ACE/Agent for Windows NT v 4.0

The ACE/Agent for Windows NT software, when used in conjunction with Security Dynamics' ACE/Server software and SecurID tokens, provides two-factor authentication protection to Windows NT machines.

Two-factor authentication is more secure than a password because the user must verify his or her identity by presenting two identifying factors instead of just one:

- the user's PIN (something that she alone knows), and
- the most recently generated SecurID tokencode (something that is unique and cannot be counterfeited).

When a user attempts to logon to a protected ACE/Agent machine, she is prompted for a SecurID PASSCODE. The user enters her PASSCODE and an authentication request is sent over a TCP/IP network to the ACE/Server, where the PASSCODE is validated. Unauthorized persons are denied access to the machine, while authorized SecurID tokenholders gain access easily.

Important! You must have at least a trial version of the ACE/Server software running on your network in order to utilize the ACE/Agent. No SecurID authentication can take place without an ACE/Server.

For more information about obtaining ACE/Server software or SecurID tokens, visit the Security Dynamics Web site at **http://www.securid.com**.

{button ,JI(`SDCONTRL.HLP',`SecurID_tokens')} SecurID tokens overview

{button ,JI(`SDCONTRL.HLP',`WEB_Overview')} WebID overview

Read Me First!

Important! You must have at least a trial version of the ACE/Server software running on your network in order to utilize ACE/Agent for Windows NT v 4.0.

No SecurID authentication can take place without the ACE/Server.

For more information about obtaining ACE/Server software or SecurID tokens, visit the Security Dynamics Web site at **http://www.securid.com**.

{button ,JI(`SDCONTRL.HLP',`ACE_Client_for_Windows_NT_v_4.1')} ACE/Agent for Windows NT v 4.0 overview

{button ,JI(`SDCONTRL.HLP',`WEB_Overview')} WebID overview

{button ,JI(`SDCONTRL.HLP',`SecurID_tokens')} SecurID tokens overview

SecurID Tokens - Overview

SecurID tokens are small hardware devices or software applications that generate unpredictable codes. The codes change at a specified interval, typically sixty seconds.

Every authorized user on a protected ACE/Server system is assigned a SecurID token to use when accessing a protected ACE/Agent. The code generated by the token is one part of the user's SecurID PASSCODE, which is required for positive user authentication and system access.

There are currently five types of SecurID tokens:

- the standard SecurID card
- the SecurID PINPAD
- the SecurID Key Fob
- SoftID, a software-based token that is installed directly on the user's machine, and
- the SecurID modem, a v34 modem that is installed on the user's machine

For more information about obtaining SecurID tokens, visit the Security Dynamics Web site at **http://www.securid.com**.

Contacting Security Dynamics

For more information about obtaining the SecurID tokens and ACE/Server software needed to make your ACE/Agent for Windows NT v 4.0 software functional, visit the Security Dynamics Web site at **http://www.securid.com**.

Deciding Which Users Will Be SecurID Tokenholders

Security Dynamics strongly recommends that ***all*** users of an ACE/Agent machine be SecurID tokenholders.

To protect local access, you can choose to challenge every local user for a PASSCODE or you can make specific users who are to be challenged members of the SDLOCAL group. This group is created for you in the User Manager when you install ACE/Agent for Windows NT.

With remote-access users, you can choose to challenge every remote user for a PASSCODE or you can make users who are to be challenged members of the SDREMOTE group. This group is also created for you when you install ACE/Agent for Windows NT.

Users in a Domain Environment

If you are using ACE/Agent for Windows NT on Domain Controllers, enable the software ***first*** on the Primary Domain Controller and ***then*** on the Backup Domain Controllers.

When you install ACE/Agent for Windows NT on a Domain Controller, the setup program creates the new groups Domain SDLOCAL and Domain SDREMOTE.

These two groups are global groups. Please note that:

- members of Domain SDLOCAL will be PASSCODE-challenged whenever they log on locally to ***any*** ACE/Agent-protected Windows NT machine within the domain
- members of Domain SDREMOTE will be PASSCODE-challenged whenever they dial-in to ***any*** ACE/Agent-protected Windows NT machine within the domain.

Because Domain Controller users are always global domain users as well, when they log on to the Domain Controller, the ACE/Agent software checks both the local and global groups.

SecurID Security and Accountability

It is important for you to be aware of ACE/Server and Windows NT security issues. The User Responsibilities section in the SecurID token authentication instructions explains these security issues.

Because user accountability is a critical part of system security, the ACE/Server creates an audit trail of all authentication requests as well as of all ACE/Server administrative operations. Refer to the ACE/Server Administration documentation for information about this audit trail.

When the ACE/Server is properly configured, the audit trail reliably identifies which user was responsible for each action logged.

Because it is based on two-factor authentication, user identification information in the ACE/Server audit trail provides stronger legal evidence of who performed the recorded activity than information based on a password alone. A user so identified cannot disown responsibility for security breaches perpetrated under his identity.

ACE/Agent also posts messages in the Windows NT Event Viewer. For more detailed information about these messages, see the Troubleshooting topics.

Ensuring ACE/Agent Security

To ensure the security of the protected system, it is essential that:

- every user maintain the secrecy of her PIN
- every user immediately notify an administrator if her PIN has been learned by anyone else
- every user ensure the physical security of her token and immediately notify an administrator if her token is missing
- every user follow the system’s standard logoff procedures so as not to leave an opening in the system for an intruder to enter

In addition, you should remember that:

- to protect local access, the ACE/Agent software must be installed on each Windows NT machine on the Local Access Network.
- to protect Web access, the ACE/Agent software must be installed on a Web server running Microsoft Internet Information Server.
- to protect remote access, the ACE/Agent software must be installed on the Windows NT machine that users will dial-in to. **There is no need to install ACE/Agent software on the remote computers**.

ACE/Agent Programs

All SecurID protection programs are executed either on the ACE/Agent machine or on the machine running the ACE/Server.

The following files comprise the ACE/Agent for Windows NT software. They are stored in the **\system32** directory, which is a subdirectory of the machine’s %SYSTEMROOT%.

aceclnt.dll The module that communicates with the ACE/Server and handles the API calls.

aceclnt.dll The module that communicates with the ACE/Server and handles the API calls.

clntchk.exe The program that displays configuration information.

sdcontrl.cpl The program that an administrator uses to configure the ACE/Agent settings.

sdgina.dll The Security Dynamics graphical identification and authentication module that authenticates designated local users.

sdiisutl.dll The Security Dynamics module that provides utility functions for the IIS extensions.

sdmsg.dll The module that stores the event log messages.

sdras.dll The Security Dynamics module that authenticates designated remote users.

sdtest.exe The program that verifies that user authentication can take place.

The following are additional files that the ACE/Agent for Windows NT program uses. They are stored in your **\system32\aceclnt** directory:

sdiis.dll The Security Dynamics IIS CGI extension.

sdiisflt.dll The Security Dynamics IIS filter extension.

***.htm** Various HTML templates files that you can edit to customize the appearance of the WebID authentication interface.

license.txt A text file containing a copy of the ACE/Agent for Windows NT licensing agreement, whose terms you agreed to prior to running the setup program.

Before You Enable ACE/Agent Protection

Before you enable ACE/Agent protection on any Windows NT machine, it is very important for you to understand the ACE/Server system and its features. Some of these features include New PIN mode, client activations, and group memberships.

If you have any concerns or questions about these or any other ACE/Server administration tasks, see the ACE/Server user documentation or contact your ACE/Server administrator.

If you intend to use the ACE/Agent software to protect files on a Web server, you should be aware of special concerns regarding virtual Web servers. If you are running virtual Web servers, you must define a secondary ACE/Agent node for each additional IP address. Ask your ACE/Server administrator or consult the ACE/Server user documentation for instructions on how to define secondary nodes.

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

System Setup Tasks

Before you begin using the ACE/Agent for Windows NT software, you must perform the following tasks:

{button ,JI(`SDCONTRL.HLP',`WEB_ACE_Server_Tasks')} Verify that the ACE/Server is available and the ACE/Agent is registered

{button ,JI(`SDCONTRL.HLP',`Tokenholder_Setup_Tasks')} Register the tokenholders

ACE/Server Setup Tasks

Before you begin using the ACE/Agent for Windows NT software, the following ACE/Server tasks must be complete:

- The ACE/Server software has been installed on a network machine that will provide the ACE/Server authentication service for the ACE/Agent.

  Important! You must have at least a trial version of the ACE/Server software in order to use the ACE/Agent. No SecurID authentication can take place without an ACE/Server running on your network.

  For more information about obtaining ACE/Server software, visit the Security Dynamics web site at **http://www.securid.com**.

- The Windows NT machine that will be protected has been registered as a client of the ACE/Server. If the Windows NT machine is a client of a v 1.X ACE/Server, the client type should be **UNIX**. If the Windows NT machine is a client of a v 2.X or later ACE/Server, the client type should be **Net OS Client**.

- The ACE/Server administrator has made the file sdconf.rec available to you, and you have copied it to the Windows NT machine's **system32** directory. The **system32** directory is a subdirectory of the %SYSTEMROOT%.

Tokenholder Setup Tasks

Before you begin using the ACE/Agent for Windows NT software, the following tokenholder setup tasks must be complete:

- The Users who will be challenged for PASSCODEs have been registered as tokenholders in the ACE/Server database, and their tokens have been activated. These processes are covered in the ACE/Server user documentation.

  Important! Each tokenholder’s ***Windows NT*** username must be registered in the ACE/Server database. These usernames ***cannot*** contain spaces and ***must not*** exceed forty characters. For Windows NT username parameters, run the User Manager application in the Administrative Tools.
- The Users who will be challenged for PASSCODEs have been given their assigned and activated tokens and copies of the authentication instructions.
- The Users who will be challenged remotely have been given copies of the instructions for configuring their remote computers. A Microsoft Word version of these instructions, called **ras_conf.doc**, was also copied into your **\system32\aceclnt** directory during installation.
- The Users who will be challenged on the Web are using Web browsers that support FORMs and Persistent Client State HTTP Cookies .

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

Distributing Authentication Instructions

The users who will be challenged for PASSCODEs must be provided with copies of the SecurID authentication instructions.

These instructions were copied into the special **\system32\aceclnt** directory during installation so that you can print them or post them on a network drive for users to print themselves.

The files are in Microsoft Word 6.0 format and are named as follows:

- **loc_card.doc** - instructions for local users who will be authenticating with a Standard SecurID card or a SecurID Key Fob.
- **loc_pin.doc** - instructions for local users who will be authenticating with a SecurID PINPAD.
- **ras_card.doc** - instructions for remote users who will be authenticating with a Standard SecurID card or a SecurID Key Fob.
- **ras_pin.doc** - instructions for remote users who will be authenticating with a SecurID PINPAD.

System Requirements Checklist

In order for certain ACE/Agent protection features to be available on the Windows NT machine, the following requirements must be met:

{button ,JI(`SDCONTRL.HLP>(w95sec)',`WEB_ACE_Server_Tasks')} ACE/Server requirements

{button ,JI(`SDCONTRL.HLP>(w95sec)',`WEB_New_Local_protection_requirements')} Local Protection Requirements

{button ,JI(`SDCONTRL.HLP>(w95sec)',`WEB_New_Web_protection_requirements')} Web Protection Requirements

{button ,JI(`SDCONTRL.HLP>(w95sec)',`WEB_New_Remote_access_protection_requirements')} Remote Access Protection Requirements

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

Local Protection Requirements

In order for Local protection features to be available on the machine, the following requirements must be met:

- The machine must have at least 16 MB of memory (RAM).
- The machine must be running TCP/IP and be configured for static IP addresses.

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

Web Protection Requirements

In order for the Web protection features to be available on your Web server, the following requirements must be met:

- The disk partition containing the Web server directories should be an NTFS partition. The FAT file system is highly unsecure and is not recommended.
- The Web server machine is ***not*** acting as a master or slave ACE/Server.
- The Web server machine must have a Secure Sockets Layer (SSL) certificate installed to ensure that transmission of critical information is not compromised.

  For more information about how to obtain an SSL certificate from a Certificate Authority, such as VeriSign, read "Chapter 5: Securing Your Site Against Intruders" in the Microsoft Internet Service Manager's online help or visit the VeriSign Web site at **http://www.verisign.com/microsoft/**.
- WebID supports Microsoft Internet Explorer versions 3.0 and later and Netscape Navigator versions 1.1 and later browsers. Other browsers may work, but you should consult their manufacturers to make sure the programs support FORMs and Persistent Client State HTTP Cookies.

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

Remote Access Protection Requirements

If you will be using ACE/Agent software to protect remote access connections, make sure the RAS machines that users will dial-in to meet the following requirements.

- Normal dial-in access to the Windows NT machine must already be enabled, but it should be disabled during installation and configuration of the ACE/Agent software.
- The Windows NT machine used for remote access should be physically inaccessible to all unauthorized persons. If it is not secure in this way, someone could unload the ACE/Agent **.dll** files and eliminate SecurID protection.
- Dial-in or Web client stations must be running Windows NT 3.51 or later, Windows 95, or Windows for Workgroups 3.11.

{button See Also,AL(`GetStart;WebIDRequirements',0,`',`')}

Changing ACE/Agent Security Settings

To configure the ACE/Agent security settings:

1 From the Start menu, choose **Settings > Control Panel**.

2 In the window that opens, double-click the **ACE/Agent** icon. The ACE/Agent control panel opens.

3 When the ACE/Agent control panel opens, click the appropriate tab to configure

- Local Access protection
- Remote Access protection
- Web protection

Note: When you finish setting security options, you must use the Windows NT User Manager to add individual members to the SDLOCAL and SDREMOTE groups.

{button ,JI(`SDCONTRL.HLP',`WEB_Adding_Users_To_Groups')} Adding Users to Groups

Configuring the ACE/Agent “Main” Properties Page

The Main properties page indicates the ACE/Agent features that are available for activation and configuration.

To activate ACE/Agent security features:

1. From the Start menu, open the ACE/Agent Control Panel.
2. Click the appropriate tab to enable or disable
   - Local Access protection
   - Remote Access protection
   - Web protection

   Note: If you modify any security settings, you must restart Windows NT for the new settings to take effect.
3. To test that ACE/Agent authentication has been correctly implemented without restarting Windows NT
   - click the Test Authentication with ACE/Server button.
4. To uninstall the ACE/Agent software
   - click **Uninstall of ACE/Agent for Windows NT**

To review the security features available for activation:

1. The Component Status panel indicates if the components are installed and the corresponding security features are available for activation.
   - If a tab is not displayed in the ACE/Agent Control Panel, the Component Status provides a brief description of the problem.
2. If a tab is missing from the ACE/Agent Control Panel, review the following topics to verify that you have the proper software installed and enabled on the workstation.
   - System Requirements Checklist
   - Before You Begin
   - Getting Started

Configuring Local Access Protection

The Local properties page governs local access security. Local access control can be configured to PASSCODE challenge

- all local users
- users who are members of the SDLOCAL group
- users who are members of the Domain SDLOCAL group

The SDLOCAL group is created during installation. When you install the software on a Domain Controller, a global group named Domain SDLOCAL is also created. After you have set the security options, you are given an opportunity to add members to these groups.

To enable local PASSCODE protection:

1 In the ACE/Agent Control Panel, click the Local access properties page.

2 Click **Enable Local Access Security**. The **Challenge All Users**, **Screensaver Security**, and **Reserve Password** options become available.

   - If you want ***all*** local users to be challenged for a PASSCODE, select **Challenge All Users**.

     If you do not choose this option, only members of the SDLOCAL group or the Domain SDLOCAL group will be challenged for a PASSCODE.

