Tivoli software

IBM

Certification Study Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0

- Helps you achieve Tivoli Access Manager for Enterprise Single Sign-On certification
- Explains the certification path and prerequisites
- Includes sample test questions and answers

Axel Buecker
Azania Abebe
Benjamin Schroeter

Redbooks

ibm.com/redbooks

International Technical Support Organization

Certification Study Guide: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0

August 2009

SG24-7784-00

Note: Before using this information and the product it supports, read the information in “Notices” on page vii.

First Edition (August 2009)

This edition applies to IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.0.1.

Contents

Notices vii
Trademarks viii

Preface ix
The team that wrote this book ix
Become a published author xi
Comments welcome xi

Chapter 1. Certification overview 1
1.1 IBM Professional Certification Program 2
1.1.1 Benefits of certification 3
1.1.2 Tivoli Software Professional Certification 4
1.2 Tivoli Access Manager for Enterprise Single Sign-On V8.0 certification . . . 7
1.2.1 Job description and target audience 7
1.2.2 Key areas of competency 7
1.2.3 Required prerequisites and skill levels 8
1.2.4 Test 000-020 objectives 9
1.3 Recommended educational resources 28
1.3.1 Courses 28
1.3.2 Publications 30

Chapter 2. Planning 33
2.1 Considerations for deployment 34
2.2 Solution design 35
2.2.1 Basic solution definition 35
2.2.2 Design approach 36
2.2.3 Project phases and deployment stages 37
2.3 System architecture 38
2.3.1 Logical component architecture 40
2.3.2 Additional Components 51
2.3.3 Security requirements 51
2.3.4 Physical architecture 56
2.4 Solution considerations 60
2.4.1 Application profiles 60
2.4.2 Considering second factor and machine types 61
2.4.3 Core strategies 62
2.4.4 Policy management strategy 63
2.4.5 Authentication strategy 63
2.4.6 Integration strategy 65

2.4.7 High availability and scalability 68
2.4.8 Upgrades and migration strategy 72

Chapter 3. Deployment and implementation 75
3.1 Installation overview 76
3.1.1 System requirements 77
3.1.2 Deployment architecture 77
3.1.3 Create administrative users 79
3.1.4 Install the IMS database software 80
3.1.5 Install the IMS Server 80
3.1.6 Initial IMS Server configuration 82
3.1.7 Specify IMS Server settings using AccessAdmin 83
3.1.8 Install the AccessAgent 85
3.1.9 Install AccessStudio 87
3.2 AccessProfile configuration 88
3.2.1 Standard AccessProfiles 90
3.2.2 Advanced AccessProfiles 101
3.3 Web Workplace 109

Chapter 4. Configuration 111
4.1 IMS configuration steps after installation 112
4.2 Enterprise directory 112
4.3 IMS Provisioning Bridge 115
4.4 Provisioning Agent 117
4.5 Remote Access Integration solution 120
4.6 AccessAgent for Citrix 121
4.7 User role assignment 122
4.7.1 Re-assigning roles for help desk users 122
4.7.2 Automatic role assignment for large deployments 123
4.8 Managing policies 124
4.8.1 Policy template 126
4.9 Usage workflows 129
4.9.1 Personal workstation 130
4.9.2 Shared workstation configuration 130
4.10 Thin client solution 133
4.11 Using the IMS Configuration Utility 135
4.12 Using AccessAdmin 136
4.13 Using AccessAssistant 138
4.14 Strong authentication 139
4.14.1 USB Key authentication 141
4.14.2 OTP token authentication 142
4.14.3 RFID authentication 142
4.14.4 Active RFID authentication 144

4.14.5 Fingerprint authentication 144
4.14.6 Authorization code authentication 145
4.14.7 Mobile active code authentication 148
4.15 Password self-service 150
4.16 Auditing and reporting 151
4.16.1 IMS Server housekeeping 152
4.16.2 Tamper-evident audit logs 153

Chapter 5. Administration 155
5.1 Managing AccessProfiles using AccessStudio 156
5.1.1 How AccessStudio works 156
5.1.2 AccessStudio basic concepts 157
5.1.3 AccessStudio advanced concepts 157
5.1.4 AccessStudio interface 158
5.1.5 Managing authentication services 158
5.1.6 Managing application objects 159
5.1.7 Account data items and templates 160
5.1.8 Signatures 160
5.1.9 Validating functions 160
5.1.10 AccessProfile testing 160
5.1.11 Downloading, uploading, and saving information 161
5.1.12 Backing up IMS Server data 161
5.2 IMS Server configuration and maintenance 162
5.2.1 Configuring the IMS Server 162
5.2.2 IMS Server maintenance 162
5.2.3 Backing up the database 162
5.2.4 Viewing logs 163
5.3 AccessAdmin user search and maintenance 163
5.4 Policy management 164
5.4.1 Defining policies 164
5.4.2 Viewing and setting system policies 165
5.4.3 Viewing and setting policy priorities 165
5.5 Reports and audit logs 166
5.5.1 Viewing and printing audit logs 166
5.5.2 Viewing and printing audit reports 166
5.5.3 Integrating an audit log with a commercial reporting tool 167
5.5.4 Maintaining audit logs 167
5.6 Migration strategy and considerations 167
5.6.1 Switching to another IMS Server 167
5.6.2 Copying AccessProfiles between IMS Servers 168
5.6.3 Configuration tips 169
5.6.4 Preparing the IMS database 170

Chapter 6. Performance tuning and problem determination 171
6.1 Optimizing IMS Server performance 172
6.1.1 Improving server scalability and availability 173
6.1.2 Distributed IMS using replicated databases 175
6.2 Improve AccessAgent performance 176
6.3 Microsoft Operations Manager 176
6.4 Problem determination 179
6.4.1 Installation issues 179
6.4.2 IMS Server issues 184
6.4.3 AccessAgent issues 186
6.4.4 Other issues 194
6.4.5 Documenting a PMR 197

Appendix A. Sample questions 201
Questions 202
Answers 206

Related publications 207
IBM Redbooks 207
Other publications 207
Online resources 208
How to get Redbooks 208
Help from IBM 208

Index 209

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.

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.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DB2®	Lotus®	Redbooks (logo) ®
IBM®	Notes®	Sametime®
Lotus Notes®	Redbooks®	Tivoli®

The following terms are trademarks of other companies:

Novell, the Novell logo, and the N logo are registered trademarks of Novell, Inc. in the United States and other countries.

Oracle, JD Edwards, PeopleSoft, Siebel, and TopLink are registered trademarks of Oracle Corporation and/or its affiliates.

SAP, and SAP logos are trademarks or registered trademarks of SAP AG in Germany and in several other countries.

VMware, the VMware "boxes" logo and design are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions.

J2EE, Java, JavaScript, JDBC, JMX, JVM, Sun, Sun Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Active Directory, Excel, Internet Explorer, JScript, Microsoft, Outlook, SQL Server, Win32, Windows Server System, Windows Server, Windows Vista, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Preface

This IBM® Redbooks® publication is a study guide for the “IBM Certified Deployment Professional - IBM Tivoli® Access Manager for Enterprise Single Sign-On V8.0” certification test, test number 000-020, and is meant for those who want to achieve IBM Certifications for this specific product.

The IBM Tivoli Access Manager for Enterprise Single Sign-On Certification, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who work with the implementation of the IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.0 product.

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that will be encountered in the exam.

This publication does not replace practical experience, and it is not designed to be a stand-alone guide for any subject. Instead, it is an effective tool which, when combined with education activities and experience, can be a very useful preparation guide for the exam.

The team that wrote this book

This book was produced by a team of specialists from around the world working at the International Technical Support Organization (ITSO), Austin Center.

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of software security architecture and network computing technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 23 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

Azania Abebe is a Certified Senior Security Consultant with the IBM Software Services, Tivoli Security, and Privacy Practice. He has extensive industry experience in the identity management space specializing in the delivery of Tivoli-based technologies and enterprise solutions around identity and access management. He has over 14 years combined experience in information technology and software development of enterprise applications. Currently, Azania focuses on architecting solutions and advising IT organizations on effective alignment of IT infrastructure, security requirements, and business objectives.

Benjamin Schroeter is a pre-sales Security Consultant for identity and access management at IBM in Berlin, Germany. He has 4 years of experience in IT Security with focus on design and implementation of software solutions. He is a Tivoli Certified Professional and an IBM Certified Teacher, giving classes on various Tivoli products. He holds a degree in Applied Computer Science from the University of Cooperative Education in Stuttgart, Germany.

Thanks to the following people for their contributions to this project:

Emma Jacobs, Diane Sherman
International Technical Support Organization

Brian Goldsmith, Judy Green, Vladimir Jeremic, Gino Maa, Daryl Romano, Chris Weber, Peter Wolf
IBM

Become a published author

Join us for a two- to six-week residency program! Help write a book dealing with specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients.

Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our books to be as helpful as possible. Send us your comments about this book or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an e-mail to:

  redbooks@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

1

Certification overview

In this chapter, we provide an overview of the skill requirements necessary to obtain an IBM Advanced Technical Expert certification.

The following sections are designed to provide a comprehensive review of specific topics that are essential for obtaining the certification:

- IBM Professional Certification Program
- Tivoli Access Manager for Enterprise Single Sign-On V8.0 certification
- Recommended educational resources

1.1 IBM Professional Certification Program

Having the right skills for the job is critical in the growing global marketplace. IBM Professional Certification, designed to validate skill and proficiency in the latest IBM solution and product technology, can help provide that competitive edge. The IBM Professional Certification Program Web site is available at:

http://www.ibm.com/certify/index.shtml

The IBM Professional Certification Program offers a business solution for skilled technical professionals seeking to demonstrate their expertise to the world.

The program is designed to validate your skills and demonstrate your proficiency in the latest IBM technology and solutions. In addition, professional certification can help you excel at your job by giving you and your employer confidence that your skills have been tested. You can deliver higher levels of service and technical expertise than non-certified employees and move on a faster career track. Professional certification puts your career in your control.

The certification requirements are difficult, but not impossible. Certification is a rigorous process that differentiates you from everyone else.

The mission of IBM Professional Certification is to:

- Provide a reliable, valid, and fair method of assessing skills and knowledge.
- Provide IBM with a method of building and validating the skills of individuals and organizations.
- Develop a loyal community of highly skilled certified professionals who recommend, sell, service, support, and use IBM products and solutions.

The IBM Professional Certification Program has developed certification role names to guide you in your professional development. The certification role names include IBM Certified Specialist, IBM Certified Solutions/Systems Expert, and IBM Certified Advanced Technical Expert for technical professionals who sell, service, and support IBM solutions.

For technical professionals in application development, the certification roles include IBM Certified Developer Associate and IBM Certified Developer. IBM Certified Instructor certifies the professional instructor.

The IBM Professional Certification Program provides a structured program leading to an internationally recognized qualification. The program is designed for flexibility by enabling you to select your role, prepare for and take tests at your own pace, and, in some cases, select from a choice of elective tests best suited to your abilities and needs. Some roles also offer a shortcut by giving credit for a certification obtained in other industry certification programs.

You might be a network administrator, systems integrator, network integrator, solution architect, solution developer, value-added reseller, technical coordinator, sales representative, or educational trainer. Regardless of your role, you can start charting your course through the IBM Professional Certification Program today.

1.1.1 Benefits of certification

Certification is a tool to help objectively measure the performance of a professional on a given job at a defined skill level. Therefore, it is beneficial for individuals who want to validate their own skills and performance levels, their employees, or both. For optimum benefit, the certification tests must reflect the critical tasks required for a job, the skill levels of each task, and the frequency by which a task has to be performed. IBM prides itself in designing comprehensive, documented processes that ensure that IBM certification tests remain relevant to the work environment of potential certification candidates.

In addition to assessing job skills and performance levels, professional certification can also provide such benefits as:

- For employees:
  - Promotes recognition as an IBM Certified Professional
  - Helps to create advantages in interviews
  - Assists in salary increases, corporate advancement, or both
  - Increases self-esteem
  - Provides continuing professional benefits
- For employers:
  - Measures the effectiveness of training
  - Reduces course redundancy and unnecessary expenses
  - Provides objective benchmarks for validating skills
  - Makes long-range planning easier
  - Helps to manage professional development
  - Aids as a hiring tool
  - Contributes to competitive advantage
  - Increases productivity, morale, and loyalty
- For Business Partners and consultants:
  - Provides independent validation of technical skills
  - Creates competitive advantage and business opportunities
  - Enhances prestige of the team
  - Contributes to IBM requirements for various IBM Business Partner programs

Specific benefits can vary by country (or region) and role. In general, after you become certified, you should receive the following benefits:

- Industry recognition

  Certification can accelerate your career potential by validating your professional competency and increasing your ability to provide solid, capable technical support.

- Program credentials

  As a certified professional, you receive (through e-mail) your certificate of completion and the certification mark associated with your role for use in advertisements and business literature. You can also request a hardcopy certificate, which includes a wallet-size certificate. IBM Professional Certification acknowledges the individual as a technical professional. The certification mark is for the exclusive use of the certified individual.

- Ongoing technical vitality

  IBM certified professionals are included in mailings from the IBM Professional Certification Program.

1.1.2 Tivoli Software Professional Certification

The IBM Tivoli Professional Certification Program offers certification testing that sets the standard for qualified product consultants, administrators, architects, and partners.

The program also offers an internationally recognized qualification for technical professionals who are seeking to apply their expertise in today's complex business environment. The program is designed for those who implement, buy, sell, service, and support Tivoli solutions and who want to deliver higher levels of service and technical expertise.

Whether you are a Tivoli customer, partner, or technical professional wanting to put your career on the fast track, you can start your journey to becoming a Tivoli Certified Professional today.

Benefits of being Tivoli certified

Tivoli Certification has the following benefits:

- For the individual:
  - IBM Certified certificate and use of logos on business cards
  - Recognition of your technical skills by your peers and management
  - Enhanced career opportunities
  - Focus for your professional development

- For the Business Partner:
  - Confidence in the skills of your employees
  - Enhanced partnership benefits from the Business Partner Program
  - Higher rates for billing out your employees
  - Stronger customer proposals
  - Demonstration of the depth of technical skills available to prospective customers
- For the customer:
  - Confidence in the services professionals handling your implementation
  - Ease of hiring competent employees to manage your Tivoli environment
  - Enhanced return on investment (ROI) through more thorough integration with Tivoli and third-party products
  - Ease of selecting a Tivoli Business Partner that meets your specific needs

Certification checklist

To pursue certification, follow the steps in this checklist:

1. Select the certification you would like to pursue.
2. Determine which tests are required by reading the certification role description.
3. Prepare for the test by using the following resources:
   - Test objectives
   - Recommended educational resources
   - Sample assessment test
   - Other reference materials
   - Opportunities for experience

   Note: These resources are available from each certification description page and from the test information page.

4. Register to take a test, by contacting one of our worldwide testing vendors:
   - Prometric
   - Pearson Virtual University Enterprises (VUE)

   Note: When providing your name and address to the testing vendor, be sure to specify your name exactly as you want it to appear on your certificate.

5. Take the test. Be sure to keep the Examination Score Report provided upon test completion as your record of taking the test.

   Note: After you take the test, the results and demographic data (including name, address, e-mail, and phone number) are sent from the testing vendor to IBM for processing (allow two to three days for transmittal and processing). After all the tests required for a certification are passed and received by IBM, your certificate will be issued.

6. Repeat steps 3 on page 5 - 5 until all required tests are successfully completed for the certification. If you must meet additional requirements (such as another vendor certification or exam), follow the instructions on the certification description page to submit these requirements to IBM.
7. After you meet the requirements, you will receive an e-mail asking you to accept the terms of the IBM Certification Agreement.
8. Upon your acceptance, you receive an e-mail with the following deliverables:
   - A Certification certificate in PDF format, which can be printed in either color or black and white
   - A set of graphic files containing the IBM Professional Certification mark that is associated with the certification achieved
   - Guidelines for the use of the IBM Professional Certification mark
9. To avoid an unnecessary delay in receiving your certificate, ensure that your current e-mail is on file by keeping your profile up to date. If you do not have an e-mail address on file, your certificate will be sent by postal mail.

   Certificates are sent by e-mail. However, you may also contact IBM at the following e-mail address to request a paper copy of the certificate, including a laminated wallet-sized card:

   mailto:certify@us.ibm.com

Note: IBM reserves the right to change or delete any portion of the program, including the terms and conditions of the IBM Certification Agreement, at any time without notice. Some certification roles offered through the IBM Professional Certification Program require recertification.

1.2 Tivoli Access Manager for Enterprise Single Sign-On V8.0 certification

In this section, we categorize the certification process for IBM Tivoli Access Manager for Enterprise Single Sign-On.

Important: IBM offers the following promotion code, which is good for a 15% discount on the indicated Tivoli certification exams if taken at any Prometric testing center:

- Code: 15T020
- Percentage off: 15%
- Valid for exams: 000-020

1.2.1 Job description and target audience

An IBM Certified Deployment Professional - Tivoli Access Manager for Enterprise Single Sign-On V8.0 is an individual who has demonstrated the ability to design, implement, and support an IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0 solution. This person is expected to perform the tasks independently a majority of the time with limited assistance from peers, product documentation, and vendor support services, and in some situations, take leadership and provide mentoring to peers.

1.2.2 Key areas of competency

The following key areas of competency are required for you to pass the Certification Test 000-020.

- Describe the Tivoli Access Manager for Enterprise Single Sign-On architecture and components.
- Implement a Tivoli Access Manager for Enterprise Single Sign-On solution based on customer requirements, and environment based on solution design.
- Install and configure prerequisites to Tivoli Access Manager for Enterprise Single Sign-On.
- Understand Tivoli Access Manager for Enterprise Single Sign-On strong authentication support.
- Use available interfaces to configure and administer the Tivoli Access Manager for Enterprise Single Sign-On environment.
- Perform performance tuning and problem determination for Tivoli Access Manager for Enterprise Single Sign-On.

1.2.3 Required prerequisites and skill levels

The prerequisites and skill levels you should have before taking Certification Test 000-020 are listed in Table 1-1. Skill levels are defined after the table.

Table 1-1 Prerequisites and skill levels

Prerequisite	Skill level
Basic HTML and JavaScript™ fundamentals	3
Databases (SQL, Oracle® and DB2®)	3
Directory services fundamentals	3
VBScript and JScript®	3
Operating system administrative skills for Windows®	2
Security policy management concepts	2
TomCat Web server fundamentals	2
Programming fundamentals	2
User registry installation	2
Networking concepts	2
PKI fundamentals	2
Firewall concepts	2
Security communication protocols	1
TCP/IP fundamentals	1
XML skills	1

Skill levels are defined as follows:

- Level 1: Basic Skill/Knowledge: Familiarity with basic functionality and concepts; might have to rely on assistance from documentation or other resources.
- Level 2: Working Skill/Knowledge: Working knowledge of functionality and concepts; can use product or explain concepts with little or no assistance.
- Level 3: Advanced Skill/Knowledge: Substantial experience with functionality or concepts; can teach others how to use functionality or explain concepts.
- Level 4: Expert Skill/Knowledge: Extensive and comprehensive experience with functionality or concepts; can create or customize code, architecture, or processes.

1.2.4 Test 000-020 objectives

Let us look more closely at the six objectives for this test:

- Planning
- Implementation
- Deployment
- Configuration
- Administration
- Performance tuning and problem determination

Section 1: Planning

The section provides more information about the planning area of the test:

- Given access to the customer, their hardware, applications, and policies, collect and analyze the customer's requirements so that a solution document is created. The emphasis is on being able to perform the following tasks:
  - Arrange a kick-off meeting with stakeholders.
  - Interview the appropriate personnel.
  - Review the security infrastructure of the customer.
  - Identify and understand the customer's single sign-on requirements:
    i. Determine key objectives for Enterprise Single Sign-On project.
    ii. Collect the list of applications to be included in project.
    iii. Analyze the customer's environment.
  - Identify the auditing requirements.
  - Create a solution document.
- Given the topology of the client network (number of PCs, subnets, and so on), the number of users, and the network link capacity, measure the network performance and analyze IBM Tivoli Access Manager for Enterprise Single Sign-On's impact on the environment so that an estimate of the maximum network bandwidth consumed is available. The emphasis is on being able to perform the following tasks:
  - Identify the most active period of time when users tend to log into IBM Tivoli Access Manager for Enterprise Single Sign-On.
  - Estimate the number of users involved.
  - Estimate the size of their wallets by taking into account the number of accounts stored, number of profiles, and so on.
  - Estimate the average number of automatic fill of credentials that are done over the same period.

- Identify the synchronization interval.
- Use this information and generate an estimate of the maximum network bandwidth consumed.

- Given the customer's environment, explain the solution architecture so that a solution document with minimum hardware and software requirements for the solution is created. The emphasis is on being able to perform the following tasks:
  - Arrange a meeting with customers.
  - Explain the functionality of the IMS Server.
  - Explain the type of information stored and managed by the DB and where it has to be running.
  - Explain the use of LDAP.
  - Explain the purpose of Load Balancer.
  - Explain several administration tools that an administrator can use for different purposes (AccessAdmin, AccessAssistant, and AccessStudio).
  - Explain where the AccessAgent has to be installed and the purpose.
  - Explain the minimum hardware and software requirements for each component including supported clients.
  - Explain any consideration regarding network requirements for supported clients and supported servers.
  - Explain supported Web Browsers.
  - Explain supported Thin Clients.
  - Create a document with minimum hardware and software requirements for the solution.
- Given access to the customer applications, collect and analyze the customer application requirements so that an Application Profile checklist/document is created. The emphasis is on being able to perform the following tasks:
  - Arrange a kick-off meeting with stakeholders.
  - Get a representative desktop and application list.
  - Review the customer applications in scope.
  - Identify and understand customer's specific application requirements:
    i. Determine which applications are Web, Windows, mainframe, Java™, and others.
    ii. Determine which application password change workflow is required.
    iii. Determine password policies for each application.

iv. Determine if any applications share credentials (that is, a common LDAP).

v. Identify any potentially *challenging* applications.

vi. Identify mechanisms and personnel for password resets/expiry.

– Obtain or create credentials on the applications for testing purposes.

– Create an Application Profile checklist/document.

