Betrusted®

UniCERT

Version 5.2.1

Administrator's Guide for Windows

Written and published by Betrusted.

License and credits

Betrusted licenses UniCERT. By installing and/or using this software product, you accept the terms and conditions of the current standard Betrusted license agreement. If you do not have a current copy of this agreement and would like to see it, please contact the Betrusted contracts department. If you have a signed license agreement with Betrusted for this software product, the terms and conditions of that signed license agreement take precedence over the standard terms and conditions.

Third-party licenses and credits

UniCERT uses the following third-party libraries:

- XMLSec, copyright © 2002 Aleksey Sanin.
- LibXML, copyright © 1998-2002 Daniel Veillard.
- LibEAY, copyright © 1995-1998 Eric Young (eay@cryptsoft.com)
- XML4c, copyright © 1999-2000 The Apache Software Foundation.

For more information on the licensing for these libraries, see the `<install directory>\docs\thirdpartylicense.txt` file supplied with UniCERT v5.2.1.

Contents

Chapter 1

Getting started with UniCERT

This guide describes the tasks you perform to configure and start UniCERT. The tasks, such as setting up database accounts for PKI entities and using the UniCERT Token Manager to manage multiple PKCS#11 devices, are organized as chapters. You can perform most tasks by running wizards or utilities, which guide you through the steps required to configure and start UniCERT.

Ensure you read the *UniCERT v5.2.1 Product Overview* prior to reading this guide and read the *UniCERT Core v5.2.1 Installation Guide* before you attempt to set up UniCERT.

Setting up UniCERT v5.2.1 on a single computer

This section explains how to set up UniCERT for the first time so that several components run on a single computer. You might use this setup for demonstration or testing purposes. More detailed information, that expands on the steps in this section, is provided in the various guides in the documentation set. We refer to these guides where appropriate. For a detailed description of this deployment, see Chapter 3, *Getting ready for your PKI deployment*, in the *UniCERT Core v5.2.1 Installation Guide*.

Complete the following tasks to set up UniCERT v5.2.1 for the first time:

1. Install, at a minimum, one CA and one CAO. Refer to *UniCERT Core v5.2.1 Installation Guide* for information on installing UniCERT components. You can set up other UniCERT components at a later time.
2. Create user accounts on the Oracle database for the CA and CAO using the Database Wizard (see Chapter 2, *Using the Database Wizard*).
3. Start the CAO using **Start>Programs>Betrusted UniCERT v5.2.1>CA Operator**.
4. The CAO displays the **User Profile Logon** dialog, which asks you to create your user profile. Click **Cancel** to exit out of this dialog. Before you can create a user profile, you first need to create a new

PKI and register the CA and CAO, generating their keys and certificates.

5. Select **File>New>Policy**, and the CAO displays a wizard for creating registration policies (RPs). Follow the on-screen instructions to create RPs for the CA and CAO. Alternatively, you can use the default RPs provided with the installation. See Chapter 2, *Defining registration policies for certification*, in the *UniCERT v5.2.1 Configuration Guide* for more information on RPs, and Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on setting up a PKI.
6. Save your RPs using **File>Save As**. Two files are created for each RP, one with an `.rpf` extension and one with an `.xml` extension. Check that these two files have been saved to the directory you specified. If they do not exist, resave your RPs.
7. Create a new PKI using **File>Create New PKI**. Follow the on-screen instructions to create the PKI. As part of these instructions, you create a user profile on a database account. In this case it means logging onto the CA database account that you created using the Database Wizard in step 2 and importing the CA and CAO RPs that you created in step 5. These details (with the exception of sensitive information such as passwords) are remembered for subsequent starts.
8. Save the personal secure environment (PSE) files for the CA and CAO when prompted. You need these PSE files for creating the crypto profiles in the next step. You can save the PSE files to disk or smart card.

Store your PSEs and smart cards securely at all times, as they contain your keys and other sensitive information. Log off your account and remove your smart card from the reader if you leave your computer for any reason.

Refer to Chapter 4, *Creating and initializing your PKI* in the *UniCERT v5.2.1 Configuration Guide* for more information on saving PSEs. You can also generate and save the PSEs on a different computer to the computer where the CAO is installed. This is discussed in Chapter 5, *Generating keys on different computers*.

9. Create crypto profiles for the CA and CAO using the CAO (see Chapter 4, *Creating and initializing your PKI* in the *UniCERT v5.2.1 Configuration Guide*). Alternatively, you can create crypto profiles using the UniCERT Token Manager (see Chapter 3, *Using the UniCERT Token Manager*).
10. Start the CAO using the crypto profiles you created in step 9, following the on-screen instructions. Again, you must log onto the CAO user account that you created in step 2.

11. Edit the CA's properties. To do this, double-click the CA icon in your PKI to display the CA's properties screen, and select the **Server Parameters** tab. The CA's default properties are displayed. If required, change **Host Name** to the name of the computer from which the CA will run, and change **Port Number** to a port that is available.

We recommend that you disable all ports not in use on the computer hosting the CA service. For more information on using UniCERT securely, see Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

12. Click **Apply** or **OK** for the changes to take effect and save your PKI.
13. Run the Service Manager and select **Service>New Instance**. Follow the wizard's instructions to add a new instance of a CA (see Chapter 4, *Using the UniCERT Service Manager*).
14. Right-click the instance name and select **Start**. The Service Manager prompts you for the CA's crypto profile (see step 9) and the database logon information (see step 2). The CA service then starts.
15. The CAO connects to the CA. Check that this connection has been established, it is displayed in the bottom right corner of the CAO main screen.

Once you have successfully completed these setup tasks, you can install and set up other UniCERT components. Refer to Chapter 7, *Defining your PKI* in the *UniCERT v5.2.1 Configuration Guide* for instructions on how to do this.

Setting up UniCERT v5.2.1 on different computers

This section explains how to set up UniCERT for the first time with different components running on different computers. More detailed information that expands on the steps in this section is provided in the various guides in the documentation set. We refer to these guides where appropriate. For more information on deploying UniCERT in different configurations, see Chapter 3, *Getting ready for your PKI deployment*, and Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

Read the *UniCERT Core v5.2.1 Installation Guide* before you attempt to set up UniCERT.

In the following steps, we explain how to set up the CAO on one computer and the CA on a different computer:

1. Install a CA on one computer and a CAO on a different computer. Ensure you also install instances of the Database Wizard, the Key Generator, and the Token Manager on both computers. Refer to the *UniCERT Core v5.2.1 Installation Guide* for information on installing UniCERT components. You can install and set up other UniCERT components at a later time.
2. Create user database accounts for the CA and CAO on their own computers using the Database Wizard (see Chapter 2, *Using the Database Wizard*).

Ensure the Oracle client is installed on any computer on which you are creating user accounts using the Database Wizard.

3. Start the CAO using **Start>Programs>Betrusted UniCERT v5.2.1>CA Operator**. The CAO displays the **User Profile Logon** dialog, which asks you to create your user profile.
4. Click **Cancel** to exit out of this dialog. Before you can create a user profile, you first need to initialize your PKI and register the CA and CAO, generating their keys and certificates on their own computers.
5. Select **File>New>Policy**, and the CAO displays a wizard for creating registration policies (RPs). Follow the on-screen instructions to create RPs for the CA and CAO. Alternatively, you can use the default RPs provided with the installation. See Chapter 2, *Defining registration policies for certification*, in the *UniCERT v5.2.1 Configuration Guide* for more information on RPs.
6. Save your RPs using **File>Save As**. Two files are created for each RP, one with an `.rpf` extension and one with an `.xml` extension. Check that these two files have been saved to the directory you specified. If they do not exist, resave your RPs.
7. Create a new PKI using **File>Create New PKI**. Follow the on-screen instructions to create the PKI. As part of these instructions, you create a user profile, which means logging onto the CA database account (on the CA's computer) that you created using the Database Wizard in step 2 and importing the CA and CAO RPs that you created in step 5. These details (with the exception of sensitive information such as passwords) are remembered for subsequent starts.
8. The wizard asks you if you want to generate the entity's keys locally (on the CAO computer) or export the request and generate the keys remotely (on the CA computer). Select to generate the keys remotely. A file with a `.kgf` extension is created. See

Chapter 5, *Generating keys on different computers*, for more information.

You can generate your entity's keys locally; however, for security reasons this is not recommended as you have to transport your entity's private keys to the CA computer.

9. Save the PSE file for the CAO when prompted. You need these PSE files for creating the crypto profiles in step 14. You can save the PSE files to disk or smart card. Refer to Chapter 4, *Creating and initializing your PKI*, in the *UniCERT v5.2.1 Configuration Guide* for more information.

Store your PSEs and smart cards securely at all times, as they contain your keys and other sensitive information. Log off your account and remove your smart card from the reader if you leave your computer for any reason.

10. Follow the wizard's instructions and choose to resume your PKI creation at a later time.
11. Load the `.kgf` extension on the CA computer and use the Key Generator to generate the keys and certificates. See Chapter 5, *Generating keys on different computers*, for more information on generating keys on another computer.
12. Load the updated `.kgf` file back onto the CAO computer.
13. In the CAO, select **File>Create New PKI** and click **Have PKI file.** Locate your updated `.kgf` file and click **Next**. The CAO resumes where you left off in step 10. Follow the on-screen instructions to complete the process.
14. Create crypto profiles for the CA and CAO on their respective computers using the UniCERT Token Manager (see Chapter 3, *Using the UniCERT Token Manager*).
15. Start the CAO using the crypto profiles you created in step 14, following the on-screen instructions. Again, you must log onto the CAO user account that you created in step 2.
16. Edit the CA's properties. To do this, double-click the CA icon in your PKI to display the CA's properties screen, and select the **Server Parameters** tab. Change **Host Name** to the name of the computer from which the CA will run, and change **Port Number** to a port that is available.

We recommend that you disable all ports not in use on the computer hosting the CA service. For more information on using UniCERT securely, see Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

17. Click **Apply** or **OK** for the changes to take effect and save your PKI.
18. On the CA computer, run the Service Manager and select **Service> New Instance**. Follow the wizard's instructions to add a new instance of a CA (see Chapter 4, *Using the UniCERT Service Manager*).
19. Right-click the instance name and select **Start**. The Service Manager prompts you for the CA's crypto profile (see step 14) and the database logon information (see step 2). The CA service then starts.
20. The CAO connects to the CA. Check that this connection has been established: It is displayed in the bottom right corner of the CAO main screen.

Once you have successfully completed these setup tasks, you can install and set up other UniCERT components. Refer to the *UniCERT Core v5.2.1 Installation Guide* for information on installing other UniCERT components, and refer to Chapter 7, *Defining your PKI*, in the *UniCERT v5.2.1 Configuration Guide* for instructions on creating and registering other PKI entities. If you want to install UniCERT components on different computers, follow the steps in Chapter 5, *Generating keys on different computers*.

Chapter 2

Using the Database Wizard

The UniCERT components store configuration information, certificates, certificate revocation lists (CRLs), authority revocation lists (ARLs), and event logs in an Oracle database. Use the Database Wizard to create user accounts and database instances for your PKI entities and to configure the underlying database structures.

Checking parameters in Oracle init<SID>.ora file

Before running the Database Wizard, check that the parameters in the Oracle `init<SID>.ora` file have the correct values. This file is located in the `<ORACLE_BASE>\admin\<INSTANCE_NAME>\pfile` directory on the computer where your Oracle server is installed.

To check the parameters:

1. Open the `init<SID>.ora` file in the `<ORACLE_BASE>\admin\<INSTANCE_NAME>\pfile` directory for editing.
2. Ensure that the value of the `max_enabled_roles` parameter is 148.
3. Ensure that the value of the `open_cursors` parameter is 300.
4. Close the file.

If you change these parameters, stop and restart the database before proceeding.

Running the Database Wizard

Ensure that you have already installed and configured Oracle, as explained in the *UniCERT v5.2.1 Database Administrator's Guide,* and installed the UniCERT components for which you want to create database instances or user accounts.

If you installed the Oracle server on a remote computer, you can run the Database Wizard from the local computer where the Oracle client is installed. The Database Wizard creates the user accounts and configures the database on the remote Oracle server.

To run the Database Wizard, follow these steps:

1. Click **Start>Programs>Betrusted UniCERT v5.2.1>Database Wizard**. After several seconds, the Database Wizard starts and the **Database Logon** dialog is displayed, as in Figure 1.

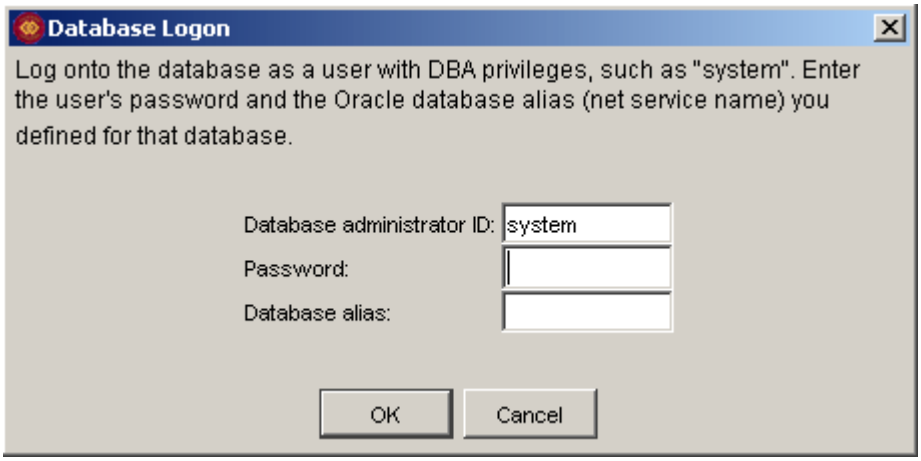


Figure 1: Logging onto the database

The Oracle user must have the correct permissions for directories used in the Database Wizard procedures. See the *UniCERT v5.2.1 Database Administrator's Guide* for more information.

2. Connect to the Oracle database that you created for UniCERT:
   - **Database administrator ID**: Enter a username that has Oracle database administrator privileges, such as `system`.

If you have not already done so, change the default Oracle database administrator's password to ensure only authorized administrators of your PKI can log onto the CA, RA, and KAS databases.

   - **Password**: Enter the database administrator's password.
   - **Database alias**: Enter the database alias (net service name) for the database created with Oracle. In most cases, this is the system identifier (SID) or Global Database Name that you defined when you created the Oracle database.

If you are not sure what the value of database alias is, look up the value for the net service name in the local Oracle configuration file, `TNSNAMES.ORA`. For more information, see the *UniCERT v5.2.1 Database Administrator's Guide*.

3. Click **OK**. The **UniCERT Database Wizard: Welcome** screen is displayed, as in Figure 2.

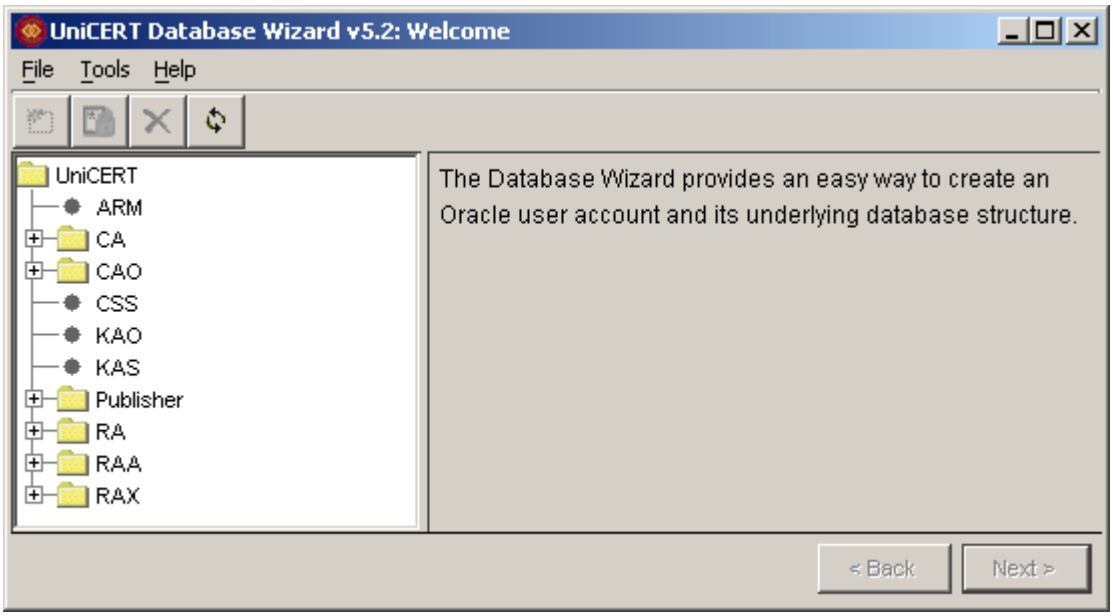


Figure 2: The UniCERT Database Wizard main screen

This **UniCERT Database Wizard: Welcome** screen displays the UniCERT component list in alphabetical order. Table 1 explains the toolbar buttons.

Table 1: The Database Wizard toolbar buttons

Button	Description
	Click the **Refresh List** button to show the latest information in the component list. This is the only button that is available when you first start the Database Wizard.
	Select a component and click the **Create New Entity** button to create a new database account for that component. For information on how to create a new database account, see *Creating user accounts* on page 10.
	Expand a component to see the database accounts that have been created for it. Select an account and click the **Update Password** button to change its passphrase. For more information, see *Updating a database password* on page 18.
	Expand a component to see the database accounts that have been created for it. Select an account and click the **Remove the selected entity** button to delete the account. For more information, see *Deleting a user account or database* on page 20.

