Contents

About the Keon Management Console

The Keon Management Console is a standalone Java application that you use to manage your Keon Security Server database.

Each Manager in the Keon Management Console contains menus and a Toolbar, a selection table, a Search Space, and a Workspace. The selection table is located on the left-hand side of the screen, the Search Space is located above the selection table, and the Workspace is located on the lower right-hand side of the screen.

Related Topics

"How to Use the Menus" on page 6

"How to Use the Toolbar" on page 7

"How to Use the Workspace" on page 8

"How to Search for Database Records" on page 9

"How to Select Database Records" on page 11

How to Use the Menus

- Use the File menu to add, save, and delete records, import users, import and export certificates, define labels for custom data fields, and exit.
- Use the Edit menu to clear or reset the selection table, or select all records in the selection table.

  Note: Click **Clear** to clear one or more selected rows from the selection table. Clearing rows does **not** remove records from the database. To remove selected records from the database, click **Delete**. Click **Reset** to restore records to their "last-saved" state.

- Use the View menu to switch between Managers.
- Use the Help menu to access online Help.

For explanations of the Toolbar actions, click **About the Toolbar**.

Accelerator keys (for example, CTRL+N) are listed beside some menu items.

How to Use the Toolbar

The Toolbar buttons are shortcuts to frequently used menu actions.

- Click **New** to add a record to the database.
- Click **Save** to save changes to the currently selected records in the current Manager.
- Click **Save All** to save changes to all the records you have modified.
- Click **Reset** to restore selected records to their "last-saved" state.
- Click **Hints** to display helpful troubleshooting information and view error messages.
- Click **Delete** to remove selected records from the database.
- Click **Select All** to select all the records in the selection table.
- Click **Clear** to clear selected rows from the selection table.

Important: The Management Console caches your work until you save it. Changes you make to a record are not written to the database until you click **Save** or **Save All**.

The status of your network connection is displayed on the far right-hand side of the Toolbar.

- **Connected** means the Management Console is connected to the database but no data is being transmitted.
- **Communicating** means data is being saved to or loaded from the database.
- **Disconnected** means the Management Console has lost the database connection because of a network failure or Keon service failure.

How to Use the Workspace

Each Manager has its own Workspace. When you select a record in the selection table, the record's data displays in the Workspace. You can edit the text in any white text box, but you cannot edit gray boxes. Pink boxes indicate required data or invalid data.

The User and Group Manager Workspaces have tabs across the top. Click these tabs to display cross-Manager property sheets. For example, you can view or edit a user's Agent, group, and credentials assignments by clicking **Assignments** in the User Manager Workspace.

Note: Some actions open a secondary dialog box for you to enter or view data.

How to Search for Database Records

Use the Search space to produce a working list of database records in the selection table.

To maximize efficiency, searches are background processes. If you are performing a lengthy search on a very large database, you can perform other Management Console tasks while the search continues. However, if your database is large, Security Dynamics recommends that you limit your searches.

You select a primary search criterion from the drop-down list (for example, **By User ID**), and type a unique secondary criterion string in the text box.

(In the Credential Manager, you can also select a secondary criterion from a drop-down list, and then type a unique tertiary criterion in the text box.)

You can also search by range. You enter the range (for example, **a** to **f**) in the Search space and the records that fall in this range are sorted and displayed in the selection table.

Note: Digits are sorted as text, not as numbers. For example, if you search for the range **jsmith1** to **jsmith3**, records containing **1** are displayed first, followed by records with **2**, and so on. The results of such a search are displayed in the following order: **jsmith1**, **jsmith10**, **jsmith111**, **jsmith2**, **jsmith21**, **jsmith3**.

If you click **Replace**, the current selection table rows are cleared before the search results display.

If you click **Append**, the search results are added to the current selection table contents.

In addition, you can use an asterisk (*) to perform a wildcard search on most objects.

Note: In the Report Manager, you cannot use a combination of the asterisk and a string. For example, to include only those users whose last names are in the **A** to **F** range, type **A** in the **From** box and **F** in the **To** box. (Do ***not*** type **A*** or **F***.)

The following procedure describes how to perform a typical search in the User Manager.

To search for all users whose name begins with “j”:

1. In the User Manager, select **By User ID** from the primary criterion drop-down list.
2. Type **j*** in the secondary criterion box.
   - If you click **Replace** (the default), the current selection table rows are cleared before the new search results display.
   - If you click **Append**, the search results are added to the selection table.
3. Click **Search**.

How to Select Database Records

The selection table displays the current working list of records. Pink boxes indicate required data or invalid data.

You construct the working list in the Search space. See How to Search for Database Records.

- To select a record, highlight a row in the selection table.
- To select multiple records, hold down the SHIFT key or the CTRL key, and then highlight the rows you want to select.
- To select all rows in the selection table, click **Select All** on the Toolbar or on the Edit menu, or press CTRL+A.

When you create a database record, an empty row is added to the selection table.

How to Search the Online Help

To search the Management Console online Help, open the Help viewer, click the magnifying glass icon, enter your query in the **Find** box, and press ENTER. The names of Help topics that match your query are displayed in the left pane of the Help viewer.

The search engine uses a technique called “relaxation ranking” to identify and score specific passages of text that are most likely to answer your query.

The red circles in the first column indicate the ranking of the matches for that topic. A filled-in circle indicates a strong match; an empty circle indicates a weak match.

The number in the second column indicates the number of times the query was matched in the listed topic.

1

User Manager

To be written.

How to Add a User

Use this procedure to create a user record and store it in the database.

Before you begin, you must know the user's first and last name, and User ID. You can also decide whether you want to define custom data fields. (See "How to Define Custom Data Fields" on page 15.)

If you are adding a user to represent an application (such as SAP), Security Dynamics recommends that you use the following naming convention for the User ID: **HOSTUSER_*hostname***. For example, **HOSTUSER_SAP**.

If you are adding multiple users with similar default values, consider creating a user record template and importing users. See "How to Make a User Record Template" on page 16 and "How to Import Users" on page 17.

To add a user:

1. In the User Manager, click **New**.
   The Workspace clears, and an empty row is added to the selection table.
2. Type the User ID, first name, and last name in the appropriate boxes.
3. Type additional information, as appropriate, in the labeled boxes.
4. If the user is a Keon administrator, click **Keon Administrator**.
5. If you want to secure the user's access to the system or assign a group to a user, complete one or more of the following procedures:
   How to Assign Smart Cards
   How to Assign Virtual Cards
   How to Assign Access Rights to a User
   How to Assign a Group to a User
6. Click **Save** to save the changes to the database.

Related Topics

"How to Edit a User" on page 39

"How to Delete a User" on page 40

How to Define Custom Data Fields

By default, the User Information panel in the User Manager contains boxes labeled **Label 1** to **Label 10**. You can define Custom Data field labels to further identify users. For example, **Label 1** can be **Phone Number** or **Social Security Number**.

In the Reports Manager, you can use information in the Custom Data fields to generate customized user reports. See "How to Generate a Custom Report" on page 101.

Note: To remove a Custom Data field from the display, edit the custom label to be an empty string.

To define Custom Data fields:

1. On the File menu in the User Manager, click **Customize**.
2. In the Custom Data Fields dialog box, type a label (1 to 31 characters) for each custom data field you want to define.
3. Click **OK**.

Related Topics

"How to Add a User" on page 14

"How to Edit a User" on page 39

How to Make a User Record Template

You can designate a user record as a template to provide default values for user information, including group and access rights assignments or administrator status. These default values are filled in for every user added after you specify the template, but you can override the default values. When you finish using a template, you can clear the template so that new records do not have default values, or you can specify another template with a different set of default values.

The user record template is defined only for the current session.

To create a user record template:

1. In the User Manager, select a user record that has the default values you want to use for all user records, or create one to your specifications.
2. With the record you want to use as a template selected, click **Use as Template** on the Edit menu.

   All new user records that you add will have the default values in this template.

Note: To clear a template, click **Clear Template** on the Edit menu. The user record is no longer designated as a template, but is not deleted from the database.

Related Topics

"How to Import Users" on page 17

"How to Add a User" on page 14

How to Import Users

You can create a file containing User IDs, first names, and last names, and import this file to the selection table in the User Manager. If you also make a user record template, you can set up multiple users with the same custom data fields, groups, and access rights.

Before you begin, you must

- Create a file of new users. See “How to Create a File of New Users” on page 18.
- Decide whether to make a user template. See “How to Make a User Record Template” on page 16.

