RSA® Certificate Manager 6.9 build 566 Readme

This document lists what is new and changed in RSA Certificate Manager 6.9 build 566 (Certificate Manager). It includes installation information, as well as information about the fixed issues and the known issues. Read this document before installing the software.

For the complete Certificate Manager documentation set, go to the Certificate Manager page on RSA Link or contact RSA Customer Support.

Contents:

New Features

There are no new features in this release of Certificate Manager.

Enhanced Functionality

This release of Certificate Manager is designed to include the following:

- Embedded component GNU tar 1.13.25 replaced with libarchive bsdtar 3.3.3.
- Embedded components upgraded to the latest secure version: RSA BSAFE Micro Edition Suite 4.1.6.1.
- Fixes for specific issues. For more information, see Fixed Issues.

Package Contents

The Certificate Manager package for this hotfix release is designed to contain the following:

- `RSACM-v6.9build566r-package.zip`, for systems running a Windows operating system
- `RSACM-v6.9build566r-solaris-package.tar`, for systems running a Solaris operating system
- `RSACM-v6.9build566r-linux-package.tar`, for systems running a Red Hat Enterprise Linux operating system
- `RSACM-v6.9build566r-SuSE-linux-package.tar`, for systems running a SUSE Linux operating system
- Product documentation consisting of this *Readme* document in Portable Document Format (PDF).

Note: In the event of a discrepancy, this *Readme* document takes precedence over the *RSA Certificate ManagerAdministrators Guide*, the *RSA Certificate Manager Vettor's Guide*, the *RSA Certificate Manager Installation Guide*, and the Help information.

Installation

You must perform all the tasks in the "Preparing to Install" section in the "Installing Certificate Manager" chapter of the *RSA Certificate Manager Installation Guide*, before installing the hot fix files for this release.

Install the Full Build

To install the full build of Certificate Manager, use the appropriate file from this package. On systems running a:

- Windows operating system, use `RSACM-v6.9build566r-WIN32.zip`.

  Note: During Certificate Manager installation, install the Microsoft Visual C++ 2013 Redistributable Package by agreeing to the Microsoft Software License Terms.

- Solaris operating system, use `RSACM-v6.9build566r-sparc-sun-solaris.tar`.

  Note: Take the following actions if this error occurs: `ld.so.1: httpsd: fatal: libgcc_s.so.1: open failed: No such file or directory`

  – Set `LD_LIBRARY_PATH` to the location of `libgcc_s.so.1`
  `export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/<path to libgcc_s.so.1>`

  – Re-install Certificate Manager.

- Red Hat Linux operating system, use `RSACM-v6.9build566r-linux.tar`.
- SUSE Linux operating system, use `RSACM-v6.9build566r-SuSE_linux.tar`.

For full instructions on how to install Certificate Manager, see the *RSA Certificate Manager Installation Guide*.

Install the Hot Fix Files

This section describes how to install the hot fix files. Instructions to install the hotfix files on the following platforms are provided:

- Windows Operating System
- Solaris or Linux Operating Systems.

Note: The hot fix files can be installed on any previous Certificate Manager 6.9 installation.

Windows Operating System

This hotfix does not require a new installation of the product, but rather a drop-in replacement of files into the appropriate Certificate Manager directory and updating the Help.

To apply Certificate Manager 6.9 build 566:

1. Stop all Certificate Manager services.
2. Extract the files from `SSLC_CryptoCME_Libs-WIN32.zip` provided with this drop-in package.
3. Replace the following files located at `\WINDOWS\system32` (for Windows 32-bit operating system) or `\Windows\SysWOW64` (for Windows 64-bit operating system) with the ones in the unzipped folder:
   - `ccme_base.dll`
   - `ccme_ecc.dll`
   - `ccme_eccaccel.dll`
   - `cryptocme2.dll`
   - `cryptocme2.sig`
4. Create a backup of the Certificate Manager installation directory.
5. Copy `RSACM-v6.9build566r-dropin-WIN32.zip` to the installation directory.
6. Extract the files from the zip file, ensuring the new files replace the old files.

   Note: If you modified any xuda templates in your Certificate Manager installation, you must make those modifications again.

   Note: If you are upgrading from Certificate Manager 6.9 build551 or later, skip Step 7.

7. Update the Help information. In the `<INSTALL_DIR>\WebServer\admin-server\ca\help` directory, extract the files from `rcm-help.zip`, ensuring the new files replace the old files.
8. If you are upgrading from:
   - Certificate Manager 6.9 build 559 or earlier, go to Step 9.
   - Certificate Manager 6.9 build 560, complete steps 9.f, 9.g, 9.h, 9.i and 10.b, then go to Step 12.
   - Certificate Manager 6.9 build 561 or 562, complete steps 9.f, 9.g and 9.h, and then go to Step 13.
   - Certificate Manager 6.9 build 563 or later, complete steps 9.f, 9.g and 9.h, and then go to Step 14.

9. Create a backup of `<INSTALL_DIR>\WebServer\Conf\httpd.conf` and edit the file as follows:

   a. Add the following line for virtual hosts of Administration, Enrollment and Renewal Server above the `SSLCipherSuite` directive to disable SSLv2 and SSLv3:

   ```
   SSLProtocol all -SSLv2 -SSLv3
   ```

   b. For each virtual host of Administration, Enrollment, and Renewal servers, update the `SSLCipherSuite` directive as follows:

   ```
   SSLCipherSuite EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:
      AES256-SHA:EDH-DSS-AES128-SHA:EDH-RSA-AES128-SHA:
      AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:
      DES-CBC3-SHA
   ```

   c. Comment the following line:

   ```
   SSLSessionCache none
   ```

   d. Uncomment the following line:

   ```
   SSLSessionCache dbm:logs/ssl_scache
   ```

   e. Uncomment the following line:

   ```
   SSLSessionCacheTimeout 300
   ```

   f. If HTTPS support CMP messages is enabled, add the following line before the `ServerName` directive under the `RSA CMP Enroll Server configuration` virtual host section:

   ```
   DocumentRoot "<INSTALL_DIR>\WebServer\cmp"
   ```

   g. If Restful WebService is enabled, add the following line before the `ServerName` directive under the `RSA Rest Server configuration` virtual host section:

   ```
   DocumentRoot "<INSTALL_DIR>\WebServer\rcm"
   ```

   h. Search for *IfModule mod_alias.c*.

