BMC Software

BMC Provisioning Module for RSA Authentication Manager

RSA Secured Implementation Guide
Administrative Interoperability

Last Modified: June 27, 2010

Partner Information

Product Information	
Partner Name	BMC Software
Web Site	http://www.bmc.com
Product Name	BMC Provisioning Module for RSA Authentication Manager
Version & Platform	5.0.00 (Windows, Solaris and AIX)
Product Description	BMC Provisioning Module for RSA Authentication Manager allows BMC Identity Enterprise SecurityStation administrators to provision RSA Authentication Manager users, groups and RSA SecurID tokens.
Product Category	Provisioning

Solution Summary

This document contains detailed information about the BMC Provisioning Module version 5.0.00 for RSA Authentication Manager, which enables BMC Identity Enterprise SecurityStation to perform provisioning operations on RSA Authentication Manager managed systems. The provisioning module's deployment environment includes the following components:

BMC Provisioning Module (PM): The BMC Provisioning Module for RSA Authentication Manager is designed to interact with RSA Authentication Manager 7.1 (the managed system). The primary task of this module is to translate the information sent from BMC Identity Enterprise SecurityStation through the services manager and pass it to the managed system using RSA Authentication Manager API calls.

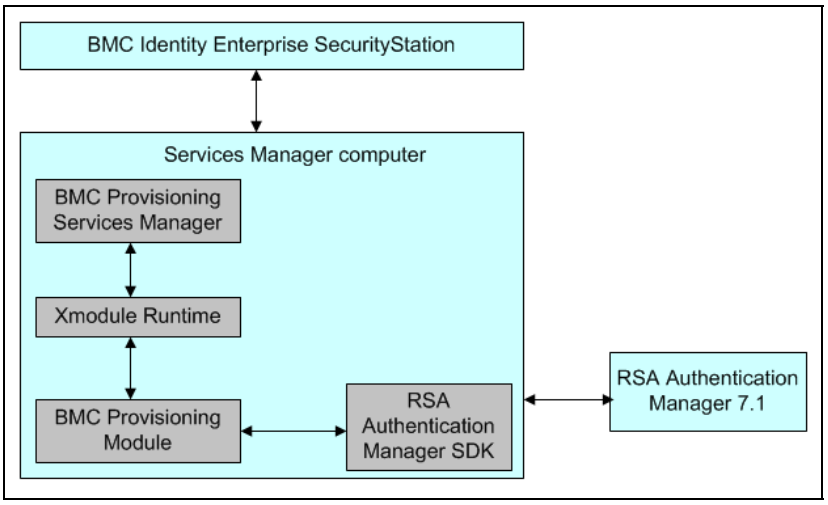
BMC Provisioning Services Manager (SM): This component is an interface between the provisioning module and BMC Identity Enterprise SecurityStation. The services manager receives transaction requests from BMC Identity Enterprise SecurityStation and passes them to the provisioning module. Messages from the module to BMC Identity Enterprise SecurityStation are passed using the callable services provided by the services manager.

XModule Runtime: The Provisioning Module for RSA Authentication Manager was developed using the BMC Identity XModule Studio. The module uses X-Module framework APIs from the following classes*:

- XSA_Framework
- XSA_FrameworkBase
- XSA_Connector

RSA Authentication Manager: RSA Authentication Manager is the management component of the RSA SecurID two-factor authentication solution. It is used to verify authentication requests and administer authentication policies for enterprise networks.

RSA Authentication Manager 7.1 SDK: The RSA Authentication Manager 7.1 SDK contains the RSA Authentication Manager API.



The deployment diagram above illustrates the relationships between the system's components.

* See the *BMC Provisioning Module Administrator Guide for RSA Authentication Manager* and XModule Studio documentation for more details about the framework API.