To import users:

1. In the User Manager, on the File menu, click **Import**.
2. When prompted, locate the file of new users, and double-click the filename.

How to Create a File of New Users

A new users file contains User IDs, first names, and last names, separated by commas. You can use this file to import users to the selection table in the User Manager.

Use the following format:

```
jsmith,john,smith
rwhite,robert,white
```

To create a file of new users:

1. Using any text editor, create a text file containing User IDs, first names, and last names, separated by commas.
2. Save the file.

Related Topics

"How to Import Users" on page 17

"How to Make a User Record Template" on page 16

How to Assign Smart Cards

A Smart Card is a physical card with embedded memory that identifies and provides information about a user.

Before you begin to assign Smart Cards to users, you must select one or more users. (If you are adding a new user, the user is selected already.)

You can assign Smart Cards to users in the following ways:

- Assign Smart Cards Manually
- Assign Smart Cards with Serial Numbers Loaded from a File
- Assign Smart Cards with System-Generated Serial Numbers

Related Topic

"Smart Card Serial Number Entry Methods" on page 19

Smart Card Serial Number Entry Methods

Manual entry. You select users one at a time in the selection table and assign a serial number.

Read from file. You select a set of users and specify a file that lists the same users and associates each user with a serial number. After you click **Load**, the User Manager reads the entries in the file and assigns each serial number to the specified user.

System generation. You select a set of users, enter a starting serial number and click **Generate**. The User Manager assigns this number to the first user in the set and increments the serial number by one for each successive user in the list.

Related Topic

"How to Assign Smart Cards" on page 19

How to Assign Smart Cards Manually

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)

- Know whether the Smart Cards are v 4.x compatible.
- Decide whether to generate a Smart Card assignment report. See “How to Generate a Smart Card Assignment Report” on page 23.

To assign Smart Cards manually:

1. In the User Manager, click **Assignments** and **New Smart Cards** to open the New Smart Cards dialog box with the selected users listed in the selection table.
2. Select a user, and click **Manual Entry**.
3. In the **Identifier** box, type a serial number for the selected user.
4. If the Smart Cards are v 4.x compatible, check **v 4.x Compatible**.
5. Repeat steps 2 to 4 until all Smart Cards are assigned.
6. If you want to generate a Smart Card assignment report, check **Save Report to File**.
7. Click **OK**.
   If you checked **Save Report to File**, you can specify a folder and filename for the report.
8. Click **Save** or **Save All** to save the changes to the database.

Related Topic

“How to Assign Smart Cards” on page 19

How to Assign Smart Cards with Serial Numbers Loaded from a File

Before you begin, you must

- Create a file of Smart Card serial numbers. See How to Create a File of Smart Card Serial Numbers.
- Select one or more users. (If you are adding a new user, the user is selected already.)
- Know whether the Smart Cards are v 4.x compatible.
- Decide whether to generate a Smart Card assignment report. See “How to Generate a Smart Card Assignment Report” on page 23.

To assign Smart Cards with serial numbers loaded from a file:

1. In the User Manager, click **Assignments** and **New Smart Cards** to open the New Smart Cards dialog box with the selected users listed in the selection table.
2. Select all the users specified in your file.
3. Click **Read from File**.
4. Type the pathname and filename in the **File Name** box.
   OR
   Click **Browse** to locate the file, and then double-click the filename to enter it into the **File Name** box.
5. Click **Load** to copy the card assignments in the file to the User Manager.
   A serial number is assigned to each user specified in the file and displayed in the right-hand column next to or opposite the user's name.
6. If the Smart Cards are v 4.x compatible, check **v 4.x Compatible**.
7. If you want to generate a Smart Card assignment report, check **Save Report to File**.
8. Click **OK**.
   If you checked **Save Report to File**, select a folder and type a filename (or accept the default filename of **SmartCartAssigns.txt**).
9. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Smart Cards" on page 19

How to Create a File of Smart Card Serial Numbers

A Smart Card serial numbers file contains User IDs and associated serial numbers. You can use this file to assign Smart Cards to users.

Use the following format:

```
# This is a comment.
# userID = Serial Number
user01 = 8762345332
```

```
user02 = 1234567890
```

To create a file of Smart Card serial numbers:

1. Using any text editor, create a text file containing User IDs and serial numbers.
2. Save the file.

Related Topic

"How to Assign Smart Cards with Serial Numbers Loaded from a File" on page 20

How to Assign Smart Cards with System-Generated Serial Numbers

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)
- Know whether the Smart Cards are v 4.x compatible.
- Decide whether to generate a Smart Card assignment report. See "How to Generate a Smart Card Assignment Report" on page 23.

To assign Smart Cards with system-generated serial numbers:

1. In the User Manager, click **Assignments** and **New Smart Cards** to open the New Smart Cards dialog box with the selected users listed in the selection table.
2. Select all the users for whom you want to generate serial numbers.
3. Click **System-Generate**.
4. In the **Serial Number** box, type a serial number for the first selected user.
5. If the Smart Cards are v 4.x compatible, click **v 4.x Compatible**.
6. Click **Generate**.

   A serial number is assigned to each selected user and displayed in the right-hand column next to or beside the user's name. (The numbers are consecutive in ascending order.)

7. If you want to generate a Smart Card assignment report, check **Save Report to File**.
8. Click **OK**.

   If you checked **Save Report to File**, select a folder and type a filename (or accept the default filename of **SmartCartAssigns.txt**).
9. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Smart Cards" on page 19

How to Generate a Smart Card Assignment Report

A Smart Card assignment report is a file that contains User IDs and associated serial numbers.

To generate a Smart Card assignment report:

1. In the User Manager, in the New Smart Cards dialog box, check **Save Report to File**.

   When you finish assigning Smart Cards and click **OK**, the Serial Number Assignments dialog box opens.
2. Select a folder and type a filename (or accept the default filename of **SmartCardAssigns.txt**).
3. Click **OK**.

Related Topic

"How to Assign Smart Cards" on page 19

How to Assign Virtual Cards

A Virtual Card is a software record stored on a user's computer that identifies and provides information about a user. Each Virtual Card is protected by a time-based hardware token or a password (or both).

Before you begin, you must select one or more users. (If you are adding a new user, the user is selected already.) You can also decide how to protect the Virtual Cards, and if the protection includes a password, the method to use for applying the password to the Virtual Cards.

Note: A v 4.x-compatible card cannot be converted to time-based hardware token protection after it is created.

You can assign Virtual Cards in the following ways. The password procedures apply to all Virtual Cards with passwords, whether or not the Virtual Cards are protected by time-based hardware tokens.

- Assign Time-Based Hardware Token-Protected Virtual Cards without Passwords
- Assign Virtual Cards with a Password for Each User
- Assign Virtual Cards with a Single Password for Multiple Users
- Assign Virtual Cards with Passwords Loaded from a File
- Assign Virtual Cards with System-Generated Passwords

Related Topics

"How to Assign Time-Based Hardware Token-Protected Virtual Cards without Passwords" on page 26

"How to Assign Virtual Cards with a Password for Each User" on page 27

"How to Assign Virtual Cards with a Single Password for Multiple Users" on page 28

"How to Assign Virtual Cards with Passwords Loaded from a File" on page 29

"How to Assign Virtual Cards with System-Generated Passwords" on page 32

"Virtual Card Protection Methods" on page 25

"Virtual Card Password Creation Methods" on page 25

Virtual Card Protection Methods

A Virtual Card can be unlocked with a time-based hardware token, by the entry of a password known only to the assigned user, or by both methods, depending on the protection method you specify.

- **Password-protected**. The user enters a password to unlock the Virtual Card.
- **Time-based hardware token-protected**. The user enters only a PASSCODE (PIN plus tokencode) to unlock the Virtual Card.
- **Password-protected and time-based hardware token-protected**. When the user is connected to the network, the user enters a password to unlock the Virtual Card. When the user works offline, the user enters a PASSCODE (PIN plus tokencode) to unlock the Virtual Card.

Related Topic

"How to Assign Virtual Cards" on page 24

Virtual Card Password Creation Methods

- **System generation**. You select a set of users. The User Manager assigns a Virtual Card for each user and generates a unique password to unlock the card. (You can set the password length during Keon configuration.)
- **Manual entry of a password for each Virtual Card**. You select a single user and type and confirm a password for each card you assign. The user must change this one-time password the first time the Virtual Card is used.
- **Manual entry of a password for all Virtual Cards**. You select a set of users and enter and confirm a single password for all the users' cards. The user must change this one-time password the first time the Virtual Card is used.
- **Read from File**. You select a set of users and specify a file that lists the same users and associates each user with a password. The users must change these one-time passwords the first time they are used.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Time-Based Hardware Token-Protected Virtual Cards without Passwords

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)
- Know whether the users are Keon Desktop Administrators.
- Know that you cannot protect v 4.x-compatible Virtual Cards with time-based hardware tokens.
- Decide whether to generate a Virtual Card assignment report. See "How to Generate a Virtual Card Assignment Report" on page 31.

