



RSA SecurID Ready Implementation Guide Administrative Interoperability

Last Modified: March 21, 2005

Partner Information

Product Information	
Partner Name	Thor Technologies
Web Site	www.thortech.com
Product Name	Xellerate
Version & Platform	8.0.1 or higher, MS-Windows 2000, 2003 , Sun Solaris 9, Red Hat Enterprise Linux
Product Description	<p>Xellerate Identity Manager is the most comprehensive and scalable Enterprise Identity Management solution in the marketplace. It offers unparalleled flexibility and adaptability as it extends its security and compliance management solution across the heterogeneous business processes and managed platforms that make up the large enterprise. In addition to being a best-in-class platform, Xellerate offers a set of proven tools that automate most time-consuming development, implementation and support tasks.</p> <p>Xellerate Identity Manager provides the following business benefits:</p> <ul style="list-style-type: none">- Reduces security risks- Ensures compliance with corporate policies and regulatory requirements- Dramatically reduces the cost of providing and managing access to valuable corporate resources- Increases productivity and operational efficiency- Enables IT to be more responsive to evolving business requirements
Product Category	User Management / Identity Management Systems



Solution Summary

Xellerate's integration with RSA Authentication Manager enables automated provisioning and de-provisioning of users within the Authentication Manager and also supports assignment / un-assignment, registration and testing of tokens for a User. In addition, this Integration is typically deployed with customer-specific provisioning and approval workflow for physical token distribution.

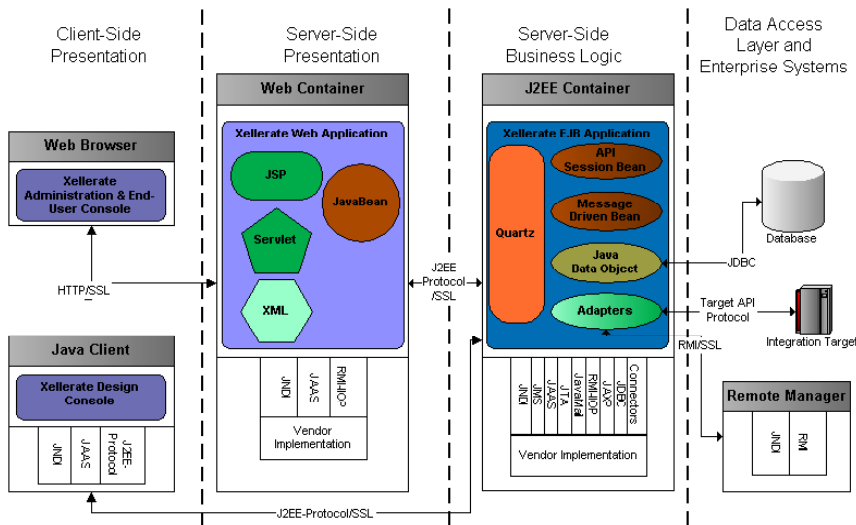
Together, they enable an Enterprise to manage the life cycle of Users with Tokens/Passwords using both Hardware and Software tokens.

Partner Integration Overview : User Functions	
Add a user to the RSA ACE Authentication Manager Database	Yes
Delete a user from the RSA ACE Authentication Manager Database	Yes
Modify user information	Yes
Set User Password	Yes
Get User ID (Find Users in ACE Authentication Manager Database)	Yes
Get User Info	Yes
Get Group Membership	Yes
Get Serial By Login	Yes
Change User Authentication Method (PASSCODE or TokenCode)	Yes
Reconcile RSA ACE Authentication Manager Database Users with the User Management	Yes
Partner Integration Overview : Token Functions	
Support for Standard Card, Key Fob, PINPAD, and SoftID	Yes
Assign a token	Yes
Assign a token by number	Yes
Un-assign/Rescind a user's token	Yes
Clear a token's PIN	Yes
Set PIN to Next Token Code Mode	Yes
Enable a token	Yes
Disable a token	Yes
Track Lost Tokens	Yes
List Token Info (Retrieve Status of a Token)	Yes
Test Login	Yes

System Architecture

Following is the main architecture of Xellerate. The Remote Manager is the interface to the ACE Authentication Manager and its Admin API:

Xellerate Physical Architecture-(Detail)

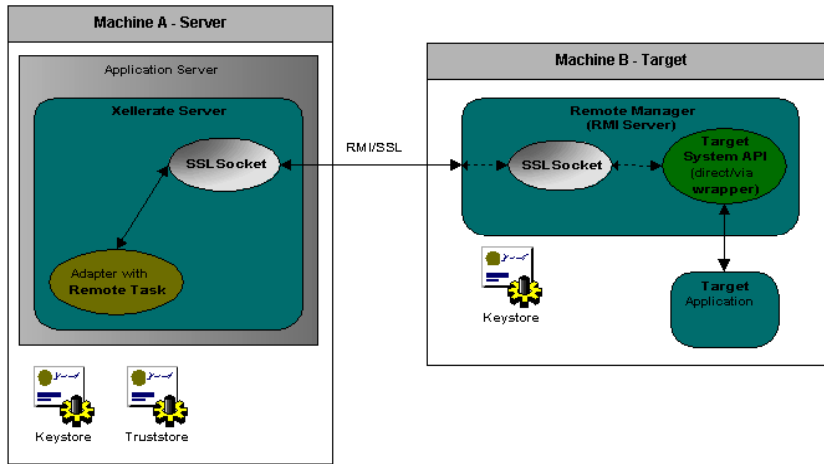


Thor Technologies - Proprietary and Confidential



This diagram describes the Security Model used for the communication between the Xellerate Server and the Remote Manager:

Remote Manager Security



Thor Technologies - Proprietary and Confidential



Product Requirements

Partner Product Requirements: Windows Xellerate Design Console	
CPU	Intel Pentium III processor 700 MHz
Memory	64MB RAM
Storage	25MB Storage
Partner Product Requirements: Windows Xellerate Server / Database Server	
CPU	Intel Pentium III processor 700 MHz
Memory	1GB RAM
Storage	4GB Storage
Operating System	
Platform	Required Patches
Microsoft Windows 2000 Server	SP4
Microsoft Windows 2003 (Standard or Enterprise)	

Partner Product Requirements: Solaris Xellerate Server / Database Server	
CPU	SUN Ultra 10
Memory	1GB RAM
Storage	20GBB Storage
Operating System	
Platform	Required Patches
Sun Solaris 8 or 9	Latest Patch Cluster

Additional Software Requirements	
Application	Additional Patches
Oracle 9i release 2 or	(9.2.0.4)
SQL Server 2000	SP3a
JBoss 3.2 or	
BEA WebLogic Server 8.1 or	SP2
IBM WebSphere 5.0.2.6	
Java JDK	JDK (the same version on which Xellerate server is running has to be installed on ACE Authentication Manager Server)

Xellerate ACE Integration Installation/Configuration

Resource Adapter Installation

Introduction

The following install procedure will refer to 2 Servers:

Xellerate Server – The server where XL Server is installed

Target Resource – The server where the ACE Authentication Manager is installed.

Overview

This section contains the following information:

- Instructions for copying the resource adapter files into the appropriate directory.
- Instructions for copying external code (i.e., code from an outside operating system, third-party application or target system) into the appropriate directory.
- Instructions for installing the external software (if any), so Xellerate can communicate with the target system.
- Instructions for configuring the target system, so Xellerate can handshake with it.

