



RSA Secured Implementation Guide For User Management Products

Last Modified: January 23, 2007

Partner Information

Product Information	
Partner Name	M-Tech Information Technology Inc.
Web Site	http://www.mtechit.com/
Product Name	P-Synch / ID-Synch
Version & Platform	P-Synch Version 6.X, ID-Synch 4.X (Windows 2000/2003)
Product Description	<p>P-Synch is a total password management solution that includes password synchronization, self-service reset, security policy enforcement, profile builders, and more.</p> <p>ID-Synch is a user provisioning solution that enables organizations to effectively manage user access across global, heterogeneous environments. ID-Synch includes automated self-service and delegated setup and management of user accounts. ID-Synch is a comprehensive provisioning solution that can improve network security, user productivity and reduce operating costs for a rapid ROI.</p>
Product Category	Provisioning



Solution Summary

P-Synch and ID-Synch integrate with RSA Access Manager to provide one unified console for management of your user and group information. By logging into ID-Synch, system administrators can create new user accounts that are automatically added to the RSA Access Manager Entitlements Server. Administrators can also manage entitlements to RSA Access Manager protected applications via this same administrative console.

P-Synch and ID-Synch also support user self-registration and password reset for RSA Access Manager.

Partner Integration Overview	
Provisioning Method	RSA Access Manager Admin API / RunTime API
User Management	Yes
User Property Management	Yes
User Password Management	Yes
Group Management	Full
Basic Entitlements Management	Add user to entitlement only. More entitlement support to be added in future releases of ID-Synch.
Smart Rules Management	No
User Self-Service Support	Yes

Product Requirements

Partner Product Requirements: P-Synch Server	
CPU	Pentium IV class or better x86
Memory	Minimum 256 MB RAM
Storage	Minimum 10 GB SCSI Disk
Firmware Version	
Operating System	
Platform	Required Patches
Windows 2000	All Patch Levels Supported
Windows 2003	All Patch Levels Supported

Partner Product Requirements: ID-Synch Server	
CPU	Pentium IV class or better x86
Memory	Minimum 256 MB RAM
Storage	Minimum 10 GB SCSI Disk
Firmware Version	
Operating System	
Platform	Required Patches
Windows 2000	All Patch Levels Supported
Windows 2003	All Patch Levels Supported

Partner Product Requirements: Optional Proxy Server	
CPU	Pentium IV class or better x86
Memory	Minimum 256 MB RAM
Storage	Minimum 10 GB SCSI Disk
Firmware Version	
Operating System	
Platform	Required Patches
Windows 2000	All Patch Levels Supported
Windows 2003	All Patch Levels Supported

Additional Software Requirements (P-Synch Server)	
Application	Additional Patches
Access Manager Admin API	5.5+
Access Manager RunTime API	5.5+
Java 2 Standard Edition	1.4+
IIS, SunOne, or Apache web server	

Additional Software Requirements (ID-Synch Server)	
Application	Additional Patches
Access Manager Admin API	5.5+
Access Manager RunTime API	5.5+
Java 2 Standard Edition	1.4+
IIS, SunOne, or Apache web server	

Additional Software Requirements (Optional Proxy Server)	
Application	Additional Patches
Access Manager Admin API	5.5+
Access Manager RunTime API	5.5+
Java 2 Standard Edition	1.4+

Product Configuration

Before You Begin

This section provides instructions for integrating the partners' product with RSA Access Manager. This document is not intended to suggest optimum installations or configurations. It is assumed that the reader has both working knowledge of the two products to perform the tasks outlined in this section and access to the documentation for both in order to install the required software components. All products/components need to be installed and working prior to this integration. Perform the necessary tests to confirm that this is true before proceeding.

Installation Prerequisites

- Before attempting the integration you should have a fully working installation of P-Synch / ID-Synch & RSA Access Manager.
- The name and port number of your Entitlements and Dispatcher / Key servers should be known.
- An administrative account should be created within RSA Access Manager, which can list, create, and delete users/groups as well as reset passwords for every user to be managed.
- Ensure that an IIS, iPlanet, or Apache web server is installed on your P-Synch / ID-Synch server(s).
- Ensure that the Java 2 runtime environment is installed on your P-Synch / ID-Synch server(s), and that jvm.dll in your system PATH.
- Ensure that the RSA Access Manager Admin and RunTime APIs are installed on your P-Synch / ID-Synch server(s) and that the full path to these files are in the system CLASSPATH environment variable:
 - ct_admin_api.jar
 - asn1.jar
 - certj.jar
 - jsafe.jar
 - ct_runtime_api.jar
 - jsafeJCE.jar
- Also ensure that the full path to the P-Synch / ID-Synch agtctrust5.jar file is also in CLASSPATH (the default location is C:\Program Files\P-Synch\default\agent\agtctrust5.jar).
- Reboot the P-Synch / ID-Synch server(s) after updating the system PATH and CLASSPATH environment variables.

