

Feature Comparison: Cisco Secure ACS for Windows Compared to Cisco Secure ACS for UNIX

Introduction

Cisco Secure ACS for UNIX Version 1.0 was introduced in 1992. The original version supported the Terminal Access Controller Access Control System Plus (TACACS+) only. Cisco Secure ACS for Windows was originally released as EasyACS in 1997. This version, too, supported TACACS+ only. Cisco Secure ACS v2.0 for UNIX and the newly renamed CiscoSecure ACS 2.0 for Windows NT added support for Remote Authentication Dial-In User Service (RADIUS). Though similar in functionality, each product preceded along its own line of development with different development teams. The Enterprise Management Business Unit (EMBU) acquired support for Cisco Secure ACS for Windows as part of the enterprise management suite in 2000.

This bulletin will compare the overall feature sets of both platforms, as well as examine the advantages and disadvantages of Cisco Secure ACS for Windows and Cisco Secure ACS for UNIX and discuss issues related to migrating from the UNIX-based product to the Windows version.

Overview of Cisco Secure ACS for UNIX

Cisco Secure ACS for UNIX runs on a Sun Solaris platform. For administration, it supports both an HTML and Java graphical user interface (GUI) and a command-line interface, both of which can be used remotely. It offers most of the standard AAA functions with perhaps proxy support and Extensible Authentication Protocol (EAP) 802.1x support being the only major omissions. For storage of configuration information, Cisco Secure ACS for UNIX can support a number of databases, which include Sybase SQLAnywhere, Sybase Enterprise, and Oracle Enterprise. (A no-charge SQLAnywhere database is included with the Cisco Secure ACS for UNIX license and is limited to a 5,000-user database.) Most large-scale customers prefer to use the Oracle and Sybase Enterprise database platforms to provide replication and fault-tolerance functionality.

Overview of Cisco Secure ACS for Windows

Cisco Secure ACS for Windows runs on Windows 2000 Server, Windows Server 2003 and a Windows based appliance. Cisco Secure ACS for Windows is similar to Cisco Secure ACS for UNIX in that it uses a Web-based front end, but its feature set differs greatly. Where the Cisco Secure ACS for UNIX GUI is protocol-oriented, requiring the user to have a detailed understanding of the AAA protocols, the Cisco Secure ACS for Windows GUI attempts to reduce the user's level of AAA knowledge by providing menus with more details and easy access to help information.

Note: Cisco Secure ACS v3.1 for Windows and later cannot be installed on Windows NT 4.0 systems.

Direct Comparison

Providing a feature-by-feature comparison of the two products is difficult because their layouts differ, primarily because of the differences between the operating systems on which each product was developed. Another difficulty is that the two products were developed by separate teams, at different times, using different philosophies. Nevertheless, this bulletin attempts to provide a one-to-one comparison, given the constraints of each application's organization.

Network Access Server Configuration

Table 1 compares the two products' network-access-server configurations.

Table 1. Configuration of Network Access Servers

	Cisco Secure ACS for UNIX	Cisco Secure ACS for Windows
Network access servers		
TACACS+	Configured in either the AAA section of the standard GUI or in the.cfg file	Configured in the network configuration section
Client attributes	Host name or IP address	IP address only; multiple entries allowed; wildcards allowed; address ranges; can be sorted into network device groups (NDG) and network access filtering (NAF) from within shared profile components
	Shared secret on a per device basis	Shared secret on a per device basis or on an NDG basis
	Message catalog; file containing the messages to be displayed from the specified network access server	
	Number of username retries	
	Number of password retries	See user configuration
		Single-connect TACACS+ AAA client
		Log update and watchdog packets from this AAA client
RADIUS	Configured in the advanced configuration section	Configured in the network configuration section
Client attributes	IP address	IP address only; multiple entries allowed; wildcards allowed; address ranges
	Shared secret	Shared secret
	RADIUS vendor dictionaries:	RADIUS vendor dictionaries:
	Internet Engineering Task Force (IETF)	IETF
	Altiga	Cisco IOS® Software/Cisco PIX® Firewall
	Ascend	Cisco Aironet® Access Points (1200, 1100, 350 and 340)
	Cisco IOS Software (version-specific)	Cisco VPN 3000
		Cisco VPN 5000
		Ascend
		Nortel
	Dictionaries are configurable	Dictionaries are configurable
		Log update/watchdog packets from this AAA client
		Log RADIUS tunneling packets from this AAA client

Figures 1 and 2 show how TACACS+ network access servers are configured on Cisco Secure ACS for UNIX. Figure 3 shows the RADIUS network access server configuration window under the advanced GUI. Compare this to Cisco Secure ACS for Windows in figures 4 through 6. Figure 4 shows the different network device groups. Figure 5 shows the network access servers in the network device group. Figure 6 shows the configuration window for the individual network access server.

Figure 1. Cisco Secure ACS for UNIX Network Access Server Selection Window (TACACS+)

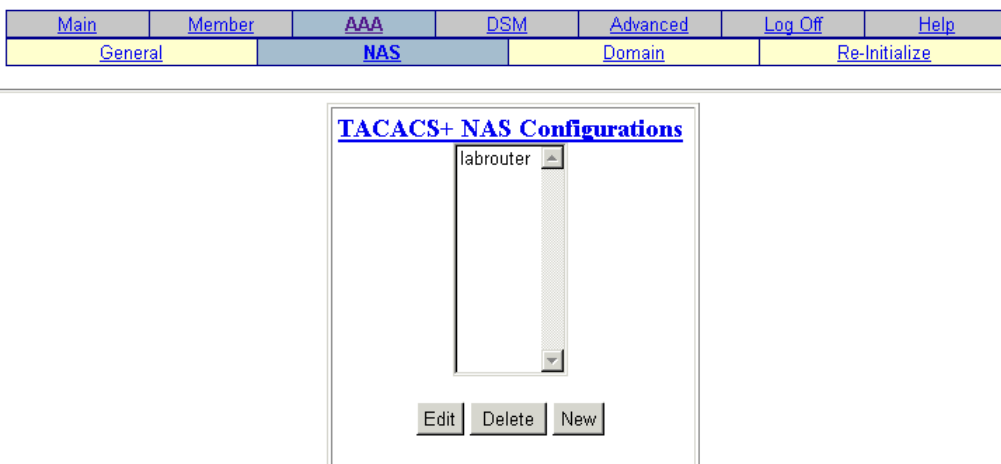


Figure 2. Cisco Secure ACS for UNIX Network Access Server Configuration Window (TACACS+)

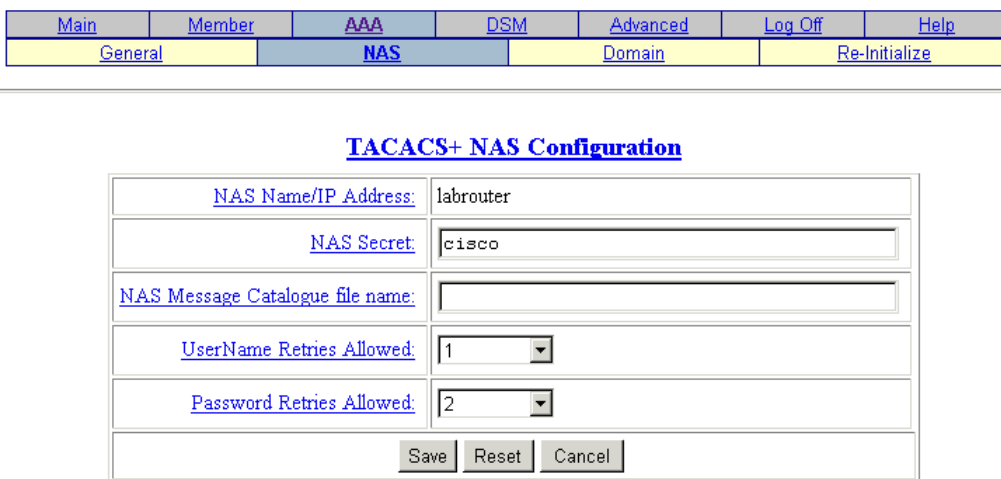


Figure 3. Cisco Secure ACS for UNIX Network Access Server Configuration Window (RADIUS)

