



Tivoli software

Increase user productivity and security by integrating identity management and enterprise single sign-on solutions.



April 2006

Contents

- 2 Overview**
- 3 Rely on a proven enterprise single sign-on solution**
- 4 Automate credential provisioning and deprovisioning while facilitating audits**
- 5 Understand how the software works**
- 7 Review the steps involved in integration**
- 8 Leverage an easy-to-use administrative console**
- 9 Facilitate auditing with event logging and reporting capabilities**
- 9 Conclusion**
- 10 About Tivoli software from IBM**
- 11 For more information**

Overview

Many organizations are looking for a complete identity management solution that includes enterprise single sign-on (ESSO) as a key component. To help achieve this goal, IBM delivers leading software in the form of IBM Tivoli® Identity Manager and IBM Tivoli Access Manager for Enterprise Single Sign-On software:

- *Tivoli Identity Manager* provides a secure, automated and policy-based solution to help organizations effectively manage user accounts and passwords — from creation to termination, across both legacy and e-business environments. Tivoli Identity Manager helps increase user and IT efficiency, lower costs and facilitate efforts related to compliance and audits.
- *Tivoli Access Manager for Enterprise Single Sign-On* helps organizations advance their identity management, compliance and authentication initiatives by simplifying, extending and securing enterprise single sign-on for end users. Tivoli Access Manager for Enterprise Single Sign-On also helps organizations enhance productivity by simplifying user experiences, reduce help-desk costs related to passwords and optimize security by eliminating poor password management by end users.
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter* enables organizations to integrate both of these offerings. This adapter extends the capability of the Tivoli Access Manager for Enterprise Single Sign-On base solution by directly distributing application credentials from Tivoli Identity Manager to Tivoli Access Manager for Enterprise Single Sign-On. The integration of these two solutions eliminates the need for end users to register — or even see or know — their application credentials and initial passwords as configured and provisioned through Tivoli Identity Manager.

This white paper describes Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter, how it integrates Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On, and the steps an organization must take to facilitate that integration. Furthermore, it describes how organizations deploy and administer the adapter.

Highlights

Use a solution that can scale to tens of thousands of users

Rely on a proven enterprise single sign-on solution

The base Tivoli Access Manager for Enterprise Single Sign-On product is the market-leading ESSO solution powered by Passlogix. The Passlogix solution is licensed by more than two million users at more than 200 customer sites, including the largest ESSO deployment in the world. The United States Postal Service used the software to deploy single sign-on for 7,000 applications to 165,000 users in just eight months.

Tivoli Access Manager for Enterprise Single Sign-On software is designed to help organizations securely bridge:

- Any form of user authentication — Microsoft® Windows® login, smart card, biometric, token and more.
- Any enterprise application — client/server, Java™, Web, legacy or homegrown.
- Any enterprise infrastructure directory, database, network file share and so on.
- Any work mode — desktop, offline, kiosk and shared workstation.

Furthermore, Tivoli Access Manager for Enterprise Single Sign-On is designed to complement IBM Tivoli Access Manager for e-business. The ESSO software tightly integrates to provide single sign-on to Tivoli Access Manager for e-business, which provides fine-grained authorization and entitlements to Web-based resources according to each user's role or group. Both products can share the same directory so that a user is only defined once.

In addition to helping organizations achieve the core benefits of single sign-on, Tivoli Access Manager for Enterprise Single Sign-On delivers quick time to value because it is easy to configure, deploy and administer.

Highlights

Give end users single sign-on from day one

Automate credential provisioning and deprovisioning while facilitating audits

In most organizations, end users have to know, remember and enter their application credentials. This is a particular hassle on the first day a user begins work or takes on a new set of responsibilities and permissions. But when an organization uses Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter, application credential provisioning and deprovisioning between Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On are automated. Consequently, organizations no longer need to physically distribute credentials to end users who must enter them manually into Tivoli Access Manager for Enterprise Single Sign-On. Instead, administrators directly create, edit and delete user credentials through Tivoli Identity Manager. End users can enjoy single sign-on from day one and are no longer responsible for keeping track of their own application credentials – all while helping maximize security.

When end users no longer need access to systems, the integration between the Tivoli applications enables Tivoli Identity Manager to not only remove the users' system and application access but also automatically delete their credentials from the Tivoli Access Manager for Enterprise Single Sign-On data store. Controlling the appropriate level of access helps maximize security and assists with compliance initiatives by demonstrating enforcement of internal controls to auditors.