Copying the Resource Adapter Files

Copy the resource adapter files in the ACE folder into the following location:

```
<XELLERATE_HOME>\xellerate\XLIntegrations\
```

Configuring the Xellerate Server

To configure the Xellerate Server, update the following file:

```
<XELLERATE_HOME>\xellerate\bin\xlStartServer.bat
```

- Add the following as its first line:

```
set PATH=<XELLERATE_HOME>\xellerate\XLIntegrations\  
ACE\lib\ACE52;%PATH% (for ACE 5.2)
```

or

```
set PATH==<XELLERATE_HOME>\xellerate\XLIntegrations\  
ACE\lib\ACE50;%PATH% (for ACE 5.0)
```

Configuring the Target System

Use the following steps to configure the target system.

Setting up the Remote Manager

1. You need to set up a Remote Manager on the ACE Authentication Manager Server in a directory <XL_REMOTE>. Please see the *Xellerate Installation Guide* for more information on installing the Remote Manager.

Note: The JDK needs to be installed on the target system (i.e., ACE Authentication Manager Server for Remote Manager installation and operation). Use the JDK version that is similar to the one used for Xellerate Server.

Note: For Solaris, an ACE admin user needs to be created, as a pre-installation requirement for ACE Authentication Manager. This admin user is the file owner of ACE Authentication Manager installation. Install Remote Manager using the same ACE admin credentials.

2. Create a directory <ACE_HOME> on the ACE Authentication Manager Server. From the Xellerate Server, copy the contents of <XELLERATE_HOME>/xellerate/XLIntegrations/ACEremotePackage\ to <ACE_HOME>\.

For Solaris 9,

Login to the Solaris server with the user credentials of the ACE Authentication Manager File Owner (which was created as a pre-installation instruction for ACE Authentication Manager) and then create the directory.

Note: In case of copying files from Windows to Solaris, all data transfer from ftp client must use Binary Mode. Also, after copying to Solaris server, relevant files must be checked for ^M characters. Required operations like “dos2unix” must be carried out.

Copy all the files while using the ACE admin credentials, as described previously.

3. To update the class files, copy <ACE_HOME>\lib\liACE.jar files to the directory <XL_REMOTE>\xlremote\JavaTasks.

4. Update the library files by editing the following file,

<XL_REMOTE>\xlremote\remotemanager.bat

Set the following parameters as the first line in the file.

```
set PATH=<ACE_HOME>\lib\ACE52;%PATH% (for ACE 5.2)
```

or

```
set PATH=<ACE_HOME>\lib\ACE50;%PATH% (for ACE 5.0)
```

For Solaris 9,

Update the file,

`<XL_REMOTE>\xlremote\remotemanager.sh`

and then add the following lines:

```
export ACE_HOME=<ACE_HOME>
```

```
export ACE_INSTALL=<-ACE_INSTALL->
```

5. In the case of RSA ACE Server 5.0, copy

`<ACE_INSTALLATION>\ace\utils\toolkit\apidemon.exe`

to

`<XL_REMOTE>\xlremote\`

Setting up the Remote Manager as a TRUSTED source for Xellerate Server

1. Edit the file,

`<ACE_HOME>\scripts\ACEExportRMCert.bat`

Set the following parameters,

```
set XL_REMOTE=<XL_REMOTE>
```

```
set JAVA_HOME=<JDK_HOME>
```

and execute `ACEExportRMCert.bat`.

For Solaris 9,

Edit the file,

`<ACE_HOME>\scripts\ACEExportRMCert.sh`

Set the following parameters,

```
export XL_REMOTE=<XL_REMOTE>
```

```
export JAVA_HOME=<JDK_HOME>
```

and execute `ACEExportRMCert.sh`

This creates a security certificate file `AceRMgr.cer` in `<ACE_HOME>\scripts\config\`

2. From the ACE Authentication Manager Server, copy the file,

`<ACE_HOME>\scripts\config\AceRMgr.cer`

to

`<XELLERATE_HOME>\xellerate\XLIntegrations\ACE\scripts\config\`

3. Edit the file,

`<XELLERATE_HOME>\xellerate\XLIntegrations\ACE\scripts\ACEImportRMCert.bat`

And enter the line,

```
set JAVA_HOME=<JDK_HOME>
```

and execute `ACEImportRMCert.bat`

When the following question appears, in the command prompt:

```
Trust this certificate?
```

Type **“yes”**.

Configuring Strong Authentication between the Xellerate Server and the Remote Manager

1. Edit the file,

<XELLERATE_HOME>\xellerate\XLIntegrations\ACE\scripts\ACEGenExpXLCert.bat

by setting the following parameters:

```
set XELLERATE_HOME=<XELLERATE_HOME>
set JAVA_HOME=<JDK_HOME>
```

Then execute it. A key is generated and it also creates a security certificate file, *XLServer.cer* in <XELLERATE_HOME>\xellerate\XLIntegrations\ACE\scripts\config.

2. Modify the file,

<XELLERATE_HOME>\xellerate\config\xlconfig.xml

Traverse along the following tree:

<xl-configuration> → <Security> → <XLPKIPProvider> → <Keys>

and add another child element “AceServerKey” in addition to the existing ones (eg. “PrivateKey”) as:

```
<PrivateKey>
  <Alias>xell</Alias>
  <Password encrypted="true">PYpvQz19aT2Tn7sFzW7gYQ==</Password>
</PrivateKey>
<AceServerKey>
  <Alias>ace</Alias>
  <Password encrypted="false">aceServer</Password>
</AceServerKey>
```

The password becomes encrypted the next time the server is run.

3. Copy the generated, exported certificate *XLServer.cer*, in Xellerate Server from <XELLERATE_HOME>\xellerate\XLIntegrations\ACE\scripts\config\

to

<ACE_HOME>\scripts\config\

on the Ace Authentication Manager Server.

4. Edit the file,

<ACE_HOME>\scripts\ACEImportXLCert.bat

Set the following parameters,

```
set JAVA_HOME=<JDK_HOME>
```

```
set XL_REMOTE=<XL_REMOTE>
```

and execute *ACEImportXLCert.bat*.

For Solaris 9,

Set the following parameters,

```
export XL_REMOTE=<XL_REMOTE>
```

```
export JAVA_HOME=<JDK_HOME>
```

and execute *ACEImportXLCert.sh*.

When the following question appears, in the command prompt:

Trust this certificate?

Type **“yes”**.

Resource Adapter Deployment

Overview

For Xellerate to communicate with the external resources on which it will create, delete and/or update users and organizations accounts (or to perform reconciliation functions with the data and accounts on these systems), you *must* complete the following steps:

1. **Import Resource Adapter Files**—The files that contain the bulk of the information necessary for Xellerate to communicate with the target system are known as *resource adapter* files. Import them into Xellerate.
2. **Define Resource Assets**—Specify the values for the <target_resource> parameters that are required by Xellerate.
3. **Compile Adapters**—Compile the adapters that were imported into Xellerate.

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

Importing Resource Adapter Files

To import the resource adapter files into Xellerate:

1. Launch the **Xellerate Designer Console** (Java Client).
2. Navigate to the **Deployment Utility** form (Xellerate Administration>Deployment Utility).
3. Select the **Import** tab.
4. Browse to locate the file, *XLIACEUser.xml* (<Xellerate_Home>\xellerate\XLIntegrations\ACE\xml).
5. Click **Import**.
6. Browse to locate the file, *XLIACEToken.xml* (<Xellerate_Home>\xellerate\XLIntegrations\ACE\xml).
7. Click **Import**.

The XML file is imported.

