again.

**Step 9** Select the connection profile you want to modify. Click **More**.

Edit entry and modem properties for the five advanced tabs:

- Basic—To change the connection name, telephone number, or modem.
- Server—Leave the protocol as TCP/IP (the default) and leave the Software Compression and PPP LCP extensions options enabled. Check the TCP/IP settings, enable the Server Assigned IP address if the NAS is providing an IP address or enter a preassigned static address IP address. Leave the server type as PPP:Windows, Windows NT 3.5, Internet (the default).
- Script—To add or change startup scripts—no changes needed.
- Security—Select the appropriate security protocol option:
  - Accept any authentication including clear text—Select this option to support both PAP and CHAP security.
  - Accept only encrypted authentication—Select this option for CHAP only.

**Note** Do not select the "Accept only MS encrypted authentication" option.

- X.25—To add or change window sizing options (modulo size).

**Step 10** Select **Dial** to make the connection.

With the password aging option turned on in the CiscoSecure ACS for Windows NT server, you receive a greeting message, and a message indicating how long the password will be active and when you last logged in.

If your password is in the “Warning Period” or “Grace Period,” you are prompted to change it. If you fail to change your password by the final date, your password will expire and must be administratively reset.

## CAA Configuration Supporting Messaging

Use the CAA Configurator to set up the CAA configuration for your remote user PCs.

**Step 1** If you have not already done so, install and run the CAA Configurator as described in the *CiscoSecure Authentication Agent Quick Reference Card*.

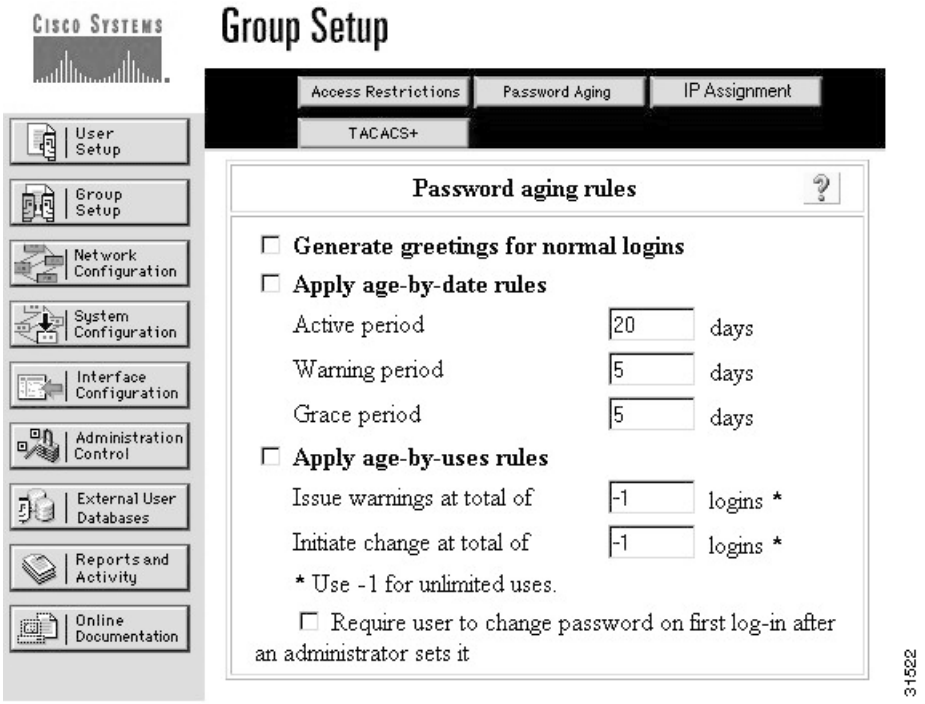
**Step 2** While setting up your user files with the CAA Configurator, be sure to specify or enable the Messaging Service option.

