



**ENTRUST**

SECURING A WORLD IN MOTION

# Entrust Authority Security Manager 8.1 SP1

nShield® HSM Integration Guide for Windows Server  
2008 R2

---

**Version: 1.5**

**Date: Friday, November 27, 2020**

Copyright © 2019-2020 nCipher Security Limited. All rights reserved.

Copyright in this document is the property of nCipher Security Limited. It is not to be reproduced, modified, adapted, published, translated in any material form (including storage in any medium by electronic means whether or not transiently or incidentally) in whole or in part nor disclosed to any third party without the prior written permission of nCipher Security Limited neither shall it be used otherwise than for the purpose for which it is supplied.

Words and logos marked with ® or ™ are trademarks of nCipher Security Limited or its affiliates in the EU and other countries.

Mac and OS X are trademarks of Apple Inc., registered in the U.S. and other countries.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Information in this document is subject to change without notice.

nCipher Security Limited makes no warranty of any kind with regard to this information, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. nCipher Security Limited shall not be liable for errors contained herein or for incidental or consequential damages concerned with the furnishing, performance or use of this material.

Where translations have been made in this document English is the canonical language.

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

nCipher is an Entrust company.

Entrust, Datacard, and the Hexagon Logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.

---

# Contents

1	Introduction .....	5
1.1	This product .....	5
1.1.1	Product configuration .....	5
1.1.2	Supported nCipher functionality .....	5
1.1.3	Requirements .....	6
1.2	This guide .....	6
1.3	More information .....	7
2	Procedures .....	8
2.1	Installing the HSM .....	8
2.2	Installing the nShield Security World Software and creating the Security World .....	8
2.3	Installing and configuring Critical Path Directory Server 5.0 .....	9
2.3.1	Installing Critical Path Directory Server 5.0 .....	9
2.3.2	Configuring the DSA for use with your Entrust setup .....	9
2.3.3	Managing the DSA using the Directory Server iCon administrator interface .....	12
2.4	Installing PostgreSQL Server 8.3.11 .....	13
2.5	Installing and configuring Entrust Authority Security Manager 8.1 SP1 .....	14
2.5.1	Installing Entrust Authority Security Manager .....	14
2.5.2	Configuring the Entrust CA .....	14
2.5.3	Initializing the CA with 1-of-N OCS .....	17
2.5.4	Initializing the CA with K-of-N OCS .....	17
2.5.5	Installing Entrust Authority Security Manager 8.1 Service Pack 1 (SP1) .....	18
2.5.6	Moving a CA key pair between software and HSM protection .....	18
2.5.6.1	Importing the key from software to hardware .....	19
2.5.6.2	Exporting the key from hardware to software .....	19
2.6	Installing and configuring Entrust Entelligence 7.0 .....	20
2.6.1	Installing Entrust Entelligence 7.0 .....	20
2.6.2	Configuring Entrust Entelligence 7.0 .....	20
2.6.3	Installing Entrust Security Manager Administration .....	21
3	Troubleshooting .....	22

---

Contact Us .....	23
Europe, Middle East, and Africa .....	23
Americas .....	23
Asia Pacific .....	23

# 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
Windows Server 2008 R2 Enterprise SP1	8.1 SP1	11.60	Yes	Yes	Yes
Windows Server 2008 R2 Enterprise	8.1 SP1	11.50	Yes	Yes	Yes
Windows Server 2008 R2 Enterprise	8.1 SP1		Yes	Yes	—

### 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	Windows Server 2008 R2 Enterprise x64	nShield Security World Software 11.60 Critical Path Directory Server 5.0 PostgreSQL Server 8.3.11 Entrust Authority Security Manager 8.1
Client	Windows Server 2003 R2 x86 SP2	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. Install PostgreSQL Server 8.3.11.
5. 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.
6. 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 **C:\Program Files (x86)\nCipher\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 **setup.exe**.
2. Accept all defaults and ensure that the machine's correct name is displayed.
3. When installation is complete, restart the machine and log in as an Administrator.

