



RSA ClearTrust Ready Implementation Guide For User Management Products

Last Modified 04/21/03

1. Partner Information

Partner Name	Thor Technologies
Web Site	www.thortech.com
Product Name	Thor Xellerate
Version & Platform	Xellerate version 7.2.1 for Windows and Solaris
Product Description	<p>Xellerate by Thor Technologies is an advanced, yet flexible, provisioning system for granting and revoking access to enterprise applications and managed systems. Xellerate enables an enterprise to implement request and provisioning processes with the exact degree of automation desired - introducing manually executed functions where needed and automating others where suitable.</p> <p>With the Xellerate ClearTrust Adapter, RSA ClearTrust accounts may be created, revoked, and maintained within a provisioning context.</p>
Product Category	Provisioning

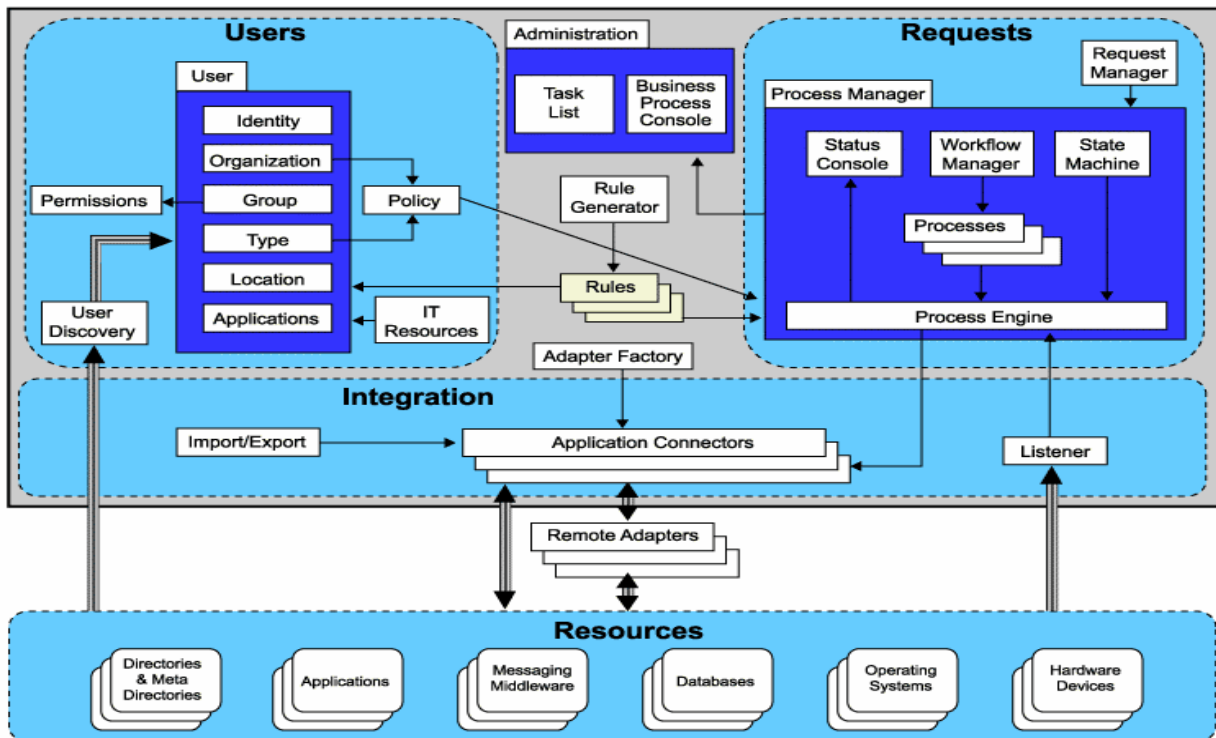


2. Contact Information

	Sales contact	Support Contact
Email	sales@thortech.com	support@thortech.com
Phone	925 462-3032	925 462-3032
Web	www.thortech.com	www.thortech.com

3. Solution Summary

Feature	Details
Provisioning Method	RSA ClearTrust Java Admin API,
User Management	Yes
User Property Management	Yes
User Password Management	Yes
Group Management	Full
Basic Entitlements Management	Full
Smart Rules Management	N/A
User self-service support	Yes



4. Product Requirements

This section describes the platforms, target systems and versions of Xellerate that are compatible with the integration. Specifically:

- A list of all versions of Xellerate that are compatible with this integration
- All compatible operating systems and platforms
- The name of the target system with which Xellerate will interact
- All external code that is necessary to run the integration successfully

