ENTRUST

SECURING A WORLD IN MOTION

Entrust Authority Security Manager 8.1 SP1

nShield® HSM Integration Guide for Linux

Version: 1.3

Date: Thursday, November 26, 2020

nCipher Security Limited
Registered Office: One Station Square,
Cambridge, CB1 2GA, United Kingdom
Registered in England No. 11673268

Contents

1 Introduction

1.1 This product

Entrust Authority Security Manager is a Public-Key Infrastructure (PKI) that manages digital certificates and can publish Certificate Revocation Lists (CRLs). The nCipher Hardware Security Modules (HSMs) are used to securely store and manage:

- The key pair for the Certificate Authority (CA).
- The key pair for the CRLs.

Throughout this guide, the term HSM refers to nShield Solo, nShield Connect, and nShield Edge products.

1.1.1 Product configuration

The integration between the HSM and Entrust Authority Security Manager has been successfully tested in the following configurations:

Operating system	Entrust version	Security World Software	nShield Solo support	nShield Connect support	nShield Edge support
Red Hat Enterprise Linux Server release 6.0 x64	8.1 SP1	11.70	—	Yes	—
Red Hat Enterprise Linux Server release 5.8 x64	8.1 SP1	11.70	—	Yes	—

To integrate Entrust Authority Security Manager 8.1 SP1 with nCipher HSM, you must install a 32-bit version of the Security World Software, irrespective of the Operating System architecture i.e. for both 32-bit and 64-bit OS, install a 32-bit version of Security World Software.

1.1.2 Supported nCipher functionality

Key Generation	Yes
Key Management	Yes
Key Import	—
Key Recovery	Yes
1-of-N Operator Card Set	Yes
K-of-N Operator Card Set	Yes
Softcards	Yes

Module-only Key	-
Strict FIPS Support	Yes
Load Balancing	Yes
Fail Over	Yes

Fail Over and Load Balancing are not supported with the nShield Edge.

1.1.3 Requirements

To integrate the HSM and Entrust Authority Security Manager, you need the server and client machines to be set up as follows:

	Hardware	Software
Server	Red Hat Enterprise Linux Server release x 64	nShield Security World Software 11.70 Critical Path Directory Server 5.0 PostgreSQL Server 8.3.11 Entrust Authority Security Manager 8.1 SP1
Client	Windows XP Professional Version 2002 Service Pack 3	Security Manager Administration Console 8.1 Entrust Entelligence 7.0

Before attempting to install the software, we recommend that you familiarize yourself with the Entrust Authority Security Manager documentation and setup process and that you have the *User Guide* for your HSM available.

You also need to consider the following aspects of HSM administration:

- The number and quorum of Administrator Cards in the Administrator Card Set (ACS), and the policy for managing these cards.
- The number and quorum of Operator Cards in the OCS, and the policy for managing these cards.
- Whether the Security World should be compliant with FIPS 140-2 level 3.
- Key attributes such as the key size, persistence, and time-out.
- Whether there is any need for auditing key usage.

1.2 This guide

This document explains how to set up and configure an Entrust PKI installation with an HSM. The instructions in this document have been thoroughly tested and provide a straightforward integration process. There may be other untested ways to achieve interoperability.

This guide may not cover every step in the process of setting up all the software. For more information about installing Entrust, see the Entrust documentation.

1.3 More information

For more information about the HSM, see the *User Guide* for the HSM.

Additional documentation produced to support your nCipher product is in the document directory of the CD-ROM or DVD-ROM for that product.

2 Procedures

To integrate Entrust Authority Security Manager and HSM:

1. Install the HSM.
2. Install the nShield Security World Software, and configure the Security World.
3. Install and configure Critical Path Directory Server 5.0:
    a. Install Critical Path Directory Server 5.0.
    b. Configure the Directory System Agent (DSA) for use with your Entrust setup.
    c. Manage the DSA using the Directory Server iCon administrator interface.
4. Create Master Users for controlling the Security Manager software through the Security Manager Control Command Shell.
5. Install PostgreSQL Server 8.3.11.
6. Install and configure Entrust Authority Security Manager 8.1 Service Pack 1 (SP1):
    a. Install Entrust Authority Security Manager.
    b. Configure and initialize the Entrust CA.
    c. Initialize the CA with 1-of-N OCS
    or Initialize the CA with K-of-N OCS.
    d. Install Entrust Authority Security Manager 8.1 Service Pack 1 (SP1).
    e. Move a CA key pair between software and HSM protection.
7. Install and configure Entrust Entelligence 7.0.