   Under the directive `<Directory <INSTALL_DIR>\WebServer\icons>`, change **Options Indexes MultiViews** to **Options None**.

   i. Under `RSA CM SCEP server configuration`, add the following lines after `SSL_PKI_PORT`:

   ```
   #verify the signature of certificate responses, '1' for
      verify '0' for disable
   VerifySignature 1
   ```

10. Create a backup of `<INSTALL_DIR>\Xudad\conf\xudad.conf` and edit the file as follows:

    a. Add the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

    ```
    SSLProtocol "all -SSLv2 -SSLv3"
    ```

b. Add the following line above the `crypto_providers` directive to verify signatures after signing operations are complete:

```
verifysignature 1
```

Note: RSA recommends setting `verifysignature` to 1, or any other non-zero value, to verify signatures after signing. Setting `verifysignature` to 0 leaves the Secure Directory Server prone to the Lenstra side-channel Attack Vulnerability.

11. Create a backup of `<INSTALL_DIR>\LogServer\conf\xslogconf.xml` and edit the file to add the following line after the `ServerSSLKey` configuration parameter to disable SSLv2 and SSLv3:

```
<CONFIG_PARAM>
   <!--
   This parameter specifies the SSLProtocol that are allowed
   for the SSL connection. This protocol is used to set up
   secure communications with clients connecting to the
   logging server.
   Default: None, this file must exist.
   -->
   <PARAM_NAME> SSLProtocol </PARAM_NAME>
   <PARAM_VALUE> all -SSLv2 -SSLv3 </PARAM_VALUE>
</CONFIG_PARAM>
```

12. Update the CMP Configuration file.

    a. Stop the CMP Server.

    b. Edit `<INSTALL_DIR>\CmpServer\conf\cmp.conf` and after the `usecmpssltosign` directive, add the following:

```
verifysignature=1
```

Note: If you are upgrading from Certificate Manager 6.9 build 563 or later, skip Step 13.

13. Install the Microsoft Visual C++ 2013 Redistributable Package on the target machines.

    The Redistributable Package executable file, `vcredist_x86.exe`, is in the `<INSTALL_DIR>\Utils` folder.

14. Open `<INSTALL_DIR>\WebServer\conf\httpd.conf` and complete the following edits:

    a. Uncomment the following line:

```
LoadModule headers_module modules/mod_headers.so
```

    b. Search for *ErrorLog logs/enroll-cipher.log* under **RSA Enrollment Server configuration**. Add the following lines below the *ErrorLog* directive:

```
Header always set X-Frame-Options DENY
Header set Content-Security-Policy "frame-ancestors 'none';"
```

c. Search for *ErrorLog logs/admin-cipher.log* under **RSA Administration Server configuration**. Add the following lines below the *ErrorLog* directive:

```
Header always set X-Frame-Options SAMEORIGIN
Header set Content-Security-Policy "frame-ancestors 'self';"
```

d. Search for *ErrorLog logs/renewal-cipher.log* under **RSA Renewal Server configuration**. Add the following lines below the *ErrorLog* directive:

```
Header always set X-Frame-Options DENY
Header set Content-Security-Policy "frame-ancestors 'none';"
```

15. Start all Certificate Manager services.

Note: If you are upgrading from Certificate Manager 6.9 build 563 or later, skip Step 16.

16. Under System Configuration, click LDAP Rules and search for the following:

```
# This rule allows Enrollment server and SCEP server read access and
# Admin server write access to the xuda_config object.
access to dn="CN=Config"
```

and append the following line:

```
by dn="md5=<cmpservercert md5>" read
```

Note: If you are upgrading from Certificate Manager 6.9 build 560 or later, skip Step 17.

17. Update the profile and the schema of the directory server.
See Update the Profile and the Schema of the Directory Server.

Note: If you are upgrading from Certificate Manager 6.9 build 555 or later, Step 18 to Step 20 are not required.

18. Enable the HTTPS support for CMP messages.
See Enable the HTTPS support for CMP messages.

19. Update the CMP Configuration file.

a. Stop the CMP Server.

b. Edit `<INSTALL_DIR>\CmpServer\conf\cmp.conf` and after the `usecmpssltosign` directive, add the following directives:

- `report_counter_frequency` and specify the value in seconds.
- `iteration_count` and specify 2048 or some other numeric value to a maximum of 8192.
- `timeoutbuffer`, and specify the value in seconds.
- `verifysignature=1`.

Note: If you are using the 3gpp plug-in, then continue from step c, otherwise go to step d.

c. Edit `<INSTALL_DIR>\CmpServer\conf\ss.dat` and after the `whitelist_file` directive, add the following directives:

- `blacklist_file=filename` where filename is the name of the XML file that contains the list of CN values against which the requestor's CN is checked. If CN present in XML file CMP request will rejected.
- `cntocheck=1` or `2` or `3`. The default value is 0.To verify the CN value in the Sender field of the header and body of a CMP request.
- `addcapubs=0` or `1`. To include the certificate chain of the issuing CA either in the caPubs field(1) or in the extraCerts field(0) of the CMP response.
- `verifyVPKI=true` or `false`. Whether to process the certificate enrollment request if sender certificate details are not present in the extraCerts.
- `verifyUniqueSubject=0` or `1`. To enable (`1`) or disable (`0`) unique subject name checking.

d. Start the CMP Server.

20. Enable the Restful webservice. See the instructions at Enable Restful Webservices.

Solaris or Linux Operating Systems

This hotfix does not require a new installation of the product, but rather a drop-in replacement of files into the appropriate Certificate Manager directory and updating the Help.