Integration Requirements

Item	Description
<i>Xellerate Versions</i>	<i>Xellerate v.7.2.1 and higher</i>
<i>Platforms – Xellerate</i>	<i>Windows 2000 Solaris v8, Solaris v9</i>
<i>Target Systems</i>	<i>RSA ClearTrust v5.5 and v5.52</i>
<i>Platforms – Target Systems</i>	<i>Windows 2000/2003, Solaris</i>
<i>External Code</i>	<i>JDK 1.4.2, the ct_runtime_api.jar file, and the ct_admin_api.jar file</i>

Integration Module

The following table describes the files that comprise this integration. For each file, both the name and full path (from the root of the <thor_installation>xellerate\XLIntegrations directory) are listed. **Note:** Contact the Thor Sales Department at sales@thortech.com in order to obtain a CD that contains the integration files listed.

Integration Files

File Name with Path	Description
<i>cleartrust/xml/XLIClearTrust.xml</i>	<i>This file contains all components of the RSA ClearTrust integration that can be transferred from one database to another. These components include the ClearTrust resource asset type, the custom process form, the process task, entity, and pre-populate adapters (along with their mappings), the provisioning process, and the pre-populate rules to be used with this integration.</i>
<i>cleartrust/xml/XLICT/XLICTAutoSaveAdapter.xml</i>	<i>This file contains the adapter required to enable the AutoSave feature on the RSA ClearTrust provisioning process form. As a result, Xellerate can provision ClearTrust automatically (i.e., without manual intervention).</i>
<i>cleartrust/lib/xlicleartrust.jar</i>	<i>This file contains all of the java classes needed to connect to the RSA ClearTrust server and perform administrative functions.</i>
<i>cleartrust/docs/</i>	<i>This folder contains all of the documents that are relevant for this integration.</i>
<i>cleartrust/test/config/config.properties</i>	<i>This file contains the properties that are used to connect to the RSA ClearTrust server. These properties should be used to ensure that a connection can be established to the</i>

File Name with Path	Description
	<i>server. Otherwise, the RSA ClearTrust adapters cannot be used to connect to the server.</i>
<i>cleartrust/test/lib/xlicleartrusttest.jar</i>	<i>This file contains the test classes needed to connect to the RSA ClearTrust serve and perform administrative functions.</i>
<i>cleartrust/Xellerate Adapter for RSA ClearTrust License Agreement.pdf</i>	<i>This file contains the Xellerate Adapter for RSA ClearTrust License Agreement</i>

5. Product Configuration

Overview

This section contains instructions for:

- copying the integration files and external code (i.e., code from an outside operating system, third-party application or target system) into the appropriate directories
- changing the default Java version used by Xellerate
- updating the classpath files for both the Windows and Solaris platforms (i.e., the **classpath.bat** and **classpath.sh** files, respectively)
- copying the JSEE Provider Libraries into the appropriate directory
- modifying the **xellerate_object.cfg** file
- configuring the target system to communicate with Xellerate

Installation prerequisites

This document is intended for individuals with the following Thor Xellerate experience and responsibilities:

- Installing and configuring Xellerate.
- Integrating Thor Xellerate with other third-party systems.
- Managing User Resource Objects and working with Xellerate PPDs

Before attempting this integration, one should be familiar with the following concepts:

- A thorough understanding of Thor Xellerate and RSA ClearTrust.
- A basic familiarity of Thor Xellerate and RSA ClearTrust administrator consoles.

In addition, RSA ClearTrust 5.5 and Xellerate should be installed, configured and tested. See the products' respective installation and configuration documentation.

Copying the Integration Files and External Code

1. Copy the RSA ClearTrust integration package, which is provided by Thor Technologies, Inc., into the **<thor_installation>\xellerate\XLIntegrations** directory.
2. Copy the **ct_admin_api.jar** from the **<CT_installation>\lib** directory into the **<thor_installation>\xellerate\ext** directory.
3. Copy the **ct_runtime_api.jar** from the **<CT_installation>\lib** directory into the **<thor_installation>\xellerate\ext** directory.

Updating the Default Java Version

1. Download and install JDK 1.4.2 into the machine that is hosting Xellerate.
2. Open either the **xellvars.bat** or the **xellvars.sh** file. Specify the location where JDK 1.4.2 is installed by modifying the **JAVA** variable. For example:

```
Set JAVA=c:\j2sdk1.4.2_03
```

Note: JDK 1.4 is required to communicate with the ClearTrust server.