You can also access the toolbar's options in the following way:

- By selecting the appropriate button from the toolbar

- By right-clicking an entity and selecting the required option from the right-click menu
- By selecting the appropriate option from the **Tools** menu

Creating user accounts

The instructions in the following sections explain how to create user accounts for your UniCERT components. The steps for creating user accounts and databases for the CA, RA, and KAS are similar. Likewise, the steps for creating the user accounts for the CAO, CSS, RA eXchange, ARM, and KAO are similar; ensure that you create their accounts on the associated database, as follows:

- Create the CA, CAO, and CSS accounts on the CA database instance that you specify.
- Create the RA user, RA Auditor (RAA on the Database Wizard screens), RA eXchange (RAX on the Database Wizard screens), and ARM accounts on the RA database instance that you specify.
- Create the Publisher user account on the Publisher database instance that you specify.
- Create the KAS and KAO accounts on the KAS database instance that you specify.

We explain how to create a CA user account and database and how to create a CAO user account. For information on creating CA, RA, and KAS user accounts and databases, follow the instructions in *Creating a CA user account and database* on page 10. For information on creating CAO, CSS, RA eXchange, RA Auditor, ARM, and KAO user accounts, follow the instructions in *Creating a CAO user account* on page 13.

We explain how to create a Publisher user account separately, as some of the fields on the screens are slightly different (see *Creating a Publisher user account and database* on page 15).

For security purposes, we recommend that you create separate user accounts for all UniCERT components.

Creating a CA user account and database

These instructions explain how to create a CA user account and database. The Database Wizard creates the CA account on the CA database.

1. In the **UniCERT Database Wizard: Welcome** dialog, click **CA** in the component list. The **Create New Entity** button becomes available.

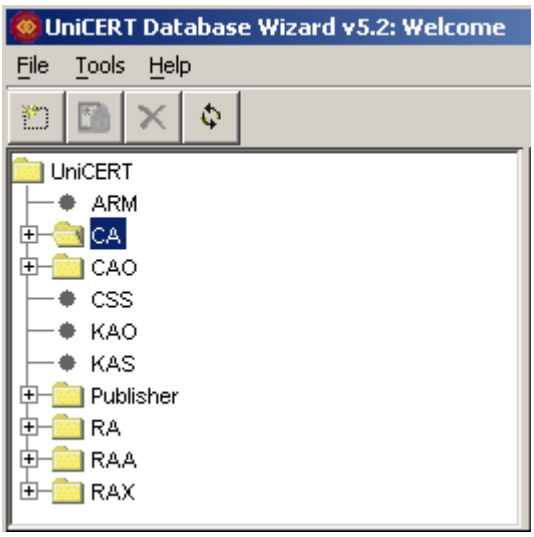


Figure 3: Creating a CA user account

2. Click the **Create New Entity** button, or right-click **CA** in the component list and select **Create Entity**. The **Create CA** dialog is displayed, as in Figure 4.

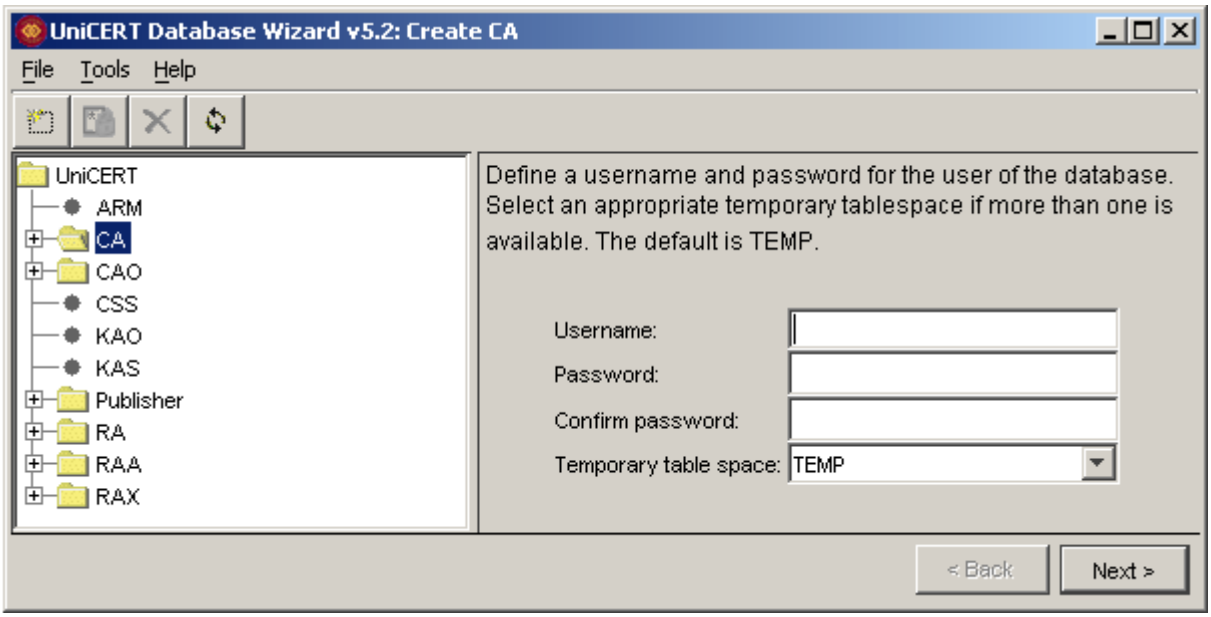


Figure 4: The CA parameters

3. Specify values for the CA user account in the Oracle database:
   - **Username**: Enter a username for the CA. The username must be 30 characters or fewer, and it must start with an alphabetic character (a to z). Do not use quotation marks or parentheses, the opening single quote (‘), any of the ~ % ^ & * - = + ; : \ , . /

£ @ { } [ ] < > symbols, the question mark (?), or the exclamation mark (!).

If you subsequently delete a CA username profile, you cannot reuse that name, unless you first manually remove the temporary tablespace files on the Oracle server.

- **Password**: Enter a password for the CA. The password must be at least 8 characters and a maximum of 30 characters in length. Do not use quotation marks or the @ and {} symbols.
- **Confirm password**: Enter the same password to confirm that it was entered correctly.
- **Temporary table space**: Select the temporary tablespace, if more than one is available. Unless there is a compelling reason to do otherwise, use the default temporary tablespace `TEMP`.

4. Click **Next**. The dialog displayed in Figure 5 is displayed.

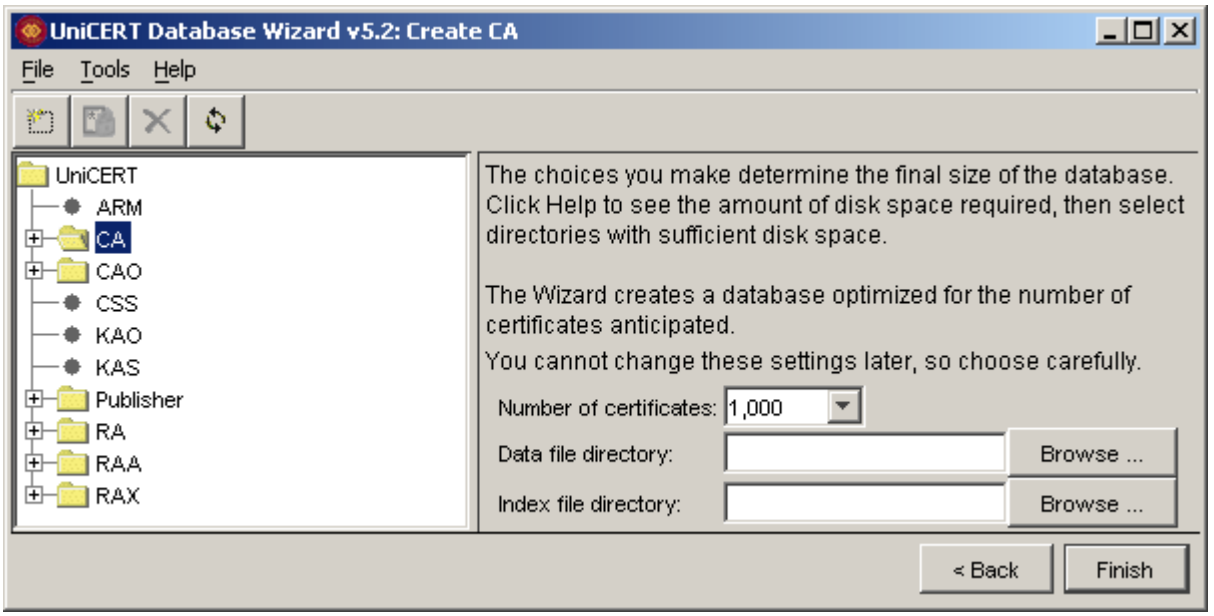


Figure 5: The CA database parameters

5. Specify values for the CA database size:
   - **Number of certificates**: From the drop-down list, select the approximate number of certificates for the CA. Select a number greater than the number you expect to need.
   - **Data file directory**: Enter a location for the data file directory or click **Browse** to select a location. You may want to specify directories on different drives for load balancing purposes. The directories must be located on the computer where the Oracle server is running. See the Oracle documentation for guidelines on selecting directories. Do not use quotation marks

or parenthesis, the back tick (‘), the @, *, and ~ symbols, the question mark (?), or the exclamation mark (!) in path names.

— **Index file directory**: Enter a location for the index file directory or click **Browse** to select a location. You may want to specify directories on different drives for load-balancing purposes. The directories must be located on the computer where the Oracle server is running. See the Oracle documentation for guidelines on selecting directories. Do not use quotation marks or parenthesis, the back tick (‘), the @, *, and ~ symbols, the question mark (?), or the exclamation mark (!) in path names.

6. Click **Finish**. The Database Wizard saves the specified parameters and begins to create the requested database structures.
7. The Database Wizard displays a message dialog informing you that the database structures are to be created. Click **OK**.
8. When the processing is complete, the Database Wizard displays a message informing you that the user account and database structures were successfully created. Click **OK**.
9. In the **UniCERT Database Wizard** main screen, the component list shows the newly created CA user account. Select **File>Exit** if you are finished using the Database Wizard or create an account for another UniCERT entity.

To create RA or KAS user accounts, follow steps 1-9, replacing CA with RA or KAS where appropriate.

Creating a CAO user account

These instructions explain how to create a CAO user account. You must create a CA user account and database before creating a CAO user account, as the Database Wizard creates the CAO account on the CA database.

Ensure you create an RA user account and database before creating an RA Auditor, RA eXchange, or ARM user account. Likewise, ensure you create a KAS user account and database prior to creating a KAO user account.

To create CAO user account:

1. In the **UniCERT Database Wizard** dialog, click **CAO** in the component list, as in Figure 6. The **Create New Entity** button becomes available.

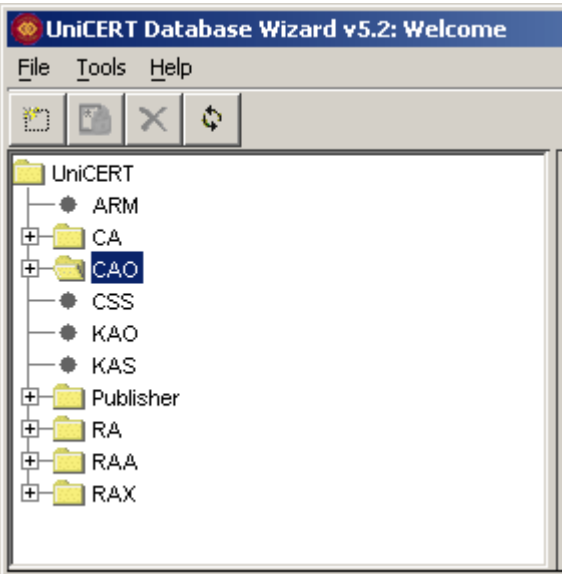


Figure 6: Creating a CAO user account

2. Click **Create New Entity**, or right-click **CAO** and select **Create Entity**. The **Create CAO** dialog is displayed, as in Figure 7.

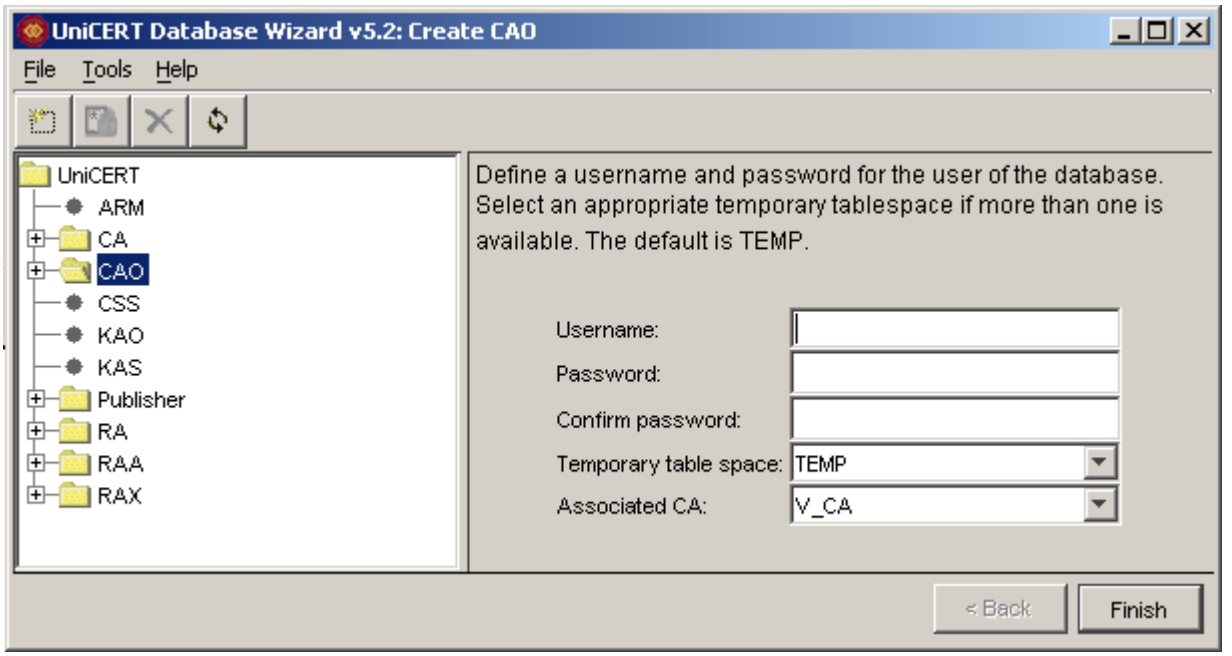


Figure 7: The CAO parameters

3. Specify values for the CAO user account on the CA Oracle database instance:
   - **Username**: Enter a username for the CAO. The username must be 30 characters or fewer, and it must start with an alphabetic character (a to z). Do not use quotation marks or parentheses, the opening single quote (‘), any of the ~ % ^ & * - = + ; : \ , . /

£ @ { } [ ] < > symbols, the question mark (?), or the exclamation mark (!).

If you subsequently delete a CAO username profile, you cannot reuse that name, unless you first manually remove the temporary tablespace files on the Oracle server.

- **Password**: Enter a password for the CAO. The password must be at least 8 characters and a maximum of 30 characters in length. Do not use quotation marks or the @ and {} symbols.
- **Confirm password**: Enter the same password to confirm that it was entered correctly.
- **Temporary table space**: Select the temporary tablespace, if more than one is available. Unless there is a compelling reason to do otherwise, use the default temporary tablespace `TEMP`.
- **Associated CA**: Select the appropriate CA from the drop-down list. The CAO user you create is now associated with the specified CA database and has access to that data.

If you are creating an ARM, RA Auditor, or RA eXchange user account, **Associated CA** is replaced by **Associated RA** on the screen. Select the appropriate RA from the drop-down list. If you are creating a KAO user account, **Associated CA** is replaced with **Associated KAS** on the screen. Select the appropriate KAS from the drop-down list.

4. Click **Finish**.
5. When the processing is complete, the Database Wizard displays a message informing you that the user account was successfully created. Click **OK**.
6. In the **UniCERT Database Wizard** main screen, the component list shows the newly created CAO user account. Click **Exit** if you are finished using the Database Wizard or create an account for another UniCERT entity.

To create CSS, RA eXchange, RA Auditor, ARM, or KAO user accounts, follow the instructions in steps 1-6, replacing CAO with CSS, RA eXchange, RA Auditor, ARM, or KAO where appropriate.

Creating a Publisher user account and database

These instructions explain how to create a Publisher user account and database. The Database Wizard creates the Publisher user account on the Publisher database.

Follow these steps to create a Publisher user account and database:

1. In the **UniCERT Database Wizard: Welcome** dialog, click **Publisher** in the component list. The **Create New Entity** button becomes available, as in Figure 8.

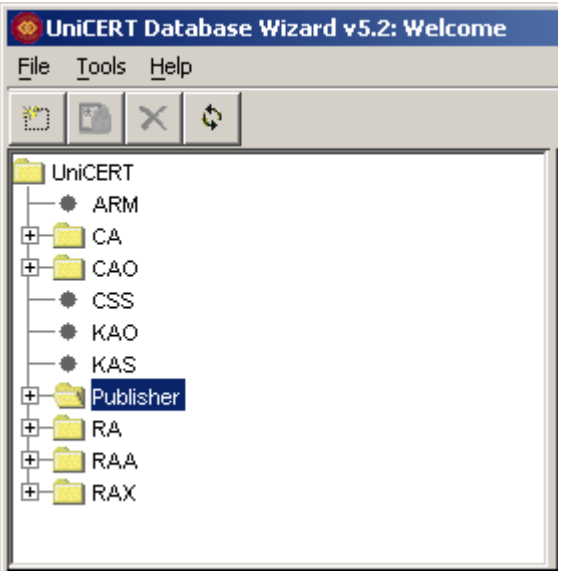


Figure 8: Creating a Publisher user account

2. Click **Create New Entity**, or right-click **Publisher** and select **Create Entity**. The **Create Publisher** dialog, similar to that in Figure 9, is displayed.