To apply RSA Certificate Manager 6.9 build 566:

1. Stop all Certificate Manager services.
2. Extract the files from the appropriate tar file provided with this drop-in package. On systems running a:
   - Red Hat Linux operating system, `SSLC_CryptoCME_Libs-RH_Linux.tar`
   - SUSE Linux operating system, `SSLC_CryptoCME_Libs-SuSE_Linux.tar`
   - Solaris operating system, `SSLC_CryptoCME_Libs-sparc-sun-solaris.tar`.
3. Replace the following files located at **/usr/lib** with the ones in the untarred folder:
   - `libccme_base.so`
   - `libccme_ecc.so`
   - `libccme_eccaccel.so`
   - `libcryptocme2.so`
   - `libcryptocme2.sig`

Note: Make sure that you logon as the root user and give proper permissions to the users to access the library files.

4. Create a backup of the Certificate Manager installation directory.
5. Copy the appropriate tar file to the installation directory. On systems running a:
   - Solaris operating system, use `RSACM-v6.9build566r-dropin-sparc-sun-solaris.tar`.
   - Red Hat Linux operating system, use `RSACM-v6.9build566r-dropin-linux.tar`.
   - SUSE Linux operating system, use `RSACM-v6.9build566r-dropin-SuSE_linux.tar`.
6. Extract the files from the tar file, ensuring the new files replace the old files.

   Note: If you are upgrading from Certificate Manager 6.9 build 551 or later, skip stepStep 7.

7. Update the Help information, in the `<INSTALL_DIR>/WebServer/admin-server/ca/help` directory, extract the files from `rcm-help.tar` ensuring the new files replace the old files.
8. Ensure the permissions and ownership of the extracted files match the permissions and ownership of other files in the same directories.

   For example, the files in the `/WebServer` directory must be readable by the user and/or group under which the server runs. If you encounter permission problems, change the ownership of the files in the `<INSTALL_DIR>/WebServer` directory to the user and group under which the Certificate Manager Web Server was installed.

   From the `<INSTALL_DIR>` directory, enter:

   ```
   chown -R <install_user>:<install_group> WebServer
   ```

   Note: If you modified any xuda templates in your Certificate Manager installation, you must make those modifications again.

9. If you are upgrading from:
   - Certificate Manager 6.9 build 559 or earlier, go to Step 10
   - Certificate Manager 6.9 build 560, complete steps 10.f, 10.g, 10.h, 10.i, and 11.b, then go to Step 13
   - Certificate Manager 6.9 build 561 or later, complete steps 10.f, 10.g, and 10.h, then go to Step 14.
10. Create a backup of `<INSTALL_DIR>/Web Server/conf/httpd.conf` and edit the file as follows:
    a. Add the following line for virtual hosts of Administration, Enrollment and Renewal Server above the `SSLCipherSuite` directive to disable SSLv2 and SSLv3:

       ```
       SSLProtocol all -SSLv2 -SSLv3
       ```

b. For each virtual host of Administration, Enrollment, and Renewal servers, update the `SSLCipherSuite` directive as follows:

```
SSLCipherSuite EDH-DSS-AES256-SHA:EDH-RSA-AES256-SHA:
   AES256-SHA:EDH-DSS-AES128-SHA:EDH-RSA-AES128-SHA:
   AES128-SHA:EDH-DSS-DES-CBC3-SHA:EDH-RSA-DES-CBC3-SHA:
   DES-CBC3-SHA
```

c. Comment the following line:

```
SSLSessionCache none
```

d. Uncomment the following line:

```
SSLSessionCache shm:logs/ssl_scache(512000)
```

e. Uncomment the following line:

```
SSLSessionCacheTimeout 300
```

f. If HTTPS support CMP messages is enabled, add the following line before the `ServerName` directive under the `RSA CMP Enroll Server configuration` virtual host section:

```
DocumentRoot "<INSTALL_DIR>/WebServer/cmp"
```

g. If Restful WebService is enabled, add the following line before the `ServerName` directive under the `RSA Rest Server configuration` virtual host section:

```
DocumentRoot "<INSTALL_DIR>/WebServer/rcm"
```

h. Search for *IfModule mod_alias.c*.

Under the directive `<Directory <INSTALL_DIR>/WebServer/icons>`, change **Options Indexes MultiViews** to **Options None**.

i. Under `RSA CM SCEP server configuration`, add the following lines after `SSL_PKI_PORT`:

```
#verify the signature of certificate responses, '1' for
   verify '0' for disable
VerifySignature 1
```

11. Create a backup of `<INSTALL_DIR>/Xudad/conf/xudad.conf` and edit the file as follows:

a. Add the following line above the `cipherlist` directive to disable SSLv2 and SSLv3:

```
SSLProtocol "all -SSLv2 -SSLv3"
```

b. Add the following line above the `crypto_providers` directive to verify signatures after signing operations are complete:

```
verifysignature 1
```

Note: RSA recommends setting `verifysignature` to 1, or any other non-zero value, to verify signatures after signing. Setting `verifysignature` to 0 leaves the Secure Directory Server prone to the Lenstra side-channel Attack Vulnerability.