3. Add a REM command to the `SET BCJAR=.\ext\bcprov-jdk13-111.jar` setting in the `classpath.bat` or the `classpath.sh` file.
4. Remove the REM command from the `SET BCJAR=.\ext\bcprov-jdk14-120.jar` setting in the `classpath.bat` or the `classpath.sh` file.

Updating the Classpath Files

To update the classpath files, add these files to the `<thor_installation>\Xellerate\classpath.bat` or `<thor_installation>\Xellerate\classpath.sh` files:

1. `.\ext\ct_admin_api.jar;`
2. `.\ext\ct_runtime_api.jar;`
3. `.\XIIntegrations\ClearTrust\lib\xliClearTrust.jar`

Copying the JSSE Provider Libraries

Important: These files are required only when the ClearTrust server is running in Mutual Authentication (SSL_AUTH) mode.

Copy the following files from the `<CT_installation>\lib` directory into the `<JAVA>\jre\lib\ext` directory:

- `activation.jar`
- `asn1.jar`
- `certj.jar`
- `ct_ws.jar`
- `i18n.jar`
- `jcifs.jar`
- `jintegra.jar`
- `jnet.jar`
- `jsafe.jar`
- `jsafeJCE.jar`
- `ldapjdk.jar`

Updating the xellerate_object.cfg File

To update the `xellerate_object.cfg` file, add `xliClearTrust.jar` to the `Integration.jarnames` entry. For example:

```
Integration.jarnames=xliActiveDirectory.jar, xliExchange2000.jar,  
xliExchange55.jar, xliIPlanet.jar, xliSolaris8.jar, xliWindowsNT4.jar,  
xliClearTrust.jar
```

Configuring the Target System

To configure the target system, access RSA ClearTrust and create a default Administrative group named *allusers*. This group is to be used with all users who are members of ClearTrust.

Note: For groups that already exist within ClearTrust, you must map them to Xellerate. For more information on linking ClearTrust groups to Xellerate, refer to the **Mapping ClearTrust Groups to Xellerate** section on page 12.

6. Product Deployment

Overview

For Xellerate to communicate with the external resources on which it will create, update, and/or delete user and organization accounts, you *must* complete the following steps:

1. **Import Integration Files.** First, you need to import the files into Xellerate, which contain the bulk of the information that is necessary for Xellerate to communicate with the outside resources. These files are known as **integration** files.
2. **Define Resource Assets.** Next, you must specify the values for the parameters of the resources that are required by Xellerate to handshake with it.
3. **Map ClearTrust Groups to Xellerate.** Then, you must map existing ClearTrust groups to Xellerate. This is accomplished through the **Lookup Definition** form.
4. **Compile Adapters.** Then, you have to compile the adapters, which were imported into Xellerate, so they can be used to perform their designated actions within the target resource.
5. *Optional.* **Configure Xellerate to Provision Users with ClearTrust Automatically.** Lastly, you can setup Xellerate, so it can provision its users with ClearTrust automatically.

Note: A general explanation of these procedures is provided within the *Xellerate Framework Guide*.

Importing Integration Files

The table below contains the names of the .xml integration files that must be imported into Xellerate in order to perform the functionality associated with the integration.

Note: For more information on importing integration files into Xellerate, refer to the *Xellerate Administrator's Guide*.

Important: If you will be importing multiple integration files into Xellerate, be sure that you import them in the correct order (otherwise, the integration may not function as anticipated). Import the files in the order in which they are listed in the table below.

Integration Files Table

Item	Selection
<i>Import the ClearTrust resource asset type, the custom process form, the process task, entity, and pre-populate adapters (along with their mappings), the resource object, the provisioning process, and the pre-populate rules to be used with this integration.</i>	<i>XLICleartrust.xml</i>
<i>This file contains the adapter required to enable the AutoSave feature on the ClearTrust provisioning process form. As a result, Xellerate can provision ClearTrust automatically (i.e., without manual intervention).</i>	<i>XLICTAutoSaveAdapter.xml</i>

Defining Resource Assets

The table within this section lists:

- The names of the resource assets you have created within Xellerate to allow it to connect to your target system.
- The names of the resource asset types on which the resource assets are based (that come pre-defined within the .xml file).
- The default connection parameters (and default values, if applicable) associated with each distinct resource asset.
- Whether the resource assets are to be used to call methods on APIs, which reside on machines that are external to Xellerate (i.e., are the **Remote Manager** lookup fields populated).
- The names of the remote managers, if any, which are associated with the resource assets (provided that remote managers are to be used with the resource assets).