Furthermore, Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter provides a high level of administrative control. For example, when application passwords are reset in Tivoli Identity Manager, Tivoli Access Manager for Enterprise Single Sign-On is simultaneously

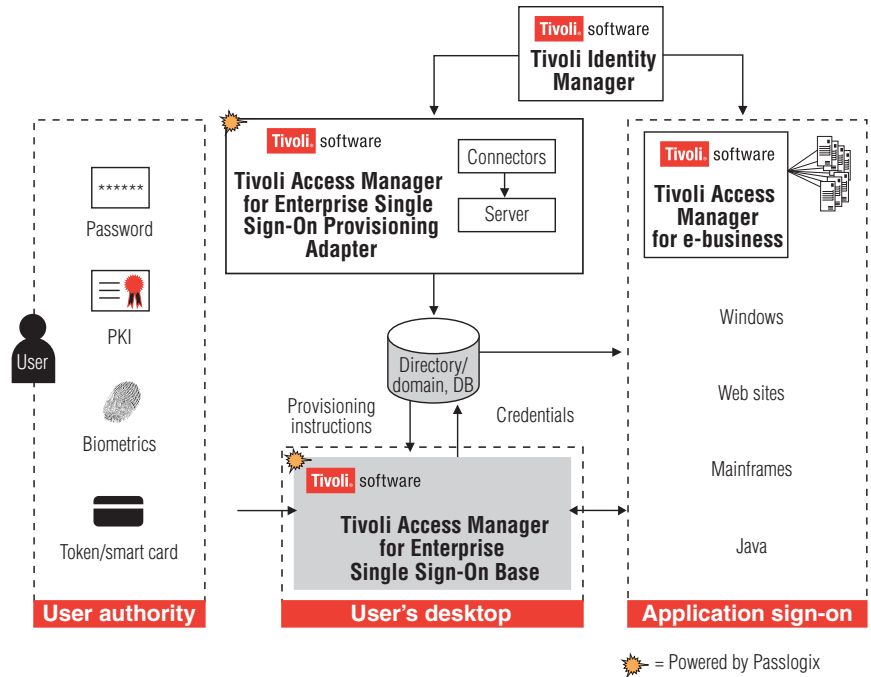
updated so that it always has the correct password. Additionally, it extends audit and reporting capabilities to include information about applications and use of applications that are configured in Tivoli Access Manager for Enterprise Single Sign-On but that fall outside the Tivoli Identity Manager umbrella. Administrators can use the adapter to view a list of all users who are allowed to use a particular application. Or, conversely, they could see all the applications that a particular user can access.

Understand how the software works

When Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter receives instructions from Tivoli Identity Manager that contain credential data, it informs individual Tivoli Access Manager for Enterprise Single Sign-On agents about application configurations that have been added, deleted or changed by:

- Normalizing these instructions into a format that Tivoli Access Manager for Enterprise Single Sign-On can understand.
- Placing them into the directory object for the appropriate user.

When Tivoli Access Manager for Enterprise Single Sign-On synchronizes with the database or directory, it reads and processes the instructions and updates the entries as needed in its local credential cache. Depending on the instructions it receives, Tivoli Access Manager for Enterprise Single Sign-On may add, modify or delete credentials in the appropriate user's local credential cache. Finally, Tivoli Access Manager for Enterprise Single Sign-On synchronizes the credentials back to the database directory object for that user.



Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter application architecture.

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter includes the following components:

- **Server** — accepts account credential provisioning information through a Web services interface. It also communicates that information to Tivoli Access Manager for Enterprise Single Sign-On clients by placing provisioning instructions into the directory or data store they use.
- **Console** — provides a Web-based administration GUI for communicating with the server.
- **Command line interface (CLI)** — enables applications and administrators to communicate with the server.
- **Connector** — integrates the server and Tivoli Identity Manager through the CLI. The connector is a Java-based class library that is implemented as a workflow extension and can be incorporated into any Tivoli Identity Manager provisioning operation. Consequently, administrators can add, edit and delete application credentials for end users through the Tivoli Identity Manager interface. The connector works on any platform where Tivoli Identity Manager runs.

Highlights

Integrate the software in the way that works with your Tivoli Identity Manager deployment

Review the steps involved in integration

Although the connector in Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter must run on a Windows-based PC, organizations can handle integration in two different ways:

- When Tivoli Identity Manager is installed on a Windows-based PC, organizations can use a provided local invocation class library to communicate with the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.
- When Tivoli Identity Manager is installed on a non-Windows-based computer (which must still support Java), organizations can install a Remote Method Invocation (RMI) client that can remotely invoke the connector.