The module's functionality can be divided into the following groups of transactions between BMC Identity Enterprise SecurityStation and RSA Authentication Manager:

Provisioning Transactions: The module's provisioning transactions are initiated from within BMC SecurityStation and allow administrators the ability to:

- Create/Manage/Delete RSA Authentication Users
- Define RSA Authentication Manager Groups
- Add/Remove Users to/from Groups
- Enable/Disable/Assign/Unassign User Tokens
- Define User Passwords
- Change Users' Authentication Methods
- Define General Managed System Parameters

Reconciliation Transactions: The module's reconciliation transactions use BMC's Standard Offline Interceptor (SOFFI) component to synchronize data between BMC Identity Enterprise SecurityStation and RSA Authentication Manager. SOFFI determines if any changes have been made to RSA data by anything other than the module's provisioning transactions and the Service Manager updates BMC SecurityStation data as necessary. The configuration and use of reconciliation transactions are outside of the scope of this document. For details about the reconciliation transactions, see the *BMC Provisioning Module Administrator Guide for RSA Authentication Manager.*

BMC Identity Enterprise SecurityStation - RSA Authentication Manager Overview	
Support for Standard Card, Key Fob, PINPAD, and SoftID	Yes
Add a user to the RSA Authentication Manager Database	Yes
Modify user information	Yes
Assign a token	Yes
Un-assign a user's token	Yes
Delete a user from the RSA Authentication Manager Database	Yes
Clear/Reset a token's PIN	Yes
Enable a token	Yes
Disable a token	Yes
Change User Authentication Method (PASSCODE or Tokencode)	Yes
Reconcile RSA Authentication Manager data with the User Management database	Yes

Note: This is a subset of the module's functionality. A full list and description of the module's features as well as instructions on how to use these features are outside of this document's scope. See the *BMC Provisioning Module Administrator Guide for RSA Authentication Manager* or visit http://www.bmc.com/support **for additional information.**

Product Requirements

Partner Product Requirements: BMC Provisioning Module for RSA Authentication Manager	
Resource	**Requirement**
CPU	BMC Provisioning Module for RSA Authentication Manager operates on any hardware configuration supported by any of the relevant configurations (for example, Intel Pentium and AMD64 processor).
Memory	The amount of physical memory required by the provisioning module depends on the amount of RSA Authentication Manager data that will be managed.
Storage	1 GB

Operating System
Visit http://www.bmc.com/support for a list of supported platforms and required patches.

Additional Software Requirements	
Application	**Requirement**
BMC Identity Enterprise SecurityStation (ESS) version 7.5.00 or later.	BMC Identity Enterprise SecurityStation (ESS) version 7.5.00 or later is required for this integration.
RSA Authentication Manager 7.1 SDK SP3	RSA Authentication Manager 7.1 SDK SP3 should be installed on the provisioning module's host.
Java Development Kit (JDK) 1.5	Sun Java Development Kit (JDK) 1.5 should be installed on the provisioning module's host.

Note: Consult RSA and BMC documentation for a complete list of requirements and supported platforms.

Partner Product Configuration

This section provides instructions for integrating RSA Authentication Manager resources into the BMC Provisioning Services Manger environment. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of BMC Provisioning Services Manager, RSA Authentication Manager and their respective components, as well as the ability to perform the tasks outlined in this section. Administrators should have access to the relevant product documentation in order to install, configure and use these products.

BMC Provisioning Services Manger and RSA Authentication Manager must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

The variables below appear throughout the guide and should be replaced with their corresponding values:

Variable Name	Description
CACERTS_KEYSTORE_PASSWORD	The password for Java's system-wide keystore, cacerts; its default value is "**changeit"**.
JAVA_HOME	The Java JDK's root directory on the RSA Authentication Manager host
RSA_AM_HOME	The RSA Authentication Manager server's installation directory
SDK_HOME	The RSA Authentication Manager SDK's root directory
SERVER_NAME	The RSA Authentication Manager host name
WEBSPHERE_HOME	The IBM WebSphere application server's installation directory
SERVICE_MANAGER_HOME	The BMC Provisioning Services Manager's installation directory

Pre-Installation

This section contains instructions that may need to be performed before installing the module, depending on the state of the host environment. It is divided into the following subsections:

- **Obtain and Install the RSA Authentication Manager 7.1 SP3 SDK**
- **Install Java 1.5**
- **Enable Secure Communication Between the Connector and the Server's API**
- **Define Provisioning Module Administrators**
- **Test the Environment**

Obtain and Install the RSA Authentication Manager 7.1 SP3 SDK

The RSA Authentication Manager 7.1 SDK SP3 is not included with the provisioning module, and it must be obtained from RSA Security and installed before the module can be configured. Contact RSA Security for details about downloading a copy of the SDK and instructions to install it. Ensure that it has been installed on the BMC Provisioning Services Manager host before proceeding.

Important: The RSA Authentication Manager 7.1 SP3 SDK is not included with the provisioning module and must be obtained from RSA Security and installed on the BMC Provisioning Services Manager host machine.

Install Java 1.5

Sun Java Development Kit (JDK) 1.5 must be installed on the provisioning module's host. Follow the steps below to do so:

1. Ensure that RSA Authentication Manager is running and that its Admin Console is accessible.
2. Download and install JDK 1.5. Go to http://java.sun.com/j2se/ for more information.
3. Set the *JAVA_HOME* environment variable to the directory in which JDK 1.5 was installed.
4. Set the *PATH* environment variable to the *JAVA_HOME*/*bin*.
5. Open a command prompt on the Authentication Manager server's host, go to the *RSA_AM_HOME/appserver/weblogic/server/lib* directory and enter the following command:

```
java –jar ../../../modules/com.bea.core.jarbuilder_1.0.0.0.jar -profile
wlfullclient
```

6. Locate the following files and copy each one to the *SDK_HOME*/lib/java directory on the client host:
   - *RSA_AM_HOME/appserver/license.bea*
   - *RSA_AM_HOME/appserver/modules/com.bea.core.process_5.3.0.0.jar*
   - *RSA_AM_HOME/appserver/weblogic/server/lib/wlfullclient.jar*
   - *RSA_AM_HOME/appserver/weblogic/server/lib/wlcipher.jar*
   - *RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoAsn1.jar*
   - *RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoCore.jar*
   - *RSA_AM_HOME/appserver/weblogic/server/lib/EccpressoJcae.jar*

Enable Secure Communication Between the Connector and the Server's API

During the RSA Authentication Manager installation process, the system creates a self-signed root certificate and stores it in *RSA_AM_HOME/server/security/SERVER_NAME.jks*. Before the connector can use the RSA Authentication Manager APIs to communicate with the server, the certificate must be exported from this directory and imported into a keystore for the module. Perform the following procedures to enable this server – connector communication:

- **Export the Server Root Certificate**
- **Import the Server Root Certificate**
- **Set the Command Client's Username and Password**

Export the Server Root Certificate

Run the **keytool** utility to export the RSA Authentication Manager server's root certificate as follows:

1. Open a command prompt on the server's host, go to the *RSA_AM_HOME/appserver* directory and enter the following command:

```
jdk/jre/bin/keytool -export -keystore
RSA_AM_HOME/server/security/SERVER_NAME.jks -file am_root.cer
-alias rsa_am_ca
```

2. When prompted for the keystore password, leave the password field empty and press ***Enter***. Ignore the warning message displayed by the keytool.

Import the Server Root Certificate

In order to import RSA Authentication Manager's root certificate into the API client's keystore:

1. Locate the RSA Authentication Manger root certificate file that was exported in the previous section and copy it to the target provisioning module's host computer.

2. Change directories to *JAVA_HOME/jre/bin* and enter the following command:

```
keytool -import -keystore SDK_HOME/lib/java/trust.jks -storepass
CACERTS_KEYSTORE_PASSWORD -file am_root.cer -alias rsa_am_ca
-trustcacerts
```

Note: The default cacerts keystore password is "changeit".

Set the Command Client User Name and Password

During the RSA Authentication Manager installation process, the system creates a user name and password to secure connections to the API command server. These credentials are randomly generated and unique to each deployment. As such, each client must have its corresponding set of credentials to establish a command server connection.