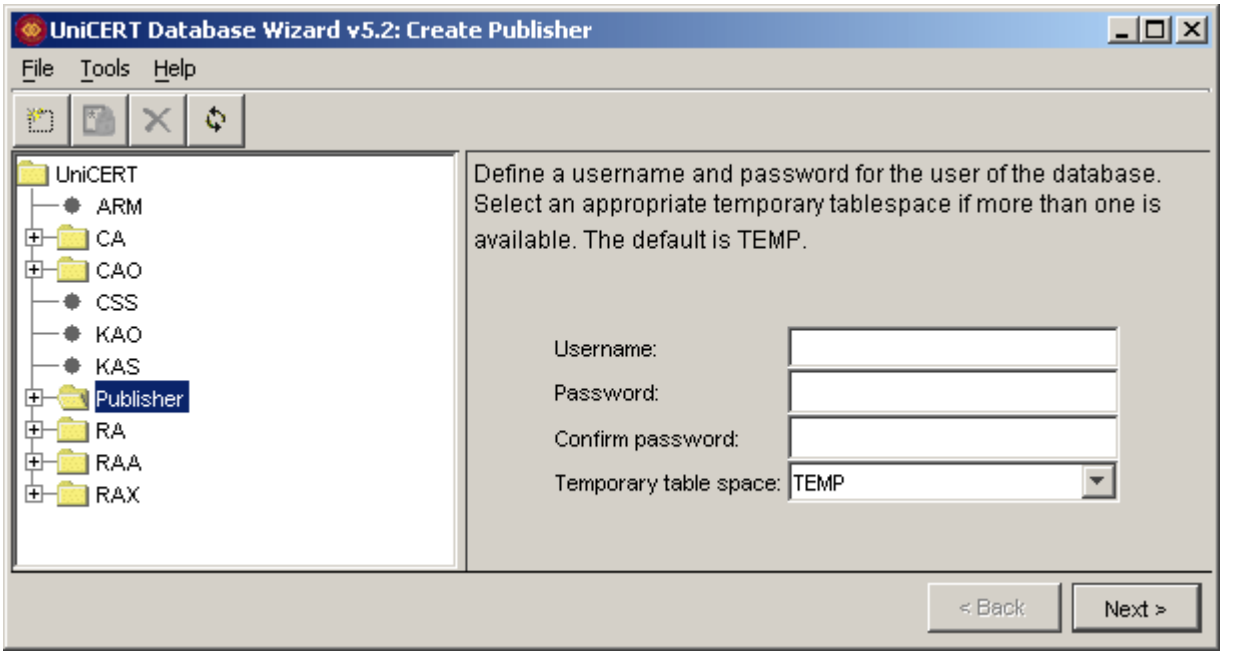


Figure 9: Publisher parameters

3. Specify values for the Publisher user account on the Publisher database instance:

— **Username**: Enter a username for the Publisher. The username must be 30 characters or fewer, and it must start with an alphabetic character (a to z). Do not use quotation marks or parentheses, the opening single quote (‘), any of the ~ % ^ & * - = + ; : \ , . / £ @ { } [ ] < > symbols, the question mark (?), or the exclamation mark (!).

If you subsequently delete a Publisher username profile, you cannot reuse that name, unless you first manually remove the temporary tablespace files on the Oracle server.

— **Password**: Enter a password for the Publisher. The password must be at least 8 characters and a maximum of 30 characters in length. Do not use quotation marks or the @ and {} symbols.

— **Confirm password**: Enter the same password to confirm that it was entered correctly.

— **Temporary table space**: Select the temporary tablespace, if more than one is available. Unless there is a compelling reason to do otherwise, use the default temporary tablespace `TEMP`.

4. Click **Next**.

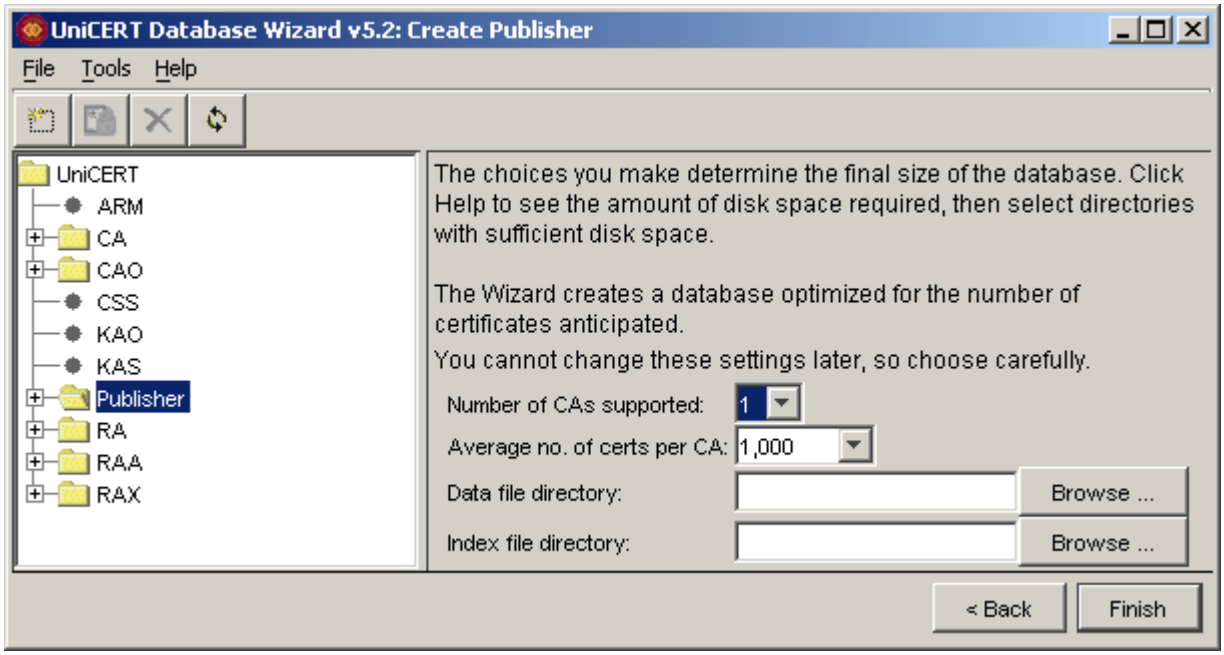


Figure 10: Publisher database parameters

5. Specify values for the Publisher database size. You cannot changes these settings later:

— **Number of CAs supported**: From the drop-down list, select the number of CAs to which your Publisher entity will connect. The maximum number you can enter is 10.

- **Average number of certificates per CA:** From the drop-down list, select the approximate number of certificates that each CA will process. Select a number greater than the number you expect to need.
- **Data file directory**: Enter a location for the data file directory or click **Browse** to select a location. You may want to specify directories on different drives for load-balancing purposes. The directories must be located on the computer where the Oracle server is running. See the Oracle documentation for guidelines on selecting directories. Do not use quotation marks or parenthesis, the back tick (‘), the @, *, and ~ symbols, the question mark (?), or the exclamation mark (!) in path names.
- **Index file directory**: Enter a location for the index file directory or click **Browse** to select a location. You may want to specify directories on different drives for load-balancing purposes. The directories must be located on the computer where the Oracle server is running. See the Oracle documentation for guidelines on selecting directories. Do not use quotation marks or parenthesis, the back tick (‘), the @, *, and ~ symbols, the question mark (?), or the exclamation mark (!) in path names.

6. Click **Finish**. The Database Wizard saves the specified parameters and begins to create the requested database structures.
7. The Database Wizard displays a message dialog informing you that the database structures will be created. Click **OK**.
8. When processing is complete, the Database Wizard displays a message informing you that the user account and database structures were successfully created. Click **OK**.
9. In the **UniCERT Database Wizard** main screen, the component list contains the newly created Publisher user account. Select **File>Exit** if you are finished using the Database Wizard or create an account for another UniCERT entity.

Updating a database password

You can update or change the password of any account in the component list. We recommend that you do this on a regular basis to increase secure operation of your UniCERT setup.

1. In the **UniCERT Database Wizard** dialog, expand the component list to view user accounts and select the account for which you want to change the password. The **Update Password** button (see Table 1) becomes available.
2. Click the **Update Password** button. Alternatively, right-click the entity for which you want to change the password and select **Update Password**. The **Update Password** dialog, similar to that in Figure 11, is displayed.

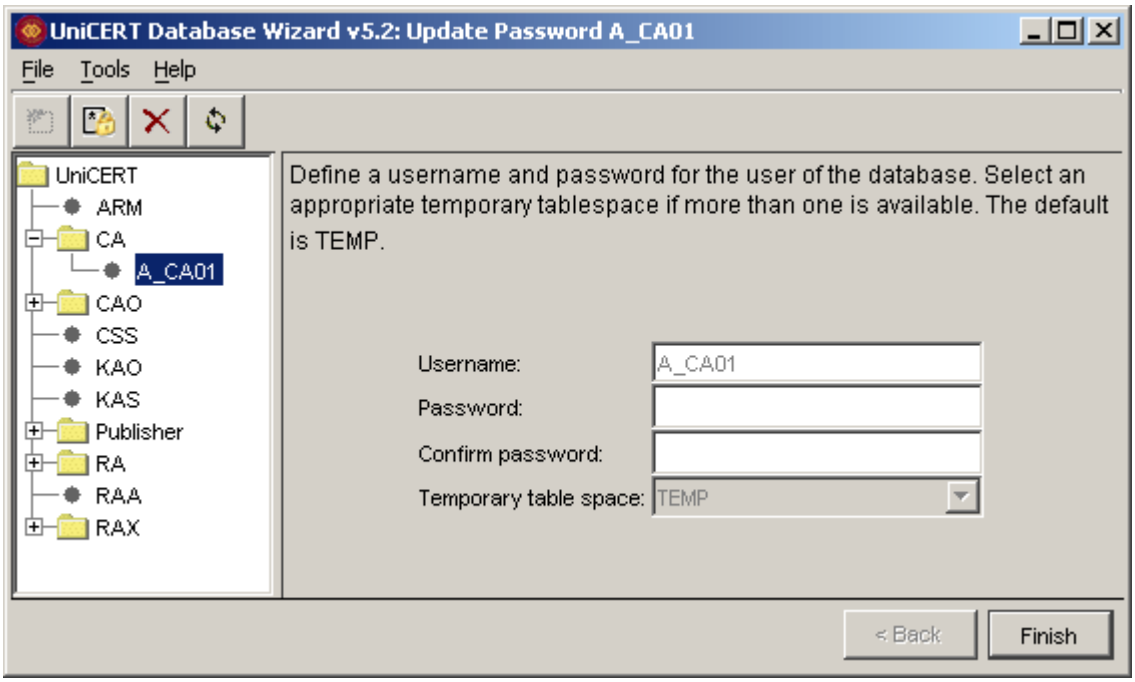


Figure 11: Password update parameters

3. Specify a new password and confirm it. You cannot edit the other options. The password must be at least 8 characters and a maximum of 30 characters in length. Do not use quotation marks or the @ and {} symbols.

We strongly recommend that you change the password on user accounts on a regular basis. In this way you can restrict access to sensitive PKI components to authorized users. See Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on securely deploying UniCERT.

---

4. Click **Finish**. The Database Wizard saves the updated password.
5. When the processing is complete, the Database Wizard displays a message informing you that the password has been changed. Click **OK**.

Deleting a user account or database

You can delete any user account or database instance in the component list using the Database Wizard.

Deleting a database user account or a database instance is a serious step. Ensure only authorized, competent administrators have access to this functionality. For a more detailed discussion on security issues, see Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

If you delete a database instance, the user accounts for all components using that database are also removed. For example, if you delete a CA database and user account, any CSS or CAO user accounts on that database are also removed.

To delete a user account or database, follow these steps:

1. Expand an entry in the component list and select an account. The **Remove the selected entity** button is activated.
2. Click **Remove the selected entity** button. Alternatively, right-click the entity and select **Remove Entity**.
3. Click **Yes** to confirm you want to delete the entity. The Database Wizard removes the account, or database and associated accounts. It then displays the **Remove Completed** screen. If you are removing a database, that is, a CA, RA, KAS, or Publisher account, note which temporary tablespace files require manual removal.
4. Click **OK**. If you are removing a database, manually remove the temporary tablespace files from your Oracle database.

Chapter 3

Using the UniCERT Token Manager

If you have a cryptographic hardware device with a PKCS#11 compliant interface, you can use the UniCERT Token Manager to manage multiple PKCS#11 devices and to initialize and administer the tokens or smart cards that the hardware device uses. You can also change the PINs protecting tokens, as well as administer the objects stored on tokens or smart cards.

In addition, you can use the Token Manager to create crypto profiles. UniCERT v5.2.1 uses crypto profiles to store the configuration information required to start UniCERT components. This configuration information includes details of the location of the personal secure environment (PSE) file, whether the PSE is split, and details of any PKCS#11 devices used. Each UniCERT component has its own crypto profile.

In this document we use the term PKCS#11 device to refer to the logical view of a cryptographic hardware/software token or smart card, as the UniCERT Token Manager does not distinguish between these PKCS#11 types.

Token Manager functionality

The Token Manager provides the following functions:

- Creating, modifying, and testing crypto profiles
- Changing passphrases on PSE files
- Splitting PSEs
- Copying PSEs and certificates from token to disk and vice versa

- Viewing the attributes of objects
- Deleting objects such as PKCS#11 devices, PSEs, crypto profiles and PKCS#12 files

Not all vendors' tokens, particularly the international versions, support all of these features. However, the majority of the PKCS#11 products that UniCERT supports provide the necessary functionality. Check your vendor information for details of supported features for each device.

Tokens contain private and public storage areas. Private storage is the memory that requires authorized access using a PIN. The private keys and non-UniCERT file objects that you add are always stored in a token's private storage area.

Depending on the vendor's implementation, the private storage is either on the token itself or it is on the associated PKCS#11 device hard disk. For example, nCipher encrypts private keys using keys from the PKCS#11 device as well as the token, and then stores the encrypted keys on the hard disk.

In contrast, PSEs are stored in the public areas of smart cards.

For information on the supported PKCS#11 devices, see Chapter 2, *Installation prerequisites*, in the *UniCERT Core v5.2.1 Installation Guide*.

Starting the UniCERT Token Manager

To start the Token Manager, double-click its icon on your desktop or select **Start>Programs>Betrusted UniCERT v5.2.1>Token Manager**. The Token Manager main screen appears, as shown in Figure 12.

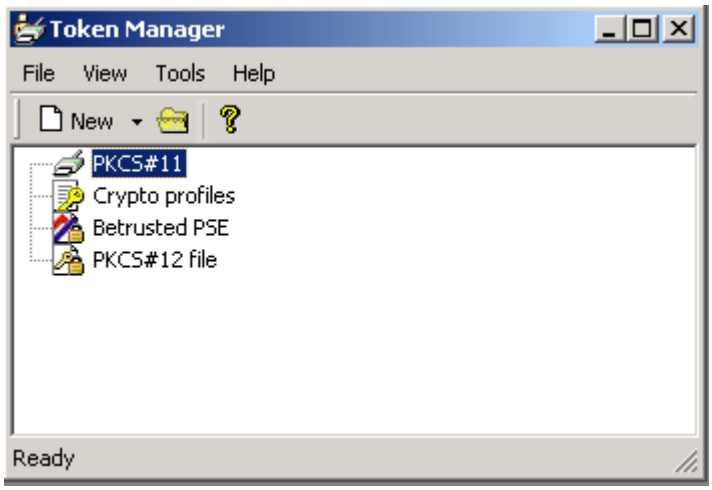


Figure 12: The Token Manager main screen

We recommend that you do not access a token using the Token Manager while the token is being used by another application. For example, if you are already using a token with the UniCERT CAO, close the CAO before you use the Token Manager to manage the token.

The Token Manager main screen contains four options:

- **PKCS#11**: Use this option to manage a PKCS#11 token or device.
- **Crypto profiles**: Use this option to create and manage crypto profiles.
- **Betrusted PSE**: Use this option to manage PSE files.
- **PKCS#12 file**: Use this option to manage PKCS#12 files.

Managing tokens and devices

Use the Token Manager to manage multiple PKCS#11 devices and tokens.

Installing a token or device

In UniCERT terms, installing a token or device means associating the device with the appropriate driver and giving it a friendly name. The driver itself must already be installed on your computer. To install a token or device, follow these steps:

1. Click **PKCS#11** and select **Tools>Token>Install**, or right-click **PKCS#11** in the main Token Manager screen and select **Install**. The Token Manager prompts you to specify your PKCS#11 device's DLL.
2. Browse to the directory where your device's `.dll` file is located, select it, and click **Open**. You are asked for a friendly name for your device or token (see Figure 13).

The friendly name is the name by which the device or token is displayed in the Token Manager and by which it is identified by other UniCERT components.

The friendly name is case-sensitive, and you must use the same friendly name if you install the device on different computers.

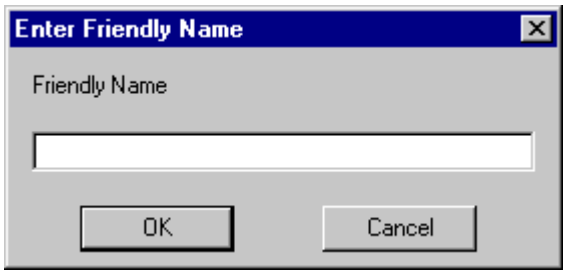


Figure 13: Entering a friendly name

Once you have specified the friendly name, the Token Manager returns you to the main screen and displays the new PKCS#11 device. In the example shown in Figure 14, a Datakey device is installed with the friendly name "Datakey".

Figure 14: Installing PKCS#11 tokens

Opening your token or device

To open your token or device, follow these steps:

1. In the Token Manager main screen, right-click the icon representing the token or device and select **Open**. Alternatively, select the type of device you want to open and choose **File>Open**.
2. Enter your user PIN and click **OK**.

Your token or device opens, and you can access the information stored on it.

Initializing your token or device

Initializing a token or device is the process of preparing it before information is written to it, similar to formatting a floppy disk. As part of the initialization process, you assign a PIN to the token to protect access to it.

Consider protecting access to sensitive information stored on your hardware security module (HSM) or PKCS#11 device, by using the M of N feature. M of N requires several users to log onto the HSM, each using their own token, before access to the HSM for administration purposes is permitted.