All these procedures are described in the following sections.

2.1 Installing the HSM

Install the HSM using the instructions in the *Hardware Installation Guide* for the HSM. We recommend that you install the HSM before configuring the nShield Security World software with your Entrust setup.

2.2 Installing the nShield Security World Software and creating the Security World

Install the Security World Software and create the Security World as described in the *Quick Start Guide* for the HSM. This document assumes that:

- You are installing an offline root Certificate System.
- A new root key is generated during installation.

After creating the Security World, configure the **cknfastrc** environment variables:

1. Open the file named cknfastrc in the directory where the Security World Software is installed. The default directory is /opt/nfast/.
2. Add the following environment variables to the file:

```
CKNFAST_NO_UNWRAP=1
CKNFAST_NO_ACCELERATOR_SLOTS=1
CKNFAST_LOADSHARING=1
CKNFAST_OVERRIDE_SECURITY_ASSURANCES=none
```

For Enhanced Database Protection (EDP) use CKNFAST_LOADSHARING=0 after enabling the database hardware protection. Restart the system for load sharing to work.

For more information about the environment variables used in cknfastrc, see the *nShield PKCS #11 library environment variables* section in the *User Guide* for the HSM.

When using a K-of-N cardset where K>1, set CKNFAST_LOADSHARING=0.

2.3 Installing and configuring Critical Path Directory Server 5.0

This section describes how to:

- Install Critical Path Directory Server 5.0.
- Configure the DSA for use with your Entrust setup.
- Manage the DSA using the Directory Server iCon administrator interface.

2.3.1 Installing Critical Path Directory Server 5.0

Critical Path Directory Server is based on X.500 recommendations and LDAPv3 standards; your Entrust setup uses it to store the user profiles that the Entrust Administrator creates.

To install Critical Path Directory Server 5.0:

1. Obtain the Critical Path Directory Server software and run the rpm file:

```
rpm -ivh CPDS-5.0-0.i386.rpm
```

3. Accept all defaults and ensure that the machine's correct name is displayed.

2.3.2 Configuring the DSA for use with your Entrust setup

To configure the DSA for use with your Entrust setup:

1. In the command line run commands of the following form (which shows the example DSA created with Critical Path Directory Server):

```
[root@ptd9500-VM1 opt]# cd cpds
[root@ptd9500-VM1 cpds]# mkdir DSA
[root@ptd9500-VM1 cpds]# cd DSA/
[root@ptd9500-VM1 DSA]# source ~/.bash_profile
CPDS-5.0-0
[root@ptd9500-VM1 DSA]# odsecreate
```

   These example commands create a DSA in the current working directory.

4. You are prompted to provide the information required to get the DSA up and running so that you can get a Directory User Agent (DUA) to bind to it. If you do not know the form in which to enter the information, press Return without entering any information.

   

   A DUA is a process that accesses the directory service on behalf of the users and administrators. The DUA communicates with the DSA using the Directory Access Protocol (DAP) or Lightweight Directory Access Protocol (LDAP).

5. Follow the process described in the following table to configure the DSA for use with the Entrust CA:

Text on screen:	You enter:
Please enter the name of the DSA	**cn=EntrustDSA**
Please enter the name of the DSA administrator	**cn=diradmin**
Please enter the administrator's password	*<Administrator's password>*
The DSA can support RFC1006 comms, or IDM, or both Will the DSA support RFC1006 comms (Y/N)?	**Y**
Please enter the t-selector for RFC1006 DAP/DSP	**1001**
Please enter the t-selector for RFC1006 shadowing.Press return for no shadowing, this can be added later	Press [RETURN]
Shadowing protocol will not be added Will the DSA support IDM comms (Y/N)?	**N**