12. Create a backup of `<INSTALL_DIR>/LogServer/conf/xslogconf.xml` and edit the file to add the following line after the `ServerSSLKey` configuration parameter to disable SSLv2 and SSLv3:

```
<CONFIG_PARAM>
   <!--
   This parameter specifies the SSLProtocol that are allowed
   for the SSL connection. This protocol is used to set up
   secure communications with clients connecting to the
   logging server.
   Default: None, this file must exist.
   -->
   <PARAM_NAME> SSLProtocol </PARAM_NAME>
   <PARAM_VALUE> all -SSLv2 -SSLv3 </PARAM_VALUE>
</CONFIG_PARAM>
```

13. Update the CMP Configuration file.

    a. Stop the CMP Server.

    b. Edit `<INSTALL_DIR>/CmpServer/conf/cmp.conf` and after the `usecmpssltosign` directive, add the following:

    ```
    verifysignature=1
    ```

14. From the `<INSTALL_DIR>` directory, enter the following:

    ```
    chmod 755 Utils
    ```

15. Open `<INSTALL_DIR>\WebServer\conf\httpd.conf` and complete the following edits:

    a. Uncomment the following line:

    ```
    LoadModule headers_module modules/mod_headers.so
    ```

    b. Search for *ErrorLog logs/enroll-cipher.log* under **RSA Enrollment Server configuration**. Add the following lines below the *ErrorLog* directive:

    ```
    Header always set X-Frame-Options DENY
    Header set Content-Security-Policy "frame-ancestors 'none';"
    ```

    c. Search for *ErrorLog logs/admin-cipher.log* under **RSA Administration Server configuration**. Add the following lines below the *ErrorLog* directive:

    ```
    Header always set X-Frame-Options SAMEORIGIN
    Header set Content-Security-Policy "frame-ancestors 'self';"
    ```

    d. Search for *ErrorLog logs/renewal-cipher.log* under **RSA Renewal Server configuration**. Add the following lines below the *ErrorLog* directive:

    ```
    Header always set X-Frame-Options DENY
    Header set Content-Security-Policy "frame-ancestors 'none';"
    ```

16. Start all Certificate Manager services.

Note: For systems running the Solaris 10 operating system, take the following actions if this error occurs: `ld.so.1: httpsd: fatal: libgcc_s.so.1: open failed: No such file or directory`

– Set `LD_LIBRARY_PATH` to the location of `libgcc_s.so.1`
```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/<path to libgcc_s.so.1>
```

– Restart the services.

Note: If you are upgrading from Certificate Manager 6.9 build 563 or later, skip Step 17.

---

17. Under System Configuration, click LDAP Rules and search for

```
# This rule allows Enrollment server and SCEP server read access and
# Admin server write access to the xuda_config object.
access to dn="CN=Config"
```

and append the line

```
by dn="md5=<cmpservercert md5>" read
```

Note: If you are upgrading from Certificate Manager 6.9 build 560 or later, skip Step 18.

---

18. Update the profile and the schema of the directory server.
See Update the Profile and the Schema of the Directory Server.

Note: If you are upgrading from Certificate Manager 6.9 build 555 or later, Step 19 to Step 21 are not required.

---

19. Enable HTTPS support for CMP messages.
See Enable the HTTPS support for CMP messages.
20. Update the CMP Configuration file:
    a. Stop the CMP Server.
    b. Edit file located at `<INSTALL_DIR>/CmpServer/conf/cmp.conf` and after the `usecmpssltosign` directive, add the following directives:
        - `report_counter_frequency` and specify the value in seconds.
        - `iteration_count` and specify 2048 or some other numeric value to a maximum of 8192.
        - `timeoutbuffer`, and specify the value in seconds.
        - `verifysignature=1`.
    c. If you are using the 3gpp plug-in, then continue from step (d), otherwise go to step (e).

d. Edit `<INSTALL_DIR>/CmpServer/conf/ss.dat` and after the `whitelist_file` directive, add the following directives:

- `blacklist_file=filename` where filename is the name of the XML file that contains the list of CN values against which the requestor's CN is checked. If CN present in XML file CMP request will rejected.
- `cntocheck=1` or `2` or `3`. The default value is 0.To verify the CN value in the Sender field of the header and body of a CMP request.
- `addcapubs=0` or `1`. To include the certificate chain of the issuing CA either in the caPubs field(1) or in the extraCerts field(0) of the CMP response.
- `verifyVPKI=true` or `false`. Whether to process the certificate enrollment request if sender certificate details are not present in the extraCerts.
- `verifyUniqueSubject=0` or `1`. To enable (`1`) or disable (`0`) unique subject name checking.

e. Start the CMP Server.

21. Enable the Restful webservice. For instructions see Enable Restful Webservices.

Update the Profile and the Schema of the Directory Server

To update the profile and the schema:

1. Make sure that all Certificate Manager services are running.
2. If you use the internal database (Berkeley DB), go to Step 6.
3. If you use Sun ONE Directory Server, to update the schema:
   a. Copy `69rcm-sun-one-schema.ldif` into the Sun ONE Directory Server's Server schema directory, `/<SunOne_install_Directory>/Sun/MPS/slapd_<system_name>/config/schema/`, where `system_name` is the computer hostname.
   b. Restart the directory server.
4. If you are using Microsoft ADAM or Active Directory, to update the schema:
   a. Go to **ADAM ADSI EDIT** and expand the schema. Locate an entry similar to `CN=Schema,CN=Configuration,CN={GUID}`
   b. For example: `CN=Schema,CN=Configuration,CN={C3D7C1A9-DCC8-496D-94E3-513B4465AA62}`
   c. Copy `CN={GUID}`.

d. At the **ADAM Tools Command Prompt**, enter the following:

```
ldifde -i -f "ActiveDirectory Schema file path" -s
servername:portnumber -k -j . -c "dc=company,dc=com"
"CN={GUID}"
```

The parameters are described in the following table.

Parameter	Description
ActiveDirectory Schema file path	The path to **69b555to69b558rcm-active-directory-schema-update.ldif.** **Note:** If upgrading from Certificate Manager 6.9 build 553 or later, update the schema using `69b553to69b558rcm-active-directory-schema-update.ldif`. Otherwise, update the schema using `69rcm-active-directory-schema-update.ldif` and `69b553to69b558rcm-active-directory-schema-update.ldif`.
Sever Name	The name of the computer on which ADAM is installed.
Port Number	The LDAP communications port of the ADAM instance.
CN={GUID}	The data that you copied; for example, `CN={C3D7C1A9-DCC8-496D-94E3-513B4465AA62}`.

e. Restart the services of ADAM instances.