We recommend that you set M of N up so that a majority of users are required to log onto the device. For example, if you have five users who are authorized to use the HSM, set the M of N feature so that three of the five users are required to log onto the HSM.

The Luna CA3 token from SafeNet supports M of N authentication. Check your vendor documentation for information on other tokens.

See Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on configuring UniCERT securely.

If you enable the M of N feature on the Luna CA3 token, you cannot disable it later. Even reinitializing the token does not deactivate this feature. If you decide you no longer want this feature, send the token to Betrusted for reinitialization.

Some PKCS#11 devices need to be initialized before they can be used. Other devices do not need to be initialized (or you might have to initialize them using a vendor-supplied tool, such as the Luna PED, instead of the UniCERT Token Manager).

If you have already set up your token and it contains keys and certificates, ensure you do not initialize the token. Initializing your token erases all objects currently stored on it.

To initialize your token or device, follow these steps:

1. In the Token Manager main screen, select the token you want to initialize and select **Tools>Token>Initialize**.
2. Ensure that the selected token is not already initialized or does not contain information that you need to keep, and confirm that you want to initialize it.
3. Specify a label for your token and enter a new user PIN and a new Security Officer (SO) PIN as prompted (see Figure 15).

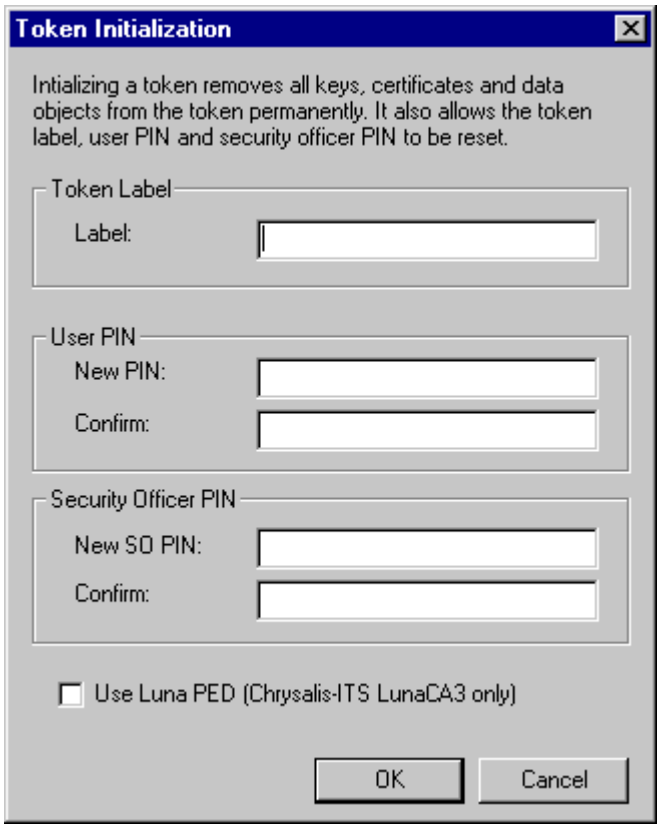


Figure 15: Entering a new label and passwords

The label is the unique name for the token on the PKCS#11 device displayed in the main Token Manager dialog; you are prompted for this label when using the token or device.

The SO is the equivalent of a superuser. The SO has more permissions for using a token than a normal user does and can manage a group of token users. For example, if a user forgets his PIN or blocks access to his token by entering the wrong PIN too often, the SO can reinitialize his token with a new PIN, once she is satisfied that the user should retain his token and its access rights. The PKCS#11 standard specifies that an SO manages tokens and their PINs, allowing only the SO to initialize the token.

Some vendors do not implement the SO or vary slightly in their implementation of this feature (see your vendor's documentation for details). However, you still have to enter an SO PIN in the **Token Initialization** dialog. For tokens that do not support the SO feature, the data in the SO PIN field is simply ignored.

If you are using a Luna PED, ensure you select **Use Luna PED** on all screens that display this option.

4. Click **OK**. The Token Manager takes a few moments to complete the initialization and confirms when it is done.
5. Click **OK** to return to the main Token Manager screen.

Changing your token's PIN

Periodically change the PINs you use to access your tokens to ensure that they remain secure, and that no unauthorized person can access them.

We recommend that you change the token user PIN at regular intervals. However, the SO's PIN does not need to be changed as frequently, because the SO does not normally access the token often.

The Token Manager provides two options for changing PINs: **Change PIN** and **Change SO PIN**.

Changing the user PIN

To change your token's user PIN, follow these steps:

1. Right-click the token in the Token Manager main screen and select **Change PIN**. The Token Manager prompts you to close the PKI device if it is in use.
2. Select **Yes** to continue.
3. Enter your new PIN in both fields as shown in Figure 16 and click **OK**.

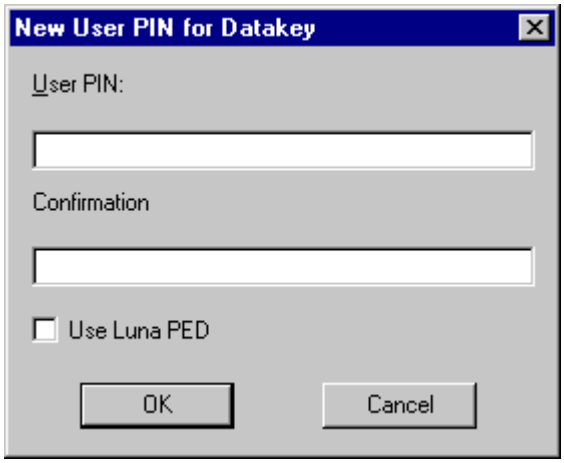


Figure 16: Changing the user PIN

4. Enter the old user PIN to access your token as shown in Figure 17. Click **OK** when you have entered the old PIN.

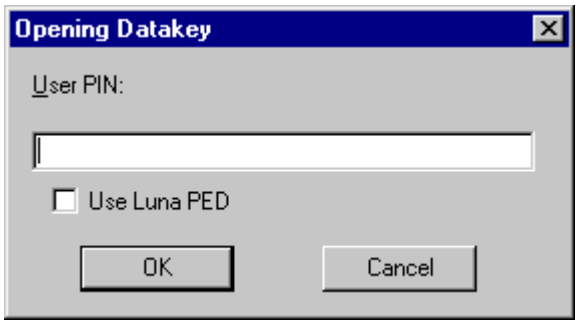


Figure 17: Opening the token using the old PIN

Your user PIN is changed, and the token is closed. You need the new PIN to open the token the next time.

Changing the SO PIN

To change your token's SO PIN, follow these steps:

1. In the main Token Manager screen, right-click the token and select **Change SO PIN**, or click the token and then select **Tools>Token> Change SO PIN**.
2. Select **Yes** to continue when prompted to close the token.
3. Enter and confirm your new SO PIN and click **OK** as shown in Figure 18.

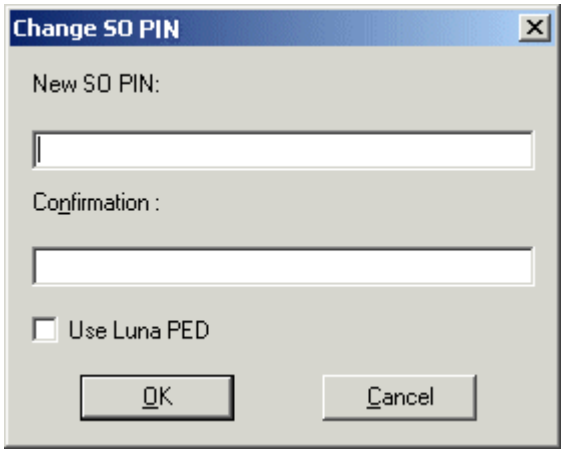


Figure 18: Changing the SO PIN

4. Enter the old SO PIN so your token can be accessed in order to change the PIN. Click **OK**.

Your SO PIN is changed, and the token is closed. You need the new PIN to open the token the next time.

Loading a PSE file onto a token or device

You can only store one PSE per token. To load a PSE file onto a token or device, follow these steps:

1. Right-click the open token and select **Load PSE**.
2. Select the PSE you are loading onto your token and click **Open**. The PSE file is loaded on to the selected token.

Once you have stored the PSE file on your token, you can delete or export it. These procedures are outlined in *Deleting a PSE file from a token or device* and *Exporting a PSE file from a token or device*.

We recommend that you make backup copies of your PSE file. If you create backups on magnetic tape, floppy disks, or optical media, store them in a secure location. For more guidance on managing your PKI, see Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

Deleting a PSE file from a token or device

If the identity associated with the PSE file is no longer valid in your PKI, for example, if the person associated with the PSE is no longer trusted, or she has changed her role in your PKI and you have issued her with new keys, you can delete her old PSE. Ensure you also delete any stored backup copies of the PSE once you are certain you do not need the keys it contains to access old messages encrypted with those keys.

To delete a PSE file from a token or device, select the **Personal Secure Environment** option, right-click, and select **Delete**. When prompted, confirm you want to delete the selected PSE file. The PSE file is removed from the token or device.

Exporting a PSE file from a token or device

If you originally created your PSE file on your token or device, you can use the export option to create a backup copy on your computer.

We recommend that you make backup copies of your PSE file. If you create backups on magnetic tape, floppy disks, or optical media, store them in a secure location. If you subsequently delete the PSE, remember to delete the backup copy. For more guidance on managing your PKI, see Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide*.

To export a PSE file from a token or device, select the **Personal Secure Environment** option, right-click and select **Export**. Specify a name for the PSE file you are exporting and the directory where you are saving it and click **Save**.

Uninstalling your token or device

To uninstall your device or token, that is, remove it from the list of PKCS#11 devices available in the Token Manager, follow these steps:

1. Click the device you are uninstalling and select **Tools>Token> Uninstall**.
2. Confirm you want to uninstall your device, as prompted.

Your token or device is removed from the Token Manager. This does not affect the driver installed for the token.

Working with crypto profiles

UniCERT v5.2.1 uses crypto profiles to store the configuration information required to start UniCERT services, such as the CA, CSS, KAS, RA, and RA eXchange, or to log onto UniCERT applications. This configuration information can include details of the location of the PSE file, whether the PSE is split, and details of any devices used.

Each UniCERT component has its own crypto profile, created on the computer on which it is run. For example, a crypto profile for a service typically stores information about the location of the PSE file and where the keys are stored; the keys might be stored on an associated HSM, such as Luna CA3 or SureWare Keyper. Then when you select the crypto profile to start the service, the Service Manager asks for the PSE's passphrase and the PIN for the HSM. See Chapter 4, *Using the UniCERT Service Manager*, for more information.

Creating a crypto profile

Before you create a crypto profile for a PKI entity, you must already have a PSE for that entity. For more information on creating PSEs for an entity, see Chapter 4, *Creating and initializing your PKI*, in the *UniCERT v5.2.1 Configuration Guide*.

To create a crypto profile, follow these steps:

1. Right-click **Crypto profiles** in the Token Manager main screen and select **Create**. The **Enter new crypto profile name** dialog is displayed.
2. Enter the name you want to assign to your new profile and click **OK**. The Token Manager displays the screen shown in Figure 19.

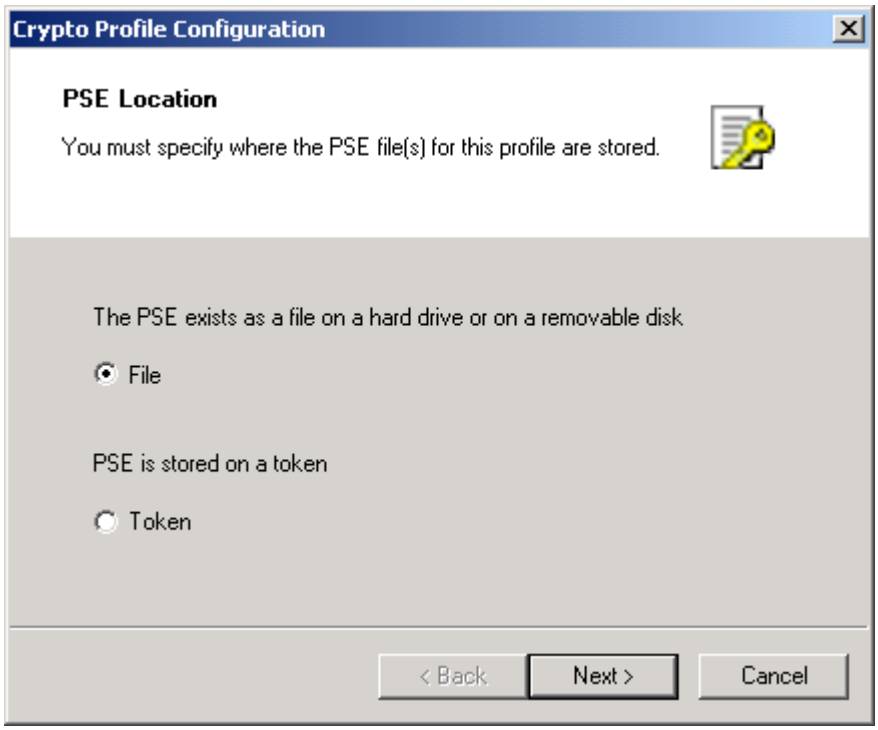


Figure 19: The PSE location screen

3. Choose whether the PSE file for this profile is stored in a file on your local computer, or on a token. Click **Next**. If your PSE is stored in a file, go to *Using a PSE stored in a file* on page 31. If it is stored on a token, go to *Using a PSE stored on a token* on page 33.

Using a PSE stored in a file

If your PSE is located in a file, the Token Manager displays the screen shown in Figure 20.

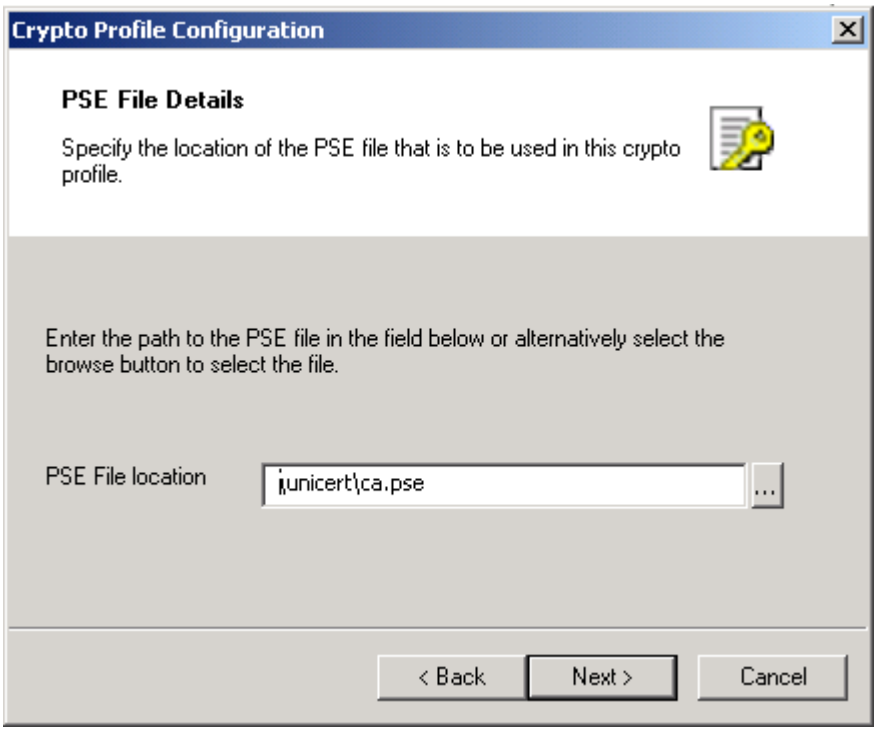


Figure 20: The PSE File Details screen

Complete the creation of your crypto profile as follows:

1. Enter the location of the PSE file in the **PSE File location** field. Alternatively, click the **Browse** button ("...") to browse to the location where the PSE file is stored.
2. Click **Next**. The Token Manager displays a dialog prompting you to enter the passphrase for the PSE file.
3. Enter the passphrase and click **OK**.

If you are using a split PSE, you are prompted to specify the location of the rest of the split PSE followed by a prompt to specify the passphrase for that part of the split PSE.

When you have completed this step, the Token Manager displays the information to create the crypto profile in a screen similar to that in Figure 21.

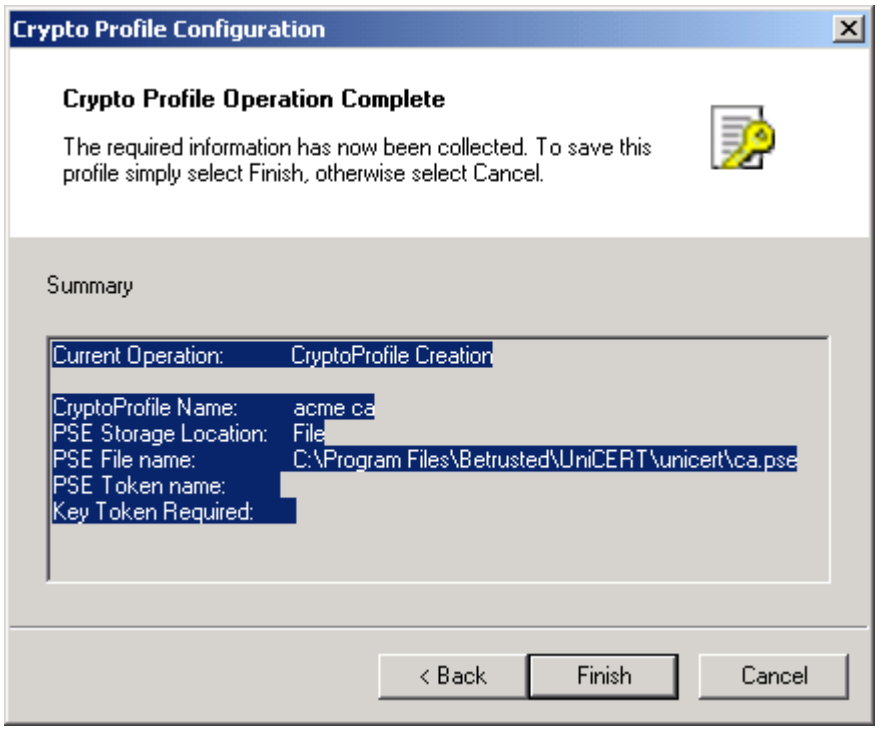


Figure 21: The CryptoProfle Operation Complete screen

The dialog displays the details of the new crypto profile, for example, the name of the profile and the PSE filename.