Configuration steps required to enable RSA Access Manager provisioning via ID-Synch

1. Create a new RSA Access Manager target on the ID-Synch server.

The screenshot shows the 'Target information' configuration page in the RSA Access Manager console. The page is titled 'Target information' and includes a sidebar with navigation options like 'Targets', 'Workflow', 'Inventory', etc. The main content area contains a form with the following fields and values:

- Target identifier: ACCESSMGR6
- Target type: RSA ClearTrust
- Target description: Access Manager 6
- Target address: accessmgr6/5601/acce
- Login IDs are case-sensitive:
- Users must have accounts:
- Run list utilities:
- List attributes (if supported by system):
- Use ID filters to include only certain users and accounts:
- Source of profile IDs:
- Import orgchart from this system:
- Uses standard IDs (auto-associate):
- Check accounts on this target for uniqueness when creating new profile IDs: Use default value (Effective setting: Yes)
- Verify passwords on this target:
- Target available for IDA user management:
- Target available for IDR user management:
- Allow other users to claim auto-associated accounts from this target:
- Allow users to remove claims on accounts: Use configured default
- Target type on which to update the definitions of managed groups: (none)
- Minimum number of authorizers: 0
- Number of rejections before the resource is rejected (0=infinite): 0
- Agent timeout: 300
- List timeout: .1
- Minimum list file size: 50
- Program to set the case of new IDs (built-in: upper.pss, lower.pss): lower.pss
- List of proxies to run list/agents on: (empty)
- Target information URL: (empty)
- Request attribute to use as the container DN for this target: (empty)
- Application to be included in the certification process:

At the bottom of the form, there are buttons for 'Update', 'Admin IDs', and 'Delete'.

 **Note:** Target Address: accessmgr6/5601/accessmgr6/5608
(<entitlements server>/<port>/<dispatch server>/<port>)

2. Set the administrative ID / password for the RSA Access Manager administrator created above.

Back Home Refresh Logout

TECH IDM SUITE

Targets Workflow Inventory Web modules Security Maintenance Reports My password

ID: superuser
Name: superuser

Admin IDs for target ACCESSMGR6

Administrator ID: admin
Password: ****
Confirm password: ****

Delete

Administrator ID:
Password:
Confirm password:

Update

3. Optionally, create templates for provisioning new users.

Back Home Refresh Logout

TECH IDM SUITE

Targets Workflow Inventory Web modules Security Maintenance Reports My password

ID: superuser
Name: superuser

Template information

Add new

ID: ACCESSMGRUSER
Description: * Access Manager User
Target system ID: * Access Manager 6 (ACCESSMGR6)
Account to use for replication: * TUser1
Run an agent or use implementers to fulfill requests?: agent
Password required:
Minimum number of authorizers: * 0
Number of rejections before the resource is rejected (0=infinite): * 0
Rejection of this template blocks entire request:
Location: (none)
Type: (none)

Update Delete

This template depends on these templates:

ID	Description

Add

Roles that include this template:

ID	Description
ACCESSMGRROLE	Access Manager Role

Authorizers for this template:

ID	Name

Add

Implementers for this template:

ID	Name

Add

- Optionally, create roles for provisioning new users.

Back Home Refresh Logout

TECH
IDM SUITE

Targets Workflow Inventory Web modules Security Maintenance Reports My password

ID: superuser
Name: superuser

Authorizers
Locations
Object types
Template accounts
Roles
User classes
Request attributes
Managed groups
Request queue
Network resources
Options

Role information

Add new

ID: ACCESSMGRROLE
Description: * Access Manager Role
Minimum number of authorizers: * 0
Number of rejections before the resource is rejected (0=infinite): * 0
Location: (none)
Type: (none)

Update **Delete**

This role includes these sub-roles:

ID	Description

Add

This role includes these templates:

ID	Description
ACCESSMGRUSER	Access Manager User

Delete

Add

Authorizers for this role:

ID	Name

Add

RSA Access Manager User Management functions provided by P-Synch / ID-Synch

P-Synch Functions

- Self Service Password Resets
- Administrative / Help Desk Password Resets.
- Transparent Password Synchronization (Only for LDAP back-end data stores).
- Password Expiry

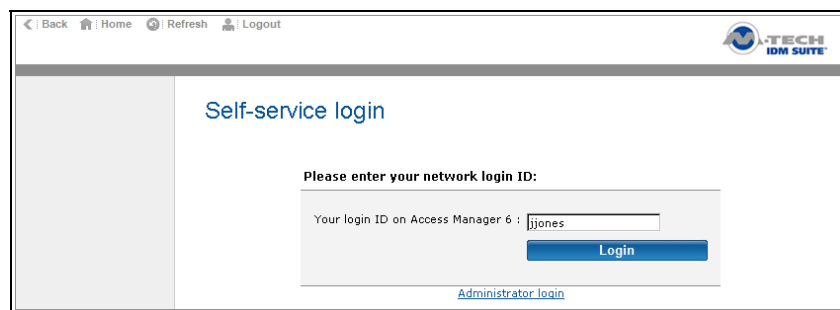
ID-Synch Functions

- Provision New Access Manager users/administrators.
- Remove Access Manager users/administrators.
- Modify Access Manager user/administrator attributes (including user properties & entitlements).
- Enable/Disable Access Manager users/administrators.
- Add Access Manager users/administrators to groups.
- Remove Access Manager users/administrators from groups.
- Provision new Access Manager user groups.
- Remove Access Manager user groups.