5. If using AD LDS, see Install and Configure AD LDS to work with Certificate Manager.

   Note: If you are upgrading from Certificate Manager 6.9 build 555 or later, go to step 7.

6. In Certificate Manager, go to **`https://hostname:admin-port/ca/admin/updateprofiles6.9.xuda`**.

   The certificate extension profiles are updated.

7. Go to **`https://hostname:admin-port/ca/admin/schemaUpdate.xuda`**.

   The schema is updated.

8. Restart the Certificate Manager services.

Install and Configure AD LDS to work with Certificate Manager

Before you install AD LDS, ensure that Microsoft .NET Framework 3.5.1 is installed on your machine.

To configure Certificate Manager for High Availability with AD LDS:

1. Create an instance of AD LDS, or use an existing installation of AD LDS.
2. Update the AD LDS schema.
3. Import the converted Certificate Manager data.

To install an AD LDS instance and a partition:

1. Open the AD LDS Set up Wizard.
   a. Select **Start** > **Server Manager** > **Roles** > **Add Roles** > **Active Directory Lightweight Directory Services**.
   b. Select **Start** > **Administrative Tools** > **Active Directory Lightweight Directory Services Setup Wizard**.
2. Create an AD LDS instance.
   a. Select **A unique instance**.
   b. Give the instance a name, for example, **RSA-CM**.
   c. Unless another application is using **389** and **636**, accept the default ports.
   d. Select **Yes, create an application directory partition**, and give it a name, for example, DC=rsa,DC=com.

      This DN is the basedn you enter in the **plugin.conf** file in Certificate Manager.
   e. Accept the default file locations.
   f. Accept the default, **Network service account**, for permissions.
   g. For AD LDS administrators, select **Currently logged on user**.
   h. Select **Import the selected LDIF files for this instance of AD LDS**, and add all the files to the schema.

      You require these files to add users.
   i. On the Ready to Install page, verify if the information is correct, and click **Next**.
3. After installation, start **ADSI Edit**.
4. Configure the connections to this AD LDS partition.
   a. Highlight **ADSI Edit**.
   b. Select **Action** > **Connect to**.
   c. Enter a connection name.

d. Under the **Connection point** section, select the option **Select or enter a Distinguished name (DN) or Naming Context:**, and enter the partition name, for example, `DC=rsa,DC=com`.

   This is the basedn you enter in the `plugin.conf` file in Certificate Manager.

e. Under the **Computer** section, select **Select or enter a domain or server: (Server | Domain [:port])**, and enter the server name and port number in this format: `<server name>:<port>`

f. Click **OK**.

5. Create a container for users.

   a. Click **Action** > **New** > **Object**, and select **organizationalUnit** to create an organizational unit under the application directory partition.

   b. Specify a name for the organizational unit. If you name it **users**, in the previous example, the DN is OU=users,DC=rsa,DC=com.

6. Create a new user to bind to AD LDS using LDAP.

   a. Click **Action** > **New** > **Object**, and select **user**.

   b. Specify a name for the user. If you use the name **CMAdministrator**, in the previous example, the DN is CN=CMAdministrator,OU=users,DC=rsa,DC=com.

      This is the binddn that you enter in the `plugin.conf` file in Certificate Manager.

7. Set a password for the user created in the previous step.

   a. Right-click the user name, and select **Reset password**.

   b. Enter a password and confirm the same.

      This is the bindpw that you enter in the `plugin.conf` file in Certificate Manager.

8. Activate the user's account.

   a. Right-click the user, and select **Properties**.

   b. Select **msDS-UserAccountDisabled** in the list, and click **Edit**.

   c. Select **False**, and click **OK**.

9. Make the user an AD LDS administrator for the partition.

   a. Click **CN=Roles**.

   b. Right-click **CN=Administrators**, and select **Properties**.
   In the previous example, the DN of the Administrators group is CN=Administrators,OU=users,DC=rsa,DC=com.

   c. In the Attribute Editor, select the **member** attribute, and click **Edit**.

   d. Click **Add DN**.

e. Enter the DN of the user you want to make the administrator.
In the previous example, the DN of this user is `CN=CMAdministrator,OU=users,DC=rsa,DC=com`.

f. Apply the changes.

To update the AD LDS schema:

1. Obtain the GUID for the schema partition:
   a. Start **ADSI Edit**.
   b. Highlight **ADSI Edit**.
   c. Select **Action** > **Connect to**.
   d. Enter a connection name, for example, schema.
   e. Leave the server name as localhost.
   f. Unless you selected a different port during installation, accept the default port number of **389**.
   g. Click **Select a well known naming context** and, from the drop-down list, select **Schema**.
   h. Connect through the account of the currently logged-on user.
   i. Click **OK**.
   j. Expand the new connection.

      The schema naming context is the final entry in the DN **CN=Schema,CN=Configuration,CN={GUID}**.

      The DN looks similar to the following example: `CN=Schema,CN=Configuration,CN={29A13F57-4526-4912-89B9-C13879CA6280}`.
   k. Copy **CN={GUID}**.
2. Open the Command Prompt, and enter:

   ```
   C:\Windows\System32>ldifde.exe -i -f
   <pathname>\69rcm-active-directory-schema.ldif
   -s <servername>:<portnumber> -k -j
   -c "dc=company,dc=com" "cn={<GUID>}"
   ```

   where:

   – `pathname` is the location where you stored the schema update file.
   – `servername` is the name of the computer on which AD LDS is installed.
   – `portnumber` is the LDAP communications port of the AD LDS instance.
   – `cn={<GUID>}` is the data you copied in Step 1; for example, `CN={CE656C6E-4B25-4E6B-BAB8-19B3116B84B2}`
3. Press **Enter**.

   When the file is imported, a confirmation message is displayed.