To assign time-based hardware token-protected Virtual Cards without passwords:

1. In the User Manager, click **Assignments** and **New Virtual Cards** to open the New Virtual Cards dialog box with the selected users listed in the selection table.

   A Virtual Card identifier for the first selected user (based on the User ID and the number of Virtual Cards assigned to the user) is displayed in the **Identifier** box.

2. Select all the users to whom you want to assign Virtual Cards with time-based hardware token protection.
3. Accept the default key length, or select a value from the **Key Length** drop-down list.
4. If the user is a desktop administrator, check **Desktop Administrator**.
5. If you want to generate a Virtual Card assignment report, check **Save Report to File**.
6. Click **Time-Based Hardware Token**.
7. Click **OK**.

If you checked **Save Report to File**, you can specify a folder and filename for the report.

8. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Virtual Cards with a Password for Each User

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)
- Know whether the users are Keon Desktop Administrators.
- Know that you cannot protect v 4.x-compatible Virtual Cards with time-based hardware tokens.
- Decide how to protect the Virtual Cards. See "Virtual Card Protection Methods" on page 25.
- Decide whether to generate a Virtual Card assignment report. See "How to Generate a Virtual Card Assignment Report" on page 31.

To assign Virtual Cards with a password for each user:

1. In the User Manager, click **Assignments** and **New Virtual Cards** to open the New Virtual Cards dialog box with the selected users listed in the selection table.

   A Virtual Card identifier for the first selected user (based on the User ID and the number of Virtual Cards assigned to the user) is displayed in the **Identifier** box.

2. Select a user.

3. Accept the default key length, or select a value from the **Key Length** drop-down list.

4. If the user is a desktop administrator, check **Desktop Administrator**.

5. Click the appropriate protection method: **Password**, **Time-Based Hardware Token**, or **Both**.

6. Click **Manual Entry**.
7. Type a password in the **Password** box, and then type the password again in the **Confirm** box.
8. Repeat steps 2 to 8 until all Virtual Cards are assigned.
9. If you want to generate a Virtual Card assignment report, check **Save Report to File**.
10. Click **OK**.

    If you checked **Save Report to File**, you can specify a folder and filename for the report.
11. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Virtual Cards with a Single Password for Multiple Users

Before you begin, you must

- Select multiple users.
- Know whether the users are Keon Desktop Administrators.
- Know that you cannot protect v 4.x-compatible Virtual Cards with time-based hardware tokens.
- Decide to protect the Virtual Cards with passwords only. See "Virtual Card Protection Methods" on page 25.
- Decide whether to generate a Virtual Card assignment report. See "How to Generate a Virtual Card Assignment Report" on page 31.

To assign Virtual Cards with a single password for multiple users:

1. In the User Manager, click **Assignments** and **New Virtual Cards** to open the New Virtual Cards dialog box with the selected users listed in the selection table.

   A Virtual Card identifier for the first selected user (based on the User ID and the number of Virtual Cards assigned to the user) is displayed in the **Identifier** box.

2. Select all the users to whom you want to assign Virtual Cards with a single password.
3. Accept the default key length, or select a value from the **Key Length** drop-down list.
4. If the users are desktop administrators, check **Desktop Administrator**.
5. Click the appropriate protection method: **Password**, **Time-Based Hardware Token**, or **Both**.
6. Click **Manual Entry**.
7. Type a password in the **Password** box, and then type the password again in the **Confirm Password** box.
8. If you want to generate a Virtual Card assignment report, check **Save Report to File**.
9. Click **OK**.

   If you checked **Save Report to File**, you can specify a folder and filename for the report.
10. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Virtual Cards with Passwords Loaded from a File

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)
- Know whether the users are Keon Desktop Administrators.
- Know that you cannot protect v 4.x-compatible Virtual Cards with time-based hardware tokens.
- Decide how to protect the Virtual Cards. See "Virtual Card Protection Methods" on page 25.
- Create a password file. See "How to Create a Virtual Card Password File" on page 31.

- Decide whether to generate a Virtual Card assignment report. See "How to Generate a Virtual Card Assignment Report" on page 31.

To assign Virtual Cards with passwords loaded from a file:

1. In the User Manager, click **Assignments** and **New Virtual Cards** to open the New Virtual Cards dialog box with the selected users listed in the selection table.

   A Virtual Card identifier for the first selected user (based on the User ID and the number of Virtual Cards assigned to the user) is displayed in the **Identifier** box.

2. Select all the users for whom passwords are specified in your file.

3. Accept the default key length, or select a value from the **Key Length** drop-down list.

4. If the user is a desktop administrator, check **Desktop Administrator**.

5. Click the appropriate protection method: **Password** or **Both**.

6. Click **Read from File**.

7. Type the pathname and filename in the **Enter File Name** box.

   OR

   Click **Browse** to locate the file, and then double-click the filename to enter it into the **Enter File Name** box.

8. Click **Load** to copy the passwords in the file to the table.

   A password is assigned to each user specified in the file and displayed in the right-hand column (when the column has focus) next to or beside the user's name.

   Important: Make sure that the passwords are not seen by any unauthorized person.

   ---

9. If you want to generate a Virtual Card assignment report, check **Save Report to File**.

10. Click **OK**.

    If you checked **Save Report to File**, type a filename for the report (or accept the default filename of **VirtualCardsPWAssigns.txt**).

11. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Create a Virtual Card Password File

A Virtual Card password file contains User IDs and associated one-time passwords. You can use this file to assign Virtual Cards to users.

Important: Before you begin, you must be aware of a potential security risk. Create the password file in a protected directory that only you can read, and delete the file as soon as possible.

Use the following format:

```
# This is a comment.
# userID = one-time password
user01 = ID12345
user02 = ID67890
user03 = abc123
```

To create a Virtual Card password file:

1. Using any text editor, create a text file containing User IDs and one-time passwords.
2. Save the file to a protected directory that only you can read.

Related Topic

"How to Assign Virtual Cards with Passwords Loaded from a File" on page 29

How to Generate a Virtual Card Assignment Report

A Virtual Card assignment report is a file that contains User IDs and associated one-time passwords.

Important: Before you begin, you must be aware of a potential security risk. Save the report to a protected directory that only you can read, and delete the file as soon as possible.

To generate a Virtual Card assignment report:

1. In the User Manager, in the Virtual Cards dialog box, check **Save Report to File**.

   When you finish assigning Virtual Cards and click **OK**, the Save Password Assignments dialog box opens.

2. Select a protected folder that only you can read, and type a filename for the report (or accept the default filename of **VirtualCardsPWAssigns.txt**).
3. Click **Save** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Virtual Cards with System-Generated Passwords

Before you begin, you must

- Select one or more users. (If you are adding a new user, the user is selected already.)
- Decide how to protect the Virtual Cards. See "Virtual Card Protection Methods" on page 25.
- Know that you cannot protect v 4.x-compatible Virtual Cards with time-based hardware tokens.
- Decide whether to generate a Virtual Card assignment report. See "How to Generate a Virtual Card Assignment Report" on page 31.

To assign Virtual Cards with system-generated passwords:

1. In the User Manager, click **Assignments** and **New Virtual Cards** to open the New Virtual Cards dialog box with the selected users listed in the selection table.

   A Virtual Card identifier for the first selected user (based on the User ID and the number of Virtual Cards assigned to the user) is displayed in the **Identifier** box.

2. Select all the users to whom you want to assign Virtual Cards with system-generated passwords.

3. Accept the default key length, or select a value from the **Key Length** drop-down list.
4. If the user is a desktop administrator, check **Desktop Administrator**.
5. Click the appropriate protection method: **Password** or **Both**.
6. Click **System-Generate**, and then click **Generate Passwords**.

   A new password is assigned to each selected user and displayed in the right-hand column (when the column has focus) next to or beside the user's name so that the password can be given to the user.

   Important: Make sure that the passwords are not seen by any unauthorized person.

7. If you want to generate a Virtual Card assignment report, check **Save Report to File**.
8. Click **OK**.

   If you checked **Save Report to File**, you can specify a folder and filename for the report.
9. Click **Save** or **Save All** to save the changes to the database.

