Note: Before using this information and the products it supports, be sure to read the general information under “Notices” on page 23.

Fifth Edition (November, 2015)  
This and other publications related to the IBM 4765 PCIe Cryptographic Coprocessor can be obtained in PDF format from the product Web site. Click on the PCIe Cryptographic Coprocessor link at http://www.ibm.com/security/cryptocards, and then click on the Library link.

Reader’s comments can be communicated to IBM by contacting the Crypto team at crypto@us.ibm.com.

© Copyright International Business Machines Corporation 2011, 2015.  
Note to U. S. Government Users—Documentation related to restricted rights Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.
## Contents

About this document ........................................................................................................................................... vi
Prerequisite knowledge ........................................................................................................................................ vi
Typographic conventions ............................................................................................................................... vi
Related publications ........................................................................................................................................... vi
Summary of changes ...................................................................................................................................... vii
Overview ........................................................................................................................................................ 1
Supported hardware and software ................................................................................................................... 2
Using CCA Backup/Restore ............................................................................................................................ 3
   Install CCA BR ........................................................................................................................................ 3
   Before using CCA BR .............................................................................................................................. 3
   Launch CCA BR ...................................................................................................................................... 3
   Adapter functions .................................................................................................................................... 4
      Select an adapter ................................................................................................................................... 5
      Obtain adapter status .......................................................................................................................... 5
   Backup functions ...................................................................................................................................... 7
      Backup selected information .............................................................................................................. 7
      Backup all information ....................................................................................................................... 9
   Restore functions ..................................................................................................................................... 10
Using the CCA test initialization utility ......................................................................................................... 15
   Install CCA Init ...................................................................................................................................... 15
   Launch CCA Init ..................................................................................................................................... 15
   CCA Init results ..................................................................................................................................... 16
Using the CCA HSM utility ............................................................................................................................... 17
   Install CCA HSM ..................................................................................................................................... 17
   Launch CCA HSM ..................................................................................................................................... 17
   CCA HSM output ..................................................................................................................................... 17
   CCA-related status and master key information ....................................................................................... 17
   Coprocessor related information ............................................................................................................. 18
   Diagnostic information ........................................................................................................................... 18
   Date/time information ............................................................................................................................ 19
   Function control vector information ...................................................................................................... 19
   Profiles information ............................................................................................................................... 20
   Roles information .................................................................................................................................... 20
Troubleshooting ............................................................................................................................................. 22
   CCA BR ................................................................................................................................................. 22
   CCA HSM .............................................................................................................................................. 22
Notices .......................................................................................................................................................... 23
   Copying and distributing softcopy files ................................................................................................. 23
   Trademarks ............................................................................................................................................. 23
List of abbreviations and acronyms ............................................................................................................... 24
Index ............................................................................................................................................................ 25
Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select adapter window</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>CCA BR main window with adapter selected</td>
<td>4</td>
</tr>
<tr>
<td>3</td>
<td>Adapter menu</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>Adapter Status window with diagnostics</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>Adapter Status window with CCA status</td>
<td>6</td>
</tr>
<tr>
<td>6</td>
<td>Adapter Status window with adapter info</td>
<td>6</td>
</tr>
<tr>
<td>7</td>
<td>Backup menu</td>
<td>7</td>
</tr>
<tr>
<td>8</td>
<td>Backup select roles window</td>
<td>7</td>
</tr>
<tr>
<td>9</td>
<td>Backup select profiles window</td>
<td>8</td>
</tr>
<tr>
<td>10</td>
<td>Backup select key storage files window</td>
<td>8</td>
</tr>
<tr>
<td>11</td>
<td>Key storage file error</td>
<td>9</td>
</tr>
<tr>
<td>12</td>
<td>Backup select archive file window</td>
<td>9</td>
</tr>
<tr>
<td>13</td>
<td>Backup all window</td>
<td>10</td>
</tr>
<tr>
<td>14</td>
<td>Backup success dialog</td>
<td>10</td>
</tr>
<tr>
<td>15</td>
<td>Restore menu</td>
<td>11</td>
</tr>
<tr>
<td>16</td>
<td>Restore window</td>
<td>12</td>
</tr>
<tr>
<td>17</td>
<td>Browse selection window</td>
<td>12</td>
</tr>
<tr>
<td>18</td>
<td>Restore window with files selected</td>
<td>13</td>
</tr>
<tr>
<td>19</td>
<td>Restore profile password prompt dialog</td>
<td>13</td>
</tr>
<tr>
<td>20</td>
<td>Restore profile password confirmation dialog</td>
<td>13</td>
</tr>
<tr>
<td>21</td>
<td>Restore success dialog</td>
<td>14</td>
</tr>
<tr>
<td>22</td>
<td>CCA Init warning</td>
<td>15</td>
</tr>
<tr>
<td>23</td>
<td>CCA Init results</td>
<td>16</td>
</tr>
<tr>
<td>24</td>
<td>CCA-related status and master information</td>
<td>18</td>
</tr>
<tr>
<td>25</td>
<td>Coprocessor information</td>
<td>18</td>
</tr>
<tr>
<td>26</td>
<td>Diagnostic information</td>
<td>19</td>
</tr>
<tr>
<td>27</td>
<td>Date/time information</td>
<td>19</td>
</tr>
<tr>
<td>28</td>
<td>FCV information</td>
<td>20</td>
</tr>
<tr>
<td>29</td>
<td>Profiles information</td>
<td>20</td>
</tr>
<tr>
<td>30</td>
<td>Roles information</td>
<td>21</td>
</tr>
</tbody>
</table>
Index of Tables
Table 1 Supported hardware and software....................................................................................................2
Table 2 List of required ACPs......................................................................................................................11
About this document
This document contains information to help you use the IBM Cryptographic Common Architecture (CCA) Utilities for the IBM 4765 PCIe Cryptographic Coprocessor. These utilities include:

- CCA Backup/Restore
- CCA Test Initialization
- CCA HSM

This manual should be used in conjunction with the manuals listed under “Related publications” in this section.

Prerequisite knowledge
The reader of this book should understand how to use IBM 4765 CCA.

Typographic conventions
This publication uses the following typographic conventions:

- Commands that you enter verbatim onto the command line are presented in monospace type.
- Variable information and parameters, such as file names, are presented in italic type. Variables in commands are enclosed in <> symbols. For example:
  COMMAND parameter1 <variablename>
- Constants are presented in bold type.
- The names of items that are displayed in graphical user interface (GUI) applications, such as pull-down menus, check boxes, radio buttons, and fields, are presented in bold type.
- Items displayed within pull-down menus are presented in bold italic type.
- Function names are presented in italic type.
- System responses in a shell-based environment are presented in monospace type.
- Web addresses and directory paths are presented in italic type.
- Syntax diagrams follow these typographic conventions. Optional items appear in brackets. Lists from which a selection must be made appear in braces with vertical bars separating the choices. For example:
  COMMAND firstarg [secondarg] {a | b}
  A value for firstarg must be specified. secondarg may be omitted. Either a or b must be specified.

Related publications
Publications about IBM’s family of cryptographic coprocessors are available at:

Publications about the IBM 4765 PCIe Cryptographic Coprocessor and CCA are available at:

Various publications about cryptography are available at:

Summary of changes

This edition of IBM 4765 PCIe Cryptographic Common Architecture Backup/Restore User Guide contains product information that is current with the IBM 4765 PCIe Cryptographic Coprocessor announcements.
Overview
Starting with CCA release 4.2, a set of CCA utilities, including backup and restore, initialization, and HSM (crypto adapter) information, are available on the IBM System x® workstation release of CCA.

CCA Backup/Restore can be used to accomplish these tasks:

- Obtain diagnostic and status information about adapters that have CCA installed.
- Back up CCA roles, profiles, and keys (key storage keys) to a file on the server. Master keys are not backed up.
- Restore CCA roles, profiles, and keys (key storage keys) from a CCA backup file on the server.

Use the CCA Initialization utility to initialize CCA on the adapter for development and test.

The CCA HSM utility displays status and diagnostic information about CCA and the IBM 4765.