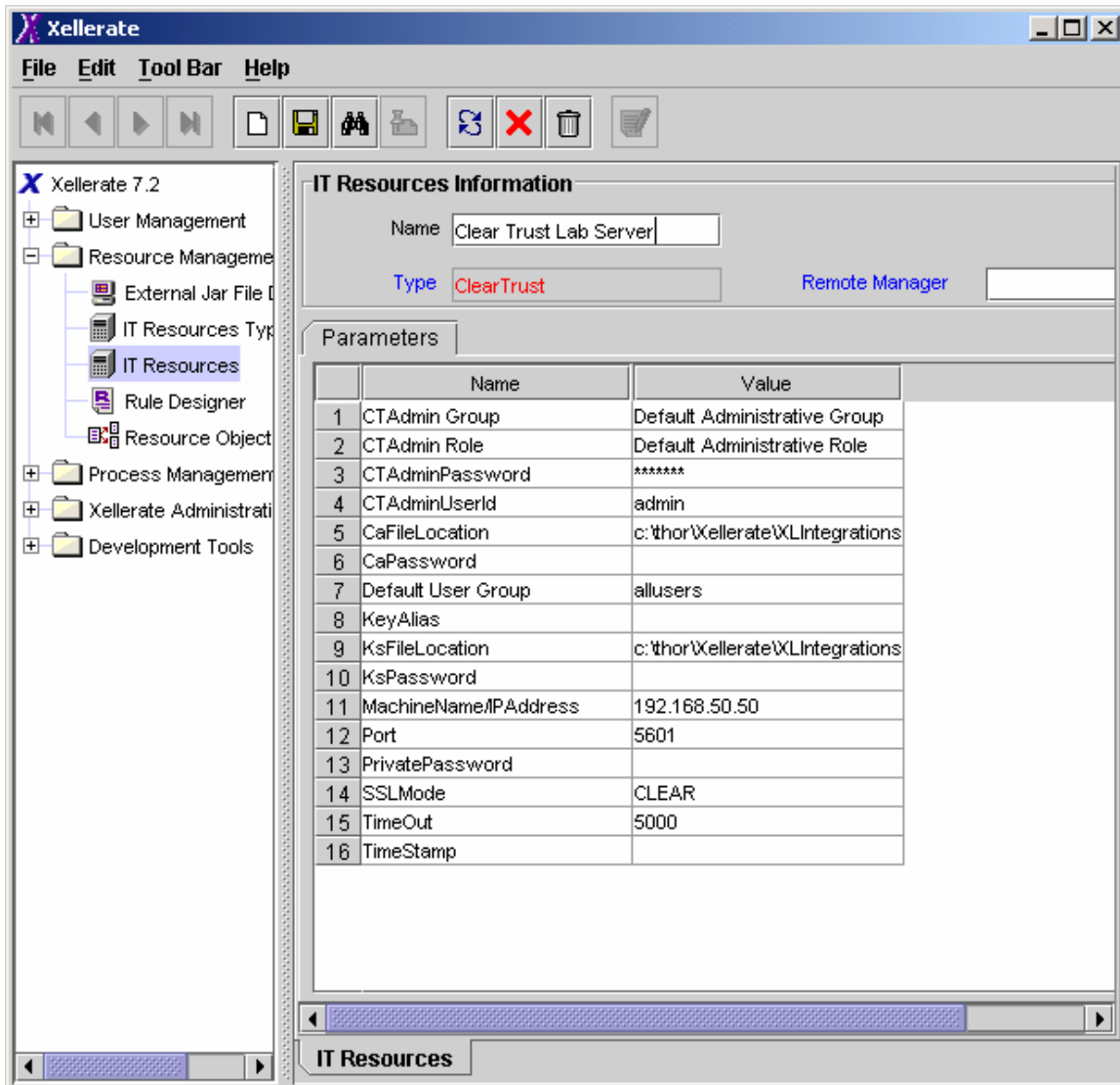
Note: For more information on defining resource assets within Xellerate, refer to the *Xellerate Administrator's Guide*.