- Given access to the customer's test hardware, applications, test credentials, and IBM Tivoli Access Manager for Enterprise Single Sign-On installers, collate the data so that the components of the staging environment is determined and documented. The emphasis is on being able to perform the following tasks:

  – Acquire test server, test workstations, and IBM Tivoli Access Manager for Enterprise Single Sign-On software.

  – Reach an agreement with the customer to use recommended staging environment.

  – Identify test applications that should be installed on the test workstations.

  – Identify test user accounts.

    i. Verify which accounts to use for IBM Tivoli Access Manager for Enterprise Single Sign-On administrator account.

    ii. Verify which accounts to use for IBM Tivoli Access Manager for Enterprise Single Sign-On lookup account.

    iii. Verify which accounts to use for IBM Tivoli Access Manager for Enterprise Single Sign-On user accounts.

    iv. Verify which accounts to use for application profile creation/testing.

  – Determine host name/URL to be used for staging IMS Server.

  – Identify the DB to be used and obtain valid DB credentials.

  – Identify the directory server to be used and obtain valid credentials.

  – Create a staging environment document.

- Given access to the customer's Single Sign-On Project Manager, hardware, network administrator, and an estimate of the maximum network bandwidth consumed, determine high availability (HA) and load balancing environment requirements so that a high availability design document is created. The emphasis is on being able to perform the following tasks:

  – Arrange a meeting with single sign-on project manager, enterprise network administrator, and infrastructure personnel.

- Collect information about existing network bandwidth and usage statistics and load infrastructure existing in the customer environment.
- Collect information necessary to estimate hardware sizing for HA:
  i. Collect peak hour traffic estimates for one-time password (OTP) login and AccessAdmin logins/second.
  ii. Determine peak installation and user sign-up rates.
  iii. Collect IMS database utilization and clustering requirements.
  iv. Collect load balancing architecture requirements.
- Share the collected information with the IBM Tech Line.
- Size hardware requirements for HA.
- Architect high availability solution for IBM Tivoli Access Manager for Enterprise Single Sign-On components.
- Create a high availability design document.

- Given access to the AccessAgent installer, the domain controller, client machine, and a network share accessible to all clients, create an AccessAgent Installation Group Policy Object of Active Directory® (GPO) and deploy it to the client machines. The emphasis is on being able to perform the following tasks:
  - Review the Active Directory infrastructure.
  - Copy the AccessAgent installer to some network share which is accessible to all clients.
  - Create a new GPO or identify an existing GPO to setup for AccessAgent Installation.
  - Configure changes to the GPO.
  - Add the client machine into the scope of this GPO.
  - Restart the client machine.
- Given the business requirement document, determine a Windows session management strategy so that a deployment recommendation for session management in the customer environment is created. The emphasis is on being able to perform the following tasks:
  - Review the security infrastructure of the customer.
  - Identify and understand customer's session management requirements:
    i. Determine key objectives for shared/roaming and personal workstation.
    ii. Collect the usage of fast user switching in the environment.

iii. Collect the usage of kiosk environment.

iv. Collect the second factor information.

– Create the Windows session management strategy document.

- Given the authentication mechanisms, second factor options, and access to the customer's authentication requirement, determine a strong authentication strategy so that a strong authentication strategy is documented. The emphasis is on being able to perform the following tasks:
  - Analyze customer's authentication requirements.
  - Identify the areas of authentication setup:
    i. Analyze any second factor authentication policy requirements.
    ii. Analyze the Mobile ActiveCode requirement.
    iii. Analyze any OTP requirement.
  - Identify the second factor or factors to use: passive radio frequency identification (RFID), active RFID, Fingerprint, and USB SmartCard.
  - Validate the appropriate reader, if applicable:
    i. Identify the readers that are compatible with the hardware.
    ii. Check the readers that are compatible with the operating systems supported by IBM Tivoli Access Manager for Enterprise Single Sign-On.
    iii. Eliminate the list further by comparing the readers with the ones supported by IBM Tivoli Access Manager for Enterprise Single Sign-On.
  - Document the strong authentication strategy.
- Given the customer's requirements, determine the need and identify resources for any integration with IBM Tivoli Access Manager for Enterprise Single Sign-On application programming interface (API), so as to define an integration strategy (if required). The emphasis is on being able to perform the following tasks:
  - Determine whether any customer's requirements need integration with IBM Tivoli Access Manager for Enterprise Single Sign-On API.
  - Identify the IBM Tivoli Access Manager for Enterprise Single Sign-On API that can meet the requirement (for example, IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning API).
  - Define strategy and provide the implementer (possibly yourself) information or documentation necessary to implement the integration.

- Given the prerequisites for databases, prepare the database so that the database is ready for IMS Server installation. The emphasis is on being able to perform the following tasks:
  - Identify customer database requirements.
  - Prepare the Database for the IMS Server installation.
  - Verify the network connection between the IMS Server and the Database Server if those are in different workstation or servers.
  - Obtain relevant access to create the database instance to be used by IMS Server.
  - Determine the path of the database (where it is installed).
  - Synchronize the system clocks if IMS database and IMS Server will be running on different machines.
- Given requirements for upgrade, analyze the existing Tivoli Access Manager for Enterprise Single Sign-On environment so that an appropriate upgrade strategy is created. The emphasis is on being able to perform the following tasks:
  - Determine upgrade steps.
  - Identify existing infrastructure affected by upgrade steps.
  - Identify necessary stakeholders in upgrade.
  - Create an update strategy document containing this information, and with a notification plan.

Section 2: Implementation

The section provides more information about the implementation area of the test:

- Given access to the customer applications and test credentials, utilize the AccessStudio wizard so that working AccessProfiles are created for the customer's applications. The emphasis is on being able to perform the following tasks:
  - Verify access to necessary applications.
  - Verify valid credentials for all applications.
  - Validate workflows required for each application (for example, change password, login, logout, and session timeout).
  - Verify whether a profile exists.
  - Create AccessProfile using Assistant (wizard).
  - Test AccessProfile.

- Given access to the customer applications and test credentials, utilize the AccessStudio advanced profiling so that working AccessProfiles are created for the customer's applications. The emphasis is on being able to perform the following tasks:
  - Verify access to necessary applications.
  - Verify valid credentials for all applications.
  - Validate workflows required for each application (for example, change password, login, logout, and session timeout).
  - Verify whether a profile does not exist.
  - Create AccessProfile using Advanced profiling.
  - Test AccessProfile.
- Given a functional IMS Server, set up the IMS Server and implement Web Workplace on the IMS Server so that a functional Web workplace is available. The emphasis is on being able to perform the following tasks:
  - Identify required Web workplace behavior and applications to be enabled.
  - Create Web AccessProfiles for identified Web applications.
  - Set Web Workplace-related policies.
  - Embed Web Workplace links into customer portal or VPN.

Section 3: Deployment

The section provides more information about the deployment area of the test:

- Given the IBM Tivoli Access Manager for Enterprise Single Sign-On Server installer, set up the server component so that the IMS Server is installed successfully. The emphasis is on being able to perform the following tasks:
  - Verify the operating system prerequisite and free disk space.
  - Install and configure the Database and configure the enterprise directory.
  - Verify the IMS prerequisites.
  - Run the installer of the Server.
  - Configure host name details and database instance details during the installation.
  - Verify that the IMS Server is installed on the system.
- Given a test workstation, the customer's requirement, and an existing IMS Server, install IBM Tivoli Access Manager for Enterprise Single Sign-On AccessAgent so that it is installed on the workstation with correct configurations. The emphasis is on being able to perform the following tasks:
  - Ensure that the machine to be installed on will get the correct machine policy template as defined in template assignments on AccessAdmin.

- Ensure that an AccessAgent installer package is available and has been customized for the deployment. (Possible customizations include banner graphic, registry edits, `.ini` file options, and editing the installer `.msi` file to point to the location of configuration files).
- Ensure that second factor hardware is connected, if needed.
- Ensure that drivers for second factor hardware are installed, if needed.
- On the workstation, run the `.msi` to install IBM Tivoli Access Manager for Enterprise Single Sign-On AccessAgent. A restart is necessary on completion. This step can be done manually or through any software deployment tool.

- Given the IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio installer, set up the AccessStudio component so that AccessStudio is installed on the customer system. The emphasis is on being able to perform the following tasks:
  - Verify the operating system prerequisite and free disk space.
  - Install the AccessStudio.
  - Verify that the AccessStudio is installed on the system.

Section 4: Configuration

The section provides more information about the configuration area of the test:

- Given the requirements for IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server integration with a provisioning system, implement the Provisioning Bridge so that the user provisioning workflows are implemented successfully. The emphasis is on being able to perform the following tasks:
  - Identify the minimum requirements for both of the provisioning system and IMS Server that can integrate with the IMS.
  - Create an IMS Bridge account at IMS for use by the Provisioning Bridge.
  - Configure a key store for the IMS Provisioning Bridge on the provisioning server.
  - Configure the IMS Provisioning Bridge (to point to the correct key-store, IMS, and so on).
  - If the provisioning system does not provide an out-of-the-box integration with IMS, investigate the following information:
    i. If the system is based on J2EE™ or supports Java interfaces, integrate with the IMS Bridge Java APIs.

ii. If the system is capable of making command-line calls, integrate with the IMS Bridge command-line interfaces (tools) into the system.

iii. If the system is capable of making SOAP calls, integrate with the IMS SOAP interfaces.

– If the provisioning system provides an out-of-the-box integration with IMS, configure it accordingly.

– Test the system for successful integration with the Provisioning Bridge.

- Given the IBM Tivoli Access Manager for Enterprise Single Sign-On Solution, implement the provisioning agent so that the provisioning agent is implemented on the customer environment. The emphasis is on being able to perform the following tasks:
  – Set up a new IMS Bridge using the IMS Configuration Utility.
  – Configure the correct certificates.
  – Configure the IBM Tivoli Access Manager for Enterprise Single Sign-On provisioning agent.
  – Test and install the provisioning agent.
  – Verify that the provisioning agent is implemented on the system.
- Given an enterprise directory, implement the directory integration with IBM Tivoli Access Manager for Enterprise Single Sign-On so that IBM Tivoli Access Manager for Enterprise Single Sign-On is successfully integrated with enterprise directory structure. The emphasis is on being able to perform the following tasks:
  – Identify the appropriate directory connector.
  – Configure the enterprise directory using IMS Configuration Utility.
  – For Microsoft® Active Directory (AD) deployments, enable *AD password sync* where appropriate.
  – Test the enterprise directory.
- Given a VPN solution, a remote browser, a second factor authenticator, access the configuration pages and configure so that a user can use the remote access solution with VPN. The emphasis is on being able to perform the following tasks:
  – Configure the IMS using the Configuration Utility.
    i. Open the IMS Configuration Utility Web page.
    ii. Configure Mobile ActiveCode (MAC)/one-time password (OTP) Settings.
    iii. Configure Message Connector settings.

iv. Enable MAC/OTP for SSL VPN.

v. Configure Remote Authentication Dial-In User Service (RADIUS) interface.

– Configure integration with the SSL VPN Appliance as indicated in IBM Tivoli Access Manager for Enterprise Single Sign-On Remote Access Integration Guide.

- Given an understanding of the customer's requirements, customize user policies so that the user policy templates are designed, and subsequently configured on the IMS Server. The emphasis is on being able to perform the following tasks:
  - Create the User Policy templates based on customer's requirements.
  - Identify the default user policy template.
  - Determine the user directory attribute to be used for assignment.
  - Configure the assignment attribute in the IMS Configuration Utility.
  - Implement the policies in AccessAdmin.
  - Customize individual user policies if necessary.
- Given access to the solution document and customer's IBM Tivoli Access Manager for Enterprise Single Sign-On environment, configure workstation usage workflows so that the desired workstation usage workflows are created. The emphasis is on being able to perform the following tasks:
  - Configure personal workstation usage workflow:
    i. Set up IAM Enterprise in a personal workstation.
    ii. Implement personal workstation lock, unlock, logon, and logoff scripts, if necessary.
  - Configure usage workflows for shared desktop:
    i. Determine usage workflows for shared desktop.
    ii. Implement shared desktop lock, unlock, logon, and logoff scripts, if necessary.
  - Configure usage workflows for private desktop:
    i. Determine usage workflows for private desktop.
    ii. Implement private desktop lock, unlock, logon, and logoff scripts, if necessary.
  - Configure usage workflows for roaming desktop:
    i. Determine usage workflows for roaming desktop.
    ii. Implement roaming desktop for Citrix/TS environment.
- Given access to the solution document and customer's IBM Tivoli Access Manager for Enterprise Single Sign-On environment, define the machine

policy templates and assignments so that the desired machine template policy with assignments is created. The emphasis is on being able to perform the following tasks:

- Create new machine policy templates based on customer's requirements:
  i. Configure authentication policy.
  ii. Configure wallet policy.
  iii. Configure sign-up policy.
  iv. Configure shared workstation policy and accessagent policy.
  v. Create the rules for assignment.
- Select one of the new machine policy template as the default policy to be used.
- Change the template assignment of existing machines if reassignment is required.

- Given a functional IMS Server and client requirements for the thin client, deploy the corresponding thin client solution so that the thin client is working. The emphasis is on being able to perform the following tasks:
  - Determine the type of remote server (Microsoft Terminal Server or Citrix).
  - Install AccessAgent on the remote server and ensure it is configured as a shared single session workstation. Set the server's AccessAgent policies.
  - Enable port redirection and mapping if using Radio-Frequency Identification (RFID).
  - Test out the configuration.
- Given access to a Citrix server and customer's requirement on Citrix, integrate AccessAgent with Citrix so that automation is enabled for published applications. The emphasis is on being able to perform the following tasks:
  - Analyze the user policy on the Citrix server.
  - Create Citrix machine policy template with the network provider policy set to enabled.
  - Assign the Citrix server to the Citrix machine policy template.
  - Install AccessAgent on Citrix server.
  - Verify that the AccessAgent icon is visible on the local machine system tray when user logs into Citrix published application.
  - Test the published application for Single Sign-on (or other automation) on Citrix.

- Given access to customer's audit requirement, configure and generate the audit logs so that the audit log report is created. The emphasis is on being able to perform the following steps:
  - Define custom audit logs to be generated by the agents, if necessary.
  - Configure the audit log events listed on the server interface.
  - Select the search criteria for audit logs.
  - Define the specific duration for which the audit logs are required and generate the report.
  - Use published log database schema to generate reports using an external reporting tool, if necessary.
  - Print the Audit log report.
- Given the customer's housekeeping requirements, configure the functionality on IBM Tivoli Access Manager for Enterprise Single Sign-On IMS so that the server installation is automatically maintained in a desired state in the future. The emphasis is on being able to perform the following tasks:
  - Determine frequency of housekeeping.
  - Determine the items to be included in housekeeping, including log pruning, database backup, and server configuration backup.
  - Use IMS configurator tool to set up housekeeping tasks in accordance with customer's requirements.
  - Alternatively use customer-defined housekeeping tasks.
- Given the customer's requirements, determine the process to customize IBM Tivoli Access Manager for Enterprise Single Sign-On so that the requirements are met and the system can be implemented successfully. The emphasis is on being able to perform the following tasks:
  - Configure the IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server:
    i. After installation, modify the IMS configuration settings to address requirements such as enterprise directories to be integrated, AccessAdmin user interface customizations, housekeeping, and so on.
    ii. Restart the service and run through the Setup Assistant on AccessAdmin to configure the default user policy template, machine policy templates and assignments, and system policies.
    iii. Review the system policies, machine policy templates (and assignments), and user policy templates (and assignments). Create new ones if necessary.
    iv. Review and create the required saved audit searches.

- Customize the IBM Tivoli Access Manager for Enterprise Single Sign-On AccessAgent package:
  i. Review and make changes to the package based on Graphical Identification and Authentication, Logon Banner, IMS Server fully qualified domain name (FQDN), and requirements in the `.ini` file.
  ii. Review and make changes to default registry settings in the deployment options registry file.
  iii. Add in any files or scripts to be distributed with the installer in the `config` folder.
  iv. Review and make changes to the MSI installer file based on software distribution mechanism.
  v. Install any third-party components required for second factor support prior to AccessAgent install.
- Customize the IBM Tivoli Access Manager for Enterprise Single Sign-On AccessProfiles. Review the application screens and Single Sign-On workflow requirements for each application and profile them accordingly.
- Test the customizations and obtain the customer's sign off.

- Given a running IMS Server, run the IMS configuration utility so that the IMS Server is configured. The emphasis is on being able to perform the following tasks:
  - Open IMS configuration utility.
  - Use the IMS configuration utility.
    i. Set up new enterprise directories.
    ii. Provide IMS administrator.
    iii. Set up housekeeping.
    iv. Set up advance settings, and so on.
  - Save changes and stop the IMS Server.
  - Restart the IMS Server.
- Given the requirements for an application's authentication to be augmented using IBM Tivoli Access Manager for Enterprise Single Sign-On OTP functionality, implement a solution so that the OTP authentication using third-party token requirements is addressed. The emphasis is on being able to perform the following tasks:
  - Configure the IMS Server to enable OTP (time-based or Open AuTHentication (OATH), or both) for the authentication service to be strengthened.
  - Install OTP token support on the IMS.

- Configure RADIUS authentication for the application (server) whose authentication service is to be strengthened.
- Enable users sign up (registration) through AccessAdmin.
- Set the ActiveCode enabled bindings for each token user.
- Set the requisite User and System policy settings.
- For OATH based OTP tokens, set the OATH look-ahead number and token reset window.
- Configure the bypass option for OTP authentication.
- Test the solution to ensure it to meets the customers requirements.

- Given the requirements for an application's authentication to be augmented using IBM Tivoli Access Manager for Enterprise Single Sign-On MAC functionality, implement a solution so that the MAC authentication requirements are addressed. The emphasis is on being able to perform the following tasks:
  - Configure MAC settings on the IMS Server.
  - Configure an existing message connector on the IMS Server for the selected MAC delivery channel. (Or develop a new message connector)
  - Configure the IMS Server's RADIUS authentication interface if the application supports RADIUS authentication:
    i. Configure the application's authentication server to perform RADIUS authentication with the IMS RADIUS server.
    ii. Configure the application's server to direct the client to display the MAC challenge screen on first authentication step success.
    iii. Customize the application's client user interface to show appropriate messaging on the MAC challenge screen.
  - For non-RADIUS authentication supporting applications do the following:
    i. Customize the application logon interface to include a request for MAC or provide a separate MAC request page.
    ii. Develop a SOAP client with the ability to make authentication calls and MAC request calls to the IMS.
  - Configure a bypass option for MAC authentication.
  - Test the solution to ensure it to meet the customer's requirements.
- Given user availability, functional AccessAgent, and IMS components, utilize AccessAgent or AccessAssistant sign-up functionality so that users are

successfully signed up with IBM Tivoli Access Manager for Enterprise Single Sign-On. The emphasis is on being able to perform the following tasks:

- Ensure user has second factor available if applicable (RFID badge and so on).
- Sign up using:
  - AccessAgent sign-up process
  - AccessAssistant
  - External provisioning system

- Given access to the solution document, customer's IBM Tivoli Access Manager for Enterprise Single Sign-On Environment, and system policies, define the self-service functionality so that the self-service functionality is available. The emphasis is on being able to perform the following tasks:
  - Define secret question list for end users to sign up during first time login based on customer's requirements.
  - Enable self-service functionality and set the corresponding policies required to authorize:
    i. Enable self-service password reset.
    ii. Enable self-service second factor registration.
    iii. Enable self-service for authorization code generation.
  - Test and deploy the self-service functionality.
  - Include the self-service definitions in the user policy templates.
- Given a functional IMS Server, configure user access to AccessAssistant so that AccessAssistant is working. The emphasis is on being able to perform the following tasks:
  - Set AccessAssistant-related system policies.
  - Configure AccessAssistant-related policies in user policy templates.
  - Configure AccessAssistant-related policies for specific users.
  - Test access for users.
- Given the organization security policy, configure the IMS system policy so that IMS system policy is configured successfully. The emphasis is on being able to perform the following tasks:
  - Review the default system policy settings.
  - Modify the default system policy settings according to the customer's requirements through AccessAdmin.
  - Wait for the sync period for the application of this system polices.
  - Verify that the IMS Server policy is configured successfully.

- Given access to the customer's environment and business requirements, set policy priorities so that the policy priority is implemented. The emphasis is on being able to perform the following tasks:
  - Analyze customer's policy requirements.
  - Determine the scope of the policy (such as machine, user, system policy).
  - Modify the policy priorities and execute the command-line tool.
- Given the customer's requirements regarding application screens and workflows (application design document), modify an existing profile so that each application can be profiled successfully to meet the requirements. The emphasis is on being able to perform the following tasks:
  - Determine the modifications required in order to make the existing profile work accordingly.
  - Determine details like account data template, authentication service (and groups), to be used in the profile.
  - Complete the application design template based on the options determined.
  - Test out the profile.
- Given an IMS Server installation, define the IMS Server administrator and set up the roles for administrators, help desk, and user so that the users have been assigned to roles. The emphasis is on being able to perform the following tasks:
  - Provision the IMS Server administrator user.
  - Log on to the AccessAdmin as the Administrator.
  - Search for users.
  - Choose a user to change his role.
  - Open administrative policies.
  - Change the role user and updated.
  - Enable the automatic role assignment for large deployments if necessary:
    i. Run the IMS configuration utility.
    ii. Specify the AD attribute for automatic role assignment.
    iii. Restart the IMS Server.
  - Assign help desk through user policy templates.
- Given multiple configured databases and an installed IMS Server solution, configure an additional data source so that an additional data source is available in the IMS Server. The emphasis is on being able to perform the following tasks:
  - Map the input of data source with appropriate databases information (IMS, Log or external).
  - Configure the external attributes in the data source.

- Update the configuration and restart the IMS Service.
- Verify that the configuration of the data source is complete.