### 2.3.2 Configuring the DSA for use with your Entrust setup

To configure the DSA for use with your Entrust setup:

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

```
C:\>md DSADATA\DSA3
C:\>cd DSADATA\DSA3
C:\DSADATA\DSA3>odsecreate.cmd
```

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

- 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).

- 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	<b>cn=EntrustDSA</b>
Please enter the name of the DSA administrator	<b>cn=diradmin</b>
Please enter the administrator's password	<i>&lt;Administrator's password&gt;</i>
The DSA can support RFC1006 comms, or IDM, or both Will the DSA support RFC1006 comms (Y/N)?	<b>Y</b>
Please enter the t-selector for RFC1006 DAP/DSP	<b>1001</b>
Please enter the t-selector for RFC1006 shadowing. Press return for no shadowing, this can be added later	Press <b>[RETURN]</b>
Shadowing protocol will not be added Will the DSA support IDM comms (Y/N)?	<b>N</b>
Please enter the port number for LDAP. Press return for no LDAP, this can be added later	<b>389</b>
Please enter the license key	<i>&lt;license key&gt;</i>
Do you wish to include the extensibleObject defined in RFC 2252 (Y/N)?	<b>Y</b>
Do you wish to include the Java(tm) Objects schema defined in RFC 2713 (Y/N)?	<b>Y</b>

Text on screen:	You enter:
Do you wish to include the CORBA Objects schema defined in RFC 2714 (Y/N)?	<b>Y</b>
Do you wish to include the LDAP as a NIS Schema defined in RFC 2307 (Y/N)?	<b>Y</b>
Do you wish to include the UPS Common schema defined by Critical Path (Y/N)?	<b>Y</b>
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	<b>N</b>
Please enter the name of the search base in the DSA  It must be either a country, organization, organizational unit, domain or locality	<b>o=Entrust,c=gb</b>
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	<b>cn=manager</b>
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	<b>Y</b>
Do you wish to start the DSA (Y/N)?	
Starting the DSA  Creating the file 'ds.properties'  Writing ldap/attributes.cfg  Writing ldap/objectclasses.cfg  Writing ldap/syntaxes.cfg  Writing ldap/matchingrules.cfg	

Text on screen:	You enter:
<p>Writing ldap/oidtable.at</p> <p>Writing ldap/oidtable.oc</p> <p>Writing oidslocal</p> <p>odssched 9769 started</p>	
<p>Please Note &gt;&gt;&gt; =====</p>	
<p>The file <b>entrustdirectorysetup.ini</b> has been created, it has been copied to the Windows folder for use by the Entrust/Authority Configuration Utility.</p> <p>If Entrust software is being run on a different Windows machine copy this file to the Windows folder on the machine where the Entrust/Authority Configuration Utility is to be run.</p> <p>(For example, Copy to C:\WINDOWS folder on that machine.)</p>	<p>Press [RETURN]</p>

### 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	<b>C:\DSADATA\DSA3</b>
friendly name of DSA	EntrustDSA
managers DN	<b>cn=diradmin</b>
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 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 Windows operating system ([SM\\_81\\_Win\\_PostgreSQL\\_8311\\_setup.exe](#)).
2. To start installing the PostgreSQL database for Entrust Security Manager 8.1 SP1, double-click the setup file [SM\\_81\\_Win\\_PostgreSQL\\_8311\\_setup.exe](#).
3. Accept the license agreement for the installation.
4. Accept the default destination folder ([C:\Program Files \(x86\)\Entrust](#)) for installing the Entrust PostgreSQL Database program files, and then click [Next](#).
5. In the [Select Drive for Database](#) window, accept the default location as drive [C:\](#), and then click [Next](#).
6. In the [Database Transaction Log Drive](#) window, select the drive that will host database logs, then click on [Next](#). The default path is [C:\](#).
7. In the [Possible Data Security Issue](#) dialog box which states:

For Security of your data, we recommend that Transaction log should be stored in separate partition. Would you like to change your selection?

Select [No](#).

