Enhancing Password Management by Adding Security, Flexibility, and Agility

IBM Redbooks Solution Guide

The number of logins and passwords that employees must manage on a daily basis continues to be a source of frustration and lost productivity. Employees must remember login information for numerous applications. Many of these applications require different user names and passwords, different password complexity requirements, and forced password changes in shorter intervals. The number of logins that an employee must manage grows with the deployment of each additional business application. The corporate help desk often endures the process of restoring lost or forgotten login information for an employee. These factors together contribute to security risks and increase help desk costs that few organizations can afford not to address.

By using IBM® Security Access Manager for Enterprise Single Sign-On, your organization can address these serious security, productivity, and compliance challenges in a centrally managed solution. Figure 1 illustrates an overview of this solution.

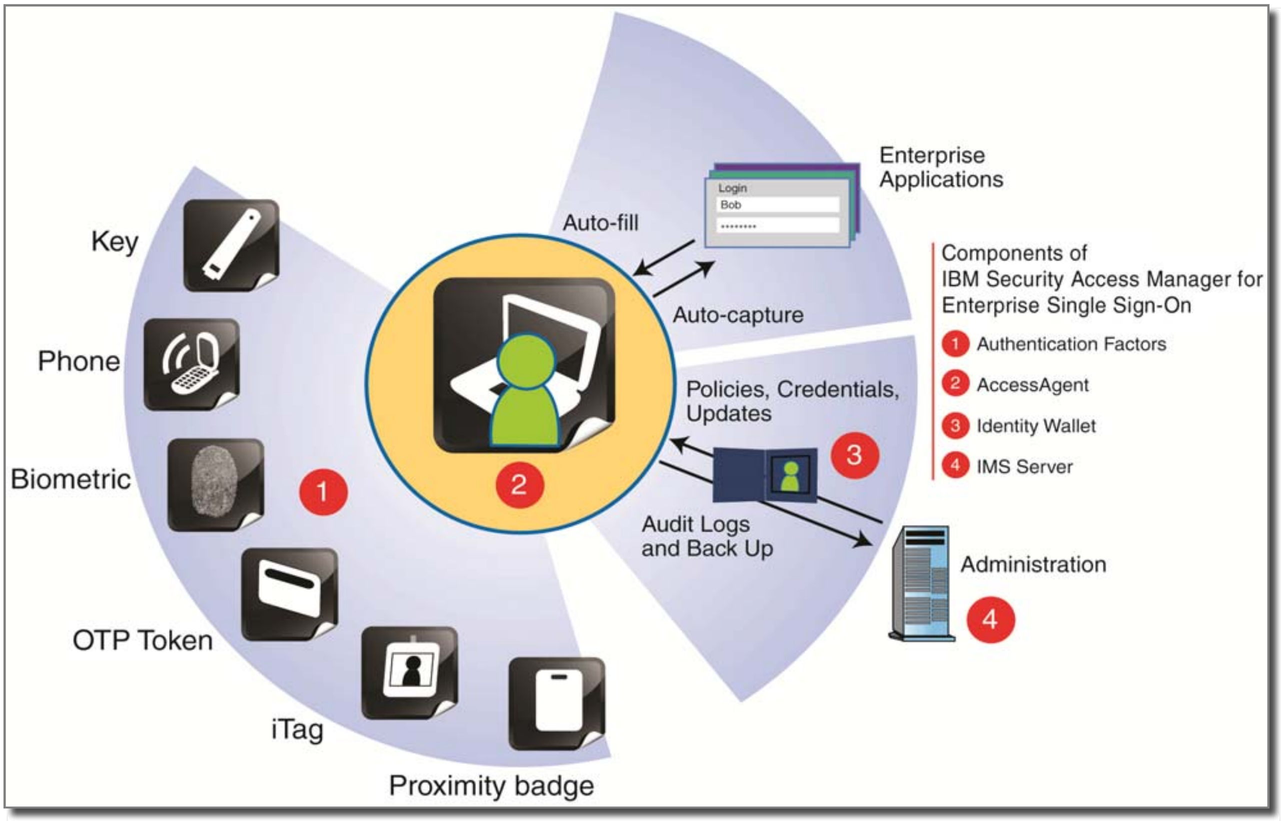

Figure 1. Overview of IBM Security Access Manager for Enterprise Single Sign-On

Did you know?

