

JJEDS Quick Reference Guide for Supervisors

Accessing J&J business information anywhere, anyplace, and anytime is critical to maintaining our competitive advantage. JJEDS helps us achieve this objective while protecting our valuable information resources. With JJEDS, each employee and business partner uses a USB "identity token" for authenticating to J&J systems and applications. This establishes a unique "Digital Identity" for each individual, which increases security and eliminates the need for multiple passwords.

This guide provides you with general information on the procedures of a Supervisor. For more in depth information, please visit the JJEDS help website at:
<https://jjeds.jnj.com/training/jjedshelp.htm>

Supervisors have new responsibilities in JJEDS, which include:

1. Assisting a Direct Report (Employee or Partner) to Obtain His or Her Digital Identity
2. Resetting Your Direct Report's Digital Identity Enrollment

These tasks are explained in this guide. In order to perform them you will need a Digital Identity. If you do not have a Digital Identity, you will need to assign a Personal Delegate who has a Digital Identity to perform these tasks on your behalf.

Assigning Personal Delegates

By assigning Personal Delegates, you help ensure that the Digital Identities of your Direct Reports are managed effectively.

It is recommended that you consider three of the following candidates:

- Administrative Assistants
- Two of your most senior Direct Reports
- One of your peers
- If you have employees who are physically located away from you, you should select one or two Personal Delegates who are located in the same area as these employees

Supervisors and their Personal Delegates can do the following:

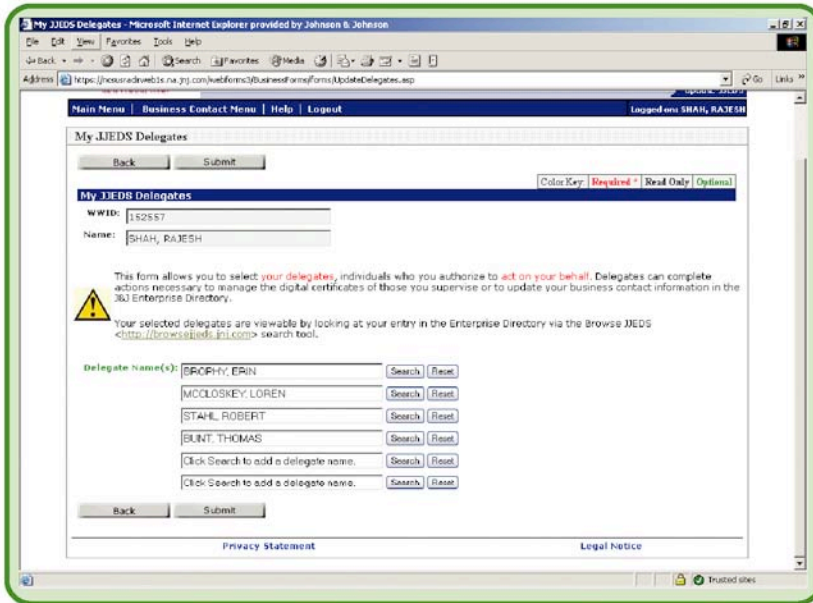
- Provide a Direct Report with the Identity Verification Code (IVC) he or she will need when obtaining a Digital Identity
- Reset a Direct Report's enrollment process (if he or she loses, breaks or is locked out his or her identity token)
- Initiate recovery of a Direct Report's encryption certificate in special circumstances
- Sponsor a partner/contractor
- Update business contact information

To assign Personal Delegates, follow the steps below. (Please note that it is not necessary for you to have a Digital Identity to assign a Personal Delegate.)

1. Go to <http://updatejjeds.jnj.com>.
2. Click on "My JJEDS Delegates."
3. If you have an identity token, insert it into your computer's USB port. If you do not have an identity token, click cancel and enter your WWID and J&J Network password at the prompt and proceed to step 6.
4. Select your name in the "Client Authentication" drop-down menu and click on "OK."



5. Enter your Pass Phrase and click on "OK."
6. The main menu displays. Under the heading "Delegate Form," click on "Update My Delegates." A screen with spaces for Personal Delegate names displays.