To obtain the command client user name and password from RSA Authentication Manager:

1. Open a command prompt on the RSA Authentication Manager host, change directories to *RSA_AM_HOME/utils* and enter the following command:

```
rsautil manage-secrets --action list
```

2. When prompted, type the master password, and the system will display the list of internal system passwords.

3. Locate the command client user name and password. For example:

```
Command Client User Name ..................: CmdClient_vKr9aLK9
Command Client User Password ..............: e9SHbK0W4i
```

Each username and password pair will be needed for the associated client to connect to the command server. See the Configure MSCS Parameters section for more details.

Important: Do not change the command client user name or password.

Define Provisioning Module Administrators

The following three administrator user accounts must be created before installing the provisioning module. Each of these accounts is required to contain the **Auth Mgr Realm Admin Role**:

- **The Default Administrator Account**
- **The Unattended Administrator Account**
- **The Managed System Administrator Account**

> **Note: Each of the following administrator accounts must contain the Auth Mgr Realm Admin Role.**

A Default Administrator Account - The Services Manager uses the Default Administrator Account to perform operations in the Managed System. The user name and password for this account is specified during installation. The Default Administrator must be an administrator who has been assigned the **Auth Mgr Realm Admin** administrative role.

Unattended Administrator Account - BMC Identity Enterprise SecurityStation uses the Unattended Administrator Account to change Managed System users' passwords during password synchronization. The user name and password for this account is specified in the BMC Identity Enterprise SecurityStation when setting up the Managed System. The Unattended Administrator must be an administrator who has been assigned the **Auth Mgr Realm Admin** administrative role.

Managed System Administrator Account - The Managed System administrator account is used to perform administrative functions in RSA Authentication Manager (e.g. adding users, assigning tokens, etc.) during provisioning transactions. The user name and password for this account is specified in BMC Identity Enterprise SecurityStation when setting up the Managed System. The Managed System Administrator must be an administrator with Auth Mgr Realm Admin administrative role assigned to it.

See the *BMC Provisioning Module Administrator Guide for RSA Authentication Manager* for more information about these accounts including instructions on how to troubleshoot connection errors.

Test the Environment

The BMC Provisioning Module installation CD includes a utility called testpm.jar, which can be used to verify that the module's environment has been configured properly. Before beginning the installation process, follow the instructions below to run this utility:

1. Copy testpm.jar and bmcrsa.properties from the *Install* directory on the installation CD to the RSA Authentication Manager SDK's *java* directory (SDK_HOME/lib/java).

2. Change directories to SDK_HOME/lib/java and edit the bmcrsa.properties file to provide values for the following properties:

   - *java.naming.provider.url = t3s://<the fully qualified host name of the RSA Authentication Manager Server host>:7002*
   - *com.rsa.cmdclient.user* = <the command client *username* >
   - *rsa.portal.user = <the user name provided during RSA Authentication Manager installation an RSA Authentication Manager administrator's user name>*

   For example:

   - *java.naming.provider.url = t3s://rsa-sec-vmsvrv2.secvmsvr02dc.local:7002*
   - *com.rsa.cmdclient.user = CmdClient_vKr9aLK9*
   - *rsa.portal.user = dheadley*

3. Execute the following command to confirm that the JAVA version is 1.5.0_11:

```
java -version
```

4. Change to the SDK_HOME/lib/java directory and enter the following commands:

```
java -Dbea.home="SDK_HOME/lib/java"
-Dweblogic.security.SSL.trustedCAKeyStore="SDK_HOME/lib/java/trust.jks" -
jar testpm.jar
```

5. Enter the command client user password when prompted.

6. Enter password for the portal user specified in the *bmcrsa.properties file* when prompted. If the utility displays the RSA Authentication Manager instance name, the environment has been set up correctly.