A frequent user complaint is the requirement to remember multiple passwords, and a major security weakness in computer security is weak password selection. Security breaches as a result of weak passwords or insecure management of passwords are common. Providing a centralized solution for password management and self-service, flexible strong authentication mechanisms, and the capability to use shared and virtual workstations make the IBM Security Access Manager for Enterprise Single Sign-On solution stand out.

Business value and solution overview

IBM Security Access Manager for Enterprise Single Sign-On can help you solve the password paradox. Users must remember only one password and no longer must deal with strong passwords for all corporate applications. They authenticate once, and IBM Security Access Manager for Enterprise Single Sign-On does the rest. IBM Security Access Manager for Enterprise Single Sign-On provides the following major business value:

- Managing passwords in a security-rich fashion

  IBM Security Access Manager for Enterprise Single Sign-On secures password-related applications and data. It uses the strongest cryptography that is available, including Advanced Encryption Standard (AES) and Triple Data Encryption Standard (DES). IBM Security Access Manager for Enterprise Single Sign-On complies with Federal Information Processing Standard (FIPS) 140-2 to help financial institutions, government agencies, healthcare, and other organizations meet the stringent privacy and security regulations that govern their operations. IBM Security Access Manager for Enterprise Single Sign-On also offers second-factor authentication to further increase security. It allows mixing and matching of different factors, depending on the user or machine. If these factors exist, IBM Security Access Manager for Enterprise Single Sign-On can use them.

- Reducing help desk costs and improving employee productivity

  The IBM Security Access Manager for Enterprise Single Sign-On self-service password reset functionality can reduce or eliminate costs that are associated with forgotten passwords and lost employee productivity due to account lockouts. Forgotten passwords and account lockouts, as a result of too many failed attempts, can burden the company help desk. IBM Security Access Manager for Enterprise Single Sign-On provides configurable functions so that users can perform password self-service in ways that meet various security requirements. How users interact with password changes, resets, and account lockout and unlock functions can be customized and allowed or disallowed based on configurable policies. IBM Security Access Manager for Enterprise Single Sign-On grants companies the flexibility to decide whether these password and account service functions stay with the help desk, the user, or a combination of both. The password reset function provides the capability to reset your IBM Security Access Manager for Enterprise Single Sign-On password to regain access to your desktop environment. It does not reset any application-specific passwords.

- Demonstrating compliance through auditing and reporting

  IBM Security Access Manager for Enterprise Single Sign-On includes built-in auditing and reporting for fine-grained user activities on the enterprise desktop. It can record audit events, including user login and logout of applications. The audit mechanism can be customized to capture other relevant information that is related to user activities. The product ships with several included reports, but custom reports can be generated because all audit data is in a single relational database that can be queried.

- Easy to deploy

  Implementing and managing IBM Security Access Manager for Enterprise Single Sign-On is made effective with a web-based administrative console, superior directory integration, and easily deployable client-side software. All administrative functions are performed from a centralized web administrative console (AccessAdmin). Point-and-click wizards in the AccessStudio application walk an administrator through the tasks of profile configuration. An administrator can access the AccessAdmin console from anywhere that a web browser can connect to the server. IBM Security Access Manager for Enterprise Single Sign-On uses a pre-existing user repository without the need to modify the directory schema or any other aspect of the user repository.

- High performance

  In all private, shared, and roaming desktop environments, IBM Security Access Manager for Enterprise Single Sign-On can deliver uncompromising speed. It uses minimal resources when providing a single sign-on (SSO) experience for users to their applications. With its event-specific resource usage, the effect of IBM Security Access Manager for Enterprise Single Sign-On on both the client and the network is minimal. No additional hardware or software is required.

- Integrating with an enterprise identity management system

  The IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge extends the benefits that are generated by IBM Security Access Manager for Enterprise Single Sign-On through the automation of the credential distribution process. The IBM Security Access Manager for Enterprise Single Sign-On Provisioning Bridge uses its API libraries to allow identity management software to automatically provision IBM Security Access Manager for Enterprise Single Sign-On user credentials. This way, users never have to know their user name or password for their applications because it can be managed transparently for them.

  If users need to know their user name and password for a particular application, they can obtain that information by accessing the credential store (Wallet). This access is possible only if they are authenticated to IBM Security Access Manager for Enterprise Single Sign-On. If they are not working at a workstation with an AccessAgent, they can access that information by using the AccessAssistant web browser-based interface. Even if not integrated with identity management software, IBM Security Access Manager for Enterprise Single Sign-On allows for a highly available and secure password-reveal process through these components.