Example RSA Access Manager / P-Synch / ID-Synch logon screens

Self-service login

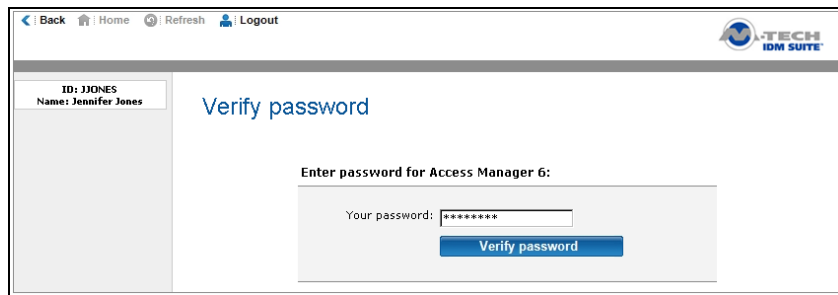
1. Enter your Access Manager login ID.



The screenshot shows a web browser window with the following elements:

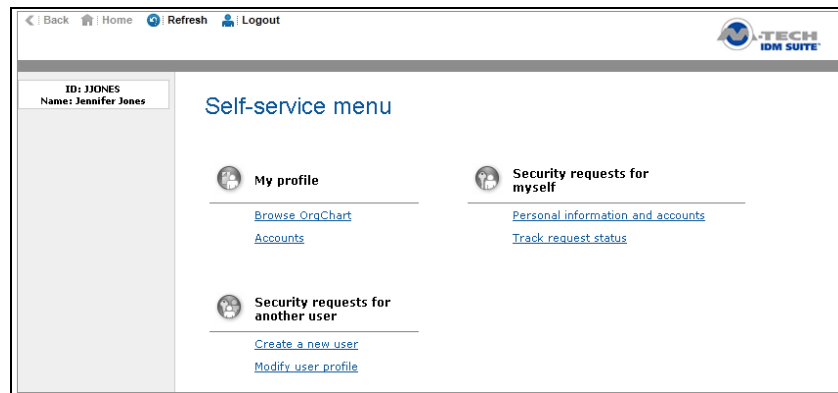
- Browser navigation bar: Back, Home, Refresh, Logout.
- Logo: TECH IDM SUITE.
- Section header: Self-service login.
- Text: Please enter your network login ID:
- Form: Your login ID on Access Manager 6 :
- Link: [Administrator login](#)

2. Enter your Access Manager password.



The screenshot shows a web browser window with the URL bar containing navigation icons for Back, Home, Refresh, and Logout. The page title is "Verify password". On the left, a sidebar displays the user's ID as "JJONES" and Name as "Jennifer Jones". The main content area has the heading "Verify password" and a sub-heading "Enter password for Access Manager 6:". Below this is a text input field labeled "Your password:" containing seven asterisks. A blue button labeled "Verify password" is positioned below the input field. The top right corner features the "TECH IDM SUITE" logo.

3. Use the self-service interface to create or modify user accounts or reset and synchronize your passwords.



The screenshot shows a web browser window with the URL bar containing navigation icons for Back, Home, Refresh, and Logout. The page title is "Self-service menu". On the left, a sidebar displays the user's ID as "JJONES" and Name as "Jennifer Jones". The main content area has the heading "Self-service menu" and three sections, each with a user icon:


- My profile**
 - [Browse OrgChart](#)
 - [Accounts](#)
- Security requests for myself**
 - [Personal information and accounts](#)
 - [Track request status](#)
- Security requests for another user**
 - [Create a new user](#)
 - [Modify user profile](#)

The top right corner features the "TECH IDM SUITE" logo.

Certification Checklist for User Management Products

Date Tested: January 05, 2007

Certification Environment		
Product Name	Version Information	Operating System
RSA Access Manager	6	Windows 2003
P-Synch / ID-Synch	P-Synch 6.X, ID-Synch 4.X	Windows 2000

Test Case	Result
 Note: All test cases should be performed via the User Management Administrative Interface	
Users	
Create new user	✓
Modify user properties	✓
Display user	N/A
Remove user	✓
Reset user password	✓
User self-service password reset	✓
Groups	
Create new group	✓
Modify group properties	N/A
Display group properties	N/A
Remove group	✓
Add user to group	✓
Remove user from group	✓
Basic Entitlements	
Create new entitlement	N/A
Modify entitlement	N/A
Display entitlement	N/A
Remove entitlement	N/A
Add user to entitlement	✓
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

BSD/PAR

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