     When you select **Challenge All Users**, the **Reserve Password** feature is automatically marked as well. This is done to prevent you from enabling the **Challenge All Users** feature without setting a reserve password.

     If you enable the **Challenge All Users** feature without setting a reserve password and an interruption occurs in your ACE/Server authentication service, all users will be locked out of the protected machine. For this reason, you should ***always*** set a reserve password when enabling the **Challenge All Users** feature. See Using the Reserve Password.

   - If you wish to have users reauthenticate every time their desktop screen saver activates, select **Enable Screen Saver Security**. This option takes effect only if screen saver password protection is available on the Windows NT machine and if password protection has been enabled for the user account through the Desktop Control Panel application.

3 Click **Apply** to accept the new settings.

4 If you would like the changes to take effect immediately, restart Windows NT.

{button ,JI(`SDCONTRL.HLP',`HIDD_MAIN')} Configuring the ACE/Agent

Configuring Remote Access Protection

The Remote properties page governs the security of remote-access accounts. If RAS is enabled on the Windows NT machine, the message in the Component Status panel of the Main ACE/Agent properties page reads “Remote: Security Features Available.”

To enable PASSCODE protection for members of SDREMOTE:

1 In the ACE/Agent control panel, click the Remote access properties page.

2 Select **Enable Remote Access Security**.

3 If you want all remote users to be challenged for a PASSCODE, select **Challenge All Users**.

- If you do not choose this option, only remote users who are members of SDREMOTE or Domain SDREMOTE group will be challenged for a PASSCODE.
- If you do ***not*** want the Windows NT Event Log to resolve usernames when users log on, check the **Do not resolve username in Event Log messages** option. Enabling this option will save remote users time during the logon process. However, it will prevent you from filtering Log events by user.

4 If you do not want your remote users to see the DOMAIN: prompt during remote login, check the **Disable Domain Prompt** option and type the domain name that remote users belong to in the **Default Domain** field. At login, the user will only see the USERNAME: and PASSCODE: prompts.

After the user enters a valid PASSCODE, the user will be authenticated to the default domain.

5 If you want your remote users to see a custom greeting message when they are prompted for their username and PASSCODE, check the **Enable Logon Greeting** option and type your custom greeting in the scrollable box below the **Enable Logon Greeting** checkbox.

6 Click **Apply** to accept the new settings.

7 If you would like the changes to take effect immediately, restart Windows NT.

Note: The SDREMOTE group was created during installation. If the ACE/Agent software resides on a Domain Controller, a global group named Domain SDREMOTE was also created. After you have set the security options, you will be given an opportunity to add members to these groups.

{button ,JI(`SDCONTRL.HLP',`HIDD_MAIN')} Configuring the ACE/Agent

Deciding to Use the Reserve Password

The reserve password feature is supported ***only*** by SDGINA, the local access security process. Remote-access users must successfully use PASSCODE authentication if their accounts are configured to require it. However, administrators of SDRAS accounts should read this section in order to understand the security issues.

If a user is in the SDLOCAL or Domain SDLOCAL group and local authentication is enabled, the user will not be able to access the Windows NT machine if there is a network failure or some other problem that prevents the Windows NT machine from communicating with the ACE/Server. This could present a problem if you plan to have all users PASSCODE challenged. Click the Examples button to review ways to configure your system and avoid this problem.

{button ,JI(`SDCONTRL.HLP',`WEB_Reserve_Password_Examples')} Example

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_Reserve_Password')} Enabling the Reserve Password

{button ,JI(`SDCONTRL.HLP',`HIDD_SDGINA')} Enabling Local Access Protection

Reserve Password Examples

Example 1

You can set up one user account with administrator privileges that is not PASSCODE protected. Most people think of this first, but it is not a good idea because it creates a security hole: you now have an account with full access that is less protected than accounts with less privilege.

Example 2

If you are using a domain, you can physically secure the machine running as the Domain Controller (that is, put it in a locked office for which only the network administrator has the key) and disable network logons to this machine. In the event of a problem, this machine could be used to disable the requirement for PASSCODE authentication.

Example 3

You can use the **Reserve Password** feature of ACE/Agent for Windows NT. If you have enabled the **Reserve Password** and the Windows NT system is unable to communicate with the ACE/Server at the time of authentication, instead of displaying a message that the ACE/Server is unreachable, the system displays a prompt to enter a reserve password.

A user who knows the reserve password can use it in place of PASSCODE authentication. This solution is not as strong a security measure as example 2, but it is better than example 1.

Enabling the Reserve Password

To enable the Reserve Password:

1. In the ACE/Agent Control Panel, click the Local properties page.
2. If it is not selected already, select **Enable Local Access Security**.
3. Select **Enable Reserve Password**.
4. Enter the reserve password you want to use in the **Password** field. The password must be 6 to 12 characters long and must contain at least one digit and one letter. Reserve passwords are case sensitive.
5. Press TAB.
6. Enter the password again in the **Confirm** field.
7. Click **Apply** to confirm the new settings.

The reserve password is encrypted and stored in the registry, but it will be accessible only to the ACE/Agent for Windows NT process. It cannot be modified with the tools used to manipulate user passwords.

The reserve password should be changed after each use. If you enable the **Reserve Password** option and ever tell it to a user, Security Dynamics recommends changing the reserve password as soon as the user has logged on to the protected machine.

If you disable the **Reserve Password** option by turning off **Enable Reserve Password** and clicking **Apply**, the Reserve Password is cleared. Also, if you disable local SecurID authentication by turning off **Enable Local Access Security** and click **Apply**, the reserve password is cleared.

To test that the **Reserve Password** option is enabled, disconnect the network connection, log off, and log back on.

{button ,JI(`SDCONTRL.HLP',`WEB_Reserve_Password')} Deciding to Use the Reserve Password

{button ,JI(`SDCONTRL.HLP',`HIDD_SDGINA')} Enabling Local Access Protection

Adding Users to Groups

You can add members to a group at any time using Windows NT User Manager. When you installed ACE/Agent during Windows NT installation, the setup program created two local groups

- SDLOCAL
- SDREMOTE

If the machine is a Domain Controller, the installation process also created two global groups:

- Domain SDLOCAL
- Domain SDREMOTE

When you finish setting security options, you must use the Windows NT User Manager for Domains to add individual users to the Domain SDLOCAL and Domain SDREMOTE groups.

To PASSCODE-challenge users and groups:

If you wish to PASSCODE-challenge:

all local users	select **Challenge All Users** on the Local properties page
some local users	add the users to the SDLOCAL group and do **not** select **Challenge All Users** on the Local properties page
all remote dial-in users	select **Challenge All Users** on the Remote properties page
some remote users	add the users to the SDREMOTE group and do **not** select **Challenge All Users** on the Remote properties page
domain users logging to any ACE/Agent in the domain	add the users to Domain and do not select **Challenge All Users** on the Local properties page
domain users dialing-in to any ACE/Agent in the domain	add the users to Domain and do not select **Challenge All Users** on the Remote properties page

To add members to a group:

1 Open the Windows NT User Manager.

2 Double-click the name of the group. A dialog box with the names of the current members displays.

3 Click **Add**. A list of users who are not in the group displays.

4 Click the name of a user you want to add to the group and click **Add**.

5 Repeat step four to add each additional user.

6 Click **OK**. The users you selected are now members of the selected group.

7 Click **OK** to close the User Manager.

You can add members to the ACE/Agent groups at any time using the User Manager.

Testing Authentication

You must restart the Windows NT machine in order for the security settings you have chosen to take effect. However, you can test that ACE/Agent authentication has been correctly implemented without restarting. This test verifies that sdconf.rec points to the appropriate ACE/Server and that your system is configured properly for authentication.

Testing will go more smoothly if you use a token with a PIN that is already registered in the ACE/Server database. However, if you test authentication with a token in New PIN mode, you will go through the actual New PIN procedure, and the PIN will be registered in the ACE/Server database. If you are new to SecurID authentication and need assistance with New PIN mode, read the instructions in **\system32\aceclnt** that correspond to your token type (**loc_card.doc** or **loc_pin.doc**).

If the token you are testing has a PIN, you need to know the PIN.

Note: Because authentication is being tested, not confirmed, it is not necessary for the owner of the token to be a member of SDLOCAL or Domain SDLOCAL.

{button ,JI(`SDCONTRL.HLP',`WEB_TEST_AU_STANDARD_FOB_WITH_PIN')} Testing Authentication Using a Standard Card or Key Fob if the Token Already has a PIN

{button ,JI(`SDCONTRL.HLP',`WEB_TEST_AU_STANDARD_FOB_NO_PIN')} Testing Authentication Using a Standard Card or Key Fob if the Token Does Not Have a PIN

{button ,JI(`SDCONTRL.HLP',`WEB_TEST_AU_TOKEN_HAS_PIN')} Testing Authentication using a PINPAD Card if the Token Has a PIN

{button ,JI(`SDCONTRL.HLP',`WEB_TEST_AUTH_TOK_NO_PIN')} Testing Authentication using a PINPAD Card if the Token Does Not Have a PIN

Testing Authentication Using a Standard Card or a Key Fob if the Token Already Has a PIN

1 Open the ACE/Agent Control Panel.

2 In the Main properties page, click **Test Authentication with ACE/Server**.

3 At the prompt, enter the username of the tokenholder.

4 At the **Enter PASSCODE** prompt, enter the PIN followed by the tokencode displayed by the token.

5 Click **OK**. The system displays a message that the user was successfully authenticated.

6 If the system displays an **Access denied** message, repeat the process.

Note

- If you see any other messages, consult the installation and configuration messages section in the ACE/Server user documentation.
- If you repeat the process and are still denied access, follow the instructions for testing authentication with a standard card or key fob without a PIN.

{button ,JI(`SDCONTRL.HLP',`WEB_Testing_Authentication')}   Testing Authentication

Testing Authentication Using a Standard Card or a Key Fob if the Token Does Not Have a PIN

1 Open the ACE/Agent Control Panel.

2 In the Main properties page, click **Test Authentication with ACE/Server**. You are prompted for a username and PASSCODE.

3 Enter the username of the tokenholder.

4 At the **Enter PASSCODE** prompt, enter the tokencode displayed by the token and click **OK**. The New PIN dialog box displays.

5 Follow the New PIN procedure in the authentication instructions and click **OK**. The authentication prompt displays.

6 Enter the username of the tokenholder.

7 At the **Enter PASSCODE** prompt

- enter the PIN followed by the tokencode displaying in the LCD of the token
- click **OK**

8 If everything is properly implemented and configured, the system displays a message that the user successfully authenticated.

9 If the system displays an **Access denied** message, repeat the process.

If you see any other messages, consult the installation and configuration messages section in the ACE/Server user documentation.

{button ,JI(`SDCONTRL.HLP',`WEB_Testing_Authentication')} Testing Authentication

Testing Authentication Using a PINPAD Card if the Token Already Has a PIN

1 Open the ACE/Agent Control Panel.

2 In the Main properties page, click **Test Authentication with ACE/Server**.

3 At the prompt, enter the user name of the tokenholder.

4 Enter the PIN in the card and press the diamond (◆) near the bottom of the card.

5 At the **Enter PASSCODE** prompt, enter the tokencode displayed by the token.

6 Click **OK**. The system displays a message that the user was successfully authenticated. If the system displays an **Access denied** message

- press the **P** at the bottom of the card
- wait for a new tokencode to display
- repeat the process

If you are still denied access, follow the instructions for testing authentication with a PINPAD card without a PIN.

{button ,JI(`SDCONTRL.HLP',`WEB_Testing_Authentication')}   Testing Authentication

Testing Authentication Using a PINPAD Card if the Token Does Not Have a PIN

1. Open the ACE/Agent Control Panel.
2. In the Main properties page, click **Test Authentication with ACE/Server**. You will be prompted for a username and PASSCODE.
3. Enter the username of the tokenholder.
4. Enter the tokencode displayed by the token and click **OK**.
5. In the New PIN dialog box, follow the New PIN procedure in the authentication instructions.
6. Enter the username of the tokenholder.
7. Enter the PIN in the card and press the diamond (◆) near the bottom of the card.
8. At the **Enter PASSCODE** prompt, enter the tokencode displayed by the token.
9. Click **OK**. The system displays a message that the user was successfully authenticated. If the system displays an **Access denied** message
    - press the **P** at the bottom of the card
    - wait for a new tokencode to display
    - repeat the process

If you see any other messages, consult the installation and configuration messages section of the ACE/Server user documentation.

{button ,JI(`SDCONTRL.HLP',`WEB_Testing_Authentication')} Testing Authentication

Configuring the Internet Service Manager for Web Protection

Before you enable SecurID protection on your Web server, you must first configure the Password Authentication settings in the Microsoft Internet Service Manager.

In order to fully utilize the WebID features, you ***must*** have a Secure Sockets Layer (SSL) certificate installed on the Web server. If you do not have an SSL certificate installed, the Web authentication username and PASSCODE will not be encrypted before transmission.

Note: For more information about how to obtain an SSL certificate from a Certificate Authority, such as VeriSign, read “Chapter 5: Securing Your Site Against Intruders” in the Microsoft Internet Service Manager online help or visit the VeriSign Web site at **http://www.verisign.com/microsoft/**.

{button ,JI(`SDCONTRL.HLP',`WEB_Configuring_Password_Authentication')}   Configuring Password Authentication Properties

{button ,JI(`SDCONTRL.HLP',`WEB_Configuring_Global_WebID_Settings')}   Configuring Global WebID Settings

{button ,JI(`SDCONTRL.HLP',`WEB_WebID_Administration')}   Accessing WebID from the Internet Service Manager

Configuring Password Authentication Properties

1 From the Start menu, select **Programs > Microsoft Internet Server > Internet Service Manager**.

2 Highlight the name of the World Wide Web server that will be Web protected.

3 From the Properties menu, select **Service Properties**.

4 Click the **Service** tab. The Service Properties page displays.

n To permit an anonymous user to browse the Web server directories using the username and password defined in the Anonymous Logon pane, select **Allow Anonymous**. This option does not bypass the file- and directory-level security permissions that have been set using the Windows NT Explorer's security tools.

Note: Do not select **Allow Anonymous** if you are using a FAT file system to contain sensitive information.

n To activate password authentication for users accessing the Web server, enable either **Basic (Clear Text)** or **Windows NT Challenge/Response**. If you do not select either option, users running the Microsoft Internet Explorer browser will receive an “A required header is missing/not found” error and will not be authenticated.

- **Basic (Clear Text)** provides password authentication for all Internet browsers. If you choose this option, Security Dynamics strongly recommends that you have an SSL certificate installed on the Web server. Otherwise, the usernames and passwords that users enter will be transmitted in unencrypted clear text, which is highly unsecured.
- **Windows NT Challenge/Response** allows Microsoft Internet Explorer users to access files on a Web server without being prompted for a username and password. Users are only prompted for a PASSCODE if they attempt to access a SecurID-protected page. This option does not support users running browsers other than Microsoft Internet Explorer. Do not enable **Windows NT Challenge/Response** if the username the tokenholder uses to logon to her own machine is different than the username that is recorded in the ACE/Server database.

  Note: To make sure that all users are able to authentication on the Web server, it is best to enable BOTH **Basic (Clear Text)** and **Windows NT Challenge/Response**.

{button ,JI(`SDCONTRL.HLP',`WEB_Configuring_the_Internet_Service_Manager')} Configuring the Internet Service Manager for Web Protection

Accessing WebID from the Internet Service Manager

The WebID feature set allows quick and easy graphical administration of protected pages and their global settings through a special properties page in the ACE/Agent Control Panel application.

Note: You must stop and restart WWW service from the IIS Manager after making any changes in the Web protection page.