Each utility is described in the sections that follow.
### Supported hardware and software

Table 1 shows the set of hardware and software that is supported by the CCA utilities.

<table>
<thead>
<tr>
<th>Hardware / software</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating systems</td>
<td>With the purchase of the IBM 4765:</td>
</tr>
<tr>
<td></td>
<td>• 32-bit Novell® SUSE® Linux Enterprise Server 11 Service Pack 3 (SLES 11.3)</td>
</tr>
<tr>
<td></td>
<td>With the purchase of the IBM 4765 and the separate purchase of an add-on feature:</td>
</tr>
<tr>
<td></td>
<td>• 64-bit Novell® SUSE® Linux Enterprise Server 11 Service Pack 3 (SLES 11.3)</td>
</tr>
<tr>
<td></td>
<td>• 32-bit Red Hat Enterprise Linux 6.5 (RHEL 6.5)</td>
</tr>
<tr>
<td></td>
<td>• 64-bit Red Hat Enterprise Linux 6.5 (RHEL 6.5)</td>
</tr>
<tr>
<td>CCA</td>
<td>4.4.55, 4.4.20, and 4.4.16</td>
</tr>
<tr>
<td>Java</td>
<td>6</td>
</tr>
</tbody>
</table>
Using CCA Backup/Restore

This section contains an illustration of how to use CCA Backup/Restore to obtain diagnostic information, back up CCA information, and restore information. In this document, CCA Backup/Restore will be referred to as CCA BR.

Install CCA BR

CCA BR is installed as a part of CCA. When installing CCA, select the Custom install option and then select Smart Card Utility Programs. If you have already installed CCA without this option, run the installer again and choose Modify an Existing Instance. Select Add Features and then select Smart Card Utility Programs. Refer to the 4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual for instructions about installing CCA.

Before using CCA BR

Before you use CCA BR to back up or restore CCA information, you must ensure that your adapter has a function control vector (FCV) loaded. Use CNM to ensure that the FCV is loaded.

To launch CNM, navigate to the directory containing CNM and then run the program:

```
 cd /opt/IBM/4765/cnm
 ./csulcnm
```

Select Authorization on the Crypto Node menu. Then select Load. Choose the correct FCV file and click OK. On the verification dialog, click On the verification dialog, click Yes.

You must have an FCV loaded before launching CCA BR to back up CCA information on the originating system, and you must also have an FCV loaded before launching CCA BR to restore CCA information on the receiving system.

Launch CCA BR

To launch CCA BR, run the shell script (/opt/IBM/4765/cnm/cca_backup_restore). When it is launched, CCA BR displays its main window and prompts you to select an adapter. See Figure 1 on page 4.

Note: CCA BR must be run as root. If you run CCA BR via sudo the environment variables may not be set up correctly. CCA BR requires Java6.
Select the adapter you want to work with and then press Select. The main window is displayed as in Figure 2.

On the CCA BR main window, you can perform adapter functions, backup functions, and restore functions.

**Adapter functions**

The Adapter menu allows you to select and work with IBM 4765 adapters that have CCA loaded. See Figure 3 on page 5.
Select an adapter
To select an adapter to work with, press Select on the Adapter menu. The Select Adapter window is displayed (see Figure 1 on page 4). Select the adapter you want to work with and press OK. The CCA BR main window is displayed again. You can obtain status, back up CCA information, and restore CCA information for the selected adapter.

Obtain adapter status
Press Status on the Adapter menu. The CCA BR Adapter Status window is displayed. This window displays diagnostic, CCA, and adapter information. The first set of information is the diagnostic information. You can use this information to monitor important adapter status, including low battery warnings. See Figure 4.

To see the CCA status window, select CCA Status Info. CCA information similar to that in Figure 5 on page 6 is displayed.
Figure 5 Adapter Status window with CCA status

To see the adapter information window, select Adapter Info. Adapter information is displayed. See Figure 6 for an example.

Figure 6 Adapter Status window with adapter info
Backup functions
Before you use CCA BR to back up CCA data, ensure that the FCV is loaded. If you are unsure whether the FCV is loaded, perform these steps:

1. Launch CNM. Select Authorization on the Crypto Node menu. Then select Load. Choose the correct FCV file and click OK. On the verification dialog, click Yes.
2. Exit CCA BR (if it is running) and restart it. It must be started after the FCV is loaded.