4. Click **Finish** to commit these changes, or click **Cancel** to exit back to the Token Manager main screen.

Using a PSE stored on a token

If your PSE is stored on a token, the Token Manager displays the screen shown in Figure 22.

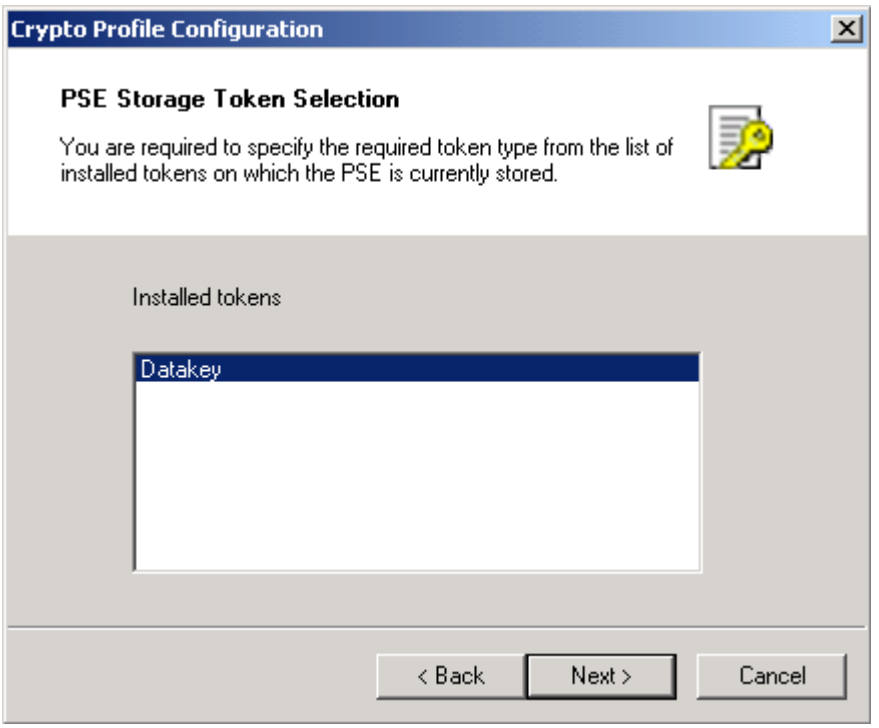


Figure 22: The PSE Storage Token Selection screen

Complete the creation of your crypto profile as follows:

1. Select the required token on which the PSE is stored from the list of tokens in the **PSE Storage Token Selection** screen.
2. Click **Next**. The Token Manager displays a dialog prompting you to enter the passphrase for the PSE file.
3. Enter the passphrase and click **OK**. The Token Manager displays a screen similar to that in Figure 21. The dialog displays the details of the profile, for example, the name of the profile and the PSE token name.
4. Click **Finish** to commit these changes, or click **Cancel** to exit back to the Token Manager main screen.

Modifying a crypto profile

Modifying a crypto profile allows you to update the information about the location of the PSE associated with the crypto profile you select.

To modify a crypto profile, right-click the required profile in the Token Manager main screen and select **Modify**, or select the relevant crypto profile and choose **Tools>CryptoProfiles>Modify**. The Token Manager displays a screen similar to Figure 19. Follow the steps described in *Using a PSE stored in a file* on page 31 or *Using a PSE stored on a token* on page 33, depending on the location of your PSE.

Testing a crypto profile

Testing a crypto profile allows you to check if the PSE associated with a particular crypto profile is at the correct location or if you have the correct token in the device reader (in the case of smart cards).

To test a crypto profile, either right-click the crypto profile you are testing and select **Test** or select the relevant crypto profile and choose **Tools>CryptoProfiles>Test**. When prompted, enter the passphrase for the associated PSE file and click **OK**. The Token Manager returns a dialog indicating whether the test was successful. Click **OK** to return to the main Token Manager screen.

If the test fails, one of the following may be the cause:

- The PSE is no longer at the configured location.
- The PIN for the token or the passphrase for the PSE is invalid.
- You inadvertently inserted the wrong token into the reader.

Confirm that you have the correct token. If it is, modify the crypto profile to match the correct location and passphrases/PINs for the entities.

Deleting a crypto profile

In certain circumstances, you might want to delete a crypto profile. Always ensure that the crypto profile is not required by a service in your PKI.

To delete a crypto profile, right-click the required crypto profile and select **Delete**, or select the crypto profile you want to delete and choose **Tools>CryptoProfiles>Delete**. The Token Manager displays a dialog asking you to confirm your deletion. Click **Yes** to delete the selected crypto profile.

Do not delete a crypto profile that is still required by a component. Deleting a crypto profile may cause some applications to fail to start.

Managing your PSE and PKCS#12 files

You can use the Token Manager to manage both PSE and PKCS#12 files.

Loading a file

To open a PSE or PKCS#12 file in the Token Manager, follow these steps:

1. Right-click **Betrusted PSE** or **PKCS#12 file** as appropriate and select **Open**.
2. Specify or browse to the location of the required file in the file locator dialog. Click **Open**.

3. Enter the passphrase of the file when prompted and click **OK**. The Token Manager returns to the main screen, which now displays details about your key and your certificate stored on your PSE or PKCS#12, as shown in Figure 23.

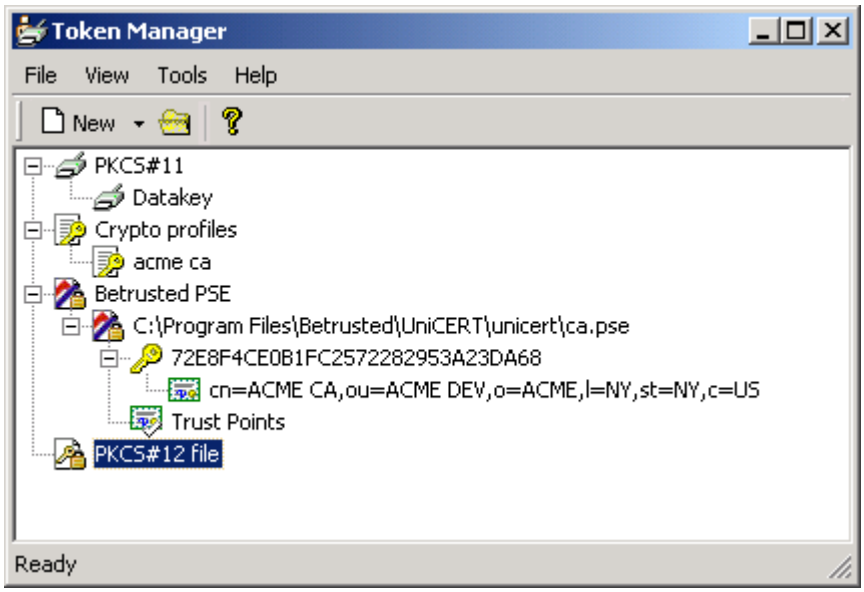


Figure 23: Adding a PSE file

The following details are displayed:

- The name and path of the PSE or PKCS#12 file
- The friendly name for each key
- The associated certificate
- The associated trust points (see *Using trust points* on page 39)

If the friendly name associated with the key is in binary, the Token Manager cannot display it, showing blocks in its place.

Changing a passphrase

You can change the passphrase associated with a PSE or PKCS#12 file. We recommend that you change passphrases on a regular basis to ensure they are not compromised. See Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on best practice for managing your PKI.

The steps required to change the passphrase on a PSE file differ depending on whether the PSE file is split. See *Changing a passphrase on a PSE or PKCS#12 file* on page 37 and *Changing a passphrase on a split PSE file* on page 37 for more information.

Changing a passphrase on a PSE or PKCS#12 file

To change the PSE or PKCS#12 passphrase, follow these steps:

1. Right-click the name of the PSE or PKCS#12 file and select **Change Passphrase**. You are warned that changing the passphrase requires that your PKI device be closed.
2. Click **Yes** to continue and close the device, or click **No** to quit. If you click **Yes**, a dialog is displayed that asks you to enter your new passphrase and confirm it.
3. Enter the new passphrase, confirm it, and click **OK**. Ensure the passphrase you choose has a mixture of ASCII characters (at least one capital, one numeric, one symbol) and is eight characters long, for example, `PassPhrase1!`

If you are changing the passphrase on an older version of a PSE file, you are asked if you want to upgrade it to the latest format. Click **Yes** to update it and **Yes** to save the changes.

4. Specify whether you are saving the PSE file with the new passphrase to file or token.

The file is closed in order for the changes to take effect and is no longer displayed on the Token Manager's screen. Open it using the new passphrase (see *Loading a file* on page 35).

Changing a passphrase on a split PSE file

To change the passphrase on a split PSE, follow these steps:

1. Right-click the name of the PSE file and select **Tools>PSE>Change Split PSE passphrase**.
2. Specify whether the PSE is stored on file or token.
3. Select the PSE part whose passphrase you are changing. You can change the passphrase on each part of a split PSE independently of the other parts.
4. Specify the current passphrase and click **OK**.
5. Enter the new passphrase, confirm it, and click **OK**.

The Token Manager confirms the passphrase has been changed successfully.

Splitting a PSE

The facility to split a PSE provides additional security for authorizing access to PSEs and the information contained on them. It requires

several users to provide their passphrases in order to open the PSE before access is permitted.

If splitting a PSE, we recommend you ensure that a majority of users are required to open the PSE. For example, if you are splitting a PSE into five pieces, we recommend that at least three of the five users are required to open the PSE before the PSE can be accessed.

While we recommend that you use an HSM to protect the PSE for the CA, CAO, and RA, consider splitting the PSE for other entities in your PKI. See Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on securing your UniCERT PKI. .

If you split the PSE for any of the UniCERT services, you cannot set the startup type for that service to automatic in the Service Manager. We strongly recommend that you set the startup type for all services to manual. See Chapter 4, *Using the UniCERT Service Manager*, for more details.

To split an existing PSE file, follow these steps:

1. Right-click the name of the PSE file and select **Split**. You are warned that splitting the PSE requires that your PKI device be closed.
2. Click **Yes** to continue and the Token Manager closes the device, or click **No** to quit. The Token Manager displays a dialog asking you to specify how you are splitting your PSE file, as shown in Figure 24.

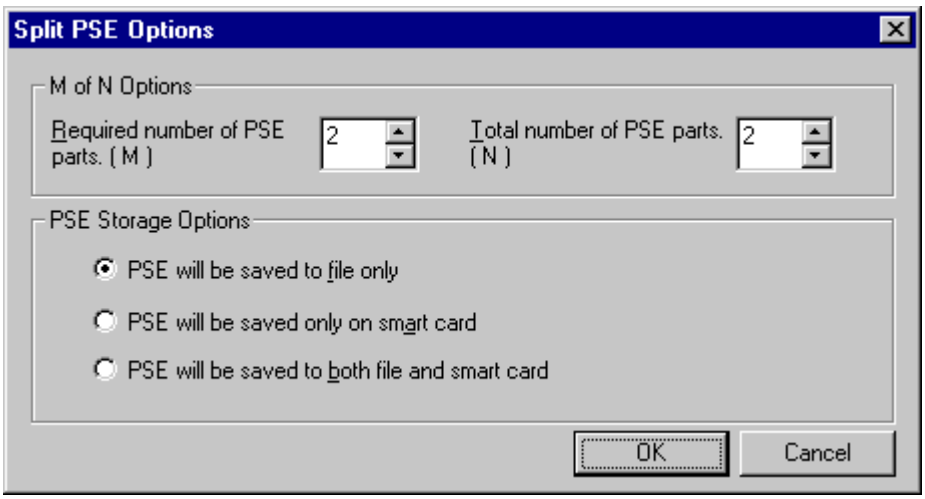


Figure 24: The Split PSE Options screen

3. Specify the required number of PSE parts that must be entered before the device can be accessed, the total number of parts the

PSE is split into, and where you are going to save the PSE file, on file, smart card, or both. Click **OK**.

4. Specify and confirm the passphrases for each PSE part.

Viewing the key properties

To view the key properties, right-click the PSE and select **Properties**. The PSE's key size, key type, and key identifier are displayed as shown in Figure 25.

Figure 25: Sample PSE's properties

Closing a PSE

Follow these steps to close a PSE:

1. Right-click the PSE you want to close and select **Close**. If you have an older version of a PSE, update it as prompted.
2. Select **Yes** if you have, for example, changed the PSE's passphrase and want to save the changes.

Using trust points

When validating a chain of certificates or a certificate path, each certificate is validated using a certificate further up the chain until you reach the top, that is, the trust point. A trust point is a certificate that you can use to validate the top of a certificate chain. A trust point can be a root or local CA certificate. In general, trust points are certificates with long validity periods and a low likelihood of being revoked. They are usually verified using some out-of-band means, for example, advertising a hash in a newspaper or on a Web site.

Trust points are only applicable to PSEs.

Trust points are listed in the Token Manager main screen for any PSE you have open. If no trust points are listed, you can add a trust point to the PSE.

To add a trust point to a PSE, follow these steps:

1. Right-click **Trust Points** and select **Add**.
2. Specify the location of the required certificate (`.crt`) file and click **Open**.
3. The Token Manager adds the certificate to the list of trust points.

Exporting keys

You can export your key pair as a PKCS#12 file as follows:

1. Right-click the friendly name of the key in the PSE or PKCS#12 and select **Export**.
2. Enter a passphrase for the new PKCS#12 and confirm it. Click **OK**.
3. Save the PKCS#12 file as prompted.

Store these PKCS#12 files securely, as they contain keys.

Loading a certificate

You load a certificate into a PSE or a PKCS#12 file as follows:

1. Right-click the friendly name of the key and select **Load Certificate**.
2. Select the certificate you are loading and click **Open**. The certificate is loaded onto the selected PSE or PKCS#12 file and associated with the selected key.

Exporting a certificate or certificate chain

You can export a certificate or certificate chain from a PSE or PKCS#12 file as follows:

1. Right-click the certificate you wish to export and select **Export> Certificate** or **Export>Certificate Chain**.
2. Save the certificate/certificate chain by clicking **Save** in the dialog.

Exiting the Token Manager

We recommend that you do not install the Token Manager on a computer that is accessible to other users and that you do not leave it running. Before you exit the Token Manager, save any changes you have made to PSE and PKCS#12 files, and close them.

To exit the Token Manager, select **File>Exit**.

Chapter 4

Using the UniCERT Service Manager

The UniCERT Service Manager allows you to install and run multiple UniCERT services on a single computer, making it easier for one administrator to manage the PKI. The Service Manager has a simple GUI where you add service instances and configure new service types.

The Service Manager supports the following UniCERT service types:

- The CA
- The RA
- The RA eXchange
- The Publisher
- The Publisher File Monitor
- The Key Archive Server (KAS)
- The Directory Content Checker
- The Directory Service Availability Monitor
- The Advanced Registration Module (ARM)
- The CMP Handler
- The SCEP Handler
- The email Handler
- The Certificate Status Server (CSS)

When you install a service, the Service Manager automatically adds it to the registry. You can also configure certain service properties, such as the startup mode.

Ensure that the Service Manager has been installed on the computers on which you want to run each of these services.

Starting the UniCERT Service Manager

Select **Start>Programs>Betrusted UniCERT v5.2.1>Service Manager** to start the Service Manager. The **UniCERT Service Manager** screen is displayed, as in Figure 26.

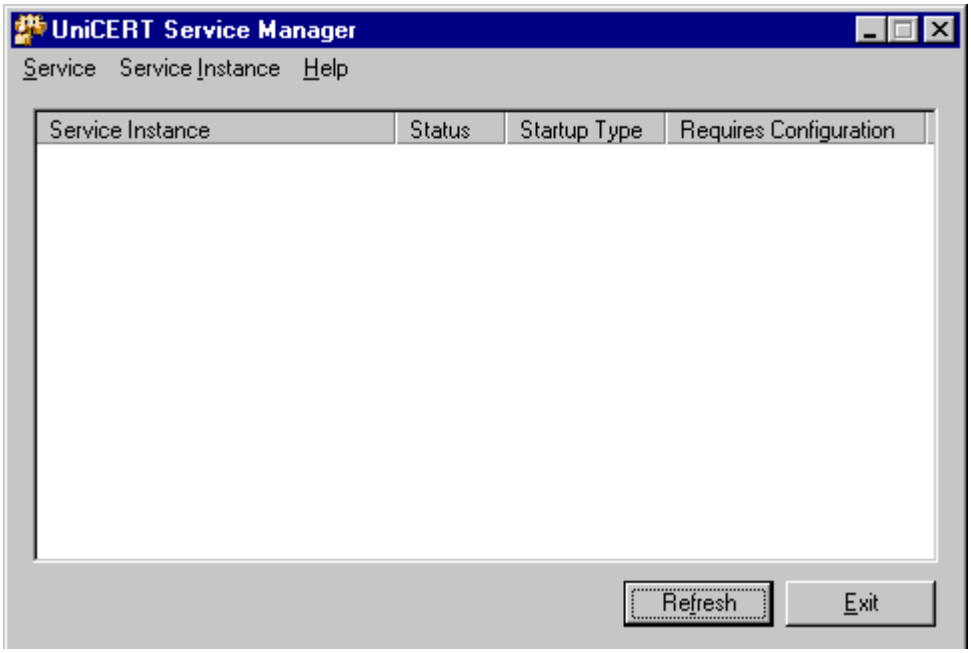


Figure 26: The UniCERT Service Manager startup screen

The startup screen displays the following columns:

- **Service Instance**: This column displays the name of the service, for example, CA, and the name you have given the service instance, for example, Acme CA.
- **Status**: This displays the current running status of the service, for example, **Running** or **Stopped**.
- **Startup Type**: This column shows the type of startup you have defined for this instance. Startup can be one of three modes:
  - Manual: You have to manually start the service any time you reboot the computer. Nonsensitive information, for example a username, is stored in the registry. Sensitive information, such as user passphrases for crypto profiles and database accounts, is not stored in the registry.