To import the converted Certificate Manager data:

1. Ensure that you have entered the AD LDS partition name in the `basedn` in the **plugin.conf** file in Certificate Manager.
2. From the Command Prompt, enter the following:

   ```
   C:\Windows\System32>ldifde.exe -i -f
   <pathname>\rcm-converted.ldif -s
   <servername>:<portnumber> -k -j
   ```

   where:

   - `pathname` is the location where you stored the converted data file.
   - `rcm-converted.ldif` is the file that you have created while setting up the first instance of Certificate Manager. For more information, see "Installing and Configuring RSA Certificate Manager for High Availability" in the "High Availability" chapter, in the *Installation Guide*.
   - `servername` is the name of the computer on which AD LDS is installed.
   - `portnumber` is the LDAP communications port of the AD LDS instance.
3. Press **Enter**.

   When the file is imported, a confirmation message is displayed.

Enable the HTTPS support for CMP messages

Note: If you are upgrading from Certificate Manager 6.9 build 555 or later, the following steps are not required.

After installing the hot fix files you must reissue a copy of the Enrollment Server certificate to generate the SSL certificate, `cmpenroll.cert`, and the private key, `cmpenroll.key`. The SSL certificate and the private key are required to send and receive CMP messages over HTTPS.

To enable the HTTPS support for CMP messages:

1. Copy `<INSTALL_DIR>/WebServer/ssl/certs/enroll.cert` and rename the copied file to `cmpenroll.cert`.

   However, if you are upgrading from an earlier version to Certificate Manager 6.9 build555, skip to Step 3.
2. Copy `<INSTALL_DIR>/WebServer/ssl/private/enroll.key` and rename the copied file to `cmpenroll.key`.
3. Reissue the `cmpenroll.cert` certificate.
   a. On the Certificate Manager Administrative Console, click **Administrator Operations**.
   b. Under **Server Certificates**, click **Re-issue**.
   c. Select an **Issuer** and a **Jurisdiction** to sign the SSL keys.

d. Select **Internal Certificates**, and from the drop-down list, select the server certificate, `WebServer\ssl\certs\cmpenroll.cert`

e. Click **Next**.

The Reissue Server Certificate page opens.

The new validity period, subject DN components, and server key algorithm for the server certificate are populated from the old certificate. Modify these values if required.

f. Select **Generate New Key Pair**.

g. Click **Re-Issue**.

4. Edit `<INSTALL_DIR>/Webserver/conf/httpd.conf` and add the following lines in the CMP Enroll Server Configuration section:

```
SSLEngine on
SSLVerifyClient none
SSLVerifyDepth 10
SSLCipherSuite DES-CBC3-SHA
SSLProtocol all -SSLv2 -SSLv3
# Private key for the server (for browser requests)
SSLCertificateKeyFile <Path of cmpenroll.key file>
# Signed certificate for the server (for browser requests)
SSLCertificateFile <Path of cmpenroll.cert file>
```

5. (Optional) To enable client authentication, modify the lines added in the previous step as follows:

```
SSLEngine on
SSLVerifyClient require
SSLVerifyDepth 10
SSLCipherSuite DES-CBC3-SHA
SSLProtocol all -SSLv2 -SSLv3
# Private key for the server (for browser requests)
SSLCertificateKeyFile <Path of cmpenroll.key file>
# Signed certificate for the server (for browser requests)
SSLCertificateFile <Path of cmpenroll.cert file>
SSLCACertificateFile <file path of PEM-encoded CA
Certificates for Client Auth>
```

6. Restart all Certificate Manager services.

Enable Restful Webservices

Note: If you are upgrading from Certificate Manager 6.9 build 555 or later, the following steps are not required.

After installing the hotfix files you must reissue a copy of the Enrollment Server certificate to generate the SSL certificate, `restServer.cert`, and the private key, `restServer.key`.

To enable Restful interface:

1. Copy `<INSTALL_DIR>/WebServer/ssl/certs/enrollServer.cert` and rename the copied file to **restServer.cert**.
2. Copy `<INSTALL_DIR>/WebServer/ssl/private/enroll.key` and rename the copied file to **restServer.key**.
3. Reissue the `restServer.cert` certificate.
   a. On the Certificate Manager Administrative Console, click **Administrator Operations**.
   b. Under **Server Certificates**, click **Re-issue**.
   c. Select an **Issuer** and a **Jurisdiction** to sign the SSL keys.
   d. Select **Internal Certificates**, and from the drop-down list, select the server certificate, `WebServer/ssl/certs/restServer.cert`
   e. Click **Next**.

      The Reissue Server Certificate page opens.

      The new validity period, subject DN components, and server key algorithm for the server certificate are populated from the old certificate. Modify these values if required.
   f. Select **Generate New Key Pair**.
   g. Click **Re-Issue**.
4. Edit `<INSTALL_DIR>/Webserver/conf/httpd.conf` and add the following lines at the end of file.

```
##############################################
###  RSA Rest Server configuration         ###
##############################################

###
# The following VirtualHost for a non-secure Web Server
###
Listen <port>

<VirtualHost _default_:<port>>
DocumentRoot "<INSTALL_DIR>/WebServer/rcm"
ServerName <hostname>
<Location /rcm>
SetHandler  rcm
</Location>

ErrorLog    logs/rest-error.log
```