- Bringing SSO to kiosk machines and virtual desktops

  The convenience of allowing others to share a workstation unfortunately does not come without risks. Too often users walk away from a kiosk machine without logging off, potentially exposing sensitive data. IBM Security Access Manager for Enterprise Single Sign-On addresses this threat by its ability to automate the termination of inactive sessions and application shutdown. That automation includes such features as automatic walk away logouts, through radio frequency identification (RFID) proximity keys, or smart card removal.

  IBM Security Access Manager for Enterprise Single Sign-On provides robust session management support for roaming desktop implementations. It uses technologies, such as Microsoft Windows Terminal Services and Citrix XenApps, and uses shared desktops or kiosk machines and private desktops. Users can roam easily and securely from one workstation to another. IBM Security Access Manager for Enterprise Single Sign-On also includes support for securing virtual desktop infrastructure (VDI) technologies, such as VMware View. Additionally, IBM Security Access Manager for Enterprise Single Sign-On includes thin client and client-less access through roaming desktop mode and through Web Workplace.

Solution architecture

IBM Security Access Manager for Enterprise Single Sign-On provides its SSO functionality by introducing a layer that authenticates a user one time and then automatically detects and handles subsequent requests for user credentials.

IBM Security Access Manager for Enterprise Single Sign-On can be divided into the following architectural components, as illustrated in Figure 1:

- Authentication factors

  IBM Security Access Manager for Enterprise Single Sign-On supports various authentication factors to authenticate the user. In addition to the standard user name and password-based authentication, the user can be authenticated by a proximity or building badge. Examples are active or passive RFID, a fingerprint, a one-time password (OTP) that is provided by Short Message Service (SMS) or OTP token, or a USB token.

- AccessAgent

  AccessAgent runs on every Windows desktop endpoint, Windows Server Terminal Services session, VMware vSphere virtual desktop interface session, and Citrix XenApp Presentation Server session. AccessAgent is responsible for authenticating the user. It can automate SSO into Windows and to the set of applications that are defined in AccessProfiles. AccessAgent can extend the Windows Graphical Identification and Authentication (GINA) dynamic link library (DLL) chain to provide additional functions for self-service or strong authentication.

- Identity Wallet

  The Identity Wallet (or Wallet) holds the user credentials that are required for SSO. It is loaded from the IBM IMS™ Server into AccessAgent after successful authentication of the user so that it is available even when the endpoint is disconnected from the computer network. To protect the credentials against tampering or stealing, the Identity Wallet is encrypted with a strong encryption mechanism.

- IMS Server

  The IMS Server is the central repository for user data, AccessProfiles, Identity Wallets, and machine profiles. The IMS Server provides a web-based interface to administer users and policies.

Usage scenarios

In this usage scenario, a healthcare provider operates several stand-alone clinics, where each clinic occupies its own building and provides preventive care, cardiac surgery, and outpatient services. The healthcare provider consists of a large group of medical and supporting staff that are directly employed by the company and a smaller group of independent surgeons that are contracted by the company.

The healthcare provider maintains financial data and private customer data (patients, research partners, and affiliated hospitals). Most records are kept in electronic form in SAP systems. In addition, email is available to the entire staff of the company to communicate internally and with the outside world (patients and external partners).

Figure 2 shows the architecture diagram of the healthcare company, which includes major communication lines between the separate network zones.