Related Topic

"How to Assign Virtual Cards" on page 24

How to Assign Access Rights to a User

Before you begin, you must

- Select one or more users.
- Have at least one Agent on an Agent Host.

To assign access rights to a user:

1. In the User Manager, click **Assignments** and **Assign** to open the Assign Access Rights dialog box with Keon Agents listed in the selection table.
2. If you want to search for an Agent, click **Lookup**.
3. Select an Agent.

   Note: The parameters displayed in the **Parameters** panel depend on the selected service.

4. In the **Parameters** panel, type the appropriate parameters in the labeled boxes.
5. Click **OK**.
6. Click **Save** to save the changes to the database.

Related Topics

"How to Edit a User's Access Rights" on page 35

"How to Remove a User's Access Rights" on page 36

How to Edit a User's Access Rights

Before you begin, you must select a user in the selection table and a set of access rights in the Access Rights tree. You cannot use this procedure to edit a Keon Agent.

To edit a user's access rights:

1. In the User Manager, click **Assignments** and **Edit** to open the Edit Access Rights dialog box with the user's access rights (except for passwords) displayed in the **Parameters** panel.
2. Edit the appropriate parameters in the labeled boxes.
3. Click **OK**.
4. Click **Save** to save the changes to the database.

Related Topic

"How to Edit an Agent" on page 69

"How to Assign Access Rights to a User" on page 34

"How to Remove a User's Access Rights" on page 36

How to Remove a User's Access Rights

Before you begin, you must select a user in the selection table.

To remove a user's access rights:

1. In the User Manager, click **Assignments**.
2. In the **User Access Rights** area, double-click the access rights folder icon until a document icon displays.
3. Click the document icon (for an Oracle Agent, this icon is labeled **GIVENUSER**; for a Lotus Notes Agent, this icon is labeled **Default Parameters Values**).
4. Click **Remove**.
5. Click **Save** to save the changes to the database.

Related Topic

"How to Delete an Agent" on page 70

"How to Assign Access Rights to a User" on page 34

"How to Edit a User's Access Rights" on page 35

How to Assign a Group to a User

Before you begin, you must

- Select a user.
- Define one or more groups.

To assign a group to a user:

1. In the User Manager, click **Assignments** and **Edit** to open the Assign Groups to User dialog box.
2. Select one or more groups in the **Available Groups** list, and click **Add**.
3. Click **OK**.
4. Click **Save** to save the changes to the database.

How to Remove a Group Assigned to a User

Before you begin, you must select a user.

To remove a group assigned to a user:

1. In the User Manager, click **Assignments** and **Edit** to open the Assign Groups to User dialog box with a list of groups assigned to the selected user.
2. Select one or more groups in the **Groups** list, and click **Remove**.
3. Click **OK**.
4. Click **Save** to save the changes to the database.

How to Edit a User

Before you begin, you must select one or more users.

To edit a user:

1. Edit information in the appropriate labeled boxes.
2. If you want to edit a user's Smart Card or Virtual Card information, see "How to Edit a Credential" on page 62.
3. If you want to edit a user's group information, see "How to Edit a Group" on page 43.
4. If you want to edit a user's access rights, see "How to Edit a User's Access Rights" on page 35.
5. Click **Save** to save the changes to the database.

Related Topics

"How to Delete a User" on page 40

"How to Add a User" on page 14

How to Delete a User

When you delete a user, you also delete the user's Smart Cards, Virtual Cards, and associated access rights.

Before you begin, you must select one or more users.

Note: When you delete a user, the database is immediately updated.

To delete a user:

1. In the User Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to delete the user from the database immediately.

Related Topic

"How to Edit a User" on page 39

2

Group Manager

To be written.

How to Add a Group

Use this procedure to create a group and store it in the database.

You can use groups to associate users with common characteristics such as location, job type, or department.

Before you begin, you must know that

- A group must have a unique name
- A group's access rights apply to each member of the group

To add a group:

1. In the Group Manager, click **New**.
   The Workspace clears, and an empty row is added to the selection table.
2. In the **Group Name** box, type a unique name for the group.
3. If you want to assign access rights to the group, or add group members, complete one or both of the following procedures:
   "How to Assign a User to a Group" on page 44
   "How to Assign Access Rights to a Group" on page 46
4. Click **Save**.

Related Topics

"How to Edit a Group" on page 43

"How to Rename a Group" on page 49

"How to Delete a Group" on page 50

How to Edit a Group

Before you begin, you must select one or more groups. If you select more than one group, you cannot rename the groups.

To edit a group:

1. In the Group Manager, edit the appropriate boxes.
2. If you want to add or remove group members, or edit the group's access rights, complete one or more of the following procedures:
   "How to Assign a User to a Group" on page 44
   "How to Remove a User Assigned to a Group" on page 45
   "How to Edit a Group's Access Rights" on page 47
3. Click **Save** to save the changes to the database.

How to Assign a User to a Group

Before you begin, you must select one or more groups.

To assign a user to a group:

1. In the Group Manager, click **Members**.
2. Click **Membership** (for a single group) or **Add Only** (for multiple groups) to open the Assign Users to Group dialog box.
3. Select one or more groups in the **Available Users** list, and click **Add**.
4. Click **OK**.
5. Click **Save** to save the changes to the database.

How to Remove a User Assigned to a Group

Before you begin, you must select a group.

To remove a user assigned to a group:

1. In the Group Manager, click **Members**.
2. Select one or more users from the **Group Members** list.
3. Click **Remove**.

How to Assign Access Rights to a Group

Before you begin, you must select one or more groups.

To assign access rights to a group:

1. In the Group Manager, click **Access Rights** and **Assign** to open the Assign Access Rights dialog box with a list of Keon Agents in the selection table.
2. Select a Keon Agent.

   Note: The parameters displayed in the **Parameters** panel depend on the selected Keon Agent.

3. If you want to search for an Agent, click **Lookup**.
4. In the **Parameters** panel, type the appropriate parameters in the labeled boxes.
5. Click **OK**.
6. Click **Save** to save the changes to the database.

Related Topics

"How to Edit a Group's Access Rights" on page 47

"How to Remove a Group's Access Rights" on page 48

How to Edit a Group's Access Rights

Before you begin, you must select a group in the selection table and a set of access rights in the Access Rights tree.

To edit a group's access rights:

1. In the Group Manager, click **Access Rights** and **Edit** to open the Edit Access Rights dialog box with the group's access rights (except for passwords) displayed in the **Parameters** panel.
2. Edit the appropriate parameters in the labeled boxes.
3. Click **OK**.
4. Click **Save**.

Related Topics

"How to Edit an Agent Host" on page 75

"How to Remove a Group's Access Rights" on page 48

How to Remove a Group's Access Rights

Before you begin, you must select a group in the selection table and a set of access rights in the Access Rights tree.

To remove a group's access rights:

1. In the Group Manager, click **Remove**.
2. Click **Save** to save the changes to the database.

Related Topic

"How to Delete an Agent Host" on page 76

How to Rename a Group

Before you begin, you must select a group. If you select more than one group, you cannot rename the groups.

To rename a group:

1. In the Group Manager, type the new name for the group in the **Group Name** box.
2. Click **Save** to save the changes to the database.

Related Topic

"How to Edit a Group" on page 43

How to Delete a Group

Before you begin, you must select one or more groups.

Note: When you a delete a group, the database is immediately updated.

To delete a group:

1. In the Group Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to delete the group from the database immediately.

Related Topics

"How to Edit a Group" on page 43

"How to Rename a Group" on page 49

How to Add an Agent Host

Before you begin, you must know

- The unique name of the Agent Host you want to add
- A node key (usually 4 to 8 characters). You can set the length during Keon configuration.

To add an Agent Host:

1. In the Agent Host Manager, click **New**.
   The Workspace clears, and an empty row is added to the selection table.
2. In the **Agent Host Name** box, type the name of the Agent Host.
3. Click **Verify** to verify the IP address.
4. In the **Enter Node Key** box, type the node key.
5. In the **Confirm** box, type the node key again.
6. Click **Save** to save the new Agent Host information and create the Agent Host's Virtual Card.

How to Edit an Agent Host

No aspect of an Agent Host can be edited, except for the Virtual Card's Node Key. See "How to Edit a Credential" on page 62.

How to Delete an Agent Host

Before you begin, you must

- Select one or more Agent Hosts.
- Know whether the Agent Host is acting as a server.