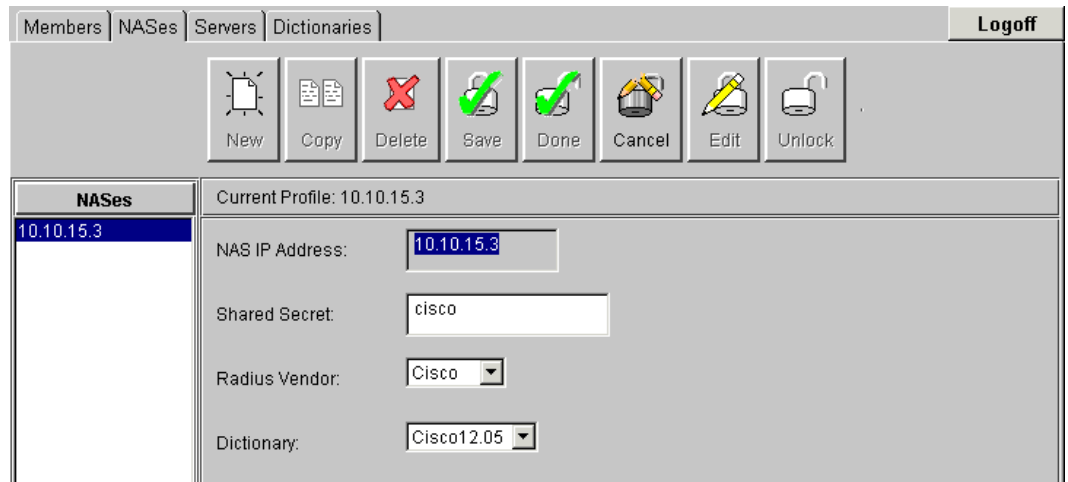


Figure 4. Cisco Secure ACS for Windows Network Device Group Selection Window

Network Configuration

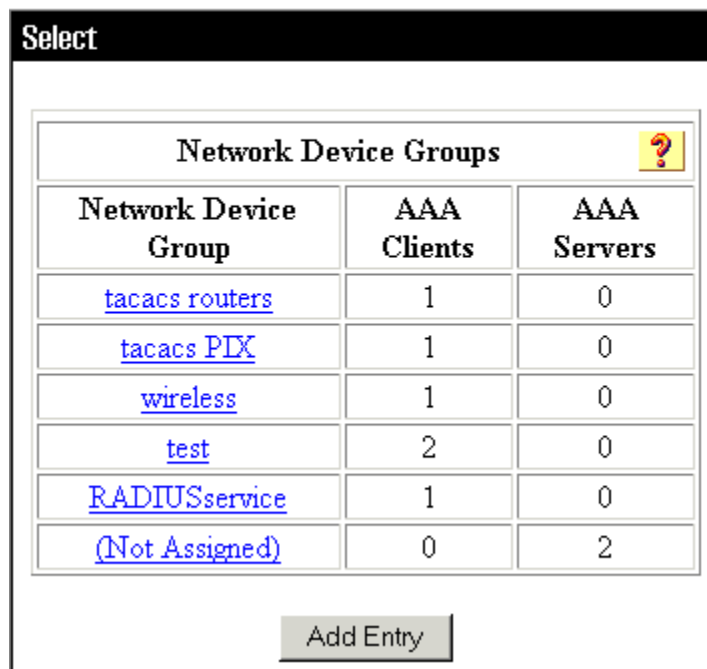


Figure 5. Cisco Secure ACS for Windows Network Access Server Selection Window

Select

tacacs routers AAA Clients		
AAA Client Hostname	AAA Client IP Address	Authenticate Using
Lab Router 1	192.168.79.229	TACACS+ (Cisco IOS)

Add Entry

tacacs routers AAA Servers		
AAA Server Name	AAA Server IP Address	AAA Server Type
None Defined		

Add Entry

Figure 6. Cisco Secure ACS for Windows Network Access Server Configuration Window

AAA Client Setup For Lab Router 1

AAA Client IP Address	<input type="text" value="192.168.79.229"/>
Key	<input type="text" value="cisco123"/>
Network Device Group	<input type="text" value="tacacs routers"/>
Authenticate Using	<input type="text" value="TACACS+ (Cisco IOS)"/>
<input checked="" type="checkbox"/> Single Connect TACACS+ AAA Client (Record stop in accounting on failure).	
<input type="checkbox"/> Log Update/Watchdog Packets from this AAA Client	
<input type="checkbox"/> Log RADIUS Tunneling Packets from this AAA Client	

User and Group Administration

Table 2 compares how user and group administration differs between the two products.

Table 2. User and Group Administration

	Cisco Secure ACS for UNIX	Cisco Secure ACS for Windows
Members (users and groups)		
Groups	Added via advanced GUI or by CLI	Added via GUI or by csutils
Users	Added via general GUI, advanced GUI, or by CLI	Added via GUI or by csutils
User vs. administrators	No distinction	Administrator configurations are performed and stored in a separate section
Non-protocol		
Passwords	User or group attribute	User attribute only
	Different passwords for different types	Different passwords for PAP vs. CHAP, Microsoft CHAP, ARAP
Type	AppleTalk Remote Access Protocol (ARAP)	Windows 2000/NT PAP
	Challenge Handshake Authentication Protocol (CHAP)	Windows 2000/NT CHAP
	Clear	RSA PAP
	Crypto	External Open Database Connectivity (ODBC) PAP
	DES	External ODBC CHAP
	Enigma	External ODBC MS-CHAP
	File	Generic Lightweight Directory Access Protocol (LDAP) PAP
	Outbound PAP	Generic Tokencard RADIUS
	Password Authentication Protocol (PAP)	
	SDI	
	Skey	
	System	
No password		
Activation control	Manually or by start date	Manually
Deactivation control	Number of failed attempts at user configuration, group configuration, or global configuration	Number of failed attempts at user configuration only
	Date exceeded	Date exceeded
TACACS+ reply/check attributes	Both group and user level	Both group and user level
	Limited configuration at the standard GUI level; full configuration at the advanced GUI level	Fully configurable at either the group or user level; the TACACS+ attributes to be configured are selectable
	All TACACS+ attributes are configurable either from group or user	The following TACACS+ passwords can be configured only at the user level:
		TACACS+ Enable Control
		TACACS+ Enable Password
	TACACS+ Outbound Password	
RADIUS reply/check attributes	Both group and user level	Both group and user level
	Only configurable at the advanced GUI level	Fully configurable at either the group or user level; the RADIUS attributes to be configured are selectable
		Microsoft attributes
Attribute configuration	Attributes are added via a series or progressive pull-down windows and value-entry boxes	Attributes are labeled and available; selection is made by check boxes, pull-down menus, or value-entry boxes

The two products differ significantly in how each supports user, group, administrator, and unknown-user configurations.

Users

Both products allow only a single entry of a username. In Cisco Secure ACS for UNIX, the administrator may configure TACACS+ either through member administration (Figure 7) or by using the advanced GUI (Figure 8). For RADIUS configuration, Cisco Secure ACS for UNIX is limited to the advanced GUI. By contrast, Cisco Secure ACS for Windows does all configurations for a single user in one window (Figure 9).

Figure 7. Cisco Secure ACS for UNIX User Configuration Window (GUI)