7. Exit the command window.

Installation

This section contains instructions for installing the BMC Provisioning Module for RSA Authentication Manager. It is divided into the following subsections:

Install the BMC Provisioning Services Manager

Install BMC Provisioning Services Manager if it has not already been installed. See the appropriate guide from the following list for installation procedures:

- *BMC Provisioning Services Manager Installation Guide for Microsoft Windows*
- *BMC Provisioning Services Manager Installation Guide for Solaris*
- *BMC Provisioning Services Manager Installation Guide for AIX*

Add the BMC Provisioning Module for RSA Authentication Manager

1. For instructions on how to add a BMC Provisioning Module, see the appropriate installation guide from the list above.

2. After the module has been installed, the installer will display the **Finish Provisioning Module Setup** dialog box. Select **Yes** to configure the Managed System Configuration Set (MSCS) parameters and click **Finish**.

3. For AIX installations only, set the *LIBPATH* environment variable as follows:

```
setenv LIBPATH
SERVICE_MANAGER_HOME/PM/3rd_party/JRE-
1.5.00/bin/j9vm:SERVICE_MANAGER_HOME/PM/3rd_party/JRE-1.5.00/bin
```

Note: The following step only applies to AIX installations.

Configure MSCS Parameters

Use the BMC Provisioning Services Manager Administration Console to configure the managed system's MSCS parameters. See the *BMC Provisioning Services Manager Administrator Guide* for details. The module's mandatory parameters are described in the table below:

BMC Provisioning Module for RSA Authentication Manager's Mandatory MSCS Parameters		
Parameter	**Description**	**Values**
ATTACH_DLL	Enter the name of the provisioning module DLL. By default, the name is built using the MSCS_PM_DLL_TMPL template.	Default: **BmcXagCTSAdapter.dll**
COMMAND_CLIENT_USER	Enter the command client username.	
COMMAND_SERVER_URL	Enter the command server URL. This is the java.naming.provider.url property's value in the bmcrsa.properties file.	
CONTEXT_FACTORY_CLASS	Enter the JNDI factory class.	Default: **weblogic.jndi.WLInitialContextFactory**
DEFAULT_ADMIN	Enter the Default Administrator's username.	
IDENTITYSOURCE_NAME	Enter the name of the RSA Authentication Manager identity source.	Default: **Internal Database**
MSCS_NAME	Enter a name that represents the RSA Authentication Manager Server that the module will manage. This name must be specified in BMC Identity Enterprise SecurityStation when the managed system is defined.	The MSCS name cannot be longer than 12 characters.
RealmDomain_Name	Enter the name of the RSA Authentication Manager Security Domain	Default: **System Domain**

The table below describes the module's optional parameters:

BMC Provisioning Module for RSA Authentication Manager's Optional MSCS Parameters		
Parameter	**Description**	**Values**
DESCRIPTION	Enter a description for the managed system.	
MAX_CONN	Enter the number of RSA Authentication Manager connections to request in each call.	Default: ***5***
MAX_GROUPS	Enter the number of RSA Authentication Manager groups to request in each call.	Default: ***10***
MAX_USERS	Enter the number of RSA Authentication Manager users to request in each call.	Default: ***10***

Modify the Provisioning Module Parameters

Follow the steps below to modify the provisioning module's parameters:

1. Launch the Services Manager Administration Console:
   - For Windows installations, select **Start →Programs →BMC Provisioning →Services Manager →** <instance name> **→SM Administration Console**.
   - For Solaris and AIX, run the *SMAdmin*.sh script.
2. Select **AceServer** in the left pane and click **PM Parameters** in the Services in the console.
3. Replace every occurrence of "External Library Path" in the parameter value column with *SDK_HOME/lib/java.*
4. Click **Add Parameter** and add the following parameter value pairs:

PM Parameter	Value
XSA_JVM_OPTION_0	**-Dbea.home="C:/sdk/lib/java"**
XSA_JVM_OPTION_1	**-Dweblogic.security.SSL.trustedCAKeyStore="C:/sdk/lib/java/trust.jks"**
XSA_JVM_OPTION_2	**-Xms=256m**
XSA_JVM_OPTION_3	**-Xmx=1024m**

Note: In the table above, *SDK_HOME* is *C:\sdk* and the *trust.jks* keystore is located in the *C:\sdk\lib\java* directory.