7. Next to the first available space, click on the button marked "Search."
8. A search form appears. Search by first/last name, WWID, or e-mail address for the person you would like to assign as a Personal Delegate, and then click on "Search."
9. The search result will appear in a pop-up screen. Select the person you wish to assign as you delegate.
10. Click on the "OK" button on the bottom right. A list of your Personal Delegates, which includes the newly added one, displays.
11. If you wish to clear the individual you selected as a delegate, click the button marked, "Reset."
12. Click on "Submit."
13. When the message "Successfully updated information in JJEDS" displays, click on "OK."
14. Close Internet Explorer.

1. Assisting a Direct Report (Employee or Partner) to Obtain His or Her Digital Identity

As a Supervisor or Personal Delegate, it is your responsibility to identity-proof your direct reports and provide them with their IVC, which will be e-mailed to you once they initiate the process of obtaining a Digital Identity. Here is how this part of the process works:

1. The Direct Report logs onto the JJEDS web site at <https://jjeds.jnj.com> by typing in his or her WWID, and generates a Certificate Authorization Code (CAC) and an IVC.
2. The Direct Report receives his or her CAC via e-mail.
3. You receive the Direct Report's IVC via an encrypted e-mail from the JJEDS Certification Authority if you have a Digital Identity, or via an unencrypted e-mail if you do not.

DO NOT forward this e-mail to the Direct Report.

4. Either print it out and hand it directly to the Direct Report, or read the IVC directly to the Direct Report by phone (NOT via voicemail).

NOTE: If the CAC and/or IVC are lost, the Supervisor or Personal Delegate will have to assist the Direct Report to recover his or her Digital Identity, as described in the next section.

2. Resetting Your Direct Report's Digital Identity Enrollment

If a Direct Report does one of the following, the Supervisor or Personal Delegate will need to reset the Direct Report's enrollment process:

- Has been locked out of identity token by typing Pass Phrase incorrectly 5 times
- Loses or breaks identity token
- Loses CAC or IVC
- Leaves the Company

Follow these steps:

1. Insert your identity token into your computer's USB port.
2. Go to the JJEDS website (<https://jjeds.jnj.com>), enter your WWID, and click on "Continue."
3. Select your name in the "Client Authentication" drop-down menu, and click on "OK."
4. Enter your Pass Phrase and click on "OK."
5. Hold your pointer over "Manage Others' Certificates." A drop-down menu displays.
6. Move your pointer over "Direct Reports." Another menu displays.
7. Click on "Reset Direct Report's Enrollment Process." The "Reset User's Enrollment Process" screen appears.
8. In the "Reset Enrollment Process For:" drop-down menu, select the name of the Direct Report for whom the process needs to be reset.

CAUTION: Please ensure you choose the correct name that requires the reset. Choosing someone who does not require a reset will result in the deletion of his or her Digital Identity from JJEDS.



9. Click on "Reset Enrollment."

- If the Direct Report does not have a Digital Identity, a screen displays stating that the Direct Report's IVC and CAC were reset, and *you will have reached the end of the process.*
- If the Direct Report does have a Digital Identity, a screen displays informing you that you are about to revoke his or her Digital Identity certificate. On that screen, choose the reason for revocation from the displayed list. Click on "Reset Enrollment." A confirmation screen will appear.

Once you have reset your Direct Report's enrollment process, contact the Direct Report, and inform him or her that you have completed the reset. The Direct Report must then do the following (described in A through G):