Section 5: Administration

The section provides more information about the administration area of the test:

- Given AccessStudio, administrative privileges on the IMS Server, access to applications and notification when applications are modified, the AccessProfiles should be reviewed and updated so that they are always up to date and working correctly. The emphasis is on being able to perform the following tasks:
  - Evaluate applications which are to be updated or changed to validate if the AccessProfile remains functional.
  - Modify AccessProfile so that it is able to work with old version as well as the new version.
  - Test in a staging environment.
  - Deploy to production IMS Server when new profile is working correctly.
- Given access to the Solution Document, the customer's IBM Tivoli Access Manager for Enterprise Single Sign-On environment, and Disaster Recovery (DR) site, determine and establish a DR regime so that an effective failover to DR environment is achieved in the event of a failure in the production environment. The emphasis is on being able to perform the following tasks:
  - Determine failover and recovery criteria for IBM Tivoli Access Manager for Enterprise Single Sign-On components.
  - Determine backup and restore strategy for IMS database.
  - Set up DR environment in a separate site or location.
  - Test DR environment for failover situations.
- Given the IMS Server, manage audit logs and reports through the IMS Server so that audit logs and reports can be viewed by the Administrator. The emphasis is on being able to perform the following tasks:
  - Search the audit logs based on the query.
  - Save the query for the audit Logs.
  - Search the reports on the IMS Server based on user information, token, user information, and help desk activity.
  - Manage the reports based on the page size.
- Given that a new server host is prepared, the IMS database is on a separate host and the DNS and load balancer configuration is changed to accommodate new DNS name, move the IMS to another server host machine

so that IMS is successfully migrated to a different server machine. The emphasis is on being able to perform the following tasks:

- Back up the entire IMS folder from the original server and copy to new server.
- If the DNS name is changed, re-generate IMS SSL certificate using the new DNS name, and import to the IMS keystore on new server.
- Set up IMS to run as a Windows service on the new server.
- Start up IMS (within the IMS cluster environment, if applicable) and test.
- If there are multiple IMS Servers, repeat above steps.

- Given database access, migrate the IMS database to a different database server so that the IMS is operational with a new database server. The emphasis is on being able to perform the following tasks:
  - Stop all IMS Servers.
  - Move IMS database from one database instance/server to another.
  - Create database account (with required privileges) for IMS to use and test access to the database using this account.
  - Reconfigure IMS configuration file on IMS to point to the new database server and to use the new DB account credentials.
  - Restart IMS and test.
  - If there are multiple IMS Servers, repeat the configuration change on each server (or copy over `ims.xml` file), and restart.

Section 6: Performance tuning and problem determination

The section provides more information about the performance tuning and problem determination area of the test:

- Given an existing IBM Tivoli Access Manager for Enterprise Single Sign-On installation, identify and implement measures for improving performance so that the server and client components perform at optimal levels. The emphasis is on being able to perform the following tasks:
  - Identify and address opportunities for Improving Server performance, for example, configure Java memory parameters on the IMS Web server or configure the LDAP lookup timeout on a directory connector.
  - Identify and address opportunities for Improving AccessAgent performance, for example, performance can be tuned by removing unnecessary ApplicationProflies, lowering the log level, and excluding AccessAgent installation folder from certain runtime scans, adjust the synchronization interval between client and server, adjust communication timeouts, and so on.

  - Identify and address opportunities for improving database performance, for example, log pruning, changing memory allocated to database, and create indexes.

- Given an issue with the IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server functionality, troubleshoot the server utilizing tools provided so that the issue can be identified. The emphasis is on being able to perform the following tasks:
  - Identify that the problem at hand is an IMS Server issue, and obtain the result-code provided in the IMS error logs (or on the Status page in AccessAdmin).
  - Identify the cause of the specific error code in the diagnostics pages.
  - If the result-code is related to integrate with the enterprise directory, utilize the enterprise directory troubleshooting capability provided by the diagnostics pages.
  - Identify the issue.
- Given an IBM Tivoli Access Manager for Enterprise Single Sign-On installation with lost connectivity to the IMS Server, troubleshoot IMS connectivity issues so that the connectivity problem can be identified. The emphasis is on being able to perform the following tasks:
  - Determine if the client machine is in the network.
  - Determine if certificates between the IMS and the Agent are set up correctly.
  - Determine if an intervening firewall between the client machine and IMS Server causes this issue.
  - Determine if any network configuration issues, such as DNS problems, exist.
  - Determine if an intervening application protector between the client machine and IMS Server causes this issue.
  - Determine if some personal firewall or anti-spyware is blocking traffic from winlogon.exe.
  - Determine if the registry settings are corrupted or configured incorrectly, if AccessAgent is pointing to the wrong IMS Server.
  - Check to see if the IMS Server is up and running (ping test, visual inspection, and so on).
  - Check to ensure that the IMS Service is running (`services.msc`).
  - Try to *Set IMS Server Location* from a client workstation.
  - Identify the connectivity issue.

- Given IBM Tivoli Access Manager for Enterprise Single Sign-On operation issues with users, computers or servers, recover from common user or computer situations so that the issue is resolved. The emphasis is on being able to perform the following tasks:
  - Understand common issues affecting:
    - Users: For example, user forgets password, user forgets key
    - Computers: For example, the user tries to log on to AccessAgent and unlock the computer but it is unsuccessful
    - Servers: For example, IMS Server database has failed
  - Start the appropriate recovery workflow.
  - Resolve the issue.

1.3 Recommended educational resources

Courses and publications are offered to help you prepare for certification tests. Although the courses and publications are recommended before taking a certification test, they are not required.

1.3.1 Courses

This section provides information about the currently available or planned Tivoli Access Manager for Enterprise Single Sign-On courses. Refer to the Tivoli software education Web site to find the appropriate courses and education delivery vendor for each geography:

`http://www.ibm.com/software/tivoli/education`

If you want to purchase Web-based training courses or are unable to locate a Web-based course or classroom course at the time and location you desire, contact one of our delivery management teams:

- Americas:

  `mailto:tivamedu@us.ibm.com`

- EMEA:

  `mailto:tived@uk.ibm.com`

- Asia Pacific:

  `mailto:tivtrainingap@au1.ibm.com`

Note: Course offerings are continuously being added and updated. If you do not see courses listed in your geographical location, contact the delivery management team.

General training information is available at the following Web site:

http://ibm.com/training

You may also refer to the existing Test Preparation Roadmap for Tivoli Access Manager for Enterprise Single Sign-On at the following Web site:

http://www.ibm.com/certify/tests/map020.shtml

IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0 Deployment and Administration course

The IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment and Administration course is for administrators and implementers who are responsible for administering and implementing a desktop single sign-on solution. Topics include an overview of the product, installation and configuration of the components, creating single sign-on profiles, and basic integration with IBM Tivoli Identity Manager. The course consists of lecture and hands-on lab exercises.

Course duration

This is a four-day, classroom course.

Objectives

After completing this course, you should be able to:

- Describe the components of IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0.
- Install and configure the IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0 server.
- Configure machine profiles for groups of personal or shared workstations.
- Deploy the access agent component for desktop single sign-on.
- Use Access Studio to create template-based single sign-on profiles.
- Use Access Studio to create advanced single sign-on profiles.
- View reports and audit information.
- Perform a simple integration with IBM Tivoli Identity Manager 5.0.

Outline of course topics

The course contains the following topics:

1. Overview
2. Server
3. Policies
4. Agent
5. Roles
6. Shared Workstations
7. Basic Access Studio
8. Advanced Access Studio
9. Reporting
10. Deployment Scenarios
11. Integration

Required skills

Before taking this course, you should possess knowledge and skills in:

- Microsoft Windows 2003 Server with Active Directory (basic operating-system administration skills)
- Microsoft SQL Server® Express
- IBM Tivoli Directory Server

1.3.2 Publications

IBM Tivoli Access Manager for Enterprise Single Sign-On guides and Redbooks publications are useful tools for preparing to take Test 000-020.

Product documentation

Refer to the following guides as a source of information:

- *IBM Tivoli Access Manager for Enterprise Single Sign-On* online help and information center, (only available online as HTML version, either on the Tivoli publications Web site or through your local installation)

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/welcome.htm

- *IBM Tivoli Access Manager for Enterprise Single Sign-On User Guide Version 8.0.1*, SC23-9950
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Administrator Guide Version 8.0.1*, SC23-9951

- *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Help Desk Guide Version 8.0.1*, SC23-9953

IBM Redbooks publication

Refer to *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350, which states:

> Everyone feels the pain of too many passwords to remember, and everyone can relate to the security exposure of weak passwords, chosen for convenience or passwords placed in proximity to the workstation for a quick reminder that, unfortunately, can allow more than the intended user into the system and network. The average user today has about four passwords or more and security policies that focus on password complexity and password change frequency make it even harder.
>
> This book introduces IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0, which provides single sign-on to many applications without a lengthy and complex implementation effort. Whether you are deploying strong authentication, implementing an enterprise-wide identity management initiative, or simply focusing on the sign-on challenges of a specific group of users, this solution can deliver the efficiencies and security that come with a well-crafted and comprehensive single sign-on solution.
>
> This book is a valuable resource for security officers, administrators, and architects who want to understand and implement an identity management solution in a medium scale environment.

2

Planning

Thorough planning is one important part of the Tivoli Access Manager for Enterprise Single Sign-On deployment exercise. In this chapter, we discuss the aspects of planning an IBM Tivoli Access Manager for Enterprise Single Sign-On solution. The following high-level steps are required:

- Understand the customer security infrastructure and single sign-on requirements.
- Gather the requirements for the enterprise single sign-on solution.
- Design and implementing the enterprise single sign-on solution.
- Document the solution.

As part of the Tivoli Access Manager for Enterprise Single Sign-On deployment, the topics addressed in this chapter should be part of the first stage of planning.

An important note is that multiple phases might occur because of organization, infrastructure, or business demands. Therefore, revisiting these guidelines several times throughout the deployment might be helpful.

Supplemental information is available at the IBM Tivoli Access Manager for Enterprise Single Sign-On Wiki:

http://www.ibm.com/developerworks/wikis/display/tivoliaccessmanagerfortesso/Home

2.1 Considerations for deployment

Although Tivoli Access Manager for Enterprise Single Sign-On provides user-friendly tools for deploying and managing the product, a number of factors must be considered before embarking on the deployment.

Planning document

As with any deployment, a planning document should be written that outlines the scope, the phases, and the time-line of the deployment. At a minimum, the planning document should include the following details:

- Deployment approach

  Because Tivoli Access Manager for Enterprise Single Sign-On involves deploying software to user workstations, the deployment should be carefully planned to avoid adversely impacting users. Rollout to the enterprise should be approached in phases, starting by using Tivoli Access Manager for Enterprise Single Sign-On to secure the common desktop applications and then gradually adding new capabilities, such as other custom applications.

- Distribution of the software to the desktops

  The Tivoli Access Manager for Enterprise Single Sign-On component for the desktop is a Windows-based application referred to as the *AccessAgent*. The AccessAgent communicates with the IMS Server[1] to synchronize data changes with the server. However, the AccessAgent can cache data locally (on disk) based on policy. As such, it is able to perform most of its functions even if it is not connected to the IMS at any point in time.

  Another aspect to consider is *user education*. After the AccessAgent has been distributed to the desktop the user is initially prompted to *sign up* for use of Tivoli Access Manager for Enterprise Single Sign-On. This can be a forced action, but it can be configured so the user has the choice to sign up now or at a later time. The uninformed user might be confused about how to make the decision. Sometimes, users also have to interact with the client software if they want Tivoli Access Manager for Enterprise Single Sign-On to manage their password for a new application. A good practice is to announce upcoming deployments well in advance and to offer a simplified step-by-step help guide to support users through the sign-up process.

[1] The Tivoli Access Manager for Enterprise Single Sign-On Integrated Management System (IMS) is one of the central components of the overall solution. More information can be found in 2.3, “System architecture” on page 38.

- Corporate security policies

  Certain configuration parameters in Tivoli Access Manager for Enterprise Single Sign-On are likely to be governed by corporate security policies. The administrative configuration console (*AccessAdmin*) provides flexible configuration of security policies for users, machines, application, and authentication mechanisms. You should work closely with security officers to ensure the policy is correctly represented in the solution.

- Password reset strategy

  The ability for users to reset their own password on their own desktop machine is a powerful tool for the enterprise. However, be careful when formulating the series of questions users must answer in order to reset their passwords. Issues of privacy and cultural sensitivity should be taken into account. You should review your security questions with your legal department before going forward with your deployment to ensure the questions are in compliance with local privacy laws.

Other documents

The initial project definition is usually based on the business and functional requirements that triggered this project along with documentation, such as the IT architecture, security architecture, or equivalent. These documents identify the business context, the factors that influenced the solution, and, typically, the business and technical requirements for the solution.

2.2 Solution design

One of the first important steps of a Tivoli Access Manager for Enterprise Single Sign-On deployment is to define the project's scope, which involves collecting details about the current environment, gathering the requirements, and finally creating the solution document.

In this section, we describe processes required for designing an enterprise single sign-on foundation based on Tivoli Access Manager for Enterprise Single Sign-On. We discuss an organization’s overall structure, the business objectives, the business requirements, and functional requirements.

2.2.1 Basic solution definition

The solution enables an enterprise to extend capability to allow employees to use single sign-on from private, shared, and roaming desktops as well as personal desktops for applications using the basic profiling wizard. It also includes basic password reset and self-service functionality.

Several variations of the solution exist, as follows:

- Basic single sign-on solution

  The basic solution includes an *AccessAgent* that is deployed to each user workstation and a single *IMS Server* to centrally manage users, policies, and configuration parameters through *AccessAdmin*, the administrative interface. In this solution, the user is able to rely on Tivoli Access Manager for Enterprise Single Sign-On to log them into Windows applications, Web applications, and other applications configured into Tivoli Access Manager for Enterprise Single Sign-On. You should also expect to configure *user*, *machine*, and *authentication policies*.

- Basic single sign-on solution with session management

  Mobile employees can enjoy the benefits of single sign-on by accessing their applications from Windows Terminal Services clients or Citrix MetaFrame clients. You should expect to configure Terminal Services or Citrix MetaFrame prior to deploying the AccessAgent, as well as configure the Terminal Services or Citrix MetaFrame policy settings in AccessAdmin.

- Single sign-on solution with user life cycle management

  Tivoli Access Manager for Enterprise Single Sign-On user credentials can be provisioned and de-provisioned automatically when, for example, a new user's Active Directory ID has to be created or deleted when they leave the company. This approach requires configuration of a Provisioning Bridge and de-provisioning parameters in combination with an identity management solution such as IBM Tivoli Identity Manager.

- Single sign-on with two-actor authentication

  Configure a strong second authentication factor for one or more users and machines.

These variations of the solution can be intermixed throughout an enterprise to match the requirements of various corporate entities.

2.2.2 Design approach

In this section, we consider how the security design objectives can be realized using Tivoli Access Manager for Enterprise Single Sign-On. Our goal is to produce a plan that includes a set of smaller implementation steps where the end-result satisfies the functional requirements and, therefore, also satisfies the original business requirements.

Although business and functional requirements are the main parts of the security design objectives, we also have to consider other non-functional requirements and constraints. These can include objectives that are necessary to meet

general business requirements, or practical constraints on constructing security sub-systems. Tivoli Access Manager for Enterprise Single Sign-On implementations often involve non-functional requirements relating to:

- Backup and recovery
- Performance and capacity
- Change management

The steps involved in producing an implementation plan are:

1. Prioritize the requirements.
2. Map the requirements to Tivoli Access Manager for Enterprise Single Sign-On features.
3. Define the tasks that are involved in using those features to satisfy the requirements, and estimate the effort that is required for each task.

After mapping the requirements to Tivoli Access Manager for Enterprise Single Sign-On features and creating a list of implementation tasks, certain tasks might require a longer implementation time.

2.2.3 Project phases and deployment stages

Based on the priorities of the customer's business requirements and the levels of effort of the different implementation tasks, split the project into appropriate logical phases to be executed sequentially. Each phase should be deployed in stages.

Most companies use a staged approach to deploying new solutions into their IT infrastructure. We describe four stages here, although some companies might have more and might use different terminology for the stage names. The deployment stages are:

1. Development

   During development, the deployment procedures for the current stage are created. This stage involves installing and configuring the product based on the goals of the phase.

2. Test

   During the test stage, the test group receives the software and procedures from the development group and executes the documented deployment procedures. The test group reports any issues that it encounters to the development group, who updates the procedures. This cycle continues until the test team is satisfied with the reliability of the deployment procedures.

3. Pilot

   The pilot stage involves deploying the solution to a relatively small number of users to address any issues in the configuration and deployment procedures. The software is deployed into a production environment and, thus, is typically performed by a group other than the test group. Solutions involving software distribution to clients can be particularly costly to redeploy to a large number of seats. The pilot stage is important in those types of solutions. This stage can discover issues that are not discovered during the test stage.

4. Production

   Production deployment takes place when the pilot phase has proven the viability of the solution. The same procedures used in the pilot phase are used in the production deployment. However, production deployment includes the entire scope of users of the solution.

2.3 System architecture

In this section, we discuss the logical and physical architecture of Tivoli Access Manager for Enterprise Single Sign-On and its most fundamental components.

Tivoli Access Manager for Enterprise Single Sign-On provides its single sign-on functionality by introducing a layer that authenticates a user once and then automatically detects and handles subsequent requests for user credentials. Figure 2-1 on page 39 depicts an overview of the solution.

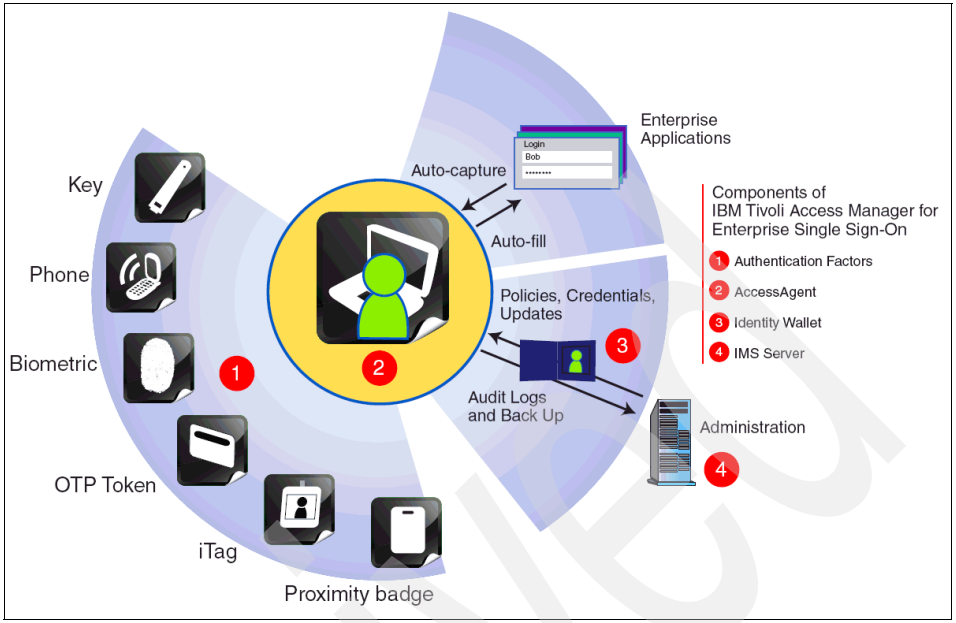

Figure 2-1 Product overview

Tivoli Access Manager for Single Sign-On can be divided into the following four functions:

- Authentication factors

  Tivoli Access Manager for Enterprise Single Sign-On supports different *authentication factors* to authenticate the user. Besides the standard user name/password authentication, the user can be authenticated by means of a proximity or building badge such as active or passive RFID, a fingerprint, a one-time password provided by SMS or OTP[2] token, or a USB token.

- AccessAgent

  The *AccessAgent* runs on every Windows desktop endpoint, Microsoft Windows Server® Terminal Services session, and Citrix MetaFrame Presentation Server session. The AccessAgent is responsible for authenticating the user. It can automate single sign-on into Windows and to the set of applications that are defined in *AccessProfiles*. The AccessAgent can extend the Windows Graphical Identification and Authentication (GINA) DLL chain to provide additional functions for self-service or strong authentication.

[2] Short Message Service (SMS), one-time password (OTP)

- Identity wallet

  The *identity wallet* (or *Wallet*) holds the user credentials that are required for single sign-on. It is loaded from the IMS Server into the 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 *Integrated Management System Server* (IMS Server) is the central repository for user data, AccessProfiles, identity wallets, and machine profiles. The IMS Server provides a Web-based interface to administrate users and policies.

2.3.1 Logical component architecture

The logical component model illustrates the software components that are being used to build a system. Tivoli Access Manager for Enterprise Single Sign-On consists of the following components:

- AccessAgent

  The client component is installed on all systems that require single sign-on (SSO) functionality. This client can be installed on Windows clients, as well as Microsoft Terminal Services and Citrix MetaFrame/Xen systems.

- Terminal Server or Citrix MetaFrame AccessAgent

  The AccessAgent includes a server mode that is automatically enabled when deployed on a Microsoft Windows Terminal Server or a Citrix Presentation Server.

- IMS Server

  The IMS Server provides the administrative, reporting, help desk and password reset functionality. AccessAdmin and AccessAssistant are the tools used to provide this management and reporting capability. Also, the infrastructure to communicate with and manage the AccessAgents (clients) is managed through the IMS Server.

- IMS Database

  The IMS Server uses a database to store configuration, policy, application profiles, and log and audit data. The IMS database can be implemented using either Oracle, Microsoft SQL Server, or IBM DB2.

- AccessAdmin

  The AccessAdmin is the Web-based management console used by administrators and help desk employees to manage users and policies on an IMS Server.

- AccessStudio

  The AccessStudio application is used by administrators to create AccessProfiles (Windows only).

- Provisioning Bridge

  The Provisioning Bridge helps automate the user credential distribution process so that identity management solutions such as Tivoli Identity Manager can provision and remove user involvement in the credential provisioning and management process.

Figure 2-2 depicts the overall logical component architecture.