Note: You cannot delete an Agent Host that is acting as a server. However, you can still delete the Agent Host's associations, including Agents and access rights. When you delete an Agent Host, the database is immediately updated.

To delete an Agent Host:

1. In the Agent Host Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to delete the Agent Host from the database immediately.

How to List Agents Associated with a Particular Agent Host

1. In the Agent Host Manager, select the Agent Host for which you want to display the Keon Agents.

   In the **Agents** box, a list of all the Agents associated with the selected Agent Host is displayed.
2. Double-click the Agent name to display the access method and comments.

How to Add an Agent to an Agent Host

See “How to Add an Agent Host” on page 51.

How to Remove an Agent from an Agent Host

See “How to Delete an Agent Host” on page 53.

3

Credential Manager

To be written.

How to Create a Credential

See:

“How to Assign Smart Cards” on page 19

“How to Assign Virtual Cards” on page 24

“How to Add an Agent to an Agent Host” on page 77

The PIN Unlocking Key

Anyone who knows the PIN unlocking key has direct access to the associated credential.

Important: Displaying the PIN unlocking key is a potential security risk.

At Keon configuration, you can set a parameter to prevent PIN unlocking keys from being displayed for Virtual Cards.

How to Search for a Credential

In the Credential Manager, you can search for a credential by credential type, and optionally restrict the search by specifying a secondary search criterion.

How to Export a Credential

You can export a credential to your local file system so that you can move the credential. For example, you can export a Virtual Card in order to move it to a laptop that does not have Web access. Similarly, you can export an Agent Host Virtual Card in order to move it from one server to another.

Note: You cannot export a smart card.

Before you begin, you must select a credential.

To export a credential:

1. In the Credential Manager, on the File menu, click **Export**.
   The Export Virtual Card to File dialog box opens.
2. Specify the pathname and filename for the output file.

   Note: By default, the directory is set to your home directory, and the file extension is **.kpg**.
3. Click **Save**.

How to Edit a Credential

Use this procedure to edit the protection method or password for a Virtual Card.

Before you begin, you must select a Virtual Card.

To edit a credential:

1. In the Credential Manager, select the new protection method or type the new password (or both).
2. Click **Save**.

Related Topics

"Virtual Card Protection Methods" on page 25

"Virtual Card Password Creation Methods" on page 25

"How to Delete a Credential" on page 63

How to Delete a Credential

Before you begin, you must select one or more Virtual Cards.

Note: You cannot use this procedure to delete an Agent Host Virtual Card. When you delete a credential, the database is immediately updated.

To delete a credential:

1. In the Credential Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to immediately delete the credential from the database.

How to Help Users Who Have Forgotten Their Passwords

Before you begin, you can search for all Virtual Cards by User ID.

To help users who have forgotten their passwords:

1. In the Credential Manager, select the Virtual Card of a user with a forgotten password.
2. Assign a new password and notify the user.
3. Repeat steps 1 and 2 until all the users with forgotten passwords are assigned new passwords.

The users will be asked to change their passwords after they log in.

How to Find Out Who is Assigned to a Particular Credential

In the Credential Manager, search for credentials by serial number. The Workspace displays the attributes for the credential.

How to Show or Hide Password Guidelines

In the Credential Manager, click **Show Password Guidelines** to display the rules for valid passwords.

Click **Hide Password Guidelines** to hide the **Password Guidelines** panel and change the button text to **Show Password Guidelines**.

4

Agent Manager

To be written.

How to Add an Agent

Before you begin, you must know

- The name of the service to which you want to connect
- The Agent Host on which the service resides
- The access method (usually a port number) through which the Agent Host and the service communicate

To add an Agent:

1. In the Agent Manager, click **New**.
   The Workspace clears, and an empty row is added to the selection table.
2. From the drop-down list in the **Service** panel, select the service with which you want to associate the Agent.
   The **Description** box fills in with a description of the service.
3. From the **On Agent Host** drop-down list, select the Agent Host on which the Agent will reside.
4. In the **Access Method** box, type the access method by which the Agent Host will communicate with the service.
5. In the **Comment** box, type a description of the access method.
6. Click **Save**.

How to Edit an Agent

Before you begin, you must

- Select an Agent.
- Know the new access method by which the Agent Host will communicate with the service.

To edit an Agent:

1. In the Agent Manager, in the **Access Method** box, type the new access method.
2. In the **Comment** box, type a description of the new access method.
3. Click **Save**.

Related Topic

"How to Delete an Agent" on page 70

How to Delete an Agent

When you delete an Agent, you also delete the Agent's associated access methods.

Before you begin, you must select one or more Agents.

Note: When you delete an Agent, the database is immediately updated.

To delete an Agent:

1. In the Agent Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to delete the Agent and the associated access methods from the database immediately.

Related Topic

"How to Edit an Agent" on page 69

How to Copy Access Rights from an Agent to a New Agent

Before you begin, you must select an Agent that has the access rights that you want a new Agent to have.

How to copy access rights from an Agent to a new Agent:

1. In the Agent Manager, click **Edit – Access Method Copy**.

   The Workspace clears, and a row is added to the selection table with the service and Agent Host of the previously selected Agent.

   Note: You can edit the new Agent until you save the changes.

2. Click **Save**.

   You can edit the individual access rights.

Related Topic

"How to Edit an Agent" on page 69

5

Agent Host Manager

To be written.

How to Add an Agent Host

Before you begin, you must know

- The unique name of the Agent Host you want to add
- A node key (usually 4 to 8 characters). You can set the length during Keon configuration.

To add an Agent Host:

1. In the Agent Host Manager, click **New**.
   The Workspace clears, and an empty row is added to the selection table.
2. In the **Agent Host Name** box, type the name of the Agent Host.
3. Click **Verify** to verify the IP address.
4. In the **Enter Node Key** box, type the node key.
5. In the **Confirm** box, type the node key again.
6. Click **Save** to save the new Agent Host information and create the Agent Host's Virtual Card.

How to Edit an Agent Host

No aspect of an Agent Host can be edited, except for the Virtual Card's Node Key. See "How to Edit a Credential" on page 62.

How to Delete an Agent Host

Before you begin, you must

- Select one or more Agent Hosts.
- Know whether the Agent Host is acting as a server.

Note: You cannot delete an Agent Host that is acting as a server. However, you can still delete the Agent Host's associations, including Agents and access rights. When you delete an Agent Host, the database is immediately updated.

To delete an Agent Host:

1. In the Agent Host Manager, click **Delete**.
2. In the Confirm Delete dialog box, click **Yes** to delete the Agent Host from the database immediately.

How to List Agents Associated with a Particular Agent Host

1. In the Agent Host Manager, select the Agent Host for which you want to display the Keon Agents.

   In the **Agents** box, a list of all the Agents associated with the selected Agent Host is displayed.
2. Double-click the Agent name to display the access method and comments.

How to Add an Agent to an Agent Host

See “How to Add an Agent Host” on page 74.

How to Remove an Agent from an Agent Host

See “How to Delete an Agent Host” on page 76.

6

Report Manager

To be written.

Report Categories

- **Users reports.** This category focuses on users' usage statistics, group memberships, and Agent/Agent Host associations. See "How to Generate Reports About Users" on page 89.
- **User Authentication Statistics reports.** This report focuses on the number of successful and denied authentication attempts during a specified time range. See "How to Generate a Report About Users' Authentication Statistics" on page 99.
- **User Credentials reports.** This category focuses on Smart Cards and Virtual Cards. See "How to Generate a Report About User Credentials" on page 91.
- **Agent Host Credentials reports.** This category focuses on Agent Hosts. See "How to Generate a Report About Agent Host Credentials" on page 92.
- **Groups reports.** This category provides such information for selected groups as the number of users in each group, and the names and User IDs of group members. See "How to Generate a Report About Group Memberships" on page 98.
- **Keon Audit Log reports.** This category focuses on event messages that are logged in the Keon audit log. See "How to Generate Reports Based on the Keon Audit Log" on page 94.
- **Agents/Hosts reports.** This category focuses on Keon Agents that are installed on a selected Agent Host. See "How to Generate a Report About Keon Agents and Agent Hosts" on page 93.

How to Set Up a Report

This procedure describes how to set up a report. See “Report Categories” on page 80.

To set up a report:

1. In the **Category** box of the Report Manager, click the type of report. The default is **Users**.
2. In the **By** box, click the focus of the report.

   The **Report Description** box displays a brief description of the report type. The description changes when you select a different focus.
3. Below the **By** box, depending on what you have selected as the focus of the report, you may need to specify the focus criteria of the report.
4. In the table of report fields in the Workspace
   - Clear the **Display** checkbox next to each report field that you want to exclude from the report.
   - Check the **Display** checkbox next to each report field that you want to include in the report.