Important: Make sure that you import the resource adapter files in the correct order, or your resource adapter may not work. For more information on importing resource adapter files into Xellerate, refer to the *Xellerate Administrator's Guide*.

Defining IT Resource Assets

IT Resources are used in Xellerate to describe how and where to connect. For ACE Integration we use a Remote Manager as the ACE API is not network aware.

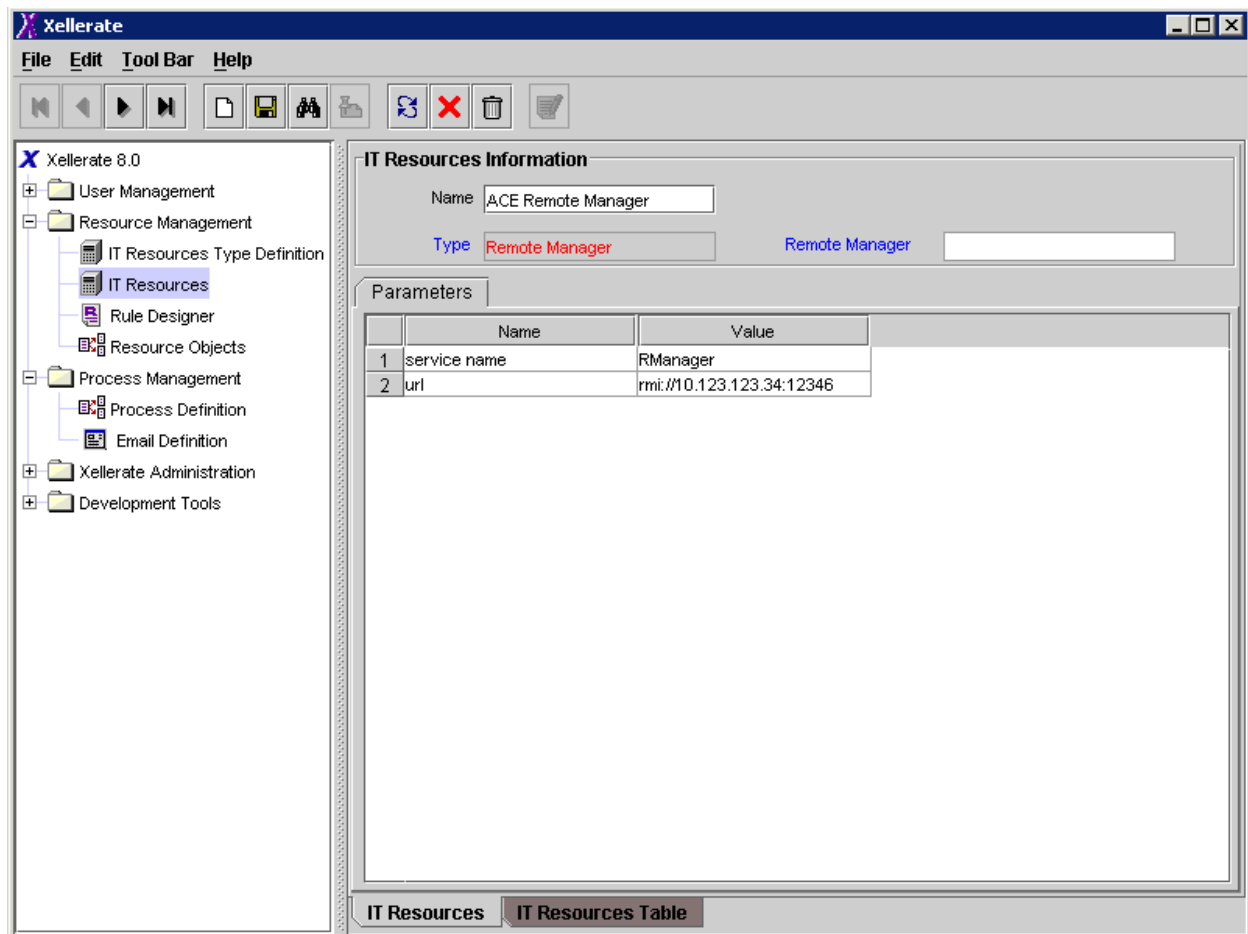
Note: For more information on defining resource assets within Xellerate, refer to the *Xellerate Administrator's Guide*.

Remote Manager IT Resource Definition: ACE Remote Manager

Item	Selection
What is the name of the resource asset?	ACE Remote Manager
What is the name of the resource asset type?	Remote Manager
What are the default values for the parameter fields of the resource asset?	service name=RManager url=rmi://10.123.123.34:12346
Is the resource asset to be used to call a method on an API, which resides on a machine that is external to Xellerate?	No
If "Yes," what is the name of the remote manager?	N/A

** N/A = Not Applicable

Here is a screenshot of the IT Resource Definition in Xellerate Design Console:



ACE Authentication Manager IT Resource Definition: ACE Server - Remote

Item	Selection
What is the name of the resource asset?	ACE Server – Remote
What is the name of the resource asset type?	ACE Server
What are the default values for the parameter fields of the resource asset?	ACEAdminMode=Host or Remote ACEAdminPassCode=123456 (will get encrypted after saving) ACEAdminUserId=jbeg
Is the resource asset to be used to call a method on an API, which resides on a machine that is external to Xellerate?	Yes
If “Yes,” what is the name of the remote manager?	ACE Remote Manager

Here is a screenshot of the IT Resource Definition in Xellerate Design Console:

The screenshot displays the Xellerate Design Console interface. On the left is a tree view showing the project structure: Xellerate 8.0, User Management, Resource Management (expanded), IT Resources Type Definition, IT Resources (selected), Rule Designer, Resource Objects, Process Management, Process Definition, Email Definition, Xellerate Administration, and Development Tools. The main workspace is titled 'IT Resources Information' and contains the following fields:

- Name: ACE Server - Remote
- Type: ACE Server
- Remote Manager: ACE Remote Manager

Below these fields is a 'Parameters' section with a table:

	Name	Value
1	ACEAdminMode	Host
2	ACEAdminPassCode	*****
3	ACEAdminUserId	xlace

At the bottom of the console, there are two tabs: 'IT Resources' and 'IT Resources Table'.

Compiling Adapters

The table below lists all the adapters that were imported into Xellerate when the XML resource adapter file was deployed. These adapters will need to be compiled before you can use them 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*.

Table

Example:

Item	Selection
What are the names of the adapters that are being imported into Xellerate and need to be compiled?	ACE CREATE USER ACE DELETE USER ACE ASSIGN TO GROUP ACE ASSIGN TO GROUP ACE ENABLE TOKEN ACE DISABLE TOKEN ACE TEST LOGIN ACE SET PIN ACE SET PIN TO NTC ACE TRACK LOST TOKEN ACE ASSIGN TOKEN ACE REMOVE TOKEN ACE PrePop FirstName ACE PrePop LastName ACE PrePop DefLogin

