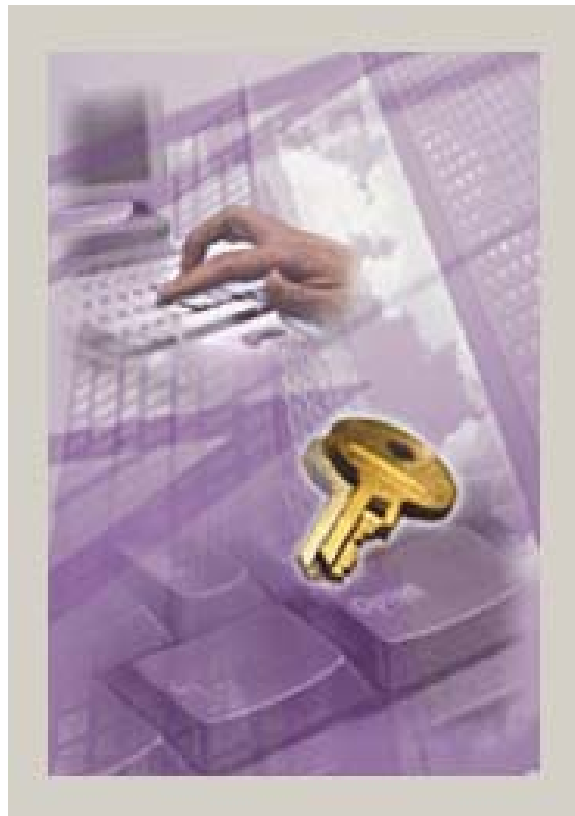


Entrust Help

(Draft 2006-06-28/TDGS)



Technical Documentation and Graphics Section
RCMP Headquarters

(back side of cover in printed version)

Contents

- ENTRUST OVERVIEW 1**
 - Online Help Information..... 1
 - RCMP Entrust Policy Centre..... 1
 - Purpose Of Entrust..... 1
 - Primary Functions..... 2
 - Token Overview 3
 - Token Software..... 3
 - PKI Certificate Request 3
 - Entrust Future Direction 3
 - System Support..... 4

- ACTIVATION OVERVIEW 5**
 - Activation Steps..... 5

- ACTIVATION TECHNICAL SETUP 6**
 - Software Installation Requirement 6
 - Software Installation Details..... 6
 - Entrust Installation Using A Script Overview 6
 - Entrust Installation Using a CD 7
 - Entrust Installation Using NAL..... 8

- ACTIVATION USER PROCEDURES 13**
 - Hardware Token Initialization 13
 - Entrust Profile..... 14
 - Entrust Profile Creation..... 14
 - Entrust Profile Recovery With Token 19
 - Token Expiry 22

- ENTRUST LOGIN/LOGOUT 23**
 - Entrust Login 23
 - Entrust Logout 24
 - Entrust Single Login icons..... 24
 - Entrust Options Settings 26
 - Time-Out 26
 - Password Change 27
 - Export/Import Key 27

- OFFLINE WORK PROCEDURES 30**
 - Offline Work Overview 30
 - Offline Login 30
 - Offline / Online Switch..... 31

ENTRUST FILE PROCESSING	33
Encrypting & Signing	33
Encrypting Files For Yourself	33
Encrypting Files For Recipients	34
Decrypt and Verify Secured Files.....	35
Decrypt, Verify and Open Secured File.....	37
Secure Delete	37
 ENTRUST/ICE AND SECURED FOLDERS	 39
Entrust/ICE Overview	39
Entrust/ICE Main Window	39
Entrust ICE Start-up	40
Auto-Protection Folder Setup	40
Copy or Move Files Automatically.....	41
Add Folder to Send To Menu	42
Remove Folder from Send To Menu	42
Delete Plaintext After Encrypting.....	42
Encrypt File for Recipient List	43
 QUICK REFERENCE	 44
Quick Reference Table	44
 Glossary of Terms	 47
 Index	 49

ENTRUST OVERVIEW

Online Help Information

This version of the RCMP Entrust Online Help (dated June 28, 2006) was created by:

- Technical Documentation & Graphics Section,
Information Management Branch,
CIO Sector,
RCMP Headquarters,
Ottawa Ontario, Canada
K1A 0R2
- **Phone:** (613) 998-6208 **Fax:** (613) 993-2290

This Online Help is available in HTML Help (.htm) format, Compiled HTML Help (.chm) format, and Portable Document Format (PDF).

- The HTML Help is best for viewing online. Internet Explorer and Windows 98 or later can open a ".chm" file.
- The PDF version is best for local printing, if required.

The online help and any version of it (including printed or PDF versions) are copyrighted under the following copyright:

© (2006) Her Majesty the Queen in Right of Canada as represented by the Royal Canadian Mounted Police (RCMP)

The logo for Canada, featuring the word "Canada" in a serif font with a red maple leaf above the letter 'a'.

RCMP Entrust Policy Centre

The policy centre currently in charge of RCMP Entrust is:

- Security Infrastructure Services,
Enterprise Computing Services
Infrastructure Engineering & Development,
CIO Sector,
RCMP Headquarters,
Ottawa Ontario, Canada.
K1A 0R2

Purpose Of Entrust

Treasury Board has directed the RCMP to use Entrust software to secure electronic communication.

Entrust has many security features which include strong authentication protection using a black token (a customized Entrust USB token that a user plugs into a USB port on their computer), Entrust user Identification (Entrust ID) and Password.

Entrust may also be referred to as a **PKI** (Public **K**ey **I**nfrastructure) application since it uses **PKI** objects.

Entrust is an encryption software tool that provides users with a method to send and receive protected documents to and from authorized recipients. Your Entrust ID and Password are your electronic identity, therefore you must not share them with anyone.

Note: *If you need to send or receive protected documents or email messages that are classified up to the Protected "B" level, you need Entrust. This includes the transmission and receipt of communications within protected applications such as CPIC Web, PROS IQT and Livescan.*

Entrust provides:

- Confidentiality - ensures only intended recipients are able to read documents.
- Authentication - ensures that the parties involved are who they say they are.
- Non-repudiation - prevents the sender from denying any involvement.
- Integrity - guarantees information has not been altered during transmission of the file.

Note: *When you are using Entrust encryption, if you digitally sign an e-mail or a file, it is as legally binding as your hand-written signature on a paper document.*

Entrust can only be used with sensitive data up to, and including, the Protected "B" level. Protected "C" and classified documents must be kept secured in other ways and never stored on a computer connected to NPSNet.

Primary Functions

The following are the primary functions that **Entrust** provides. More detailed information is described further in this help file.

- Document Encryption / Decryption
- Digital Signature
- Email Encryption / Decryption
- Folder Encryption with "ICE".
- Secure File Deletion

In this online help the word **Entrust** is used to refer to the Entrust software suite which includes (but is not limited to) the following software:

- **Entrust/Entelligence** (enables applications to work with Entrust/PKI)
- **Entrust/PKI** (public-key infrastructure)
- **Entrust/ICE** (file protection utility)

- **Entrust/TrueDelete** (file deletion utility)

Token Overview

To enhance security, the RCMP has chosen approved USB Federal Information Processing Standards Publication (FIPS) Level-1 hardware tokens that work with Entrust.

The token is coloured black. When you store your Entrust profile on a hardware token, you can be sure that your cryptographic information is not saved to disk. Hardware tokens are also portable and difficult to tamper with.

- If you are an RCMP employee and you need a black token for Entrust, contact the Central Help Desk.
- If you are a non-RCMP employee and you need a token for Entrust to use a specific application, contact the application's policy centre or **LRA (Local Registration Authority)** representative.

Token Software

The **Token Utilities** software package produced by **Datakey Incorporated** provides the **Cryptographic Interface Provider (CIP)** function that works with Entrust to securely store your Entrust profile on your hardware token. The token is read by the system when ready to work with encrypted documents or digital signatures.

The **Datakey CIP** function initializes the hardware token before an Entrust profile can be stored on it. For additional details, refer to **Hardware Token Initialization**.

PKI Certificate Request

The PKI Certificate Request (also known as the Entrust validation process) is a one-time process to register a person as an authorized Entrust user. To register: complete the **PKI.fab** form in **FormFlow**. After the form is signed by your supervisor, submit the form as directed by the instructions on the form. You will receive a **Reference Number** and **Authorization Code** assigned by the PKI Administration group in Ottawa. The Reference Number and Authorization Code are used to create one Entrust profile.

Normally, you will receive the **Reference Number** and **Authorization Code** in separate documents, one directly from your PKI Administrator and one from your supervisor. This is done to maintain the level of security required by Entrust.

Note: *Do not give both of your Entrust codes to anyone (not even your LAN Administrator). Do not share both of your Entrust codes with anyone.*

For instructions on activating your Entrust profile, see **Activation Overview**.

Entrust Future Direction

RCMP policy requires that you use **Entrust**, in conjunction with a **hardware token**, to secure the transmission and receipt of sensitive electronic files (up to and including the Protected "**B**" level). The hardware token provides the portable function of your Entrust Profile.

Future use of Entrust will/can include:

- Remote Access via **Contivity** (Replacement for **Defender**).
- **Forms**
- InfoWeb; protected "A" or "B" Web-based environment.
- New Applications such as:
 - CPIC Web,
 - NCDB,
 - PROS,
 - etc.

System Support

Support for Entrust is provided by the **Central Help Desk** in Ottawa: 1-800-461-7797.

ACTIVATION OVERVIEW

Activation Steps

In order to arrange access to Entrust there are three steps:

- The technical setup must be arranged by your LAN Administrator. Other technical personnel may be involved depending on your division organization. See **Activation Technical Setup** for details.
- You must apply for access. See **PKI Certificate Request**.
- You must initialize your token. See **Activation User Procedures**.

ACTIVATION TECHNICAL SETUP

Software Installation Requirement

Before a **hardware token** is initialized or an Entrust Profile is created, both the **Datakey** and **Entrust** software must be installed on the user's computer.