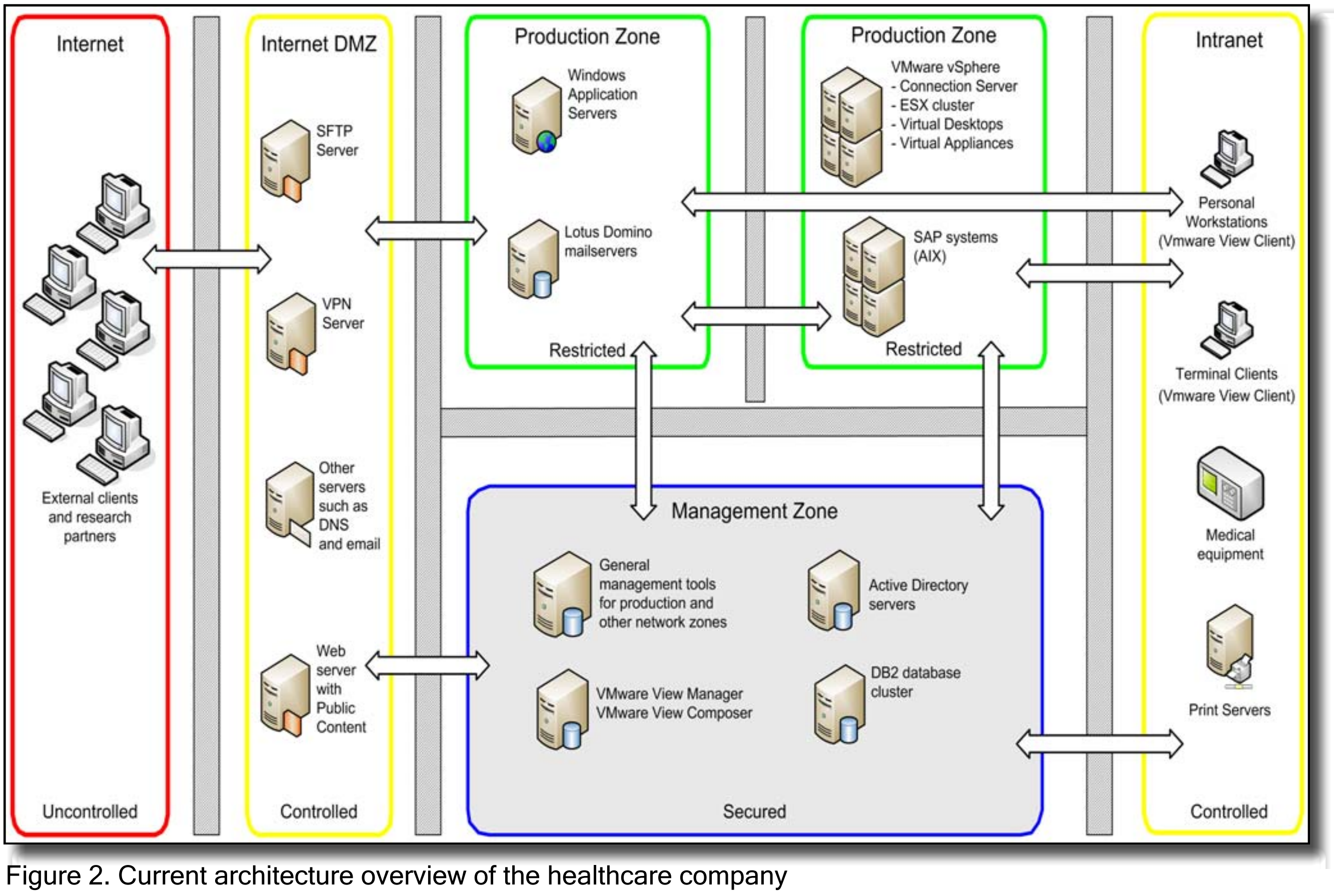

Figure 2. Current architecture overview of the healthcare company

The healthcare company wants to achieve the following short-term business goals:

- Improve the quality and availability of patient care and satisfaction by delivering an excellent, individualized healthcare experience.
- Increase the protection of all patient-related information, and address the diverse security risks that are driven by compliance requirements, emerging technologies, and data explosion.
- Facilitate the management and demonstration of the overall compliance posture with data privacy laws and industry regulations, such as Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI-DSS).

Overall, the healthcare company wants mature security solutions that can prevent information leaks and that can ensure trustworthy authentication and individual traceability and accountability of all actions that affect the patients.

The following components are deployed for a base-level implementation of IBM Security Access Manager for Enterprise Single Sign-On:

- Central user repository or directory

  The central user repository can be one of several supported repositories, including Active Directory, Novell, and generic Lightweight Directory Access Protocol (LDAP). The central user repository must be in place before installing any IBM Security Access Manager for Enterprise Single Sign-On components. In the healthcare company environment, the central user repository is Active Directory, as shown in Figure 2.

- IMS Server

  The IMS Server is an application that is based on Java that runs on its own instance of IBM WebSphere® Application Server. It can be a software installation on a Windows server platform, or it can be integrated in a packaged virtual appliance. The IMS Server is deployed in the Management Zone shown in Figure 2.

- IMS database

  The IMS database stores all of the configuration, policy, and user data for IBM Security Access Manager for Enterprise Single Sign-On. This database can be created on an existing database server, or it can be installed on the same system with the IMS Server. The supported databases include IBM DB2®, Microsoft SQL, and Oracle. In the healthcare company environment, an existing DB2 database is used as the database, as shown in Figure 2.