To view the Web protection page:

1 From the Start menu, select **Programs > Microsoft Internet Server > Internet Service Manager**.

2 The Internet Service Manager dialog box opens.

3 Click the SecurID icon in the toolbar, or choose **WebID Control** from the Tools menu.

4 The Microsoft Internet Service Manager opens and displays the Web properties page.

{button ,JI(`SDCONTRL.HLP',`HIDD_Directories')} Enabling Web Protection

WebID Overview

ACE/Agent for Windows NT features WebID, a feature set that allows you to SecurID-protect selected pages and directories on a World Wide Web server.

When you enable Web protection on a directory or file, users who attempt to view the Web page containing the protected material are prompted for a SecurID PASSCODE . If the user enters a valid PASSCODE, she is given access to the page; if the user does not enter a valid PASSCODE, she is denied access.

Only those users who are registered as tokenholders in your ACE/Server database are able to access SecurID-protected Web pages. As a result, you can use your Web site as both a public resource available to anonymous users and a highly secure Intranet for posting confidential information to trusted users.

The WebID feature set allows quick and easy graphical administration of protected pages and their global settings through the Web protection page in the ACE/Agent Control Panel application.

Note: WebID protects **http** and **https** URLs. Due to the security risks associated with ftp file transfers across the Internet (e.g., anonymous user access), WebID does not protect files on an ftp server.

The following protocols are not supported by WebID:

- ftp
- news
- gopher
- telnet
- wais

Configuring Web Protection Settings

The WebID feature set allows quick and easy graphical administration of protected pages and their global settings through the Web properties page in the ACE/Agent Control Panel application.

When you enable Web protection on a directory or file, users who attempt to view the Web page containing the protected material are prompted for a SecurID PASSCODE. If the user enters a valid PASSCODE, she is given access to the page; if the user does not enter a valid PASSCODE, she is denied access to the page.

{button ,JI(`SDCONTRL.HLP',`HIDD_Directories')}   Enabling Web Protection

{button ,JI(`SDCONTRL.HLP',`WEB_Domain_Cookies')}   Enabling Domain Cookies

{button ,JI(`SDCONTRL.HLP',`WEB_Assuring_that_Every_Connection_is_Secure')}   Assuring Every Connection is Secure

{button ,JI(`SDCONTRL.HLP',`WEB_Preventing_Disk_Caching')}   Preventing Disk Caching

Web Protection Properties Page

To enable ACE/Agent protection on Web pages:

1 Open the Web protection properties page.

2 Select **Enable WebID Features Set**. The text of the various Web protection features darkens, indicating that they are ready to be configured.

3 Click **Select Files to Secure.** The Select files to secure dialog box opens and displays the files and directories on the Web server arranged in a standard Windows file tree format. The house icon at the top of the tree indicates the root or home directory of the server.

- To browse through the contents of the server, double-click the directory icons.

4 You can choose to protect:

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_entire_server')} Protecting an entire server

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_directory')} Protecting a specific directory

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_file')} Protecting a specific file

5 the entire server or individual directories (of URLs) and files (individual URLs) on the server. To enable Web protection

- point to the files or directories you wish to SecurID-protect
- click the right mouse button.

6 You must stop and restart your Web server in order for WebID configuration changes to take effect.

Note: While WebID includes the option to protect individual Web server files, it is more efficient and secure to protect the entire directory that contains the file. When you protect a directory, each file or subdirectory you add to the directory later will be protected automatically.

Enabling Web Protection on a Server

To protect Web pages on a server:

1 Open the Web protection page.

2 If it is not checked already, check the **Enable WebID Features Set** box.

3 Click **Files to Secure**.

4 When the Select file to Secure dialog box opens, point at the house icon and click the right mouse button.

5 A SecurID icon appears to the left of the home icon, indicating that every page on the server is SecurID-protected.

6 Click **OK** to confirm the changes.

Note: Any files or directories that you add to the server in the future will be automatically SecurID-protected.

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_directory')} Enabling WEB protection on a specific directory

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_file')} Enabling WEB protection on a specific file

Enabling Web Protection on a Directory

It is best to protect entire directories, since any files or subdirectories that you add to the directory in the future are automatically protected by SecurID.

To protect Web pages in a specific directory:

1 Open the Web protection page and click **Select Files to Secure**.

2 The Select Files to protect dialog box opens and displays the directories and files on the Web server.

Browse through the tree to find the directory you want to protect and point at that directory's icon. For example, if in the URL **http://www.home.com/products/** you want to protect the contents of **products**, point at the **products** directory.

3 To enable protection on a

n directory, click the right mouse button

n series of directories, hold down the right mouse button and drag the pointer across the icons

4 The subordinate directories in the tree disappear and a SecurID icon appears beside the protected directory, indicating that all of the files in the directory are SecurID-protected.

5 Click **OK** to confirm the changes.

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_entire_server')} Enabling WEB protection on an entire server

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_file')} Enabling WEB protection on a specific file

Enabling Web Protection on a File

WebID gives you the ability to protect individual Web server files, although this option is not as efficient as protecting the entire directory that contains the file. When you protect a directory, any files or subdirectories you add to the directory later are protected automatically.

Protecting random files instead of specific directories creates additional administrative overhead. With individual file protection, you have to enable protection on new files one-by-one, which may result in some files being overlooked and left unprotected.

To protect individual Web pages:

1 Open the Web protection page and click **Select Files to Secure**. The Web Protection page opens.

2 Click **Show Files**.

3 Browse through the tree to find the file you want to protect and point to this file’s icon.

4 To enable protection on a

- file, click the right mouse button
- series of files, hold down the mouse button and drag the pointer across the icons.

5 A SecurID icon appears, indicating that the default.old.htm file is SecurID-protected.

6 Click **OK** to confirm the changes.

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_entire_server')} Enabling WEB protection on an entire server

{button ,JI(`SDCONTRL.HLP',`WEB_Enabling_WebID_protection_specific_directory')} Enabling WEB protection on a specific directory

Configuring Global Web Protection Settings

The WebID feature set lets you configure global settings that will affect each protected directory and file. These settings include

- Cookie distribution and expiration control
- Connection security options

Remember that you must stop and restart your Web server in order for WebID configuration changes to take effect.

{button ,JI(`SDCONTRL.HLP',`WEB_Distributing_Web_ID_Cookies')} Distributing WebID cookies

{button ,JI(`SDCONTRL.HLP',`WEB_Assuring_that_Every_Connection_is_Secure')} Assuring Secure Connections using SSL

{button ,JI(`SDCONTRL.HLP',`WEB_Preventing_Disk_Caching')} Preventing Disk Caching of Protected Pages

Distributing Web ID Cookies

When a tokenholder enters a valid PASSCODE in the WebID authentication interface, the Web server gives her a cookie. The cookie is stored in the tokenholder's Web browser and acts as an admission ticket, passing user authentication information to the server every time a SecurID-protected file or directory is encountered. As a result, the tokenholder is prompted only once for a PASSCODE during the period for which her cookie is valid.

In order for the cookies to work, tokenholders must be using a Web browser that supports FORMs and Persistent Client State HTTP Cookies . See WebID Requirements for more information about supported browsers.

{button ,JI(`SDCONTRL.HLP',`WEB_Configuring_Cookie_Expiration_Controls')} Configuring Cookie Expiration Times

{button ,JI(`SDCONTRL.HLP',`WEB_Domain_Cookies')} Enabling Domain Cookies

Setting Cookie Expiration Times

A WebID cookie is valid only during the browsing session for which it was created. When the tokenholder exits his Web browser, the cookie expires and must be renewed during the next authentication session.

Before enabling the WebID cookie features, you should decide what additional expiration controls, if any, you wish to place on the cookies you hand out to tokenholders.

Cookies can be configured to expire during a browsing session

{button ,JI(`SDCONTRL.HLP',`Expiring_Cookies_Automatically_after_a_Specified_Time')} automatically after an administrator-defined period, regardless of whether or not the cookie is in use, or

{button ,JI(`SDCONTRL.HLP',`Expiring_Cookies_after_a_timeout_period')} after the cookie has remained unused for an administrator-defined timeout period.

These control features can help reduce the chance that an unauthorized user will gain access to protected pages through a Web browser that a trusted user has left unattended.

Expiring Cookies After a Timeout Period

To have idle cookies expire after a timeout period:

1 Open the Web protection page.

2 In the Cookie expiration control panel, select **Cookies expire if not in use for specified time**.

3 In the **Expiration time** field, enter the number of minutes that you want an idle cookie to last. The maximum number of minutes you can enter is 1440 (one day).

4 Click **Apply**.

To increase the effectiveness of idle timeout cookies, instruct your tokenholders to enable the **Always update pages** option in their browsers. This will ensure that the cookies are refreshed accordingly. If the cookies are not refreshed from time to time, the ACE Server will not have a chance to update the cookies and tokenholders will be asked to authenticate before the cookies' timeout period expires.

{button ,JI(`SDCONTRL.HLP',`WEB_Domain_Cookies')}   Enabling Domain Cookies

{button ,JI(`SDCONTRL.HLP',`WEB_Distributing_Web_ID_Cookies')}   Distributing WebID cookies

Expiring Cookies Automatically After a Specified Time

To have cookies expire automatically after a specified time:

1 Open the Web protection page.

2 In the Cookie expiration control panel, select **Cookies expire always after specified time**.

3 In the **Expiration time** field, enter the number of minutes that you want each cookie to last. The maximum number of minutes you can enter is 1440 (one day).

4 Click **Apply**.

{button ,JI(`SDCONTRL.HLP',`WEB_Domain_Cookies')} Enabling Domain Cookies

{button ,JI(`SDCONTRL.HLP',`WEB_Distributing_Web_ID_Cookies')} Distributing WebID cookies

Enabling Domain Cookies

By default, WebID distributes cookies that are valid only on the Web server from which they were issued. However, you can issue cookies that are valid on multiple servers in a site domain by enabling the WebID Domain Cookie feature.

Be careful when you use this feature. Because domain cookies bypass a workstation's client activations in the ACE/Server database, tokenholders carrying a domain cookie from another server might gain access to information they are usually not allowed to see.

By using the Windows NT file permissions features, in conjunction with the ACE/Server's grouping and client activation capabilities, you can configure your server or domain to be highly selective about which SecurID-protected files it allows tokenholders to view.

Note: Security Dynamics does ***not*** support the Domain Cookies feature on machines which run on the DEC Alpha and IBM PowerPC microprocessors.

{button ,JI(`SDCONTRL.HLP',`Web_Domain_Cookies_Example')} Example

To enable domain cookies:

1 Open the Web protection page.

2 Select **Enable Domain Cookies** and **Enable WebID Feature Set**.

- If you enable the Domain Cookies feature, do not use shortcuts when referencing links to other servers in a DNS domain. In order for the Domain Cookies feature to work, you must use the fully qualified DNS domain name in your URLs.

3 In the **Domain Name** field, enter the World Wide Web DNS name of the domain over which you will distribute domain cookies (e.g., widgetsinc.com). See invalid Domain Name.

4 When you click **Manage Domain Secret**, you may

- Generate a domain secret
- Import a domain secret
- Export a domain secret

{button See Also,AL(`DomSecret',0,`',`')}

Domain Cookies Example

If you use the Windows NT file permissions features in conjunction with the ACE/Server's grouping and client activation capabilities, you can configure your server or domain to be highly selective about which SecurID-protected files it allows tokenholders to view.

In this example, you are posting your salespeople quarterly performance statistics in confidential URLs on the Web server ***Sales***, which has the Domain Cookies feature enabled. If you do not restrict the user access permissions on each of the ***Sales*** URLs, a tokenholder with a domain cookie issued on server ***Engineering*** can access server ***Sales*** and see the confidential URLs. To prevent this, restrict access to these directories by assigning "Read" permission only to the appropriate tokenholders.

Note: To set security permissions, select **File > Properties > Security** in the Windows NT Explorer application

Consult your Windows NT documentation or the ACE/Server user documentation for more information about these options.

{button See Also,AL(`DomSecret',0,`',`')}

Importing a Domain Secret

Once you have created a Domain Secret and placed it on a diskette you may import the Domain Secret onto each Web server machine. On each machine

1 Open the Web protection page.

2 Select **Enable Domain Cookies** and **Enable WebID Feature Set**.

Note: If you enable the Domain Cookies feature, do not use shortcuts when referencing links to other servers in a DNS domain. In order for the Domain Cookies feature to work, you must use the fully qualified DNS domain name in your URLs.

3 In the **Domain Name** field, enter the World Wide Web DNS name of the domain over which you will distribute domain cookies (e.g., widgetsinc.com). See invalid Domain Name.

4 Click **Manage Domain Secret**.

5 When the Manage Domain Secret dialog box opens, click **Import domain secret from other station**.

6 In the Select domain secret to import dialog box, select the domain secret file and click **Open**.

7 Enter the domain secret password and click **OK**.

8 In the Web protection page, click **OK**.

Note: After you have imported the domain secret to all the Web servers in the domain that have the Domain Cookies feature enabled, you should either store the floppy disk in a secure place or destroy it to ensure that the domain secret is never compromised. Security Dynamics recommends that you **NOT** store the domain secret file in a network directory where an unauthorized user might gain access to it.

{button See Also,AL(`DomSecret',0,`',`')}

Exporting a Domain Secret

To export a domain secret:

1 Open the Web protection page.

2 Select **Enable Domain Cookies** and **Enable WebID Feature Set**.

- If you enable the Domain Cookies feature, do not use shortcuts when referencing links to other servers in a DNS domain. In order for the Domain Cookies feature to work, you must use the fully qualified DNS domain name in your URLs.

3 In the **Domain Name** field, enter the World Wide Web DNS name of the domain over which you will distribute domain cookies (e.g., widgetsinc.com). See invalid Domain Name.

4 Click **Manage Domain Secret**.

5 When the Manage Domain Secret dialog box opens, click **Export domain secret for other stations**.

6 In the Choose file name to export the domain secret dialog box, select

- the destination drive where the diskette is located
- click **OK**

7 In the Enter Password for Domain Secret file dialog box

- Enter the password you will use when importing the domain secret on other stations.
- Press TAB and confirm the password.
- Click **OK** to close all open dialog boxes.

8 In the Web protection page, click **OK**.

Note: After you have imported the domain secret to all the Web servers in the domain that have the Domain Cookies feature enabled, you should either store the floppy disk in a secure place or destroy it to ensure that the domain secret is never compromised. Security Dynamics recommends that you **NOT** store the domain secret file in a network directory where an unauthorized user might gain access to it.

{button See Also,AL(`DomSecret',0,`',`')}

Ensuring that Every Connection is Secure

If you do not have a Secure Sockets Layer (SSL) on your Web server, you are leaving your SecurID-protected pages open to replay attacks. An unauthorized person can monitor an unsecured connection, intercept a tokenholder's PASSCODE or cookie, and then use the stolen object to access protected pages.

If you attempt to enable SecurID without SSL protection you will get an alert box telling you that the connection is not secure. Security Dynamics ***strongly*** recommends enabling SSL to ensure against replay attacks, but if you wish to bypass this security measure, leave the **Require secure connections to access protected pages** checkbox unmarked.

If you have any questions about SSL or how to obtain an SSL certificate from VeriSign, consult Chapter 5 of the Microsoft IIS online help or visit the VeriSign website at **http://www.verisign.com/microsoft/**.

To require all tokenholders to use SSL connections:

1 Open the Web ID properties page.

2 In the Connection security panel, select **Require secure connection to access protected pages**.

3 Click **Apply**.

{button ,JI(`SDCONTRL.HLP',`HIDD_Directories')}   Enabling Web Protection

Preventing Disk Caching of Protected Pages

When you browse a Web site, your browser stores copies of each page you visit in disk or memory cache. Each time you click the **Back** or **Forward** button, your browser loads the copy of the page that it saved, eliminating the time it would take to contact the server and reload the entire page.