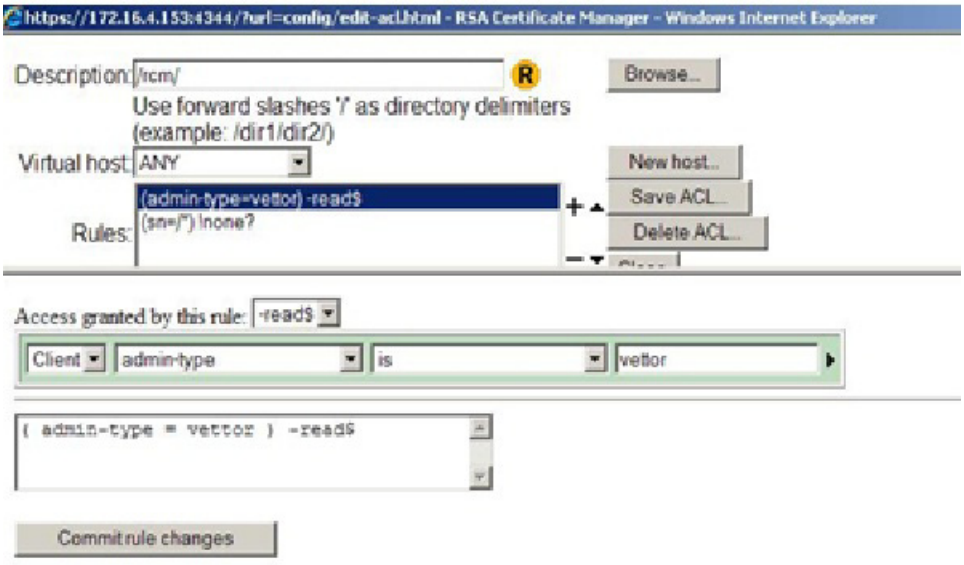
```
SSLEngine on
SSLVerifyClient require
SSLVerifyDepth  10

#   SSL Cipher Suite:
#   List the ciphers that the client is permitted to negotiate.
#   See the mod_ssl documentation for a complete list.
SSLCipherSuite AES256-SHA
SSLProtocol all -SSLv2 -SSLv3

#   Server Certificate:
SSLXudaCertificateFile <Path of admin.cert file>

#   Server Private Key:
SSLXudaCertificateKeyFile <Path of admin.key file>

# Private key for the server (for browser requests)
SSLCertificateKeyFile <Path of restServer.key file>

# Signed certificate for the server (for browser requests)
SSLCertificateFile <Path of restServer.cert file>

SSL_PKI_Host <hostname of Xudad>
SSL_PKI_Port <port of Xudad>

PerformStatusCheck
PerformACLCheck
DenyAccessIfACLRulesNotFound

XACL_PKI_Host   <hostname of Xudad>
XACL_PKI_Port   <port of Xudad>

</VirtualHost>

#########################################################
###   End of RSA Rest Server configuration         ###
#########################################################
```

5. Add a new Web ACL rule object for Rest.
   a. Click **System Configuration**.
   b. Under **Web ACLs**, click **Create ACL**.
   c. In the top panel of the ACL editor, in the Description field enter `/rcm/`.
   d. In the Virtual host field, select **ANY**.

e. Use the graphical rule editor or the rule string editor to add the following rules to the newly created ACL object as shown in the following figure.

```
( admin-type = vettor ) -read$
( sn = /* ) !none?
```

For instructions on creating or editing ACL rules, see the *RSA Certificate Manager Administrators Guide*.



f. Click **Save ACL**.

6. Restart all Certificate Manager Services.

Regenerate System Keys

Note: The following are general steps to regenerate the system keys from hardware to software. The steps are not specific to Certificate Manager 6.9 build 566, and are applicable to any previous versions of Certificate Manager.

To regenerate system keys:

1. On the Certificate Manager Administrative Console, click **Administrator Operations**.
2. Under **Re-key**, click **Regenerate System Keys**.

   For more information, see "Generating New System Authority and SSL Keys" in the *RSA Certificate Manager Administrators Guide*.
3. After regeneration of the system keys, stop the Certificate Manager services.
4. Backup `cmpenroll.cert` and `crsSigner.cert` in the `<INSTALL_DIR>/WebServer/ssl/certs` directory.
5. Backup `cmpenroll.key` and `crsSigner.key` in the `<INSTALL_DIR>/WebServer/ssl/private directory`.
6. Copy `<INSTALL_DIR>/WebServer/ssl/certs/enrollServer.cert` and rename the copied file to `cmpenroll.cert`.
7. Copy `<INSTALL_DIR>/WebServer/ssl/certs/enrollServer.cert` and rename the copied file to `crsSigner.cert`.
8. Copy `<INSTALL_DIR>/WebServer/ssl/private/enrollServer.key` and rename the copied file to `cmpenroll.key`.
9. Copy `<INSTALL_DIR>/WebServer/ssl/private/enrollServer.key` and rename the copied file to `crsSigner.key`.
10. Restart the Certificate Manager services.
11. On the Certificate Manager Administrative Console, click **Administrator Operations**.
12. Under **Server Certificates**, click **Re-issue**.
13. Select an Issuer and a Jurisdiction to sign the SSL keys.
14. Select **Internal Certificates** and from the drop-down list, select `WebServer\ssl\certs\cmpenroll.cert` as the server certificate.
15. Click **Next**.

    The **Reissue Server Certificate** page opens.

    The new validity period, subject DN components, and server key algorithm for the server certificate are populated from the old certificate. Modify these values as required.
16. Select **Generate New Key Pair**.

17. Click **Re-Issue**.
18. Repeat steps 11 to 16 to re-issue `crsSigner.cert`, choosing `WebServer\ssl\certs\crsSigner.cert` as the certificate from the drop-down list.
19. Restart the Certificate Manager services.

Fixed Issues

This section lists the issues fixed in this release of Certificate Manager: .

Table 1 Fixed Issues

ID	Description
CERTMGR-4722	RSA BSAFE Micro Edition Suite 4.1.6.1 is updated to resolve the following vulnerabilities: • An integer overflow vulnerability. (CVE-2018-11054) • An Improper Clearing of Heap Memory Before Release, *Heap Inspection,* vulnerability. (CVE-2018-11055) • An Uncontrolled Resource Consumption, *Resource Exhaustion*, vulnerability when parsing ASN.1 data. (CVE-2018-11056) • A Covert Timing Channel vulnerability during RSA decryption, also known as a Bleichenbacher attack on RSA decryption. (CVE-2018-11057) • A Buffer Over-Read vulnerability when parsing ASN.1 data. (CVE-2018-11058)
CERTMGR-4721	Improper Restriction of Rendered UI Layers or Frames, *Click Jacking*, vulnerability. Certificate Manager is susceptible to a Click Jacking vulnerability in Enrollment Server, Renewal Server and Administration Server. A remote attacker could exploit this vulnerability by routing them to another page. This release is designed to resolve the Click Jacking vulnerability.
CERTMGR-4718	The GNU tar distributed with Windows versions of Certificate Manager is vulnerable to a Path Traversal vulnerability. This release is designed to resolve the Path Traversal vulnerability.