Currently, the connector exposes the following operations:

- ChangePasslogixPassword
- AddPasslogixCredential
- DeletePasslogixCredential
- ModifyPasslogixCredential

The following steps must be followed for integration:

1. Expose provisioning operations in Tivoli Identity Manager.
2. Copy the appropriate connector to the appropriate directories in Tivoli Identity Manager.
3. Reference the connector in Tivoli Identity Manager.
4. Create a configuration file for the connector that specifies the URL and credentials for accessing the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter server.
5. Extend the Tivoli Identity Manager schema.
6. If using the RMI connector, start the RMI server to begin listening for requests from the RMI client.
7. Extend the appropriate Tivoli Identity Manager operations to call the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.
8. Configure the appropriate Tivoli Identity Manager services to be synchronized by the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter.

Highlights

Enable provisioning requests to be passed quietly

When these steps have been taken, the provisioning operations can quietly pass provisioning requests to Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter by invoking the CLI with the appropriate arguments. This integration enables Tivoli Identity Manager to synchronize credentials for Tivoli Access Manager for Enterprise Single Sign-On users with the native application credentials.

Leverage an easy-to-use administrative console

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter is administered through a simple Web-based console. The console accepts provisioning instructions from external sources and transmits them to Tivoli Access Manager for Enterprise Single Sign-On, which processes these instructions to add, modify or delete credentials from a user's credential store.

This administrative console also allows staff to generate reports on new account creation, password resets and account access removal.

Basic Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter functionality can be administered not only through the console but also by using external sources – such as the Tivoli Identity Manager administrative console – or, for manual provisioning, the CLI.

Highlights

Generate reports that can facilitate compliance efforts

Facilitate auditing with event logging and reporting capabilities

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter contains an administrator-controlled event logging capability that enables organizations to monitor and record events. The software can run a number of audit reports, such as the following:

- All users that have a particular application configured in Tivoli Access Manager for Enterprise Single Sign-On
- All applications configured in Tivoli Access Manager for Enterprise Single Sign-On for a particular user
- All provisioning requests
- Usage, based on user object detail

To analyze the event log, simply export it as a comma-separated values (CSV) file, then import the file into virtually any tool used for analysis.

Conclusion

With Tivoli Identity Manager, Tivoli Access Manager for Enterprise Single Sign-On and Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter, administrators can prepopulate and remove end users' Tivoli Access Manager for Enterprise Single Sign-On credential stores so that users never have to touch, or even know, their application credentials.

The integration between Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On through Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter helps organizations:

- Increase productivity by eliminating the need for end users to know their passwords on day one.
- Optimize security and facilitate compliance with security policies by removing access and credentials from Tivoli Access Manager for Enterprise Single Sign-On when the end user no longer requires them.
- Further reduce password-related help-desk costs by eliminating the need for users to manually enter their credentials into Tivoli Access Manager for Enterprise Single Sign-On when credentials are first issued or when they are reset.
- Reduce costs by allowing employees to reset their own passwords all at one time in Tivoli Identity Manager and to take advantage of seamless single sign-on in Tivoli Access Manager for Enterprise Single Sign-On.

About Tivoli software from IBM

Tivoli software from IBM helps organizations efficiently and effectively manage information technology (IT) resources, tasks and processes in order to meet ever-shifting business requirements and deliver flexible and responsive IT service management, while helping to reduce costs. The Tivoli portfolio spans software for security, compliance, storage, performance, availability, configuration, operations and IT lifecycle management, and is backed by world-class IBM services, support and research.

For more information

Tivoli Access Manager for Enterprise Single Sign-On Provisioning Adapter integrates Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On to help simplify and secure the process of provisioning credentials for end users. The software helps customers advance their compliance and identity management initiatives.

To learn more about Tivoli Access Manager for Enterprise Single Sign-On software, contact your IBM representative or IBM Business Partner, or visit [ibm.com/tivoli](https://www.ibm.com/tivoli)



© Copyright IBM Corporation 2005

IBM Corporation
Software Group
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
4-06
All Rights Reserved

IBM, the IBM logo, the On Demand Business logo and Tivoli are trademarks of International Business Machines Corporation in the United States, other countries or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.