- AccessAgent

  An AccessAgent is installed on each client system, Windows Terminal Server, VMware Virtual Desktop, and Citrix XenApp server that is to be managed by IBM Security Access Manager for Enterprise Single Sign-On.

- AccessStudio

  AccessStudio is an administrative tool that is used to create AccessProfiles. It must be installed on only one workstation, normally on the workstation of one or more IMS Server administrators. Because AccessStudio requires AccessAgent, you install AccessAgent on the same workstation before you install AccessStudio.

After deploying the base infrastructure components, the healthcare provider implements the following capabilities:

- Password self-service

  If users at the healthcare company forget their Microsoft Windows password, they must contact the IT support desk to have the support desk personnel reset their password on their behalf after performing the necessary security checks. IBM Security Access Manager for Enterprise Single Sign-On overcomes this problem by providing the password self-service function of the product. Users that have a connection to the IMS Server can reset their own passwords.

  By using the password self-service feature of IBM Security Access Manager for Enterprise Single Sign-On, users can reset their primary authentication from any workstation, based on a challenge-response process. (The primary authentication can be the IBM Security Access Manager for Enterprise Single Sign-On password or desktop password.) All questions are customizable and configurable. When the IBM Security Access Manager for Enterprise Single Sign-On password self-service is configured (no additional components must be installed), the user has no need to call technical support. Also, the user does not have to wait for an administrator to reset the password.

Instead, the users provide secondary secrets that they set up during the sign-up phase of AccessAgent. No additional components must be installed to use the password self-service function.

- Strong authentication using RFID

  The healthcare company wants to use a secure way of *fast user switching* for its medical staff. These users, who use the shared terminal clients that are spread throughout the hospitals, need a faster and more convenient way to log on to the system. The medical staff often need to update a patient record with a few short comments before attending to the next patient, but they need to enter brief comments frequently each day. Also, the medical staff need to enter their user name and (complex) password numerous times per day to access their virtual desktop environment, which leads to frustration. The company committed to address this issue. However, it is not willing to compromise security.

  The healthcare company opted to deploy RFID badge readers to all shared terminal clients. By using this function, the medical staff can link their RFID access badge to their SSO user name and password. The policy is designed to prompt the medical staff to present their RFID badge and their password one time each day. For the remainder of their shift, the staff can present their RFID badge to the reader, and they are automatically logged on to their SSO Wallet.

- Roaming desktop implementation

  When a user logs on to a shared workstation in a semi-public area by using a password or an RFID badge, a connection to this user's Virtual Desktop is automatically started. The process of logging on the user to this Virtual Desktop must occur through secure and tamper-proof methods.

  A user that is logged on to a Virtual Desktop must be able to use the supported applications without providing authentication credentials. This function must work the same as if those applications run on the shared workstation from where they connect. When a user logs off from a shared workstation, the roaming virtual desktop and its applications must continue to run on the Virtual infrastructure. Shared workstation inactivity policies must be as strict as possible to prevent other people from accessing a lingering Virtual Desktop session. Inactive sessions need to terminate automatically.

  The medical staff members use distributed workstations to automatically log on by using their RFID badges and connect to their virtual desktops that are hosted on a VMware ESXi Server. Figure 3 illustrates the targeted solution component architecture.