10. In the [PostgreSQL Windows \(R\) Account Password](#) window, set the password for [easm\\_entrust\\_pg](#) account, and then click [Next](#).
11. In the [Password for Database User](#) window, provide the password for the account [easm\\_entrust](#) and click on [Next](#). See the Entrust password criteria for guidelines on setting the password. If the password is weak, the wizard gives a message asking to change the password.  
Press [Yes](#) to reset the password, otherwise press [No](#) to continue with the set password.
13. In the [Password for Database Backup user](#) window, set the password for [easm\\_entbackup](#) account. To continue, click [Next](#).
14. In the [PostgreSQLDatabasePort](#) window, accept the default port 5432. To continue, click [Next](#)
15. In the [Check Setup Information](#) window, verify the paths of Program files, Database, Transaction logs, and port details. To continue with the installation, click [Next](#).
16. To complete the installation, click [Finish](#) in the [InstallShield Wizard Complete](#) window.

## 2.5 Installing and configuring Entrust Authority Security Manager 8.1 SP1

### 2.5.1 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 Windows operating system ([SM\\_81\\_Win\\_setup.exe](#)).
2. Run the installation program and accept the default installation path (`C:\Program Files (x86)\Entrust`).
3. When the installation process is complete, select the option to run the Entrust Configuration Utility, and then click **Finish**.

### 2.5.2 Configuring the Entrust CA

To configure the Entrust CA:

1. After the installation, the **Entrust Authority Security Manager Configuration** setup screen appears. If it does not appear, select **Start > Entrust > Security Manager Configuration**.
2. In **Select the configuration type**, select **Custom configuration**, and then click **Next**.
3. When prompted, enter the Enterprise licensing information that appears on your Entrust licensing card:
  - Serial Number.
  - Enterprise user limit
  - Enterprise licensing code.
4. Accept the default installation paths for the data files (`c:\authdata`) and backup files (`c:\entbackup`).
5. Enter the directory node name (*Server name*) and directory listen port (**389**).
6. Select and use LDAP directory.
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 ["Installing and configuring Entrust Authority Security Manager 8.1 SP1"](#) above) and bind the information:

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

8. Enter the information for the **Directory Administrator** and bind the information:

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

9. Verify the information for the **First Officer**, and then click **Next**:

CA DN	<b>cn=First Officer, o=Entrust, c=gb</b>
-------	--

10. Click **Next** on **Verify Directory Information** Page.
11. Use the Entrust Directory Verification Tool (**EntDVT**) to verify the settings, and then click **Next**.
12. When prompted, provide your Windows login password, and then click **Next**.
13. Select **EASM\_Entrust\_PostgreSQL** for database connection.
14. Enter the password that was assigned to **easm\_entrust** when you installed the PostgreSQL Server 8.3.11, see "[Installing and configuring Entrust Authority Security Manager 8.1 SP1](#)" on the previous page, and then click **Next**.
15. Enter the password that was assigned to the backup user when you installed the PostgreSQL Server 8.3.11, see "[Installing and configuring Entrust Authority Security Manager 8.1 SP1](#)" on the previous page, and then click **Next**.
16. When asked whether to:

InterOperate with Microsoft (TM) CryptoAPI-enable applications?

Select **No** and click **Next**.

19. Configure the following settings as appropriate, and then click **Next**:

Security Manager node name	<Server machine>
Security Manager listen port	709
Administration subsystem listen port	710
PKIX-CMP subsystem server port	829
Entrust XML administration protocol port	443

20. In the Cryptographic Information dialog, select settings as appropriate, for example:

<b>Certificate Authority</b>	
CA key generation	Hardware

CA Key Type	RSA2048
<b>Database</b>	
Database Encryption Algorithm	TripleDES-CBC-192
<b>Entrust Users</b>	
User Signing Key Type	RSA2048
User Encryption Key Type	RSA2048
<b>CA Signing Algorithm</b>	
Signature algorithm	RSA-SHA1
<b>Policy Certificate</b>	
Policy certificate lifetime	30



This integration does not support EC-P and RSAPSS algorithms

21. Click **Next**.

The system returns the following message:

Security Manager Configuration could not detect any hardware devices. Please select a new cryptographic hardware library in the next dialog

24. Click **OK**.

25. Use the nShield PKCS11 library located at **C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast.dll**.

You can confirm this location by opening the **entmgr.ini** file located in the **Entrust** directory and looking for the entry: **CryptokiV2LibraryNT = C:\Program Files (x86)\nCipher\nfast\toolkits\pkcs11\cknfast.dll**.