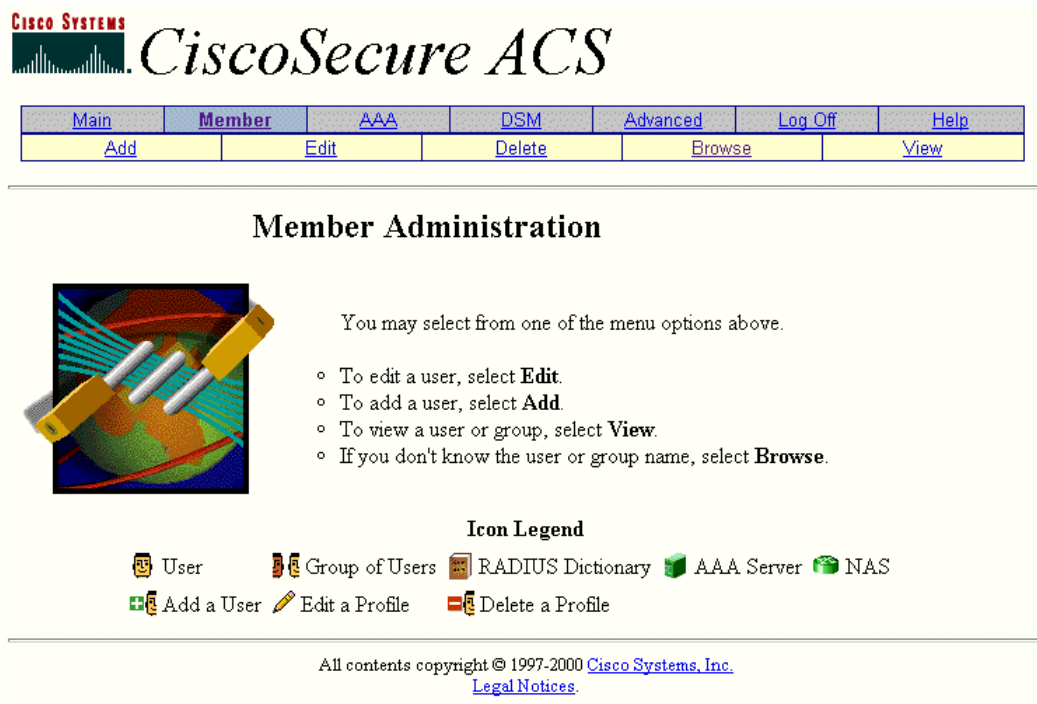
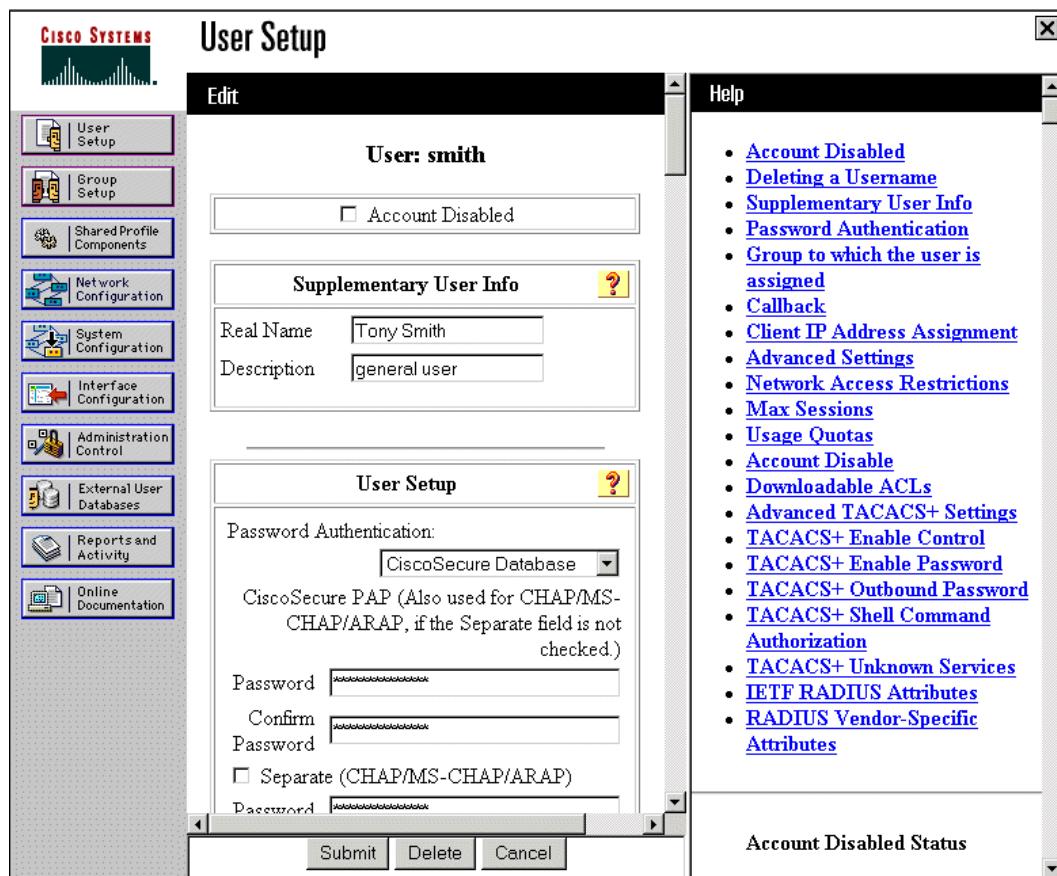


Figure 8. Cisco Secure ACS for UNIX User Configuration Window (Advanced GUI)



Figure 9. Cisco Secure ACS for Windows User Configuration Window

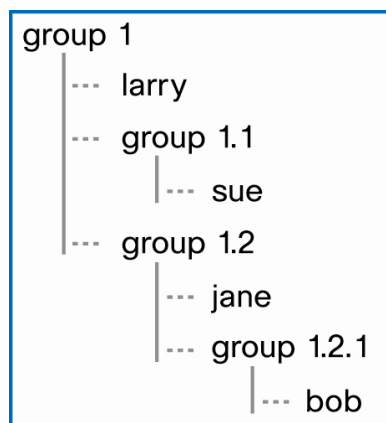


Another difference is that in Cisco Secure ACS for UNIX, the administrator first selects the group that the user will be in and then adds the user. In Cisco Secure ACS for Windows, the administrator adds the user and then selects the group from within the user configuration.

Groups

Cisco Secure ACS for UNIX supports group nesting and group inheritance. Figure 10 provides an example:

Figure 10. Group Nesting in Cisco Secure ACS for UNIX



In this example, everyone is in group 1. Each user will receive all group 1 attributes. The user larry belongs only to group 1 and is limited to those attributes unless an attribute found in the user larry configuration is the same type as in group 1, in which case the user larry configuration overrides group 1. The user sue is a member of group 1.1. Group 1.1 is a member of group 1 and will inherit the group 1 attributes. As in the user larry case, any attributes in group 1.1 that are the same type as in group 1 will override the super group configuration. This applies to all users and groups. Therefore, the user bob, a member of group 1.2.1, inherits group 1, group 1.2, and group 1.2.1 attributes, unless specific lower level attributes override the upper level attributes.

Cisco Secure ACS for UNIX is not limited to the number of groups that can be configured except as specified by the database. Cisco Secure ACS for UNIX includes SQLAnywhere as the default database. SQLAnywhere is limited to a combined number of 5000 users, groups, and network access servers.

Cisco Secure ACS for Windows does not support group nesting. Cisco Secure ACS for Windows also uses SQLAnywhere as the internal database, which does not have the same limitations as it does in Cisco Secure ACS for UNIX. Cisco Secure ACS for Windows has 500 user groups. This number is not configurable.

Administrators

Cisco Secure ACS for UNIX and Cisco Secure ACS for Windows differ greatly in the configuration of ACS administrators.

With Cisco Secure ACS for UNIX, administrators and users are configured by the same method. In Figure 11, there is a group called administrator and there is a user, superuser. Superuser can be configured for network access, as well as for administrative functions.

ACS administrators are configured in a separate location in Cisco Secure ACS for Windows (Figure 15). If network access is required for an administrator, the administrator requires a separate configuration for TACACS and RADIUS.

Migration issue: Cisco Secure ACS for Windows uses a separate configuration for ACS administrators. Cisco Secure ACS for UNIX uses the same user area as network users. This may cause problems for migrations.

Figure 11. Superuser in Advanced GUI

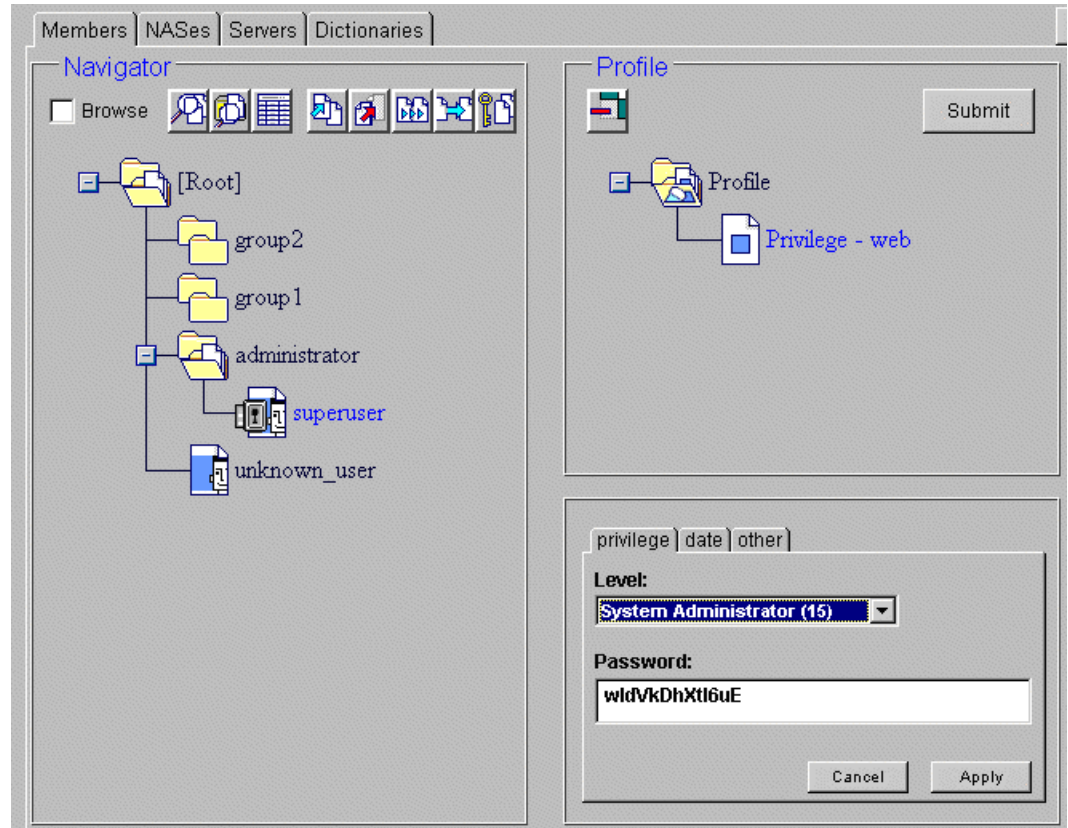


Figure 12. Adding an Administrator in Cisco Secure ACS for UNIX

Main	Member	AAA	
Add		Edit	

Add a User

[Group:](#) [Browse...](#)