Normally, this will be done by the user's LAN Administrator. If a user does not have the Datakey and Entrust software installed, they should contact the **Central HelpDesk** to arrange for the installation before attempting activation.

For details on software installation, see **Software Installation Details**.

Software Installation Details

Entrust Installation Using A Script Overview

These procedures apply to Entrust Version 6.1 SP1, Datakey 4.7 with MU 6.2 and Contivity VPN Client 4.65_18.

This topic is meant for Informatics technicians, or other authorized personnel, who will setup and configure Entrust on RCMP computers. The only supported OS platform for the Protected "B" environment is Windows 2000 with SP2 or higher.

Note: *The script will run on Windows 98 SE OS but this environment will not be actively supported.*

To run the script from CD, you require administration rights.

Note: *Security and Messaging Services Section has a script that can be deployed from NAL / Zenwork without the requirement to have administration rights. See **Entrust Installation Using NAL**.*

The script has been tested and the installation has been successful on a **ROSS** workstation with the following security software configurations:

- **English language OS**

Win2k sp2, Entrust v5.02 sp7, No datakey, Ikey2000 PE.
Win2k sp2, Entrust 6.0, datakey 4.6
Win2k sp2, Entrust 6.1 sp1, datakey 4.7, Contivity 4.65 or 4.10

Windows 98SE, Entrust 5.02 sp7, Ikey2000 PE
Windows 98SE entrust 6.0 Datakey 4.6

- **French Language OS**

Win2k sp2, Entrust v5.02 sp7, No datakey, Ikey2000 PE.
Win2k sp2, Entrust 6.0, datakey 4.6
Win2k sp2, Entrust 6.1 sp1, datakey 4.7, Contivity 4.65 or 4.10

Windows 98SE, Entrust 5.02 sp7, Ikey2000 PE
Windows 98SE Entrust 6.0 Datakey 4.6

Note: *Installation results may differ if any other software version or patch not identified preceding was installed on the workstation.*

The scripts have been designed to perform the following activities:

- remove old Datakey / Rainbow drivers,
- remove old versions of Entrust Entelligence,
- install Entrust Entelligence 6.1 SP1, SP 70850,
- install Datakey 4.7 MU 6.2 (dual-headed driver),
- install Contivity VPN 4.65 (option), and
- install the root Production CA certificate (required for the Truepass authentication process).

Entrust Installation Using a CD

Before running the setup file, make sure you do the following:

- close all applications,
- remove the token from the USB port, and
- make sure you have Administration rights.

Note: *Windows 98 Operating System known issues - if you are running the script with Entrust Version 5.02 sp7 already installed on your workstation, you may be required to re-run the script a second time to eliminate issues that are not possible to correct on the first run.*

1. Run the appropriate **SETUP.exe** file - the script chosen is dependent on your computer's Operating System (OS) language as shown following:
 - For an **English** language OS, insert the installation CD and run the **SETUP.exe** file located in the **Script4.5\EnglishOS** folder on the CD.
 - For a **French** language OS, insert the installation CD and run the **SETUP.exe** file located in the **Script4.5\FrenchOS** folder on the CD.
2. When using Windows 2000 OS, only one reboot of the system will be required; however on Windows 98SE, rebooting of the system up to **two** times may be required.
3. Insert your token in one of your computer's USB ports.
 - On Windows 98 OS only, you may be prompted to provide the "Rainbow IKey Disk"



Click on the [OK] button and then browse to the following path:
C:\Program Files\Rainbow Technologies\Ikey Driver\Drv\Win98.

- If you don't have a profile stored on your token yet, you will need to initialize it (see **Hardware Token Initialization**).
4. After your token has been initialized, you are now ready to create or recover your Entrust profile - see **Entrust Profile Creation** or ****Entrust Profile Recovery**.

If you have followed the above noted instructions and you are having technical difficulties you should :

- Re-run the script a second time,
- If re-running the script has not solved your problem, use the Windows **ADD/Remove Programs** function to remove the security software in the following order: **Rainbow Ikey Driver, Datakey CIP, Entrust Desktop Solutions** and **Nortel Networks Contivity VPN Client** and then re-run the script.

For any additional help, call the Central Help Desk.

Entrust Installation Using NAL

This topic is for LAN Managers and NSS personnel who use the Network Application Launcher (NAL) to deploy software.

Application Objects Required

Three application objects are required to deploy and install the **Entrust 6.1, Datakey** and **Contivity** applications using a script. The applications are packaged in scripting software. An executable is created to install the applications. The first **SETUP.EXE** is a wrapper which calls the other **.EXEs** to do the actual installation of the three applications.

A single application object created to install the applications will produce an error when that object calls more than one **.exes'** which are part of wrapper. System level privileges are granted to the first **.EXE** file for execution. After the first **.EXE** is unloaded from memory, system level privilege is not granted to the other **.EXEs'** in the wrapper. To prevent the NAL from producing the error, three application objects are required to deploy the Entrust / Datakey / Contivity script package.

The application objects names are **Admin Group Rights, Entrust Script Setup** and **Admin Group Rights Remove**.

There are two Application object dependencies:

1. **Entrust Script Setup** depends on Admin Group Rights.
2. **Admin Group Rights Remove** depends on Entrust Script Setup.

Admin Group Rights

Admin Group Rights object grants the user Administrator privileges on the Windows 2000 workstation and logs the user off the network.

Entrust Script Setup

Entrust Script Setup runs SETUP.EXE which is the wrapper for the applications to be installed. This object installs Entrust 6.1, Datakey and Contivity (if it is required) on the workstation/laptop.

Admin Group Rights Remove

Admin Group Rights Remove removes the user's Administrator privileges and logs the user off the network.

NAL Setup for Entrust / Datakey / Contivity Package

NAL is used, by the RCMP, to deploy Entrust / Datakey / Contivity package to workstations and laptops connected to a ROSS server. The instructions below shows how to create the NAL objects to deploy the Entrust / Datakey/ Contivity package.

Requirements:

- Windows 2000 Professional SP2 through to SP4.
- Novell Netware, version 5.1 or the latest version.
- ZENworks Application Launcher Explorer, version 3.2 or the latest version.
- Entrust / Datakey / Contivity script package. The script package is zipped with software for English and French language OS. Filename for the zipped file is Script45.zip.
- WinZip, version 8, installed on your computer.

Before proceeding please ensure:

- You have administrative rights to the Netware server.
- A drive letter is mapped to the Netware server. In this document, it is assumed that G is mapped to *SERVERNAME*\ROSS:Apps. Substitute the appropriate drive letter if it is different from G.

Procedures

Three application objects are required to deploy the Entrust / Datakey / Contivity package on workstations and laptops, connected to a ROSS server.

Copy the software to the Netware server:

- On the Intranet, go to the download site and download the zipped file Script45.zip to the local drive.
- Create the folder Entrust611 on G:\Apps.
- Right click on Script45.zip and select Extract to...
- In the Extract window, enter G:\Apps\Entrust611 and click on the Extract button. The files will be unzipped and stored under G:\apps\Entrust611. See Note.
- Exit from WinZip.


Note: *Two folders created under G:\Apps\Entrust611 includes English OS where the English script files are, and French OS where the French script files are. Also, logoff.exe, notepad.exe and popup.txt are located under G:\Apps\Entrust611.*

Application Object #1 - Admin Group Rights

1. Open **ConsoleOne**, go to the container where application objects are created. Right click on the container, select **New > Object**. In the **New Object** window, select **App:Application** and click on the **[OK]** button.
2. In the **New Application** screen, **Manually** (no .aot/.axt or .msi file) is selected by default. Click on the **[Next>]** button.
3. In Object name: field enter Admin Group Rights.
4. Click on **Display details after creation** to place a check mark against it.
5. Click on the **[Finish]** button.
6. The Properties of Admin Group Rights screen appears.
 - At the **Identification** tab, in the **Application icon title:** field enter **Entrust 6 Setup**.
 - Select **Run Options** tab and **Application**. Click on **Path to executable file:** and enter **net localgroup administrator /add interactive**.
 - On the **Run Options** tab, select **Environment**. Under **Executable security level:** select **Run as unsecure system user**.
 - On the **Run Options** tab, select **Launch Scripts**. In **Run before Launching** enter:
`##/servername\ross\apps\Entrust611\notepad.exe g\apps\entrust611\popup.txt` (where *servername* is the name of your server).
 - In the **Run after Termination** window enter:
`##/servername\ross\apps\Entrust611\logoff.exe /n` (where *servername* is the name of your server).
 - Click on the **Associations** tab. To distribute the Entrust/Datakey/Contivity package to the desired recipients, click on the **[Add]** button. Select the desired user(s), user group(s) or container containing the users.
 - Click on the **[OK]** button to exit **Properties of Admin Group Rights** screen.

Application Object #2 - Entrust Script Setup

1. Open **ConsoleOne**, go to the container where application objects are created. Right-click on the container, select **New > Object**. In the **New Object** window, select **App:Application** and click on the **[OK]** button.
2. In the **New Application** screen, **Manually** (no .aot/.axt or .msi file) is selected by default. Click on the **[Next>]** button.
3. In Object name: field enter Entrust Script Setup.
4. In Path to executable: enter `G:\apps\Entrust611\language OS/setup.exe`. (*language OS* = English OS or French OS).
5. Click on **Display details after creation** to place a check mark against it.
6. Click on the **[Finish]** button.
7. The Properties of Entrust Script Setup screen appears.

- Select **Run Options > Application**. Click on **Run application once**. A check mark appears against it.
- Click on the **Associations** tab. To distribute the Entrust/Datakey/Contivity package to the desired recipients, click on the **[Add]** button. Select the desired user(s), user group(s) or container containing the users.
- Under **Associations**, click on the selection box under the  (associate with) symbol to place a check mark in it. e.g.,




- Click on the **Availability** tab and select **System Requirements**.
- Click on the **[Add]** button, select **Application**.
- The **Application Dependencies** screen appears. Click on the drop-down list and select **False** for **Show application icon even if criteria are not met**.
- In the field for **Application Object Name**, select **Admin Group Rights** and then click on the **[OK]** button.
- Ensure **Application is installed** is enabled.
- Click on the **[OK]** button and then click on the next **[OK]** button to exit.