For added security in your PKI, we strongly recommend that you set the startup type for all services to manual. This ensures that the passphrases and PINs you use to access crypto profiles and databases are not stored on the computer where UniCERT components are running.

  - Automatic: The service starts automatically if you reboot the computer. All startup information is stored in the registry.

Sensitive information, such as passphrases for crypto profiles and database accounts, is stored in an encrypted form.

Services that start in automatic mode do not support split PSEs. If you want to use split PSEs, configure your services to start in manual mode. We strongly recommend that you do not set the startup type for services to automatic in a secure PKI setup. See Appendix A, *Using UniCERT in its evaluated configuration*, in the *UniCERT Core v5.2.1 Installation Guide* for more information on deploying UniCERT securely.

  - Disabled: Use this option if you want to temporarily disable a service for maintenance or upgrade work.

- **Requires Configuration**: This flag tells you if the service requires configuration. If the startup type is set to manual, as is recommended in security enforcing deployments of UniCERT, this option is always enabled. If the startup type is set to automatic, you only need to configure the service the first time you start it. Subsequent starts do not require configuration.

You can configure a service at a later date either by selecting **Reconfigure** from the **Service Instance** menu or by right-clicking the service name and selecting **Reconfigure**. You can only reconfigure instances that are stopped.

The Service Manager instance list on the main screen is empty until you add a new service instance and define its startup type. For instructions on how to do this, see *Adding a new service instance*.

Adding a new service instance

To add a new service instance, follow these steps:

1. Select the **Service>New Instance** option. The Service Manager displays the **Choose a Service Type** dialog showing a list of the services installed on your computer.
2. Select the service type you wish to add and click **Next**.
3. In the **Choose the Service Name** dialog, enter a friendly name for the new instance, for example, Acme CA. You can call the service instance anything you like, as long as it is unique for each instance and it is not longer than 200 characters. Click **Next**.
4. Select the startup type for the instance from the drop-down box. Choose between manual, automatic, or disabled. For an

explanation of the different startup types, see *Starting the UniCERT Service Manager* on page 42.

We strongly recommend you choose manual startup type for services in your UniCERT PKI. This ensures that only authorized users can start services and that the passphrases and PINs used to restart services are not stored on the computer where UniCERT components are installed.

If you select automatic startup mode, you must configure the service and start it for the first time. After you have started the service once, subsequent starts are automatic.

5. Click **Next**. The Service Manager displays a screen showing the details you have entered so far.
6. Click **Create** to create the new service instance. The Service Manager displays details of the new service on the main UniCERT Service Manager screen, as in Figure 27.

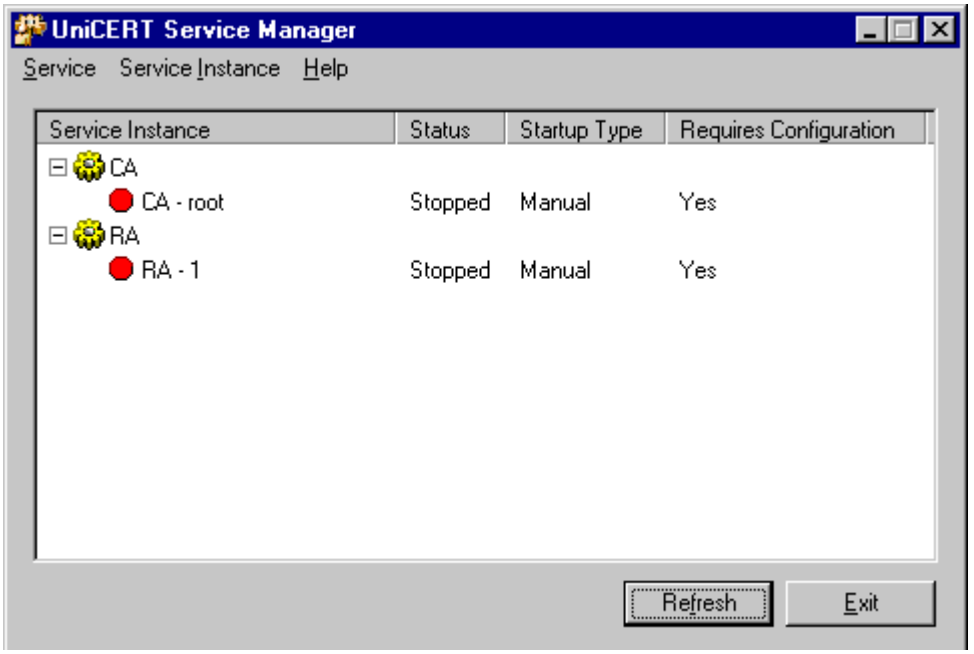


Figure 27: The main Service Manager screen

Click **Refresh** if the screen is not updated with the details of the services.

Starting a service

To start a service, follow these steps:

1. Right-click the service you are starting and select **Start** (or select **Service Instance>Start** from the menu). The Service Manager displays

a status indicator until the service has been successfully contacted.

2. The **Please Select a Crypto Profile** screen is displayed (see Figure 28). If you need to create a new crypto profile, click **New Crypto Profile** and follow the wizard. For more information, see *Working with crypto profiles* on page 30.

Figure 28: Selecting the crypto profile

If you have already created a crypto profile, right-click the required service and click **Next**.

3. Depending on the service you are starting, the Service Manager asks you to enter some or all of the following:
   - The passphrase for the crypto profile's PSE.
   - The details of the database to which you want to connect.
   - The directory to which you want to save policy templates.
   - The host name and port of a computer to which the service needs to connect.
   - The directory to which you want to save the request. This applies to the error requests and completed requests for the ARM.

Some of the UniCERT services use configuration (`.conf`) files during startup. Do not delete or rename the `.conf` files; otherwise, the service fails to start. Similarly, if you click **Cancel** while running the Service Manager, the Service Manager application freezes.

Enter these details on the subsequent screens that the Service Manager displays, clicking **Next** on each screen to continue.

4. The Service Manager displays a dialog confirming that the service initialization is complete and that the service has been started. Click **OK** to return to the Service Manager main screen.

You must start the CSS before you start the RA eXchange for the first time.

Running a service

You can stop, pause, and reconfigure a service using the Service Manager.

To perform any of these operations, do either of the following:

- Right-click the service name and select the operation you require.
- Select the **Service Instance** menu and choose the operation you require from the drop-down menu.

For example, you might want to stop a service in order to modify its properties; see *Modifying a service's properties*. To stop a service, either right-click the service name or select the **Service Instance** menu. Select **Stop** from the menu that appears. The service's status changes to stopped, and the Service Manager changes the icon next to the service name to indicate that it has stopped.

The **Pause** menu option only works for the UniCERT ARM, which is an advanced registration service.

Modifying a service's properties

You can modify the properties of a service instance after having configured it. If the service is running, using this option changes the logging level only. If the service is stopped, you can modify all of its properties, including its executable path.

To modify the properties of a service, either right-click the service and select **Properties** or highlight the service and select **Service Instance> Properties**. The Service Manager displays the **Properties** screen (see Figure 29).

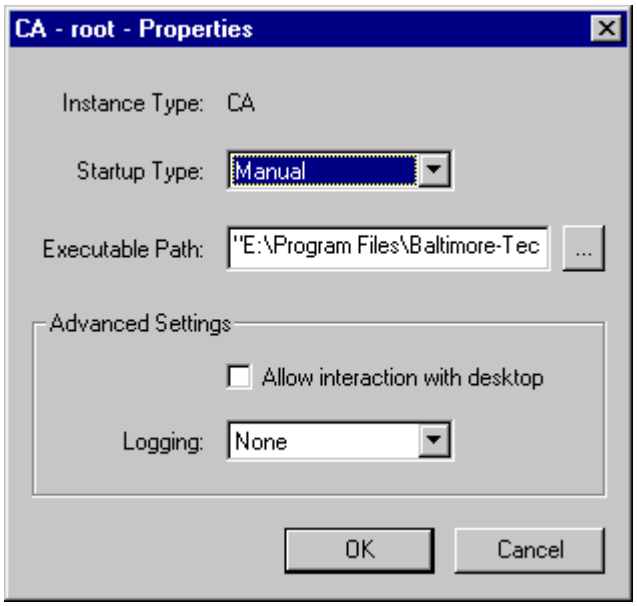


Figure 29: Modifying an instance's properties

We strongly recommend that you leave the startup type for all services as manual. In this way, you ensure that authorized administrators are present to enter passphrases or PINs if you need to reboot your PKI.

You can modify the following fields:

- **Startup type**: Select a different startup mode from the drop-down list. You can choose **Automatic**, **Manual**, or **Disabled**. For an explanation of the different startup types, see *Starting the UniCERT Service Manager* on page 42.
- **Executable path**: Enter the path to the service's executable, or click **Browse** to locate the service.
- **Allow interaction with desktop**: Enable this check box if your service requires interaction with the desktop for GUI purposes. This option is to facilitate ARM developers who have written plug-ins that contain dialogs.

We recommend that you do not create desktop dialogs for ARM services that are set to automatic startup, as you may not be present at the computer to respond to these dialogs.

- **Logging:** Use logging for troubleshooting purposes only. As logging uses valuable memory resources, we recommend that you set logging to none, unless instructed otherwise by Betrusted's Global Support Services.

Click **OK** to save the changes you made to the service's properties.

The service instance then starts automatically on system startup.

Changing the login details for an automatic service

Once you have configured a service to run in automatic mode, use the **Reconfigure** option if you need to change its login details. For example, if you have renewed the entity's certificate, it has a new PSE, and the automatic service's crypto profile provides details for the old PSE. Similarly, if you have changed the password for the service's database account, you also need to reconfigure its login details.

To change the login details:

1. Stop the automatic service if it is running.
2. Right-click the service and select **Reconfigure**, or highlight the service and select **Service Instance>Reconfigure**. The Service Manager prompts you to confirm that you want to reconfigure the service.
3. Click **Yes**. The Service Manager changes the instance's **Requires Configuration** setting to **Yes**.
4. Restart the instance and specify the new login details as prompted by the Service Manager. The Service Manager stores the new information, starts the service, and changes its **Requires Configuration** setting back to **No**.

Removing a service

You may want to remove a service from the Service Manager if you are replacing an old instance of a service with a new one or are deleting a service in its entirety from the Service Manager. To remove a service from the Service Manager, follow these steps:

1. If the service you are deleting is running, stop it by selecting **Service Instance>Stop** or by right-clicking the service and selecting **Stop**.
2. To remove the service, select **Service Instance>Delete** or right-click the service name and select **Delete** from the right-click menu. A dialog asks you to confirm your deletion.
3. Click **Yes** to delete the service.

The service is removed from the Service Manager.

Exiting the Service Manager

Click **Exit** at the bottom of the main screen to close the Service Manager.

Chapter 5

Generating keys on different computers

Most UniCERT components require that keys and certificates be generated before they can start or run. The UniCERT Key Generator is a utility that allows you to generate an entity's keys on a different computer to the Windows computer where the CAO is installed. Do this if you want to run one of the services on a different computer to where the CAO resides.

To use the Key Generator, you must first create and save a key generation file (`.kgf`) in the CAO for the entity you wish to register. You then use the Key Generator to update this file on the entity's computer.

Generating an entity's keys on another computer

You generate an entity's keys as part of its registration process:

1. Open your PKI in the CAO.
2. Register an entity by right-clicking the RP you want to use in the **Policy** tab of the **Policy Authorization** window and selecting **Register Entity**.
3. Follow the wizard, which guides you through the process of registering your entity (see the *UniCERT v5.2.1 Configuration Guide* for more information).

During the process, the CAO displays a dialog similar to Figure 30.

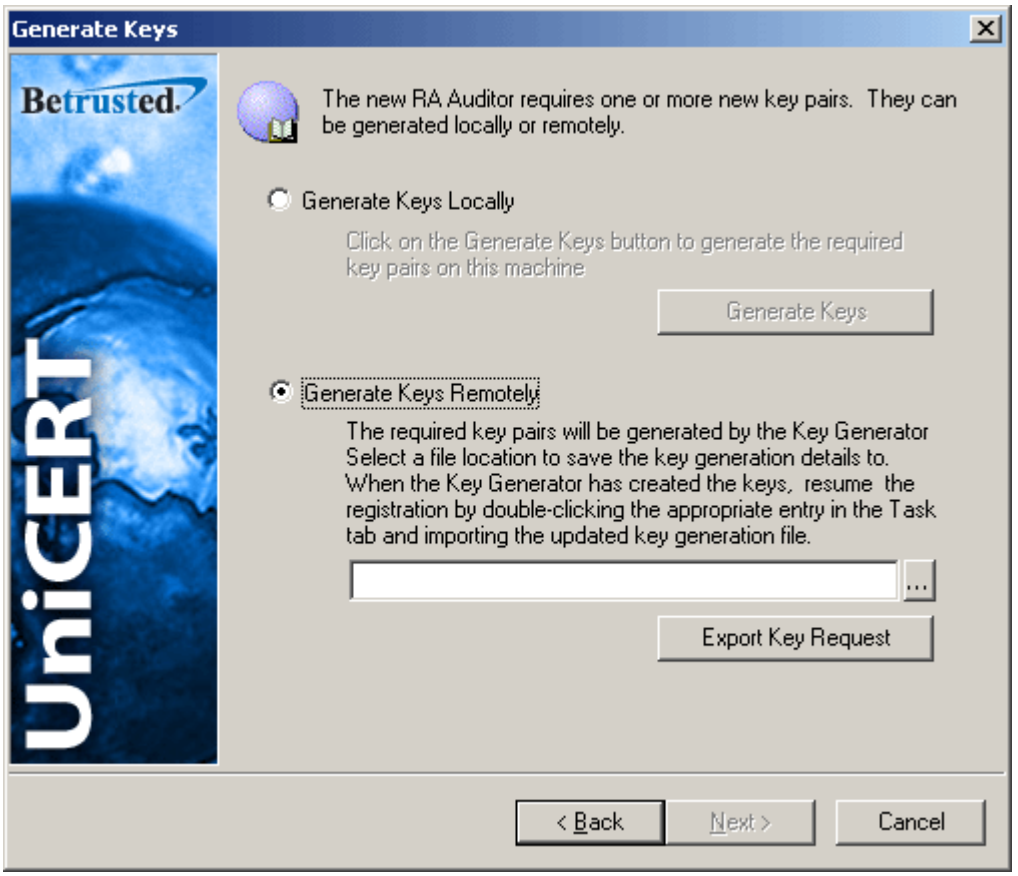


Figure 30: Choosing to generate your keys on another computer

To generate the entity's keys on another computer, follow these steps:

1. Check **Generate Keys Remotely**.
2. Browse or enter the path to the location where you want to save your key generation file (`.kgf`). Click **Export Key Request** to create the key generation file and then click **Next**.
3. Click **Resume Later**. Your progress at the CAO is saved, and the request appears on the **Tasks** tab of the **Explorer** window. You can return to where you left off once you have generated your keys in the Key Generator on the remote computer.
4. Transfer the file to the remote computer on a floppy disk or a token. Ensure you keep the token secure when you are moving between computers and always remember to remove it from the remote computer after key generation.

You now need to open the Key Generator on the remote computer to generate the entity's keys (see *Using the Key Generator* on page 51).

Using the Key Generator

To generate your entity's keys, follow these steps:

1. On the remote computer, select **Start>Programs>Betrusted UniCERT v5.2.1>Key Generator** to open the Key Generator.
2. Browse to the location of the key generation file and click **Proceed.** The Key Generator generates the keys and updates the file.
3. Save your PSE file as prompted. You can choose to split the PSE into multiple components. You can also save the PSE to file or token. If you split the PSE, you can save the different PSE components to both file and token. Click **OK**.

We recommend that you save the PSE files for sensitive entities, such as the CA, the RA, and the KAS, on HSM tokens or smart cards. HSMs provide increased security against physical tampering as well as hardware secured backup options.

4. Enter and confirm the passphrase(s) for the PSE file(s). The Key Generator displays a dialog confirming that the entity's keys have been generated.
5. Click **OK**. The Key Generator confirms the key generation process is complete.
6. Click **OK**.
7. Return with the `.kgf` file to the CAO computer.

Resuming the entity's key generation at the CAO

Start up the CAO and load the entity's updated key generation file back onto the CAO computer, as follows:

1. In the CAO, select **File>Open** to open the key generation file and click **Next**. Alternatively, you can double-click the request on the **Tasks** tab of the CAO's **Explorer** window. The CAO displays the **Resume Entity Creation Process** screen (Figure 31).
2. Browse to the location of the key generation file and click **Next**.