[User Name:](#)

[Password:](#)

[Confirm:](#)

[Web Privilege:](#) ▼

[CHAP](#)
 [Clear](#)
 [PAP](#)

Figure 13. Cisco Secure ACS for UNIX Web Privilege Selection Pull-Down Menu

[Web Privilege:](#) ▼

[Password File:](#)

Figure 14. GrpLd1 in the Cisco Secure ACS for UNIX Advanced GUI

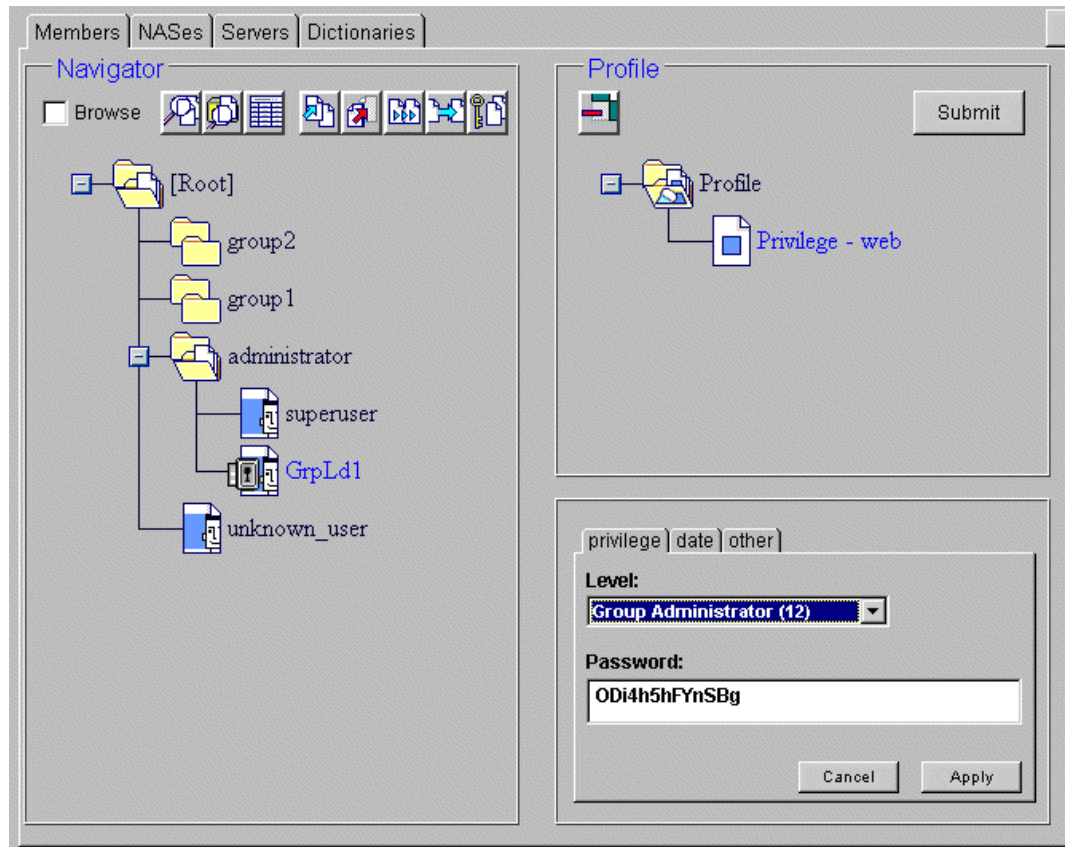


Figure 15. Cisco Secure ACS for Windows Administrator Configuration Window



Unknown User Configuration

To allow instant integration with an existing authentication system, Cisco Secure ACS for UNIX has an unknown_user profile. Cisco Secure ACS for Windows uses this profile if the system fails to find the user in the database. This profile can be set up so that its password type is one of the external authentication databases, such as SDI or UNIX. This allows Cisco Secure ACS for UNIX just to manage the authorization and accounting for the user. For example, if an unknown_user profile with password type set to system, Cisco Secure for UNIX can authenticate any unknown user with a valid UNIX username and password. This user profile is created by default and is configured in the same manner as a conventional user.

Figure 16 shows the default configuration in the Cisco Secure ACS for UNIX GUI, and Figure 17 shows it in the advanced GUI. Note that the unknown_user is not associated to a group by default. Cisco Secure ACS for UNIX does not attempt to remember an unknown user after authentication. As a result, there is no duplication occurs between the external database. Thus when a user is removed from the external authenticator, he or she will no longer be able to log in. As a result, Cisco Secure ACS for UNIX cannot provide dynamic group placement, as does Cisco Secure ACS for Windows.

Figure 16. Unknown_user in the Cisco Secure ACS for UNIX User Configuration Window

Main	Member	AAA	DSM	Advanced
Add	Edit		Delete	

Edit a User

[Group:](#) [Browse...](#)

[User Name:](#) unknown_user

[Password:](#)

[Confirm:](#)

[Web Privilege:](#)

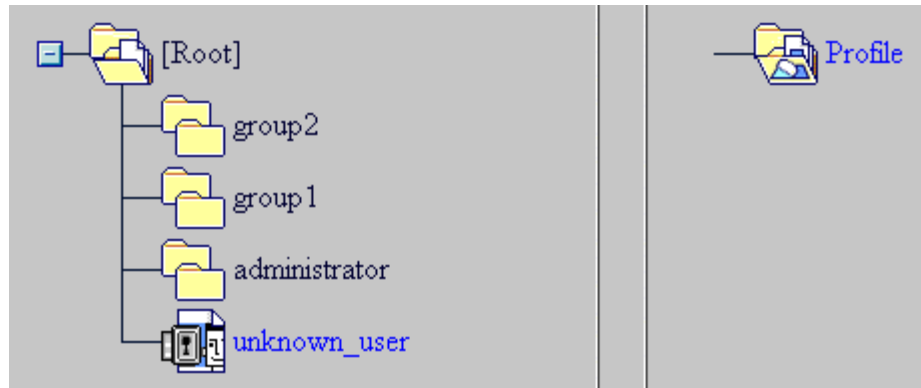
[Password File:](#)

[ARAP](#)
 [CHAP](#)
 [Clear](#)
 [DES](#)
 [No Password](#)
 [Outbound PAP](#)
 [PAP](#)

Passwords below require additional configuration:

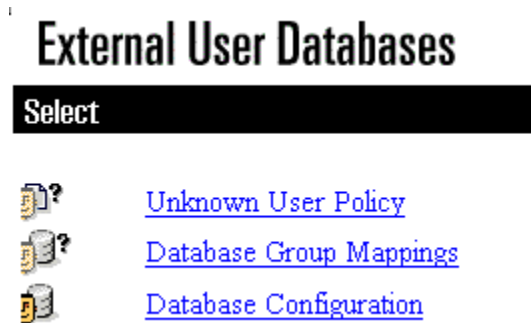
[Crypto](#)
 [Enigma](#)
 [SDI](#)
 [SKey](#)
 [System](#)

Figure 17. Unknown_user in the Cisco Secure ACS for UNIX Advanced Configuration Window



Cisco Secure ACS for Windows also understands the concept of the unknown user. The application differs from Cisco Secure ACS for UNIX in that the unknown user is not configured as a conventional user. In Cisco Secure ACS for Windows, the unknown user is configured in the external databases section (Figure 18) because external database authentication is required to verify an unknown user. On receipt of an authentication request where the user is currently unknown, Cisco Secure ACS for Windows can hunt for the user in a set of configured third-party authenticators. Cisco Secure ACS for Windows automatically creates a dynamic entry for a successfully authenticated unknown user. Future authentications for that user are directed immediately to the correct authenticator. The user's group membership is then either determined based on group membership in the external authenticator or a simple static mapping for a particular type of authenticator (SDI, Axent, etc.). The resulting group then provides all of the user's initial authorization information.

Figure 18. Cisco Secure ACS for Windows External Databases



Migration issue: Cisco Secure ACS for Windows does not have the concept of a special user record for handling an unknown user. It defines a mapping between an external database user/group membership and a Cisco Secure ACS for Windows group. Therefore, all authorization information needs to reside at the group level, as opposed to Cisco Secure ACS for UNIX, where it can reside at the user level (`unknown_user`). To migrate a Cisco Secure UNIX unknown user who has authorization information defined at the user level, a Cisco Secure ACS for Windows user group must be configured that contains the full authorization information.

It is possible in Cisco Secure ACS for UNIX to have an internal password configured for the unknown user. Cisco Secure ACS for Windows does not support this configuration. Cisco Secure ACS for Windows only supports unknown user policies with external user databases.