Application Object # 3 - Admin Group Rights Remove

1. Open **ConsoleOne**, go to the container where application objects are created. Right-click on the container, select **New > Object**. In the **New Object** window, select **App:Application** and click on the **[OK]** button.
2. In the **New Application** screen, **Manually (no .aot/.axt or .msi file)** is selected by default. Click on the **[Next>]** button.
3. In Object name: field enter Admin Group Rights Remove.
4. Click on **Display details** after creation to place a check mark against it.
5. Click on the **[Finish]** button.
6. The Properties of Admin Group Rights Remove screen appears.
 - Select **Run Options** tab and **Application**. Click on **Path to executable file:** and enter **net localgroup administrator /delete interactive**.
 - Click on **Run application once** to place a check mark against it.
 - On the **Run Options** tab, select **Environment**. Under **Executable security level:** select **Run as unsecure system user**.
 - On **Run Options** tab, select **Launch Scripts**. In the **Run after termination** window enter

##/servername\ross\apps\Entrust611\logoff.exe /n (where servername is the name of your server).

- Click on the **Associations** tab. To distribute the Entrust/Datakey/Contivity package to the desired recipients, click on the **[Add]** button. Select the desired user(s), user group(s) or container containing the users.
- Under **Associations**, click on the selection box under the  (associate with) symbol to place a check mark in it. e.g.,



- Click on the **Availability** tab and select **System Requirements**.
- Click on the **[Add]** button and select **Applications**.
- The **Application Dependencies** screen appears. Click on the drop-down list and select **False** for **Show application icon even if criteria are not met**.
- In the field for **Application Object Name**, select **Entrust Script Setup** and then click on the **[OK]** button.
- Ensure **Application is installed** is enabled.
- Click on the **[OK]** button and then click on the next **[OK]** button to exit.

ACTIVATION USER PROCEDURES

Hardware Token Initialization

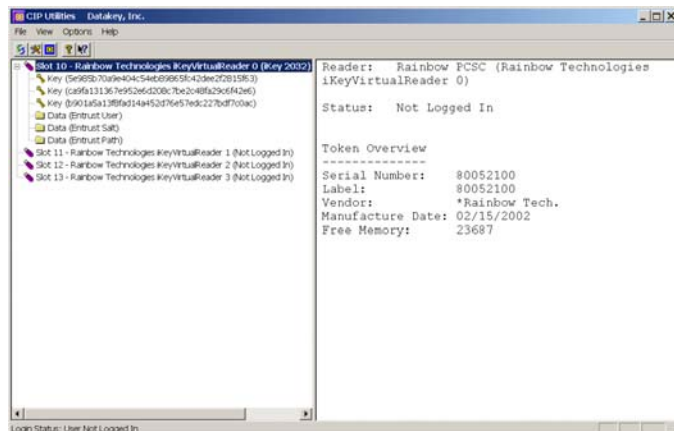
The hardware token is initialized for the following reasons:

- A user has received a new token.
- A user is storing their Entrust profile on a hardware token.
- A user cannot remember their Entrust password.

Note: *If you do not have the Datakey and Entrust software installed on your computer, contact the Central Help Desk to arrange for installation before attempting activation.*

To initialize the token do the following:

1. Insert your token in a USB port on your computer.
2. Click on Start | Programs | Entrust | Datakey CIP | CIP Utilities. The CIP Utilities dialog box appears.



3. Right-click on the Slot that identifies Rainbow Technologies iKeyVirtualReader. Select Initialize Token. The **WARNING! Token Initialization - Read carefully before continuing** dialog box appears.



4. Click on Continue Initialization.

The **Token initialization complete, Warning! Change pass phrase!** dialog box appears.



The **New Pass Phrase = PASSWORD** line means that the default password, is "PASSWORD").

Note: Remember that your default password is **PASSWORD** in upper- case letters.

5. Click on **OK**.
6. Click on **File | Exit**.

Entrust Profile

Entrust Profile Creation

Note: Your token must be initialized before your create your Entrust Profile. See **Hardware Token Initialization**.

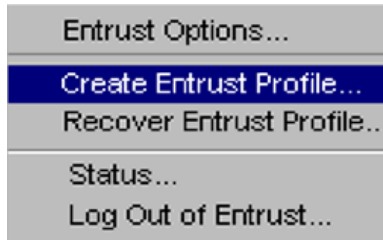
1. Insert your token into the USB port before starting up your computer.
2. Make sure your computer is connected to your network.
3. In the Windows task bar, click the Start button | Programs | Entrust | Entrust Profile | Create Entrust Profile

OR

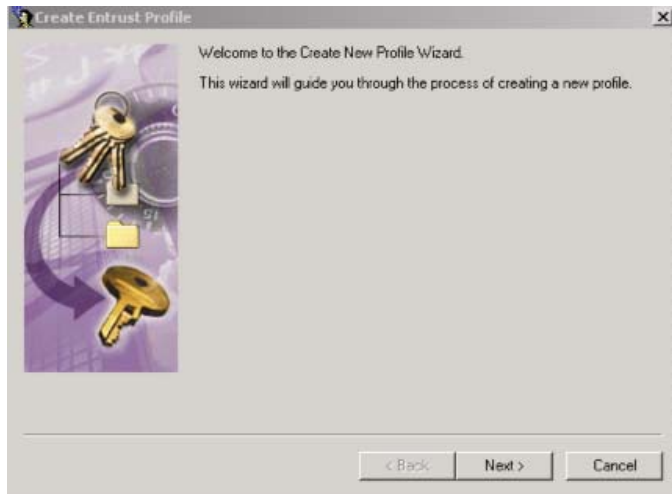
Right-click the **Entrust** icon in the Windows system tray (the yellow key with the red x above it).



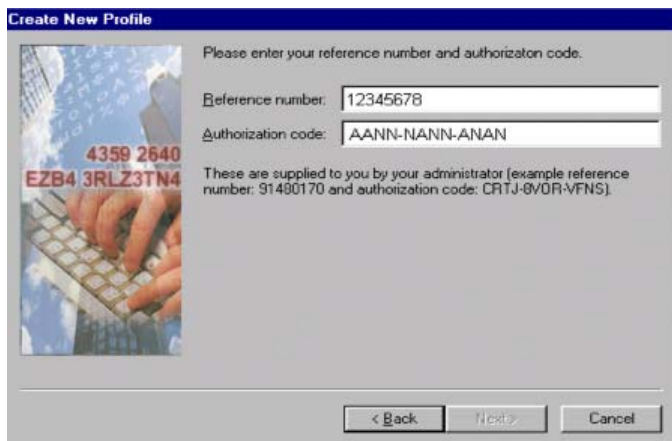
4. From the pop-up menu, select **Create Entrust Profile**.



The Welcome to the Create Entrust Profile Wizard dialog box appears.



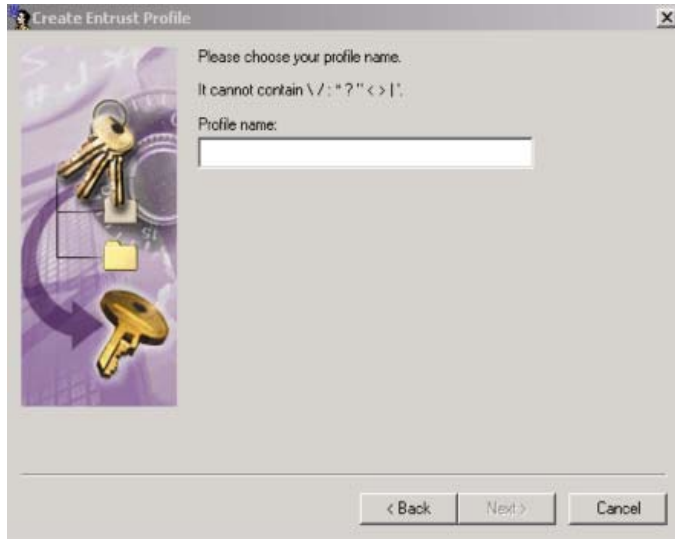
5. Click on **Next>**.



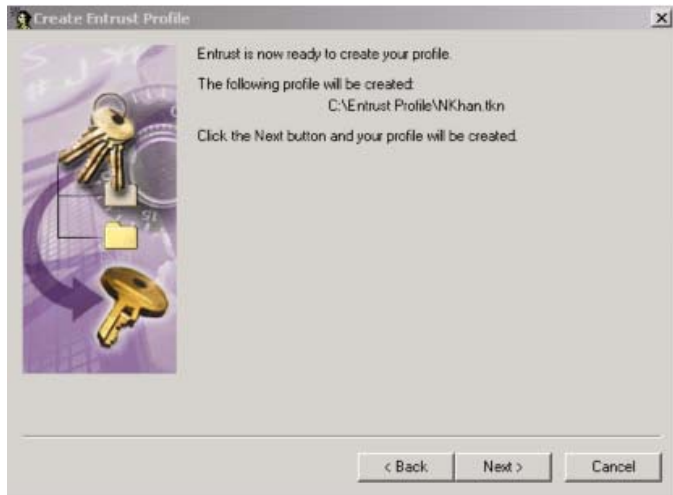
6. In the **Reference Number** field, enter the eight digit numeric **Reference Number** that was supplied to you by your **Public Key Infrastructure (PKI) Administrator**.
7. In the **Authorization Code** field, enter the 12 character **Authorization Code** (as shown in upper-case and with hyphens) that was supplied to you by your **Local Registration Authority (LRA)**.
8. Click on **Next>**.