If a tokenholder’s browser is left unattended, an unauthorized user can view pages that are stored in cache long after the tokenholder has quit his browsing session. WebID minimizes this security risk by allowing you to prevent tokenholders from disk caching protected pages. Pages that are cached in memory are not protected by this feature.

Note: Versions of the Microsoft Internet Explorer earlier than v 3.01 do not support this feature, even if you set the cache size to 0.

To prevent Web browsers from disk caching protected pages:

1 Open the Web protection page.

2 In the Connection security panel, select **Prevent caching of protected pages on clients**.

3 Click **Apply**.

{button ,JI(`SDCONTRL.HLP',`HIDD_Directories')} Enabling Web Protection

Modifying the Web Authentication Prompt

During installation, the ACE/Agent setup program copied the following HTML templates into the **%SYSTEMROOT%\system32\aceclnt** directory:

- **error.htm** - the page tokenholders see when a transmission error occurs during authentication.
- **flterror.htm** - the page tokenholders see when a filter loading error occurs.
- **newpin.htm** - the page that appears when a tokenholder's token is in New PIN mode; it allows a user to create his own PIN.
- **newpin1.htm** - the New PIN page that appears when a tokenholder is to receive an system-generated PIN.
- **newpin2.htm** - the New PIN page that appears when a tokenholder is allowed to decide whether she will create her own PIN or receive a system-generated PIN.
- **nextprn.htm** - the page that appears when a token is in Next Tokencode mode. A series of incorrect PASSCODEs during authentication puts a token into this mode. After a correct code is finally entered, the user will be prompted for another correct tokencode before being allowed access.
- **passcode.htm** - the WebID authentication prompt, where the tokenholder enters his username and PASSCODE.

These HTML templates can be edited to add custom greeting messages or graphics to the WebID authentication prompt and its companion pages.

All of the HTML template scripts (including the New PIN prompts and error pages) can be modified, so long as you do ***not*** alter the relative positions of the **%s** variables in the scripts. If you do, the authentication prompt will not be able to get information from the ACE/Server.

Note

- Editing the template files requires that you have a thorough understanding of the HTML markup language.
- When adding graphics files to the authentication prompt, be sure that the files are ***not*** loaded from a SecurID-protected directory. If these files are protected, the browser will not recognize them and will display them as broken image icon icons.

{button ,JI(`SDCONTRL.HLP',`Web_Modifying_the_Web_Authentication_Prompt_text')} Modifying the Web Authentication Prompt Text

{button ,JI(`SDCONTRL.HLP',`WEB_Adding_a_Custom_Graphic')} Adding a Custom Graphic to the WebID Authentication Prompt

Modifying the Web Authentication Prompt Text

1 Using an HTML text editor or the Notepad application, open the passcode.htm file in the **\system32\aceclnt** directory. The source HTML for the authentication prompt appears.

2 Delete the text in the <TITLE>, <H1>, or <HR> tag near the top of the page and enter your new heading or body text in its place.

For example, the tag **<H1>Welcome to Widgets, Inc.</H1>** produces the Welcome to Widgets, Inc. web page

3 Save and close the file. The Web authentication prompt will now display the new greeting to Web users.

{button ,JI(`SDCONTRL.HLP',`WEB_Adding_a_Custom_Graphic')} Adding a Custom Graphic to the WebID Authentication Prompt

{button ,JI(`SDCONTRL.HLP',`WEB_Modifying_the_Authentication_Prompt_Inteface')} Modifying the Authentication Prompt Interface

Adding a Custom Graphic to the WebID Authentication Prompt

1 Using an HTML editor or the Notepad application, open the passcode.htm file from the **\system32\aceclnt** directory.

2 Decide where you want the image to be placed on the page, then insert an <IMG> tag in passcode.htm pointing to the image file. For example, the line **<IMG SRC="/images/sherlok.gif" ALIGN="left">**, when placed below the <H1> tag, adds the image to the Welcome to Widgets, Inc. web page.

Note: The image file that you point to in the SRC path must be in an unprotected directory.

3 Save and close the file. The Web authentication prompt interface page will now display the new graphic.

{button ,JI(`SDCONTRL.HLP',`WEB_Modifying_the_Authentication_Prompt_Inteface')} Modifying the Authentication Prompt Interface

{button ,JI(`SDCONTRL.HLP',`Web_Modifying_the_Web_Authentication_Prompt_text')} Modifying the Web Authentication Prompt Text

Configuring Remote-Access Computers

Although no ACE/Agent software is installed on remote dial-in PCs, these computers must be configured to work with the SecurID-protected Windows NT that users will dial-in to.

{button ,JI(`SDCONTRL.HLP',`Web_Modifying_the_Web_Authentication_Prompt_text')} Configuring a remote PC running Windows NT 4.0

{button ,JI(`SDCONTRL.HLP',`Configuring_RAS_on_a_PC_running_Windows_NT_v_3.51')} Configuring a remote PC running Windows NT 3.51

{button ,JI(`SDCONTRL.HLP',`Configuring_RAS_on_a_PC_running_Windows_v_3.11')} Configuring a remote PC running Windows for Workgroups 3.11

{button ,JI(`SDCONTRL.HLP',`Configuring_RAS_on_a_PC_running_Windows_95')} Configuring a remote PC running Windows 95

How to Dial-In to a Protected ACE/Agent from a Remote PC

Dialing-in to a SecurID-protected ACE/Agent machine varies slightly from conventional RAS authentication process.

{button ,JI(`SDCONTRL.HLP',`Dialing_in_from_a_remote_PC_running_Windows_NT_v_4.0')} Dialing-in to a protected ACE/Agent machine from a PC running Windows NT 4.0

{button ,JI(`SDCONTRL.HLP',`Dialing_in_from_a_remote_PC_running_Windows_95')} Dialing-in to a protected ACE/Agent machine from a PC running Windows 95

{button ,JI(`SDCONTRL.HLP',`Dialing_in_from_a_remote_PC_running_Windows_Nt_v3.51_or_Windows_v_3.11')} Dialing-in to a protected ACE/Agent machine from a PC running Windows NT 3.51 or Windows for Workgroups 3.11

{button See Also,AL(`DISTAUTH;ENABLREMAC',0,`',`')}

Configuring a Remote PC running Windows NT 4.0

Note: RAS configuration instructions are also available in Microsoft Word v 6.0 format for you to distribute to remote users. This file, called **ras_conf.doc**, was copied into your **\system32\aceclnt** directory during installation.

To edit the RAS configuration on a remote computer running Windows NT 4.0:

1 From the desktop, open My Computer.

2 Double-click the Dial-up Networking icon.

3 In the window that opens, click and hold on the More button. A menu pops up. From this menu, select Edit Entry and Modem Properties.

4 Click the **Security** tab.

5 Select the **Accept any authentication including clear text** radio button.

6 Click the **Script** folder tab.

7 Select the **Pop up a terminal window** radio button.

8 Repeat these steps for each SecurID-protected phone book entry.

RAS Configuration on a Remote PC running Windows NT 3.51

Note: RAS configuration instructions are also available in Microsoft Word v 6.0 format for you to distribute to remote users. This file, called **ras_conf.doc**, was copied into your **\system32\aceclnt** directory during installation.

To edit the RAS configuration on a PC running Windows NT 3.51:

1 Within Windows NT on the remote PC, start the Remote Access program.

2 Select the Entry Name that connects the PC to the SecurID-protected Windows NT machine.

3 Click **Edit**.

4 If the third button down on the right hand side says **<<Basic**, you are in the right place. If the button says **Advanced>>**, click the button to display the correct screen.

5 Click **Security**.

6 For the **After dialing** setting, choose **Terminal**.

7 Click **OK** to confirm the setting.
The Phone Book dialog box re-displays.

8 Repeat these steps for each SecurID-protected Entry Name.

Configuring a Remote PC Running Windows for Workgroups 3.11

Note: RAS configuration instructions are also available in Microsoft Word v 6.0 format for you to distribute to remote users. This file, called **ras_conf.doc**, was copied into your **\system32\aceclnt** directory during installation.

To edit the RAS configuration on a PC running Windows for Workgroups 3.11:

1 Within Windows for Workgroups 3.11 on the client PC, start the Remote Access program.

2 Select the Entry Name that connects the PC to the SecurID-protected Windows NT machine.

3 Click **Edit**.

4 If the third button down on the right hand side says **<<Basic**, you are in the right place. If the button says **Advanced>>**, click the button to display the correct screen.

5 Select **Switch.**

6 For the **Post-connect script** setting, choose **Terminal**.

7 Click **OK** to confirm the setting.
The Phone Book dialog box re-displays.

8 Repeat these steps for each SecurID-protected Entry Name.

Configuring a Remote PC Running Windows 95

Note: RAS configuration instructions are also available in Microsoft Word v 6.0 format for you to distribute to remote users. This file, called **ras_conf.doc**, was copied into your **system32\aceclnt** directory during installation.

To edit the RAS configuration on a PC station running Windows 95:

1. Within Windows 95 on the PC, click the **Dial-Up Networking** icon.
2. Select the icon that connects the PC to the SecurID-protected Windows NT machine.
3. Hold down the right mouse button and select **Properties**.
4. Make sure the **Telephone number**, **Country code**, **Connect using**, and other fields are correct, and then click **Configure**.
5. In the header bar, click the **Options** tab.
6. Check both **Bring up terminal window after dialing** and **Display modem status**.
7. Click **OK**.
8. Click **OK** again to exit.
9. Repeat these steps for each SecurID-protected Dial-Up Connection.

Dialing-In from a Remote PC Running Windows NT 4.0

Note: Remote dial-in instructions are available in Microsoft Word v 6.0 format for you to distribute to remote users. This files, called **ras_card.doc** and **ras_pin.doc**, were copied into your **\system32\aceclnt** directory during installation.

To dial-in from a remote computer running Windows NT 4.0:

1. At the remote computer, open My Computer and double click the **Dial-Up Networking** icon.
2. From the Phonebook entry field, select the server that you want to dial in to and click **Dial**.
3. Enter your password and domain information just as you usually would. Click **OK**.
4. You will be prompted for a PASSCODE. Follow the authentication instructions for your token type, and press RETURN.

   Your remote computer is now a peer node in your Windows NT network, and you are a SecurID-authenticated user.

   If you are not required to enter a PASSCODE, **PASSCODE Not Required** will be displayed.

6. Click the **Continue** button and you will gain access.

{button See Also,AL(`DISTAUTH',0,`',`')}

Dialing-In from a Remote PC Running Windows 95

Note: Remote dial-in instructions are available in Microsoft Word v 6.0 format for you to distribute to remote users. This files, called **ras_card.doc** and **ras_pin.doc**, were copied into your **\system32\aceclnt** directory during installation.

To dial-in from a remote PC running Windows 95:

1 At the remote computer, double click **Dial-Up Networking** icon.

2 Double click **office**.

3 Click **Connect**.

4 A terminal screen displays asking for your username. If the screen is blank, press RETURN and the **Username** prompt will display.

5 Enter your username and press RETURN.

You may use the BACKSPACE key to delete any mistyped characters. In the Username field, each deletion will be automatically followed by a linefeed.

6 At the DOMAIN prompt, either press RETURN or follow the instructions for your particular Windows NT system.

7 Following the authentication instructions for your token type, complete the **Passcode** field and press RETURN.

Your remote computer is now a peer node in your Windows NT network, and you are a SecurID-authenticated user.

If you are not required to enter a PASSCODE, **PASSCODE Not Required** will be displayed.

8 Click the **Continue** button and you will gain access.

{button See Also,AL(`DISTAUTH',0,`',`')}

Dialing-in from a Remote PC Running Windows NT 3.51 or Windows 3.11

Note: Remote dial-in instructions are available in Microsoft Word v 6.0 format for you to distribute to remote users. This files, called **ras_card.doc** and **ras_pin.doc**, were copied into your **\system32\aceclnt** directory during installation.

To dial-in from a remote PC running Windows NT 3.51 or Windows for Workgroups 3.11:

1 At the dial-in computer, select **Remote Access**, the **Entry Name**, and **Dial**.

2 A terminal screen displays asking for your username. If the screen is blank, press RETURN and the **Username** prompt will display.

3 Enter your username and press RETURN.

You may use the BACKSPACE key to delete any mis-typed characters. In the Username field, each deletion will be automatically followed by a linefeed.

4 At the **DOMAIN** prompt, either press RETURN or follow the instructions for your particular Windows NT system.

5 Follow the authentication instructions for your token type, and press RETURN.

Your remote client computer is now a peer node in your Windows NT network, and you are a SecurID-authenticated user.

If you are not required to enter a PASSCODE, **PASSCODE Not Required** will be displayed.

6 Click the **Done** button and you will gain access.

{button See Also,AL(`DISTAUTH',0,`',`')}

Component Status Messages in the ACE/Agent Control Panel

The following messages appear in the Component Status panel of the Main ACE/Agent properties page.

Local: Security features available
[or] Remote: Security Features Available
[or] Web: Security Features Available

Remote: NT/RAS not properly installed

Web: IIS not properly installed

If you think one of these ACE/Agent components should be available on your system but is not, click the appropriate button below to double-check your system’s configuration.

{button ,JI(`SDCONTRL.HLP',`WEB_New_Local_protection_requirements')} Local protection requirements

{button ,JI(`SDCONTRL.HLP',`WEB_New_Remote_access_protection_requirements')} Remote access protection requirements

{button ,JI(`SDCONTRL.HLP',`WEB_New_Web_protection_requirements')} Web protection requirements

Using clntchk to View sdconf.rec

If the ACE/Agent for Windows NT machine and the ACE/Server machine do not have identical copies of the **sdconf.rec** file, communications between the two will be impossible.

To view the Windows NT client machine’s copy of sdconf.rec:

1 In a Command Prompt window, change to the **\system32** directory, which is subdirectory of the machine’s %SYSTEMROOT% (.usually named **\windows** or **\winnt**).

2 Type **clntchk**

If the **sdconf.rec** file has been copied correctly, output similar to the following will be produced. Your ACE/Server administrator will know whether these settings are appropriate.

```
configuration file is version 3
The configuration structure is 356 bytes long
The ACE/Server limits are:
Client retry is 5 times and the Client timeout is 3 seconds
There is a master and a slave configured
DES has been disabled with sdconfig
Duress mode has been disabled by sdconfig
Addresses are configured in
Number of bad Cardcodes is 3
Number of bad PINs is 3
master = server1
The address of the master ACE/Server is 10.10.10.10
slave = server2
The address of the slave ACE/Server is 10.10.10.10
The service name is securid
acmprotocol = udp
acm_port is 5500
```

If the output values contain garbage characters, the **sdconf.rec** file has been corrupted. Ask the administrator of the ACE/Server for a new copy.

Authentication Messages

The following are messages that a user might get during authentication. Click the appropriate message for more information.

Cannot load ACE/Agent DLL

ACE/Agent initialization failed

Unexpected error from ACE/Agent

Windows NT Event Viewer Messages

The following messages appear in the Windows NT Event Viewer System Log.

The user ***username*** has connected and been authenticated on port ***portnumber***

The user ***server\username*** connected on port ***portnumber*** on ***date*** at ***time*** and disconnected on ***date*** at ***time***

[or] The user ***server\username*** disconnected from port ***portnumber***.

[or] The user was authenticated as ***username1*** by the third-party security host module but was authenticated as ***username2*** by the SDRAS security host, and has been disconnected

The user connected to port ***portname*** has been disconnected because an internal authentication error occurred in the third–party security module. The error code is in the data.