It is not possible to support unknown-user behavior for password type File, because this is a Cisco Secure ACS for UNIX specific feature..

Additional Profile Differences

Attribute Fields

In Cisco Secure ACS for Windows, the administrator selects which attribute fields will be visible for group and user profiles. These attribute fields are then applied to all groups and users (Figure 19), whether or not the field will be applied to a particular group or user. However, this does prevent the administrator from having to "look around" to find the attributes that require configuration.

In Cisco Secure ACS for UNIX, attribute fields are selected as required from menus (Figure 20). The administrator must know which fields are available because no list of available fields or their locations exists.

Migration issue: As long as the profiles match between Cisco Secure ACS for UNIX and Cisco Secure ACS for Windows, there should be no difficulty. However, such things as TACACS+ command filtering might be difficult to translate from Cisco Secure ACS for UNIX to Cisco Secure ACS for Windows, because of the differing structure of databases. This will require manual redesign and configuration of the command filters in ACS for Windows.

Figure 19. Cisco Secure ACS for Windows Interface Configuration Window

Interface Configuration

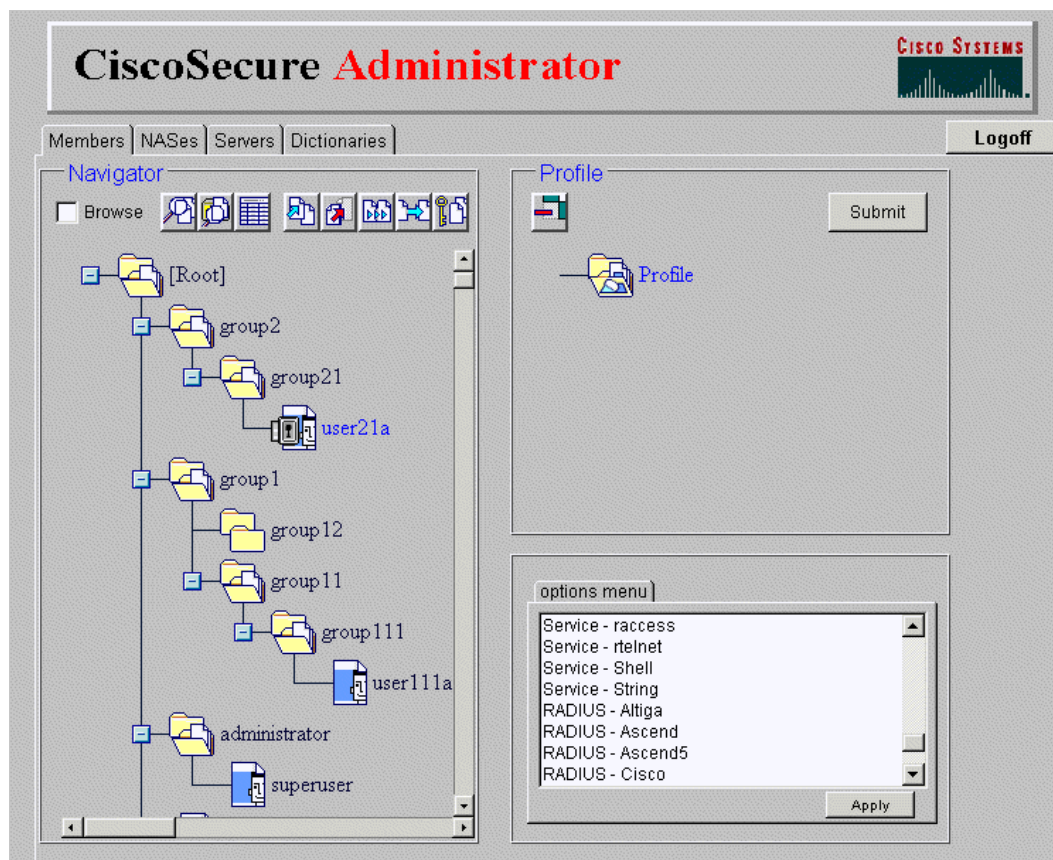
RADIUS (IETF)

User Group

- [006] Service-Type
- [007] Framed-Protocol
- [009] Framed-IP-Netmask
- [010] Framed-Routing
- [011] Filter-Id
- [012] Framed-MTU
- [013] Framed-Compression
- [014] Login-IP-Host
- [015] Login-Service
- [016] Login-TCP-Port
- [018] Reply-Message
- [020] Callback-Id
- [022] Framed-Route
- [023] Framed-IPX-Network
- [024] State
- [025] Class
- [027] Session-Timeout
- [028] Idle-Timeout

Submit Cancel

Figure 20. Cisco Secure ACS for UNIX Attributes in the Options Menu



Profile Duplication

In Cisco Secure ACS for UNIX, the administrator can copy the attributes from one profile to another. Cisco Secure ACS for Windows does not allow this procedure.

Passwords

In Cisco Secure ACS for UNIX, different passwords can be set for each of the available password types. Additionally, passwords can be set at the group level. In Cisco Secure ACS for Windows, passwords can be set only at the user configuration; the application supports different passwords only for PAP (clear text) and for CHAP, MS-CHAP, and ARAP (hashed).

In Cisco Secure ACS for UNIX, at least one password type must be defined for a user. If multiple password types are defined, then the appropriate one will be selected based on the nature of the authentication request. Associated with each password is an optional date range. This date range defines the period when the password is valid. Not to be confused with time-of-day access, this feature defines a date range (day resolution) when the password is valid. With the ability to define multiple passwords for a user or group Cisco Secure ACS for UNIX deploys the following mechanism to determine which defined password type to use for authentication (Table 3). This processing depends on the AAA protocol in use and the contents of the request packet.

Table 3. Password Mechanism for Cisco Secure ACS for UNIX

Type	Value	Description
ARAP	✓	Default password used when the user is using ARAP authentication
CHAP	✓	Default password used when the user is using CHAP authentication
Clear	✓	Default password used for clear text authentication

Crypto	✗	One-time password (OTP), CRYPTOCard token
DES	✓	DES-encrypted password (password is stored in DES-encrypted form)
Enigma	✗	OTP, Enigma
File	✗	Look for the password in a given file (file format is standard UNIX password file)
Outbound PAP	✓	Used for TACACS+ SendAuth authentication
PAP	✓	Default password used for PAP authentication
SDI	✗	OTP, SDI
Skey	✗	OTP Bellcore
System	✗	UNIX password file (can only be used for plain-text or PAP authentication)
No Password	–	No password is required for authentication (useful for voice over IP)

Protocol	Authentication Request	Password Type Precedence
RADIUS	Password in attribute 2	OTP , file, system, PAP
RADIUS	Password in attribute 3	CHAP
RADIUS	Password in attribute 181	ARAP
TACACS+	Password type PAP	OTP, PAP, system
TACACS+	Password type CHAP	OTP, CHAP
TACACS+	Password type ARAP	ARAP
TACACS+	Password type ASCII	OTP, clear, system

Note: Cisco Secure ACS for Windows stops checking passwords after a successful authentication has occurred.

Cisco Secure ACS for Windows can be configured to use privately defined passwords or can be integrated with an existing authentication service. The administrator can define up to two private passwords for each user. The first password is used for all plaintext authentications. The second password is used for CHAP, MS-CHAP, and ARAP authentications. If a second password is not defined, then the first password is used for all authentications. When an external authenticator is selected as the primary password, Cisco Secure ACS for Windows will use the secondary password only when the external authenticator cannot perform CHAP, MS-CHAP, or ARAP authentication.

Table 4 indicates the current set of external authenticators.

Table 4. External Authenticators for Cisco Secure ACS for Windows

Authenticator	PAP	CHAP	MS-CHAP	ARAP
Windows 2000/NT	✓	✗	✓	✗
Novell Netware	✓	✗	✗	✗
Security Dynamics token server	✓	✗	✗	✗
External ODBC database	✓	✓	✓	✗
Generic LDAP	✓	✗	✗	✗
Safe Word token server	✓	✗	✗	✗
CRYPTOCard token server	✓	✗	✗	✗
MCIS	✓	✗	✗	✗
Axent token server	✓	✗	✗	✗

Command Authorization

You can use TACACS+ to provide command filtering for the administration of Cisco routers, switches, and other devices that support this feature. Cisco Secure ACS for UNIX supports this feature by allowing you to define a set of commands, which are either permitted or denied, along with a list of permitted-and-denied arguments for each command. You define these command authorizations inside the shell service. You append a command in the same way as normal service authorization attributes. Each command has the properties described in Table 5.