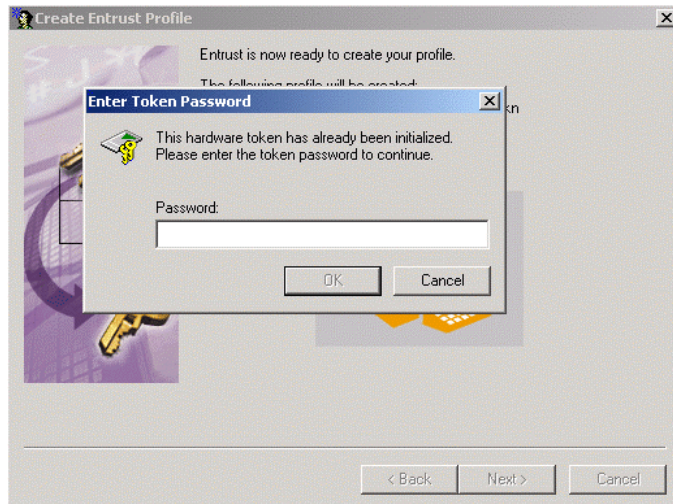
9. In the **Select a folder within which to store your profile** field, ensure that the path **C:\Entrust Profile** is displayed. Ensure the **Store profile on hardware token (card)** checkbox is selected. Your Entrust profile (.epf) file is written to the token.
10. Click **Next>**.



11. In the **Profile name** field, enter your full name OR your Employee Number.
12. Click **Next>**. The Entrust is now ready to create your profile confirmation window appears.



13. Click **Next>**. The **Enter Token Password** dialog box appears.



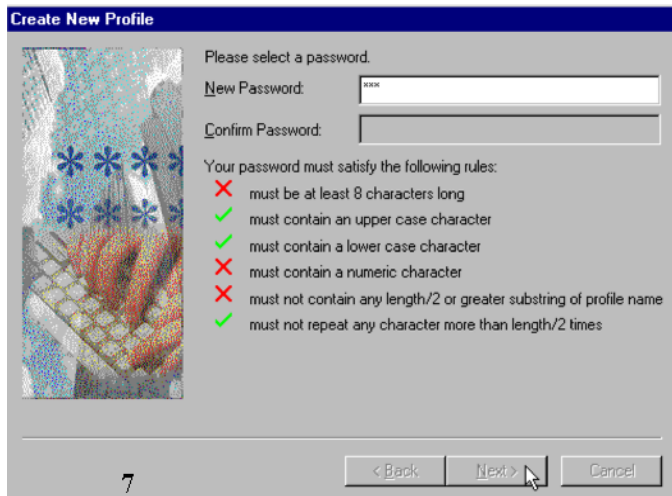
14. In the **Password:** field, enter the default Password supplied when you initialized your Token, in upper case letters., i.e., **PASSWORD** (the standard default password).
15. Click on the [**OK**] button. The **Enter Token Password** dialog box will disappear.
16. Click on the [**Next>**] button.
17. The Your Entrust profile has been successfully created dialog box appears.
18. Click **Finish**.

VERY IMPORTANT: *Once your profile has been created on your token with the system default Password, you are required to change the default Password by right clicking on the Toolbar and choosing Entrust Options.*

19. Changing your Password:

- Right click on the Entrust Key Icon located on the Toolbar and select **Entrust Options**.

- The **Entrust Login** dialog box appears.
- Enter the **Default Password**.
- The **Entrust Options** dialog box appears.
- Select the **Change Password...** option.
- The **Welcome to the change Entrust Password Wizard** dialog box appears.
- Please enter the **Default Password**.
- Click **Next>**. The **Please select a password** dialog box appears.



IMPORTANT NOTE: *Ensure that 'Caps Lock' is turned off when entering your password.*

- Create a password based on the rules identified in the dialog box.
- Enter a new password in the **New Password** field. As you type your password, you will notice each red "X" will change to a green "checkmark" as you satisfy the rules.
- Re-enter your password again in the **Confirm Password** field.
- Click on the [**Next>**] button. You will receive confirmation that you have successfully changed the default password.
- Click on the [**OK**] button and then click on the next [**OK**] button.

You are now logged on to Entrust.

- Right-click on the Entrust yellow key icon located on the bottom taskbar and select **Log Out of Entrust**.

Note: *The Signing Private Key on your token has an expiry date. See **Token Expiry** for details.*

If you forget your Password, you will have to contact your Local Registration Authority (**LRA**) to obtain a new **Reference Number** and **Authorization Code**. See **Entrust Profile Recovery With Token** for additional details.

Entrust Profile Recovery With Token

Note: *Your token must be initialized before you can recover your Entrust Profile. See **Hardware Token Initialization**.*

You need to recover a profile if:

- you've lost the original one, or
- the original one is damaged, or
- you've forgotten your password, or
- you suspect that someone has tampered with your profile.

If you don't remember your previous Entrust **Password**, contact your **Local Registration Authority (LRA)** to obtain a new **Reference number** and **Authorization code**.

To recover your Entrust profile:

1. Insert your token into the USB port before starting up your computer.
2. Make sure your computer is connected to your network.
3. In the Windows taskbar, click Start > Programs > Entrust > Entrust Profile > Recover Entrust Profile,

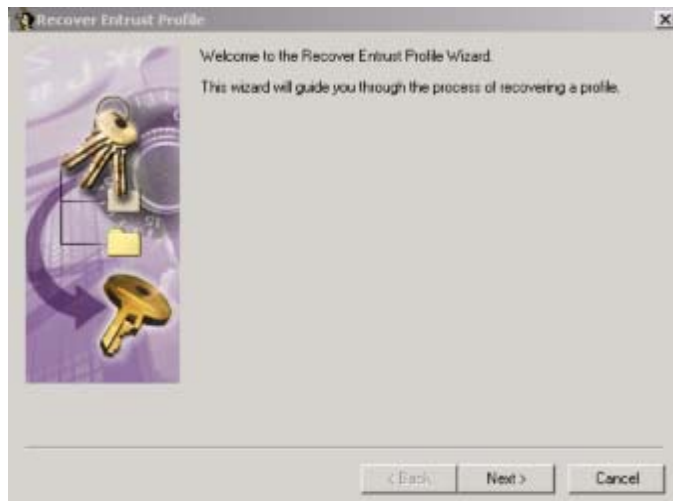
or,

Right-click the Entrust icon in the Windows tray (the yellow key with the red X above it).



4. Click **Recover Entrust Profile** from the pop-up menu.

The **Welcome to the Recover Entrust Profile Wizard** dialog box appears.



5. Click on **Next>**.

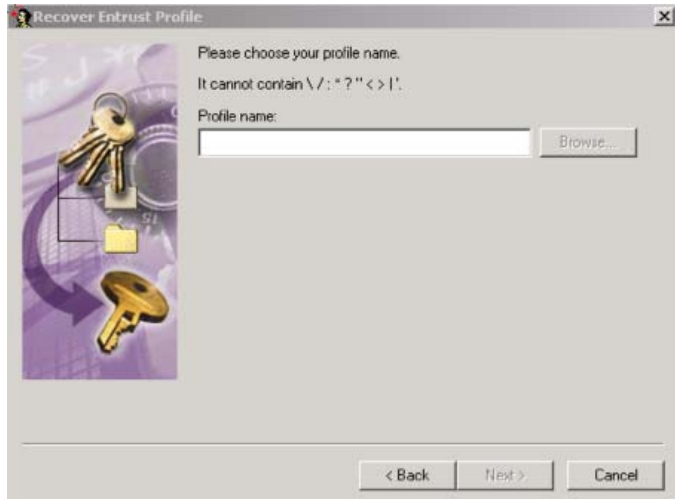
The Please enter you reference number and authorization code dialog box appears.



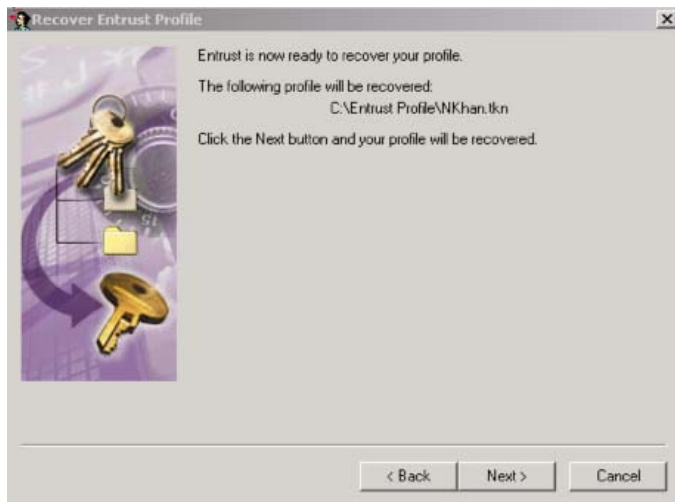
6. In the **Reference number** field, enter the eight digit numeric Reference Number that was supplied to you from your **PKI** Administrator
7. In the **Authorization code** field, enter the (12) character Authorization Code as shown in upper-case and with hyphens.
8. Click on **Next>**.



9. In the **Select a folder within which to store your profile** field, ensure that the following path is displayed: C:\Entrust Profile.
10. Ensure the **Store profile on hardware token (card)** checkbox is selected. Your Entrust profile (.epf) file is written to the token.
11. Click on **Next>**.
12. In the **Profile Name** field enter your full name **OR** your Employee Number.



13. Click **Next>**. A confirmation window appears.



14. Click on the [**Next>**] button. The **Enter Token Password** dialog box appears.
15. In the **Password:** field, enter the default Password supplied when you initialized your Token, in upper case letters., i.e., **PASSWORD** (the standard default password).
16. Click on the [**Next>**] button.
17. The next dialog box, Your Entrust profile has been successfully recovered appears. Do not insert a check mark in the "I want to export my Entrust credential" box.
18. Click **Finish**.

VERY IMPORTANT: *Once your profile has been recovered on your token with the System Default Password, you are required to change the Default Password by right clicking on the Toolbar and choosing Entrust Options.*

19. Changing your Password:
 - Right-click on the Entrust Key Icon located on the Toolbar and select **Entrust Options**.