[or] The user connected to port ***portname*** has been disconnected because of authentication timeout.

[or] The user ***username*** has connected and failed to authenticate with a third-party security device on port ***portname***. The line has been disconnected.

Event Detail Messages

Click the appropriate button to view the messages that the ACE/Agent posts in the Event Viewer application’s Event Detail.

{button ,JI(`SDCONTRL.HLP',`Category_ACE_Client')} Category **"ACE/Agent"**

{button ,JI(`SDCONTRL.HLP',`Category_Local')} Category **"Local"**

{button ,JI(`SDCONTRL.HLP',`Category_Remote')} Category **"Remote"**

{button ,JI(`SDCONTRL.HLP',`Category_Local_or_Remote')} Category **"Local *or* Remote"**

{button ,JI(`SDCONTRL.HLP',`Category_WebID')} Category **"WebID"**

Category "ACE/Agent"

Any of the following messages may appear in the Windows NT Event Detail under the category “ACE/Agent.” Click the message text for more information.

ACE/Server is not responding. Run CLNTCHK to verify port and IP address of ACE/Server

File not found: **sdconf.rec**

File incorrect size: **sdconf.rec**

Failed to create event
[or] Failed to create Semaphore
[or] Failed to create Thread
[or] Out of memory during initialization in SecurID Authentication

Failed to find required service WINSOCK

Network Timeout—ACE/Server was responding but has now stopped.

Can’t create socket during initialization in SecurID Authentication.

Category "Local"

The following messages appear in the Windows NT Event Detail under the category “Local.”

File not found: **aceclnt.dll**

User ***username***: Reserve password accepted.

User ***username*** not in SDLOCAL group. PASSCODE not required.

User ***username***: PASSCODE required. All users challenged.

Category "Remote"

The following messages appear in the Windows NT Event Detail under the category “Remote.”

Note: In all SDRAS messages, the ***username*** may be “No Carrier” or some meaningless entry. Such an entry indicates that the user hung up before authenticating, clicked on **Done** or **Continue** too early, or never set up the “After Dialing” terminal box.

User I/O Timeout—User took too long to respond.

User ***username***: PASSCODE required. All users challenged.

User ***username*** not in SDREMOTE group. PASSCODE not required.

User ***username***: Not found. User challenged for PASSCODE.

User ***username***: Domain not found. User challenged for PASSCODE.

User ***username***: Access denied. Attempt to use invalid handle. Closing connection.

[Multiple instances of] PASSCODE Incorrect.

The user connected to port COM# has been disconnected because an internal authentication error has occurred in third party security module. The error code is in the data.

Category "Local" or "Remote"

Many messages are the same for local and remote users. The “Source” entry in the Event Viewer and Event Detail indicates which program registered the event.

User ***username***: PASSCODE accepted.

User ***username***: cancelled out of “SecurID Authentication” routine.

User **<blank>** cancelled out of “SecurID Authentication” routine.

User ***username*** cancelled out of “New PIN” routine.

User ***username***: cancelled out of “Next Tokencode” routine.

User ***username***: ACCESS DENIED. ATTEMPT 1
[or] User ***username***: ACCESS DENIED. ATTEMPT 2
[or] User ***username***: ACCESS DENIED. ATTEMPT 3

User ***username***: New PIN accepted.

User ***username***: New PIN rejected.

User ***username***: Successfully logged on with Next Tokencode.

User ***username***: ACCESS DENIED. Next Tokencode failed.

User ***username***: ACCESS DENIED. Server signature invalid.

Category "WebID"

The following messages appear in the Windows NT Event Detail under the category “WebID.”

A

ACECheck processing error for userid ***username***

ACEClose processing error ***errornumber***

ACENext processing error for userid ***username***

ACEPin processing error for userid ***username*** ***.***

C

Cookie rejected. Cached client info does not match

Cookie rejected. Cookie failed MD5 test

Cookie rejected. Expired cookie

Could not find HTML template in Registry

Could not initialize Cookie Cache

Could not initialize ACE/Agent

Could not open registry key ***keyname***
[or] Could not create key ***keyname***.
[or] Could not delete registry key ***keyname***.
[or] Could not enumerate registry keys ***keynames***.
[or] Could not enumerate registry values.
[or] Could not set value ***valuename***.

Could not open HTML template ***filename***

Could not read HTML template ***filename***

Could not resolve hostname ***hostname***

Could not query value valuename

F

Failed authentication for userid ***username***

O

Out of memory in ***functionname***

N

New PIN accepted for userid ***username***

New Pin rejected for userid ***username***

New PIN requested from userid ***username***

Next code accepted for userid ***username***

Next code rejected for userid ***username***

Next code requested from userid ***username***

No cookie or corrupted information

R

Remote authentication given for userid ***username***

Remote authentication received deny for userid ***username***

Remote cookie rejected. Cookie failed MD5 test.

Remote authentication denied for userid ***username***

Cannot load ACE/Agent DLL

Test cannot find **aceclnt.dll** in the **\system32** directory. You must reinstall ACE/Agent software from the Microsoft Internet Information Server v 4.0 distribution media.

Unexpected error from ACE/Agent

The value returned by the ACE/Server is not valid. Reinstall ACE/Agent for Windows NT v 4.0 from the Microsoft Internet Information Server v 4.0 distribution media. If the problem persists, check your hardware.

The user *username* has connected and been authenticated on port *portnumber*.

A normal (authenticated) ACE/Agent-Server connection occurred

The user was authenticated as *username1* by the third-party security host module but was. . .

The user has been disconnected because his logon name and the Security Dynamics authentication name are not the same

The user server\username connected on port *portnumber* on date at time and disconnected on date at time. . .

A normal ACE/Agent disconnection has occurred.

The user connected to port portname has been disconnected. . .

There is a problem with SecurID authentication. See the Event Detail topic for more specific information.

ACE/Server is not responding.

Most likely there is some network communications problem between the ACE/Server and the ACE/Agent. Either that or the server cannot be found (because the IP address is wrong, for example), or the aceserver daemon is not running.

File not found: sdconf.rec

The **sdconf.rec** file is not in the **\system32** directory. It was either removed or never copied from the ACE/Server. Ask the ACE/Server administrator for a new copy of **sdconf.rec**.

File incorrect size: sdconf.rec

It is likely that the **sdconf.rec** file was not copied in binary mode. As the administrator for a new copy.

Failed to create event

These are internal errors. The machine may not have enough free resources to add SecurID authentication. Consider moving service(s) from this machine to another one.

Failed to find required service WINSOCK

The Windows socket interface was not found. Check the event log to find out if there is a problem with WINSOCK. Ensure that TCP/IP has been enabled on the machine.

Network Timeout—ACE/Server was responding but has now stopped.

Check to make sure the ACE/Server process is running on the server Check for a network problem such as a router malfunction or unplugged network cable.

Can’t create socket during initialization in SecurID Authentication.

Socket services may not have started. Check the event log to find out if there is a problem with the network card or the TCP/IP services.

ACE/Server is not responding. Run CLNTCHK to verify port and IP address of ACE/Server

Most likely there is some network communications problem between the ACE/Server and the ACE/Agent. Either that or the ACE/Server cannot be found (because the IP address is wrong, for example), or the **aceserve**r daemon is not running.

File not found: aceclnt.dll

Software may have been installed incorrectly or **aceclnt.dll** may have been deleted. Re-install the ACE/Agent software from the Microsoft Internet Information Server CD-ROM to correct the problem.

User *username*: Reserve password accepted.

User was asked for the reserve password and entered it correctly.

User *username* not in SDLOCAL group. PASSCODE not required.

User was not prompted for a PASSCODE. If you wish to challenge every local user who attempts to access the machine, enable the **Challenge All Users** option on the Local properties page of the ACE/Agent Control panel.

User I/O Timeout—User took too long to respond.

The Windows NT system timed out after waiting for a response from the user.

User *username*: PASSCODE required. All users challenged.

The Challenge All Users option is enabled.

User *username* not in SDREMOTE group. PASSCODE not required.

Challenge All switch is not on, and user is not in SDREMOTE group.

User *username*: Not found. User challenged for PASSCODE.

The user unknown to the system, but the user will be challenged for PASSCODE anyway.

User *username*: Domain not found. User challenged for PASSCODE.

The user may have entered the domain name incorrectly. He will be challenged for PASSCODE.

User *username*: Access denied. Attempt to use invalid handle. Closing connection.

An internal error occurred. If the message reoccurs, call the Customer Services Solutions Center.

[Multiple instances of] PASSCODE Incorrect.

If you have both RAS protection and Web protection enabled on a machine, the ACE/Agent could be sending the encrypted RAS authentication PASSCODE through the wrong IP address. Check the IP addresses of each service and the client nodes on the ACE/Server for possible addressing errors.

The user connected to port COM# has been disconnected because an internal authentication error. . .

The connection to the port has been lost due to an I/O flow error. Make sure that the Hardware Flow Control option is enabled in the Modem Configure Settings page of the RAS Control Panel.

Also make sure that the port speed setting in the RAS Control Panel is the same as the setting in the Port Control Panel.

User *username*: PASSCODE accepted.

Challenge All Users option is not on, and user is in the SDREMOTE group.

User *username*: cancelled out of “SecurID Authentication” routine.
The user cancelled after entering a ***username***.

User <blank> cancelled out of “SecurID Authentication” routine.

User cancelled without entering a ***username***.

User *username* cancelled out of “New PIN” routine.
User cancelled the authentication attempt.

User *username*: cancelled out of “Next Tokencode” routine.

The user cancelled.

User *username*: ACCESS DENIED. ATTEMPT 1.

Check the ACE/Server Activity Log.

User *username*: New PIN accepted.

The user’s New PIN was verified.

User *username*: New PIN rejected.

PIN was rejected by ACE/Server. User will need to re-authenticate to set the PIN. Check the ACE/Server Activity Log.

User *username*: Successfully logged on with Next Tokencode.

Next Tokencode accepted by ACE/Server and access granted to the user.

User *username*: ACCESS DENIED. Next Tokencode failed.

User must attempt to authenticate again.

User *username*: ACCESS DENIED. Server signature invalid.

Indicates that the identity of the ACE/Server could not be verified by the client. If you see this message, call the Security Dynamics Solutions Center.

ACECheck processing error for userid *username*.

If the **ACECheck** function returns an error, an ACE/Server timeout or some other communications error has occurred.

ACEClose processing error *errornumber*.

If the **ACEClose** function returns an error, an ACE/Server timeout or some other communications error has occurred.

ACENext processing error for userid *username*.

If the **ACENext** function returns an error, an ACE/Server timeout or some other communications error has occurred.

ACEPin processing error for userid *username*

If the **ACEPin** function returns an error, an ACE/Server timeout or some other communications error has occurred.

Cookie rejected. Cached client info does not match.

If a user is using more than one workstation, this message will appear each time he switches from one workstation to another.)

Cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the Web server with a bogus WebID cookie.

Cookie rejected. Expired cookie.

A WebID cookie has expired in response to the timeout values defined in the Web protection properties page.

Could not find HTML template in Registry.

A serious registry corruption has occurred. You must reinstall the ACE/Agent software.

Could not initialize Cookie Cache

A memory error has occurred within an internal function. Your Web server may be overloaded; you may need to purchase more physical memory.

Could not initialize ACE/Agent.

Will be preceded by a number of ACE/Agent error messages, such as "Cannot find **sdconf.rec**." Try reinstalling the **sdconf.rec** file.

Could not open registry key keyname

A serious registry corruption has occurred. You must reinstall the ACE/Agent software.

Could not open HTML template filename.

The HTML template file is missing. check the **\system32\acecInt** directory to make sure the file is still there. If not, you must copy the template from the Microsoft Internet Information Server v 4.0 distribution media.

Also check the security settings for the file. Make sure the account that the Web server is running as has Full Access privileges to the HTML file.

Could not read HTML template filename.

The HTML template file is missing. check the **\system32\aceclnt** directory to make sure the file is still there. If not, you must copy the template from the Microsoft Internet Information Server v 4.0 distribution media.

Could not resolve hostname *hostname*

The DNS function of the Web server is configured incorrectly. Prevents the use of domain cookies until the configuration is corrected.

Could not query value *valuename*

If you have enabled the Domain Cookies feature without setting a domain secret, you might get a ***valuename*** DomainData, followed by "Domain cookies are disabled."

Failed authentication for userid *username*

The ACE/Server did not grant the user access; the most common causes for this are wrong ***username*** or an invalid PASSCODE.

Out of memory in *functionname*

A memory error has occurred within an internal function. Your Web server may be overloaded; you may need to purchase more physical memory.

New PIN accepted for userid *username*

The ACE/Server verified the tokenholder’s new PIN.

New Pin rejected for userid *username*

PIN was rejected by ACE/Server. User will need to re-authenticate to set PIN. Check Activity Log on ACE/Server.

New PIN requested from userid *username*

The ACE/Server has prompted the tokenholder to create his own PIN or receive a system-generated PIN.

Next code accepted for userid *username*

Next Tokencode accepted by ACE/Server and access granted.

Next code rejected for userid *username*

User must attempt to authenticate again.

Next code requested from userid *username*

The user’s token was in Next Tokencode mode and the ACE/Server asked for the second tokencode.

No cookie or corrupted information

This message will appear each time a new user logs on to the Web server.

Remote authentication given for userid *username*

Another Web sever within the DNS domain has requested authentication of user ***username*** with a domain cookie and was given access.

Remote authentication received deny for userid *username*

A Web server requesting authentication of a domain cookie was rejected.

Remote cookie rejected. Cookie failed MD5 test.

An unauthorized user has attempted to access the Web server with a bogus WebID domain cookie.

Remote authentication denied for userid *username*

Another Web sever within the DNS domain has requested authentication of user ***username*** with a domain cookie and was not given access.

Also check the security settings for the file. Make sure the account that the Web server is running as has Full Access privileges to the HTML file.

ACE/Agent initialization failed

ACE/Agent cannot make the connection to the ACE/Server. Make sure the ACE/Server and network are operational and that all network interface cards and cables are properly installed and in good condition.

Local: Security Features Available

The machine meets the system and software requirements for the named security features.

Remote: NT/RAS not available

The machine does not meet one or more of the system or software requirements needed to enable protection of RAS connections. Go to "Remote access protection requirements" and make sure the machine meets all the requirements.

Web: IIS not available

The machine does not meet one or more of the system or software requirements needed to enable the WebID feature set. Go to "Web protection requirements" and make sure the machine meets all the requirements.

Enable Remote Access Security: check this option if you want remote users to be challenged for a PASSCODE. To challenge

- all users in SDREMOTE and Domain SDREMOTE, select **Challenge All Users**
- some remote dial-in users, add them to the SDREMOTE group and do not select **Challenge All Users**.

Disable Domain Prompt: Check this option if you do not want to your remote users to see the DOMAIN: prompt during login. If this option is set, the **Default Domain** will be used.

At login, the user will only see the USERNAME: and PASSCODE: prompts. After the user enters a valid PASSCODE, the user will be authenticated to the default domain.

Default Domain: Enter the name of the Domain that your remote users belong to.

Challenge all Users: when this option is selected, all users in all groups are challenged for a PASSCODE.

- When you PASSCODE-challenge all local access users, you should always set a reserve password. Creating a reserve password will enable users to log onto their machines if there is an interruption in network service.

OK closes the open dialog and save any changes you have made.

Cancel closes the open dialog without saving any of the changes you have made.

Enable WebID Feature Set: activates the fields on the Web protection page.

Enable Domain Cookies: enables cookies for a World Wide Web DNS domain. Do not use shortcuts when referencing links to other servers in a DNS domain. In order for this feature to work, you must use the fully-qualified DNS domain name in your URLs. See Domain Cookies.