Resource Asset Table

Item	Selection
<i>What is the name of the resource asset?</i>	<i>ClearTrust</i>
<i>What is the name of the resource asset type?</i>	<i>ClearTrust</i>
<i>What are the default values for the parameter fields of the resource asset?</i>	<ul style="list-style-type: none">• CTAdminUserId. This parameter is required. It represents the name of the ClearTrust Administrator.• CTAdminPassword. This parameter is required. It represents the password of the ClearTrust Administrator.• MachineName/IPAddress. This parameter is required. It represents the name/IP Address of the machine where the ClearTrust entitlement server is running. It is also the machine to which Xellerate will connect.• Port. This parameter is required. It represents the port number on which the ClearTrust entitlement server is running.• SSLMode. This parameter is required. It represents the SSL mode that is used to connect to the ClearTrust server.• <i>Important: Make sure that ClearTrust is running in this mode. Otherwise, Xellerate will not be able to connect to ClearTrust.</i>• TimeOut. This parameter is required. It represents the timeout value for the connection that is established between Xellerate and ClearTrust.

Item	Selection
	<ul style="list-style-type: none"> • Default User Group. This parameter is required. It represents the default user group within ClearTrust. Note: For more information on linking ClearTrust groups to Xellerate, refer to the Error! Reference source not found. section on page Error! Bookmark not defined. • CaFileLocation. This parameter is to be used only with mutual authentication. It represents the location of the CA Certificate. • CaPassword. This parameter is to be used only with mutual authentication. It represents the password for the CA Certificate. • KsFileLocation. This parameter is to be used only with mutual authentication. It represents the location of the keystore file. • KsPassword. This parameter is to be used only with mutual authentication. It represents the password of the keystore file. • KeyAlias. This parameter is to be used only with mutual authentication. It represents the Key name that is to be used with the keystore file. • PrivatePassword. This parameter is to be used only with mutual authentication. It represents the password for the private key in the keystore file. • TimeStamp. This field is currently not used. • CTAdmin Group. This parameter represents the group to which the CT Administrative user belongs. • CTAdmin Role. This parameter represents the role of the CT Administrative user.
<p><i>Is the resource asset to be used to call a method on an API, which resides on a machine that is external to Xellerate?</i></p>	<p>No</p>
<p><i>If "Yes," what is the name of the remote manager?</i></p>	<p>N/A</p>

A sample ClearTrust resource asset definition is illustrated below:



Mapping ClearTrust Groups to Xellerate

You must map any groups that exist within ClearTrust to Xellerate. This is accomplished through the *CTGroups* record of the **Lookup Definition** form. This record is imported into Xellerate via the *XLIClearTrust.xml* file.

The following procedure will show you how to link a ClearTrust group to Xellerate.

Map a ClearTrust Group to Xellerate

1. Launch Xellerate.
2. Open the Lookup Definition form.
3. Query for the *CTGroups* record. The following screen appears:

The screenshot shows the Xellerate 7.2 application window. The title bar reads 'Xellerate'. The menu bar includes 'File', 'Edit', 'Tool Bar', and 'Help'. The toolbar contains various icons for navigation and actions. The left-hand pane displays a tree view of the application's structure, with 'Xellerate 7.2' expanded to show 'Xellerate Administration', where 'Lookup Definition' is selected. The main workspace is titled 'Lookup Definition' and contains the following fields and controls:

- Code:** A text box containing 'CTGroups'.
- Field:** An empty text box.
- Lookup Type:** A radio button that is selected.
- Field Type:** An unselected radio button.
- Required:** An unchecked checkbox.
- Group:** A text box containing 'ClearTrust'.

Below these fields is a section titled 'Lookup Code Information' which contains a table:

	Code Key	Decode	Language	Country
1	allusers	allusers	en	us

Buttons for 'Add' and 'Delete' are located to the left of the table. At the bottom of the window, there are tabs for 'IT Resources', 'Lookup Definition', and 'Lookup Definition Table'.

4. Click **Add**. An empty row appears.
5. Within the **Code Key** and **Decode** cells, enter the name of the ClearTrust group. Then, type *en* into the **Language** cell and *us* into the **Country** cell.
6. Click **Save**.
7. Repeat Steps 4-6 for all ClearTrust groups that you wish to map to Xellerate.

Compiling Adapters

The table below lists all the adapters that are imported into Xellerate, via the **XLICleartrust.xml** file. These adapters **must** be compiled. Otherwise, they cannot be used to provision accounts on your target system.

Note: To compile multiple adapters simultaneously, use the **Adapter Manager** form. To compile one adapter at a time, use the **Adapter Factory** form. For instructions on how to use either of these forms, refer to the *Xellerate Administrator's Guide*.