- The **Entrust Login** dialog box appears.
- Enter the Default Password.
- The **Entrust Options** dialog box appears.
- Select the **Change Password...** option.
- The **Welcome to the change Entrust Password Wizard** dialog box appears.
- Enter the **Default Password**, i.e., **PASSWORD** (the standard default password).
- Click **Next>**.

The **Please select a new password** dialog box appears

Important Note: *Ensure that 'Caps Lock' is turned off when entering your password.*

- Create a password based on the rules identified in the dialog box.
- Enter a new password in the **New Password** field. As you type your password, you will notice the red "X" will change to a green "checkmark" as you satisfy the rules.
- Re-enter your password again in the **Confirm Password** field.
- Click on the [**Next>**] button. You will receive confirmation that you have successfully changed the default password.
- Click on the [**OK**] button and then click on the next [**OK**] button.

You are now logged in to Entrust.

- Right-click on the Entrust yellow key icon located on the bottom taskbar and select **Log Out of Entrust**.

Note: *The Signing Private Key on your token has an expiry date. See **Token Expiry** for details.*

Token Expiry

Your **Signing Private Key** stored on your Entrust token will expire **183 days** from the date that you have created or recovered your Entrust profile. To update your key, you must log in online to Entrust at least once **between day 127 and 183** for an update of your security keys to be loaded on your token. The system will not update your keys if you have logged in before day **127**.

You should log in with your Entrust token at least once every three months.

ENTRUST LOGIN/LOGOUT

Entrust Login

To log in to Entrust:

1. Insert the hardware token into the USB port
2. In the Windows taskbar, click Start > Programs > Entrust > Entrust Login.

OR

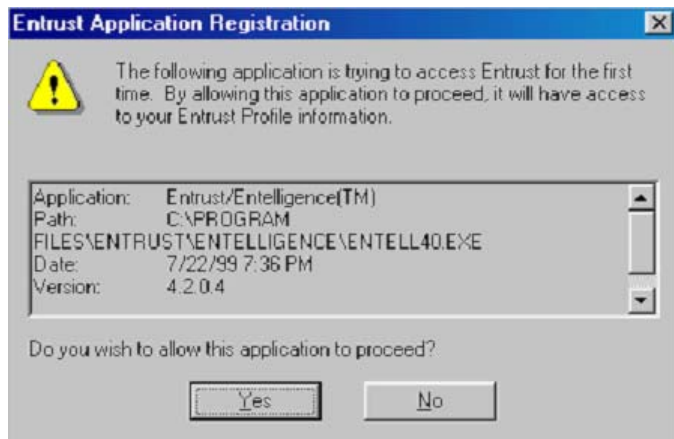
Right-click the Entrust icon in the Windows tray in the taskbar. Click **Log in to Entrust** in the pop-up menu. The **Entrust Login** dialog box appears.



Ensure that your **Profile name:** field shows a card graphic preceding your Profile Name. This means that your profile was correctly found on the Ikey Token.

3. Enter your password in the **Password** field and click **OK**.

The message dialog box will appear the first time a new Entrust-Ready application tries to access your Entrust profile.



4. Click **Yes** to login to Entrust.

A successful login to Entrust is indicated by the ‘**Yellow Key**’ without the ‘**red X**’.



Note: *If you have forgotten or mistyped your Password, you have ten attempts to type in a valid Password. After the tenth try your token will become unusable and you will require a new token.*

Entrust Logout

To prevent unauthorized users from decrypting and viewing your secured files, signing files or securely deleting files while you are away from your workstation, you should log out of Entrust.

To Logout:

1. Right-click the Entrust/Entelligence icon (the yellow key) in the system tray.



2. From the pop-up menu, select Log Out of Entrust.





A successful Log Out is indicated by a red **X** displayed over the yellow key.



Note: *Remember to remove your token and store it in a secured location.*

Entrust Single Login icons

The Windows tray in the taskbar displays your Entrust Single Login status. You will see one of four Entrust Single Login icons.

Entrust Single Login Icon	What It Means
	You are logged in to Entrust.
	Entrust has been locked because the inactivity period has expired or you used the hotkey to lock Entrust. An Entrust-Ready application is still using your profile.
	Entrust has been locked because the inactivity period has expired or you used the hotkey to lock Entrust. However, there is at least one Entrust-Ready application running that does not support Entrust Single Login. This application is not locked.
	Entrust has been locked because the inactivity period has expired or you used a hotkey to lock Entrust. There are no other Entrust-Ready

	applications running. You are logged out of Entrust.
--	---

Tip: *You can also check if you're working offline or online by opening the Entrust Status dialog box. Right-click the Entrust icon in the Windows tray. Click Status in the pop-up menu to open the Entrust Status dialog box. You will see the message "Working Offline" or "Connected to Entrust".*

Entrust Options Settings

To access the Entrust Options dialog box, do one of the following:

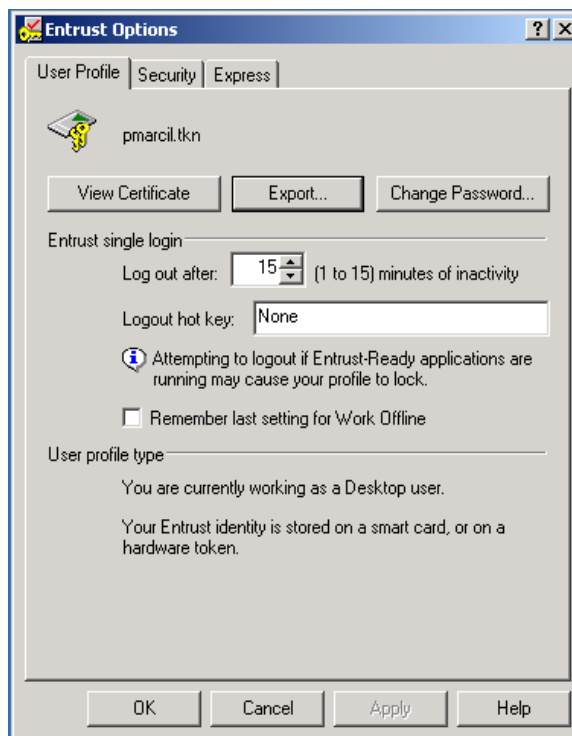
1. In the Windows taskbar, click the **Start > Programs > Entrust>Entrust Options**;

OR

2. Right-click the **Entrust** icon in the Windows system tray.



3. From the pop-up menu, click **Entrust Options**. The **Entrust Options** dialog box will appear.



From the **Entrust Options** dialog box, you should use the default settings of the program except for those described in **Time-Out** and **Password Change**.

If you want to be able to export and import certificates or keys with an Entrust user outside ROSS, you will also use the **Export...** option (see **Export/Import Key**).

Time-Out

The time-out period reduces the risk of unauthorized use or access of your Entrust Application while your logged in but away from your computer. The default in the **Log out after** field should be set to five minutes.

Setting the time-out to five minutes means that Entrust will automatically log you out after the time has elapsed after no activity.

Password Change

Click **Change Password...** and follow the prompts. Ensure that your new password satisfies all the rules. It is recommended that you change your password every three months.

Note: *If you have forgotten your password, contact the **Central Help Desk** in Ottawa.*

Export/Import Key

To export an encrypted file to a person who does not have access to RCMP Entrust you have to arrange for them to receive your Entrust key file that will enable access. This step must be approved by the Departmental Security Branch. For procedures, see **Key Export**.

To import an encrypted file from a person who does not have access to RCMP Entrust, see **Key Import to Address Book**.

Key Export

To allow Entrust users in other security domains that are not certified to send protected files to you, you must first arrange to give them your Entrust key file.

- Contact the Departmental Security Branch for approval before you export anything.

You should give these users the key file and the validation string separately (unless you give them this information in person). For example, you can send people the key file as an email attachment or stored on a diskette, and tell them the validation string in person or by telephone.

Note: *Remember that you must provide these people the validation string associated with your key file or the export will not work.*

When you give someone the validation string, you must use a method that guarantees its authenticity. For example, if you tell them the validation string by telephone, the validation string can only be considered authentic if the person to whom you give the validation string can recognize your voice.

Note: *It is best to export a new key file whenever you want to give your key file to someone. This permits immediate testing of the key file.*

To export your key file:

1. Access the Entrust Options dialog box (see Setting Options in the Entrust Options Dialog Box for details).
2. From the **Entrust Options** dialog box, click on the [**Export...**] button. The **Export Entrust Credentials** window appears.



3. Select the [Next>] button.
4. In the **Select a folder** box, enter "**c:\Entrust Profile**" and click on the [Export] button.
5. Click on the [Finish] button.
6. Send your key file from the **c:\Entrust Profile** folder to the user.

Key Import to Address Book

If you want to exchange protected files with someone whose computer is in a domain that is different from yours and is not cross-certified to securely exchange key information with your domain, you need to obtain that person's Entrust key file and associated validation string,

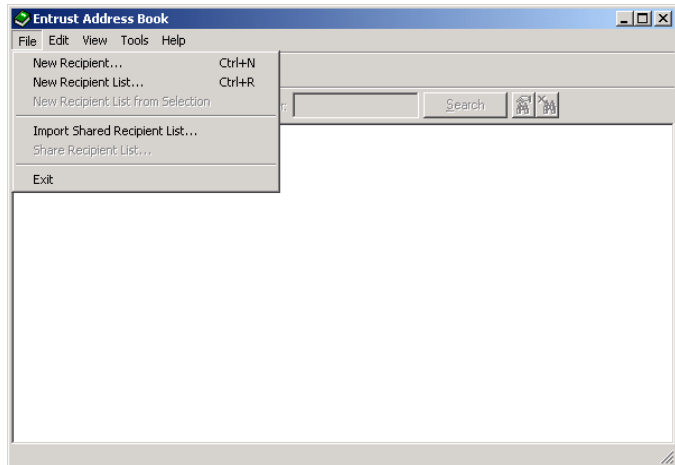
An Entrust key file provides the information required to allow you to encrypt files for someone using Entrust in another non-cross-certified domain.