See “Before using CCA BR” for information about loading the FCV before launching CCA BR in order to perform backup activities.

To back up CCA data, press either Selected or All on the Backup menu of the CCA BR main window. Selected backs up only the CCA data you select, while All backs up all of the CCA data for the selected adapter. This includes all roles, all profiles, and all key storage files. See Figure 7.

Figure 7 Backup menu

Backup selected information
If you chose Selected, the role selection window is displayed. See Figure 8.

Figure 8 Backup select roles window

Choose the role(s) you want to back up, and then press Next. The profile selection window is displayed as shown in Figure 9 on page 8.
Choose the profile(s) you want to back up, and then press Next. The key storage files selection window is displayed. See Figure 10.

Choose the Advanced Encryption Standard (AES), Private Key Access (PKA), and Data Encryption Standard (DES) key storage files you want to back up. You can use the browse… function to find your key storage files. Once you have selected the key storage files, press Next.

Note: If you specify a non-existent key storage directory or file, the error shown in Figure 11 will be
If there are no errors, Figure 12 will be displayed.

Figure 11 Key storage file error

Choose an appropriate location and file name for the CCA archive file and then press Save. The CCA archive will be created.

Note: You must choose a file name. The archive file will be stored in zip format. If you do not specify the .zip file extension, CCA BR will add .zip to the file name. Alternatively, you can specify it yourself. The backup also creates a .md5sum file, which contains a hash of the .zip file. This file is provided so that the authenticity of a backup can be verified at restore time. The two files must be kept separately, and not handled by the same person, to later guarantee the backup's authenticity. CCA BR assumes that the .zip and .md5sum files are in the same directory. If you browse for one file, it will try to fill in the other file name for you.

Backup all information

If you chose All on the Backup menu, the Backup All window is displayed. See Figure 13 on page 10.
Choose an appropriate location and file name for the CCA archive file and press \textit{Save}. The CCA archive will be created and a success message similar to the one in Figure 14 will be displayed.

\textbf{Figure 14 Backup success dialog}

\textbf{Restore functions}

You can use the \textit{Restore} menu to restore CCA data that was previously saved with CCA BR. This function is useful for loading a previously saved set of roles, profiles, and keys to a new adapter.

To restore a set of CCA data, your IBM 4765 adapter must be in an initialized state with a DEFAULT role that has the required access control points (ACPs) enabled and the FCV loaded. To get your adapter into this state, use CNM to initialize the adapter, check the DEFAULT role, and check the FCV. For additional information about using CNM, see Chapter 5 of the \textit{CCA Support Program Installation Manual}.

In CNM, follow these steps:

1. Select \textit{Initialize…} on the \textit{Crypto Node} menu and then press \textit{Yes}.

   \textbf{Warning:} Initializing the crypto node will completely wipe out the CCA data on the adapter, including the SRDIs, the master keys, the roles, and the profiles. Make sure you really want to do this before using the \textit{Restore} function.

2. Ensure that the DEFAULT role has the required ACPs enabled. Select \textit{Roles} on the \textit{Access Control} menu. Then press \textit{Edit} using the buttons at the bottom of the screen. Ensure that the ACPs listed in Table 2 are listed under \textit{Permitted Operations}. 
### Table 2 List of required ACPs

<table>
<thead>
<tr>
<th>Offset</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>X'0107'</td>
<td>One-Way Hash, SHA-1</td>
</tr>
<tr>
<td>X'0110'</td>
<td>Set Clock</td>
</tr>
<tr>
<td>X'0111'</td>
<td>Reinitialize Device</td>
</tr>
<tr>
<td>X'0112'</td>
<td>Initialize Access-Control System</td>
</tr>
<tr>
<td>X'0113'</td>
<td>Change User Profile Expiration Date</td>
</tr>
<tr>
<td>X'0114'</td>
<td>Change User Profile Authentication Data</td>
</tr>
<tr>
<td>X'0115'</td>
<td>Reset User Profile Logon-Attempt-Failure Count</td>
</tr>
<tr>
<td>X'0116'</td>
<td>Read Public Access-Control Information</td>
</tr>
<tr>
<td>X'0117'</td>
<td>Delete User Profile</td>
</tr>
<tr>
<td>X'0118'</td>
<td>Delete Role</td>
</tr>
<tr>
<td>X'0119'</td>
<td>Load Function-Control Vector</td>
</tr>
<tr>
<td>X'011A'</td>
<td>Clear Function-Control Vector</td>
</tr>
</tbody>
</table>