Table 5. Command Filtering Properties with Cisco Secure ACS for UNIX

Property	Description
Name	The name of the command being defined (in the case of Cisco IOS Software, it could be copy, interface, ip, etc.)
Time	A time period in which the command as a whole is valid
Default attribute	If set to permit, then any unmatched command lines will be permitted; otherwise they are denied
Command arguments	A set of command lines to be compared

You configure command filtering in Cisco Secure ACS for UNIX through the advanced section. You configure command filters within a "Service-shell" profile in either a group or a user profile (Figure 21). Cisco Secure ACS for UNIX allows for a default setting for command authorization of commands not configured for a particular group or user (Figure 22). You need to use several menus to configure a specific command (Figure 23). These menus cover the items found in the previous table. In the example shown, the show command is being configured for authorization filtering. The default setting is permit, and the permission for the users argument (show users) is deny. When the command authorization configuration is complete, it will show up under the service-shell profile (Figure 24). You may configure multiple arguments for a given command (Figure 25).

Migration issue: Cisco Secure ACS for UNIX allows a time option to be included with specific command authorization configurations that will control when a command is permitted or denied. The default setting is always. Cisco Secure ACS for Windows does not include the time option for command authorization.

Figure 21. Configuring Command Filters in Cisco Secure ACS for UNIX

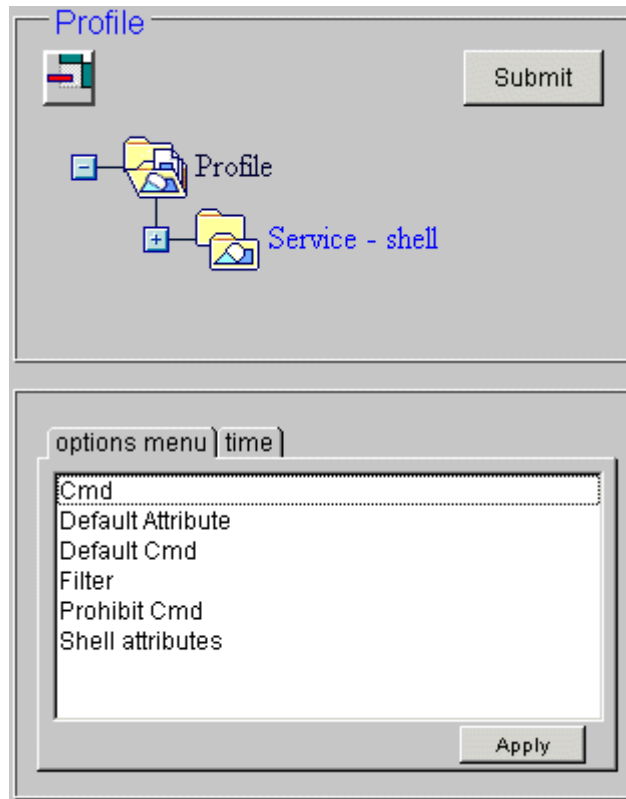


Figure 22. Default Command Attribute in Cisco Secure ACS for UNIX

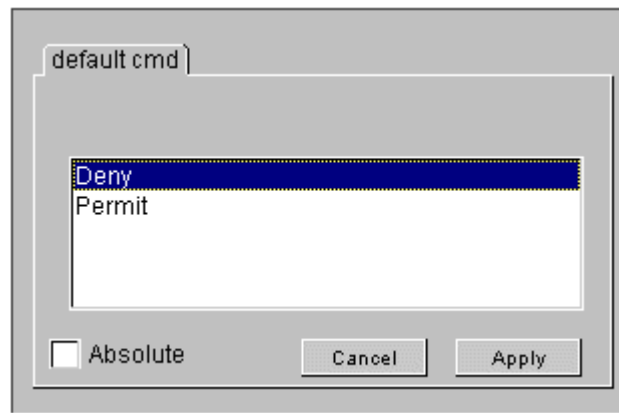


Figure 23. Command Authorization Configuration Menus for Cisco Secure ACS for UNIX

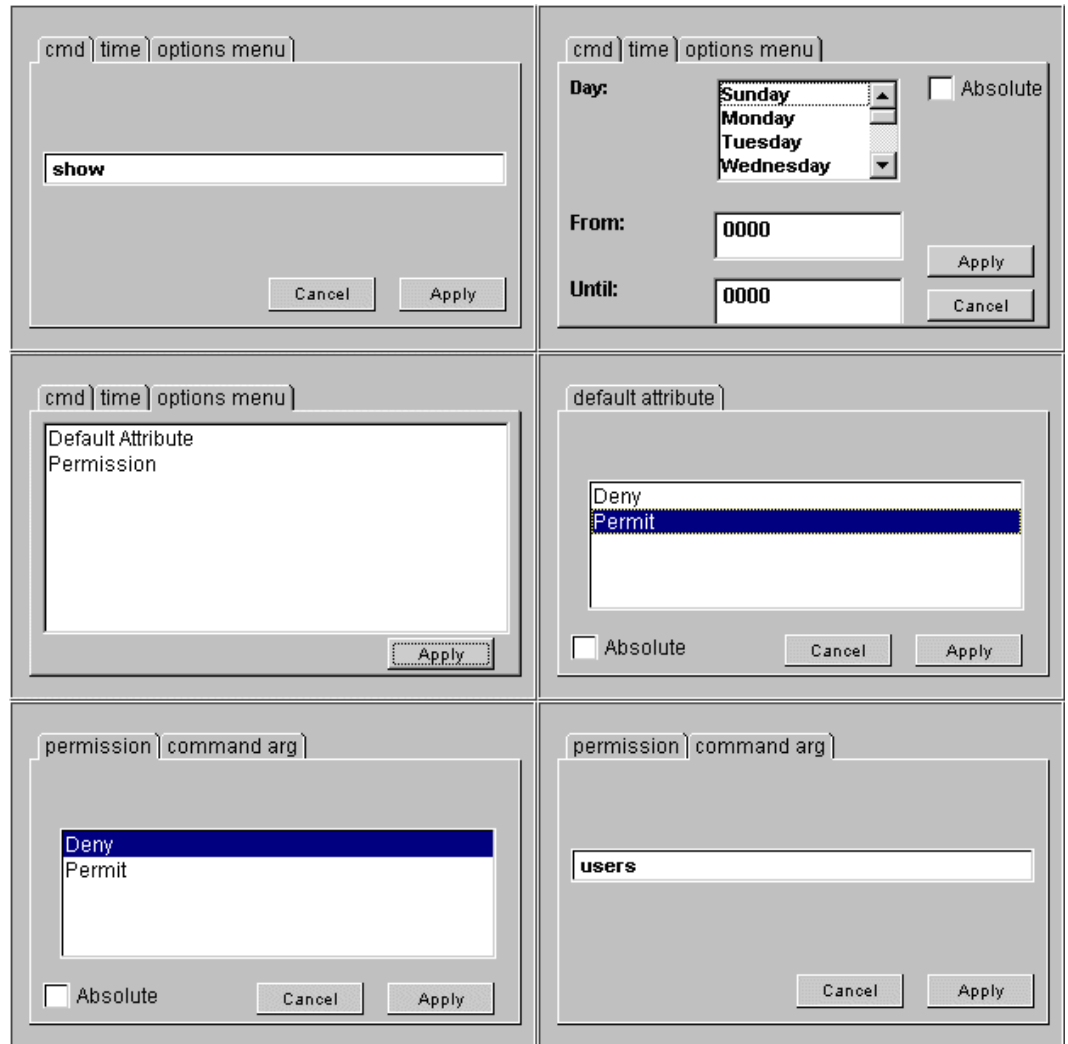


Figure 24. Final Command Authorization Configuration Example in Cisco Secure ACS for UNIX

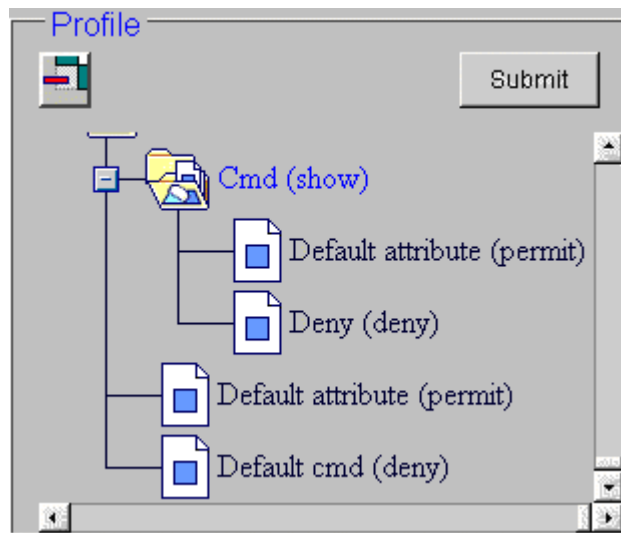
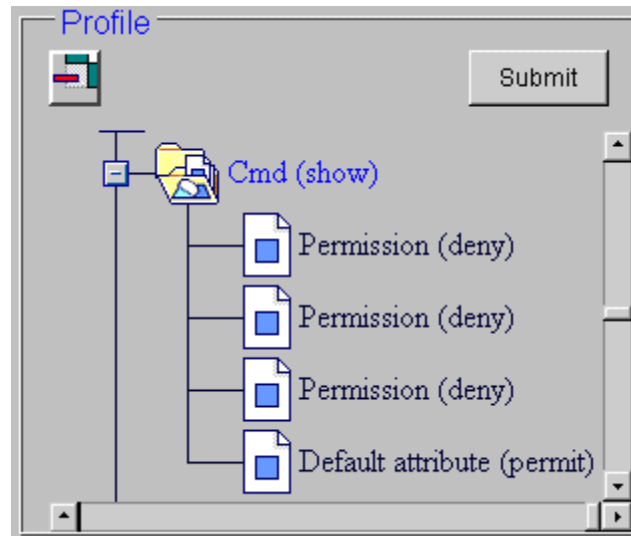


Figure 25. Multiple Command Arguments Configuration Example in Cisco Secure ACS for UNIX



Cisco Secure ACS for Windows provides similar capabilities for command authorization through the TACACS+ protocol. The application adds one further refinement to command filtering: the command authorization set. Command authorization sets enhance the scalability and manageability of setting authorization restrictions.