Domain Name: enter the DNS name of the domain over which you will distribute domain cookies. For example: widgetsinc.com

Cookies expire if not used for specified time: When this option is checked, a cookie that has been idle for an administrator-defined timeout period will expire during a browsing session.

- In the **Expiration time** field enter the number of minutes that will elapse before the cookie expires. The maximum number is 1440 minutes (one day).

Cookies expire always after specified time: when this option is checked, a cookie will automatically expire after an administrator-defined time period even if it is in use during a browsing session.

- In the **Expiration time** field enter the number of minutes that will elapse before the cookie expires. The maximum number is 1440 minutes (one day).

Expiration time: enter the number of minutes that will elapse before the cookie expires. The maximum number is 1440 minutes (one day).

Require secure connection to access protected pages: enables Secure Sockets Layer (SSL) protection of your Web pages. Security Dynamics strongly recommends that you enable SSL to ensure against replay attacks. See the Microsoft IIS documentation for information about how to order an SSL certificate from Versign Corporation.

Prevent caching of protected pages on clients: when you select this option, protected pages are not stored on client PCs. This feature will not protect pages that are already stored in memory. This feature is available only for Netscape Navigator v 2.0 or later browsers.

Select files to secure: Click this button to display the WebID file protection page. You can choose to protect the entire server or individual directories and files on the server.

- The preferred method is to protect the entire directory that contains the file. When you protect a directory, any files or subdirectories you add to the directory later are protected automatically.
- Protecting individual files is not as efficient as protecting specific directories. When you protect individual files, you must enable protection on each new file you add to a directory, which might result in some files being overlooked and left unprotected.

Test authentication with ACE/Server: click this button to verify that the ACE/Agent software has been correctly implemented. You do not need to restart Windows NT to test authentication.

Uninstall of ACE/Agent for Windows NT: click this button to uninstall the ACE/Agent for Windows NT software.

Local Component Status: indicates if ACE/Server PASSCODE protection is available to be activated on local access accounts. The default status is Security Features Available. If ACE/Server protection is not available, the Local tab does not appear in the ACE/Agent Control Panel.

Remote Component Status: indicates if ACE/Server PASSCODE protection is available to be activated on remote access accounts. The default status is Security Features Available. To change this option, you must re-install the ACE/Agent for Windows NT. If ACE/Server protection is not available, the Remote tab does not appear in the ACE/Agent Control Panel.

Enable Logon Greeting: Check this option if you want your remote users to see a custom logon greeting when they are prompted for their username and PASSCODE. Type your custom greeting in the scrollable white box below the **Enable Logon Greeting** checkbox.

Do not resolve username in Event Log messages: This option is only available if you have enabled the **Challenge All Users** option.

Check this option if you do ***not*** want the Windows NT Event Log to resolve usernames when users log on.

In large Windows Domains, checking this option helps to speed up the logon process. However, the ACE/Agent records the username as “N/A” in the Windows NT Event Log, which will prevent you from filtering events by user. (The username is recorded in the Event Detail for each logon, but only in text form.)

Custom greeting text box: Type your custom Logon Greeting in this space. This is the greeting that users will see when they dial in to the protected ACE/Agent.

For example, if your company is called Widgets, Inc., you could display the following greeting to your users:

```
Welcome to Widgets, Incorporated! Please enter your network username and SecurID
PASSCODE below.
```

The greeting can be up to 1000 characters long.

Web Component Status: indicates if ACE/Server protection is available to be activated on World Wide Web accounts. The default status is Security Features Available. If ACE/Server protection is not available, the Web tab does not appear in the ACE/Agent Control Panel.

Enable Local Access Security: check this option if you want local users to be challenged for a PASSCODE. When you check this option, the other fields on the Local properties page are activated. If you wish to challenge

- all local users, select **Challenge All Users**
- some local users, add them to the SDLOCAL group and Domain SDLOCAL and do not select **Challenge All Users**

If you deselect **Enable Local Access Security** and click the **Apply** button, the **Reserve Password** is cleared.

Enable Screen Saver Security: check this option to have users reauthenticate every time their desktop screen saver activates. This option only takes effect if

- screen saver password protection is available on the Windows NT machine
- password protection has been enabled through the Desktop Control Panel application

Enable Reserve Password: check this option if you have selected **Challenge All Users**. Creating a reserve password will enable users to log onto their machines if there is an interruption in network service.

The reserve password should be changed after each use. If you enable the Reserve Password option and tell it to a user, Security Dynamics recommends that you change it as soon as the user logs onto the system.

To test that the Reserve Password is enabled

1 Disconnect the network connection

2 Log off the network

3 Log back onto the network

Reserve Password: enter the reserve password. The password is case sensitive and must include

- at least one number
- at least one letter
- 6 to 12 characters

Confirm Password: enter the reserve password.

Generating a Domain Secret

To create a Domain Secret:

1. Open the Web protection page.
2. Select **Enable Domain Cookies** and **Enable WebID Feature Set**.
   - If you enable the Domain Cookies feature, do not use shortcuts when referencing links to other servers in a DNS domain. In order for the Domain Cookies feature to work, you must use the fully qualified DNS domain name in your URLs.
3. In the **Domain Name** field, enter the World Wide Web DNS name of the domain over which you will distribute domain cookies (e.g., “widgetsinc.com”). See invalid Domain Name.
4. Click **Manage Domain Secret**.
5. When the Manage Domain Secret dialog box appears
   - click **Generate new Domain Secret for this station**
   - click **OK**
6. You have now created a Domain Secret.
   - Security Dynamics recommends that you store the domain secret on a removable diskette. You may export the secret to a floppy diskette now or at a later time.

{button See Also,AL(`DomSecret',0,`',`')}

Domain Password

1. In the **Password** field, type a Domain Secret password that has at least six characters.
2. Re-type the new password in the **Confirm** field.
3. Click **OK**.

Password Confirm: Type the new Domain Secret password to unlock the file.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

No additional help available for this topic.

Invalid Domain Name error message: enter the correct name for this PC in the DNS Configuration dialog box.

1 In the Windows NT Control panel, double-click the Networks icon.
2 In the Network Settings dialog box, select TCP/IP protocol as the Installed Network Software and click **Configure**.
3 In the TCP/IP Configuration dialog box, click **DNS**.
4 In the DNS Configuration dialog box, enter a name in the **Domain Name** field. For example:
   widgets.com
5 Click **OK**.

No additional help available for this topic.

No additional help available for this topic.

Generate new Domain Secret for this station: Click this button to create a new Domain Secret. This Domain Secret serves as a transferable cookie that is valid on multiple servers in a site domain.

Import domain secret from other station: Click this button to import a domain secret file. The domain secret is added to the machine’s system configuration. It is not copied onto the machine’s hard disk.

- After you have imported the domain secret to all the Web servers in the domain that have the Domain Cookies feature enabled, you should either store the floppy disk in a secure place or destroy it to ensure that the domain secret is never compromised.
- Security Dynamics recommends that you do NOT store the domain secret file in a network directory where an unauthorized user might gain access to it.

Export domain secret from another machine: Click this button to copy a domain secret onto a removable diskette.

- Store the floppy disk in a secure place or destroy it to ensure that the domain secret is never compromised.
- Security Dynamics recommends that you do NOT store the domain secret file in a network directory where an unauthorized user might gain access to it.

Select files to secure: You can browse the contents of the server by double-clicking directory icons. To enable Web protection

- point to the files or directories you wish to SecurID-protect
- click the right mouse button

Manage Domain Secret: Click this button to generate a new domain secret, or to import or export an existing domain secret.

Selecting a Domain Secret File to Import

1. In the Manage Domain Secret dialog box, click **Import Domain Secret from other station**.
2. Click **OK**.
3. In the Select domain secret file to import dialog box, highlight the name of the domain secret file in the **File Name** field.
4. Click **OK**.
5. In the Enter Password to Unlock the File dialog box, enter the Password you created for the domain secret.
6. Click **OK**.
7. The new domain secret will not take effect until you restart the World Wide Web service from the Internet Service Manager.

{button See Also,AL(`DomSecret',0,`',`')}

Selecting a Domain Secret File to Export

In the Manage Domain Secret dialog box, click **Export Domain Secret for other stations**.

1 Click **OK**.

2 In the Choose file name to export the domain secret dialog box, highlight the name of the domain secret file in the **File Name** field.

3 Select the path of the destination diskette.

4 Click **OK**.

5 In the Enter Password for Domain Secret File dialog box, enter the password you created for the domain secret.

6 Press TAB and confirm the password.

7 Click **OK**.

8 The new domain secret will not take effect until you restart the World Wide Web service from the Internet Service Manager.

{button See Also,AL(`DomSecret',0,`',`')}

registry
The Windows NT registry is a directory tree that holds system, user, and application configuration information.

ACE/Agent
A computer that is protected by the ACE/Server to prevent unauthorized access. Designated users of this computer must provide a valid SecurID PASSCODE in order to log in.

ACE/Agent for Windows NT

The Security Dynamics product that protects a Windows NT machine. Although the Windows NT machine may be a server with its own clients, to the ACE/Server it is a client looking for authentication service.

ACE/Agent software
The programs that perform the authentication dialog on both ACE/Agents and third-party clients.

ACE/Server

The Security Dynamics server software running on a TCP/IP-networked server, providing authentication, administration, and audit-trail services.

You must have the ACE/Server software in order to use ACE/Agent for Windows NT v 4.0 to perform SecurID authentication.

clntchk
The utility that displays the contents of the sdconf.rec file on Windows NT clients.

dial-in
To call a computer over a telephone line only, not ISDN or X.25.

Event Viewer system log
The record of actions on a Windows NT machine.

FORM
An HTML element used to create data entry forms in a Web page.

ftp

The acronym for File Transfer Protocol, a method used for transferring files across the Internet. WebID cannot be used to secure files on ftp servers because ftp servers are usually accessed on an anonymous-user basis.

GINA

The local Graphical Identification and Authentication interface on a Windows NT machine.

IIS
The acronym for Microsoft Internet Information Server, the software that allows a Windows NT workstation to operate as a World Wide Web server.

log.rec
Encrypted audit trail file for ACE/Server v 1.X. It is more detailed than the event log on the Windows NT machine. For ACE/Server v 2.X or later, this information is stored in a database named sdlog.

Next Tokencode mode

A series of incorrect tokencodes during authentication puts a token into this mode. In this mode, after a correct code is finally entered, the user will be prompted for another token code before being allowed access.

New PIN mode
When a user’s token is in this mode, the user is required to have a new PIN in order to gain access.

Node Secret

A string of pseudorandom data known only to the client and the server. The node secret is combined with other data to encrypt client/server communications.

PASSCODE

The user's PIN ***plus*** the current tokencode displayed on the SecurID token. With a PINPAD card, the user enters his PIN directly into the token, and the token itself generates the PASSCODE.

PIN

The user’s Personal Identification Number. The PIN, along with the tokencode, make up the Security Dynamics authentication system.

protocol
An agreed convention for inter-computer communications across a network.

RAS

The Remote Access Service on Windows NT. Service is available to Windows NT, Windows 95, and Windows for Workgroups 3.11 stations.

sdconf.rec
The configuration file that must be copied from the ACE/Server master to its clients.

sdlog

Encrypted audit trail database for ACE/Server v 2.X or later. It is more detailed than the event log on the Windows NT machine. For ACE/Server v 1.X, this information is stored in a file named log.rec.

security host
The Microsoft term for a security program like ACE/Agent for Windows NT.

station

A dial-in client of a Windows NT workstation. A station can be a remote PC running Windows NT, Windows 95, or Windows for Workgroups 3.11. SecurID prompts are displayed if the workstation is SecurID protected.

SDGINA
The Security Dynamics implementation of the local Graphical Identification and Authentication interface on a Windows NT machine.

SDRAS

The Security Dynamics implementation of the Remote Access Service on Windows NT. This service is available to Windows NT, Windows 95, and Windows for Workgroups 3.11 clients.

SSL

The acronym for Secure Sockets Layer, an Internet protocol that is designed as an encryption layer below the http protocol. SSL connections use the https protocol. You must have an SSL data certificate installed on your server in order to use https. For more information about obtaining an SSL certificate for IIS, visit the VeriSign Corporation’s Web site at http://www.verisign.com/microsoft/.

SecurID token

A hardware device or software application that generates a SecurID tokencode. A token may be a PINPAD card, a standard SecurID card, a Key Fob, a SecurID modem, or a SoftID.

tokencode
The code displayed by a SecurID token. The tokencode, along with the PIN, make up the Security Dynamics authentication system.

two-factor authentication

The authentication method used by the ACE/Server system. The user must enter a secret, memorized personal identification number (PIN) ***plus*** the current code generated by the user's assigned SecurID token. With a PINPAD token, the user enters his PIN directly into the token, and the token itself generates the PASSCODE.

URL
The acronym for Uniform Resource Locator, the scheme used to address Internet resources on the World Wide Web.

WebID

The feature set in ACE/Agent for Windows NT v 4.0 that allows you to SecurID-protect files, directories, or an entire server on the World Wide Web.

World Wide Web server
A program on a networked computer that responds to requests from client stations on the World Wide Web.

Windows NT

The operating system and networking functionality available in Windows NT machines. The usual names for the directory at the top of the Windows NT system tree are

\winnt

\winnt35

\windows

These names, which are specified when Windows NT is installed, can be modified by the installer.

cookie

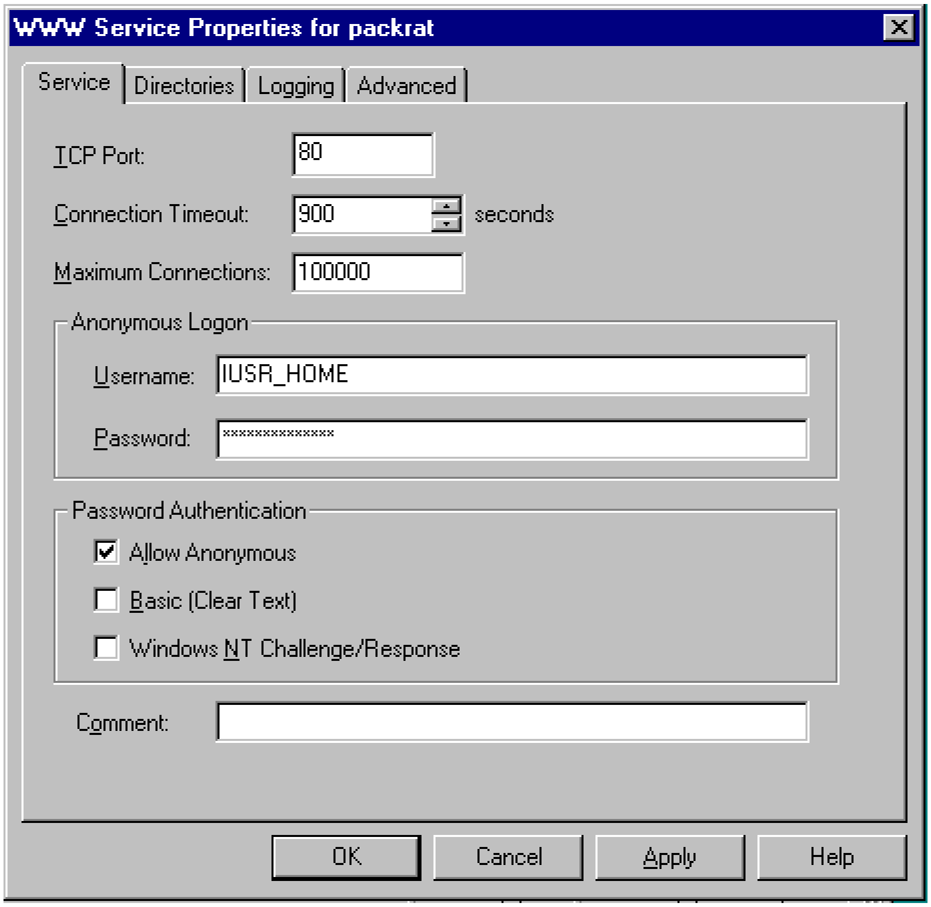
A cookie allows a tokenholder to browse any protected page on a server without being repeatedly prompted for a PASSCODE. The cookie is stored in the user’s Web browser and acts as an admission ticket, passing user authentication information to the server every time a WebID-protected URL is encountered.