As people give you copies of their Entrust key files and validation strings, import the information into your Address Book.

An Address Book contains the Entrust key files of people in other non cross-certified domains with whom you plan to exchange protected files.

After you have received the key and validation string from a user outside your domain, you can import files using the following steps:

1. Right-click on the Entrust icon (yellow key) in the bottom task bar and select the **Entrust Address Book...** option. The **Entrust Address Book** window will appear.



2. Click on **File** and then select the **New Recipient...** option.
3. Point to where the .key file is located (e.g., **a:\user.key**) and click on the [**Open**] button. A confirmation screen will appear indicating that the certificate has been imported in your **Personal Address Book**.
4. After the certificate has been imported, you can go ahead and encrypt files for that person.

OFFLINE WORK PROCEDURES

Offline Work Overview

Working offline means using Entrust or an Entrust-Ready application without connecting to the Entrust Directory or the rest of Entrust/PKI. Whenever possible, you should work online to ensure full security when you encrypt and verify data. However, you may need to work offline if your network connection is unavailable. If you're faced with this situation, your Entrust-Ready application will display a message indicating that you must work offline.

The option to **Work offline** is available to you in the **Entrust Login** dialog box the first time you start an Entrust session and each time you log in to Entrust.



Whenever you work offline, be aware of the following security implications:

- Your profile will not be updated, so if you work offline for a very long time, your certificates may expire.
- You may successfully verify a signature made by a user whose certificate is no longer valid. It is recommended that you re-verify any signatures when you establish a network connection.
- You may encrypt a file for an invalid user, for example, for a user whose certificate has been revoked.
- You may not have access to other user's certificates or to the most up-to-date certificate revocation lists.
- You can only secure files for people in the Entrust Address Book or recipient lists that you've already used.

Offline Login

1. Ensure your hardware token is in the USB port.
2. Click **Start > Programs > Entrust > Entrust Login** in the Windows taskbar.

The **Entrust Login** dialog box appears with your profile id.



3. Enter your password.
4. Select **Work offline**. The following message appears:

"If you work offline, Entrust will not be able to retrieve the most up-to-date security information for you and other users. It's a good idea to work online whenever possible."
5. Click **OK** to close this message.
6. Click **OK** in the **Entrust Login** dialog box.



You're now logged in without a connection to the Entrust Directory and the rest of Entrust/PKI.

Offline / Online Switch

You can switch between working offline and working online at any time during an Entrust session.

Whenever possible, you should work online to ensure full security when you encrypt and verify data. However, you may need to work offline if your network connection is unavailable. If you're faced with this situation, your Entrust-Ready application will display a message indicating that you must work offline.

To switch between working offline and online:

1. Right-click the Entrust icon in the Windows tray.



2. Click **Work offline** in the pop-up menu.

You'll know you're working offline if there's a checkmark beside the menu entry. If there's no checkmark, you are working online.

Tip: You can also check if you're working offline or online by opening the **Entrust Status** dialog box. Right-click the Entrust icon in the Windows tray. Click **Status** in

*the pop-up menu to open the **Entrust Status** dialog box. You will see the message "**Working Offline**" or "**Connected to Entrust**".*

ENTRUST FILE PROCESSING

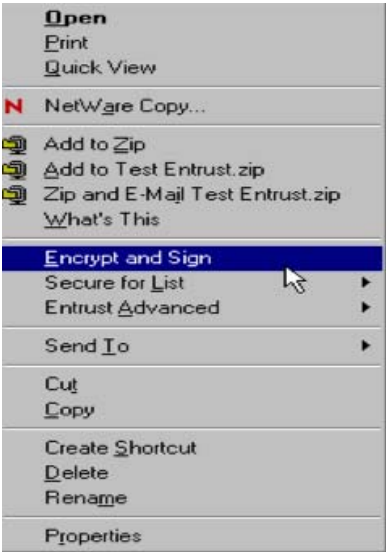
Encrypting & Signing

File types you can secure include those saved in any Word Processing, Spreadsheet, or E-mail.

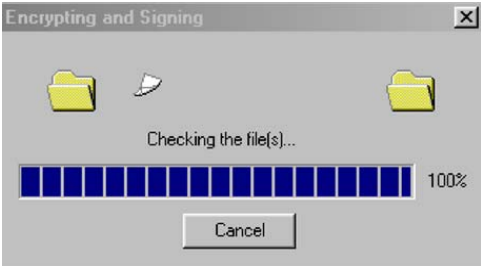
You can encrypt and sign files for yourself, or distribute encrypted files to recipients of your choice. You can provide additional assurance to your recipients by digitally signing the protected files. Your digital signature guarantees that the file(s) came from you and have not been altered since you signed them.

Encrypting Files For Yourself

1. Navigate to where your files are located using **Windows Explorer**.
2. Right-click the file(s) you want to protect.
3. From the pop-up menu, click **'Encrypt and Sign'**.

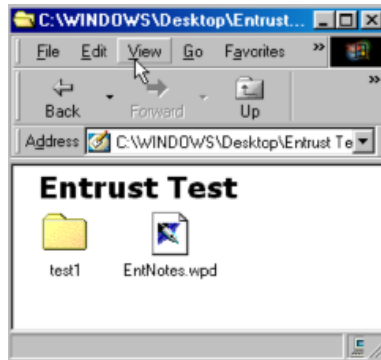


The **'Encrypting and Signing'** dialog box appears while the file is being encrypted.

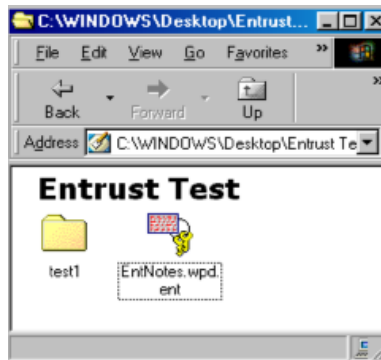


Note: *Entrust encrypts the selected files, replacing the originals with secured files. The encrypted file will have an .ent extension and Entrust icon.*

Decrypted File:



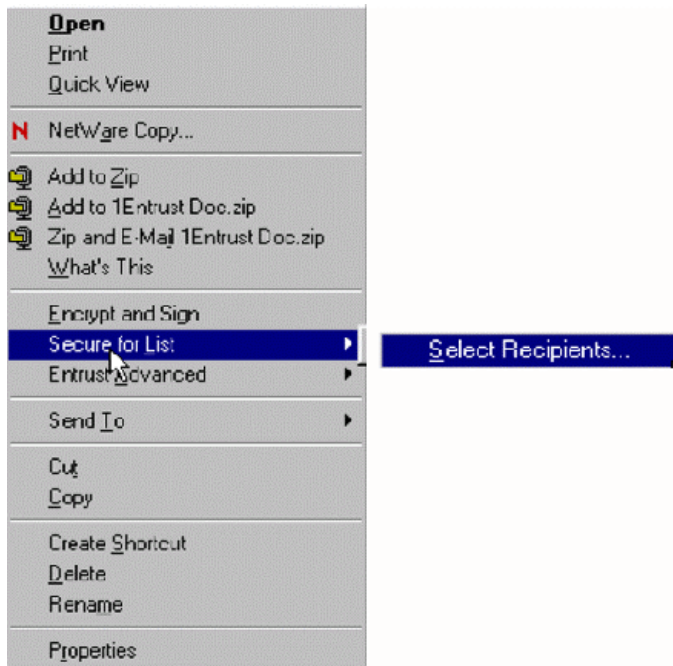
Encrypted File (.ent):



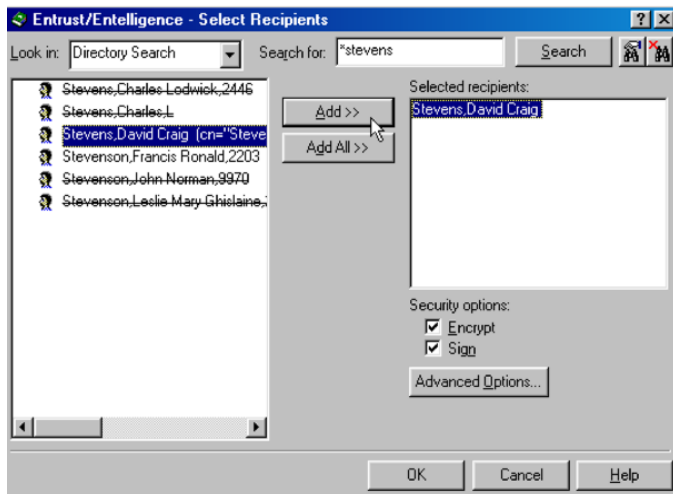
Encrypting Files For Recipients

You can encrypt files for individuals who have entries in your Entrust Directory or your Entrust Address Book. Only those you designate as recipients will be able to decrypt your files. You are automatically included as a recipient for each file you encrypt. This means you can decrypt any file you encrypt for others

1. Start Windows Explorer and navigate to where the file(s) are located.
2. Right-click the file.
3. From the pop-up menu, select Secure for List | Select Recipients....



The **Select Recipients** dialog box is displayed.



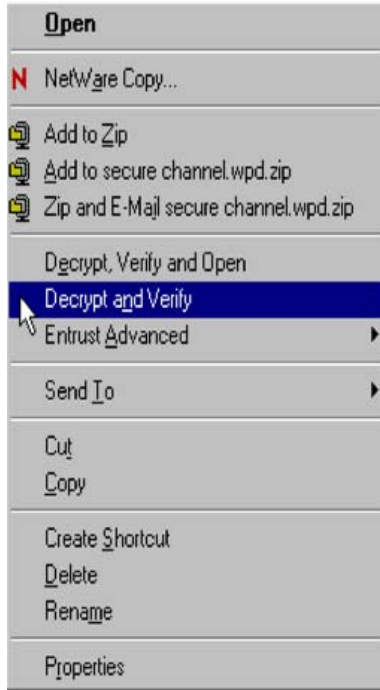
4. For **Look in:**, select Directory Search or Personal Address Book from the drop-down list.
5. For **Search for:**, enter the last name of the recipient.
6. Select a recipient or recipients in the list and drag and drop it onto the **Selected recipients:** list.
7. Click **OK**. The file is now secured for the selected recipient(s).