Text on screen:	You enter:
Please enter the port number for LDAP. Press return for no LDAP, this can be added later	**389**
Please enter the license key	*<license key>*
Do you wish to include the extensibleObject defined in RFC 2252 (Y/N)?	**Y**
Do you wish to include the Java(tm) Objects schema defined in RFC 2713 (Y/N)?	**Y**
Do you wish to include the CORBA Objects schema defined in RFC 2714 (Y/N)?	**Y**
Do you wish to include the LDAP as a NIS Schema defined in RFC 2307 (Y/N)?	**Y**
Do you wish to include the UPS Common schema defined by Critical Path (Y/N)?	**Y**
Initializing the DSA	
Reading country codes from file iso3166 admin>Reading country codes from file iso3166 admin>Log file was odscreate.000	
Please enter 'Y' to configure an empty Entrust DSA or 'N' to add the CA, Search Base (CP) and Entrust Directory Manager entries	**N**
Please enter the name of the search base in the DSA It must be either a country, organization, organizational unit, domain or locality	**o=Entrust,c=gb**
Please enter the name of the CA in the DSA. It must be a country, organization, organizational unit, domain, locality, organizational role, application processor device. Press return for top entry to be the CA	Press [RETURN]
Please enter the CA's password	*<CA's password>*
Please enter the name of the Entrust Directory Manager	**cn=manager**
Please enter the Entrust Directory Manager's password	*<Directory Manager's password>*
Initializing the Entrust DSA Changing update log	
Reading country codes from file iso3166 admin>admin>Log file was odsecreate.000 Do you wish to start the DSA (Y/N)?	Y
Starting the DSA	

Text on screen:	You enter:
Creating the file 'ds.properties' Writing ldap/attributes.cfg Writing ldap/objectclasses.cfg Writing ldap/syntaxes.cfg Writing ldap/matchingrules.cfg Writing ldap/oidtable.at Writing ldap/oidtable.oc Writing oidslocal odssched 9769 started	
Please Note >>> ==========	
The file **entrustdirectorysetup.ini** has been created, if Entrust software is being run on a Windows platform copy this file to the Windows folder on the machine where the Entrust/Authority Configuration Utility is to be run. E.g. copy to **c:\winnt** folder. Otherwise no further action is required. Please check the contents of this file to ensure all fields have been completed forinput into the Entrust / Authority Configuration Utility.	

2.3.3 Managing the DSA using the Directory Server iCon administrator interface

To enable the DSA to be configured with the Directory Server iCon administrator interface:

1. Open iCon.
2. Log in to the CPDS (Critical Path Directory Server) icon services using the Entrust Directory Manager (**cn=manager**) and password used to configure the DSA, see "Installing and configuring Critical Path Directory Server 5.0" on page 9.
3. From the main menu, select Add DSA and enter the information you provided when installing the critical path directory server, see "Installing and configuring Critical Path Directory Server 5.0" on page 9:

location of DSA	**/opt/cpds/DSA/**
friendly name of DSA	EntrustDSA
managers DN	**cn=diradmin**
managers password	*<Administrator's password>*

4. Click AddDSA to iCon. A message appears, stating that the DSA is successfully added.
5. Select the highlighted EntrustDSA link.
6. Navigate to the Options menu for this DSA and check that auto-start DSAs is set to on, and then click Change iCon Options.
7. To check that the DSA starts, click Start DSA on the previous window or on the main menu.

2.4 Create Master Users for controlling the Security Manager software through the Security Manager Control Command Shell

Master Users are responsible for controlling the Security Manager software through the Security Manager Control Command Shell.

There are three predefined Master User roles: Master1, Master2 and Master3. These user names are case-sensitive and cannot be changed. The people chosen for these roles must be present when you initialize Security Manager to choose and enter their own unique and private passwords. Also, they must have physical access to the server that hosts Security Manager, so that they can maintain the Security Manager infrastructure. These roles appear in the Security Manager software.

