WebID®
Authentication with a Standard SecurID Card or Key Fob

You have been assigned a Standard SecurID® Card or Key Fob to use when accessing WebID-protected URLs. This security token generates and displays unpredictable codes that change at a specified time interval (typically every 60 seconds).

To gain access to protected URLs, you must enter a valid SecurID PASSCODE™, which is made up of two factors:

- your secret, memorized personal identification number (PIN)
- and the current tokencode generated by your SecurID token

With a conventional Web server security system, an intruder can easily learn your password and access sensitive data under your identity. Requiring two factors ensures reliable, highly secure identification and authentication.

Because the SecurID system creates an audit trail that cannot be repudiated, you may be held accountable for activities recorded identifying you as the user. Therefore, avoid the unauthorized use of your identity and privileges by protecting your SecurID token and the secrecy of your PIN. Read "User Responsibilities" on page 4 to learn about your obligations as a tokenholder.

Before You Begin

Contact your network administrator to obtain the following information before you attempt to log in for the first time.

If you have any questions, contact your security administrator, _____, at extension _____.

Mark the applicable PIN conditions:

☐ The system will assign a PIN to you; you cannot create your own.
Read "Receiving a System-Generated PIN" on page 2.

☐ You will be allowed to use a PIN that you make up yourself.
Read "Creating Your Own PIN" on page 2.

☐ Your PIN may contain letters as well as digits.

☐ All PINs on the system must be ____ characters in length.

☐ Your PIN may contain from ____ through ____ characters.

☐ You will have a duress PIN.

Browser Requirements

To authenticate through WebID, your browser must support HTML FORMs and Persistent Client State HTTP Cookies.

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.

Receiving a System-Generated PIN

1. Start your Web browser and initiate a login session on a protected URL. The WebID login page will appear, prompting you to enter your username and a SecurID PASSCODE.
2. In the **USERNAME** field, enter the name you use to log in to the system.

For security reasons, responses to the Enter PASSCODE prompt are displayed as asterisks.

3. If you have never received a PIN for your SecurID token, in the **Enter PASSCODE** field, type the code that is currently displaying on your token.

   If your token previously had a PIN and the administrator has not cleared it, enter the old PIN followed by the code that is currently displaying on your SecurID token.
4. Click **Send**.
   (If the system displays an **Access Denied** page, wait for the tokencode in the LCD to change, then try again to log in.)
5. A "New PIN Request" page will appear, stating that you will receive a system-generated PIN.
6. Click **System Generated PIN**.
7. A system-generated PIN is displayed.
8. Memorize the PIN; **Do not write it down.**
9. Wait for the tokencode on the card to change, and then follow the instructions in "SecurID Authentication" on page 3.

Creating Your Own PIN

1. If you are going to create your own PIN, give some thought to what it will be. Do not pick an obvious number like a birthday or phone number.
2. Start your Web browser and initiate a login session on a protected URL. A WebID login page will appear, prompting you to enter your username and a SecurID PASSCODE.
3. In the **USERNAME** field, enter the name you use to log in to the system.

For security reasons, responses to the Enter PASSCODE prompt are displayed as asterisks.

4. If you have never received a PIN for your SecurID token, type the code that is currently displaying on your token in the **Enter PASSCODE** field.

   If your token previously had a PIN and the administrator has not cleared it, enter the old PIN followed by the code that is currently displaying on your SecurID token.
5. Click **Send**.
   (If the system displays an **Access Denied** page, try to log in again.)
6. A "New PIN Request" page will appear, prompting you to create your new PIN or receive one from the system.

   There are two possibilities for New PIN creation:

   - **You will create your own PIN.**
     —Select the **I will create PIN** radio button, enter and verify your PIN in the fields, and then click **Send**.
   - **You will have the system generate a PIN for you.**
     —Select the **System Generated PIN** radio button, and then click **Send**. When your new PIN appears, memorize it right away; **do not write it down**.

7. If your PIN is acceptable, the system will prompt you to wait for the code on your token to change, and then you can log in. Follow the instructions in the next section "SecurID Authentication."

   If any one of the following messages displays, correct the error and try again:

   PIN and confirmation do not match.
   PIN must be 4-8 digits.
   New PIN rejected.

   If you are still denied access, contact your security administrator.

SecurID Authentication

Follow this procedure whenever you are prompted to enter a PASSCODE:

1. In the **USERNAME** field of the "PASSCODE Request" page, type the name you use to log in to the system.
2. In the **Enter PASSCODE** field, type your PIN followed by the tokencode currently displaying in the LCD of your Standard Card or Key Fob.
3. Click **Send**.

   If you have entered a valid PASSCODE, the protected URL will display in your browser. If instead you receive an **Access denied** page, you may have typed your PASSCODE incorrectly. Wait for the token code to change, then try again to log in.

   If you are repeatedly denied access even though you are typing your PASSCODE correctly, contact your security administrator.

Note: A SecurID PASSCODE cannot be used twice. If you are challenged for another PASSCODE, you must wait for a new tokencode to appear in the LCD. The stack of countdown indicators on the left side of the LCD lets you know how soon the code will be changing.

The "Next Tokencode" Prompt

On occasion, even after you have typed your PASSCODE correctly, the system will ask you to enter the next tokencode (sometimes called a "PRN") your token generates to confirm your possession of the token.

If you are prompted for a "Next Tokencode" or "Next PRN":

1. Wait until the tokencode changes, and carefully type the new one.
2. Click **OK**.

   If you are not granted access after correctly entering the next tokencode, contact your security administrator.

Duress PINs

If your system has the duress PIN option installed, you have two PINs: a regular PIN and a duress PIN. Use your regular PIN for normal logins. Use the duress PIN if you are ever forced to log in by an unauthorized person attempting to gain system access.

If you use your duress PIN, you will be granted access and see no difference in operation. However, the next time the ACE/Server administration program is run, the administrator will be notified that you have been forced by an intruder to log in.

Your duress PIN is your regular PIN with 1 added to it but with no carrying. For example:

If your regular PIN is	Then your duress PIN is
243890	243891
243899	243890
ABCDEF	ABCDEG
ABCDEZ	ABCDEA

User Responsibilities

You are responsible for protecting the authentication factors entrusted to you. Keep your PIN secret and protect your SecurID token against loss and theft.

If an unauthorized person learns your PIN and obtains your SecurID token, this person can assume your identity. Any action taken by this intruder will be attributed to you in the system's event log.

For your own protection and that of the system, always take the following precautions:

- Never reveal your PIN to anyone. Do not write it down.
- If you think someone has learned your PIN, notify the security administrator, who will clear the PIN immediately. At your next login you will have to receive or create a new PIN to use.
- Exercise care not to lose your SecurID token or to allow it to be stolen. If your token is missing, tell an administrator immediately. The administrator will disable your token so that it is useless to unauthorized users.
- Do not let anyone access the system under your identity (i.e., log in with your PIN and a code from your SecurID token).
- It is essential to site security that you follow your system's standard logoff procedures. Failure to log off properly can create a route into the system that is completely unprotected.
- Protect your token from physical abuse. Do not immerse it in liquids, do not expose it to extreme temperatures, and do not put it under pressure or bend it. Each SecurID token comes with care instructions that you should read and follow.