**Step 3** Include the resulting *.caa configuration file on CAA installation disks or in a package and install on your remote users PCs, again, as described in *CiscoSecure Authentication Agent Quick Reference Card.*

## CiscoSecure ACS for Windows NT Sample Group Profile for Messaging Service

This section describes the minimum sample CiscoSecure ACS for Windows NT profile required to support the CAA Messaging Service. Additional configurations can also be used.

*Figure 3 Group Setup for CiscoSecure ACS for Windows NT*




- Install CiscoSecure for Windows NT 2.3 or later.

**Note** Configure CiscoSecure to use the CiscoSecure User Database. Use of the Windows NT database by CiscoSecure ACS for Windows NT is not supported.

- Select the **Interface Configuration** option.
- Select the **Advanced Options**.
- Enable the **Group Level Password Aging** display option.
- Use the existing group number or touch one of the groups and rename that group “Aging Group.” This group is for the dial-up end users who will have the password aging requirements applied against their logins.
- Select the desired Password aging rules to be applied toward that group—for the initial test select “Generate greetings for normal logins.” After the Aging group user dials up and logs into the network, theuser should see the Messaging Service greeting, “Welcome” (which will be changed to a more secure greeting message).
- Create a New User, assign that user a CHAP or PAP password, and map that user to the Aging Group.
- Test the newly added user. Use Microsoft’s Dial-Up Networking to log in to the NAS. If everything is properly configured, the user should see the appropriate Aging Message as the user is authenticated by CiscoSecure. If a message is not displayed, see the “CAA Messaging Service Tips” section on page 31 for troubleshooting tips.

# NAS Sample Messaging Configuration

The following sample configuration supports messaging for an Analog Dial-Up Networking (DUN) user with Server Assigned IP (dynamic addressing—IP assigned by the NAS).

In the following example, AAA required or recommended statements are in bold type. Statements with comments (preceded by #) are recommended to be added during the initial NAS configuration. Use Cisco IOS Release 12.05 or later.