3. If any of these ACPs is not permitted, select it in the *Restricted Operations* list and press *Permit* to add it to the list of permitted operations.

4. Ensure that the FCV is loaded. Select *Authorization* on the *Crypto Node* menu. Then select *Load*. Choose the correct FCV file and click *OK*. On the verification dialog, click *Yes*.

5. Exit CCA BR (if it is running) and restart it. It must be started after the FCV is loaded in order to perform restore activities.

**Note:** Although your adapter must have an FCV loaded before you start the restore process, CCA BR will replace that FCV with the one that was saved in the archive file during the CCA BR backup procedure.

Once the adapter is in the correct state, you can start the restore process in CCA BR. Select *All* on the CCA BR *Restore* menu, as shown in Figure 15.

![Figure 15 Restore menu](image)

The *Restore* window, shown in Figure 16 on page 12, is displayed.
Use the *Browse…* function to navigate to a valid CCA backup file, which should be named `<backupfilename>.zip`. See Figure 17 for an example.

Once you locate and select the correct `.zip` file, press *Open*. The *Restore* window is filled in as shown in Figure 18 on page 13. Locate and select the matching `.md5sum` file and press *Open*.

**Note:** The `.md5sum` file contains the hash of the backup file and is used to authenticate the validity of the backup file. It should be stored and controlled separately from the `.zip` file.
Press *Restore* to finalize the data loading process. You will be prompted for the password for the profile that was saved in the archive file. For example, if the saved profile was named *tester*, you will see a prompt like the one shown in Figure 19.

![Figure 19 Restore profile password prompt dialog](image)

You will then be prompted to confirm this password. See Figure 20.

![Figure 20 Restore profile password confirmation dialog](image)

**Note:** If you restore an archive that contains more than one profile, CCA BR will prompt you to enter and...
confirm the password for each profile in the archive.
A success dialog will be displayed as shown in Figure 21.

Figure 21 Restore success dialog
Using the CCA test initialization utility

The CCA Test Initialization utility returns CCA on an IBM 4765 to an initial state.

In this document, this utility is referred to as CCA Init. It is intended to be used for development and test purposes only, not for production.

**Install CCA Init**

CCA Init is installed as a part of CCA. When installing CCA, select the *Custom install* option and then select *Smart Card Utility Programs*. If you have already installed CCA without this option, run the installer again and choose *Modify an Existing Instance*. Select *Add Features* and then select *Smart Card Utility Programs*. Refer to the *4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual* for instructions about installing CCA.

**Launch CCA Init**

To launch CCA Init, navigate to the directory containing CNM and then run the program:

```
cd /opt/IBM/4765/cnm
./cca_test_init.e [-adapter <adapternum>] [-quiet] [-overwrite_existing_data] [-help]
```

*Note:* CCA Init must be run as *root*. If you run CCA Init via *sudo* the environment variables may not be set up correctly. CCA Init requires Java6.

See Figure 22 for an example of a CCA Init invocation without any parameters.

![Figure 22 CCA Init warning](image)

To proceed, type `y` at the prompt and then press *Enter*.

If more than one IBM 4765 is installed, use `adapternum` to specify which adapter you want to initialize, starting with 0 for the first adapter in the system. To determine which adapter is which, use the CLU status command:

```
/opt/IBM/4765/clu/csulclu <logfilename> ST <adapternum>
```

The `-quiet` option turns off verbose printing of actions taken.

Specifying the `-overwrite_existing_data` option allows CCA Init to proceed without prompting you to confirm that you want all CCA data, including master keys and key storage files, to be deleted.

