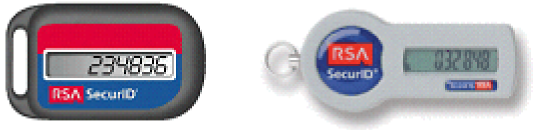
SecureID Token Quick Reference Card



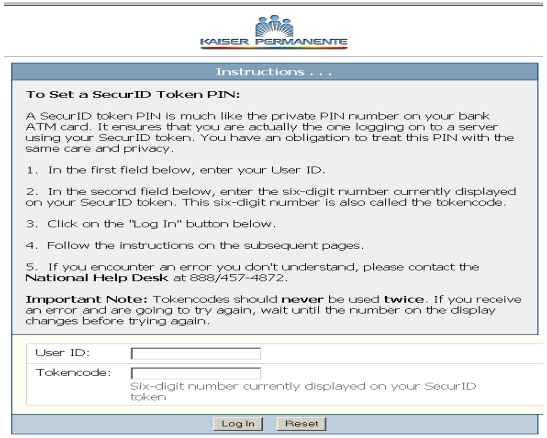
Version 1.1 - February 2007

This quick reference card contains information for operating and maintaining the SecureID Token. Remote Access users should read this card to ensure proper use of token.

Setting the SecurID Token PIN

Tokens must be assigned a PIN by the user in order to operate properly. The user must create a PIN at http://token.kp.org.

1. Type http://token.kp.org in the address field of an internet browser. ***Note:*** *You must be connected to the Kaiser Permanente network, as this is an internal web site.*
2. Press **Enter**. You will see the **SecurID: Token PIN Set | Configured Token Test . . .** screen..
3. Click **Set Token PIN**. *You will see instructions on how **To Set a SecurID Token PIN**.*
4. Follow the directions provided to establish a PIN for the token.



To Set a SecurID Token PIN:

A SecurID token PIN is much like the private PIN number on your bank ATM card. It ensures that you are actually the one logging on to a server using your SecurID token. You have an obligation to treat this PIN with the same care and privacy.

1. In the first field below, enter your User ID.

2. In the second field below, enter the six-digit number currently displayed on your SecurID token. This six-digit number is also called the tokencode.

3. Click on the "Log In" button below.

4. Follow the instructions on the subsequent pages.

5. If you encounter an error you don't understand, please contact the **National Help Desk** at 888/457-4872.

Important Note: Tokencodes should **never** be used **twice**. If you receive an error and are going to try again, wait until the number on the display changes before trying again.

User ID:

Tokencode:

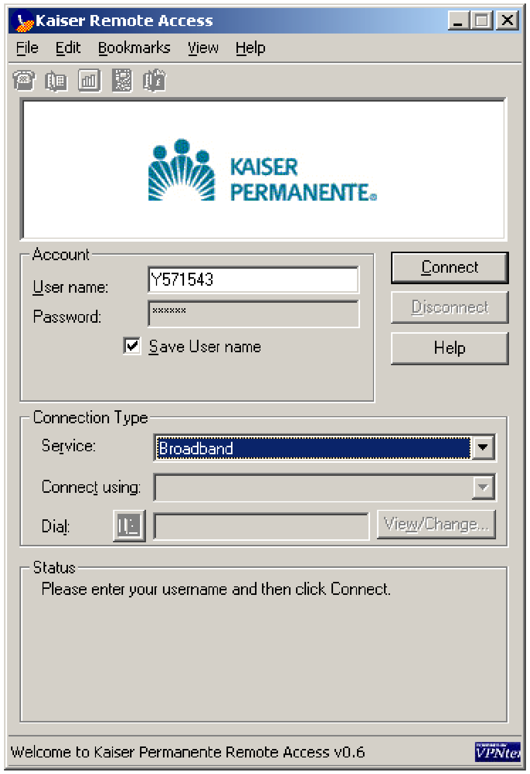
Six-digit number currently displayed on your SecurID token

Using the Token to connect to the Kaiser Network

1. Double-click on the Kaiser Remote Access icon:

Kaiser Remote Access.lnk

2. You will see the Kaiser Remote Access Screen.



Account

User name: Y571543

Password: ******

☑ Save User name

Connection Type

Service: Broadband

Connect using:

Dial:

Status

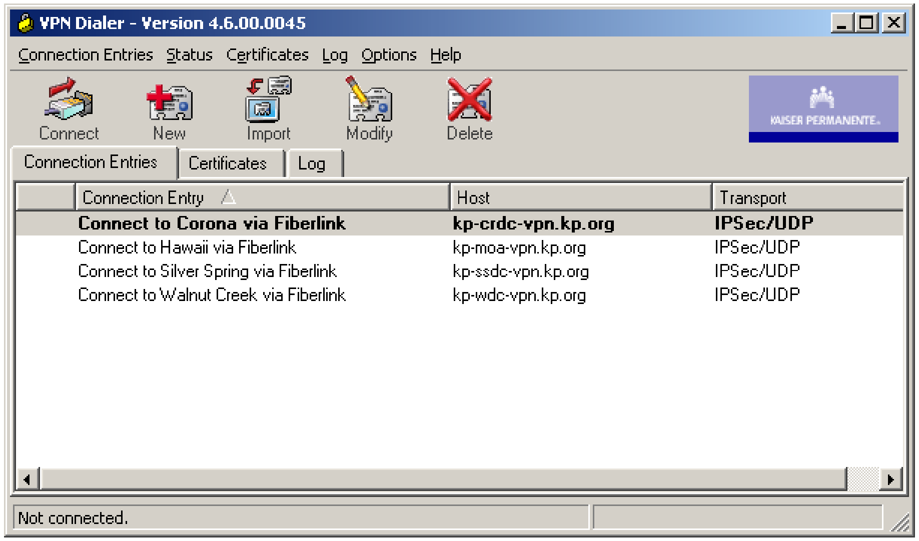
Please enter your username and then click Connect.

Welcome to Kaiser Permanente Remote Access v0.6

3. Type your Remote Access Login ID in the **User name** field. For most users the Remote Access User ID will be the NUID (i.e. D111766). *Note: The **Password** field will be pre-populated and grayed out.*

4. Select the **Connection Type** by clicking on the down arrow in the Service Field. Click **Connect**.

5. You will see the **VPN Dialer** Screen.

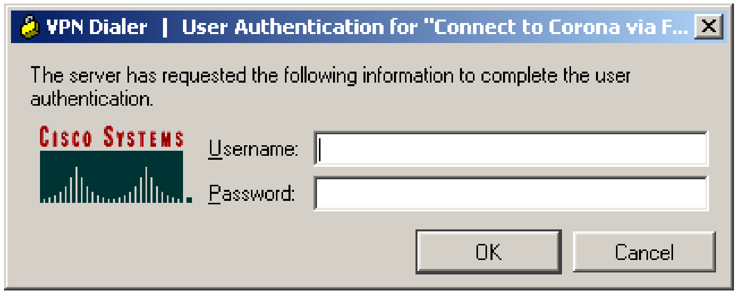

VPN Dialer - Version 4.6.00.0045
Connection Entries Status Certificates Log Options Help
Connect
New
Import
Modify
Delete
KAISER PERMANENTE
Connection Entries
Certificates
Log

Connection Entry	Host	Transport
Connect to Corona via Fiberlink	**kp-crdc-vpn.kp.org**	**IPSec/UDP**
Connect to Hawaii via Fiberlink	kp-moa-vpn.kp.org	IPSec/UDP
Connect to Silver Spring via Fiberlink	kp-ssdc-vpn.kp.org	IPSec/UDP
Connect to Walnut Creek via Fiberlink	kp-wdc-vpn.kp.org	IPSec/UDP

Not connected.

6. Select the Connection Entry that is closest to your location. Click **Connect** on the **VPN Dialer** screen.

7. You will see the **VPN Dialer | User Authentication** Screen.

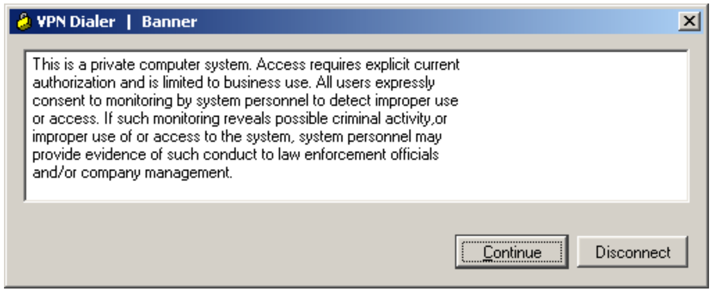

VPN Dialer | User Authentication for "Connect to Corona via F...
Cisco Systems
Username:
Password:
OK
Cancel

The server has requested the following information to complete the user authentication.