Decrypt and Verify Secured Files

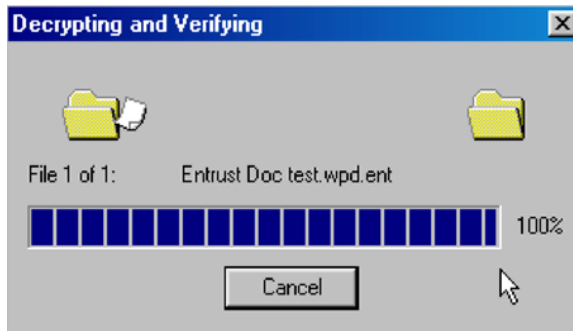
Decrypting a secured file is the process of returning a protected document to its original state, readable plaintext. You will not be able to view the contents of a protected file until it has been decrypted. A valid digital signature verifies the

originator of the file while guaranteeing that the file has not been modified since it was signed.

1. Start **Windows Explorer** and navigate to where the encrypted file(s) are located.
2. Right mouse click the encrypted file.
3. From the pop-up menu, select '**Decrypt and Verify**'.



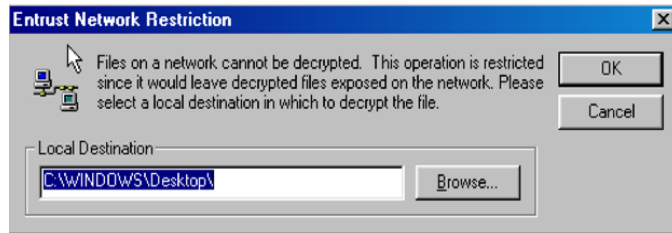
The **Decrypting and Verifying** dialog box appears displaying the selected file that is being decrypted.



4. Before attempting to decrypt a file, copy the file(s) to your local hard drive first.

Note: *You cannot decrypt a file on the network.*

If you try to decrypt a file on the network, you will see the **Entrust Network Restriction** dialog message.



The dialog box allows the selected encrypted file to be decrypted to a local hard drive destination. Just **Browse** to the location and click **OK**.

Decrypt, Verify and Open Secured File

You can double-click an encrypted file and it will be opened with the associated application. An encrypted file has an **.ent** extension.

OR

Use the following procedure:

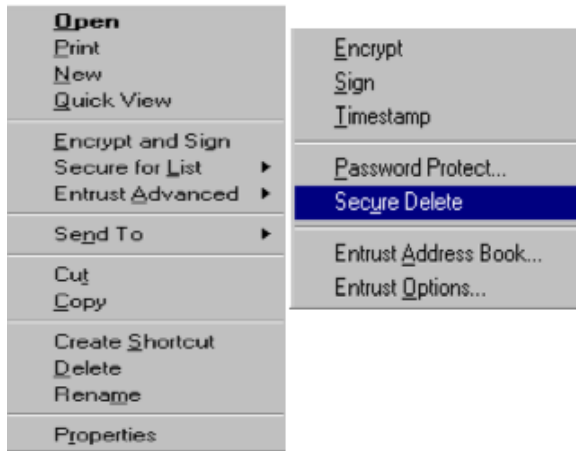
1. Start **Windows Explorer** and navigate to where the encrypted file(s) are located.
2. Right mouse click the encrypted file.
3. From the pop-up menu, select **Decrypt, Verify and Open**. The file will be opened in the associated application.

Note: *The most common reason a file cannot be decrypted is that you were not selected as an authorized recipient. If you were intended to be a recipient, contact the sender and have them encrypt and re-send the file to you.*

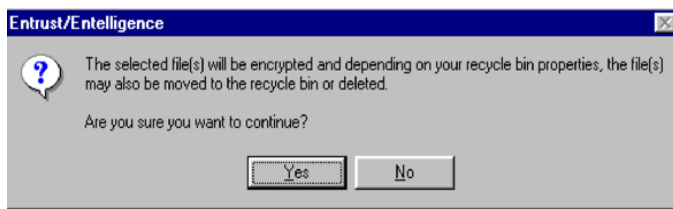
Secure Delete

When you delete a file using the **Secure Delete** feature, Entrust encrypts the file, sends it to the **Recycle Bin**, and then over-writes the disk space occupied by the original file. You can still recover the file by moving it out of the **Recycle Bin** and decrypting it.

1. Start **Windows Explorer** and navigate to where the file(s) are located.
2. Right mouse click the file(s).
3. From the pop-up menu, select **Entrust Advanced | Secure Delete**.



The **Entrust/Entelligence** dialog box appears.



4. Click on **Yes** to securely delete the file.
The file(s) you selected are encrypted and moved to the Recycle Bin.
5. Empty the **Recycle Bin**.

ENTRUST/ICE AND SECURED FOLDERS

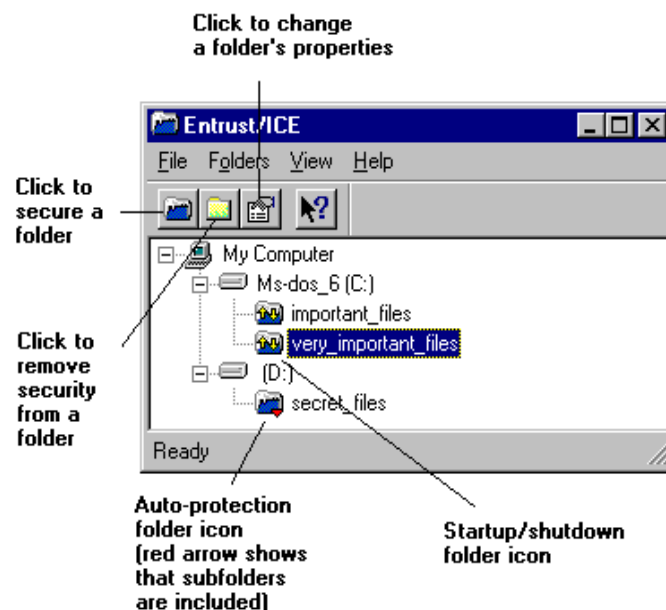
Entrust/ICE Overview

Entrust/ICE is desktop encryption software that automatically encrypts files that you save in your secure folders. This product allows the following functionality:

- Set up folders so that any files placed in them are automatically protected.
- Drag and drop or "Send To" secure folders to encrypt files.
- Securely share encrypted files with a designated group.
- Protect your laptop: files are secured if the laptop is lost or stolen.
- Automatically encrypt files on shutdown and decrypt on start-up.

Entrust/ICE Main Window

The **Entrust/ICE** main window is the control centre for Entrust/ICE. In the main display area you see a list of the folders that are currently secured with Entrust/ICE. Each folder type is represented by a distinct folder icon. The main window also contains tool icons for performing security operations.



Entrust ICE Start-up

Entrust/ICE may run automatically when you start your computer. You can also launch it at any time from the Windows Start menu. If you are not already logged in to Entrust, **Entrust/ICE** will ask you to select your Entrust profile and enter your password on start-up. **Entrust/ICE** uses the profile you created with **Entrust/Entelligence** or another Entrust client.

Once you have logged in, you will see a new icon in your Windows tray (near the clock). This is the only indication that Entrust/ICE is running. Your new tray will look something like this:




The icon in the tray becomes animated whenever Entrust/ICE is encrypting or decrypting files. Double-click this icon if you want to see the main Entrust/ICE window.

Auto-Protection Folder Setup

You can set up an auto-protection folder from the right-click menu or the Entrust/ICE main window.

To set up an auto-protection folder using the right-click menu:

1. In **Windows Explorer**, right-click the folder you wish to secure and click **Entrust/ICE**. The **Secure Folder Properties** dialog box appears.
2. Select **Secure for my eyes only** if you wish to be the only one who can decrypt the files saved in this folder. Otherwise, select **Secure for a recipient list**.
3. If you selected **Secure for a recipient list**, click on  (the drop-down button) and choose from the recipient list that appears. If you have not defined any recipient lists, this option will be unavailable. You define recipient lists through the **Entrust Address Book**.
4. Click the **Settings** tab and select **Secure all sub-folders** if you want all the folder's subfolders to have the same security properties.
5. Click **OK**. You have now created an auto-protection folder. **Entrust/ICE** will encrypt all files currently in this folder and any files you save in this folder from now on.

If you selected the **Secure all sub-folders** option, the folder will appear with a red down arrow in the Entrust/ICE main window:



If you did not select the **Secure all sub folders** option, the folder will appear without a red down arrow:



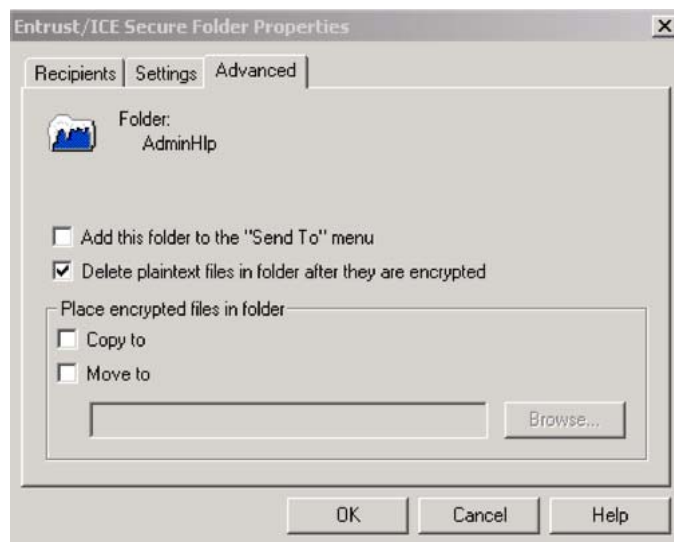
Copy or Move Files Automatically

You can set up **Entrust/ICE** to automatically copy or move the files saved in a secure folder to another folder. You set this option in the Secure Folder Properties dialog box.