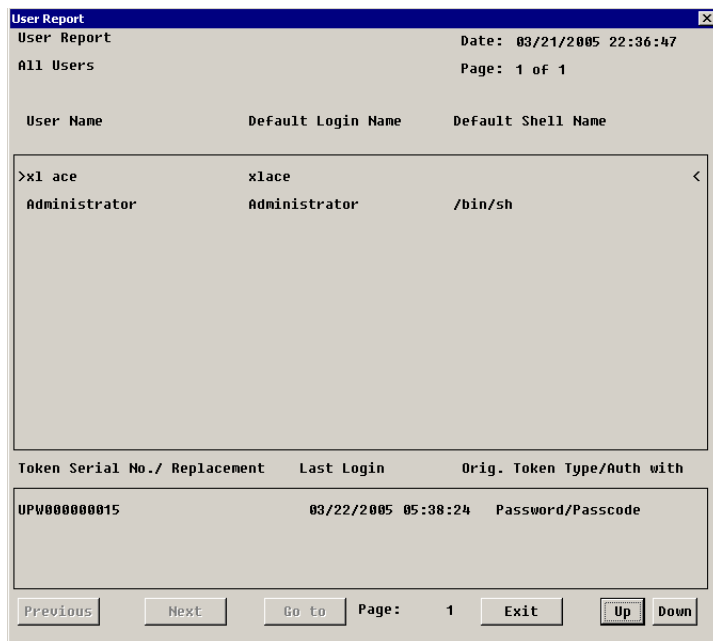
Authentication Manager Provisioning with Xellerate

Introduction

The imported integration contains the base integration that will be further integrate/enhanced in Xellerate according to your business rules requirements. What is shown here is the base Direct Provisioning Interface to show how provisioning/de-provisioning into ACE Authentication Manager works. In a real world scenario, most of these operations would be automated and users will be provisioned according to authoritative sources and entitlements/business rules. Token Provisioning (physical tokens will be requested by users/manager to be approved by managers/delegates) will be added as an additional provisioning process. That process is not contained in this integration, as it is not communicating with the ACE Authentication Manager. Token Registration is usually done as a Self Service Request that the users perform themselves using the Web Client and are a combined Assign Token, Set Pin and Test Login Request.

Before Provisioning

The users defined in ACE Authentication Manager before Xellerate provisioning:



The screenshot shows a 'User Report' window with the following content:

User Report Date: 03/21/2005 22:36:47
All Users Page: 1 of 1

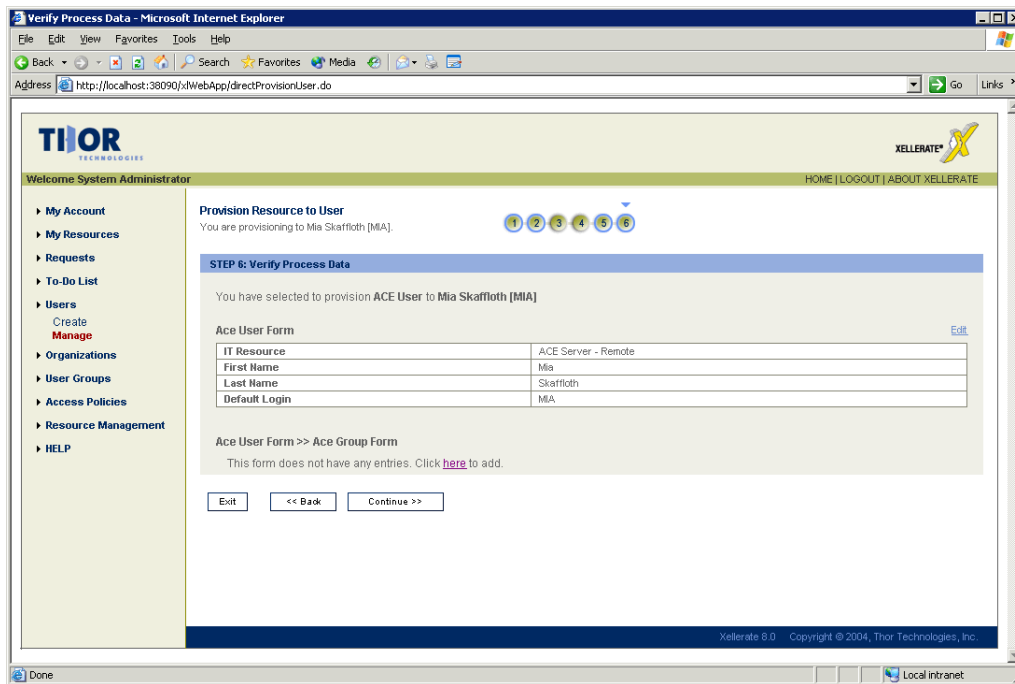
User Name	Default Login Name	Default Shell Name
>x1 ace	xlace	<
Administrator	Administrator	/bin/sh

Token Serial No./ Replacement	Last Login	Orig. Token Type/Auth with
UPW000000015	03/22/2005 05:38:24	Password/Passcode

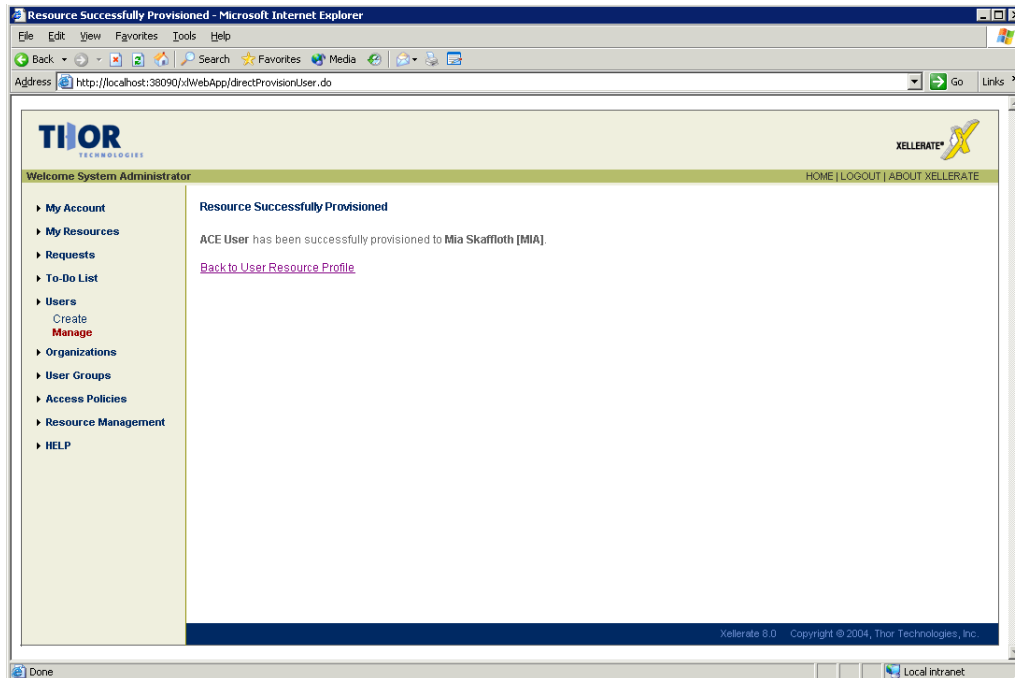
Navigation buttons: Previous, Next, Go To, Page: 1, Exit, Up, Down

Create User

Provisioning a user using the Xellerate Web Administration Client:



Confirmation of the success of the provisioning transaction:



On the ACE Authentication Manager, we can confirm the creation of the user using the Administration Client:

Edit User

First and Last Name:

Default Login:

Default Shell:

Local User Remote User

Serial Number	Token Type/Auth With	Status
Tokens:		

O: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary User

Start Date: 12/31/2000 16:00 End Date: 12/31/2009 16:00

Allowed to Create a PIN Required to Create a PIN

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

OK Cancel Apply L/S Changes Set All L/S Help

Assign Group to User

We provision an ACE Group to the user using the XL Web Client:

Ace Group Form

* Indicates a required field

Group Name * Beg and Sons [Clear](#)

Group Login * MIA

Confirmation of the success of group assignment:

Ace Group Form

* Indicates a required field

Group Name * Beg and Sons [Clear](#)

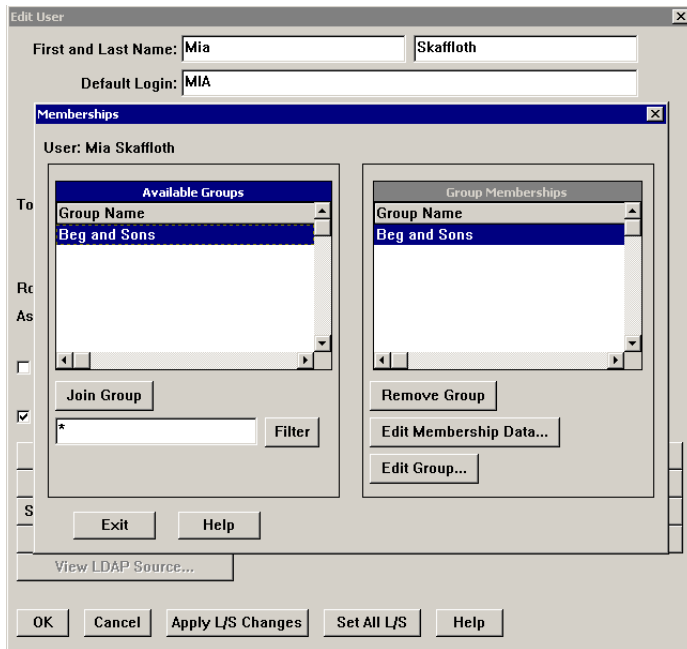
Group Login * MIA

Results 1-1 of 1 [First](#) | [Previous](#) | [Next](#) | [Last](#)

Group Name	Group Login	Remove
Beg and Sons	MIA	<input type="checkbox"/>

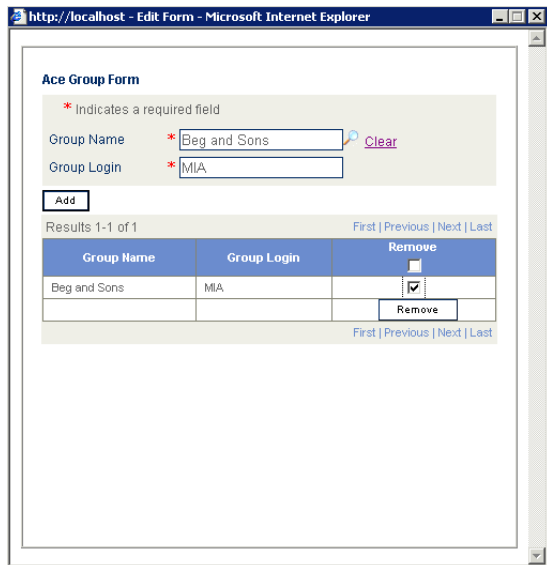
[First](#) | [Previous](#) | [Next](#) | [Last](#)

On the ACE Authentication Manager we can confirm the group assignment to the user using the Administration Client:

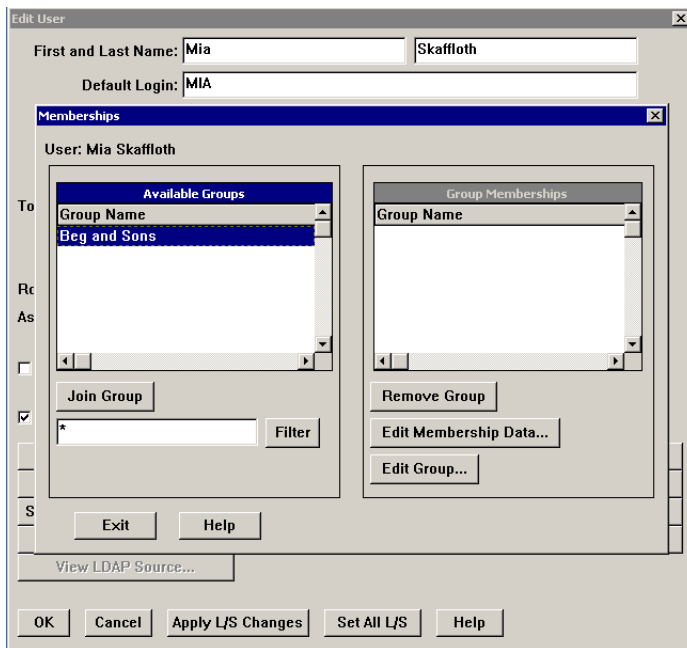


Remove Group from User

We de-provision an ACE Group from an existing user using the Xellerate Web Administration Interface:



On the ACE Authentication Manager we can confirm that the group has been removed from the user using the Administration Client:



Assign Token to User

We provision a Token to a user via the Xellerate Web Administration Interface:

Provision Resource to User

You are provisioning to Mia Skaffloth [MIA].



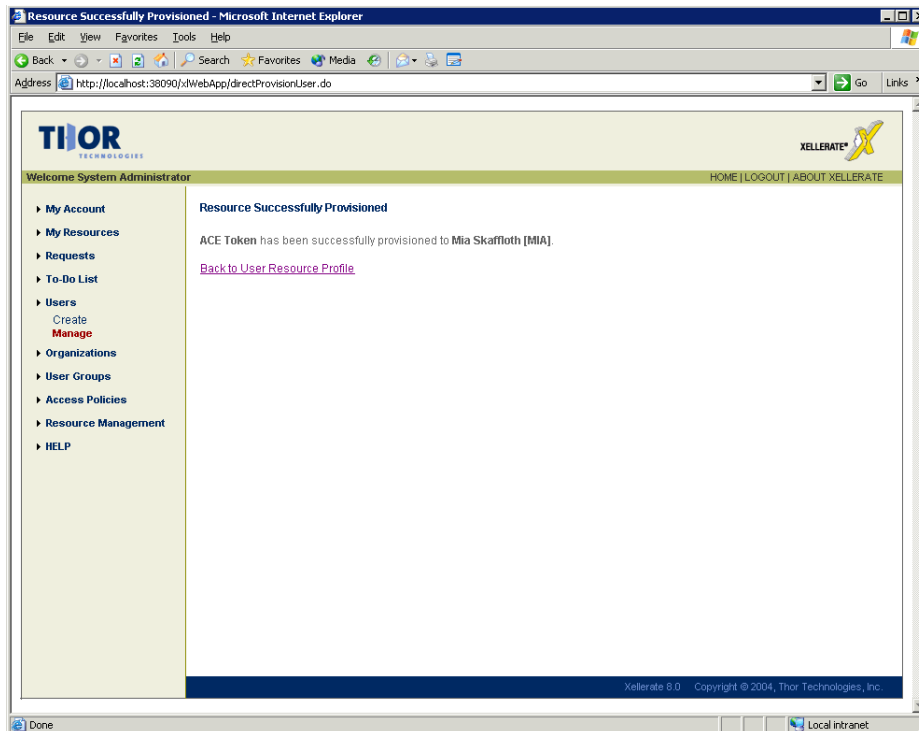
STEP 6: Verify Process Data

You have selected to provision **ACE Token** to **Mia Skaffloth [MIA]**

Ace Token Form [Edit](#)

IT Resource	ACE Server - Remote
Token Serial Number	23788180
Pin	
Re-enter Pin	
Set Pin	0
Curent Token Code	
Test Login	0
Set Pin to HTC	0
Number of passwords	
Lifetime (Hours)	
Number of Digits	
Set Lost	0

Confirmation of the success of the provisioning transaction:



On the ACE Authentication Manager we can confirm the token assignment to the user using the Administration Client:

Edit User

First and Last Name:

Default Login:

Default Shell:

Local User Remote User

Serial Number	Token Type/Auth With	Status
000023788180	Key Fob/Passcode	Enabled;New PIN Mode

O: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary User

Start Date: 12/31/2000 16:00 End Date: 12/31/2009 16:00

Allowed to Create a PIN Required to Create a PIN

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

OK Cancel Apply L/S Changes Set All L/S Help

Set Pin on Token

We set a pin on the token using the Xellerate Web Administration Client:

The screenshot shows a web browser window titled "http://localhost - Edit Form - Microsoft Internet Explorer". The main content is the "Ace Token Form". At the top, it says "* Indicates a required field". The form contains the following fields and controls:

- IT Resource: Text box containing "ACE Server - Remote" with a "Clear" link.
- Token Serial Number: Text box containing "23788180".
- Pin: Password field with "*****".
- Re-enter Pin: Password field with "*****".
- Set Pin: Check box, which is checked.
- Current Token Code: Text box.
- Test Login: Check box, which is unchecked.
- Set Pin to NTC: Check box, which is unchecked.
- Number of passwords: Text box.
- Lifetime (Hours): Text box.
- Number of Digits: Text box.
- Set Lost: Check box, which is unchecked.
- AD Attribute Value: Text box containing "1".

A "Save" button is located at the bottom left of the form.

On the ACE Authentication Manager we can confirm the set pin operation using the Administration Client:

The screenshot shows the "Edit User" dialog box. The "First and Last Name" field contains "Mia Skaffloth" and the "Default Login" field contains "MIA". The "Default Shell" field is empty. The "Local User" radio button is selected. Below this is a table of tokens:

Serial Number	Token Type/Auth With	Status
000023788180	Key Fob/Passcode	Enabled

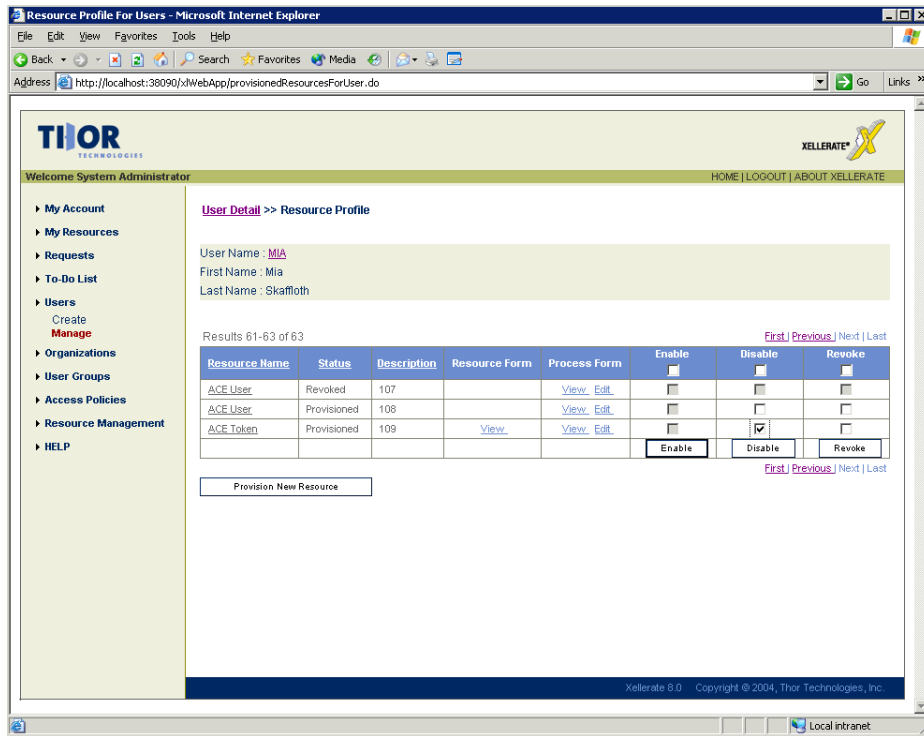
Below the table, it says "O: Original token R: Replacement for previous token". The "Role" is "<none>". The "Assigned Profile" is empty. The "Temporary User" checkbox is unchecked. The "Start Date" is "12/31/2000 16:00" and the "End Date" is "12/31/2009 16:00". The "Allowed to Create a PIN" checkbox is checked, and the "Required to Create a PIN" checkbox is unchecked. At the bottom, there is a grid of buttons:

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

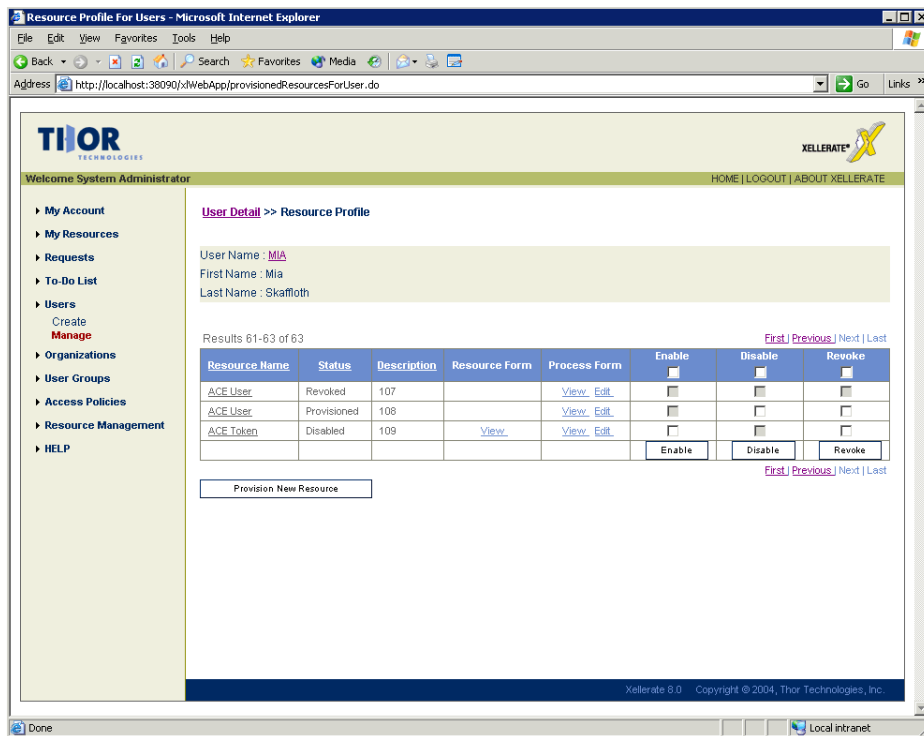
At the very bottom, there are buttons for "OK", "Cancel", "Apply L/S Changes", "Set All L/S", and "Help".