   At least one of the fields marked with an asterisk must be selected.
5. In the **Sort by** box, click the field name by which the report items will be sorted.
6. Click a **Report Format** option. The default is **HTML**.

To generate a report:

1. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
2. Click **Generate Report**.

   If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

“Report Categories” on page 80

“How to Preview a Report’s Format” on page 83

“How to Save a Report” on page 84

“How to View a Report” on page 85

“How to Print a Report” on page 87

“How to Cancel a Report” on page 88

How to Preview a Report's Format

Use this procedure to preview a report's format before generating a report that will take a long time to finish.

Before you begin, you must specify a program for viewing reports in either HTML or CSV format. See "How to Set Up Report Viewers" on page 86

To preview a report's format:

1. In the **Generate Option** box, click **Preview Report Format**.
2. Click **Generate Report**.
   When the Report Manager finishes generating the first 20 entries of the report, it displays them in the application that you have specified for viewing a report of that format.

Related Topics

"How to Set Up a Report" on page 81

"How to View a Report" on page 85

How to Save a Report

Before you begin, you must set up a report. See “How to Set Up a Report” on page 81.

To save a report:

1. In the **Generate Option** box, click **Save Report to a File**.
2. Click **Generate Report**.
3. In the Save Report As dialog box, type the full pathname and filename of the file into the **File Name** box.

   OR

   Click **Browse** to select the filename.
4. Click **Save**.

   When the Report Manager finishes generating the report, it saves the report in the file that that you have specified.

How to View a Report

Before you view a report, you must

- Set up the report. See “How to Set Up a Report” on page 81.
- Set up a report viewer. See “How to Set Up Report Viewers” on page 86.

To view a report:

1. In the **Generate Option** box, click **View Entire Report**.
2. Click **Generate Report**.
   When the Report Manager finishes generating the report, it starts the application that you have specified for viewing a report of the selected format. If you have not specified an application, the internal default viewer is used.

Related Topic

“How to Preview a Report’s Format” on page 83

How to Set Up Report Viewers

Before you can view a generated report in either HTML or CSV (comma-separated values) format, you can specify the application you want to use for viewing reports in the selected format.

To set up report viewers:

1. On the **File** menu of the Report Manager, click **Set Up Viewers**.
2. In the Set Up Default Report Viewers dialog box, type the full pathname of the Web browser's executable file (***.exe**) in the **Default HTML Viewer** box.

   OR

   Click **Browse** to select the file.
3. In the **Default CSV Viewer** box, type the full pathname of the spreadsheet program's executable file (***.exe**).

   OR

   Click **Browse** to select the file.
4. Click **OK**.

Related Topic

"How to View a Report" on page 85

How to Print a Report

You cannot print a report directly from the Report Manager, but you can print generated reports through other programs.

Before you begin, you must set up the report. See “How to Set Up a Report” on page 81.

To print a generated report using the View Entire Report option:

1. Set up a Web browser for viewing the report if it is in HTML format, and/or a spreadsheet program for viewing the report if it is in CSV format. See “How to Set Up Report Viewers” on page 86.
2. Click **View Entire Report** in the **Generate Option** box.
3. After the Report Manager finishes generating the report, the report is displayed in the program that you specified for viewing reports of that format. Use the **Print** command to print the report.

   For HTML format, multiple HTML pages may be generated if the report has more than 200 records. In this case, you must navigate through each hyperlink and print each page separately.

To print a generated report that has been saved to a file:

1. Click **Save Report to a File** in the **Generate Option** box.
2. In the Save Report As dialog box, specify the filename of the report.
3. Using a program that displays files of the same format as the report file, display and print the contents of the file.

Related Topic

“How to Set Up Report Viewers” on page 86

How to Cancel a Report

If you cancel a report, all report entries that have been generated so far are discarded and cannot be viewed or saved.

To cancel a report:

Click **Cancel Report**.

How to Generate Reports About Users

You can generate reports about users that focus on the following information:

- **Set of users.** This report focuses on either all users or a specified subset of users. See “How to Generate a Report About a Set of Users” on page 95.
- **Basic user statistics.** This report includes information about all users, and administrators, including users who belong to groups or who are associated with Keon Agents and Agent Hosts. See “How to Generate a Report About Basic User Statistics” on page 97.
- **Group memberships.** This report focuses on the members of selected groups. See “How to Generate a Report About Group Memberships” on page 98.
- **Agent and Agent Host associations.** This report focuses on which users are associated with selected Agents and Agent Hosts. See “How to Generate a Report About Users’ Agent and Agent Host Associations” on page 100.
- **Custom Data fields.** In any report about users, you can also include Custom Data fields. See “How to Generate a Custom Report” on page 101.

Related Topic

“Report Categories” on page 80

How to Generate a Report About Groups

1. In the **Category** box of the Report Manager, click **Groups**.
2. Click **Select Groups**.
3. In the Select Groups for Report dialog box, click one or more groups in the **Available Groups** list box, and then click **Add**.

   OR

   To display the **Available Groups** list differently, click the sorting approach in the **Search for Groups** box and specify search criteria, and then click **Search**.
4. When you finish selecting groups, click **OK**.
5. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
6. In the **Sort by** box, click the field name by which the report items will be sorted.
7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**.
10. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

“How to Generate a Report About Group Memberships” on page 98

“Report Categories” on page 80

How to Generate a Report About User Credentials

1. In the **Category** box of the Report Manager, click **Credentials**.
2. If you want to focus on credentials by using their identification numbers, click **User Credentials By Identifier** in the **By** box, and then specify the range of identification numbers in the **From** and **To** boxes.

   If you type an asterisk (*) in the **From** box, all numbers will be included in the report.

   OR

   If you want to focus on credentials by using their expiration times, click **User Credentials By Expiration Date** in the **By** box, and then type a date in both the **Between** and the **And** boxes to indicate a range of expiration dates.
3. In the **Credential Type** box, click the credential you want to include in the report. The default type is **All User Credentials**.
4. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
5. In the **Sort by** box, click the field name by which the report items will be sorted.
6. Click a **Report Format** option. The default is **HTML**.
7. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
8. Click **Generate Report**.
9. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

“Report Categories” on page 80

How to Generate a Report About Agent Host Credentials

1. In the **Category** box of the Report Manager, click **Credentials**.
2. If you want to focus on credentials by using their identification numbers, click **Agent Host Credentials By Identifier** in the **By** box, and then specify the range of identification numbers in the **From** and **To** boxes.

   If you type an asterisk (*) in the **From** box, all numbers will be included in the report.

   OR

   If you want to focus on on credentials by using their expiration times, click **Agent Host Credentials By Expiration Date** in the **By** box, and then type a date in both the **Between** and the **And** boxes to indicate a range of expiration dates.
3. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
4. In the **Sort by** box, click the field name by which the report items will be sorted.
5. Click a **Report Format** option. The default is **HTML**.
6. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
7. Click **Generate Report**.
8. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

“Report Categories” on page 80

How to Generate a Report About Keon Agents and Agent Hosts

1. In the **Category** box of the Report Manager, click **Agents/Hosts**.
2. In the **Agent Host** box
   - Click **All** to include all Agent Hosts in the report
     OR
   - Click the Agent Host that you want to include in the report
3. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.
   At least one of the fields marked with an asterisk must be selected.
4. In the **Sort by** box, click the field name by which the report items will be sorted.
5. Click a **Report Format** option. The default is **HTML**.
6. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
7. Click **Generate Report**.
8. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

“Report Categories” on page 80

How to Generate Reports Based on the Keon Audit Log

You can generate reports based on the Keon audit log that focus on the following information:

- **All log entries.** For each recorded event, this report can provide a timestamp, a severity level, the log message, and the names of the facility and sender host responsible for sending the event to the log. See How to Generate a Report on All Keon Audit Log Entries.
- **Selected audit log entries.** This report allows you to specify criteria for narrowing the search of the audit log. See How to Generate a Report on Selected Keon Audit Log Entries.
- **Audit log entry statistics.** This report can provide data on the number of successful or denied authentication attempts, authentications by facility or severity level, and the average number of authentications attempted per day. See How to Generate a Report on Keon Audit Log Statistics.

All audit log reports can provide all log entries found in the audit log.

Related Topic

“Report Categories” on page 80

How to Generate a Report About a Set of Users

Use this procedure to generate a report either about all users, or about a set of users that you specify according to a range of last names.