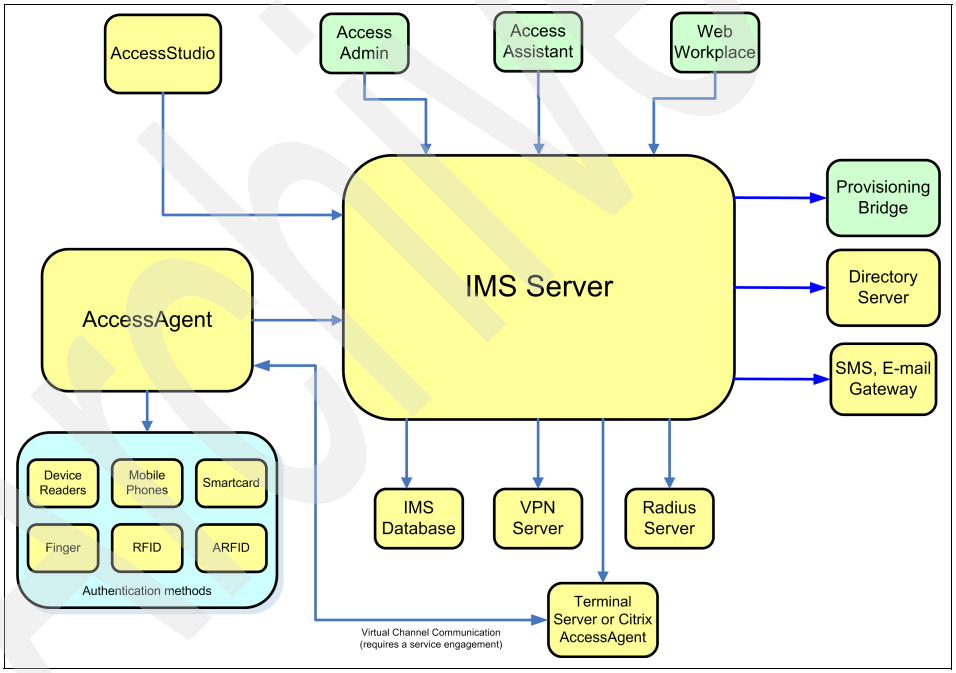

Figure 2-2 Logical component architecture

AccessAgent

The AccessAgent is the client software that is installed onto all Windows workstations and Terminal Servers or Citrix MetaFrame and configured to connect to the designated IMS Server. Figure 2-3 depicts the architecture of the AccessAgent.

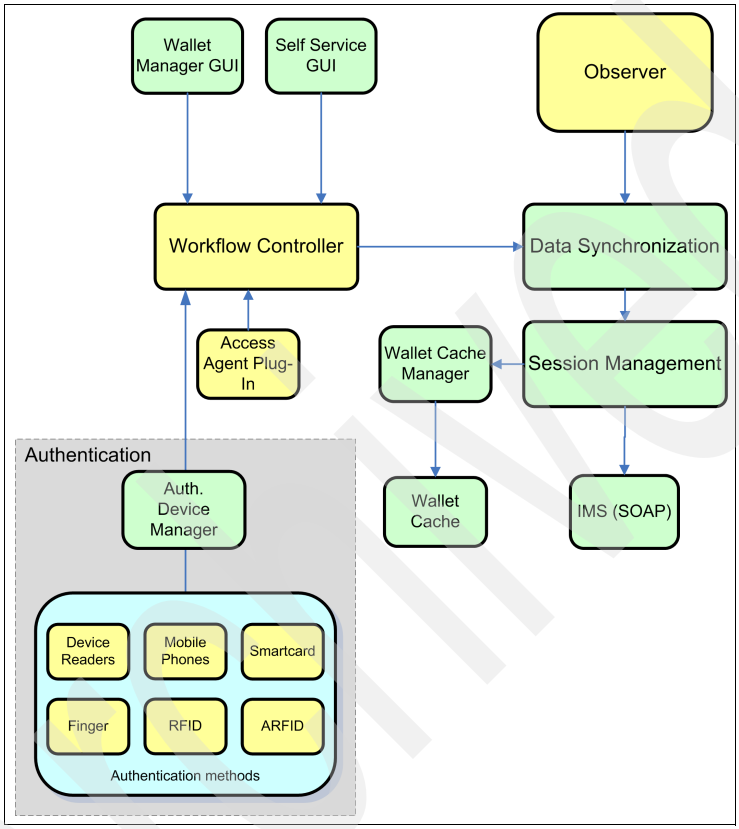

Figure 2-3 AccessAgent architecture

Let us take a closer look at the following AccessAgent's function blocks:

- Authentication
- Data synchronization
- Wallet manager GUI
- Self-service GUI
- AccessAgent Observer module
- AccessAgent Plug-in
- Session management

Authentication

Authentication defines how the system validates users so they gain access to Tivoli Access Manager for Enterprise Single Sign-On, for example, using a password, biometrics, token, and so on.

Tivoli Access Manager for Enterprise Single-Sign-On supports the concept of a separation of the authentication of the user itself and the authentication against the Windows desktop.

For more information about authentication refer to 2.4.5, “Authentication strategy” on page 63.

Authentication Device Manager

The *Authentication Device Manager* integrates the authentication user interface with the main Tivoli Access Manager for Enterprise Single Sign-On AccessAgent. The Authentication Device Manager validates the credentials provided by the authenticator against a system authentication service, such as a Windows domain, Radius Server, LDAP repository, and so on. The Authentication Device Manager serves as a conduit between the authentication factors and the AccessAgent.

Data synchronization

The *data synchronization* component synchronizes AccessProfiles, a user's identity wallet and various policy settings with the IMS Server and submits user's application access audit events to the IMS Server. The AccessAgent contacts the IMS Server on start up, on each user login, and on periodic intervals to synchronize data changes with the server. However, the AccessAgent can cache data locally (on disk) that is based on a policy. As such, it is able to perform most of its functions even if it is disconnected from the IMS Server.

Wallet Manager GUI

The *Wallet Manager GUI* enables the user to manage the application credentials stored in the personal identity wallet.

Self-service GUI

A GINA extension is used to implement the *self-service user interface* for the user to manage the desktop password and authentication factors.

For more information about Password self-service, refer to 4.15, “Password self-service” on page 150.

AccessAgent Observer module

The *AccessAgent Observer module* is one of the core elements of Tivoli Access Manager for Enterprise Single Sign-On. The module is hooked into various

applications, and consults the appropriate AccessProfile (created using the AccessStudio application) to perform the necessary logon/logoff and automation actions. When an application presents a request for credentials, the Observer module is responsible for the appropriate action. The Observer module architecture is depicted in Figure 2-4.

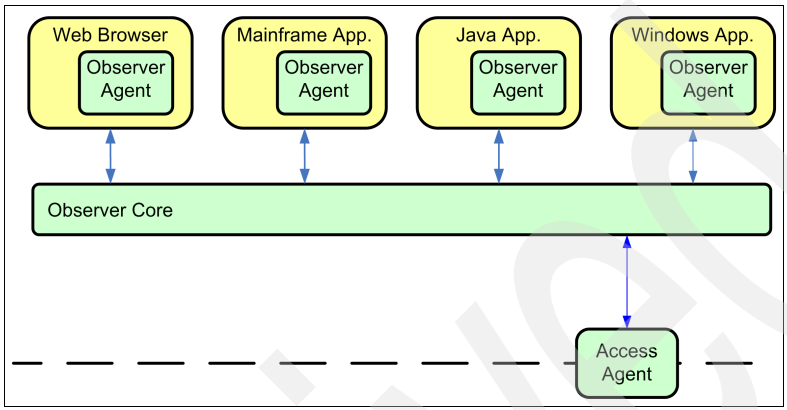

Figure 2-4 AccessAgent Observer module architecture

The AccessAgent Observer module is composed of a core module and a number of agent instances that are hooked (through Windows APIs) into every launched Windows application, for example, IBM Lotus® Notes® application, Microsoft Outlook®, Microsoft Internet Explorer®, and so on. The behavior of the *AccessAgent Observer agents* within each application is driven by a set of behavioral specifications called an *AccessProfile* (for details on AccessProfiles refer to 3.2, "AccessProfile configuration" on page 88).

Each *AccessProfile* entails a set of definitions for the AccessAgent Observer agent module to watch for and execute accordingly. The set includes:

- For Windows applications, the name of the executable
- A set of behavioral states, such as pre-logon or post-logon

  States represent specific situations where the state machine must look for certain triggers to occur (similar to a flowchart). A state can have multiple triggers. For example, in the `after_application_launched` state, you can look for the login window or a change-password window to appear. One trigger can have multiple actions. When a login window appears, you can inject user credentials and click **OK**.

  A profile writer can define as many states in a state machine as required.

- The state definitions, listed here with each state, are:
  - A set of workflow triggers: *when*
  - Signatures that belong to a specific trigger: *where*
  - A set of workflow actions: *what*

The agent retrieves the required AccessProfiles and user credentials from the AccessAgent Observer core module, which in turn communicates with the remainder of the AccessAgent for data synchronization and workflow session management services.

The Observer architecture consists of the following modules:

- Workflow trigger module

  The AccessAgent Observer agent module detects requests for credentials but not restricted to, in a variety of ways, depending on application type (Web, Windows, and Mainframe/Host). Triggers cause transitions between states in the state engine. At the end of the day a trigger defines *when* a condition is true.

- Workflow action module

  An action can be performed in response to a trigger. That is, a workflow action defines *what* has to be done if a trigger becomes true.

- Windows application observer agent

  Responds to requests for user credentials from Windows applications.

- Mainframe and host application observer agent

  Responds to requests for user credentials from mainframe and host applications.

- Web application observer agent

  Responds to requests for user credentials from Web applications.

- Java application observer agent

  Responds to login and password change requests for virtually all Java applications and applets built on the Sun™ Java™ Runtime Engine 1.4.1 or later.

AccessAgent Plug-In

The AccessAgent Plug-In is a block of VBScript or JavaScript code that performs some custom action required as part of a workflow trigger or workflow action inside an AccessProfile. This block of code can make calls into the Windows OS and into an AccessAgent Plug-In API by using the user's Windows and Tivoli Access Manager for Enterprise Single Sign-On privileges. Administrators

typically use this extension facility to implement customized authentication, access control, or workflow automation for a specific application.

Session management

Tivoli Access Manager for Enterprise Single Sign-On supports two main usage configurations: *personal workstations* and *shared workstations*. The personal workstation configuration is typically used in organizations where users are assigned their own workstations. The shared workstation configuration, for example, can be found in health care organizations where doctors and nurses share workstations that are deployed throughout the hospital. Tivoli Access Manager for Enterprise Single Sign-On supports *fast user switching* through any of the following desktop schemes:

- Shared desktop
- Private desktop
- Roaming desktop

Let us further discuss the supported schemes for shared workstations:

- Fast user switching through shared desktop

  Shared desktops allow multiple users to use one generic Windows desktop in a workstation. Because each user does not have to log on to Windows, the switching of users is quicker. However, after switching from user A to user B, the application contexts for user A will be lost. If user A returns later and switches the workstation back to user A's account, the user must re-launch the applications. For the scheme, AccessProfiles must be created to automatically log off enterprise applications when user switching occurs.

- Fast user switching through private desktop

  Private desktops allow multiple users to have their own Windows desktops in a workstation. The scheme uses the *local user session management* feature of the AccessAgent, which allows users to retain the existing user's desktop session during switching of users. When user A returns to the workstation to unlock it, AccessAgent switches to user A's earlier desktop session, allowing user A to resume the previously incomplete or interrupted work.

  However, an existing desktop can be logged off if the workstation runs out of resources (for example, memory) to accept a new user logon. If the user logs on at another workstation, the user still has to re-launch the applications. Because security is very important for the private desktop operation, refer to "How the private desktop feature ensures security" on page 55.

- Fast user switching through roaming desktop

  Roaming desktops provide users with Windows virtual desktops to *roam* to their points of access, from workstation to workstation. With roaming sessions, a user can disconnect from the current virtual desktop or

application session at a client, log on to another client, and continue the desktop or application session at a new client. The scheme requires the use of either a Microsoft Windows Server Terminal Services session or Citrix MetaFrame Presentation Server session.

If the AccessAgent is configured for shared workstation operation, the workflow session management module is responsible for the desktop switching between the different users.

The best desktop operation mode possible for a given deployment situation depends on several conditions, such as the amount of memory available at every desktop or whether the required applications support more than one instance.

Terminal Server or Citrix Presentation Server AccessAgent

The AccessAgent includes a *server mode* that is automatically enabled when deployed on a Microsoft Windows Terminal Server or a Citrix Presentation Server. A separate instance of the server-side AccessAgent is launched for each terminal session. When a new terminal session is started, the server-side AccessAgent looks for the client-side AccessAgent across a virtual channel established between the terminal server and its (RDP) client. Subsequently, Wallet changes and logon/logoff events from either side are communicated to each other over the virtual channel. For example, if the user captures a new application credential on the server session (and synchronizes it to the IMS), the server AccessAgent notifies the client side AccessAgent, which then separately performs a synchronization with the IMS to retrieve the new application credential. To enable the virtual channel communication feature, a service engagement is necessary to provide the applicable software.

IMS Server

The IMS Server provides a central point of administration and control. It enables centralized management of *user identities*, *AccessProfiles*, and *authentication policies*. It also provides *loss management* of authentication tokens, *certificate management*, and *audit management*. The IMS Server interfaces with other applications through *IMS Connectors* and *IMS Provisioning Bridges*. The IMS Server can be configured with *AccessAdmin*. Lower-level configuration settings for the IMS Server can be configured with the *IMS Configuration Utility*, which is accessible by administrators. IMS exposes an internal SOAP API that is used by AccessAdmin, AccessStudio, and AccessAgent.

Figure 2-5 shows the IMS Server architecture.

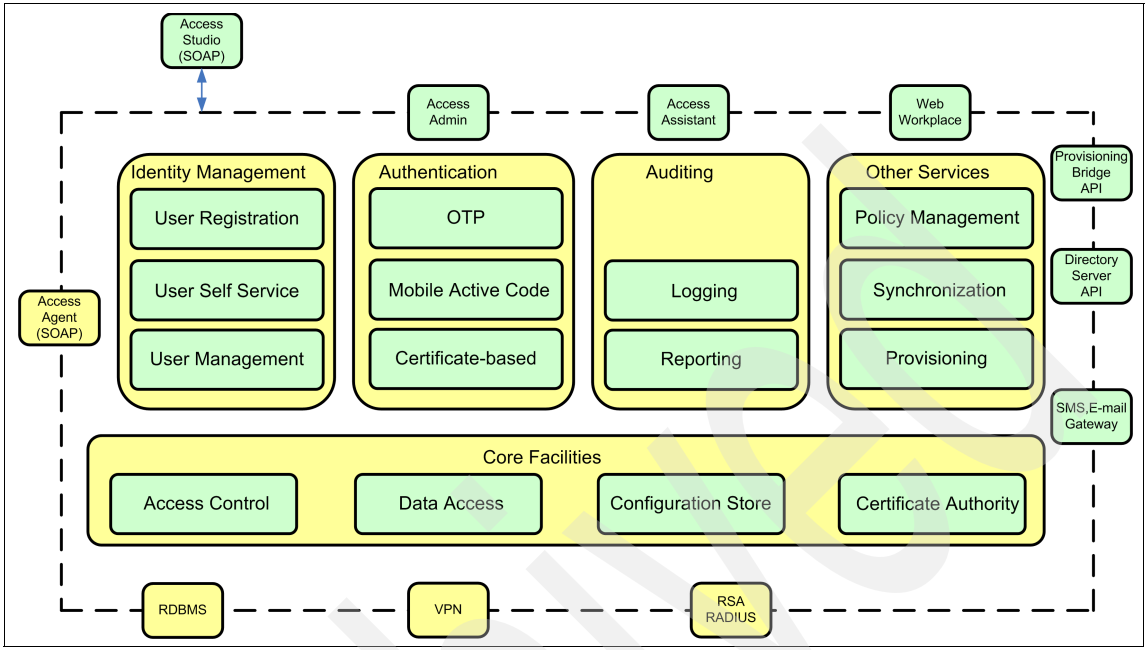

Figure 2-5 IMS Server architecture

The IMS Server is a Web-based application developed in Java and runs on top of an Apache Tomcat[3] application server. During installation of the IMS Server software, the applications server gets installed too.

In this section, the following IMS Server components are discussed:

- Identity management
- Authentication
- Auditing
- Other services

Identity management

The IMS Server provides basic *identity management* functions like such as enrollment and password management for users and administrators. Supported by a self-service module, users are able to manage their own credentials, for example, resetting their password.

[3] More information about the Apache Tomcat application server can be found at: http://tomcat.apache.org/

Authentication

The IMS Server provides a one time password mechanism called ActiveCode. This ActiveCode is a strong authentication mechanism to authenticate users online or when their desktop has no connection to the IMS Server. To allow VPN servers to authenticate with a one-time password, the IMS also provides a RADIUS interface.

Auditing

The auditing framework captures identity information and events in the database to allow administrators to generate reports for identity auditing, such as:

- List of application accounts for a user
- Policy changes performed on a user by an administrator or help desk
- Successful and failed application logons and logoffs
- Summary table of the number of times each user logs on to each application within a period of time

In addition to the standard events listed, users can create custom events to track application-specific events. For details, refer to 4.16, “Auditing and reporting” on page 151.

To analyze the audit log, administrators can generate identity auditing reports by using an SQL query tool (for example, Microsoft Excel®, Microsoft SQL Query Analyzer, Crystal Reports, and so on).

Other services

Tivoli Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its components. These policies are configurable through various means. Policies have different visibility and scope and can be applicable system-wide, or only to certain groups of users. The applicability of a policy is determined by its scope, which can be *system*, *user*, or *machine*.

The provisioning automates the user credential distribution process so that identity management solutions such as IBM Tivoli Identity Manager (ITIM) can provision and remove user involvement in the credential provisioning and management process. Refer to 2.4.6, “Integration strategy” on page 65 for details about the integration of Tivoli Access Manager for Enterprise Single Sign-On and Tivoli Identity Manager.

The provisioning bridge Java API can be installed on a third-party provisioning system to communicate with IMS to perform user provisioning operations. The third-party system communicates to the IMS by using JMX™.

IMS database

The IMS relies on an external relational database to store its system data and user data. It also stores all its audit logs into the same or a separate database instance. The IMS application communicates with the database using JDBC™.

AccessAdmin

The AccessAdmin component is the Web-based management console used by administrators and help desk employees to manage users and policies on an IMS Server. Different access rights are granted to the administrator and help desk roles. Certain configurations (for example, system policies) can only be viewed but not modified by the help desk staff.

AccessStudio

The AccessStudio application is used by administrators to create AccessProfiles required to support sign-on/sign-off and custom workflow automation. The AccessStudio application provides:

- A wizard mode is for administrators to easily generate AccessProfiles for most applications, by walking through the set of application windows and mapping selected fields and controls used for logon, logoff, and other application behaviors.
- An advanced mode is for administrators to create AccessProfiles for complex applications or where complex workflow automation is required.
- A test mode is for administrators to test a generated AccessProfile against the target application.
- An upload function to IMS Server is for finished AccessProfiles.

The AccessStudio must be installed on an existing AccessAgent installation. The user must have an administrator role and must have an active AccessAgent session before downloading from or uploading to the IMS Server is possible.

Provisioning bridge

The *provisioning bridge* automates the user credential distribution process so that identity management solutions such as Tivoli Identity Manager can provision and remove user involvement in the credential provisioning and management process. For more information refer to 4.3, “IMS Provisioning Bridge” on page 115.

2.3.2 Additional Components

Tivoli Access Manager for Enterprise Single Sign-On also includes the following additional modules:

- Provisioning Agent

  The Provisioning Agent is an application that monitors an Active Directory periodically for deletion of users to trigger a corresponding deletion or revocation of the user's account or Wallet on the IMS Server. This application is intended for deployments where a user provisioning system (like Tivoli Identity Manager) is not deployed, because it helps the administrator from having to separately revoke a user's Tivoli Access Manager for Enterprise Single Sign-On account when deleting the user from Active Directory.

- AccessAssistant

  The AccessAssistant is a Web-based interface that enables users to manage their identity wallet. They can reset their Tivoli Access Manager for Enterprise Single Sign-On password, change the reset questions/answers, and view, add, edit, or delete user names/passwords inside their wallet.

- Web Workplace

  The Web Workplace provides a Web-based interface that enables the user to log on to enterprise Web applications by simply clicking on links, without the need to remember the passwords for individual applications. Users can also access applications hosted on Citrix MetaFrame or Terminal Servers through the Web Workplace without further logins. To securely implement this functionality, use SSL VPN connections.

2.3.3 Security requirements

In order to better understand how Tivoli Access Manager for Enterprise Single Sign-On implements operational security we first need to identify which information assets and procedures have to be secured. Tivoli Access Manager for Enterprise Single Sign-On handles the following types of sensitive data:

- Application credentials

  These credentials are stored on behalf of a user to provide automated access to enterprise applications.

- Encryption keys

  These cryptographic keys are used to protect the user credentials.

- Authentication factors

  This secret data provided by a user is for proving one's identity to the system. This includes the user's Tivoli Access Manager for Enterprise Single Sign-On password, biometric data, onetime passwords, and so on.

- Audit logs

  Audit logs must be protected against tampering.

All the sensitive data items listed must be protected as they flow through the system. Thus, the security requirements for Tivoli Access Manager for Enterprise Single Sign-On can be specified as follows:

- Secure storage

  If sensitive data has to be stored, either on the server or the clients, it must be stored in an encrypted form.

- Secure processing

  Sensitive data must be in an unencrypted form while it is being used. The system should prevent other user programs from accessing the unencrypted data while it is held in memory.

- Secure communication

  Sensitive data must be protected from eavesdroppers as it travels between the components.

Securing Wallets

In this section, we discuss how Tivoli Access Manager for Enterprise Single Sign-On protects all sensitive data items in the different components.

Secure storage

When a user signs up with Tivoli Access Manager for Enterprise Single Sign-On, a random cryptographic key, called the common symmetric key (CSK), is generated. This CSK is unique to the user and is used for encrypting the user's credentials in the Wallet. The CSK, in turn, is encrypted using a key derived from either the user's Tivoli Access Manager for Enterprise Single Sign-On password or secret question-and-answer. The user's authentication factors, such as the password, are not stored anywhere in the system. The CSK can be obtained in unencrypted form only when users authenticate themselves by providing their correct Tivoli Access Manager for Enterprise Single Sign-On password. The CSK can then be used to decrypt the credentials and is discarded when the user logs off.

Secure storage can be on the server or on clients:

- Secure storage on the server

  The IMS Server stores only the encrypted forms of the user's credentials and CSK in its database, so even breaking into the database does not reveal the CSK nor the credentials. Moreover, the access controls on the database are configured in such a manner that only an IMS Server-specific database account and the database administrators are granted access to the data.