Disable Token

We disable an Token from an existing user's record using the Xellerate Web Administration Interface:



Confirmation of the success of the de-provisioning transaction:



On the ACE Authentication Manager we can confirm that the token is disabled using the Administration Client:

Edit User

First and Last Name:

Default Login:

Default Shell:

Local User Remote User

Serial Number	Token Type/Auth With	Status
000023788180	Key Fob/Passcode	Disabled

0: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary User
Start Date: 12/31/2000 16:00 End Date: 12/31/2009 16:00

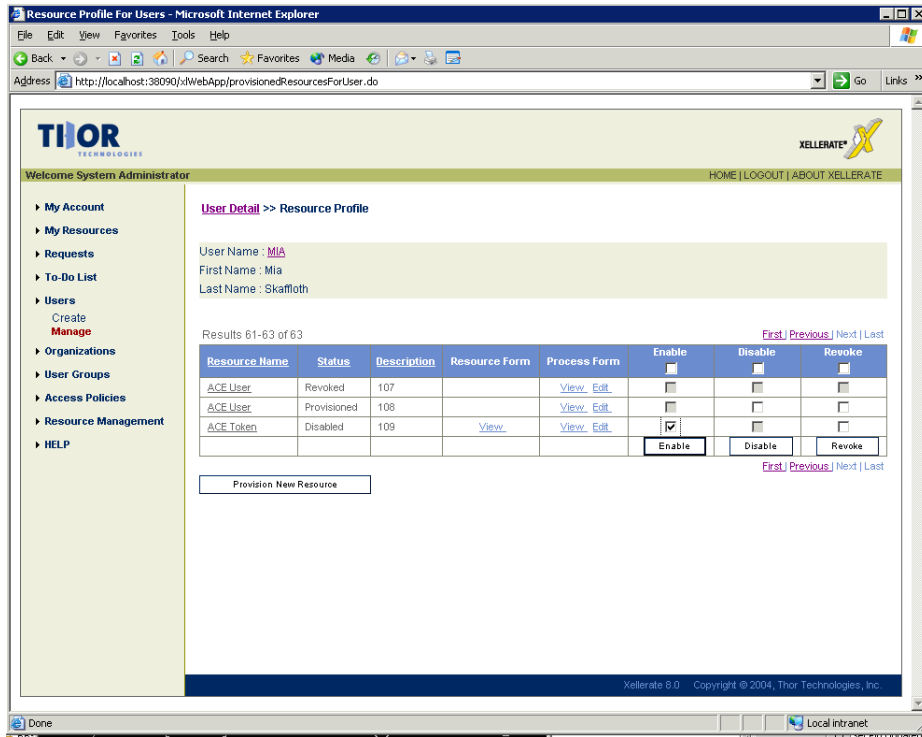
Allowed to Create a PIN Required to Create a PIN

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

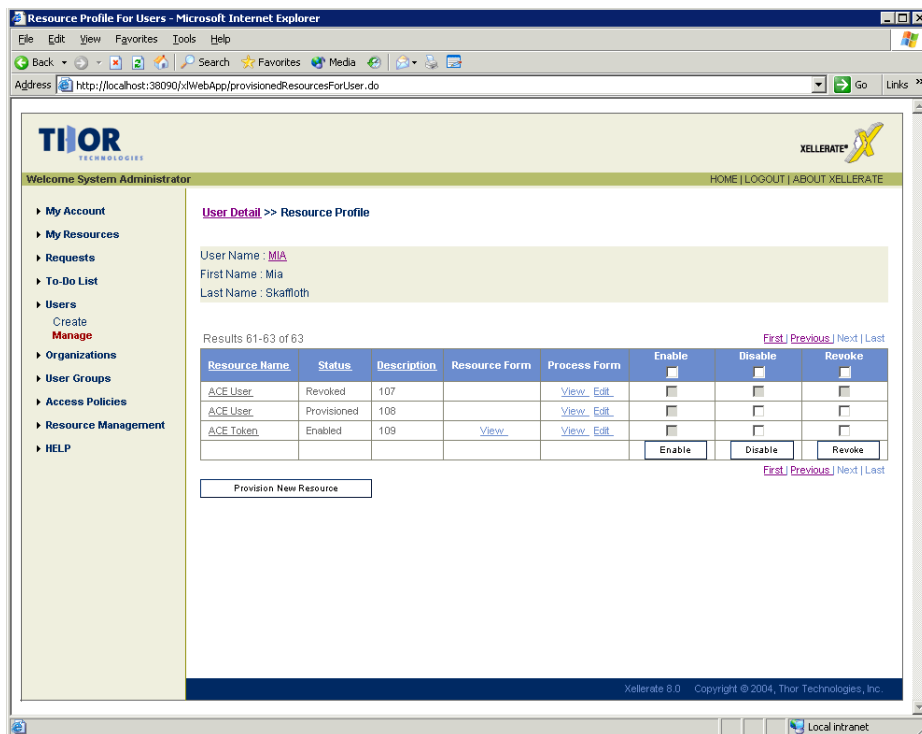
OK Cancel Apply L/S Changes Set All L/S Help

Enable Token

We enable an ACE Token on a existing user record via the Xellerate Web Administration Interface.



Confirmation of the success of the transaction:



On the ACE Authentication Manager we can confirm that the token is enabled using the Administration Client:

Edit User

First and Last Name:

Default Login:

Default Shell:

Local User Remote User

Serial Number	Token Type/Auth With	Status
000023788180	Key Fob/Passcode	Enabled

Tokens:

O: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary User

Start Date: 12/31/2000 16:00 End Date: 12/31/2009 16:00

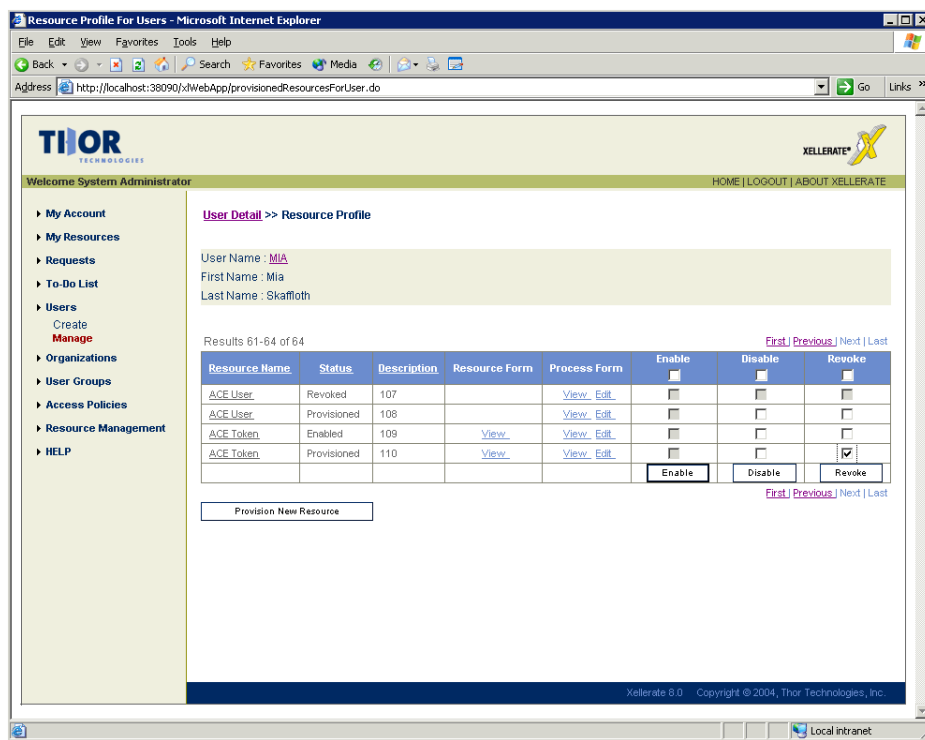
Allowed to Create a PIN Required to Create a PIN