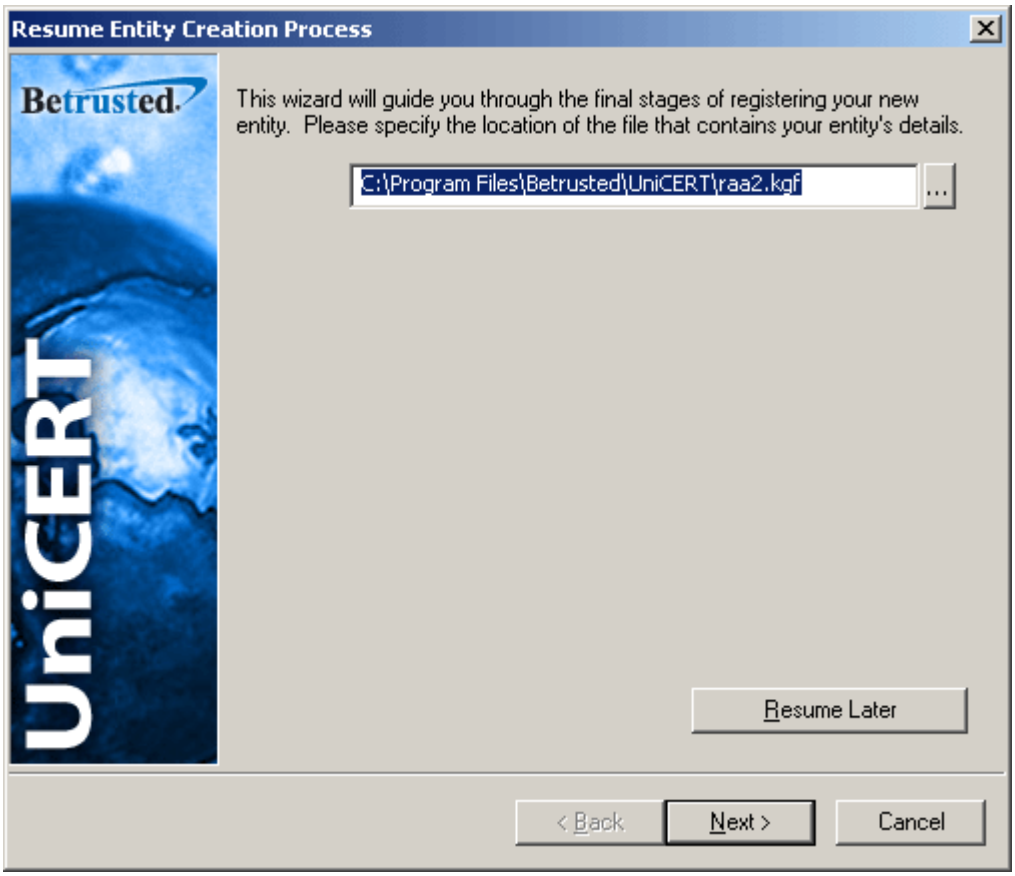


Figure 31: Resuming the entity's registration

3. Click **Submit Request** to send the request to the CA to be processed. When the CA issues the entity's certificate, the CAO displays the screen in Figure 32.
4. Leave the default options selected, click **Complete Registration**, and click **Next**.

Figure 32: Completing the registration process

The CAO displays a request summary, similar to that in Figure 33. It provides you with options to do the following:

- Update and save the PSE, PKCS#12, or key generation file.
- Export certificates.
- Add the entity to the PKI.
- View the registration details.

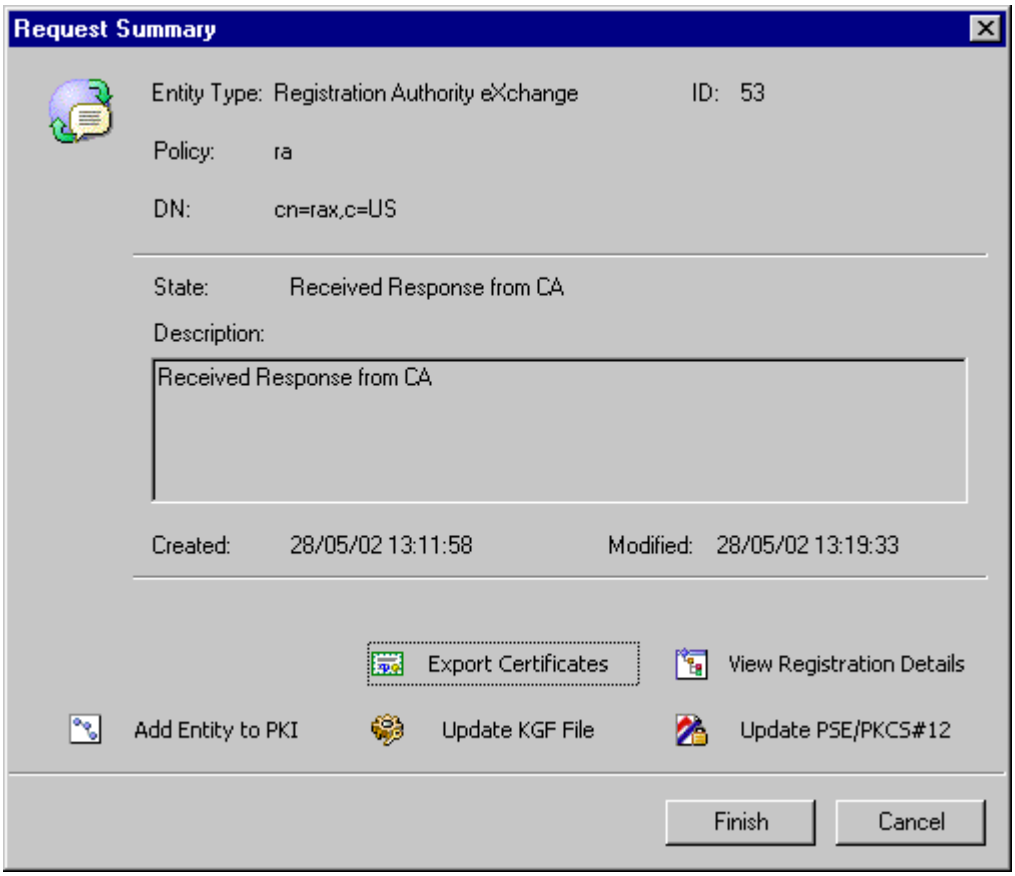


Figure 33: The Request Summary screen

5. Click **Finish** to complete the entity's registration.
6. Transfer the `.kgf` file back to the remote computer. See *Completing the key generation on the remote computer*.

Completing the key generation on the remote computer

To complete your entity's key generation, follow these steps:

1. Select **Start>Programs>Betrusted UniCERT v5.2.1>Key Generator** to open the Key Generator.
2. Browse to the location of the updated key generation file and click **Proceed.** The Key Generator updates the file.
3. Specify the location of your PSE file as prompted.
4. Select the PSE file you created in *Generating an entity's keys on another computer* on page 49.
5. Enter the passphrase for the PSE file.
6. Specify the PSE storage options and click **OK**. The Key Generator confirms the key generation process is complete.

Chapter 6

Using the RA Event Viewer

UniCERT records auditable events in an events log on the RA database. Each system or operator action is associated with the identity of the entity that caused the event and the time that the event occurred. This means that users responsible for auditing your PKI, such as the RA Auditor user, can trace all events and report problems as soon as they occur.

The RA Event Viewer is a Windows only application, and a CAO user, an RA Auditor, or an RA user can use it to administer the audit events in the RA database. The choice of which user to use depends in part on the geographic distribution of your PKI, the complexity of your PKI, and the operating systems that you use. For example, if you are running the RA on Solaris with the RA's keys on hardware, that RA user cannot be used to run the RA Event Viewer (without making the hardware token available on the Windows computer).

Likewise, it may not be feasible to use the CAO to administer the audit events in the RA database. This chapter discusses how you use the RA Event Viewer to view error, alert, warning, and information event logs and to create your own log queries.

For information on monitoring events and setting up the RA Auditor, see Chapter 9, *Configuring an RA Auditor entity*, and Chapter 25, *Monitoring events*, in the *UniCERT v5.2.1 Configuration Guide*.

Opening the RA Event Viewer

To open the RA Event Viewer, follow these steps:

1. Select **Start>Programs>Betrusted UniCERT v5.2.1>RA Event Viewer**. The **User Profile Logon** screen shown in Figure 34 appears, prompting you to specify your user profile details.

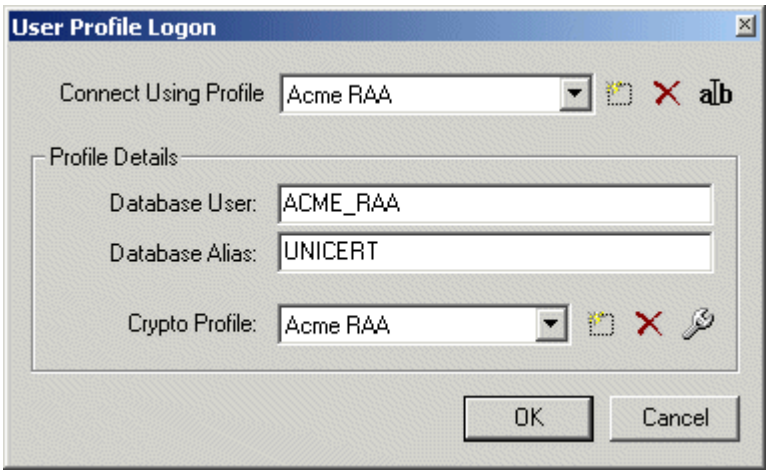


Figure 34: User Profile Logon

A user profile specifies your RA database account details and its crypto profile. For more information on user profiles, see the *UniCERT v5.2.1 Configuration Guide*. For details on switching user profiles and on the use of the icons on this screen, see *Modifying options on the user profiles dialog* on page 63.

2. The first time you run the RA Event Viewer, create a new user profile by specifying your RA database account details and the associated cryptographic profile for the user profile you are creating. Enter these details and click **OK**.

Once you have created a user profile, the RA Event Viewer remembers this information. When you next run the viewer, the additional details are automatically filled in. You can create several user profiles and switch between them without shutting down and restarting the RA Event Viewer.

---

3. Enter the passphrase for your RA's PSE as shown in Figure 35.

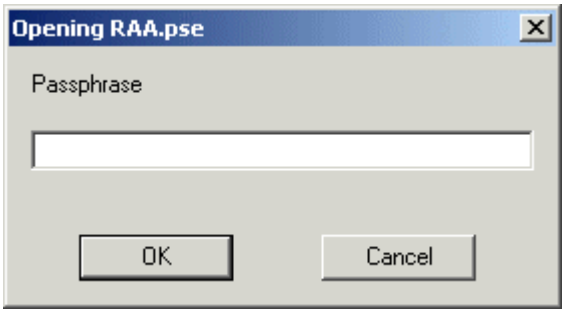


Figure 35: Open the RA's PSE

4. Enter your RA's database passphrase as shown in Figure 36 and click **OK**.

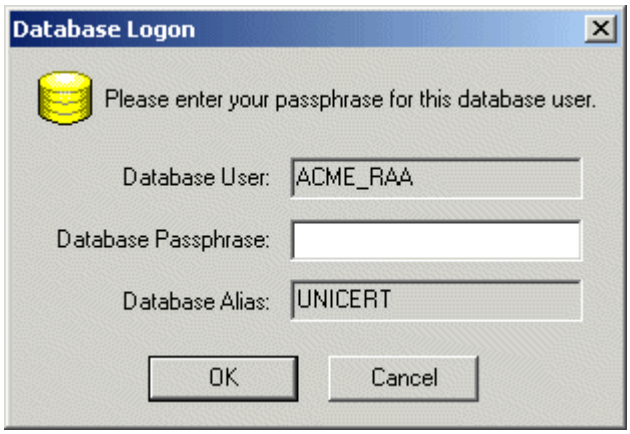


Figure 36: Database logon details

The RA Event Viewer main screen is displayed, as shown in Figure 37.

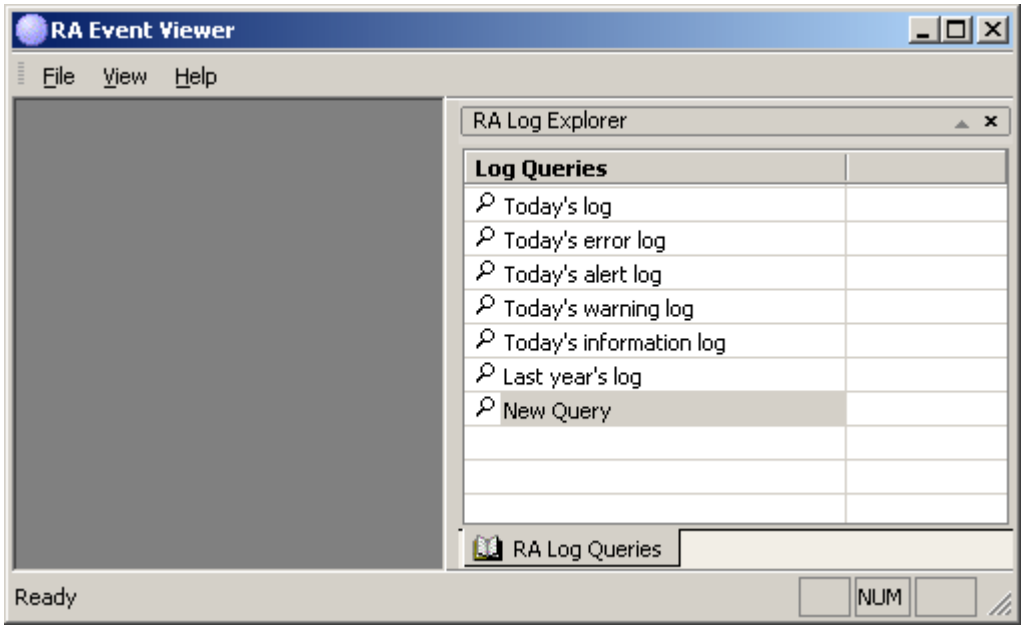


Figure 37: The RA Event Viewer main screen

Accessing the RA Event Viewer logs

Use the RA Event Viewer to monitor events using the default log queries. You can also create your own log queries. The latter is a more powerful option, as you can execute specific queries to locate particular events, for example, based on correct event codes or severity warnings.

Viewing the default log files

There are six default queries provided with the RA Event Viewer as shown in the **Log Queries** window in Figure 37. To examine the log, double-click the query you want to view.

Creating your own log query

You can construct queries to locate events with specific characteristics, for example, searching for events that occurred before a particular time today or events that occurred at a specific level of severity.

You specify dates and times in local time; however, the RA Event Viewer converts them to, and displays them in, Coordinated Universal Time (UTC).

To create log queries, follow these steps:

1. Right-click in the **RA Log Queries** window and select **Create New Query**. A new query appears on the tab.

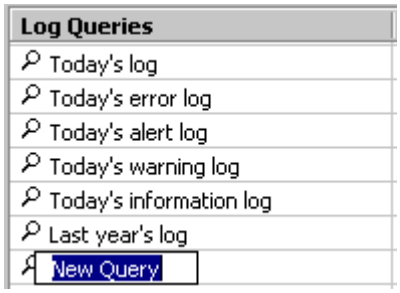


Figure 38: Creating a new query

2. Enter a name for the query, for example, `Last week's information log`.
3. Right-click it and select **Properties**. The screen shown in Figure 39 appears.

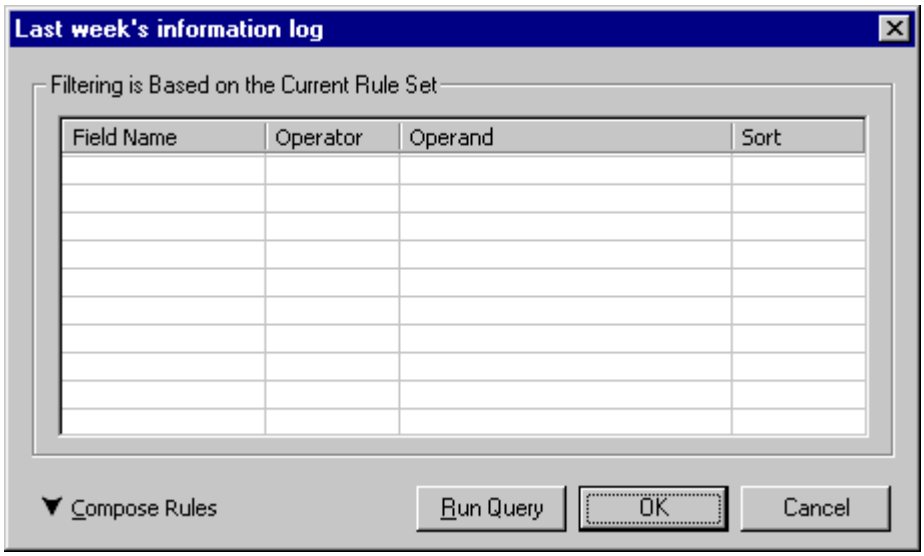


Figure 39: Viewing a log query's properties

4. Click **Compose Rules**. The **Rule Composer** appears, as shown in Figure 40.

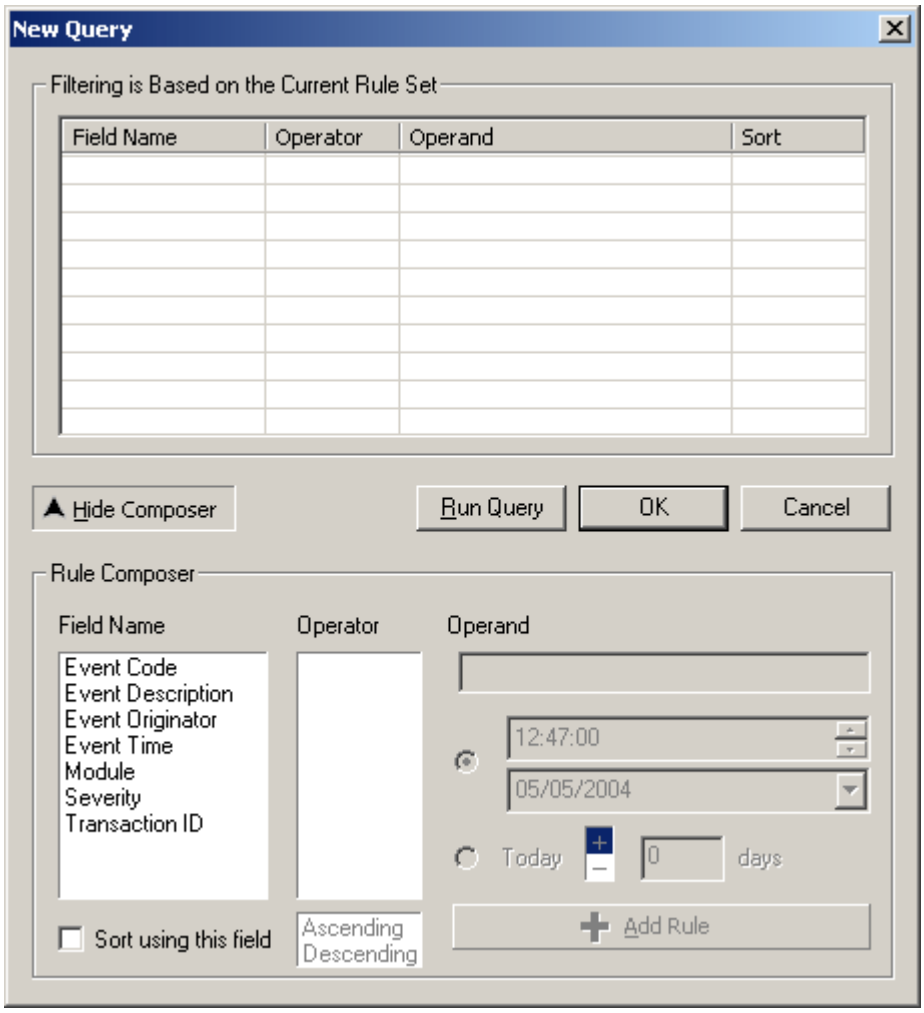


Figure 40: Composing a query

5. Select the field you want to search on from the **Field Name** box. The possible operators for the field appear in the **Operator** box. These may be any of the following:
   - **=**: Searches for field values equal to the operand.
   - **<**: Searches for field values less than the operand.
   - **>**: Searches for field values greater than the operand.
   - **<=**: Searches for field values less than or equal to the operand.
   - **>=**: Searches for field values greater than or equal to the operand.
   - **!=**: Searches for field values not equal to the operand.
   - **Contains**: Searches for field values matching the operand.
6. Select an operator and define your operand. If you are searching for an event date, use the time and date fields to define the date. You can also select **Today** to search for events that occurred within a time period entered in days before or after the day you are

searching on. For example, Figure 41 shows a rule defined to search for events that occurred before today.