Item	Selection
What are the names of the adapters that are being imported into Xellerate via the XLICleartrust.xml file?	<i>CTAdd Default Group to User</i> <i>CTAddGroup</i> <i>CTAssign Default Group</i> <i>CTCreateUser</i> <i>CTDeleteGroup</i> <i>CTDeleteUser</i> <i>CTEmailValidation</i> <i>CTEndOrPwdExpDateValidation</i> <i>CTModifyUser</i> <i>CTPrepopDateAddOneYear</i> <i>CTPrepopStartDate</i> <i>CTprepopString</i> <i>CTStringTask</i> <i>CTUpdateGroup</i>

Configuring Xellerate to Provision Users with ClearTrust Automatically

The following procedure will show you how to configure Xellerate so that it can provision its users with ClearTrust automatically (i.e., without any user intervention).

Setup Xellerate to Auto-Provision Its Users with ClearTrust

1. Launch Xellerate.
2. Open the **Deployment Utility** form.
3. Import the **XLICTAutoSaveAdapter.xml** file into Xellerate.
4. Compile the **CTPrePopServerInfo** adapter, either via the **Adapter Factory** form or the **Adapter Manager** form.
5. Open the **Form Designer** form.
6. Query for the **CT_USERS** record. Select the **Pre-Populate** tab, and click **Add**. The Pre-Populate Adapters window appears.
7. From the **Field Name** combo box, select *IT Resource*.
8. Double-click the **Rule** lookup field. From the Lookup window that appears, select *Default*. Then, click **OK**.
9. Double-click the **Adapter** lookup field. From the Lookup window that appears, select *CTPrePopServerInfo*. Then, click **OK**.
10. Enter *1* into the **Order** field.

11. Click **Save**. *Mapping Incomplete* appears within the **Adapter Status** field. In addition, the **Adapter Variables** region of the Pre-Populate Adapters window is enabled.
12. From the **Adapter Variables** region, click **Add**. The Map Adapter Variables window appears.
13. From the **Map To** combo box, select *IT Resource*.
14. From the **Qualifier** combo box, select *Clear Trust Dev*.
15. From the Map Adapter Variables window's Toolbar, click **Save**. Then, click **Close**. *Ready* is now displayed within the **Adapter Status** field of the Pre-Populate Adapters window.
16. From the Pre-Populate Adapters window's Toolbar, click **Save**. Then, click **Close**. The *CT_USERS* record is active once again. The **IT Resource** field of the custom process form can now be populated automatically. As a result, Xellerate can provision its users with ClearTrust automatically.

Certification Checklist for User Management Products

Date Tested: 04/07/04

Product	Tested Version
RSA ClearTrust	5.5
Thor Xellerate	7.2.1

Test Case	Result
Note: All test cases should be performed via the User Management Administrative Interface	
Users	
Create new user	P
Modify user properties	P
Display user	P
Remove user	P
Reset user password	P
User self-service password reset	P
Groups	
Create new group	N/A
Modify group properties	P
Display group properties	P
Remove group	P
Add user to group	P
Remove user from group	P
Basic Entitlements	
Create new entitlement	N/A
Modify entitlement	N/A
Display entitlement	N/A
Remove entitlement	N/A
Add user to entitlement	N/A
Add group to entitlement	N/A
Remove user from entitlement	N/A
Remove group from entitlement	N/A
Smart Rules	
Create new Smart Rule	N/A
Modify Smart Rule	N/A
Display Smart Rule	N/A
Remove Smart Rule	N/A
<i>*See Notes section for more information</i>	

JGS

*P=Pass or Yes F=Fail N/A=Non-available function

7. Known Issues

- For this release, the integration will support provisioning against only one RSA ClearTrust server.
- For this release, the integration will only support RSA ClearTrust. Administrators need to be created and managed via RSA ClearTrust.
- For this release, group assignment(s) will be supported by the Java version of Xellerate only.

8. Notes

- All users created will have the **isPublic** attribute set to *true* (i.e., The users will be visible to all administrator groups within RSA ClearTrust.).
- By default, the *allusers* group will be added to all RSA ClearTrust users.
- The default password policy of RSA ClearTrust will be implemented in Xellerate. If any changes are made with this policy, these changes must be reflected in Xellerate.
- Entitlement provisioning will work via group assignments in Xellerate. Once a group is assigned to a user in Xellerate, a corresponding group will be assigned to the user in RSA ClearTrust. This user will inherit the entitlements via the group assignment.