- Secure storage on the clients

  On client workstations the AccessAgent stores a copy of the encrypted credentials and CSK in a secure data file called *Cryptobox*. Data is stored in an encrypted format. The design of the Cryptobox makes it impossible to read or enumerate the stored data items without knowing their *access keys*. The access key for the credentials stored in a Cryptobox is derived both from the user's CSK and a secret known only to the AccessAgent. Therefore, the credentials can be extracted from the Cryptobox only after the AccessAgent has authenticated the user and has access to the user's CSK. The AccessAgent can be configured to delete Cryptoboxes if they have not been used for a specified number of days. This approach can minimize the risk of exposure to brute-force attacks on user credentials stored in Cryptoboxes.

Secure processing

The AccessAgent also protects sensitive data while the data resides in the computer's memory. A user's Tivoli Access Manager for Enterprise Single Sign-On password is held in the computer memory in a scrambled form. It is unscrambled only when it is used. This foils any attempt from other user programs to scan the password from the agent's memory. Similarly, memory locations that temporarily hold a user's credentials and the CSK are wiped clean after use to prevent object reuse attacks.

Secure communication

When a user logs on to Tivoli Access Manager for Enterprise Single Sign-On, the user's password is sent to the IMS Server. In addition, when the user captures new credentials or updates them, the credentials are synchronized between the IMS Server and the AccessAgent. The communication channel that carries this sensitive data is protected by using SSL. After the AccessAgent verifies the SSL certificate issued to the server, the communication is encrypted using temporary session keys. This approach prevents eavesdroppers from extracting the sensitive data from network packets.

Secure audit logs

The audit log records stored in the database can optionally be made tamper-evident through the use of hash chains and signatures. A log verification utility script can be run on demand or on schedule to verify the hash chains and signatures.

Recovering Wallets

As mentioned in the previous sections, a user's Wallet is protected by the CSK, which in turn is protected by the Tivoli Access Manager for Enterprise Single Sign-On password. If the user forgets the password, the credentials stored in the Wallet will not be available, preventing the user from accessing enterprise applications. Tivoli Access Manager for Enterprise Single Sign-On provides the user with a means to recover the Wallet, even if the password is forgotten. During registration, a user is allowed to register one or more personal secrets. These secrets are responses to questions only the user is likely to know. The system also stores the user's CSK in an encrypted form with the personal secrets. If the user forgets the password, the user must provide a specified number of correct personal secrets in order to reset the password and recover the Wallet. In this process, Tivoli Access Manager for Enterprise Single Sign-On re-encrypts the user's CSK with the new password provided by the user.

Strengthening the protection of Wallets

As Tivoli Access Manager for Enterprise Single Sign-On provides the user with the ability to log on to multiple enterprise applications, the authentication to Tivoli Access Manager for Enterprise Single Sign-On should be strengthened. Tivoli Access Manager for Enterprise Single Sign-On provides several ways to strengthen the authentication, which are discussed in this section.

Use of password policies

An enterprise can ensure users use *strong passwords* by enforcing Tivoli Access Manager for Enterprise Single Sign-On password policies. These policies include password aging, password complexity, and lockout policies that can be centrally configured on the IMS Server.

Use of authentication factors

Access to the Wallet can also be strengthened by enforcing the use of additional authentication factors such as RFID badges, biometrics, and USB smart card tokens. The use of such authentication factors increases security, as an attacker now needs to obtain both a physical token and the Tivoli Access Manager for Enterprise Single Sign-On password of a user to gain access to a Wallet. Tivoli Access Manager for Enterprise Single Sign-On can use RFID-enabled facility access badges as authentication factors. Users must present their RFID access badge and password to log on to their systems. To log on using a USB smart

card token, the users supply the smart card PIN, which is verified by the smart card itself. The private data on the smart card is protected by the PIN, which is locked out after a pre-configured number of successive failed attempts. Users with USB smart card tokens can have their credentials stored securely on the smart card instead of on a computer's hard disk. Tivoli Access Manager for Enterprise Single Sign-On uses Public Key Cryptography to authenticate the USB tokens to the IMS Server using 2048-bit RSA keypairs stored on the smart cards.

How the private desktop feature ensures security

The private desktop feature is provided by the AccessAgent. It uses the Windows operating system support to create multiple Windows desktops for different user accounts, using the user's own Windows privileges, and facilitates the switching between these desktops. This way, the private desktop is only visible to the individual user, no other user (including the administrator) can access it.

When a new user logs on from the AccessAgent GINA, the private desktop first verifies that the user is a valid user, and then creates a Windows desktop for that user. It then loads the user's Windows profile, and creates the user's shell (starting Windows Explorer, and so on) for the user to interact with the desktop. The private desktop also provides Group Policy Object (GPO) support by invoking the client side extensions to apply the group policies applicable to the user. Next, the user shell in the user's security context is created and therefore, all applications run from the desktop are executed in the user's own security context.

With the private desktop session, each desktop runs with the rights of the user's Active Directory account; therefore, access to each user's desktop or resources remains protected by Windows access control. This means that while each user account does not have administrative rights on the machine, a user cannot possibly access another user's data.

When users log off from their desktop, the private desktop gracefully logs off the users' applications by sending *end session* messages to each open window on the users' desktops. As with a normal Windows logoff, when an application is not ready to end, the private desktop displays a notification to the user and lets the user terminate the logoff processes. In the event of a system restart or shutdown, all private desktops are logged off gracefully before the system restarts or shuts down.

The private desktop is designed to prevent malicious software or some other desktop management software from switching between a current desktop to another user's desktop. If a third-party software tries to perform desktop switching, AccessAgent immediately locks the workstation. If the component of

AccessAgent that implements this security measure is somehow terminated by the administrator, the computer is restarted automatically.

This functionality also prevents the clipboard content on one desktop being accessed from another desktop session. Anything copied onto the clipboard from one desktop is prevented from being pasted into another desktop.

Windows 2000 does not support Fast User Switching (FUS), and Windows XP support for FUS is limited to non-domain logons. With the Tivoli Access Manager for Enterprise Single Sign-On private desktop, Active Directory users can use FUS with domain level security across Windows 2000 and Windows XP.

2.3.4 Physical architecture

In this section, we describe the physical components that are assembled for Tivoli Access Manager for Enterprise Single Sign-On. See Figure 2-6.

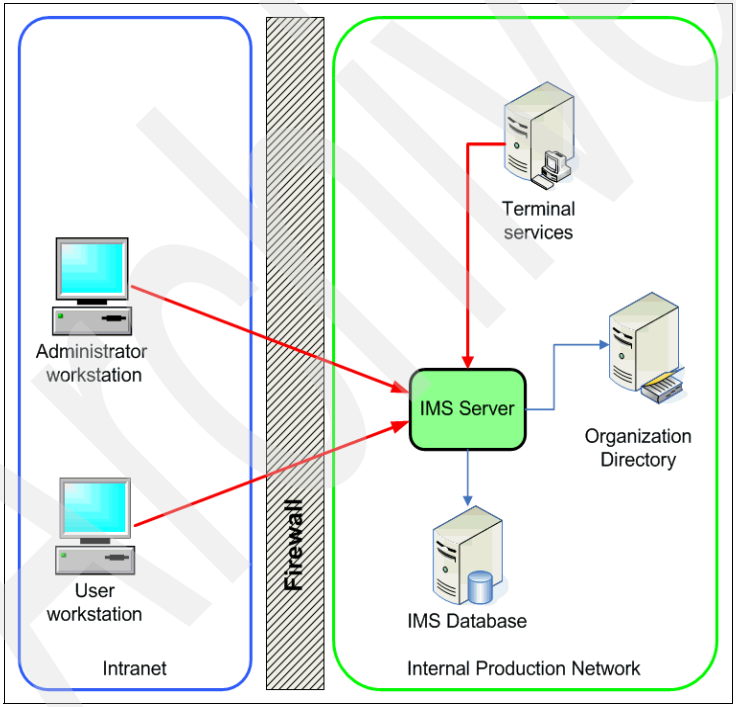

Figure 2-6 Physical base deployment architecture

AccessAgent

The AccessAgent gets deployed on user and administrator workstations either manually or by using software distribution mechanisms. Because the AccessAgent features can be configured afterward, specifying any options during the AccessAgent software installation is not necessary. Although several configuration parameters, like the IMS Server URL or whether the GINA extension should be installed, can be predefined.

AccessAgent and GINA chaining

For AccessAgents installed with the GINA option enabled, a user logs on to the AccessAgent GINA first, with the required authentication factors, whereupon the AccessAgent automatically logs on the user to Windows with the user's Windows account. The Windows GINA is not replaced and is always available as needed.

For AccessAgents installed without the GINA option enabled, the user usually logs on to Windows manually first, and then logs on separately to AccessAgent with the required authentication factors. But, this approach is not always the process, for example, for password-sync single-factor deployments, we can use the EnNetworkProvider to avoid the second login.

Availability constraints

If the AccessAgent has network connection to the IMS Server, it authenticates a user against the IMS Server by passing along the authentication credentials over HTTPS to IMS. However, if the AccessAgent is offline to the IMS, it then authenticates the user's presented credentials against cached authentication data stored on the disk. The data volume for each class of data cached at the clients is estimated at the following values:

- System data up to 300 - 400 KB
- User data 50 - 100 KB per user

Support for terminal services

The AccessAgent has a *server mode* for Microsoft Windows Terminal Server and Citrix Presentation Server. To use the single sign-on features on one of these systems, the AccessAgent simply has to be deployed on the server.

Hardware and software requirements

The AccessAgent requires a computer with a Windows operating system installed. For detailed hardware requirements, refer to the product documentation.

IMS Server

As the central repository and management point for all system and user data consumed by the AccessAgents, the Integrated Management System (IMS) performs the following functions:

- Serves as a central repository and distribution point for AccessProfiles and other system data.
- Serves as a central repository for all user data, including the credential Wallet and various authentication and access policies.
- Provides a SOAP API for AccessAgents, as well as AccessAssistant and Web Workplace servers, to authenticate users, and to retrieve and synchronize system and user data.
- Provides a SOAP API for AccessStudio to upload new or updated AccessProfiles for distribution to AccessAgents.
- Provides a SOAP API for Tivoli Identity Manager to provision application credentials into user's Wallets and users into IMS.
- Provides SOAP and RADIUS APIs for third-party software, such as VPN, to authenticate users through one-time passwords.
- Provides a Web-based interface for administrators to manage users, machines and system policies, as well as to query audit logs. The Web-based interface is named AccessAdmin.

The IMS Server consists of a group of Web-based applications developed in Java and run on top of an Apache Tomcat application server. During installation of the IMS Server software, the applications server is also installed. Administration of the Tomcat application server itself is not necessary during IMS operation.

IMS database

The IMS Server stores all its data within a relational database. The IMS database contains these classes of data:

- System data

  The class of system data includes AccessProfiles, system policies, user and machine policy templates, and other system configuration data.

- User data

  The class of user data includes application credentials and user policies.

- Machine data

  The class of machine data includes any machine policies and information about deployed machines.

- Audit logs

  Every user and administration activity is stored in the database and even the SOAP call logs are stored in the IMS database.

Note: The database can be created on an existing database server, or it can be installed on the same system where the IMS Server resides. If the IMS database and IMS Server are running on different machines, the system clocks must be synchronized. Furthermore, because the IMS Server performs all database operations on behalf of the user defined as the database administrator, a database administrator account is required.

Expected data volume

The expected data volume is important for the sizing of the IMS database server. Based on the architecture and database design, the data volume for each class of data stored on IMS is estimated at:

- System data is expected to be 10 MB or less.
- User data can reach approximately about 200 KB per user.
- Audit logs require no more than 7 GB per 1000 users for a log retention period of one year.

Supported database engines

The following types of relational databases are currently supported:

- Microsoft SQL Server 2000
- Microsoft SQL Server 2000 Desktop Engine (MSDE)
- Microsoft SQL Server 2005
- Microsoft SQL Express
- Oracle Database 9i
- Oracle Database 10g
- IBM DB2 9.5 (available in the installation CD, but must be installed separately)

2.4 Solution considerations

In this section, we outline essential practices that should be considered to ensure a successful implementation with no impact to the underlying infrastructure. Unlike typical data center or infrastructure security changes, Tivoli Access Manager for Enterprise Single Sign-On is visible to the user community and therefore requires additional care to ensure user acceptance, and minimal frustration or perceived issues with the product.

2.4.1 Application profiles

The most visible function of Tivoli Access Manager for Enterprise Single Sign-On is the ability to provide SSO to the various applications within the organizations. This core capability depends on successfully profiling the various applications with AccessStudio, an application that is part of the Tivoli Access Manager for Enterprise Single Sign-On bundle.

Profiling applications can typically be the most significant amount of time in the planning and development of the deployment, because it involves several factors, including:

- Identification of the applications

  Identifying applications might appear to be a trivial task, but one has to consider that with larger organizations, applications can vary, and some are considered most critical.

- Prioritization of these applications

  Which applications are deemed critical to the users or to such demands as compliance or regulatory guidelines? Further, considering different user communities, you might have to recognize that the importance of applications can vary across the organization.

- Understanding the applications

  Although many applications can be very predictable, it is important not to assume an application's behavior. Especially for applications developed in-house, having an *interview* with the application owner to go through a set of questions is very valuable.

2.4.2 Considering second factor and machine types

One of Tivoli Access Manager for Enterprise Single Sign-On's strengths is the ability to integrate with various second factor devices, such as badge readers or biometric devices, and the way the AccessAgent can be deployed. Let us exam some of the more typical considerations:

- Personal desktop

  The *personal desktop* is most often associated as a system that has only one user accessing it for a prolonged period of time, such as a user's mobile computer or workstation. Generally, the use of a second factor is not considered given the large population of users and the costs associated with the second factor hardware. More recently, however, with the introduction of biometric devices such as fingerprint readers built directly into the system hardware, there is some level of interest in considering second factor authentication.

- Shared workstation

  A *shared workstation* is often associated with a machine that is used by a number of users, but where there is no real concern for privacy or the importance of switching between users quickly. Customer service representatives, systems on factory floors or in retail are often the typical environments that the shared workstation would be best suited for. Here, because of the limited number of systems, it is possible that a second factor will be employed because of pre-existing security devices like proximity cards already being issued.

- Private desktop

  Within fast-paced settings, where the need to automate the steps to ensure privacy are critical, such as in medical environments with a single workstation, the *private desktop*, together with a second factor device such as proximity, RFID or biometric becomes a strong value to the user community's efficiency. Here, the value of SSO and the ability for fast switching between user sessions are paramount for a successful user experience.

- Citrix and Terminal Services

  SSO services within a Citrix or Terminal service session is a strength of Tivoli Access Manager for Enterprise Single Sign-On. Having visibility to the users who depend on this service is important. In addition, Thin Clients are also often a factor in some environments and should be considered.

Similar to the prioritization of the applications, a task should be performed to prioritize which user community and what type of client is the most important. Two considerations when developing a plan are:

- First, introduce an SSO solution to a user community and then later introduce second factor devices. Although not ideal considering that many of the policies being developed might require additional tuning, sometimes having SSO is viewed as more important for the initial deployment than to incorporate this into a second-factor strategy.
- Tivoli Access Manager for Enterprise Single Sign-On provides very fine-grained control of user sessions, from the time a user is locked out of a screen, to when users are prompted for passwords. Consider the user communities first, and recognize that a good approach might be to treat each user community separately with respect to their requirements for second factor, and the behavior of the AccessAgent.

2.4.3 Core strategies

Consider the following three strategies when deploying Tivoli Access Manager for Enterprise Single Sign-On:

1. Target a select number of priority applications as the first phase.

   As noted in 2.4.1, “Application profiles” on page 60, the profiling of applications can take a considerable amount of time. For deployments that ultimately can have hundreds of applications to profile, this can be a long period of time.

   Through the process of prioritization, determine which applications will have the broadest business impact, or user acceptance. The result is often a company wide e-mail program, or an application that forces password changes often and therefore causes frustration or calls to the help desk.

   By focusing on this small set of applications, the rate of user success is high because the Tivoli Access Manager for Enterprise Single Sign-On administrators will have a higher chance of developing the profiles correctly the first time. Having a small set of applications allows more focused feedback from the select users to ensure a successful user experience.

2. Target a representative number of users as the first deployment.

   Just as important as the selection of applications, the first phase of the deployment should focus on users that are representative of the types of users that would be using the solution, and on considerations such as geography, language, or job role. Pay special attention to this first deployment to isolate any potential user configuration changes that are desired.

3. After full rollout, begin additional phases of applications.

   When the first successful set of users is deployed, continue to increase the number of users who are using Tivoli Access Manager for Enterprise Single Sign-On for the single sign-on feature, and if in place, the password reset rules. The important focus should be on gaining acceptance of the small set of applications with the largest number of users. When the deployment reaches its targeted goal of users, begin the next phase of applications. The application profiles can be automatically distributed to the user's system the next time they synchronize. Because the users are now already familiar with the SSO solution, the SSO support for the new applications will continue to benefit the users, and no additional education or considerations around agent installations are necessary.

2.4.4 Policy management strategy

Tivoli Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its components. These policies are configurable through various means so Tivoli Access Manager for Enterprise Single Sign-On can meet the requirements of specific organizational requirements. Policies have different visibilities and scopes, and are managed by different roles.

Refer to 4.8, "Managing policies" on page 124 for more information about policy management.

For a typical deployment, you use the AccessAdmin interface to configure user, machine, and system policies before you install the AccessAgent component.

2.4.5 Authentication strategy

Authentication defines how the system validates users so they gain access to Tivoli Access Manager for Enterprise Single Sign-On. Besides the standard authentication based on user name/password, the user can be authenticated by means of a proximity or building badge such as active or passive RFID, a fingerprint, a one-time password provided by SMS or OTP token, or a USB token. One of the key features of Tivoli Access Manager for Enterprise Single Sign-On is the ability to support a variety of these authentication factors.

The authentication component consists of two layers:

- Authentication factors
- Authentication Device Manager

Authentication to Tivoli Access Manager for Enterprise Single Sign-On involves two steps:

1. The user provides credentials with the *authentication factors*.
2. The authenticator, for example a smart card or RFID reader, validates the user with the *Authentication Device Manager*.

Authentication factors

Authentication factors have different forms and functions. With the exception of password and fingerprint, users can access systems and applications with a device that works like a key. Let us first look at the basic factors:

- Password

  The *password* is used to secure access to a Wallet. The user specifies this password when signing up with the Tivoli Access Manager for Enterprise Single Sign-On AccessAgent. Signing up with the AccessAgent means registering the user with the IMS Server and creating a Wallet.

- Secret

  The user is asked to enter a *secret* when signing up for a Wallet. A secret is like a second password or a backup password. The secret should be something that the user will not forget, even if it is not used for a long time and it is not likely to change. When the user signs up, the user selects a question from a list, and then provides the answer to that question.

  If a user forgets a password, the secret enables the user to set a new password. The user can also use the secret, along with an *authorization code*, to gain temporary access to the Wallet. An authorization code is generated by a help desk employee or an administrator. If self-service is enabled, users might have to specify a number of challenge-and-response questions during sign-up.

Second authentication factors

The password can be fortified by a *second authentication factor*. The combination of the password and a building badge or USB key, for example, strengthens the user's computer security because both authentication factors must be presented to access the computer. Based on the organization's security policy, using one of the following second authentication factors can be either mandatory or optional:

- Mobile ActiveCode
- RFID card
- Active proximity badge
- Fingerprint identification
- USB key
- USB proximity key

Refer to 4.14, “Strong authentication” on page 139 for more information about each second authentication factor.

By supporting building access badges, iTag, and mobile devices for authentication, Tivoli Access Manager for Enterprise Single Sign-On is well equipped to leverage *what you already have* as a second-factor. For example, Tivoli Access Manager for Enterprise Single Sign-On enables the use of building access cards, such as the HID Prox, HID iClass, Mifare, and Indala cards, as second factors for logical access. This approach reduces the cost of acquisition, the cost of provisioning, and also the cost of support. It provides greater user convenience, relieving users from having to carry additional devices. User adoption is high and training costs are minimized because existing personal devices are leveraged to secure access to corporate networks.

Tivoli Access Manager for Enterprise Single Sign-On also enables secure remote access by combining two-factor authentication with leading SSL VPN platforms. With the solution, users can access Web, desktop, and host-based applications through an SSL VPN connection and ensure two-factor authentication with one-time password (OTP) tokens or OTP delivered to smart phones, PDAs, e-mails, or other mobile devices.

Regardless of the choice of authentication factors, administrators may centrally manage all authentication policies through the AccessAdmin interface. In addition to multi-factor authentication, administrators may also enforce application password policies through Tivoli Access Manager for Enterprise Single Sign-On.

Refer to the *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951 regarding policy settings for authenticators.

2.4.6 Integration strategy

Combining Tivoli Access Manager for Enterprise Single Sign-On and Tivoli Access Manager for e-business with a comprehensive identity management strategy allows companies to greatly reduce maintenance costs and security risks.

The integration between the provisioning bridge and Tivoli Identity Manager is accomplished by using a workflow extension that Tivoli Identity Manager uses to communicate with the provisioning bridge Web service.

Figure 2-7 illustrates the necessary physical components.