In Cisco Secure ACS for Windows, the default command authorization sets include the shell command authorization sets and the Cisco PIX command authorization sets. Cisco device-management applications, such as the CiscoWorks Management Center for PIX Firewalls, may be enabled to instruct Cisco Secure ACS for Windows to support additional command authorization set types. Command authorization sets enhance the command filtering capability as follows:

- Reusable named command authorization sets—a named set of command authorizations can be created without directly citing any user or group. Several command authorization sets can be defined, each delineating different access profiles. For example, a "help desk" command authorization set could permit access to high-level browsing commands, such as show run and could deny any configuration commands. An "all network engineers" command authorization set could contain a limited list of permitted commands for any network engineer in the enterprise. A "local network engineers" command authorization set could permit all commands, including IP-address configuration (figures 26 and 27).
- Fine configuration granularity—Associations can be created between named command authorization sets and network device groups. Thus, different access profiles can be defined for users depending on which network devices they access. The same named command authorization set can be associated with more than one network device group and used for more than one group. You can configure command authorization at the user and group levels.

Migration issue: Cisco Secure ACS for UNIX does not have a capability similar to the command authorization set. The unmatched commands option in Cisco Secure ACS for Windows is analogous to the default cmd option in Cisco Secure ACS for UNIX.

Figure 26. Accessing Command Authorization Sets Under Shared Profile Components

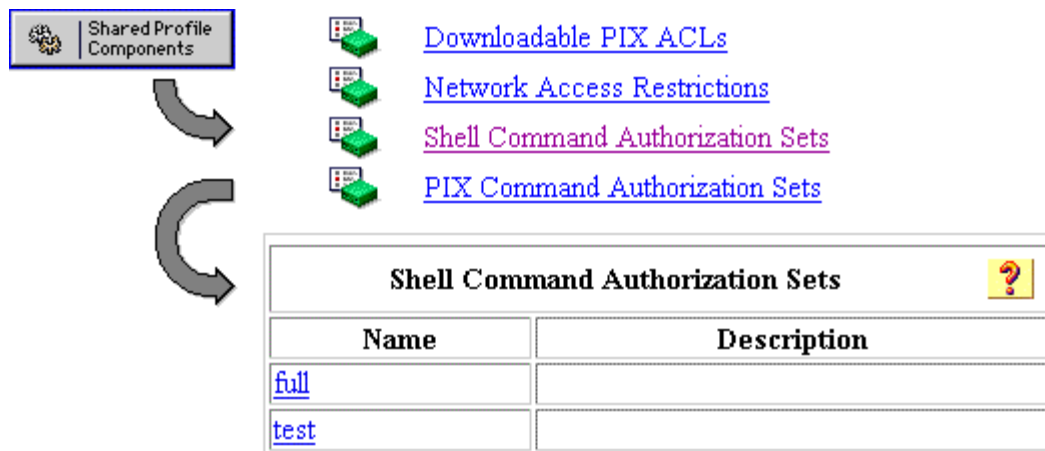


Figure 27. Configuration of a Command Authorization Set

Shell Command Authorization Set

Name:

Description:

Unmatched Commands:

- Permit
- Deny

Permit Unmatched Args

configure

enable

ip

no

show

permit running

deny user

Network Access Restrictions

Network access restrictions (NARs) provide the ability to define additional authorization and authentication conditions that must be met before a user can access the network. Both Cisco Secure ACS for UNIX and Cisco Secure ACS for Windows apply these conditions using information from attributes sent by the AAA clients (or network access server). Although there are several ways to set up NARs, all are based on matching attribute information sent by an AAA client.

Cisco Secure ACS for UNIX and Cisco Secure ACS for Windows differ substantially on what can be restricted and how the operation is performed.

Cisco Secure ACS for UNIX

Cisco Secure ACS for UNIX applies NARs using either IP address or a Domain Name System (DNS) host name (derived from the IP address provided by the network access server). The best way to show how Cisco Secure ACS for UNIX applies NARs is through a configuration example:

In this example, an organization has several network access servers in the same domain with similar names:

```
system1a.acme.com
system1b.acme.com
system1c.acme.com
system2a.acme.com
system2b.acme.com
system2c.acme.com
And so on.
```

It is necessary to conduct network-access-server filtering based on the host name for groups:

```
deny system1*.acme.com
allow *.acme.com
```

1. Go into the advanced section in the Cisco Secure GUI and edit the user or group.
2. Click the root profile for the user (Figure 28). You will get an options menu. In this menu select Filter and click Apply.
3. Click the Filter (refuse) icon (Figure 29).
4. The Filter icon is now set on (refuse). Click on the filter tab for the filter menu (Figure 30). In the "Nas:" box, enter the wildcard DNS name for one of the denied devices in the following format:

```
system1.*\acme.com
```

Here you will include such devices as system1a.acme.com, system1b.acme.com, etc. The "." is the UNIX wildcard, and the "\" protects the ".acme.com" from being wild carded.

5. When finished adding the denied devices, click the root profile for the user. You will get an options menu. In this menu, select Filter and click Apply.
6. Click the Filter (refuse) icon. In the permission menu, select Allow, and then click Apply. The Filter icon is now set on (allow). Click the icon again. Click the filter tab for the filter menu. Enter "." in all three boxes.
7. Click Submit (Figure 31).

When completed, the resulting profile from the ViewProfile command should look something like:

```
User Profile Information
user = admin1 {
profile_id = 31
profile_cycle = 2
member = admingroup1
password = clear "*****"
password = pap "*****"
privilege = web "*****" 15
```

```
refuse "system1.*\.acme.com" ".*" ".*"  
allow ".*" ".*" ".*"  
}
```

Migration issue: Cisco Secure ACS for UNIX requires authorization to be set on the network access server for this procedure to work. This differs from Cisco Secure ACS for Windows, which only requires authentication to be set on the network access server.

To enable filtering via the host name, make sure the following line in Cisco Secure ACS for UNIX.cfg is configured:

```
NUMBER config_get_names_from_dns = 1;
```

found between the lines:

```
NUMBER config_max_failed_authentication = 10;  
NAS config_nas_config =
```

This option is available in Cisco Secure ACS for UNIX v2.3(3) and later. Make sure that DNS is functioning properly on the Solaris system.