To see a list of the possible options, use the `-help` option.
CCA Init results

The steps performed by CCA Init are a standard set of steps you would normally have to perform manually to set up CCA for development and test activities. The CCA Init tool automates these steps for you. CCA Init removes all existing CCA setup and initializes CCA for development and test by performing these tasks:

- Initialize the adapter in the standard CCA manner.
- Expand the DEFAULT role to include all permissions.
- Create a profile named tester, with a passphrase of tester, and attach the DEFAULT role to that profile.
- Automatically set master keys for data encryption standard (DES) / public key algorithm (PKA) and for advanced encryption standard (AES).
- Load the function control vector (FCV).
- Initialize all three types of key storage: AES, DES, and PKA.

CCA Init writes its results to stdout. To retain this information to be viewed later, pipe the output to a file of your choice:

```
./cca_test_init.e > <somedirectory>/<outputfilename>
```

A sample set of results is shown in Figure 23.

![Figure 23 CCA Init results](image)

16 IBM 4765 CCA Utilities User Guide
Using the CCA HSM utility
The CCA HSM utility program lists various diagnostic and status information for the IBM 4765. This list can either be displayed in the windows in which it is run or can be piped to an output file for your convenience.

**Install CCA HSM**
CCA HSM is installed as a part of CCA. When installing CCA, select the *Custom install* option and then select *Smart Card Utility Programs*. If you have already installed CCA without this option, run the installer again and choose *Modify an Existing Instance*. Select *Add Features* and then select *Smart Card Utility Programs*. Refer to the *4765 PCIe Cryptographic Coprocessor CCA Support Program Installation Manual* for instructions about installing CCA.

**Launch CCA HSM**
To launch CCA HSM, navigate to the directory containing CNM and then run the program:
```
cd /opt/IBM/4765/cnm
./cca_hsm_util.e -F <somedirectory>/<outputfilename>
```
When it is launched, CCA HSM writes various status and diagnostic information about the IBM 4765 and CCA to the output file you specify.

**CCA HSM output**
CCA HSM contains these sets of information:

1. CCA-related status,
2. AES master key information,
3. coprocessor related,
4. diagnostic,
5. coprocessor date/time,
6. function control vector,
7. profiles, and
8. roles, including ACP data.

Note: When viewing the output from CCA HSM, make sure your file viewer does not wrap lines. If your 4765 has a large number of roles and/or profiles, the CCA HSM output can stretch across many columns.

The following sections describe the contents of the output produced by CCA HSM.

**CCA-related status and master key information**
CCA status information includes the MK register status as well as CCA version, date, and current role. A sample set of CCA status is shown in Figure 24 on page 18.
### Coprocessor related information

This information describes various hardware and version information for the IBM 4765. See Figure 25 for an example.

![Figure 24 CCA-related status and master information](image)

### Diagnostic information

This information describes the current state of the possible warning and tamper conditions in the IBM 4765 CCA Utilities User Guide.
4765.

**Note:** You should monitor the low battery warning on a regular basis; monthly at least, and preferably weekly. If this indicator is not *Normal*, you should use the battery replacement procedure to change the batteries as soon as feasible to prevent complete and unrecoverable loss of the IBM 4765 due to batteries that are too low to maintain the adapter. See the *IBM 4765-001 PCI-e Cryptographic Coprocessor Battery Replacement Instruction* manual for instructions on replacing the batteries in the IBM 4765.

A sample of the diagnostic output is in Figure 26.

```
*** Diagnostic Information ***
Battery State : Normal
Intrusion Latch State : Not Set
Error Log Status : Empty
Mesh Intrusion detected : No
Low Voltage Detected : No
High Voltage Detected : No
Temperature Range Exceeded : No
Radiation Detected : No

*** Environment Identifier ***
EID : TestEID
```

Figure 26 Diagnostic information

**Note:** It is normal to encounter an 8/1029 warning instead of the Environment Identifier. It is normal for the EID to not be set. See the *IBM CCA Basic Services Reference and Guide* for more information.