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

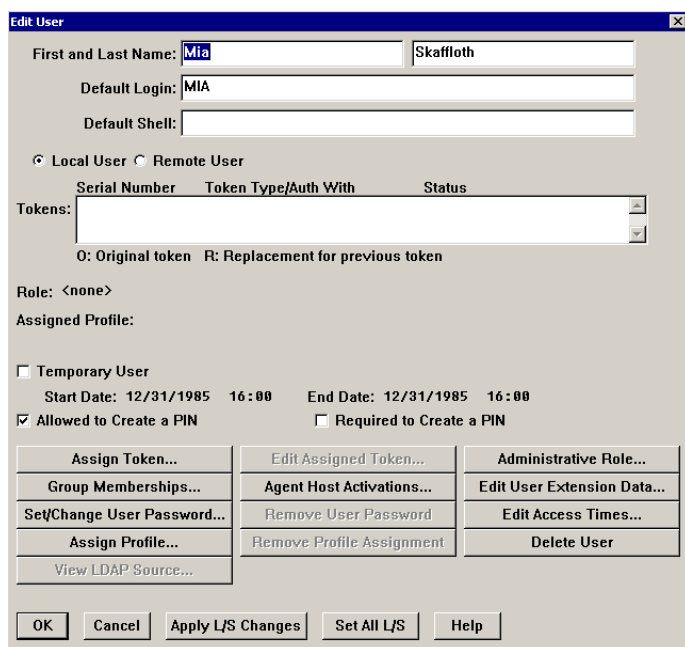
OK Cancel Apply L/S Changes Set All L/S Help

Unassign Token from User

We unassign an ACE Token from a user using the Xellerate Web Administration Interface:

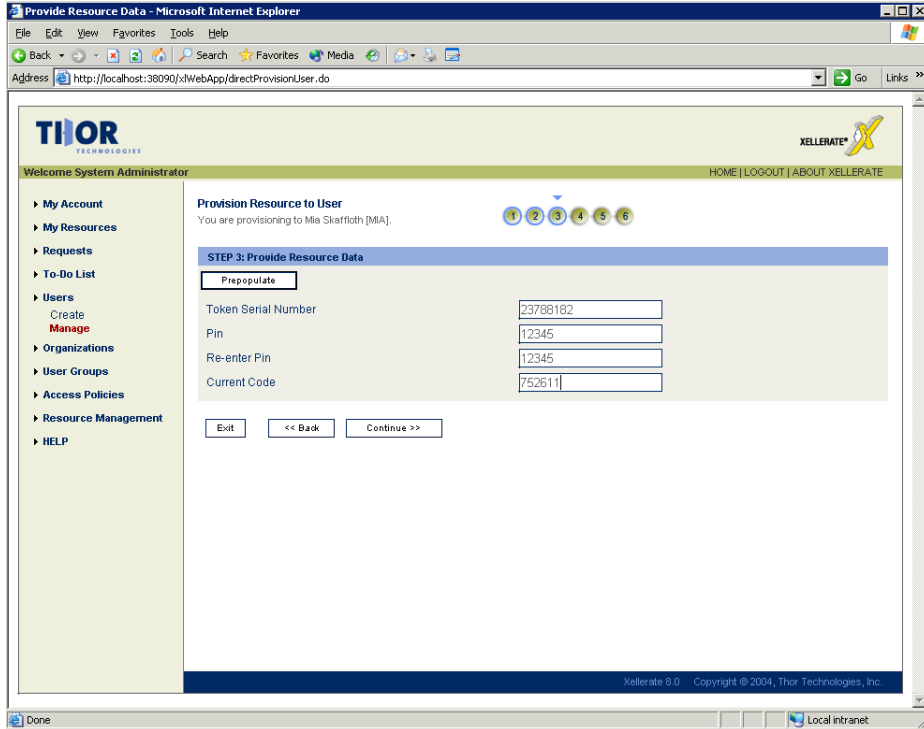


On the ACE Authentication Manager we can confirm the token is unassigned on the user using the Administration Client:

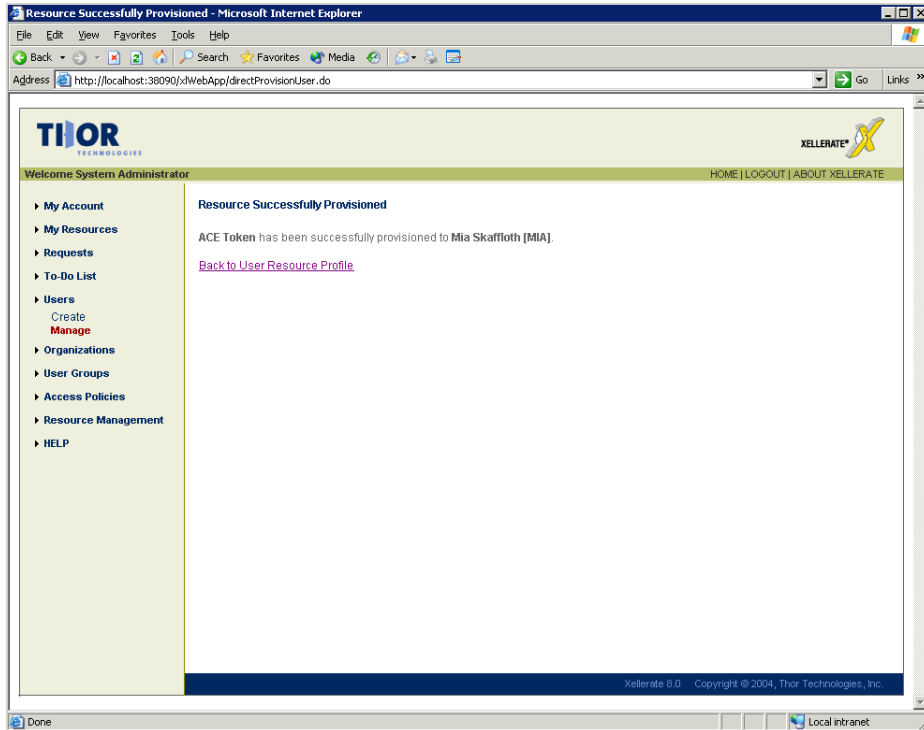


Token Registration

The Assign Token, Set Pin and Test Login operation is usually combined so that a user can Request a Token via Self Service:



Confirmation of the success of the transaction:



On the ACE Authentication Manager we can confirm that the token is enabled using the Administration Client:

Edit User

First and Last Name:

Default Login:

Default Shell:

Local User Remote User

Serial Number	Token Type/Auth With	Status
000023788182	Key Fob/Passcode	Enabled

0: Original token R: Replacement for previous token

Role: <none>

Assigned Profile:

Temporary User

Start Date: 12/31/1985 16:00 End Date: 12/31/1985 16:00

Allowed to Create a PIN Required to Create a PIN

Assign Token...	Edit Assigned Token...	Administrative Role...
Group Memberships...	Agent Host Activations...	Edit User Extension Data...
Set/Change User Password...	Remove User Password	Edit Access Times...
Assign Profile...	Remove Profile Assignment	Delete User
View LDAP Source...		

OK Cancel Apply L/S Changes Set All L/S Help

Certification Checklist

Date Tested: January 5, 2005

Certification Environment		
Product Name	Version Information	Operating System
RSA Authentication Manager	5.0 and 5.2 [178]	Windows 2000 Advanced Server
RSA Authentication Manager	5.2	Windows 2003
RSA Authentication Manager	5.2	Solaris 9
RSA Authentication Agent	N/A	N/A
RSA Software Token		
Xellerate Server	8.0.1	Windows 2003 Enterprise Edition
Xellerate Remote Manager	8.0.1	Windows 2000 Advanced Server

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

INIT / PAR

✓ = Pass ✗ = Fail N/A = Non-Available Function