Master Users use Security Manager Control Command Shell to:

- Start and stop the Security Manager service.
- Back up and restore the Security Manager data files.
- Maintain the Certification Authority (CA), including updating the CA keys.

The Primary Group for user acoount Master1, Master2, Master3 is **entrust**. The Secondary Group for user acoount Master1, Master2, Master3 is **easm_entrust_pg**.

To add Masters in Security Manager Server:

1. Go to System->Administration->Users and Groups. The User Management console opens.
2. Create groups **entrust** and **easm_entrust_pg**.
3. Create users **Master1**, **Master2** and **Master3**. Make **entrust** the primary group and **easm_entrust_pg** the secondary group of these users.
4. Add these users to the **nfast** group.

2.5 Installing PostgreSQL Server 8.3.11

To install PostgreSQL Server on the server machine:

1. Download PostgreSQL Server installer from the Entrust TrustedCare online support site for the Linux operating system (**SM_81_PostgreSQL_8311_RH_installer.tar**).
2. To start installing the PostgreSQL database for Entrust Security Manager 8.1 SP1, untar the setup file **SM_81_PostgreSQL_8311_RH_installer.tar** in **/opt/**.

3. Change directory (cd) to SM_81_PostgreSQL_8311_RH_installer.
4. Run the script install_postgres.sh.
5. Accept the license agreement for the installation.
6. Accept the default destination folder(/opt/entrust) for installing the Entrust PostgreSQL Database program files, and then press Enter.
7. Accept all default destination folders for installing other Database files, and then press Enter.
8. Enter the password for the easm_entrust_pg account, and then press Enter.
9. Confirm the password for the easm_entrust_pg account, and then press Enter.
10. Enter a password for the internal database user account (easm_entrust) and press Enter.
11. Confirm the password for the internal database user account (easm_entrust) and press Enter.
12. Enter a password for the internal database user account (easm_entbackup) and press Enter.
13. Confirm the password for the internal database user account (easm_entbackup) and press Enter.
14. Accept the default Database listen port 5432 in the Entrust Authority (TM) Security Manager PostgreSQL, and press Enter.
15. The following message will be displayed if installation is successful: "Installation and configuration of Entrust Authority (TM) Security Manager PostgreSQL Database completed".

2.6 Installing and configuring Entrust Authority Security Manager 8.1 SP1

2.6.1 Installing Entrust Authority Security Manager

To install Entrust Authority Security Manager on the server computer:

1. Download Entrust Authority Security Manager 8.1 Service Pack 1 (SP1) from the Entrust TrustedCare online support site for the Linux operating system (SM_81SP1_WithPatch173358_RH_installer.tar).
2. Untar the setup file SM_81SP1_WithPatch173358_RH_installer.tar in /opt/.
3. Change directory (cd) to SM_81SP1_WithPatch173358_RH_installer and run script install.sh.
4. Accept the license agreement for the installation.
5. Accept the default destination folder (/opt/entrust) for installing the Entrust Authority Security Manager program, and then press Enter.
6. Accept the default destination folder (/opt/entrust/authdata) for installing Security Manager CA data (authdata).
7. Enter Master1 as the name of the Linux user that will own the installation.

8. Press Enter. When the installer prompts you to add 'Master1' to the **'easm_entrust_pg'** group, press y.
9. Press Enter. When the installer prompts you to configure a CA now, press y.
10. Press Enter twice to proceed with the configuration of Entrust CA.

2.6.2 Configuring Entrust CA

To configure Entrust CA:

1. After the installation, press Enter to accept the default full path of the CA data directory.
2. When prompted, enter the Enterprise licensing information that appears on your Entrust licensing card:
   - Serial Number.
   - Enterprise user limit
   - Enterprise licensing code.
3. When prompted, enter the Web licensing information that appears on your Entrust licensing card:
   - Serial Number.
   - Enterprise user limit
   - Enterprise licensing code.
4. Press Enter for Domestic DV Serial Number, Foreign DV Serial Number and IS Serial Number.
5. Enter **1 (LDAP directory)** for the type of Directory service.
6. Enter the hostname or IP address of the machine that is hosting the Directory service and directory listen port (**389**).
7. When prompted for the CA DN and password, enter the information you provided when configuring the DSA for use with the Entrust set up (see "Configuring the DSA for use with your Entrust setup" on page 10) and bind the information:

CA DN	**o=Entrust,c=gb**
CA Directory access password	*<CA's password>*

9. Verify the information for the First Officer, and then press Enter:

CA DN	**cn=First Officer, o=Entrust, c=gb**

10. Enter the information for the Directory Administrator and bind the information:

CA DN	**cn=diradmin**
Directory access password	*<Administrator's password>*

11. Press Enter to accept default values when prompted for the following:
    - Entrust Proto-PKIX (PKIX) port [709] :
    - Entrust Administration Protocol (ASH) port [710] :
    - Certificate Management Protocol (PKIX-CMP) port [829] :
    - Entrust XML Administration Protocol (XAP) port [443] :
    - Enable XAP service? (y/n) ? [y]
12. When the installer prompts "Are you using a hardware device for the CA keys (y/n) ? [n]", type y.
13. When prompted, enter the pathname for the CryptokiLibrary as /opt/nfast/toolkits/pkcs11/libcknfast.so.
14. Select the appropriate slot for the desired type of protection.

    Example: nCipher Corp. Ltd SN : 331688d2fb5166be SLOT : 761406613
16. In the Cryptographic Information section, select settings as appropriate, for example:

CA Key Type for signing operations	RSA
RSA type and corresponding key length	RSA-2048
Algorithm for signing operations	RSA-SHA256
Type of key pair that will be used for user signing and nonrepudiation keys	RSA
RSA type and corresponding key length	RSA-2048
Type of key pair that will be used for user encryption and dual usage key pairs	RSA
RSA type and corresponding key length	RSA-2048

17. When the installer prompts 'Do you wish to work with Microsoft (R) Windows (R) applications? (y/n) ? [n]', accept the default by pressing Enter .
18. Enter the password that was assigned to easm_entrust when you installed the PostgreSQL Server8.3.11 (see "Installing PostgreSQL Server 8.3.11" on page 13), and then press Enter.
19. Enter the password that was assigned to the backup user when you installed the PostgreSQL Server8.3.11 (see "Installing PostgreSQL Server 8.3.11" on page 13), and then press Enter.
20. Accept the defaults for the algorithm that will be used for database encryption.
21. When prompted, select RootCA to create a Root Certificate Authority.
22. When the installer prompts for the following, accept the defaults by pressing Enter:

```
CA certificate lifetime 120
CA private key usage period 100
policy certificate lifetime in days 30
```

24. Verify the information and type 'yes' to finish configuration.

    For any error during the configuration process, type the section number to review the details.

25. Select 2 to exit the installation and configuration and initialize the CA later.

2.6.3 Initializing the CA with 1-of-N OCS

To initialize the Entrust Authority Security Manager with a 1-of-N OCS:

1. Open a command prompt and login as **Master1**.
2. Source the file **/opt/entrust/authdata/CA/env_settings.sh** (or **env_settings.csh**)
3. Run the command:

```
entsh -e "source /opt/entrust/authority8.1sp1/etc/FirstTimeInit.tcl"
```

5. When prompted for the passwords for Master1, Master2, Master3 and First Officer, provide the specified passwords.

    When setting passwords for Master users and the First Officer note the following constraints: the password must be at least 10 characters in length and not based on a dictionary word. Further, the characters must be both a mix of upper and lower case and include numbers.

6. When prompted for the password of the CA hardware, give the passphrase of the 1-of-N Operator Card Set.
7. When the initialization process is complete, the Entrust Master Control Command Shell informs you that the Entrust infrastructure has been set up. Press Return to exit.