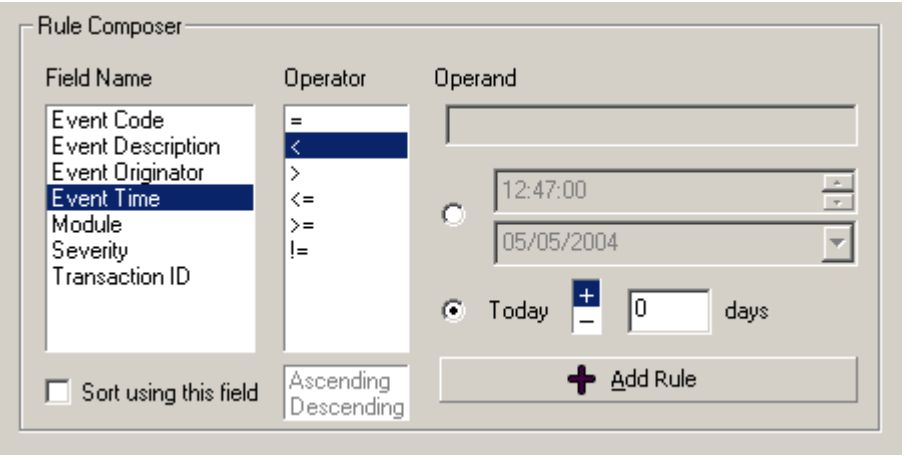


Figure 41: An example of a rule

7. Select **Sort using this field** if you want to sort your queries according to the field you are searching on, and select **Ascending** or **Descending** as the sort order. You can only apply this option to one rule in your query.

Sorting on fields that are not indexed can cause queries to take a considerable amount of time. Contact your database administrator if some queries are too slow.

8. Click **Add Rule**. The rule appears with its details on the filtering section.

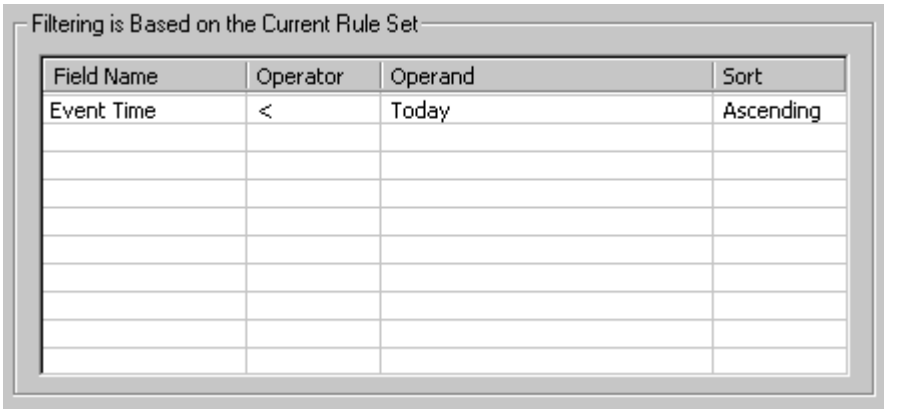
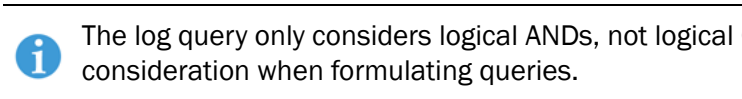


Figure 42: Rule filters

9. Add any additional rules you require for your query. For example, to limit the events to those that occurred in the last week, add the rule **Event Time >= Today - 7**. To find informational events, which have a severity of five, add the rule **Severity = 5** by

setting `Severity = Information` in the **Rule Composer**. Figure 43 shows these rules added to the filtering section.



The log query only considers logical ANDs, not logical ORs. Take this into consideration when formulating queries.

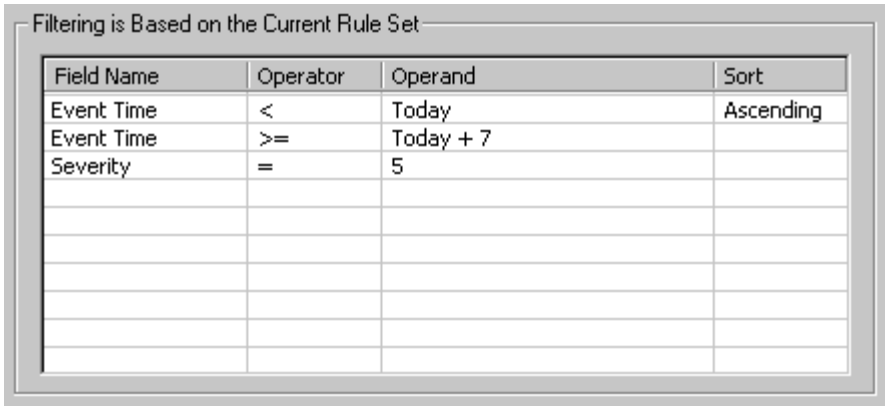


Figure 43: Rules to find informational events in the last week

10. Delete any rules you do not want by right-clicking them and selecting **Delete Rule**.
11. Click **Run Query** once you are happy with the rules you have defined. The query returns a result listing the certificates that match the query and their details (see Figure 44).

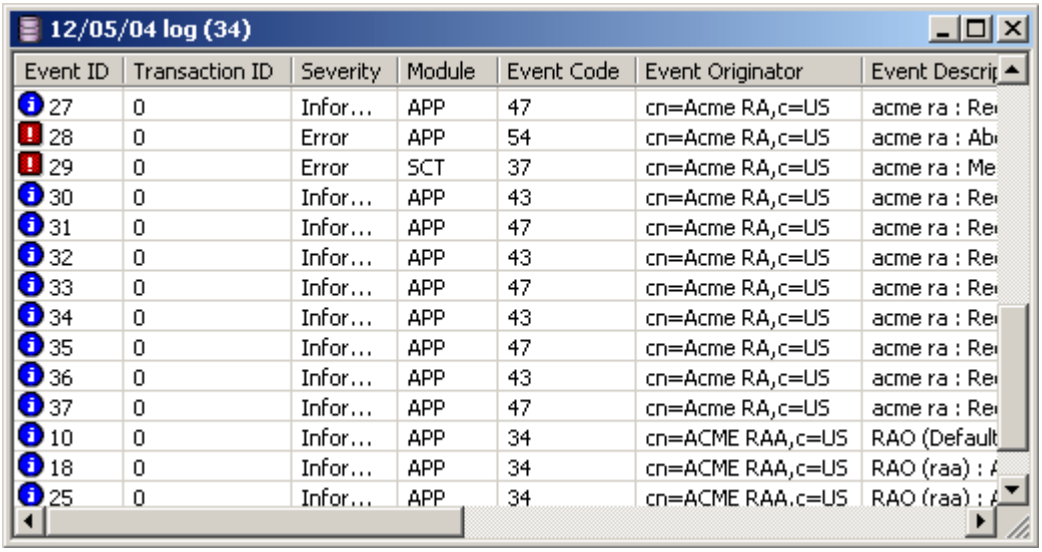


Figure 44: The query result

The event values returned in the **Severity** and **Module** columns in the log are described in the following tables. You use the event values for **Severity** and **Module** to compose your rules. Once you have added the rules, the event values are translated into their numeric

values in the rule filter. Table 2 displays the **Severity** values and their event meanings.

Table 2: Severity values and event definitions

Event values	Numeric values	Event definition
Alert	1	An event alert
Audit	2	Reserved for internal use
Error	3	An error
Warning	4	A warning
Information	5	An informational event

Table 3 displays the **Module** values and the types of events they represent.

Table 3: Module values and event definitions

Event values	Numeric values	Event definitions
APP	1	A generic event occurring from the application
AUTH	2	Reserved for internal use
COMM	3	An event occurring from a communication mechanism or port
DATA	4	Events from configuration files, input/output files, or data fields
DATABASE	5	A database event
HARDWARE	6	An event from a hardware device
POLICY	7	An event occurring from an RP
SECURITY	8	A security event, most of which are audited to the system event log
REQUEST	9	A certificate request event

Saving a log query to file

You can save the results of a log query as a tab delimited text file, which you can import into an application, such as Microsoft Excel, and then sort or search as you require. To save the results of a log query, select **File>Save As**, select a location and specify a name for the file.

Modifying options on the user profiles dialog

You can switch between user profiles (see *Switching the user profile*) and you can also modify the current user profile (see *Modifying the current user profile*).

Switching the user profile

To change the user profile you are using, follow these steps:

1. Select **File>Close Session**.
2. Select **File>Logon to Database** and select the user profile you want to open and click **OK**.
3. Enter the PSE passphrase and click **OK**.
4. Enter the passphrase for your database account and click **OK**.

Modifying the current user profile

You can modify the current user profile by using the buttons on the user profile screen as follows:

- Create a new profile.
- Delete an existing profile.
- Rename an existing profile.
- Create a new crypto profile.

Table 4 displays the meaning of these button icons.

Table 4: Explanation of button icons

Icon	Function
	New
	Delete
	Rename
	Configure

Archiving audit logs

Archiving audit logs is an important function in maintaining the security and integrity of your PKI. You can prevent the exhaustion of audit data storage space by regularly archiving your audit logs. Additionally, it means you have a backup of your audit logs should you require the information contained in them (see *Checking the integrity of the audit logs* on page 66).

To have your application archive audit logs, you must give it permission to do so. For information on how to set up the RA Auditor

to archive audit logs, see the Chapter 9, *Configuring an RA Auditor entity*, in the *UniCERT v5.2.1 Configuration Guide*.

To archive audit logs, follow these steps:

1. Select the **RA Logs Query** tab in the RA Log Explorer window.
2. Select the required log query and open it.
3. Right-click any event in the log and select **Archive log** from the menu (see Figure 45). The **Archive** dialog is displayed.

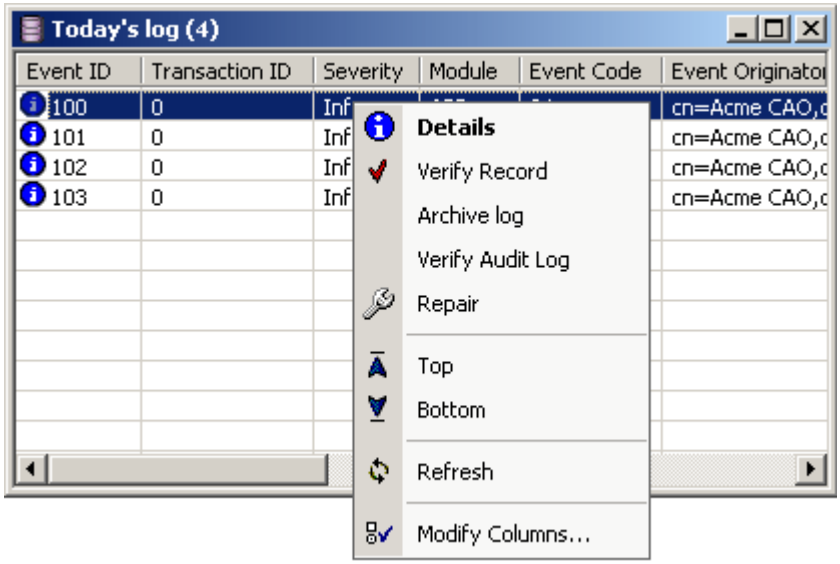


Figure 45: Log query view menu

4. From the **Archive** dialog's drop-down menu, set the date at which to stop archiving audit log entries (see Figure 46). All audit log entries on the RA database prior to this date are archived.

You can only archive audit log entries that are older than one week.

---

5. Specify the location where the archived audit log file is to be stored.

The information contained in an archived log file is sensitive. Therefore, store it securely, such as on a secure server or on a CD that you keep in a locked filing cabinet.

---

6. Click **OK**. The audit log, which is automatically named by the application, is archived to the specified location. The archived log is then removed from the database.

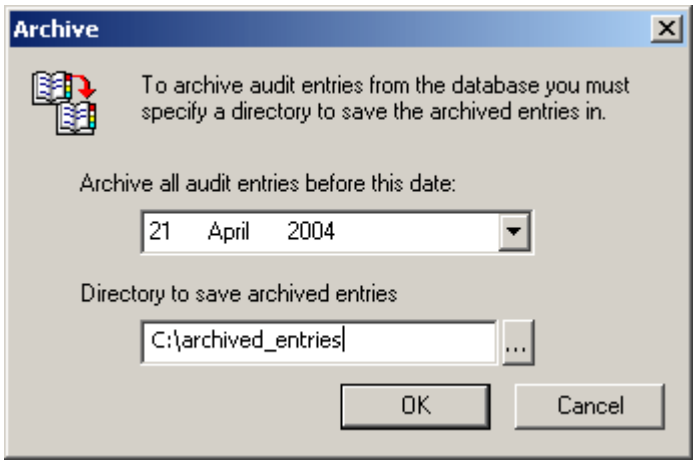


Figure 46: Archiving audit log entries

Archived logs are stored as XML files of approximately 100 MB in size, containing 10,000 entries. The use of XML files allows you some flexibility when you work on archived files, as you can import them into other applications, such as spreadsheet applications, to analyze the data.

Archived log files contain sensitive information. Therefore, if you or another authorized administrator are working on them, ensure that the log files are stored securely when you are finished.

The length of time you must retain records depends on the legal obligations and the document retention policy of your organization. If you are not familiar with them, locate this information.

If you are archiving audit logs in order to delete them, see *Deleting archived audit log files*.

Deleting archived audit log files

If you delete archived audit log files from your system, ensure you do so in a secure fashion. The audit logs contain sensitive information about end entities using your PKI; therefore, dispose of archived logs in a manner that does not compromise this information.

Do not delete your archived audit log files unless you are sure that you no longer require them.

After you have manually deleted the audit log files, we recommend the following to ensure that the logs are securely deleted from your system:

- Bypass the Windows Recycle bin when deleting files.
- After deletion, write over the file contents with zeros, for example, using a low-level disk defragmentation utility.
- Delete the Windows swap file contents.

For additional security, make an independent assessment of the commercially available system utilities that provide secure file deletion.

Checking the integrity of the audit logs

UniCERT protects audit event logs using cryptographic functions. The entity logging the audit event signs the event log when it creates it. You can detect any subsequent modifications to the audit logs by verifying the signature on an entry or by checking if an entry has been deleted.

Administrators with an auditing role in your PKI, for example, the CAO, the RA Auditor, or the KAO, are responsible for periodically running the deletion detection process and checking the audit logs for entries that do not verify. If you detect any problems during a routine check of the logs, flag the log, investigate the issue, and report the problem to your system administrator.

Back up your databases on a daily basis. They are an important resource for verifying logs and checking for deleted entries during routine audits of the event logs.

Verifying the validity of events

To verify whether an event in the event log is valid, right-click it and select **Verify Record**. The RA Event Viewer verifies the certificate chain of the event signer back to a trusted root, where the trusted root is an entity in your PKI. It also checks whether the signer had been revoked at the time it signed the event. Provided the certificate chain verifies and the signer was not revoked, the event is valid. If the signing PKI entity is revoked after the event, the entry in the event log still passes validation.

Verifying the validity of audit logs

To verify whether the audit log is valid, right-click an entry in the audit log and select **Verify Audit Log**. On the dialog that is displayed, you can check the audit log for one of the following:

- **Deletion detection only**: The RA Event Viewer runs the deletion detection process, checks to see if events have been deleted from the audit log, and reports any errors found.
- **Deletion and verification of all audit entries**: The RA Event Viewer runs the deletion detection process and verifies the signature on each event in the audit log, reporting any errors found. This option may take a significant amount of time. The application warns you that you cannot use UniCERT while this operation is in progress.

Repairing the audit log

You can repair the audit event log if any deletions (due to unauthorized modifications or tampering) are found in the event log table. By repairing the log, any deleted events that are detected are replaced with a substitute event.

Entries with invalid signatures are not repaired. Only deleted entries are repaired by returning the deletion detection information to a valid state.

To repair an audit event log, follow these steps:

1. Open the event log and right-click any of the entries.
2. Select **Repair** from the menu.

A dialog informs you of the successful repair of the log. Click **OK**.

Index

E

F

G

H

I

K

L

M

O

P

Q

R

S

T

U

V