Note

- A WebID cookie is valid only during the browsing session for which it was created. When the tokenholder exits his Web browser, the cookie expires and must be renewed during the next authentication session.

Domain secret
A cookie that is valid on multiple servers in a site domain.

WWW Service Properties dialog box



WWW Service Properties for packrat

TCP Port: 80

Connection Timeout: 900 seconds

Maximum Connections: 100000

Anonymous Logon

Username: IUSR_HOME

Password: ***************

Password Authentication

☑ Allow Anonymous

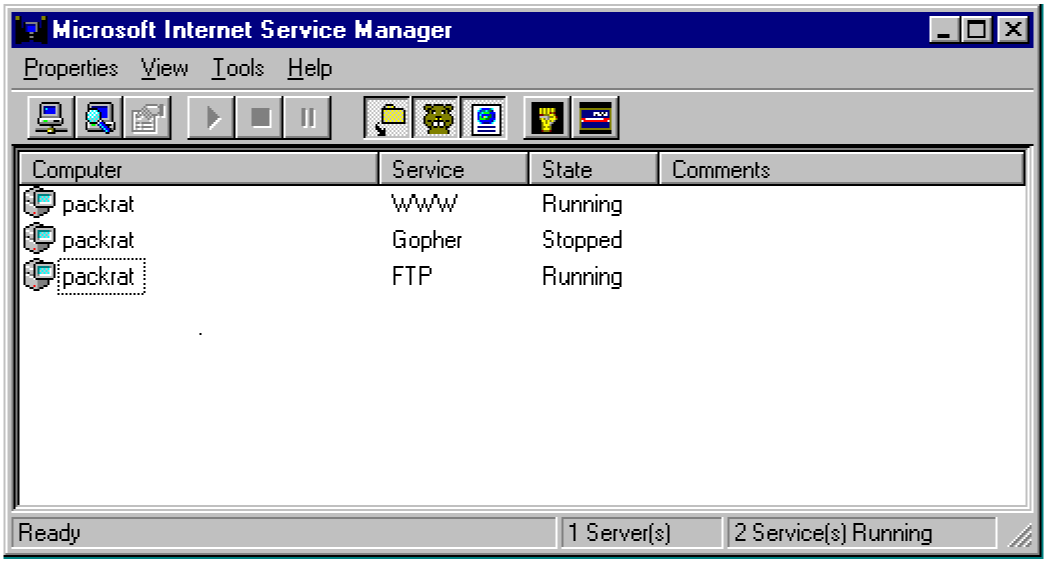
□ Basic (Clear Text)

□ Windows NT Challenge/Response

Comment:

Microsoft Internet Service Manager dialog box

- Click the SecurID icon on the toolbar to access the WebID feature set.



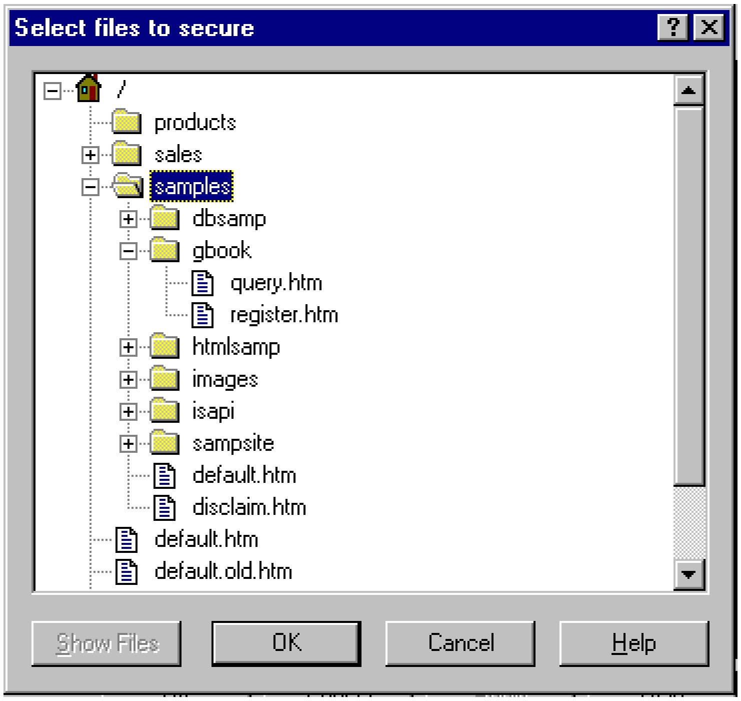
Computer	Service	State	Comments
packrat	WWW	Running	
packrat	Gopher	Stopped	
packrat	FTP	Running	

Ready | 1 Server(s) | 2 Service(s) Running

The WebID File Security Page

To enable Web protection

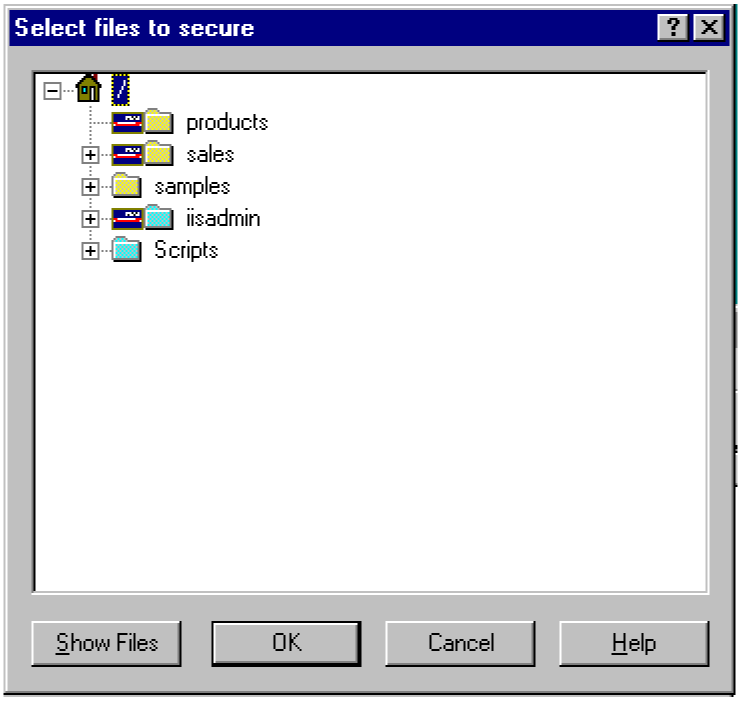
- point to the files or directories you wish to SecurID-protect
- click the right mouse button



The WebID File Security Page

To enable protection on a

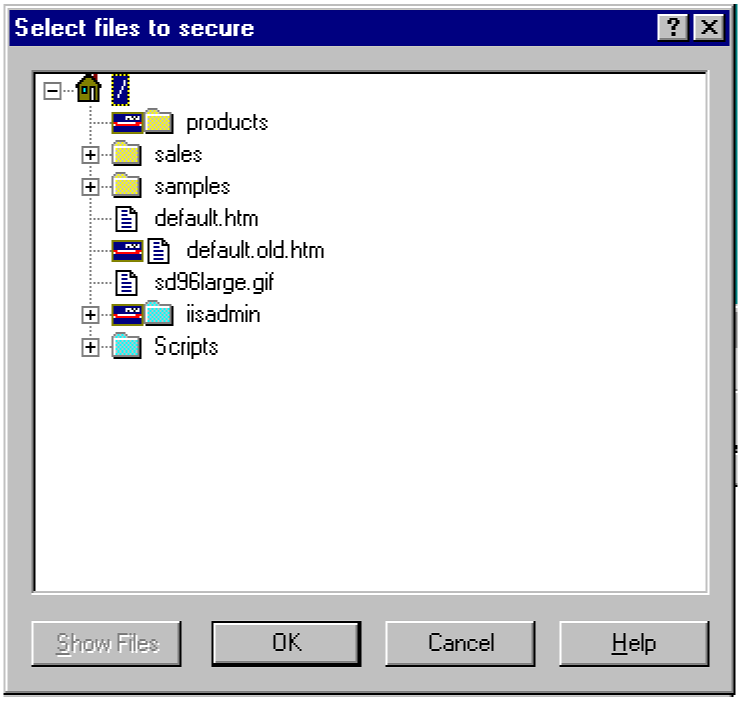
- directory, click the right mouse button
- series of directories, hold down the right mouse button and drag the pointer across the icons



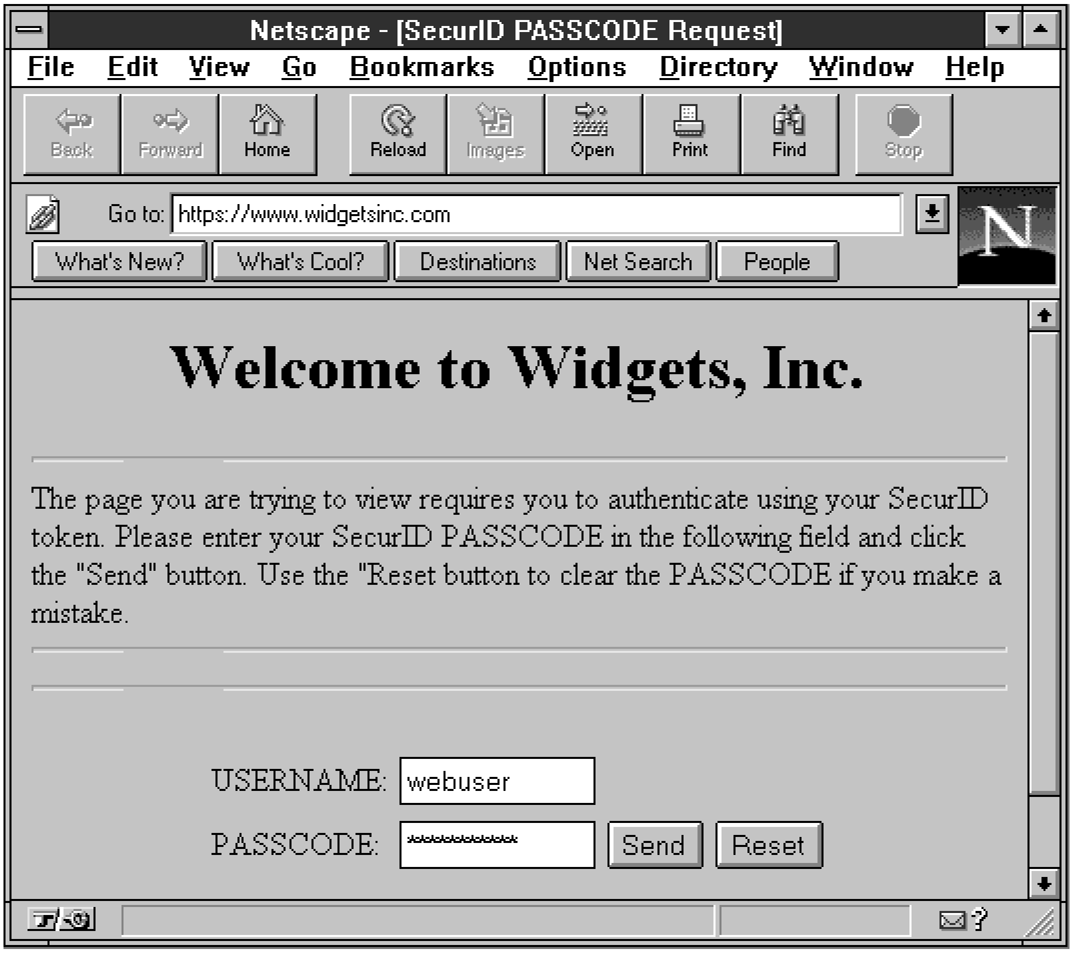
The WebID File Security Page

To enable protection on a

- file, click the right mouse button
- series of files, hold down the right mouse button and drag the pointer across the icons



Welcome to Widgets web page



Netscape - [SecurID PASSCODE Request]
File Edit View Go Bookmarks Options Directory Window Help
Back Forward Home Reload Images Open Print Find Stop
What's New? What's Cool? Destinations Net Search People
Send Reset

Go to: https://www.widgetsinc.com

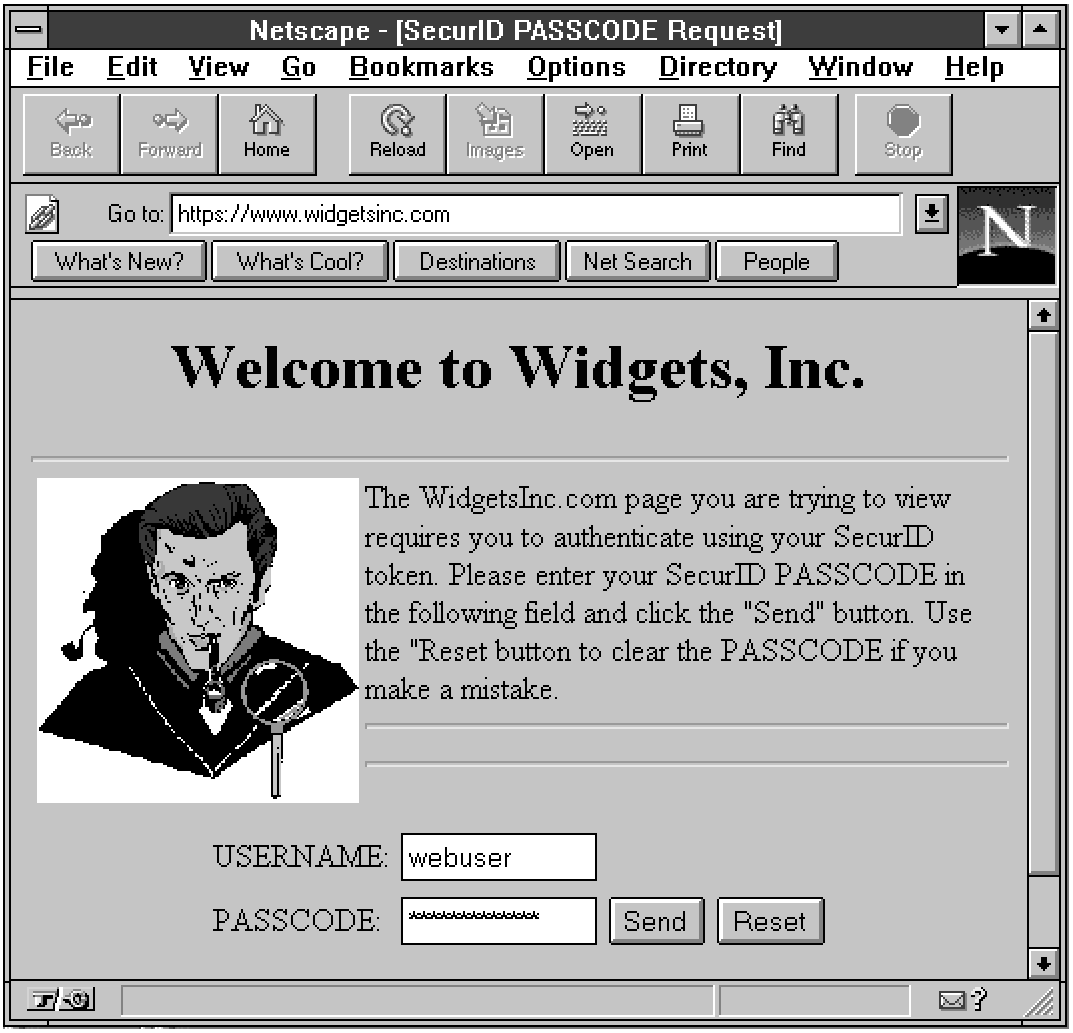
Welcome to Widgets, Inc.