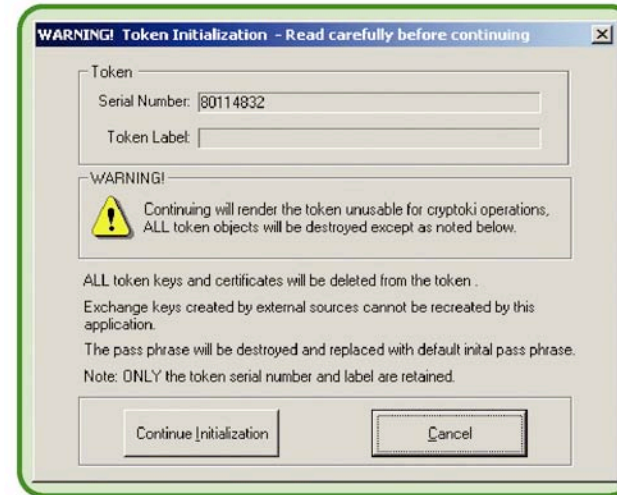
A. Replacing a Lost/Broken Identity Token

- If your Direct Report's identity token is lost (not just left at home or in the car) and a reasonable effort is made to find it, or if it is verified that the token is broken, the direct report can obtain a new identity token by:
 - Carrying a spare token if traveling to non-J&J sites.
 - Requesting a replacement token from the local Service Coordinator if the user is at a J&J location
- If neither of the above is viable, the Direct Report should contact the Help Desk or Remote Access administrator to have a new identity token directly shipped to him or her.

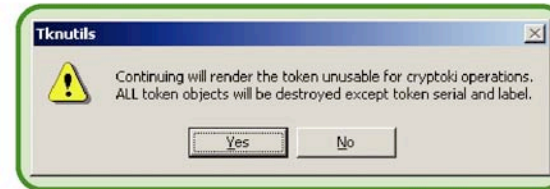
NOTE: If the Direct Report is currently using the identity token to log in remotely, he or she can call the helpdesk to receive 7-day temporary remote access, which allows him or her to log in remotely using his or her NT username and password.

B. Re-Initialize the Old Identity Token or Initialize a New Identity Token

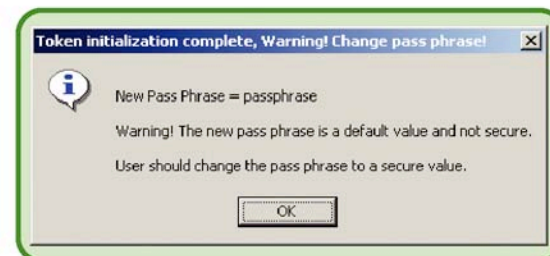
1. Insert the identity token into the computer's USB port.
2. Go to "Start → Programs → Rainbow Technologies → iKey 2000 Series Software → Token Utilities."
3. Click on "Token" on the top of the menu bar.
4. Click on "Initialize Token..."
5. A screen displays warning you concerning initializing the token.



6. Click on "Continue Initialization."
7. Another warning will appear. Click on "Yes."



8. The following screenshot will appear informing you of the new Pass Phrase and warning you to change it. Click on "OK."



C. Changing the Pass Phrase

Once initializing has completed, the Direct Report will need to change the Pass Phrase, which has now been reset to "passphrase" by default. Click on "Token → Change Pass Phrase" from the menu bar and follow the steps to change the Pass Phrase.

Note: It is recommended you use a Pass Phrase that is easy to remember and has at least 6 characters (e.g., your Secure ID pin).

D. Obtain a new CAC and IVC

Refer to "Assisting a Direct Report (Employee or Partner) to Obtain His or Her Digital Identity" section on page 1 of this guide.

E. Obtain a new Digital Identity

Refer to the JJEDS web site at <https://jjeds.jnj.com/training/jjedshelp.htm> for step-by-step instructions.

F. Recover your old Encryption Certificate

Refer to the JJEDS web site at <https://jjeds.jnj.com/training/jjedshelp.htm> for step-by-step instructions.

G. Remove the old Digital Identity (Signature Certificate) from Internet Explorer

1. Open Internet Explorer.
2. From the menu bar above, click on "Tools → Internet Options."
3. Click on the "Content" tab.
4. Click on the "Certificates..." button.
5. Scroll down and locate your name.
6. Click on your name and then click on "Remove."
7. If the name appears more than once, click on all instances and click on "Remove."
8. Click on "Close" and then click on "OK."
9. Remove and reinsert your identity token.