27. Select the appropriate slot for the desired type of protection.
28. When prompted, select **RootCA** to create a Root Certificate Authority.
29. When prompted to initialize the CA certificate, approve the initialization, and then enter the following certificate properties:

CA cert lifetime	120 months
CA private key usage period	100%

30. When the Root Certificate Authority process is complete, deselect the **Run Entrust / Master Control now** option, and then click **OK**.



## 2.5.3 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 navigate to **C:\Program Files (x86)\Entrust\Security Manager\Bin** and run the command:

```
entsh.exe" -e "source \"C:/Program Files (x86)/Entrust/Security  
Manager/etc/FirstTimeInit.tcl\""
```



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.

3. When prompted for the password for the CA hardware, provide the operator card password.
4. When the initialization process is complete, the **Entrust Master Control Command Shell** informs you that the Entrust infrastructure has been set up.

## 2.5.4 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 folder in C:\ (for example, preload).
2. Open the command prompt preload the cardset by running the following command:

```
preload -c cardsetname -f preloadfile pause
```



*preloadfile* is the full path and file name of a file to be created in the preload folder. It can have any name.

4. Type the passwords for the OCS.

5. Edit the file `cknfastrc` located in `C:\Program Files (x86)\nCipher\nfast` and add the following environment variable using the full path and file name of the file specified in step 2:

```
NFAST_NFKM_TOKENSFILE=preloadfile
```

7. Open another command prompt and run `entsh`.
8. At the `entsh$` prompt, run the `init` command:

```
entsh$ init
```



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.

## 2.5.5 Installing Entrust Authority Security Manager 8.1 Service Pack 1 (SP1)

To install the Entrust Authority Security Manager 8.1 Service Pack 1:

1. Close all open applications to prevent conflicts from open applications that use shared files during the upgrade.
2. Ensure that your Security Manager database and LDAP-compliant directory are running.
3. Download the upgrade installer (`SM_81SP1_Win_upgrade.exe`) from **Entrust TrustedCare** (<https://secure.entrust.com/trustedcare>).
4. Run the upgrade installer (`SM_81SP1_Win_upgrade.exe`) to start the upgrade. The **InstallShield Wizard** appears. Follow the Wizard to begin the upgrade.
5. A **Security Manager Control Command Shell** window appears. When prompted, enter the password for `easm_entrust`.
6. When prompted, enter your **Master User** name and password.
7. Press **Enter** to close the **Security Manager Control Command Shell** window. The **InstallShield Wizard Complete** page appears.
8. Click **Finish**.

## 2.5.6 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.

### 2.5.6.1 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.

### 2.5.6.2 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.

## 2.6 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\entrusttra.ini**

### 2.6.1 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**.

### 2.6.2 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**.

### 2.6.3 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
<b>(-8973) Could not connect to the Entrust Authority Security Manager service. Security Manager service may not be running.</b>	The Entrust service is not running in the Entrust Authority Master Control shell ( <b>entsh\$</b> ).	Open the Master Control shell ( <b>entsh\$</b> ): <ol style="list-style-type: none"> <li>1. Login with <b>Master1</b>.</li> <li>2. Run <b>Service Start</b>.</li> </ol>
<b>Entrust Login Interface is currently not running. Please start before launching this application. Entrust / Entelligence will now close.</b>	Entrust Login Interface is not running.	<ol style="list-style-type: none"> <li>1. Copy <b>etlits.exe</b> from the Entrust Desktop Solutions installation package to the Windows folder. The <b>etlits.exe</b> file can be found in <b>\Designer\Entell</b>.</li> <li>2. In the Program path and file name field, type: <b>c:\windows\etlits.exe -e</b></li> </ol>

---

# Contact Us

Web site: <https://www.entrust.com>  
Support: <https://nshieldsupport.entrust.com>  
Email Support: [nShield.support@entrust.com](mailto: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](mailto:nShield.support@entrust.com)

[nshieldsupport.entrust.com](https://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