**Date/time information**
The current date and time of the IBM 4765 in Greenwich Mean Time is produced as shown in Figure 27.

```
*** Co-Processor Date/Time(GMT) ***
Year/Month/Day hour:min:sec : 2011/09/27 13:57:54
Day in week (1=sunday) : 3
```

Figure 27 Date/time information

**Function control vector information**
CCA’s function control vector (FCV) data and master key share information is displayed as shown in Figure 28 on page 20.
**Note:** It is normal to encounter an 8/1030 warning instead of the master key share information. This refers to CCA not being set up to share or clone the master key. This is normal. See the *IBM CCA Basic Services Reference and Guide* for more information.

### Profiles information

Information about the current CCA profiles for the IBM 4765 is displayed as shown in Figure 29.

![Figure 29 Profiles information](image-url)

### Roles information

Details about each role defined in the IBM 4765, including the enabled ACPs and a listing of each ACP, is displayed. See Figure 30 on page 21 for a sample listing of the first part of the results. Some details of the access control list and individual ACPs are not shown here due to the length of the output.
### List IBM 4765 Roles

**DEFAULT**

```plaintext
>>>>>>Role name : DEFAULT
Major/Minor Version: 1/0
Comment : System default role
Req. Auth Strength: 0000
Time Limits : from 00:00 to 00:00, Valid days of week : FE
Access Control List: 00 01 00 00 01 00 01 1F
                      : 00 04 00 00 01 00 FF RO
```

<table>
<thead>
<tr>
<th>Bit</th>
<th>DEFAULT</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0107</td>
<td>ON</td>
<td>0107 One-Way Hash, SHA-1</td>
</tr>
<tr>
<td>0110</td>
<td>ON</td>
<td>0110 Set Clock</td>
</tr>
<tr>
<td>0111</td>
<td>ON</td>
<td>0111 Reinitialize Device</td>
</tr>
<tr>
<td>0112</td>
<td>ON</td>
<td>0112 Initialize Access-Control System</td>
</tr>
<tr>
<td>0113</td>
<td>ON</td>
<td>0113 Change User Profile Expiration Date</td>
</tr>
<tr>
<td>0114</td>
<td>ON</td>
<td>0114 Change User Profile Authentication Data</td>
</tr>
<tr>
<td>0115</td>
<td>ON</td>
<td>0115 Reset User Profile Logon-Attempt-Failure Count</td>
</tr>
<tr>
<td>0116</td>
<td>ON</td>
<td>0116 Read Public Access-Control Information</td>
</tr>
<tr>
<td>0117</td>
<td>ON</td>
<td>0117 Delete User Profile</td>
</tr>
<tr>
<td>0118</td>
<td>ON</td>
<td>0118 Delete Role</td>
</tr>
<tr>
<td>0119</td>
<td>ON</td>
<td>0119 Load Function-Control Vector</td>
</tr>
<tr>
<td>011A</td>
<td>ON</td>
<td>011A Clear Function-Control Vector</td>
</tr>
</tbody>
</table>

**Figure 30 Roles information**
Troubleshooting

CCA BR

This section contains various troubleshooting tips and techniques that may be useful when working with CCA BR.

- When you back up CCA information to an archive, if you encounter an error stating that all key storage files must be specified, it means either you specified a directory or a key storage file that does not exist. You can use the Browse… button to locate key storage files. The default installation directory is /opt/IBM/4765/keys.

- When you restore CCA from an archive, if you encounter an error stating that the selected adapter contains non-default roles, profiles, or keys, it means that your adapter is not in a “clean” initial state that can receive a restored set of CCA information. To wipe out your existing roles, profiles, and keys, use CNM to initialize the adapter and to add the required ACPs to the DEFAULT CCA role. See “Restore functions” on page 10 for detailed instructions. Once these steps are complete, use CCA BR to restore the archived CCA information to the initialized adapter.

- When you restore CCA from an archive, if you encounter an error stating that the ACPs are not found, it means that your DEFAULT role does not have the required ACPs enabled to perform the restore action. To add the required ACPs, use CNM to edit the DEFAULT role. See “Restore functions” on page 10 for details about editing the DEFAULT role to enable the required ACPs.