To generate a report about a set of users:

1. In the **Category** box of the Report Manager, click **Users**.
2. In the **By** box, click **All** to focus on all users and clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.

   OR

   Click **Last Name** to focus on a subset of users, and then type a string of characters representing a last name into the **From** and **To** boxes under **Last Name Range**.

   You can also use the asterisk (*) as a wildcard character.

   Note: You cannot use a combination of the asterisk and a string. For example, to include only those users whose last names are in the A to F range, type **A** in the **From** box and **F** in the **To** box. (Do ***not*** type **A*** or **F***.)

3. In the table of report fields in the Workspace
   - Clear the **Display** checkbox next to each report field that you want to exclude from the report.
   - Check the **Display** checkbox next to each report field that you want to include in the report. If you want to display all custom data fields, check the **Display All Custom Data Fields** checkbox.

   Note: At least one of the fields marked with an asterisk must be selected.

4. In the **Sort by** box, click the field name by which the report items will be sorted.

5. If you want to restrict the report according to a specific custom data field, click the field's name in the **Restrict by** box, and (optionally) type the specific field value in the **Matching** box.

   For example, if you want to limit the report to users in the Human Resources department, click **Department** in the **Restrict by** box, and then type **Human Resources** in the **Matching** box.

6. Click a **Report Format** option. The default is **HTML**.

7. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.

8. Click **Generate Report**.

9. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

"How to Generate Reports About Users" on page 89

How to Generate a Report About Basic User Statistics

1. In the **Category** box of the Report Manager, click **Users**.
2. In the **By** box, click **Statistics**.
3. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
4. In the **Sort by** box, click the field name by which the report items will be sorted.
5. Click a **Report Format** option. The default is **HTML**.
6. In the **Generate Option** box, select how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
7. Click **Generate Report**. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

"How to Generate Reports About Users" on page 89

"How to Generate a Report About Users' Authentication Statistics" on page 99

How to Generate a Report About Group Memberships

1. In the **Category** box of the Report Manager, click **Users**.
2. In the **By** box, click **Groups**.
3. Click **Select Groups**.
4. In the Select Groups for Report dialog box, select the groups that you want to specify for the report in the **Available Groups** box and click **Add**, and then click **OK**.
5. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
6. In the **Sort by** box, click the field name by which the report items will be sorted.
7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**.
10. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

“How to Generate Reports About Users” on page 89

“How to Generate a Report About Groups” on page 90

How to Generate a Report About Users' Authentication Statistics

1. In the **Category** box of the Report Manager, click **User Authentication Statistics**.
2. In the **By** box, click the focus of the report.
3. Below the **By** box, depending on what you have selected as the focus of the report, specify the focus criteria of the report.
4. In the **Between** and **And** boxes under **Authentications Attempted**, specify the range of time over which you want to know which users have attempted to authenticate.
5. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
6. In the **Sort by** box, click the field name by which the report items will be sorted.
7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, select how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

"How to Generate Reports About Users" on page 89

"How to Generate a Report About Basic User Statistics" on page 97

How to Generate a Report About Users' Agent and Agent Host Associations

1. In the **Category** box of the Report Manager, click **Users**.
2. In the **By** box, click **Agent/Host**.
3. In the **Service** box, click the type of Agent.
4. In the **Agent Host** box, click the Agent Host on which the Agent is located.
5. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
6. In the **Sort by** box, click the field name by which the report items will be sorted.
7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**.
10. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topics

"How to Generate Reports About Users" on page 89

"How to Generate a Report About Keon Agents and Agent Hosts" on page 93

How to Generate a Custom Report

Custom data fields can be included only in reports about users.

Before you begin, you must define custom data fields in the User Manager. See “How to Add a User” on page 14 or “How to Edit a User” on page 39.

To generate a report that includes custom user-defined fields:

1. In the **Category** box of the Report Manager, click **Users**.
2. In the **By** box, click the focus of the report.
3. Below the **By** box, depending on what you have selected as the focus of the report, specify the focus criteria of the report.
4. In the table of report fields in the Workspace
   - Clear the **Display** checkbox next to each report field that you want to exclude from the report.
   - Check the **Display** checkbox next to each report field that you want in include in the report. If you want to display all custom data fields, check **Display All Custom Data Fields**.

   Note: At least one of the fields marked with an asterisk must be selected.
5. In the **Sort by** box, check the field name by which the report items will be sorted.
6. If you want to restrict the report according to a specific custom data field, click the field’s name in the **Restrict by** box, and (optionally) type the specific field value in the **Matching** box.

   For example, if you want to limit the report to users in the Human Resources department, click **Department** in the **Restrict by** box, and then type **Human Resources** in the **Matching** box.

   You can also use the asterisk (*) as a wildcard character in the **Matching** box.

Note: You cannot use a combination of the asterisk and a string. For example, to include only those users in Accounting and Administration, type **A** in the **Matching** box. (Do ***not*** type **A***.)

If you do not specify a value in the **Matching** box, all users who have the selected custom data field specified for them will be included in the report.

7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, select how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

"How to Generate Reports About Users" on page 89

How to Generate a Report on All Keon Audit Log Entries

1. In the **Category** box of the Report Manager, click **Keon Audit Log**.
2. In the **By** box, click **All**.
3. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
4. In the **Sort by** box, click the field name by which the report items will be sorted.
5. Click a **Report Format** option. The default is **HTML**.
6. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
7. Click **Generate Report**.
8. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

"How to Generate Reports Based on the Keon Audit Log" on page 94

How to Generate a Report on Selected Keon Audit Log Entries

1. In the **Category** box of the Report Manager, click **Keon Audit Log**.
2. In the **By** box, click **Selection**.
3. In the **Events Occurred Between/And** boxes, type the dates and times that indicate the range of time over which you want to find the events.
4. In each of the selection criteria boxes below the **Events Occurred** boxes, specify the selection criteria that you want to use.
5. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
6. In the **Sort by** box, click the field name by which the report items will be sorted.
7. Click a **Report Format** option. The default is **HTML**.
8. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
9. Click **Generate Report**.
10. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

“How to Generate Reports Based on the Keon Audit Log” on page 94

How to Generate a Report on Keon Audit Log Statistics

1. In the **Category** box of the Report Manager, click **Keon Audit Log**.
2. In the **By** box, click **Statistics**.
3. In the table of report fields in the Workspace, clear the **Display** checkbox next to each report field that you want to exclude from the report.

   At least one of the fields marked with an asterisk must be selected.
4. In the **Sort by** box, click the field name by which the report items will be sorted.
5. Click a **Report Format** option. The default is **HTML**.
6. In the **Generate Option** box, click how the report is to be processed after the Report Manager generates it. The default is **View Entire Report**.
7. Click **Generate Report**.
8. If you want to update the report with the latest information from the database before the Report Manager generates the report, click **Refresh**.

Related Topic

"How to Generate Reports Based on the Keon Audit Log" on page 94

Glossary

Agent

See *Keon Agent*.

agent definition file

The file in the Keon database that defines the parameters for a *Keon Agent*. Formerly called the generic agent parameters (GAP) file.

Agent Host

Machine on which a Keon Agent is enabled.

asymmetric encryption

See *public key encryption*.

authentication

The process of identifying an individual to determine if he or she has the right to access a computer network, workstation, or Web site. Authentication methods include passwords, hardware tokens, software tokens, smart cards, software smart cards, and biometric devices.

bridge emulator (or bridge protocol server)

Software running on the Keon Security Server that listens on a network port to respond to *bridge protocol* requests. The bridge emulator provides backwards compatibility.

bridge protocol

The protocol used for communication between legacy components and Keon components.

CA

A certificate authority (often referred to as a certification authority or a certifying authority). A trusted third-party organization or company that issues digital certificates used to create digital signatures and public/private key pairs.

certificate

Also known as a *digital certificate*. A certificate is an electronic document binding together some pieces of information, such as a user's identity and public key.

A Certificate Authority (*CA*) typically issues certificates, but an enterprise, a government, or some other entity can sign its own certificate. This self-signed certificate is the root certificate for the entity and is used to sign subordinate certificates.

Connect Agent

See *Keon Agent*.

Credential Store

Holds a user's public key credentials (private key[s] and certificates, symmetrical encryption keys, and SSO parameters). *SecurID Smart Cards* and *Virtual Smart Cards* are Credential Stores.

CRL

Certificate Revocation List, a collection of certificates that are no longer valid.