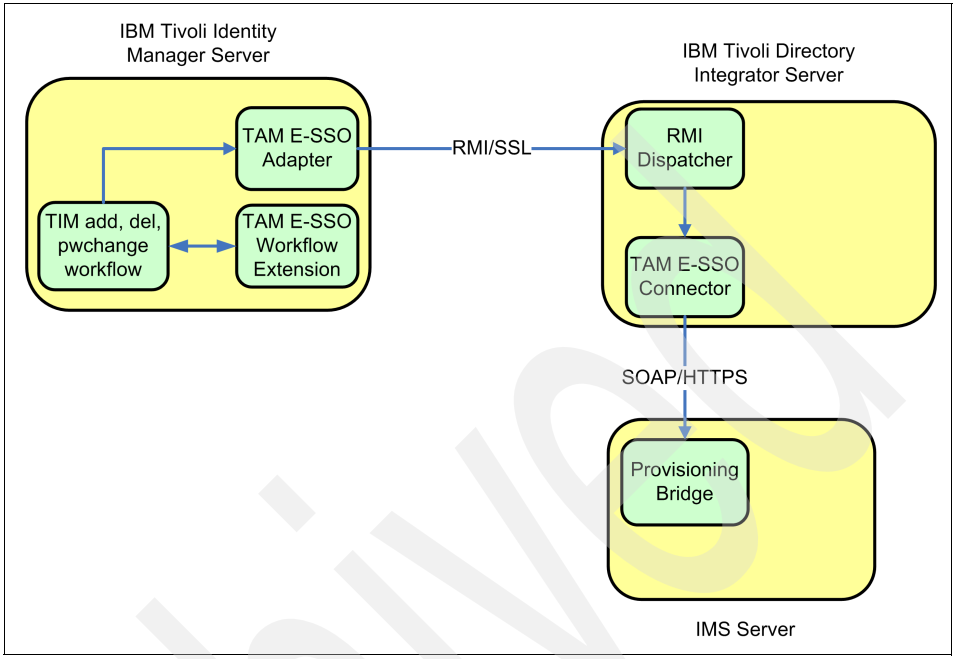

Figure 2-7 Identity Manager integration architecture

Tivoli Identity Manager has to communicate with the IMS Server to populate and manage credentials in the Wallet. The Tivoli Access Manager for Enterprise Single Sign-On provisioning bridge and workflow extension are the interface engines that act as intermediaries between the IMS Server and Tivoli Identity Manager.

Tivoli Identity Manager connects to the IMS Server with the Tivoli Access Manager for Enterprise Single Sign-On workflow extension to add account credentials to users' Wallets. To perform tasks, such as creating an IMS user, deleting an IMS user, and searching for IMS users, the workflow extension invokes operations on the provisioning bridge using the provided Tivoli Directory Integrator[4] AssemblyLines. After the workflow extension has been added to Tivoli Identity Manager, and the provisioning bridge configured on Tivoli Identity Manager, all application accounts provisioned through IBM Tivoli Identity Manager are provisioned to Tivoli Access Manager for Enterprise Single Sign-On also.

[4] IBM Tivoli Directory Integrator ships with IBM Tivoli Identity Manager. For more information, consult *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014.

The Tivoli Access Manager for Enterprise Single Sign-On *Provisioning Bridge* extends the benefits generated by Tivoli Access Manager for Enterprise Single Sign-On through the automation of the credential distribution process. The Tivoli Access Manager for Enterprise Single Sign-On Provisioning Bridge uses its API libraries to allow identity management software to automatically provision Tivoli 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 the user name or password can be managed transparently to them.

The Tivoli Access Manager for Enterprise Single Sign-On API for provisioning enables third-party identity provisioning systems to integrate with the IMS Server.

Available API types for provisioning API

Two sets of application programming interfaces (APIs) are available to integrate an identity provisioning system with Tivoli Access Manager for Enterprise Single Sign-On:

- Java API for provisioning

  This API is for identity provisioning systems that support Java-based connectors for integration with third-party systems. The Java API provides a wrapper around the SOAP API to simplify its operations. For example, encryption of application passwords is performed by the provided IMS Bridge, and is then transparent to the developer.

- SOAP API for provisioning

  If the Java API cannot be used, the developer may choose to use the SOAP API instead. The advantage of the SOAP API is that it is independent of any programming language, and the provisioning agent can potentially be written in any programming language native to the identity provisioning system.

Tivoli Access Manager for Enterprise Single Sign-On can provide real-time implementation of access security policies for users and applications.

An integration between a third-party identity provisioning system with Tivoli Access Manager for Enterprise Single Sign-On access security solution has the following results:

- A complete identity and access management solution that provides automatic application account provisioning
- A central view of all application accounts
- Sign-on/sign-off automation
- Authentication management
- User-centric audit logs and report generation
- Centralized de-provisioning for all accounts

For example, the Tivoli Access Manager for Enterprise Single Sign-On SOAP API for Mobile ActiveCode can be used to enable third-party applications to integrate with the IMS Server using SOAP, to achieve strong authentication with Mobile ActiveCode.

2.4.7 High availability and scalability

The IMS Server adopts a two-tier server architecture, with a front tier of application servers and a back-end database. As such, deploying the IMS and its database is possible in a number of configurations, ranging from low to high end.

The IMS Server and its database, and any underlying support infrastructure can be configured to achieve the availability and scalability requirements of the tangible environment. In this section, we describe three deployment models covering different deployment sizes and availability requirements.

Pilot deployments

Pilot deployments with no high availability requirements typically involve a single server machine hosting both the IMS and its database. This single-box configuration is not horizontally scalable and does not provide high-availability. The only way to support more users is to upgrade its processor capability.

Small scale deployments

Smaller environments with up to 10,000 users typically deploy a two-box clustered configuration, where each box hosts the IMS Server and the database.

In this configuration, a clustering solution such as Microsoft Cluster Server is required to maintain an active-passive pair of IMS and DB. Usually, this configuration requires that the two database hosts share a common external disk array, and that the *cluster-aware* versions of the database must be deployed. This configuration provides high-availability, because an automatic failover is initiated when the active node fails.

This configuration is typically limited to an active-passive pair and is thus not horizontally scalable. To support heavier loads, the hardware must be upgraded.

Large scale deployment model

Medium- to large-scale architectures with, for example, up to 500,000 users will adopt the standard two-tier architecture, with multiple IMS Servers in the front-tier and a clustered IMS database in the back end.

The IMS Servers must be fronted by a session-aware load-balancer. The IMS tier is thus horizontally scalable. An estimation is that each server, assuming a

two-processor dual-core 3.6 GHz Windows machine, can support up to 40 K concurrent AccessAgent sessions. As such, a deployment expecting 100 K concurrent AccessAgent sessions requires three such servers at the IMS tier to share the load.

The database tier can only be scaled vertically by default. As such, an important point is that the database host be sized correctly in accordance to the number of IMS Servers it is expected to service. A typical guideline, based on load test experiments, is to double the processor and memory capacity of the database host for every five additional IMS Servers.

Scaling up a combined IMS and database server

A single server machine hosting both the IMS and database server is sufficient for small-scale deployments. This configuration can be scaled-up in any of the following ways:

- Enhance the processor hardware (faster processor or multi processor).
- Add more RAM.
- Upgrade the disk sub-system (more disks, faster disks) and optimize the database file layout on these disks.

A single server configuration can be made highly-available by adding a second server and setting up an *active-passive* cluster over the two servers. Such a configuration typically involves:

- Use of Microsoft Cluster Service (or equivalent)
- Use of an external disk array shared by both server machines
- Use of a cluster-aware edition of the database server
- Configuring the cluster service to recognize IMS and the database as resources to be managed under the cluster

In such configuration, the cluster service monitors the following components:

- Host machines
- Health of the IMS Server
- Database services

If any of these components fail, the cluster service also triggers failover from one machine to another.

Scaling out the IMS Server

For most deployments, a two-tier architecture is suggested, with a tier of IMS Servers fronting a shared database server.

In this configuration, a hardware or software-based load balancing solution should be used to distribute the incoming traffic from various AccessAgent installations into multiple IMS Servers. The load balancing solution should support session affinity, where each client's request is consistently routed to the same IMS Server (until the server goes down, and the requests are then re-routed to another server).

Scaling up or scaling out the database server

The database server can be scaled up if performance measurements indicate that its processor, RAM, or disk is a bottleneck. In these cases, the methods for scaling up the database server include:

- Enhance the processor hardware (faster processor or multi processor).
- Add more RAM.
- Upgrade the disk sub-system (more disks, faster disks) and optimize the database file layout on these disks.

Solutions for scaling out the database server across multiple machines are typically vendor-dependent and might require a customized IMS installation process.

Components for high availability

The following three components require high availability (HA), as shown in Figure 2-8 on page 71:

- IMS Server
- Database Server
- Directory Server

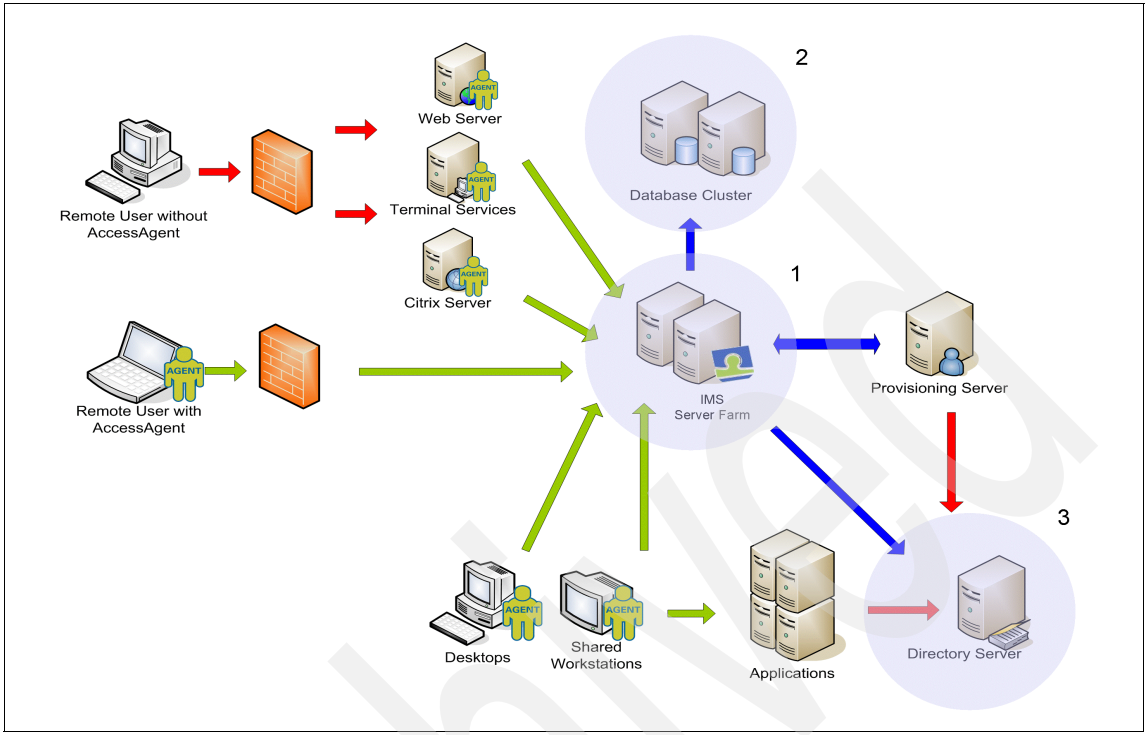

Figure 2-8 High availability architecture

Setting up the IMS Server for high availability

Two-tier deployments can make use of load balancing solutions to achieve high availability (HA). The load balancer automatically re-balances incoming traffic when a member of the server farm goes up or down. Some load balancers also support continuous monitoring of application or service status based on custom scripts (for example, pinging a certain URL), so that traffic can be re-routed if a certain application or service on a server machine fails to respond.

In the case of Microsoft NLB, each machine in the server farm can monitor the heartbeat of each other, and re-converge when a member of the farm goes up or down. However, NLB monitors only the server operating system's health. If the server operating system is up but IMS service is down, some IMS Server requests continues to be routed to that server. This issue can be addressed through some custom scripts to monitor the IMS Server.

Setting up the database server for high availability

The solutions for database server high availability (HA) are vendor-specific:

- Microsoft SQL Server Cluster (on top of Microsoft Cluster Service)
- IBM DB2 HADR
- Microsoft SQL Server Database Mirroring
- Oracle RAC

Most solutions involve an active-passive pair of database servers, except Oracle RAC, where servers are active-active.

IMS can interoperate with these highly-available database solutions, if IMS database schemas can be installed in the database to configure the IMS to recognize the database cluster/pair as one logical database.

2.4.8 Upgrades and migration strategy

The IMS Servers are always designed to be backward compatible. This typically means that a current IMS Server has the ability to work with the current version of AccessAgent, and also with older versions of the AccessAgents. Consequently, this architecture necessitates a specific sequence of upgrades for the components, with the IMS Server being the first to be upgraded.

Briefly, the steps involved in upgrading the deployment are as follow:

1. Backup the existing setup.
2. Upgrade the IMS Server.
3. Upgrade the AccessAgents in the deployment (incrementally).

After the server has been upgraded, and the machine policy templates with their assignments created, the AccessAgents can be incrementally upgraded according to the deployment upgrade plan.

Upgrading an existing installation of IMS Server

If you are upgrading your IMS Server to the latest version with the master password enabled, disable the master password before upgrading the IMS Server. After installing IMS Server, you can re-enable the master password.

Upgrading IMS Server with master password enabled

When the IMS Server's master password is enabled and the IMS Server is upgraded to version 8.0.0, the IMS Server cannot be started as a Windows service. The installer attempts to start the IMS Server as a Windows service after a successful upgrade. The issue is applicable to IMS Server version 8.0.0 with the master password enabled.

For previous versions of IMS Servers (before 8.0.0), the master password must be also disabled during an IMS Server upgrade. After installing IMS Server, re-enable the master password.

Notes:

- A fresh installation of IMS Server 8.0 is compatible only with AccessAgent 8.0 and later versions. Upgrading from earlier versions of IMS Server still have 1024-bit key pairs.
- Upgrading to IMS Server 8.0 and running the patch to upgrade to 2048-bit RSA key pairs works only with AccessAgent 8.0 and later versions.

3

Deployment and implementation

A Tivoli Access Manager for Enterprise Single Sign-On system can contain many components and requires careful planning to deploy and implement it, as we discussed in the previous chapter. In this chapter, we describe the technical implementation of the Tivoli Access Manager for Enterprise Single Sign-On base environment. First, we verify the operating system prerequisites. Then, we explain how to install the necessary components. Finally, we discuss how to deploy the enterprise single sign-on setup.

3.1 Installation overview

In this section, we focus on the concepts of a base level implementation of Tivoli Access Manager for Enterprise Single Sign-On, and the components you must be aware of when designing the deployment architecture.

Figure 3-1 depicts the basic logical components of Tivoli Access Manager for Enterprise Single Sign-On.

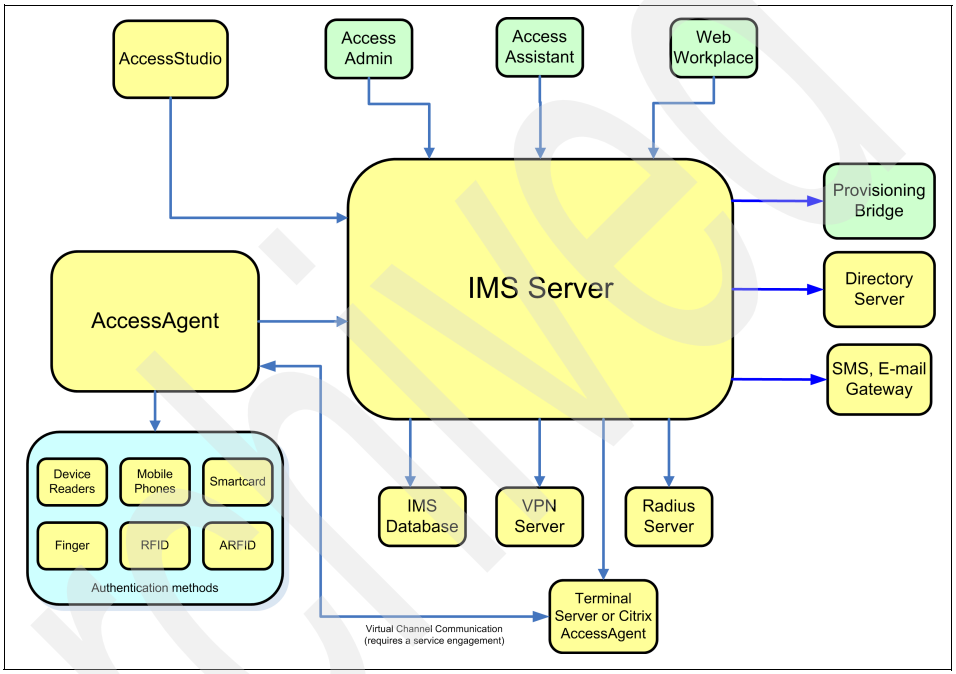

Figure 3-1 Logical component architecture

The logical component model illustrates the software components that are being used to build a system.

Components required for a base-level implementation of Tivoli Access Manager for Enterprise Single Sign-On include:

- Central user repository/directory

  The central user repository can be one of several supported repositories, including Active Directory, Novell®, and generic LDAP. The central user repository must be in place prior to installing any Tivoli Access Manager for Enterprise Single Sign-On components.

- IMS Server

  The IMS Server is installed on either an existing or dedicated server. The IMS Server is a Java-based application that runs on its own instance of Apache Tomcat, which is automatically installed with the IMS Server software.

- IMS database

  The IMS database stores all of the Tivoli Access Manager for Enterprise Single Sign-On configuration, policy, and user data. This database can be created on an existing database server, or it can be installed on the same system where the IMS Server resides. Supported databases include IBM DB2, Microsoft SQL, and Oracle.

- AccessAgent

  An AccessAgent is installed on each client system, Windows Terminal Server, and Citrix MetaFrame server that is to be managed by Tivoli Access Manager for Enterprise Single Sign-On.

- AccessStudio

  AccessStudio is an administrative tool that is used to create AccessProfiles. It has to be installed on at least one workstation, normally on that of one or more IMS administrators.

More details about the logical components can be found in 2.3.1, “Logical component architecture” on page 40.

3.1.1 System requirements

The Tivoli Access Manager for Enterprise Single Sign-On base components can be integrated into existing servers if the servers have sufficient resources. Each base component has specific software dependencies and requires prerequisites with respect to hardware and operating system platforms that are supported. For hardware requirements such as disk size, memory, and so on, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

3.1.2 Deployment architecture

The deployment architecture for a Tivoli Access Manager for Enterprise Single Sign-On-based installation is straightforward. It consists of a client-side application (AccessAgent) communicating with a central server-side application (IMS Server). Deployments can become more complex with the integration of optional advanced components such as identity management software and external data sources. Even so, the client-server model remains the same for the core Tivoli Access Manager for Enterprise Single Sign-On components.

Client-side components

Tivoli Access Manager for Enterprise Single Sign-On consists of two client-side applications, *AccessAgent* and *AccessStudio*, as follows:

- The AccessAgent is installed on user workstations and Microsoft Terminal or Citrix MetaFrame servers. Its main function is the recognition and interception of user authentication and change password dialogs. It acts on these dialogs for authentication and password change automatically depending on how policies are configured. The AccessAgent is comprised of several underlying components that also perform tasks such as:
  - Synchronizing data with the IMS Server for updating policies and profiles, and retrieving user Wallets.
  - Securely storing credentials in the Wallet on the local workstation.

  The underlying components and their architecture are discussed in 2.3, “System architecture” on page 38.
- AccessStudio is a tool that administrators use to configure or create *AccessProfiles*, which are profiles that facilitate the automatic log on, log off, and password change for applications that require authentication. AccessStudio must be installed on only one administrative workstation.

Server-side components

The server-side components consist of the *IMS Server* and the *IMS database*:

- The IMS Server is the central point of administration for user identities, AccessProfiles, authentication policies, and authentication factors. Administration is performed through a Web interface called AccessAdmin where administrators can create and modify policies, and manage users.
- The IMS database stores all Tivoli Access Manager for Enterprise Single Sign-On configuration and user objects such as policy templates, user credentials, authentication services, and AccessProfiles. How user credentials are securely stored on the database and in local user Wallets is described in “Securing Wallets” on page 52.

The AccessAgent synchronizes with the IMS Server on a regular interval to retrieve policy updates.

Target applications

The target applications can typically be grouped into the following categories:

- Windows client/server

  Typical application with a client component that is locally installed on the user's workstation. The client component requests user authentication and communicates with an application component running on a back-end server, for example Lotus Notes.

- Java-based

  The authentication dialog for this type of application was developed in Java and is sent to and executed on the user's workstation at the time that the application is launched.

- Web-based

  Applications running on a Web server that requests users to authenticate from a Web browser.

- Terminal emulators

  Terminal emulators are installed and executed locally on client workstations and are configured to communicate with back-end applications emulating a specific terminal type. Examples are 3270 terminal emulators to access host-based applications, Telnet to access UNIX® systems, and so on.

3.1.3 Create administrative users

To prepare for our base component installation and configuration, two administrative users must be created:

- Database administrator

  The IMS Server performs all database operations on behalf of the user-defined as the database administrator.

  > **Note:** For Microsoft SQL Server installation the user name and password entered must NOT be the database Administrator (SA) account. The user should have public, *db_owner* rights for the created database. The password should also not contain the dollar symbol ($)

- Active Directory / LDAP *lookup-user*

  Tivoli Access Manager for Enterprise Single Sign-On uses the lookup-user to retrieve user attributes from the Active Directory / LDAP enterprise repository. The user defined as the lookup-user should not be the primary user account for any employee, because password change or account lockout can cause

problems with authentication for all users. A good practice is to create a system account specifically for the purpose of acting as the lookup-user.

Note: Remember that if the lookup-user's password must change, then the IMS administrator must be aware of this and set the new password in the IMS Server configuration.

3.1.4 Install the IMS database software

The first base component of the Tivoli Access Manager for Enterprise Single Sign-On system is the IMS database. This database serves as the central repository for all Tivoli Access Manager for Enterprise Single Sign-On system and user data. The installation of a database is product-specific. Tivoli Access Manager for Enterprise Single Sign-On supports the following databases:

- IBM DB2 9.5
- Microsoft SQL Server 2000 Desktop Engine (MSDE)
- Microsoft SQL Server 2000, Microsoft SQL Server 2005
- Microsoft SQL Express
- Oracle 9i, 10g

Note: For Microsoft SQL Server databases, the database collation should be *SQL_Latin1_General_CP1_CS_AS.*

For detailed installation instructions of the supported platform, follow the installation instructions provided by the vendor. For Tivoli Access Manager for Enterprise Single Sign-On specific database prerequisites, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

3.1.5 Install the IMS Server

This section provides an installation overview of the Tivoli Access Manager for Enterprise Single Sign-On IMS Server. For detailed installation steps and information about the prerequisites, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

The installation steps depend on the type of installation you will be doing - new or an upgrade. To simplify the installation and configuration, the IMS Server installation uses an installation wizard. The wizard is started by clicking the `imsinstall.exe` icon in the Tivoli Access Manager for Enterprise Single Sign-On

installation CD. The initial window reminds you of the required setups; ensure you meet all the requirements before continuing with the installation.