5. Click **Save** and exit the console.

Store the User Name and Password

The provisioning module requires a user name and password to establish a connection with RSA Authentication Manager. A JAVA utility named *pm-security.jar* can be used to store these values in a file named *data.xml*, where the provisioning module can retrieve them at runtime.

Follow the instructions below to store the username and password

1. Execute the *java – version* command to confirm that the correct version of JAVA has been installed. The command should display the information in the figure below.

```
C:\>java -version
java version "1.5.0_11"
Java(TM) 2 Runtime Environment, Standard Edition (build 1.5.0_11-b03)
Java HotSpot(TM) Client VM (build 1.5.0_11-b03, mixed mode, sharing)

C:\>
```

2. Navigate to the *SERVICE_MANAGER_HOME\PM\AceServer\bin\third_party* directory and execute the following command:

   java -jar pm-security.jar MSCS_NAME Name AceServer

   replace *MSCS_NAME* with the value entered in the **Configure MSCS Parameters** section.

   Note: If the MSCS name contains special characters, enter the name in double-quotation marks. For example: "RSAAM-1".

3. Enter *1* when prompted and add the command client username.

   Note: If the command client username changes, re-run the utility, choose option *2* and enter the new username.

4. Enter the command client password when prompted.

Add the Default Administrator

A BMC Provisioning Services Manager utility named *ctsadm* must be run to create the Default Administrator. See the *BMC Provisioning Services Manager Administrator Guide* for instructions and add the Default Administrator before proceeding.

Import the Managed System Type Definition

A file named *DBexport.AceServer.TAR* must be imported into BMC Identity Enterprise SecurityStation so the module's managed system can be identified as RSA Authentication Manager. For instructions on importing a managed system type definition into BMC Identity Enterprise SecurityStation, see the description of the *instrss* utility in the *BMC Identity Enterprise SecurityStation Administration Guide*.

Post-Installation

After completing the installation procedure, perform the following steps to ensure that the provisioning module runs smoothly and successfully:

- Set the value of the *OFLI_INTERVAL* parameter to **000000** in *MSCSPARM.PRM* file.
- Perform the **Download Operation** from BMC Identity Enterprise SecurityStation.
- Run the **Standard Offline Interceptor** in *initial mode* for each RSA Authentication Manager Managed System.
- Perform the **Global Sync Operation** from BMC Identity Enterprise SecurityStation.
- (Optional) Set the *OFLI_INTERVAL* parameter to a non-zero value.

For comprehensive information about these tasks, as well as information about installing and configuring the BMC Provisioning Module for RSA Authentication Manager, see the BMC Provisioning Module Administrator Guide for RSA Authentication Manager.

Certification Checklist

Date Tested: June 10, 2010

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA Authentication Manager	7.1 SP3	Microsoft Windows Server 2003 Enterprise Edition SP2
RSA Authentication Agent	7.1 SDK SP3	Microsoft Windows Server 2003 Enterprise Edition SP2
BMC Identity Enterprise SecurityStation	7.5	Microsoft Windows Server 2003 Enterprise Edition SP2
BMC Provisioning Module for RSA Authentication Manager	5.0.00	Microsoft Windows Server 2003 Enterprise Edition SP2

Test	Result
1st time connection to RSA Authentication Manager Database	✓
User Management	
Add a user	✓
Modify a user's information	✓
Assign a token	✓
Un-assign a token	✓
Change Authentication Method	✓
Assign a password	✓
Un-assign a password	✓
Enable a user's token	✓
Disable a user's token	✓
Clear/Reset a user token's PIN	✓
Delete a user	N/A
Activate a user on a client	✓
De-Activate a user on a client	✓
Add a user to a group	✓
Remove a user from a group	✓
	N/A
No RSA Authentication Manager Server	✓

JGS / PAR

✓ = Pass ✗ = Fail N/A = Not Applicable