Figure 28. Root Profile Options Menu

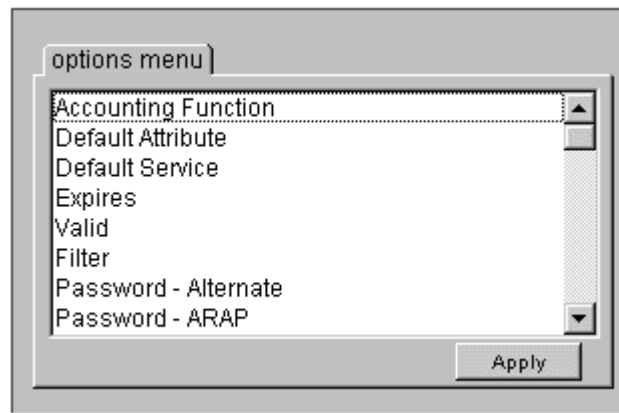


Figure 29. Profile Selection for Filter Profile

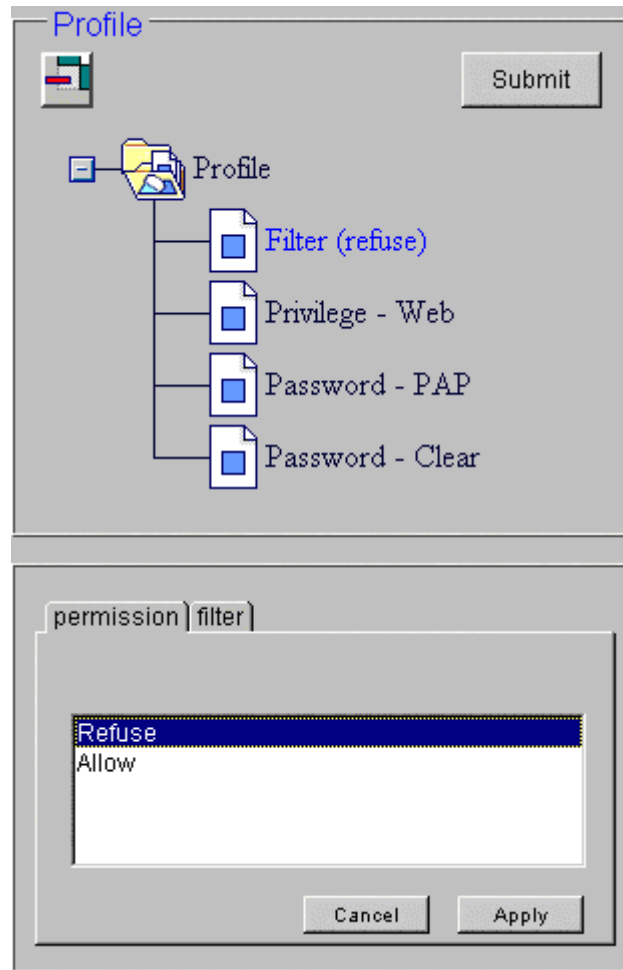


Figure 30. Filter Configuration Options

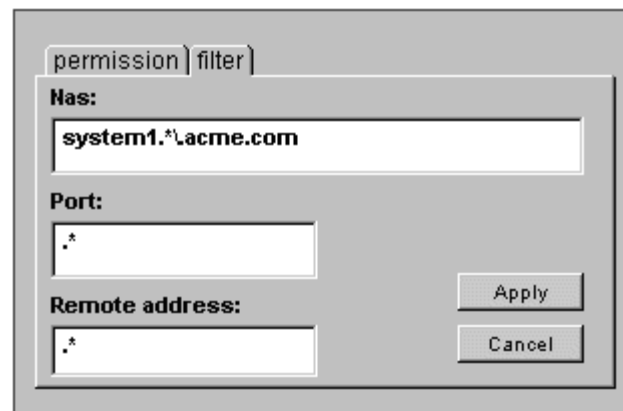
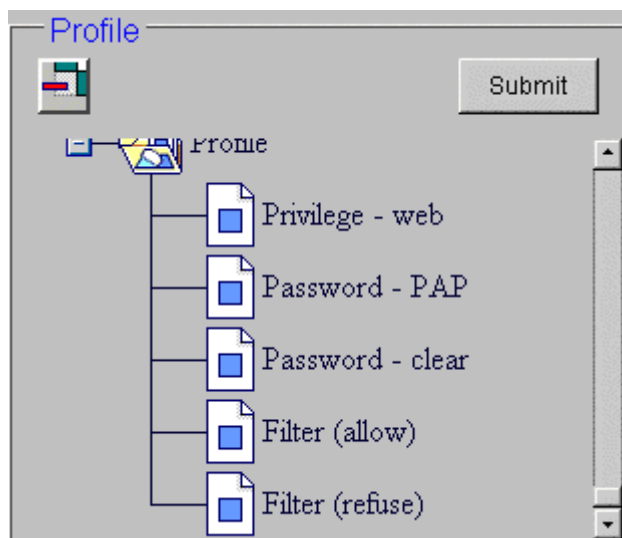


Figure 31. Final Profile Configuration for Filter Profile



Cisco Secure ACS for Windows

Cisco Secure ACS for Windows provides similar capabilities for network access restrictions (NARs). The application adds a refinement to NARs: the named profile. Shared-name NARs enhance the scalability and manageability of setting access restrictions. Named NAR profiles enhance the command filtering capability as follows:

Reusable named network access restriction profiles—a named set of network access restrictions can be created without directly citing any user or group. Several profile sets can be defined, each delineating different access profiles (figures 32 and 33). As with command, authorization sets, NARs can be configured at the group and user levels (Figure 34).

Migration issue: In addition to IP-based filters, in which the originating request relates to an IP address, non-IP-based restrictions using Calling Line Identification number (CLI) or Dialed Number Identification Service (DNIS) automatic number identification, may be used. CLI provides the caller's number and DNIS provides the number that was called. This feature in Cisco Secure ACS for Windows allows call-filtering control based on either or both CLI and DNIS. Cisco Secure ACS for UNIX does not have the capability to use CLI or DNIS for filtering.

Figure 32. Accessing NAR Named Profiles Under Shared Profile Components

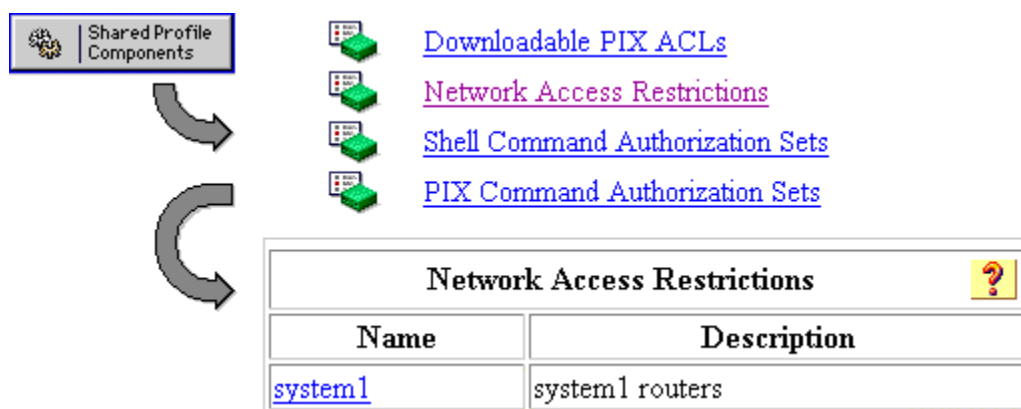


Figure 33. Named NAR Profile Configuration

Network Access Restriction

Name:

Description:

Define IP-based access restrictions

Table Defines:

AAA Client	Port	Src IP Address
NDG:system1-router	*	*

AAA Client:

Port:

Src IP Address:

Figure 34. Group-Level NAR Configuration

Network Access Restrictions (NAR) ?

Shared Network Access Restrictions

Only Allow network access when

- All selected NARs result in permit
- Any one selected NAR results in permit

NARs

system 1

>>

->

<-

<<

Selected NARs

View IP NAR

View CLI/DNIS NAR

Per User Defined Network Access Restrictions

Define IP-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	Address

remove

AAA Client: All AAA Clients

Port:

Address:

enter

Define CLI/DNIS-based access restrictions

Table Defines: Permitted Calling/Point of Access Locations

AAA Client	Port	CLI	DNIS

remove

AAA Client: All AAA Clients

Port:

CLI:

DNIS:

enter

Security

Issues of system security have been raised regarding Windows-based servers. UNIX-based systems are reported to be more secure from external threats. This issue is discussed in the white paper Securing Cisco Secure Access Control Server Running on Microsoft Windows Platforms, which can be found at

http://www.cisco.com/en/US/products/sw/secursw/ps2086/products_white_paper09186a00800887d8.shtml.

New Features in Cisco Secure ACS for Windows

Cisco Secure ACS for Windows has a number of new features that do not correspond to any features in Cisco Secure ACS for UNIX.

- Network Admission Control (NAC)
- ACS can now support up to 35,000 devices.
- Network access profiles (NAP) allows administrators to classify access requests according to network location, membership in a network device group, protocol type, or other specific RADIUS attribute values sent by the network device through which the user connects. Authentication, access control, posture validation and authorization policies can be mapped to specific profiles. An example of a profile-based policy is the ability to apply a different access policy for wireless access versus remote (VPN) access.
- ACS now uses a SQL database to store all the user and configuration information.
- Japanese browser support
- Support for group mappings for external Novell NDS databases is now done by using generic LDAP group set mappings.
- Machine Access Restrictions (MAR) Exemption Lists
- RADIUS Authorization Component (RAC) support for NAPs.
- ACS administrator permissions to improve password management and audit reports for regulatory compliance; for example, Sarbanes-Oxley (SOX).
- PEAP/EAP-TLS Support
- Logging and Reporting Extensions—support the syslog standard.
- Multiple concurrent logging destinations
- Japanese Microsoft Windows Support

Migration from Cisco Secure ACS for UNIX to Cisco Secure ACS for Windows

Cisco Systems does not currently offer any support for migrating from Cisco Secure ACS for UNIX to Cisco Secure ACS for Windows. Extraxi, a Cisco partner, provides migration services. Extraxi is located at <http://www.extraxi.com>.

**Americas Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com

Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc. Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc. and Access Registrar. Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)