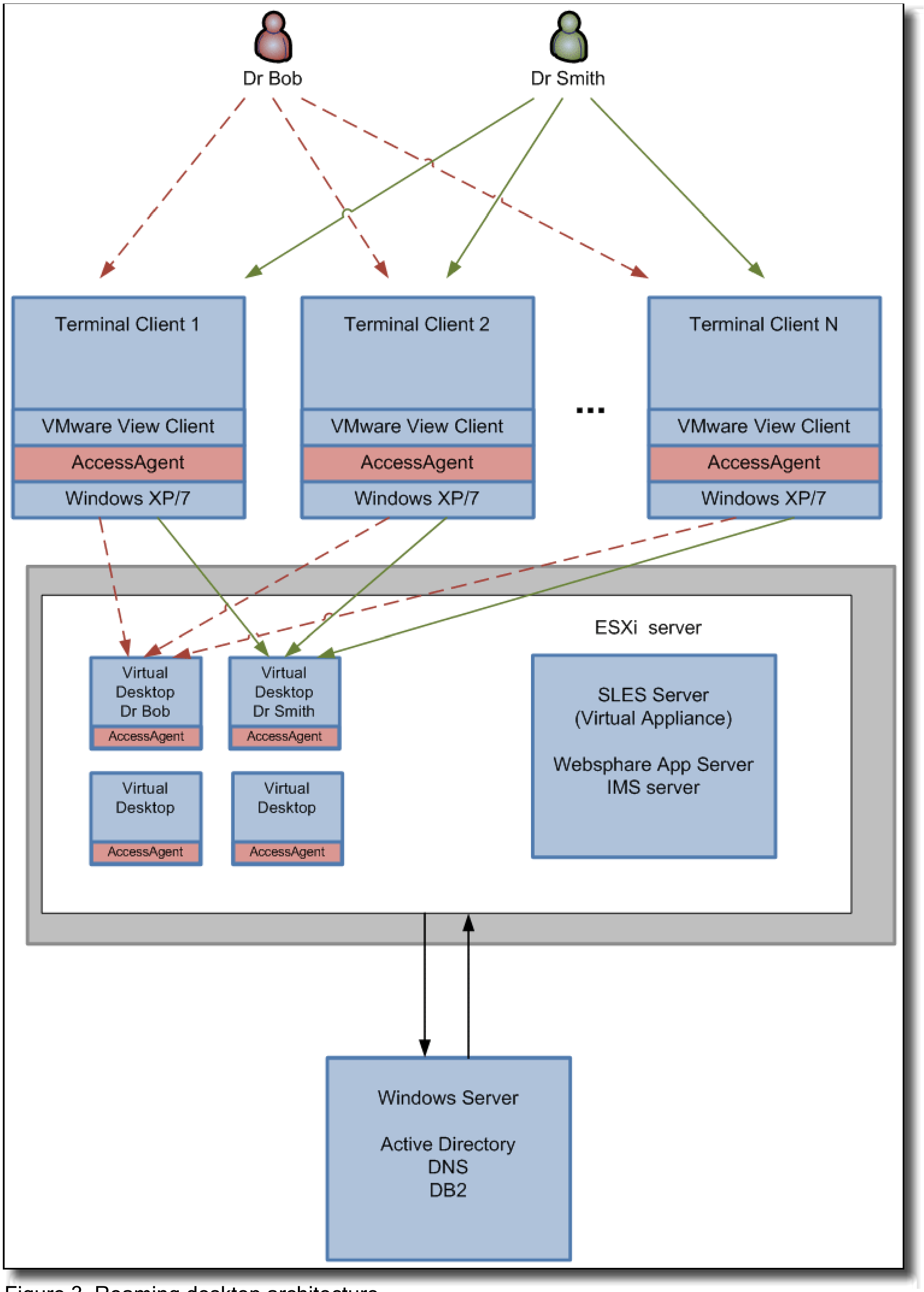

Figure 3. Roaming desktop architecture

Ordering information

This product is available only through IBM Passport Advantage®. It is not available as a shrink-wrapped product. Detailed ordering information is available in the IBM announcement letters (see the "Related information" section).

Related information

For more information, see the following documents:

- *Enterprise Single Sign-On Design Guide Using IBM Security Access Manager for Enterprise Single Sign-On 8.2*, SG24-7350
  http://www.redbooks.ibm.com/abstracts/sg247350.html?Open
- *BIO-key Biometric Service Provider for IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4892
  http://www.redbooks.ibm.com/abstracts/redp4892.html?Open
- *A Guide to Authentication Services in IBM Security Access Manager for Enterprise Single Sign-On*, REDP-4835
  http://www.redbooks.ibm.com/abstracts/redp4835.html?Open
- *A Guide to Writing Advanced Access Profiles for IBM Tivoli Access Manager for Enterprise Single Sign-On*, REDP-4767
  http://www.redbooks.ibm.com/abstracts/redp4767.html?Open
- *Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments*, REDP-4700
  http://www.redbooks.ibm.com/abstracts/redp4700.html?Open
- IBM Security Access Manager for Enterprise Single Sign-On product page
  http://www.ibm.com/software/tivoli/products/access-mgr-esso
- IBM announcement letters and sales manuals
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  On this page, enter `IBM Security Access Manager for Enterprise Single Sign-On`, and click **Search**. On the next page, narrow your search results by information type, geography, language, or all three options.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document was created or updated on December 7, 2012.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips0943.html .

Trademarks