The installation wizard offers three installation types:

- Express
- Custom
- Upgrade

Express

This option installs Microsoft SQL Server Express Edition/MSDE with the IMS Server application.

Important: Microsoft SQL Server Express Edition is not supported in a production environment and is only used with the IMS Server for demonstrations and proofs of concept.

Custom

In a custom installation, you have to:

1. Specify the fully qualified domain name of the IMS Server.

   Note: The fully qualified domain name entered here is the same that has been assigned to the certificate used for secure communication between the AccessAgent and the IMS Server. This name cannot be reset later. If you must change that name at a later time, another installation of the IMS is necessary.

2. Specify the supported database type to be used by the IMS Server.

   Note: If the IMS Server and database server are on different systems, we suggest that the clocks of both systems be synchronized. This can be achieved by configuring the Windows Network Time Protocol (NTP).

3. Specify the database connection parameters:
   - Database host name

     Enter the fully qualified host name where the database is installed.
   - Database instance (optional)

     Optionally enter the name of the database instance.

– Database port

  Enter the TCP port that was specified during the database install. The default port is automatically entered into this field.

– Database name

  Enter the name of the database.

– Administrator user name and password

  Enter the database administrator user name and password that was mentioned in 3.1.3, “Create administrative users” on page 79

Upgrade

If you are upgrading your IMS Server to the latest version with the master password enabled, disable the master password before upgrading the IMS Server. After installing IMS Server, you can re-enable the master password.

Note: For IMS Server upgrades, the existing settings (for example, Java Virtual Machine, concurrent threads, and so on) are not affected. These settings are retained and must be re-configured.

3.1.6 Initial IMS Server configuration

In this section, we give an overview of configuring the IMS Server for initial use. Immediately after the IMS Server installation has completed, the IMS Server configuration page opens so that an initial configuration can be completed.

If the configuration page does not open or you want to revisit this step later, select **Start** → **Programs** → **TAM E-SSO IMS Server** → **TAM E-SSO IMS Configuration Utility**, or manually use a Web browser on the IMS Server and point it to (your local host):

```
http://localhost:8080
```

The initial configuration consists of three tasks:

1. Specify the domain of the enterprise directory to connect to, and enter the lookup-user name and password.
2. Decide whether to synchronize the enterprise directory password and Tivoli Access Manager for Enterprise Single Sign-On password (this option is available only for Active Directory).
3. Assign an enterprise directory user to act as the IMS administrator.

Synchronizing the passwords and assigning an IMS administrator can be done later.

After successful configuration, stop and start the IMS Server as follows:

1. **Start → Programs → TAM E-SSO IMS Server → Stop IMS Service**
2. **Start → Programs → TAM E-SSO IMS Server → Start IMS Service**

3.1.7 Specify IMS Server settings using AccessAdmin

Tivoli Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its components. System, machine, and user policies each have unique and overlapping policy parameters. Policies are created and modified to enforce rules set by the business. Before production deployment, have all of your policies clearly defined as direct translations of the business security requirements. Modifying policy after deployment might be unavoidable, but a best effort should be made to define policies before deployment to production.

The IMS Server has an interface named AccessAdmin, which is consistent with the interface of AccessAgent. Different access rights are given to Administrator and Help desk roles. Administrators have full control over policies. Users assigned to the Help desk role have more limited control over policies. Refer to Table 3-1.

Table 3-1 Policies and their scopes

Policy type	Administrator permission	Help desk permission	Policy scope
System policies	Full read/write	Read only	System-wide
Machine policies	Full read/write	Read only	Machines
User policies	Full read/write	Full read/write	Users

Logging on to AccessAdmin requires certificate authentication. From the IMS Server machine, you can log on to AccessAdmin by providing a user name and password, without installing AccessAgent. If required, use the IMS Configuration Utility to allow form-based login to AccessAdmin from any machine. Otherwise the user must be logged on to a cached Wallet that has either an Administrator or a Help desk role. Certain configurations (for example, system policies and machine policies) can only be viewed but not modified by a Help desk user.

As with the AccessAgent interface, AccessAdmin has a navigation panel for accessing various functions, such as:

- User search and administration (to modify user policies, issue authorization code, unlock a locked Wallet, revoke user, and so on)
- Machine search and maintaining machine policy templates
- Creating and maintaining policy templates (can only be created and maintained by the Administrator, but Help desk can view and apply)
- Setting system and application policies (can only be modified by the Administrator, but Help desk can view)
- Accessing logs and status information

Tivoli Access Manager for Enterprise Single Sign-On AccessAdmin supports dynamic non-hierarchical groups, collapsible sections, and the setting of policies for groups and users. Attributes that define logical groups (for example, department) can be obtained directly from the corporate directory.

When the user signs up or a machine joins the IMS Server, policies are initially assigned based on the machine or user attributes that match the policy template.

Subsequently, user groups are dynamic because membership depends on the user's policies. For example, a user might belong to the group of RFID users because the authentication policy is Password + RFID. By changing the authentication policy for the user to USB Key, the user becomes a member of the group of USB Key users.

User policy modifications can be performed on individual users or on entire groups of users. A user may belong to the group of all USB Key users, as well as the group of all AccessAssistant users. Because groups are based on search criteria, they are virtual and they overlap.

User policy templates can be defined for specific groups of users to facilitate policy setting. For example, a template can be defined for the Finance department. Any new user whose department attribute is Finance will have the policies initialized with the template settings. Machine policy templates are defined for each machine that joins the IMS Server.

These policies are under `scope:machine(scp_machine)`, and keyed on the machine name. The machine policies are synchronized incrementally based on the machine name.

Machines can be assigned to an existing machine policy template, based on one or all of the following attributes:

- Machine name
- IP address
- AccessAgent version
- OU group
- Active Directory security group
- Machine tag

All policies with system, machine, or user scope can be modified through AccessAdmin. User policies can also be modified for an entire group of users by using the Search Users feature. System policies may be defined for authentication services, applications, or a combination of an authentication service and application. The Help desk role can be defined for different groups of users. A user taking on the Help desk role associated with a group, can manage (for example, authorize and revoke) users only for that group. Help desks may manage overlapping groups of users.

AccessAdmin is also used to issue authorization codes to users. Each authorization code has a selectable life span.

For initial configuration AccessAdmin defines initial system policy settings, creates a default user policy template and creates one or more machine policy templates, depending on your selection. You start the initial configuration by clicking **Setup assistant**. The Setup assistant guides you through the AccessAdmin setup process.

3.1.8 Install the AccessAgent

The next step in our basic deployment is to install the AccessAgent on all workstations that require single sign-on.

The AccessAgent performs the following primary functions:

- It monitors for applications that are configured for single sign-on, and takes action on them.
- It communicates with the IMS Server to obtain configuration data and retrieve user Wallets.
- It allows users to access their Wallets and manage their credentials.

You can pre-configure several AccessAgent setup parameters by modifying the `SetupHlp.ini` file found in the AccessAgent `Config` installation directory, prior to running the AccessAgent installer. You can also modify AccessAgent registry options by modifying the `DeploymentOptions.reg` file located in the `Reg` folder.

The `SetupHlp.ini` contains three categories of parameters:

- Options that are available only at setup time
- Options that are available at setup and AccessAgent runtime and that map to multiple registry values each
- Options that are available at setup and AccessAgent runtime and that map to one registry value each

The options that map to registry values can be modified after the AccessAgent setup, but the options only available at setup time cannot be set or changed after the AccessAgent installation. If those options are required after installation, you must first uninstall the AccessAgent, then reinstall with the setup time only parameters set as needed. Carefully review each option and determine whether modifying the values based on your deployment is necessary.

The next configuration option is important if you have to enable single sign-on for Java applications. To enable the Tivoli Access Manager for Enterprise Single Sign-On Java Observer module to trigger for Java applications, you must specify the paths to the Java Virtual Machine (JVM™) directories installed on the workstation.

Note: Modifying the options in the `SetupHlp.ini` file can assist in streamlining the deployment of AccessAgent to multiple workstations using software distribution tools that are Windows-supported.

The IMS Server location should be set during the typical setup period, which is done by setting the ImsServerName key in `SetupHlp.ini` appropriately. The AccessAgent installer will automatically download the IMS Server certificate from the IMS Server.

You can install AccessAgent using any of the following methods:

- Using an installation CD

  The installation automatically begins when the AccessAgent installation CD is run. If the installation does not begin, access the CD by using Windows Explorer and double-click the `setup.exe` file.

- Installing with a USB Key

  The installation files for AccessAgent can be placed in the storage area of the USB Key. Insert the USB Key into the port, and access the key by using Windows Explorer. Double-click the `setup.exe` file to start the installer.

- Using centralized installation by Administrator

  An organization can have a mechanism in place that automatically installs AccessAgent when the user logs on. In this case, no installation windows are displayed except the one that prompts the user to restart the computer.

Notes:

- A common problem when installing AccessAgent on a server (in particular, Windows 2003 Server) is that Windows has an advanced security option enabled by default. This option prevents AccessAgent from performing authentication with IMS Server, which means the user cannot use AccessAdmin. To disable this option, use **Start** → **Control** → **Panel** **Add/Remove programs** → **Windows** components, then uninstall Advanced Security Option.
- The AccessAgent installation in Microsoft Windows Vista® requires that the following security option be enabled in the Active Directory:

  `Interactive logon: Do not require CTRL+ALT+DEL`

  AccessAgent automatically enables this security option during installation. However, if other group policy enforcements are configured, they could prevent the AccessAgent installer from enabling the security option.

  If the setting is not enabled, users have to press Ctrl+Alt+Del to display the AccessAgent logon screen for log on.

AccessAgent uses an IMS Client Certificate for authentication when connecting to the IMS Server. The IMS Client Certificate is stored in a USB Key.

For detailed information about the setup parameters, the AccessAgent installation methods, and how to customize the banner on the AccessAgent user interface, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

After installing AccessAgent, verify that all program folders and registry entries are successfully installed in your machine. For more details, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

3.1.9 Install AccessStudio

AccessStudio is used by administrators to create AccessProfiles that contain instructions for handling automation for an application. AccessProfiles can be created and saved to a file or existing AccessProfiles on the IMS Server, or AccessAgent can be downloaded into AccessStudio and modified. After a profile

is created, it can be uploaded to the IMS Server to publish the data to the server for use in the corporate environment.

Before you install AccessStudio, ensure that all prerequisites are met, as listed in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

The installation of AccessStudio is a short process:

1. Locate the `AccessStudio-8.x.x.x.msi` installation binary and double-click it.
2. You are presented with the License Agreement window. If you agree to the terms, select **I accept the terms in the license agreement** and click **Next**. This begins the installation of AccessStudio.
3. After the install wizard completes, click **Finish**.

3.2 AccessProfile configuration

Now that we have discussed the installation and configuration of the base components, we look at the configuration of Tivoli Access Manager for Enterprise Single Sign-On so that users can begin using the single sign-on functionality for their applications.

The high-level steps for configuring applications for single sign-on are the same as for any enterprise application:

1. Configure an authentication service if one does not already exist.
2. Configure an AccessProfile if one does not already exist.
3. Move the application profile to the *enterprise authentication services*.
4. If using more than one user template, define which applications are assigned to each user template.

Understanding the relationship between AccessProfiles, applications, and authentication services is important. AccessProfiles consist of an authentication service and the logical reference to an application. The application is a logical reference to an `.exe` file or a Web site. An authentication service defines how user credentials are submitted to the application. Multiple applications can use the same authentication service. A single application object can be associated with several AccessProfiles, but you can associate an AccessProfile with only one application object,

Note: When associating more than one AccessProfile with an application object, carefully choose your signature. If more than one AccessProfile matches the event in question, none is invoked.

Authentication services can be configured as either an *enterprise authentication service*, or a *personal authentication service*. Administrators can change a service to be personal or enterprise through AccessAdmin.

Enterprise authentication services allow for greater administrative control over the user interaction with the service. Users are not allowed to delete an enterprise service account from their Wallet, and they cannot set *Never* as an option for the password entry. Additionally, audit logs are stored and generated on the IMS Server for *enterprise authentication services only*.

Personal authentication services allow users more control over how they want the AccessAgent to interact with the authentication service. Users might have an unlimited number of accounts per service; administrators are not able to grant or deny access to specific users. The administrator has the ability to disallow all personal authentication services, but not specific personal authentication services.

Note: For all corporate-related authentication services, a good practice is to set them to *enterprise authentication services* because of the enhanced administrative control and the audit logging.

The two kinds of AccessProfiles are:

- Standard AccessProfiles

  Use AccessStudio's AccessProfile Generator to create standard AccessProfiles through a series of wizard windows. Standard AccessProfiles, also known as *Simple SSO Support*, contain all logon, password, and logoff information within one or more screens. Examples are logon screens for applications, such as messaging software and e-mail software. Standard AccessProfiles also support most applications in different deployment scenarios. Use standard AccessProfiles for automating most applications.

- Advanced AccessProfiles

  For more complex applications, create advanced AccessProfiles. Advanced AccessProfiles, also known as *State Engine SSO Support*, automate operations based on various conditions. Use advanced AccessProfiles for complex logon situations, such as verification of conditions before automatic logon, greater control over what triggers an action, and the sequence of these actions.

An Access Profile has a certain defined lifetime that is based on application type:

- An application executable is considered closed when it no longer shows up in Task Manager.
- For Web sites (Web applications), when you navigate to a different Web site without closing your browser, a different AccessProfile can be loaded and your AccessProfile will be unloaded.
- For a Java applet, say your AccessProfile is written for javaw.exe, then it will be valid as long as javaw.exe is running.

Let us look more closely at the two types of AccessProfiles in 3.2.1, “Standard AccessProfiles” on page 90 and 3.2.2, “Advanced AccessProfiles” on page 101.

3.2.1 Standard AccessProfiles

Use AccessStudio to create new, import, and view existing AccessProfiles from the IMS Server or AccessAgent installed on your computer. As previously mentioned, Standard AccessProfiles, also known as *Simple SSO Support*, contain all logon, password, and logoff information within single or multiple screens. Examples are the logon screens for applications, such as IBM Lotus Sametime® Connect and CompanyMail. Standard AccessProfiles also support most applications in different deployment scenarios.

You can create standard AccessProfiles using the AccessProfile Generator. When you create an AccessProfile, the wizard automatically creates the application object and the authentication service for the AccessProfile.

Use the AccessProfile Generator to create the following types of AccessProfiles:

- Windows (Win32®, 16 bit) applications
- Web applications
- Java applet
- TTY applications (for example, PuTTY, SecureCRT)
- Mainframe or cursor-based applications
- Mainframe applications with HLLAPI support
- Other applications

Depending on the type of application and workflows that are defined for that application, creating AccessProfiles requires one or more of the following tasks:

- Creating a *logon* AccessProfile
- Creating a *change password* AccessProfile
- Creating a *logoff* AccessProfile
- Creating an *other task* AccessProfile

Note: You do not have to create a new AccessProfile for each task we listed. You can develop an application profile that includes more than one task within the same profile.

Understanding the process of creating AccessProfiles is very important. That is why we use Windows applications as a step-by-step example for creating AccessProfiles in the following section. For detailed information about creating other types of AccessProfiles, refer to the *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

Windows applications

Windows applications (for example, Win32, 16-bit), such as Company Mail, are applications that run on the Windows platform.

Most elements recognized by AccessProfiles are part of a hierarchical structure. To identify application screens and Web page elements, Tivoli Access Manager for Enterprise Single Sign-On uses *signatures*. These signatures are then communicated to AccessAgent. The next time the same fields are presented, AccessAgent automatically supplies the user credentials in their respective fields. For more information about signatures, refer to 3.2.2, “Advanced AccessProfiles” on page 101.

This section describes how to:

- Create logon AccessProfile for Windows applications
- Create a change password AccessProfile for Windows applications
- Create a logoff AccessProfile for Windows applications
- Create an other task AccessProfile for Windows applications

Create logon AccessProfile for Windows applications

We use the *Assistant* wizard to generate the AccessProfile for the Windows application, as follows:

1. Open AccessStudio by selecting **Start** → **All Programs** → **TAM E-SSO AccessStudio** → **AccessStudio**.
2. Select **New** → **AccessProfile (using Assistant)**, as shown in Figure 3-2 on page 92.

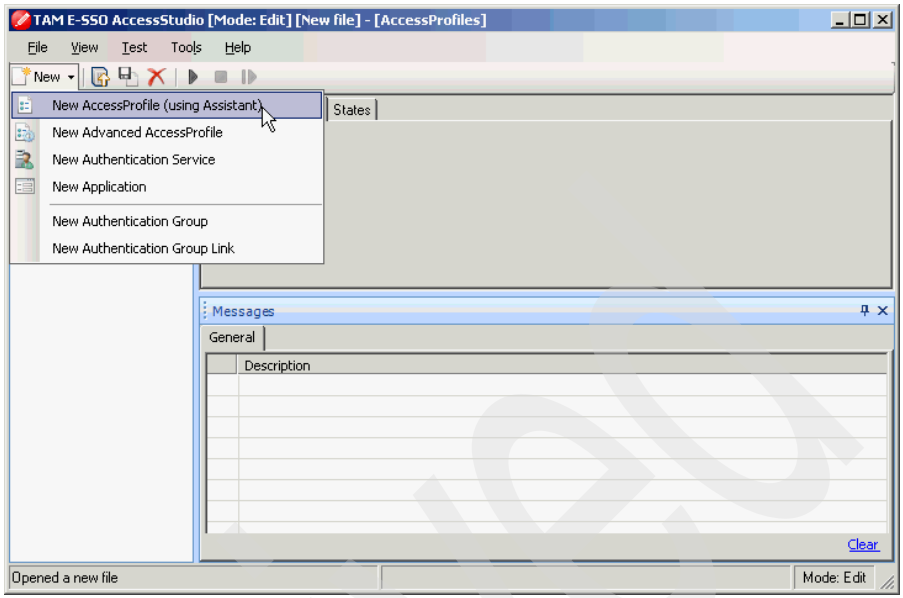

Figure 3-2 Create a new AccessProfile using Assistant

3. At the AccessProfile Generator welcome window, click **Next**.
4. Launch the application for which you want to create an AccessProfile.
5. After the application screen or Web page opens, click **Next** to proceed.
6. As shown in Figure 3-3 on page 93, enter a unique name for the application in the **Application name** field, select **Windows application** as the application type and click **Next**.

Figure 3-3 Enter an application name and select the application type

7. Select the task that you want to automate: Logon, Change password, Logoff, or Other tasks. You can add more tasks later, so start with the task you have to automate first, which is Logon. Select **Logon** and then click **Next**, as shown in Figure 3-4 on page 94.

> **Note:** Logon does not have to be the first task to automate. Depending on the workflow for your application, you may have to automate other tasks first, such as the clicking of a button or a link or the automatic pressing of certain keys.

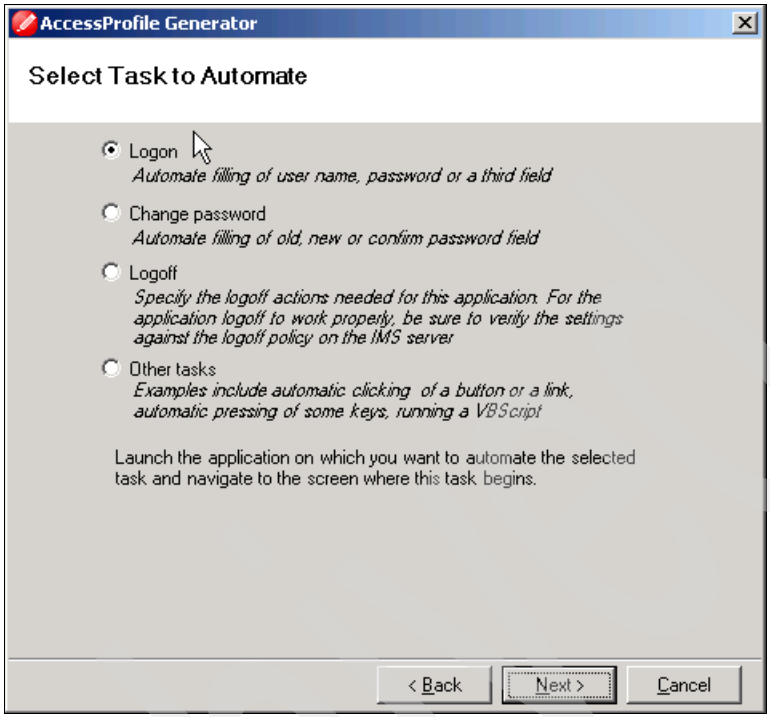

Figure 3-4 Select Logon to automate filling of user name and password

8. Enter a unique name in the **Enter a name** field for the screen or Web page you want to capture.
9. Based on your selected task, capture identification information for the fields on the application screen, as follows (the fields available for each automated task vary):
   a. Click the **Finder tool** from the AccessProfile Generator.

      Note: If the Finder tool is deactivated, activate it by clicking the **Edit Signature** link, then closing the pop-up that opens.

   b. Drag the **Finder tool** to the matching field in the application screen. As you drag the Finder tool to the application, the AccessProfile Generator selects the field or button you want to capture.
   c. When the Finder tool is positioned over the field, release the mouse button. If the field was captured successfully, the Clear option is activated. The default screen name from the application is retrieved. Click **Clear** to undo the capture.

d. Use the **Extra Field Finder** tool to capture an additional field unique to the application, if available for the selected task. The Extra Field can be a drop-down list or any domain field group.

e. Click **Advanced Settings** to perform the task only when a certain condition is satisfied. For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

10. After capturing all the application fields, click **Next** to proceed.

11. Perform one of the following steps (see Figure 3-5):

– To edit the previously captured screen, select the screen and click **Next**.

– To remove the previously captured screen, select the screen title in the list box and click **Delete**.

– The same logon screen might appear again after logoff. Select an auto-fill option for the same logon screen for subsequent logons: **Ask user, Do not auto-fill, Auto-fill,** and **Auto-fill and submit**. Based on the selection, AccessStudio will automate or not automate similar logon screens as set in this AccessProfile.