For the list of issues fixed in previous releases, see the appropriate Readme documents.

Known Issues

The following table describes the issues that remain unresolved in this release. Wherever a workaround or fix is available, it is noted or referenced in detail.

Table 2 Known Issues

ID	Description
CERTMGR-4706	Internet Explorer 11 on Microsoft Windows 10 intermittently fails to send the client certificate for authentication to the Administration Server causing SSL handshake failure. **Workaround:** Upgrade the Windows 10 operating system to Windows 10 version 1709. Alternately, clear the SSL cache on Internet Explorer 11 by going to **Tools -> Internet Options -> Content -> Clear SSL State**, and then restart the browser and access the Administrative interface again.
CERTMGR-4588	The `RestClient` utility does not support TLS 1.2 during SSL communication.
CERTMGR-4587	The `CMPHttpClient` utility does not support TLS 1.2 during SSL communication.
CERTMGR-4586	The `healthcheck.pl` utility does not support TLS 1.2 during SSL communication.
CERTMGR-4485	Installation of Certificate Manager with hardware SSL keys and System Authority keys using nCipher client version 11.70 fails with the following message: `Warning! Can't find <directory>httpd.pid to confirm httpsd is running!` The default location of the domain sockets used for communication with the hardserver was changed from `/dev/nfast` to `/opt/nfast/sockets`. Applications trying to find the sockets in their old location assume the server is not running and then fail. **Workaround:** Create a file, `/etc/nfast.conf`, with `NFAST_CREATEDEVNFAST=1` in it and then restart the hardserver. This causes the hardserver to create a symlink to the current socket directories in their old location.

Table 2 Known Issues (Continued)

ID	Description
CERTMGR-4461, CERTMGR-4443, CERTMGR-4232	On systems running a Windows operating system, installation of Certificate Manager with hardware SSL keys using Luna SA client v5.x fails. **Workaround:** Install Certificate Manager with hardware SSL keys using Luna SA client v5.x: 1. Install Luna SA Client software. 2. Create the directory `C:\Program Files\LunaG5`. 3. Copy `crystoki.ini` from `C:\Program Files\SafeNet\LunaClient` to `C:\Program Files\LunaG5`. 4. Configure Luna SA client. 5. Install Certificate Manager (selecting `crytoki.dll` from `C:\Program Files\SafeNet\LunaClient\win32`).
CERTMGR-4433	On systems running the Red Hat Enterprise Linux 6.4 or later operating system, Certificate Manager logs incorrect information in syslog. **Workaround:** Update `rsylog.conf` as follows: 1. Login in as root user where Certificate Manager is installed. 2. Stop the rsyslog service using the following command: `service rsyslog stop` 3. Edit /etc/rsyslog.conf and add the following line at the end of the file: `$EscapeControlCharactersOnReceive off` 4. Start the rsyslog service using the following command: `service rsyslog start` 5. Restart all Certificate Manager services.
CERTMGR-4409	While vetting the certificate requests using Internet Explorer 10 on a system running Windows 2008 R2, extensions cannot be selected from Mandatory Extensions and Available Extensions list. **Workaround:** Upgrade to Internet Explorer 11.
CERTMGR-4295	When a non-persistent card is inserted, then the Administration Server is not accessible if SSL keys are protected with nCipher HSM. **Workaround:** Set `CKNFAST_NONREMOVABLE=1` in the`cknfastrc` file and restart the nCipher services.
CERTMGR-4186	When installing Certificate Manager on a system running the Windows 2008 operating system (32-bit and 64-bit), the Media Verify utility crashes, although the Media Sign utility works. **Workaround:** Install Certificate Manager on a system running the Windows 2003 operating system, and run the Media Sign and Media Verify utilities.

Table 2 Known Issues (Continued)

ID	Description
CERTMGR-4034	On systems running a Linux operating system, Certificate Manager will not function properly if the system time is changed to beyond the year 2038. According to the rfc2459 “Internet X.509 Public Key Infrastructure” section 4.1.2.5, CAs conforming to this profile MUST always encode certificate validity dates through the year 2049 as UTCTime; certificate validity dates in 2050 or later MUST be encoded as GeneralizedTime. In Certificate Manager, the certificate validity TIME is stored in the following UTCTime format: YYMMDDHHMMSSZ. Certificate Manager only supports certificates with validity up to year 2050.
REGMGR-327	Unable to install renewed certificate on Microsoft Internet Explorer 9 or later on Windows 7 64-bit. The error code is 80004005. **Workaround:** Add the Enrollment Server to the list of Trusted Sites.
REGMGR-322	Registration Manager 6.8 does not work with Certificate Manager 6.9 build 553 or later. **Workaround:** Registration Manager must be upgraded to the same version as Certification Manager.

Support and Service

Access these locations for help with your RSA product:

- RSA Link

  RSA Link offers a knowledge base that contains answers to common questions and solutions to known problems. It also offers information on new releases, important technical news, and software downloads.

- RSA Customer Support

  The RSA Customer Support site on RSA Link contains information on RSA support programs plus an extensive Content Library of product-related documents such as datasheets, guides and whitepapers.

- RSA Ready

  The RSA Ready Community is a platform for customers, partners, and RSA enthusiasts to learn about products certified to interoperate with RSA products including access to integration guides.

Before You Call Customer Support

Make sure you have direct access to the computer running your RSA product software.

Please have the following information available:

- ❑ Your RSA Customer Serial Number.
- ❑ The software version number of your RSA product.
- ❑ The make and model of the machine on which the problem occurs.
- ❑ The name and version of the operating system under which the problem occurs.