CSSP

Cryptographic Security Services Protocol, the protocol used between the Keon Desktop and the Keon Security Server.

digital certificate

A file that serves as a user's electronic credentials. The certificate holds the public key and other user information that is used to authenticate a user's identity.

digital signatures

Data that accompany a file that can be used to verify the identity of the sender and attest that the file has not been modified since it left the sender.

Distinguished Name

A unique string comprised of multiple attributes that, when viewed as a whole, identify an entity (for example, a user or Certificate Authority).

For users, a Distinguished Name customarily contains at least three attributes: the user's name or user ID, the organization with which the user is affiliated, and the country of which the user is a citizen. Example: cn=Jon Doe, ou=Operations, mail=jdoe@widget.com, o=Widget Corp, c=US.

See *Subject Distinguished Name* and *Issuer Distinguished Name*.

DN

See *Distinguished Name*.

ELS

The event-logging subsystem that receives and dispatches events from the *Keon Security Server* and other parts of the system, such as the *Keon Certificate Server*.

encryption

The process of scrambling data using an encryption key so that it is very difficult for anyone other than the intended recipients to recover the original data. To decipher the message, the receiver of the encrypted data must have the proper decryption key.

enterprise access rights

Used by a Keon Agent to determine if a user has been given access to a protected application. Access rights are stored in a *PAC*.

file encryption

Technology used to encrypt and protect locally stored individual files or folders.

GAP file

See *agent definition file.*

host

A physical machine. Can have databases or agents installed on it. The Agent Host Manager in the *Management Console* handles the hosts for Keon Agents.

HTTP

HyperText Transfer Protocol. The client-server TCP/IP protocol used on the World-Wide Web for the exchange of HTML documents.

HTTPS

A secure variant of the HTTP protocol. Under HTTPS, the connection between client and server is encrypted using a Secure Socket Layer (*SSL*).

IIDC

An identity certificate. A long-life certificate issued by a CA that establishes a user's identity, used for authentication within the *PKI*. An identity certificate is the same as a *personal certificate*.

IPSec certificate

A certificate that has its key usage indicators set to permit the certificate's use in support of the IPSec (IP-layer) security protocol.

Issuer Distinguished Name

Describes the identity of the *CA* that issued a certificate. A self-signed certificate has the same subject and issuer distinguished name. See *Distinguished Name*.

Issuing Authority

Same as a Certificate Authority. See *CA*.

Keon Agent

Protects an application server and creates an authenticated, secure connection from the Keon Desktop to the application server.

Keon Certificate Server

Provides a system for issuing and managing digital certificates. Netscape Directory Server is provided to supply LDAP services to the Keon Certificate Server. Other certificate authorities can be used with Keon.

Keon Certificate Server Root signer certificate

The certificate that a Keon Certificate Server uses to sign personal certificates issued from a particular jurisdiction. Each jurisdiction managed by your Keon Certificate Server has its own root signer certificate.

The Keon Certificate Server Root signer certificate must be imported to the Keon Security Server using the Certificate Control Manager.

Keon Desktop

Provides desktop file encryption, manages single sign-on and user credentials at the desktop, and delivers services for securing e-mail, web browsers, and access to applications.

Keon general certificate

A certificate that supports login until the user applies for and receives a personal certificate issued by a certification authority. Some users may never get personal certificates.

Keon Key Recovery signer certificate

Used by *Keon Desktop* to authenticate the Key Recovery Virtual Card. This certificate is signed by the Keon Virtual Card Admin signer.

Keon Key Recovery Virtual Card

Used to log in to a Keon Desktop to recover a symmetric file encryption key. There is only one Key Recovery Virtual Card for each primary Keon Security Server.

In the event that a user is not present to decrypt needed files (for example, if the user leaves the company), an administrator uses the Key Recovery Virtual Card to log in to the user's Keon Desktop. Once logged in with this special credential store, the administrator has permission to run the admrec program to decrypt files.

Keon PAC Issuer signer certificate

Used by the Keon Security Server to sign PACs (privilege attribute certificates). The Keon Desktop uses this certificate to authenticate PACs that it receives from the Keon Security Server.

Keon Security Server

Provides authentication, authorization, certificate validation, event logging, management of security information, security information replication, and process management.

Keon Smart Card signer certificate

Used by the Keon Desktop to verify general certificates issued to SecurID Smart Cards created either by the Keon Signing Station or by a smart card vendor.

Keon Virtual Card signer certificate

Used by the Keon Desktop to verify general certificates issued to Virtual Smart Cards created with the Keon Management Console. There are two Keon Virtual Card signers, one for Keon Desktop users and one for Keon Desktop administrators.

Key Management

Closely related to a certification authority (CA) service, it provides the range of services necessary to manage the generation, transport, revocation, and renewal of public and private keys associated with certificate use.

LDAP

Lightweight Directory Access Protocol, based on the standard X.500 LDAP directory. A simple protocol that allows users to access and search disparate directories over the Internet.

Management Console

The user interface to the Keon Security Server database. The managers are User, Credential, Group, Agent Host, Agent, Certificate Control, and Report.

message digest

A unique fingerprint for a message or document created using a hashing algorithm, such as MD-5 or SHA-1. Tampering with the document will produce a different message digest.

MIME

Multipurpose Internet Mail Extensions, designed for sending multimedia electronic mail.

PAC

A privilege attribute certificate. Signed information about a user's privileges. An X.509 certificate with the user's *public key* and *Distinguished Name*. The extension area contains the *enterprise access rights* data.

PCM

Process Control Manager, a server responsible for starting and stopping other Keon Security Server processes.

PE

PIN encryptor.

personal certificate

A Keon Certificate Server or a third-party Certification Authority issues these certificates to Keon users. The personal certificate replaces the user's *Keon general certificate*. Because a personal certificate is directly associated with a user's identity, a personal certificate can be used with S/MIME-enabled applications to send and receive digitally signed and encrypted messages.

PKCS

Public Key Cryptographic Standards. A series of specifications developed by RSA Laboratories that define common cryptographic data elements and structures.

PKI

Public Key Infrastructure. Support for using public key technology. Keon Manager and Keon Desktop are PKI aware. A distributed system of users and computers that verifies the identity of a person seeking authorization to use a computer system or a network and then associates a public key with the user in a highly secure manner.

PKI token

The way to identify a user with PKI capability. Same as a *Credential Store*.

private key

Part of the public/private key pair, the private key is the only means to vouch for the identity of the owner of a digital certificate, which includes the *public key*.

PSD

Personal Security Device. See *Credential Store*.

public key

Part of the public/private key pair, an owner's public key is available to anyone. It can be used to encrypt a message that can then be decrypted only with the owner's *private key*.

public key encryption

This encryption scheme use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the recipient's public key, but only the recipient has the private key necessary to decrypt it.

RSA Public/Private Key

Used in Keon, this is the most popular asymmetric encryption algorithm implemented for the authentication of users.

SecurID Smart Card

Hardware implementation of a *Credential Store* on an RSA-capable smart card. A plastic card, similar to the size and shape of a credit card, that contains a microprocessor chip with both secure storage of public/private key data and cryptographic processing capabilities.

session encryption

When the information transferred between two hosts is encrypted to ensure the privacy and integrity of the data.

SSL

Secure Socket Layer, an open standard proposed by Netscape Communications for providing secure (encrypted and authenticated) WWW services (as well as other applications, such as mail, FTP, and Telnet) over the Internet. SSL uses RSA public-key encryption.

SSO

Single Sign-On, the process by which a user authenticates once to gain access to multiple applications and resources without having to authenticate to each resource and manage multiple passwords.

SSSO

Secure Single Sign-On. This is *SSO* using strong authentication to identify the user initially. SSSO encrypts all application traffic and uses certificates to identify both clients and servers.

Subject Distinguished Name

Establishes a relationship between the named person or entity and the public key in a certificate. See *Distinguished Name*.

two-factor authentication

A form of authentication that requires two distinct items to ensure user authenticity. Factors could include a token, personal identification number (PIN), biometric device, or smart card. A bank-issued ATM is the most common example of two-factor authentication.

Virtual Private Networks (VPNs)

A method to connect multiple remote users or remote offices to an enterprise network via the Internet.

Virtual Smart Card

Software implementation of a Smart Card. Also called a Virtual Card. A file that is encrypted either with a password or (indirectly) with a SecurID-protected decryption key.

x.509 certificate

Digital information signed by a certificate authority, an x.509 certificate contains subject-related information that links a specific user to his or her public key. The x.509 certificate contains, for example, the subject distinguished name, the RSA public key, the issuer name, and the digital signature.

Index

V

W