Note: *You may place protected files in a local folder or in a folder on a mapped network drive. You can map a drive by choosing Map Network Drive from the Tools menu in Windows Explorer, and then selecting the drive in the dialog box that appears.*

To automatically copy or move files to another folder:

1. In **Windows Explorer**, right-click the folder whose contents you want automatically copied to another folder and click **Entrust/ICE**. The **Secure Folder Properties** dialog box appears.



2. Click the **Advanced** tab.
3. In the **Place encrypted files** in folder section, select **Copy to** or **Move to**.
4. Enter the name of the destination folder in the text box beside the **Browse** button. If you cannot remember the location or name of the folder, click **Browse**, select the folder in the dialog box that appears and click **OK**.
5. Click **OK** in the **Secure Folder Settings** dialog box.

From now on, the files you save in this **Entrust/ICE** folder will be automatically copied or moved (depending on your selection) to the destination folder you selected.

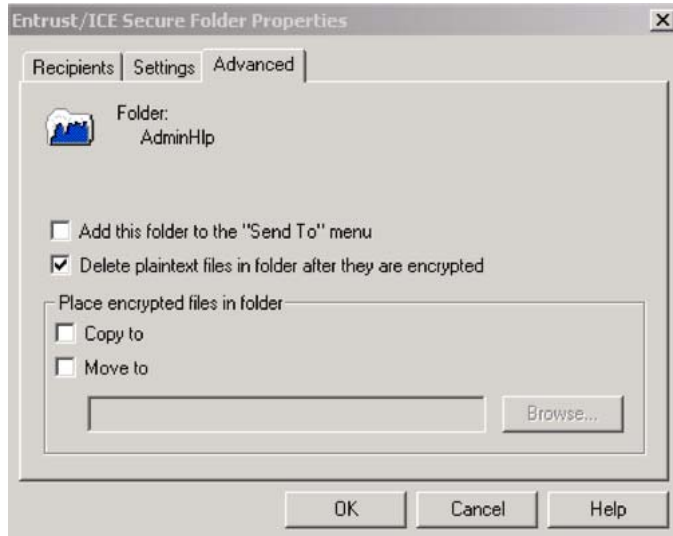
Note: *If the options in this dialog box are dimmed, your Administrator has locked this folder's properties. See Administrator options or your Entrust Administrator for more information.*

Add Folder to Send To Menu

To add a folder to the **Send To** menu

1. Ensure that **Entrust/ICE** is running.
2. In **Windows Explorer**, right-click the folder whose properties you wish to change and click **Entrust/ICE**.

The **Secure Folder Properties** dialog box appears.



3. Click the **Advanced** tab.
4. Select Add this folder to the "Send To" menu.
5. Click **OK**.

Remove Folder from Send To Menu

To remove a folder from the **Send To** menu:

1. Ensure that Entrust/ICE is running.
2. In **Windows Explorer**, right-click the folder whose properties you wish to change and click **Entrust/ICE**. The **Secure Folder Properties** dialog box appears.
3. Click the **Advanced** tab in the **Secure Folder Properties** dialog box.
4. Clear the Add this folder to the "Send To" menu checkbox.
5. Click **OK**.

Note: *If the options in this dialog box are dimmed, your Administrator has locked this folder's properties. See Administrator options or your Entrust Administrator for more information.*

Delete Plaintext After Encrypting


To change the Delete plaintext files setting:

1. Ensure that Entrust/ICE is running.
2. In **Windows Explorer**, right-click the folder whose properties you wish to change and click **Entrust/ICE**. The **Secure Folder Properties** dialog box appears.
3. Click the **Advanced** tab.
4. If you want Entrust/ICE to delete plaintext files from this folder after encrypting them, select **Delete plaintext files in folder after they are encrypted**. Otherwise, clear the option.
5. Click **OK**.

Note: *If the options in this dialog box are dimmed, your Administrator has locked this folder's properties. See Administrator options or your Entrust Administrator for more information.*

Encrypt File for Recipient List

To set up an auto-protection folder for a recipient list:

1. Ensure that **Entrust/ICE** is running.
2. In **Windows Explorer**, right-click the folder you wish to secure and click **Entrust/ICE**. The **Secure Folder Properties** dialog box appears.
3. Select **Secure for a recipient list**, click , and choose the recipient list from the list that appears.
4. Click **OK**.
5. From now on, **Entrust/ICE** will encrypt files saved in this folder for the recipient list you just selected.

Tip: The option to encrypt files for a recipient list will be unavailable if you have not defined any recipient lists. You define recipient lists through the Entrust Address Book. See Using the Entrust Address Book, Working With Recipient Lists in the Entrust/Entelligence online help for details.

Note: *If all the options in this dialog box are dimmed, your Administrator has locked this folder's properties. See Administrator options or your Entrust Administrator for more information*

QUICK REFERENCE

Quick Reference Table

Question	Answer
<p>Why do I need to use Entrust?</p>	<p>Treasury Board has mandated the RCMP to use Entrust software to securely send and receive electronic documents.</p> <p>Entrust has many features which include strong authentication onto the network by requiring a black token and a password.</p> <p>For additional details, see the Purpose Of Entrust help topic.</p>
<p>How do I Know I need Entrust?</p>	<p>If you need to send or receive protected documents or email messages that are up to and including Protected "B" level.</p> <p>This includes applications such as CPIC Web, PROS IQT, Livescan.</p> <p>For additional details see the Purpose Of Entrust help topic</p>
<p>How do I apply for access to Entrust ?</p>	<p>RCMP employees will need to complete a PKI application. For additional details, see the PKI Certificate Request topic.</p> <p>If you are a Non-RCMP employee, see your Policy Centre or LRA representative.</p>
<p>How do I obtain a black token?</p>	<p>RCMP employee's who do not already have a black token will need to contact the Central Helpdesk for a new token.</p> <p>Non-RCMP employees who need a token to access a RCMP application need to contact the application's Entrust policy centre.</p> <p>For additional details, see the Token Overview help topic</p>
<p>How do I activate my black token for the first time?</p>	<p>You can only begin this process once you have received your Authorization Code from your supervisor or (LRA) and Reference Number from the PKI Administrator.</p> <p>In order to activate your token you will need to initialize it. For additional details, see the Hardware Token Initialization help topic.</p> <p>After initializing your token, you will proceed to create your Entrust Profile on it. See the Entrust Profile Creation help topic.</p>
<p>What happens if I forget my password?</p>	<p>You will need to email or contact the Central Helpdesk (1-800-461-7797) to obtain a new Reference Number and Authorization Code.</p> <p>The process of recovery your Entrust profile is described</p>

	in the Entrust Profile Recovery With Token help topic
What happens if I lost my black token?	Report the lost token immediately to the Central Help Desk. You will need to be issued a new token and re-initialize your token.
How many times can I try to access my token before being denied access?	If you have forgotten or mistyped your password, you have 10 attempts to correctly type in your password. After the 10th try your token will become unusable and you will require a new token.
Is there an expiry date on the token?	Yes, the token has an expiry date for security reasons. You should log in with your black token onto the network at least once every three months. You do not have to worry about updating your token, as Entrust will automatically perform this task. For additional details, see the Token Expiry help topic.
How do I change my password?	See paragraph 19. Changing your Password in the Entrust Profile Creation help topic.
How do I log onto Entrust?	See the Entrust Login help topic.
How do I find more information about Entrust?	The Search capabilities and functionality of the Table of Contents, Index and Glossary in the Entrust Help will help you find the needed information. The Central Helpdesk (1-800-461-7797) is also available for questions.

Glossary of Terms

CPIC

Canadian Poilice Information Centre

NAL

Network Application Launcher

NCDB

National Criminal Data Bank

NSS

Network Services Section

PDA

Personal Digital Assistant

PROS

Police Reporting and Occurrence System

ROSS

RCMP Office Support System

PKI

Public Key Infrastructure

LRA

Local Registration Authority

Index

A

ACTIVATION OVERVIEW 5
Activation Steps 5
ACTIVATION TECHNICAL SETUP 6
ACTIVATION USER PROCEDURES 13
Add Folder to Send To Menu 42
Application Objects Required 8
Auto-Protection Folder Setup 40

C

Copy or Move Files Automatically 41

D

Decrypt and Verify Secured Files 35
Decrypt, Verify and Open Secured File 37
Delete Plaintext After Encrypting 42

E

Encrypt File for Recipient List 43
Encrypting & Signing 33
Encrypting Files For Recipients 34
Encrypting Files For Yourself 33
ENTRUST FILE PROCESSING 33
Entrust Future Direction 3
Entrust ICE Start-up 40
Entrust Installation Using a CD 7
Entrust Installation Using A Script Overview 6
Entrust Installation Using NAL 8
Entrust Login 23
ENTRUST LOGIN/LOGOUT 23
Entrust Logout 24
Entrust Options Settings 26
ENTRUST OVERVIEW 1
Entrust Profile 14
Entrust Profile Creation 14
Entrust Profile Recovery With Token 19
Entrust Single Login icons 24

ENTRUST/ICE AND SECURED FOLDERS 39
Entrust/ICE Main Window 39
Entrust/ICE Overview 39
Export/Import Key 27

H

Hardware Token Initialization 13

K

Key Export 27
Key Import to Address Book 28

N

NAL Setup for Entrust / Datakey / Contivity Package 9

O

Offline / Online Switch 31
Offline Login 30
Offline Work Overview 30
OFFLINE WORK PROCEDURES 30
Online Help Information 1

P

Password Change 27
PKI Certificate Request 3
Primary Functions 2
Purpose Of Entrust 1

Q

QUICK REFERENCE 44
Quick Reference Table 44

R

RCMP Entrust Policy Centre 1
Remove Folder from Send To Menu 42

S

Secure Delete 37
Software Installation Details 6
Software Installation Requirement 6
System Support 4

T

Time-Out 26
Token Expiry 22
Token Overview 3
Token Software 3