2.6.4 Initializing the CA with K-of-N OCS

To initialize the Entrust Authority Security Manager with a K-of-N OCS:

1. Create an empty file within folder **/opt/nfast/**, for example: **/opt/nfast/kofn**.
2. Edit the file **cknfastrc** located in **/opt/nfast** and add the following environment variable:

```
NFAST_NFKM_TOKENSFILE=location of the empty file (kofn) in /opt/nfast/ folder
```

4. Open the command prompt in one session and preload the cardset by running the following command:

```
/opt/nfast/bin/preload -c cardsetname -f <file location mentioned in nfast variable NFAST_NFKM_TOKENSFILE> pause
```

6. Type the passwords for the OCS.
7. Open another command prompt and source the file /opt/entrust/authdata/CA/env_settings.sh (or env_settings.csh).
8. Run the command:

```
entsh -e "source /opt/entrust/authority8.1sp1/etc/FirstTimeInit.tcl"
```

10. When prompted for the passwords for Master1, Master2, Master3 and First Officer, provide the specified passwords.

When setting passwords for Master users and the First Officer note the following constraints: the password must be at least 10 characters in length and not based on a dictionary word. Further, the characters must be both a mix of upper and lower case and include numbers.

11. When prompted for the password of the CA hardware, give the passphrase of the K-of-N Operator Card Set.
12. When the initialization process is complete, the Entrust Master Control Command Shell informs you that the Entrust infrastructure has been set up. Press Return to exit.

2.6.5 Moving a CA key pair between software and HSM protection

The procedures described in this section are:

- Importing the CA key pair to the HSM (from software to hardware).
- Exporting the CA key pair from the HSM (from hardware to software).

Before performing either procedure, log in as Master 1 to check that the Entrust Master Control shell is running.

2.6.5.1 Importing the key from software to hardware

To import the CA key pair from software to the HSM:

1. Open the Entrust Authority Master Control shell.
2. Begin updating the keys by running the command:

```
entsh$ ca key update
```

This prompts you to select the destination for the new CA key.

5. Select the nCipher nCipher slot as the destination for the new CA key. For example:

```
1. software
2. nCipher Corp. Ltd SN: ec7759a6ecc0b7f0 SLOT: 7614066133.
3. Cancel operation
>2
```

7. To continue to update the CA key, type y .

After you have moved the CA key to the HSM and have finished updating it, a message about the CA profile being successfully recovered appears. The Entrust Authority Security Manager configuration and integration with the HSM is now complete.

2.6.5.2 Exporting the key from hardware to software

To export the Entrust CA key pair from the HSM to software:

1. Open the Entrust Authority Master Control shell.
2. Begin updating the keys by running the command:

```
entsh$ ca key update
```

This prompts you to select the destination for the new CA key.

5. Select the software slot as the destination for the new CA key. For example:

```
1. software
2. nCipher Corp. Ltd SN: ec7759a6ecc0b7f0 SLOT: 761406613
3. Cancel operation
>1
```

7. To continue to update the CA key, type y.

After you have finished updating the CA key, its export to software is complete.

2.7 Installing and configuring Entrust Entelligence 7.0

Entrust Desktop Solutions is a collection of desktop products that add trust to a wide range of e-business transactions.

Entrust Desktop Designer (part of Entrust Desktop Solutions) is a setup and deployment tool that allows you to create custom installation packages of the Entrust Desktop Solutions software to distribute to your end users. Entrust Desktop Designer enables you to select the application and components that are on users' desktops and customize the Entrust installation package itself. This offers the flexibility of centralized control over the desktop footprint, user interface, and branding.

Before you can use Entrust Desktop Solutions products, you must have an Entrust profile. If you do not have a profile, the installation program can be configured to prompt you to create a profile at the end of the installation process.

Before installing the Entrust Security Manager Administration and Entrust Entelligence, you must copy the following files from the server to the C:\Windows directory on the client computer:

- C:\authdata\manager\epf
- C:\Program Files (x86)\Entrust\Security Manager\Tools\config\ini\entrust.ini
- C:\Program Files (x86)\Entrust\Security Manager\Tools\config\ini\entrustra.ini

2.7.1 Installing Entrust Entelligence 7.0

1. Unzip the Entrust Entelligence software: desktop_solutions_70_win32.zip.
2. Double-click autorun.exe and accept all the default options.
3. Select Install Entrust/Desktop Designer.
4. To complete the installation, click Finish.