The page you are trying to view requires you to authenticate using your SecurID token. Please enter your SecurID PASSCODE in the following field and click the "Send" button. Use the "Reset button to clear the PASSCODE if you make a mistake.

USERNAME: webuser

PASSCODE: ************

Welcome to Widgets web page



Go to: https://www.widgetsinc.com

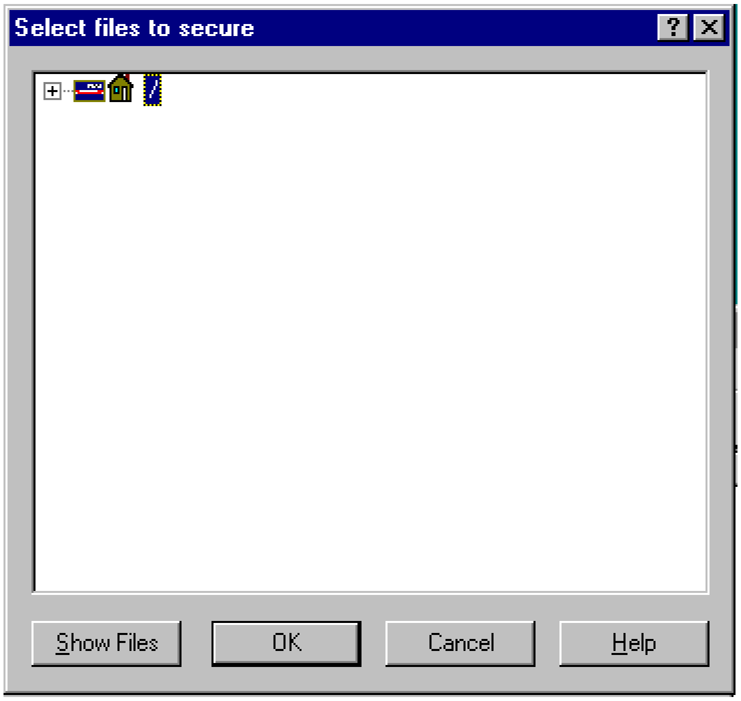
Welcome to Widgets, Inc.

The WidgetsInc.com page you are trying to view requires you to authenticate using your SecurID token. Please enter your SecurID PASSCODE in the following field and click the "Send" button. Use the "Reset button to clear the PASSCODE if you make a mistake.

USERNAME: webuser

PASSCODE: **************

The WebID File Security Page



Domain

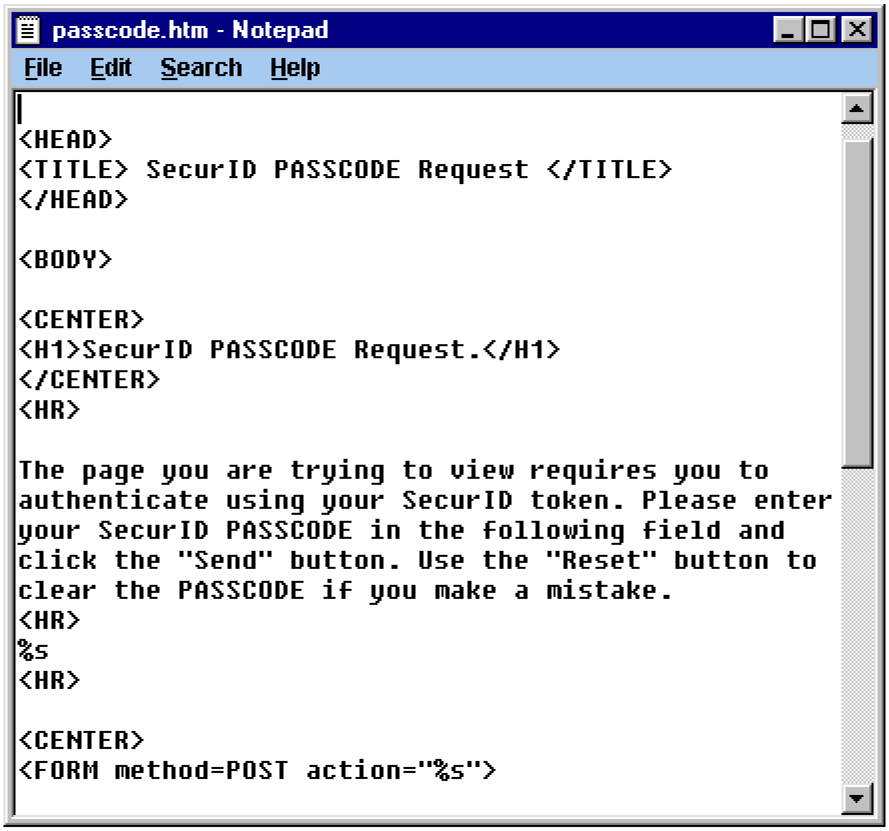
Domain refers to a World Wide Web DNS domain. It does not refer to a Windows NT domain.

Windows NT User Manager dialog box

broken image icon

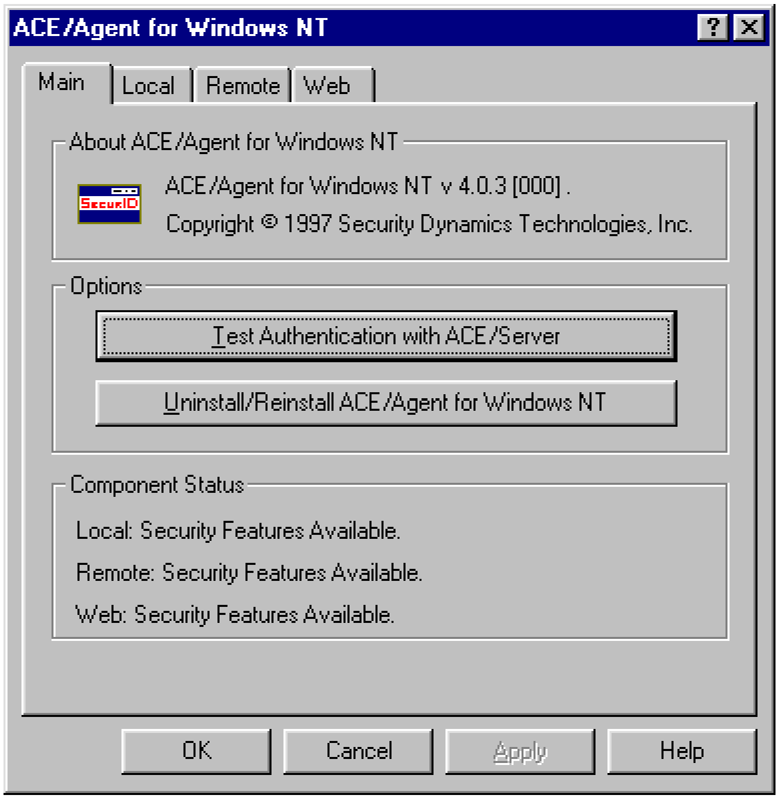
If you add a graphics image to the authentication prompt, be sure that the file is NOT loaded from a SecurID-protected directory. If the file is protected, the browser will not recognize it. Instead of displaying the graphic, the browser will display the broken image icon.

The Source HTML Code for the Authentication Prompt



```

<HEAD>
<TITLE> SecurID PASSCODE Request </TITLE>
</HEAD>

<BODY>

<CENTER>
<H1>SecurID PASSCODE Request.</H1>
</CENTER>
<HR>

The page you are trying to view requires you to
authenticate using your SecurID token. Please enter
your SecurID PASSCODE in the following field and
click the "Send" button. Use the "Reset" button to
clear the PASSCODE if you make a mistake.
<HR>
%s
<HR>

<CENTER>
<FORM method=POST action="%s">
```

Main properties page


ACE/Agent for Windows NT
?
✕
Main
Local
Remote
Web
Test Authentication with ACE/Server
Uninstall/Reinstall ACE/Agent for Windows NT
OK
Cancel
Apply
Help

About ACE/Agent for Windows NT

ACE/Agent for Windows NT v 4.0.3 [000] .

Copyright © 1997 Security Dynamics Technologies, Inc.

Options

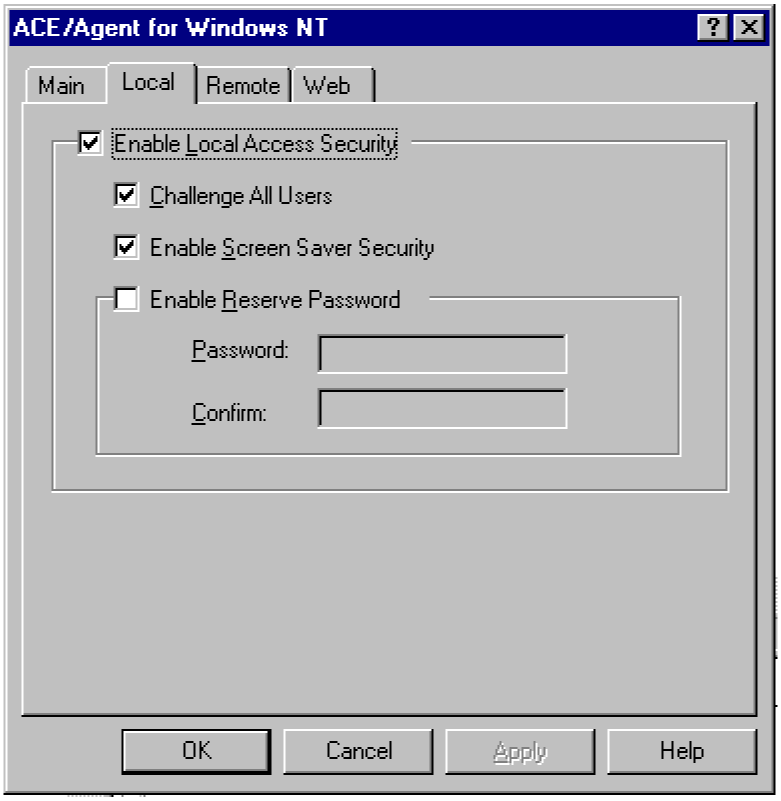
Component Status

Local: Security Features Available.

Remote: Security Features Available.

Web: Security Features Available.

Local properties page



☑ Enable Local Access Security

☑ Challenge All Users

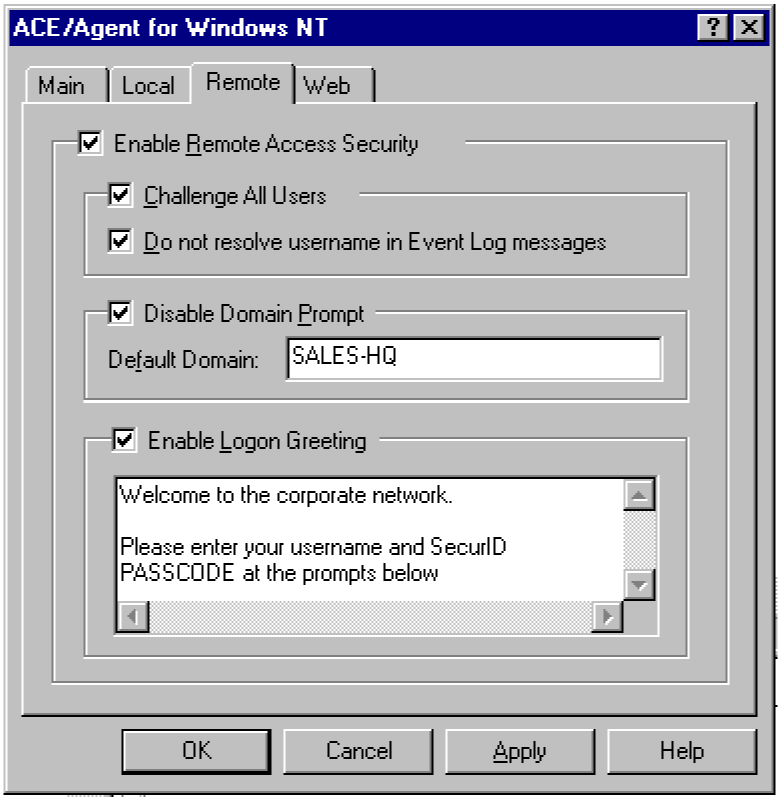
☑ Enable Screen Saver Security

□ Enable Reserve Password

Password:

Confirm:

Remote properties page



☑ Enable Remote Access Security

☑ Challenge All Users

☑ Do not resolve username in Event Log messages

☑ Disable Domain Prompt

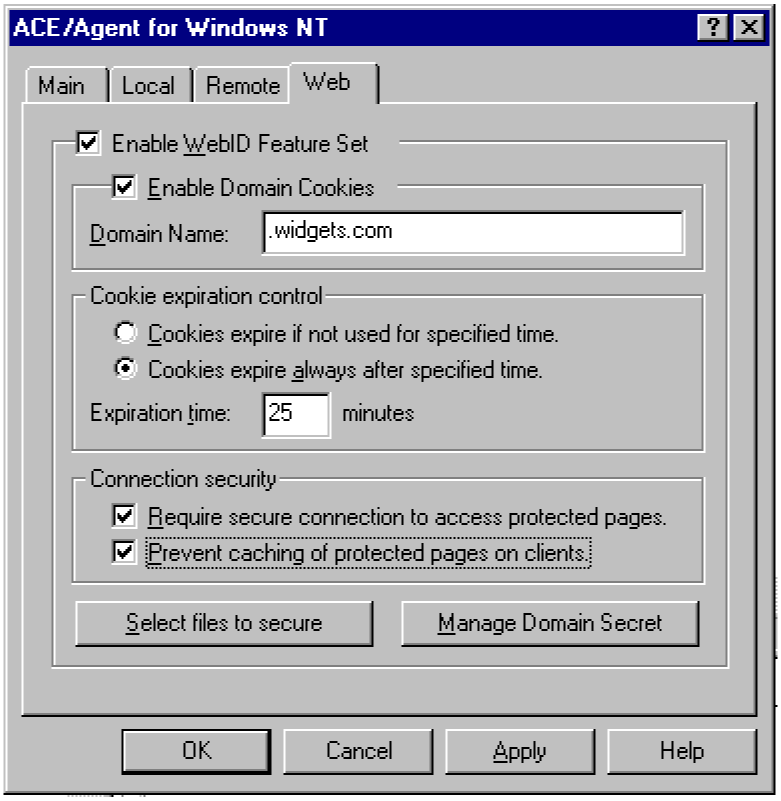
Default Domain: SALES-HQ

☑ Enable Logon Greeting

Welcome to the corporate network.

Please enter your username and SecurID
PASSCODE at the prompts below

Web properties page



☑ Enable WebID Feature Set

☑ Enable Domain Cookies

Domain Name: .widgets.com

Cookie expiration control

○ Cookies expire if not used for specified time.

● Cookies expire always after specified time.

Expiration time: 25 minutes

Connection security

☑ Require secure connection to access protected pages.

☑ Prevent caching of protected pages on clients.

ACE/Agent Control Panel tabs

%SYSTEMROOT%

The root directory of a Windows NT machine. This directory contains critical data used by the operating system. This directory is usually named **windows**, **winnt**, or **winnt50**.