- When you restore CCA from an archive, if you encounter an error stating that a key storage file is not writable, it means the host system user ID you are using does not have the necessary authority to update the key storage files. Switch user IDs or obtain write authority to the key storage directories and retry the restore operation.

- When you restore CCA from an archive, you must be able to enter the password for every profile that was backed up to that archive.

- If the list of available CCA profiles does not contain a profile that you are sure is attached to a role that has the correct ACPs enabled, make sure that the profile name contains only printable characters. It is possible to create a profile or role in CCA that contains unprintable characters in its name, but the CCA utilities do not support profiles or roles with these characters in them.

- Before you launch CCA BR to back up or restore CCA information, you must have an FCV loaded. See “Before using CCA BR” on page 3 for instructions or refer to Chapter 5 of the CCA Support Program Installation Manual for additional information.

- If you encounter permissions issues, use CNM to ensure that the X’001D’ and X’0230’ are permitted in the DEFAULT role. Exit and re-launch CCA BR.

CCA HSM

Errors and warnings in the output displayed by CCA HSM can give you information about the health of the IBM 4765 and CCA. Some possible warnings are listed below.

- It is normal to encounter an 8/1029 warning, which refers to the EID. It is normal for the EID to not be set. See the IBM CCA Basic Services Reference and Guide for more information.

- It is normal to encounter an 8/1030 warning, which refers to CCA not being set up to share or clone the master key. This is normal. See the IBM CCA Basic Services Reference and Guide for more information.
Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights or other legally protectable rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, programs, or services, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, 500 Columbus Avenue, Thornwood, NY, 10594, USA.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

Copying and distributing softcopy files

For online versions of this document, we authorize you to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine readable documentation.

Trademarks

The following terms are registered trademarks of the IBM Corporation in the United States and/or other countries or both:

IBM
System x

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACP</td>
<td>Access Control Point</td>
<td>FCV</td>
<td>Function Control Vector</td>
</tr>
<tr>
<td>AES</td>
<td>Advanced Encryption Standard</td>
<td>HSM</td>
<td>Hardware Security Module</td>
</tr>
<tr>
<td>CCA</td>
<td>Common Cryptographic Architecture</td>
<td>IBM</td>
<td>International Business Machines Corporation</td>
</tr>
<tr>
<td>CCA BR</td>
<td>CCA Backup/Restore utility</td>
<td>MK</td>
<td>Master Key</td>
</tr>
<tr>
<td>CCA HSM</td>
<td>CCA hardware security module utility</td>
<td>PCIe</td>
<td>Peripheral Component Interconnect Express</td>
</tr>
<tr>
<td>CCA Init</td>
<td>CCA initialization utility</td>
<td>PDF</td>
<td>Portable Document Format</td>
</tr>
<tr>
<td>CNM</td>
<td>Cryptographic Node Management utility</td>
<td>PKA</td>
<td>Private Key Access</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
<td>SLES</td>
<td>SUSE Linux Enterprise Server</td>
</tr>
</tbody>
</table>
Index

abbreviations .....................................................24
adapter functions ...............................................4
adapter, electing ...............................................5
backing up CCA data .........................................7
backup ...................................................................3
before using .......................................................3
  CCA BR ..........................................................3
CCA backup ........................................................3
CCA BR troubleshooting ...................................22
CCA HSM coprocessor status..........................18
CCA HSM date/time .........................................19
CCA HSM diagnostics ......................................18
CCA HSM FCV data .........................................19
CCA HSM output .............................................17
CCA HSM profiles ..........................................20
CCA HSM roles ...............................................20
CCA HSM troubleshooting ................................22
CCA Init results .................................................16
CCA restore .......................................................3
CCA status ........................................................17
hardware and software, supported .....................2
installing .............................................................
  CCA BR ..........................................................3
  CCA HSM .....................................................17
  CCA Init ........................................................15
launching ...........................................................
  CCA BR ..........................................................3
  CCA HSM .....................................................17
  CCA Init ........................................................15
master key data .................................................17
obtaining status ...............................................5
overview .............................................................
prerequisite knowledge .....................................vi
related publications ..........................................vi
notices ..................................................................23