The term “list-name,” used below in the command description, is any character string (a name) used to represent a particular list of authentication method(s) to use for a that login type.

```
5200 #s ru

Building configuration...

Current configuration:

!
version 12.05
service timestamps debug datetime msec localtime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname 5200
!
aaa new-model  # Use the new AAA access control model
aaa authentication login noaaa local   # Use local as the method for
                                         Authentication to login when the
                                         list-name is "noaaa"
aaa authentication login logintac tacacs+  # Use TACACS+ as the method for
                                             Authentication to login when the
                                             list-name is "logintac"
aaa authentication ppp ppptac tacacs+   # Use TACACS+ as the method
                                          for Authentication to use PPP
                                          (serial interfaces), when the
                                          list-name is "ppptac"
aaa accounting network start-stop tacacs+ # Use the TACACS+ Accounting format
                                            for any Start or Stop packets for
                                            network access
aaa accounting connection start-stop tacacs+  # Use the TACACS+ Accounting
                                                format for any Start or Stop
                                                packets for dial-in connections
aaa accounting update newinfo  # Update the accounting logs with any "new info" for
                                 messaging service the "new info’ is a watchdog packet
                                 (Option as of 11.2.10a required for Messaging Service
                                 to work
enable password cisco
!
username bwalery password 0 cisco
modem startup-test
no ip domain-lookup
isdn switch-type primary-5ess
!
controller T1 0   # Be sure to have active and not in a shutdown state
framing esf
clock source line primary
linecode b8zs
pri-group timeslots 1-24
!
```

```
controller T1 1
shutdown   # Configure & active if the second T1/PRI will also be used
framing esf
clock source line secondary
linecode b8zs
pri-group timeslots 1-24
!
interface Loopback0
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Ethernet0
ip address 10.4.1.30 255.255.255.0
no ip route-cache
no ip mroute-cache
no mop enabled
!
interface Serial0
no ip address
no ip route-cache
no ip mroute-cache
shutdown
no fair-queue
!
interface Serial1
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Serial0:23
ip unnumbered Ethernet0
encapsulation ppp
no ip route-cache
no ip mroute-cache
no keepalive
isdn incoming-voice modem
peer default ip address pool setup_pool
dialer idle-timeout 400
dialer-group 1
no fair-queue
ppp multilink
!
interface Serial1:23   # Configure & active if the second PRI will also be used
no ip address
no ip route-cache
no ip mroute-cache
shutdown
!
interface Group-Async1  # Create to allow for and build an analog group
ip unnumbered Ethernet0   # Dynamic Addressing by the NAS
ip tcp header-compression passive  # Type of header compression for the
                                     tcp session
encapsulation ppp  # Encapsulation method for the dial-up connection
no ip route-cache
no ip mroute-cache
async default routing  # Enables SLIP and PPP interactive mode
async dynamic address  # Allows the IP address to be assigned when the
                         protocol is initiated
async mode interactive  # Returns the line to interactive mode
```

```
peer default ip address pool setup_pool  # IP pool to assign to the
                                           dial-up connection
ppp authentication pap ppptac  # Use TACACS+ as the method for
                                 Authentication to use PPP
group-range 1 48  # Range of tty ports to be used by this Async Group
!
!
interface Dialer0
no ip address
no ip route-cache
no ip mroute-cache
dialer-group 1
!
router igrp 1
redistribute connected
network 10.0.0.0
!
ip local pool pool1 10.4.1.101 10.4.1.110  # IP Pool Range for Dynamic IP
ip local pool setup_pool 10.4.1.90 10.4.1.99  # IP Pool Range for Dynamic IP
no ip classless
ip route 10.0.0.0 255.0.0.0 Ethernet0
!
tacacs-server host 10.11.1.16  # Address of CiscoSecure Server
tacacs-server timeout 20
tacacs-server key cisco  # CiscoSecure - NAS Secret Kay
!
line con 0
exec-timeout 0 0
password cisco
logging synchronous
login authentication noaaa  # Use TACACS+ as the method for Authentication to use PPP
line 1 48
exec-timeout 0 0
autoselect during-login
autoselect ppp
modem Dialin
transport preferred telnet
transport input all
line aux 0
line vty 0
exec-timeout 0 0
password cisco  # Password for remote Telnet access
login authentication logintac  # Use TACACS+ as the method for Authentication
                                 to login, use the list-name "logintac"
length 62
width 137
line vty 1 4
exec-timeout 0 0
password cisco  # Password for remote Telnet access
login authentication logintac  # Use TACACS+ as the method for Authentication
                                 to login, use the list-name "logintac"
!
scheduler interval 1000
end
5200 #
```

## CAA Messaging Service Tips

- Check the host NAS configurations, the end users' modems, and cables. Ensure that carrier lines are connected and functioning properly.
- Verify that Microsoft Dial-Up Networking has been correctly configured on the PC and that the Windows 95 or Windows NT 4.0 is working properly.
- Verify that the CAA has been properly configured for Messaging Service.
- Verify that CiscoSecure ACS for Windows NT 2.3 or higher is installed.
- Verify that your user is correctly defined within the CiscoSecure database.
- Verify that CiscoSecure ACS for Windows NT is configured to use the CiscoSecure User Database, not the Windows NT user database.
- Verify that the CAA Client is actively running in the background. You should see the client icon in the corner of the screen (the default).
- Verify that your NAS has Cisco IOS Release 12.05 or later so that the "aaa accounting update new info" statement will work with the CCMP protocol (using the watchdog packets).

# Obtaining Documentation

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

# Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

## Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on CCO to obtain additional personalized information and services. Registered users may order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.

# Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

| Language | E-mail Address |
|---|---|
| English | tac@cisco.com |
| Hanzi (Chinese) | chinese-tac@cisco.com |
| Kanji (Japanese) | japan-tac@cisco.com |
| Hangul (Korean) | korea-tac@cisco.com |
| Spanish | tac@cisco.com |
| Thai | thai-tac@cisco.com |

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

# Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate and value your comments.