8. Type your Remote Access Login ID in the **Username** field. For most users the Remote Access User ID will be the NUID (i.e. D111766).

9. Type your token PIN and the current six-digit number shown on the token in the Password field. A new six-digit number is generated every 60 seconds.

7. Click **OK**. You will see the VPN Dialer | Banner Screen.



This is a private computer system. Access requires explicit current authorization and is limited to business use. All users expressly consent to monitoring by system personnel to detect improper use or access. If such monitoring reveals possible criminal activity,or improper use of or access to the system, system personnel may provide evidence of such conduct to law enforcement officials and/or company management.

8. Click **Continue.** You are now connected to the Kaiser Permanente intranet.

Maintenance of your SecurID Token

The token can become damaged when:

- Moved irregularly or forcefully by dropping, throwing, or spinning
- Exposed to extreme heat or cold
- Exposed to liquids

Reminders:

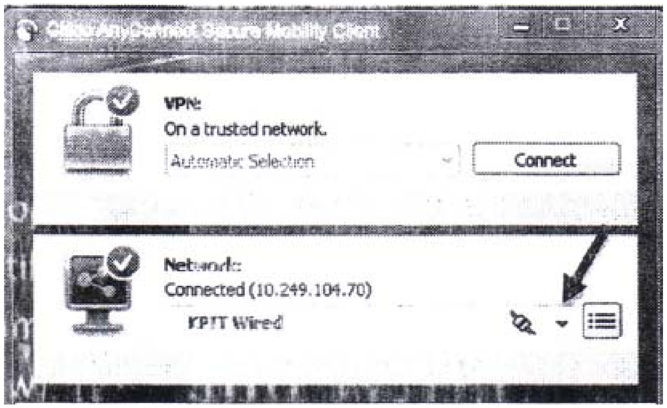
- The user's PIN must always precede the six-digit number when entering the Password.
- There are six horizontal tick marks at the beginning of each six-digit number, each tick lasts 10 seconds.
- Tokens expire: an expiration date is printed on the back of the token and should be thrown away after the expiration date.
- Please submit requests for replacement at least one month before it expires to insure uninterrupted service.
- After 12 consecutive months of inactivity, tokens will become disabled. (*submit request via the Hub*)

Link to the Hub:
http://kpnet.kp.org:81/kpit/services/ras/products/started_fiberlink.htm

For assistance, call the Corona National Help Desk at (888)457-4872 or Tie-line 8-330-1143

NEW Laptops:
Connecting to VPN and Wireless Networks

When working remotely, laptop users will need to access a wireless network and then VPN into the KP network. Newer laptops utilize the Cisco AnyConnect Secure Mobility Clint. The new client automatically selects the optimal network and is more secure. The client screen will launch upon powering on the laptop (below).



Cisco AnyConnect Secure Mobility Client

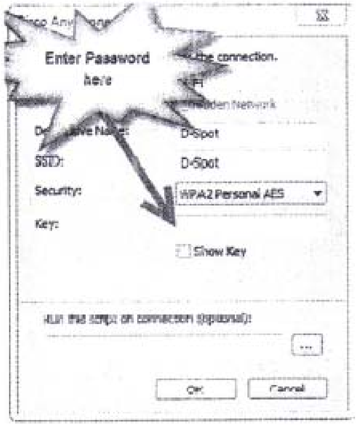
VPN:
On a trusted network.
Automatic Selection

Network:
Connected (10.249.104.70)
KPIT Wired

The user will use the drop down to select the appropriate network. If working from home, select the home wireless network to connect. AnyConnect is accessible from the system tray on the bottom right of the task bar.

Simply select the AnyConnect icon:

After selecting the desired wifi network, the below screen will populate with network specific information. The user will need to enter the password where the arrow is pointing and select connect.



SSID: D-Spot

Security: WPA2 Personal AES

Key:

☐ Show Key

*** The VPN functioinality has not changed as a result of the new AnyConnect Client.