2.7.2 Configuring Entrust Entelligence 7.0

To create a customized installation of Entrust Entelligence 7.0 (which you run later):

1. Desktop Designer opens by default after it is installed. To open Desktop Designer manually, select Start > Programs > Entrust > Entrust DesktopDesigner > DesktopDesigner.
2. Select Entrust Desktop Solutions Setup, and then click Open.
3. On the right side pane in the Entrust Desktop Designer window, select include entrust.ini file.
4. Click the Browse button that becomes selectable, and navigate to the folder C:\Windows, where the entrust.ini file is copied to.
5. Select entrust.ini and click Open.
6. Deselect Ask user to create Entrust Profile.
7. Select File > Create Setup.

   Desktop Designer displays a Save Changes warning prompt.
9. To save changes to Untitled.esp7, select Yes.

10. Save the project with a suitable name, such as **test1.esp**.
11. To create a setup without EntrustSession Toolkit, select Yes.

    The Entrust Setup Creation Wizard appears.
13. Accept all the default options. Select Open custom setup folder, and then click Finish.

    The setup completes and the directory specified for Entrust Setup Location in the Setup Creation Wizard opens. By default, this directory is set to **C:\Documents and Settings\Administrator\My Documents\Entrust Setups\EntrustSetup\test1**.
15. Close Desktop Designer.
16. Run the setup program (for example **setup.exe**) and accept the defaults.
17. Click Finish.

Entrust Entelligence is installed on the Entrust Security Manager Server with custom configurations imported from **entrust.ini**.

2.7.3 Installing Entrust Security Manager Administration

Entrust Security Manager Administration provides a graphical user interface for administrators of Entrust Security Manager. It is used for creating Entrust profiles, defining roles, and applying security policies.

To install the Entrust Security Manager Administration to work with Entrust Authority Security Manager:

1. Run the setup file **SMA_81_Setup.exe**.
2. Click Next. To complete the installation, click Finish.
3. Restart the client (Windows Server 2003 R2 SP2) to ensure that the new **.ini** files and profiles are detected.
4. Select Start > Programs > Entrust Security Administrator.
5. Click Find Profile and, in the Browse window, navigate to **C:\Windows\epf**.
6. Select **First Officer.epf**, and then click Open. The Browse window closes.
7. To log into the application, type the password for **First Officer.epf**, and then click OK.

3 Troubleshooting

The following table lists error messages that might be displayed during the procedures described in this guide.

Problem	Cause	Resolution
(-8973) Could not connect to the Entrust Authority Security Manager service. Security Manager service may not be running.	The Entrust service is not running in the Entrust Authority Master Control shell (entsh$).	Open the Master Control shell (entsh$): 1. Login with Master1. 2. Run Service Start.
Entrust Login Interface is currently not running. Please start before launching this application. Entrust / Entelligence will now close.	Entrust Login Interface is not running.	1. Copy etlits.exe from the Entrust Desktop Solutions installation package to the Windows folder. The etlits.exe file can be found in \Designer\Entell. 2. In the Program path and file name field, type: c:\windows\etlits.exe -e

Contact Us

Web site:	https://www.entrust.com
Support:	https://nshieldsupport.entrust.com
Email Support:	nShield.support@entrust.com
Online documentation:	Available from the Support site listed above.

You can also contact our Support teams by telephone, using the following numbers:

Europe, Middle East, and Africa

United Kingdom:	+44 1223 622444 One Station Square Cambridge CB1 2GA UK

Americas

Toll Free:	+1 833 425 1990
Fort Lauderdale:	+1 954 953 5229 Sawgrass Commerce Center – A Suite 130, 13800 NW 14 Street Sunrise FL 33323 USA

Asia Pacific

Australia:	+61 8 9126 9070 World Trade Centre Northbank Wharf Siddeley St Melbourne VIC 3005 Australia
Japan:	+81 50 3196 4994
Hong Kong:	+852 3008 3188 31/F, Hysan Place 500 Hennessy Road Causeway Bay Hong Kong

To get help with
Entrust nShield HSMs

nShield.support@entrust.com

nshieldsupport.entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

ENTRUST

SECURING A WORLD IN MOTION