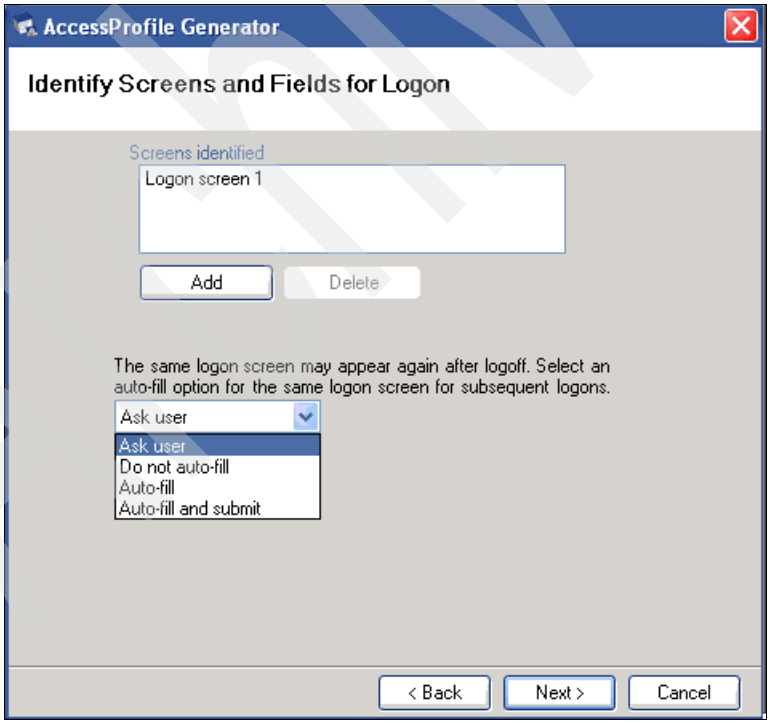

Figure 3-5 Identify additional windows and select auto-fill for subsequent logons

12. Click **Next**.
13. Specify whether you want AccessStudio to identify the successful logon by selecting one of the following options:
    - **No**. If you select this option, no success screen or message displays.
    - **Yes, identify the screen that appears upon successful logon**. If you select this option, drag the Finder tool and drop it on the success application screen or Web page. When the **Finder tool** is positioned over the screen or Web page, release the mouse button. Based on the captured item, you can also modify the screen title or text.
    - **Yes, simply detect closure of the logon screen**. If you select this option, the logon screen closes without any confirmation.
14. Click **Next**.
15. Perform one of the following actions:
    - Select **Use a previously created authentication service** and choose an authentication service from the drop-down list.
    - Select the default **Create one for me automatically** option to create a new authentication service.

    Note: AccessProfiles associated with the same authentication service belong to the same verification entity. Changes made to the logon information in one AccessProfile are reflected across all others associated with the authentication service. For more information about authentication services, refer to *"Managing authentication services" on page 107*

16. Click **Finish** to return to the AccessStudio user interface. The captured tasks and the identified screens are displayed in the General Properties tab.

    Important: Test all the AccessProfiles before uploading to IMS. For details, see the chapter about AccessProfiles for testing in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

17. Upload the AccessProfile to the IMS Server to activate it. In the Data type pane, right-click on the AccessProfile, and select **Upload to IMS**. Click **Yes** when the IMS Upload Confirmation displays. Another message box displays, indicating the success or failure of the upload.

Create a change password AccessProfile for Windows applications

Perform the following steps:

1. Follow steps 1 on page 91 - 6 on page 92 in the procedure “Create logon AccessProfile for Windows applications” on page 91.
2. Select **Change password** and click **Next**.
3. Enter a unique name for the screen you want to capture.
4. Capture identification information for the fields in the application window:
   a. Click the **Finder tool** from the AccessProfile Generator.

      Note: If the Finder tool is deactivated, activate it by clicking the **Edit Signature** link, then closing the pop-up that opens.

   b. Drag the **Finder tool** to the corresponding field in the application screen. As you drag the **Finder tool** to the application, AccessProfile Generator marks the field or button that can be captured.
   c. When the Finder tool is positioned over the field, release the mouse button. If a field was captured successfully, the **Clear** option is activated. The default screen name from the application is retrieved. Click **Clear** to undo the capture.
   d. Click **Advanced Settings** to perform the task only when a certain condition is satisfied. For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.
5. Click **Next**.
6. Select the **Change Password** screen from the Screens identified field. Perform one of the following tasks:
   – To edit the previously captured screen, select the screen and click **Next**.
   – To remove the previously captured screen, select the screen title in the list box and click **Delete**.
7. Specify whether you want AccessStudio to identify the successful changing of the password. Select one of the following options:
   – No (no success screen or message displays)
   – Yes, identify the screen that appears upon successful change password
   – Yes, simply detect closure of the change password screen.

   If you selected **Yes, identify the screen that appears upon successful change password**, drag the **Finder tool** and drop it on the success application screen or Web page. When the **Finder tool** is positioned over the

screen or Web page, release the mouse button. Based on the captured item, you can also modify the screen title or text.

8. Click **Finish** to return to the AccessStudio user interface. The captured task and the identified screens are displayed in the **General Properties** tab.

> **Important:** Test all the AccessProfiles before uploading to IMS. For details, see the chapter about AccessProfiles for testing in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

9. Upload the AccessProfile to the IMS Server to activate it. In the Data type pane, right-click on the AccessProfile, and then select **Upload to IMS**. Click **Yes** when the IMS Upload Confirmation displays. Another message box displays, indicating the success or failure of the upload.

Create a logoff AccessProfile for Windows applications

Perform the following steps:

1. Follow steps 1 on page 91 - 6 on page 92 in the procedure “Create logon AccessProfile for Windows applications” on page 91.
2. Select **Logoff** and click **Next**.
3. Select one of the following logoff methods:
   - Close the application. If you select this method, proceed to step 9 on page 99.
   - Log off gracefully. If you select this method, select a graceful logoff option and proceed to step 4.
4. Specify either a specific set of screens or only generic screens for the graceful logoff task:
   - To specify a specific set of screens and actions, select **Identify specific screens and set specific actions**, click **Next**, and go to step 5.
   - To specify screens that do not need a custom set of actions, select **Create a generic set of actions for unidentified screens**, click **Next**, and go to step 6 on page 99.
5. If you selected **Identify specific screens and set specific actions**, perform the following steps:
   a. Identify the logoff screen by entering a unique name for screen capture.
   b. Click the **Finder tool** from the Unique screen text for identification field.

Note: If the Finder tool is deactivated, save the AccessProfile as it is, then restart AccessStudio.

c. Drag the **Finder tool** to the matching field in the application screen. As you drag the **Finder tool** to the application, AccessProfile Generator marks the field or button that can be captured.

d. When the **Finder tool** is positioned over the field, release the mouse button.

e. Click **Advanced Settings** to perform the task only when a certain condition is satisfied. For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

f. Click **Next**.

6. Specify actions for logoff. Select the action you want to automate from the Available actions drop-down list. (Refer to Creating AccessProfiles that perform automation tasks in the *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956 for details.) Perform the following tasks:

   a. Select each action, enter a menu path or use the **Finder tool**, then click **Add**.

   b. Click **Next** after adding all the required logoff actions.

7. Identify the logoff screen. Select the logoff screen you have captured from the Screens (last screen if checked) field:

   – To edit the previously captured screen, select the screen and click **Next**.

   – To remove the previously captured screen, select the screen title in the list box and click **Delete**.

8. Click **Finish** to return to the AccessStudio user interface. The captured task and the identified screens are displayed in the General Properties tab.

Important: Test all the AccessProfiles before uploading to IMS. For details, see the chapter about AccessProfiles for testing in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

9. Upload the AccessProfile to the IMS Server to activate it. In the Data type pane, right-click on the AccessProfile, and select **Upload to IMS**. Click **Yes** when the IMS Upload Confirmation displays. Another message box displays, indicating the success or failure of the upload.

Create an other task AccessProfile for Windows applications

Perform the following steps:

1. Follow steps 1 on page 91 - 6 on page 92 in the procedure “Create logon AccessProfile for Windows applications” on page 91.
2. Select **Other tasks** as the task to automate. Click **Next**.
3. Enter a unique name for the other task screen to capture.
4. Based on your selected task, capture identification information for the fields on the application screen:
   a. Click the **Finder tool**, drag to the corresponding fields on the application screen. As you drag the **Finder tool** to the application, AccessProfile Generator marks the field or button that can be captured.
   b. When the **Finder tool** is positioned over the field, release the mouse button. If a field was captured successfully, the Clear signature option is activated.
   c. The default screen name from the application is retrieved. Click **Clear signature** to undo the capture.
   d. Click **Advanced Settings** to perform the task only when a certain condition is satisfied. For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.
5. Click **Next**.
6. Specify actions for the task. Select from the drop-down list of available actions. Refer to Creating AccessProfiles that perform automation tasks on page 36 in the *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956 for details. Click **Add**.
7. Click **Next**.
8. Identify the task automation screen. Select the screen you have captured from the Screens Identified field.
   – To edit the previously captured screen, select the screen and click **Next**.
   – To remove the previously captured screen, select the screen title in the list box and click **Delete**.

9. Click **Finish** to return to the AccessStudio user interface. The captured task and the identified screens are displayed in the General Properties tab.

> **Important:** Test all AccessProfiles before uploading to the IMS Server. For details, see AccessProfiles testing in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

10. Upload the AccessProfile to the IMS Server to activate it. In the Data type pane, right-click on the AccessProfile, and select **Upload to IMS**. Click **Yes** when the IMS Upload Confirmation displays. Another message box displays, indicating the success or failure of the upload

3.2.2 Advanced AccessProfiles

Advanced AccessProfiles, also known as *State Engine SSO Support*, automates operations based on various conditions. Use advanced AccessProfiles for complex logon situations, such as verification of conditions before automatic logon, greater control over what triggers an action, and the sequence of these actions.

Advanced AccessProfiles are based on a state engine, which models functions (logging in to an application, changing passwords, and so on) as a sequence of steps represented by states and transitions, shown in Figure 3-6 on page 102. A state machine also consists of triggers and actions. The AccessProfile models these sequences, leveraging its ability to monitor and interpret events on a user's desktop. For more information, see the following sections:

- "State" on page 104
- "Trigger" on page 104
- "Action" on page 105

To work with advanced AccessProfiles, be familar with the concept of "Account data" on page 106 and *"Managing authentication services" on page 107*.

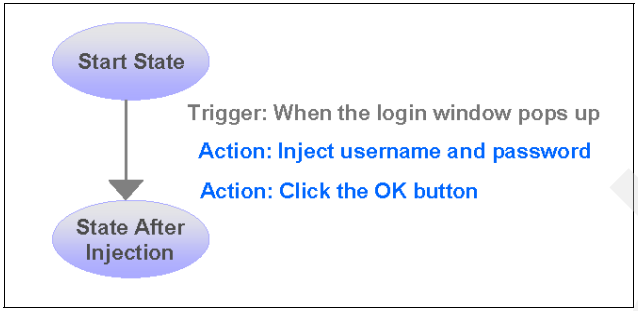

Figure 3-6 State machine flow

Most elements recognized by AccessProfiles are part of a hierarchical structure. The positioning of the element in the hierarchy, and the properties of the element itself are used by signatures to correctly identity the element.

For example, you can specify an edit control in a login window by writing a signature that refers o the control's properties (for example, control id) and also the property of its parent login window (for example, title).

Signatures

A *signature* is the construct used to uniquely identity an application (*site signature*) and component on a user interface. A visual example of components is represented by the blue arrows in Figure 3-7 on page 103.

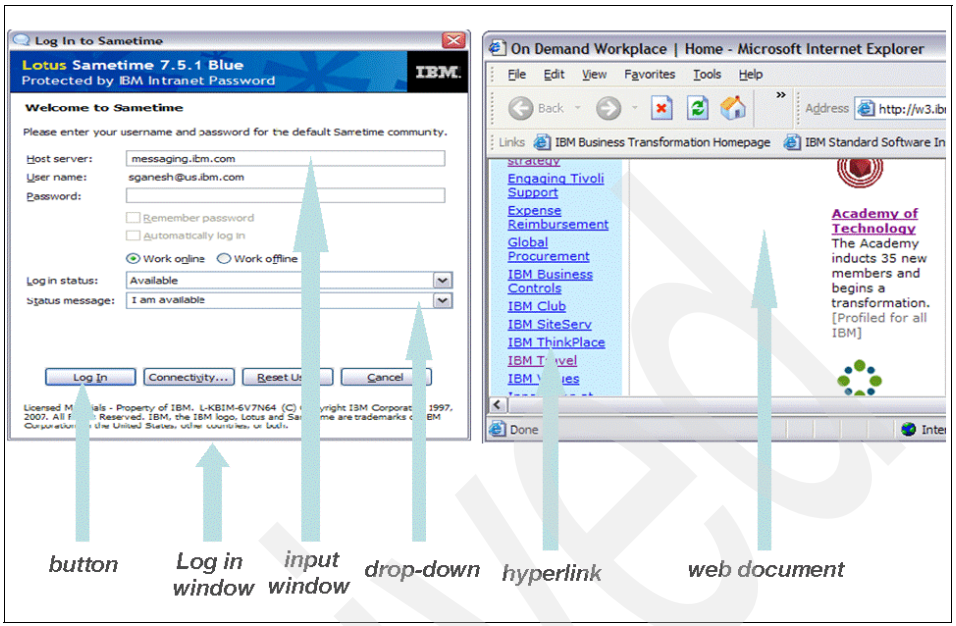

Figure 3-7 Signature: a visual example of components

Signatures contain XPath (XML Path Language), which is a language that facilitates XML document navigation to select elements and attributes. Signatures in AccessProfiles can identify the following items, listed here with examples and description:

- Executables

  `/child::exe[@exe_name="companypager.exe"]`

  The example matches `.exe` files with the name `companypager.exe`.

- Window elements (such as: edit control, buttons, and check box)

  `/child::wnd[@title="Login to CM"]/ child::wnd[@class_name#".*BUTTON.*"]`

  This example matches windows that have the title `Login to CM` and selects the descendant windows with the class name matching the regx `.*BUTTON.*` (where # is for a case-insensitive match).

- Web pages

  `/child::web[@domain="www.companymail.com" and @protocol=" http"]`

  This example matches Web pages from the URL that has a domain equal to `www.companymail.com` and protocol equal to `http`.

- HTML elements (such as: submit buttons, input controls, and so on)

  ```
  /descendent::html[@tag_name="form" and @name=""]/
  descendent::html[@tag_name="input" and @name="Passwd" and @type="password"]
  ```

  The first `html` refers to the head or the body. After that, a form descendant is found, and then a descendant of that form (of tag-name input and type password) is searched for.

- Java window elements (such as: title, class name, window position, visibility status, size, and so on)

  ```
  /child::jwnd[@title="Login" and @class_name="MyJFrame"]
  ```

  This example matches windows with title `Login` and class name `MyJFrame`.

These signatures can be edited in the AccessProfile Generator (for standard AccessProfiles), General Properties tab and XML Editor (for advanced AccessProfiles).

State

States represent specific situations where the state machine must look for certain triggers to occur (similar to a flowchart). In other words, a state indicates the current condition or status of an application (for example, signed-on status or signed-off status). You can define multiple states and associate triggers that cause a transition from one state to another. For a state transition, the following three steps happen for every state:

1. Each state has one or more triggers that are ordered.
2. An incoming event is matched with each of the triggers in order.
3. Trigger that matched indicates which state to move to.

Providing triggers that point to the same state is also possible. For example, in the *after_application_launched* state, you can look for the login window to appear or for a change password window to appear.

Each state is identified by a user-defined unique ID. You must define a start state to execute the state's transitions.

Trigger

A *trigger* is an event (appearance of window, button click, appearance of some text on an emulator screen, loading of a sign on Web page) that causes transitions between states in a state engine. When a trigger fires, it executes a set of actions defined by the administrator, and then causes transition to the next indicated state.

A trigger is required for monitoring an event on a specific construct (for example, window, button, Web page, text appearing on an emulator screen). *One trigger monitors one event type for one construct identified by a signature.* If you want to monitor events on multiple constructs, you would require those many triggers. Also, if you want to monitor different events, you must have one trigger for each event you want to monitor. A trigger match is successful when the construct it is waiting for receives that event, represented by the trigger *and* when the conditions (if any) attached to the trigger are all *true*.

Note: The only way you can transition from one state to another is when the conditions that the trigger is waiting to match are true.

AccessStudio contains predefined triggers. For a list, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

Note: AccessStudio enables customization through its VBScript and JScript plug-ins. You can customize triggers and actions if you have unique requirements. You can use VBScript and JScript in AccessStudio to create custom triggers and actions. These plug-ins are able to interact with AccessAgent and target applications.

Action

An *action* is the process performed in response to a trigger such as when the software automatically fills in the user name and password details when the logon window displays. When a trigger fires, the actions specified for that particular trigger are executed in a predefined sequence.

AccessStudio contains predefined actions that can be used to perform a set of operations in the application.

The following example describes the interaction between states, triggers, and actions:

1. The messaging software launches in the Start state.
2. The opening of the logon window fires a trigger followed by the action that automatically fills in the logon information.
3. The messenger comes to the state that is defined in the engine (after the auto fill state).
4. When the user clicks **Sign in**, a trigger is activated. The action to capture the user name and password information occurs.

5. The messenger moves to the after-capture-state.
6. A trigger is activated when the logon window displays the contacts list, and an action to save this user name and password information occurs.

The messenger returns to the Start state. See Figure 3-8

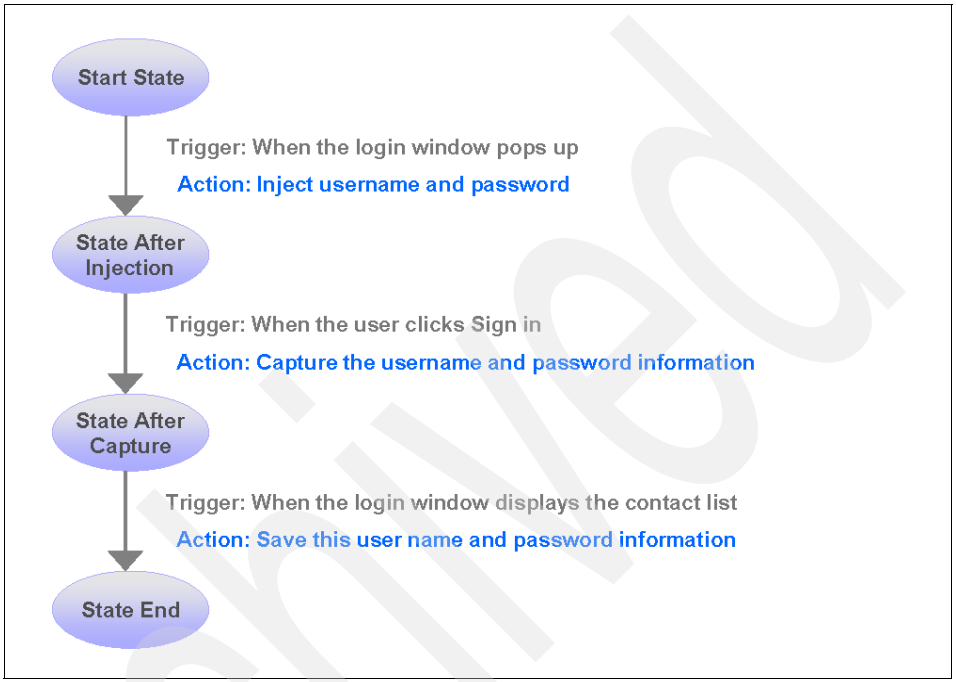

Figure 3-8 Example interaction between states, triggers, and actions

For a list of predefined AccessStudio actions, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

Note: AccessStudio enables customization through its VBScript and JScript plug-ins. You can customize triggers and actions if you have unique requirements. You can use VBScript and JScript in AccessStudio to create custom triggers and actions. These plug-ins are able to interact with AccessAgent and target applications.

Account data

Account data is the logon information required for verification against an authentication service. The account data usually refers to the user name, password, and the authentication service that stores the logon information.

AccessStudio stores the account data in a specific format known as *account data templates*. Account data templates provide information about the captured data (for example, which fields are key fields, case-sensitive, and which fields must be hidden).

Note: An account data template defines whether the field entry is:

- A secret field that requires encryption
- Case-sensitive

AccessStudio defines a set of account data template IDs. Each ID represents a particular type of account data.

A set of account data template IDs is defined in AccessStudio with each ID representing a particular type of account data. For example, the most commonly used ID (adtid_ciuser_cspwd) can be specified for applications that have one case-insensitive user name and one case-sensitive password. For more information, refer to the information about account data items and templates in *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

For company applications, the account data contains the authentication service ID (which is a user-specified name for the company authentication service), the user name, the encrypted password, and the account data template ID. The account data template ID declares that the user name field is a key field and that it is case-insensitive and is not a secret. Similarly, for the password field, the account data template specifies that it is not a key field, that it is case-sensitive, and that it is a secret (and therefore requires encryption).

A *key field* is a portion of a record that is used (possibly with other key fields) to locate a data record in a key file.

Managing authentication services

Most applications require validation of logon information by a verification entity. In AccessStudio, a reference is created to these entities through authentication services. AccessProfiles associated with the same authentication service belongs to the same verification entity. Changes made to the logon information in one AccessProfile are reflected across all others associated with the authentication service.

At a minimum, you have to provide an ID and a display name for the authentication service. Additional information are specified depending on your requirements.

Authentication services can be associated with AccessProfiles in two ways: directly and indirectly.

- Direct auth-info:

  Direct auth-info is a direct reference to an existing authentication service configured using the authentication services function in AccessStudio.

- Indirect auth-info:

  An indirect auth-info is used when you do not know which authentication service to select at the time of creating an AccessProfile. It is an indirect reference to an existing authentication service.

Associating AccessProfiles with independent authentication services is usually sufficient. However, there are rare cases where even the user interface of an application cannot identify the authentication service. In such cases, you can create an *authentication service group*, and associate multiple authentication services with this group. The authentication group link specifies which authentication service belongs to what group.

For more detailed information about managing authentication services refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On AccessStudio Guide Version 8.0.1*, SC23-9956.

Account data bag

The process of collecting the credentials is termed as *capture*. The process of actually storing the collected credentials (capture) to the user's Tivoli Access Manager for Enterprise Single Sign-On Wallet is termed as *save*. For capture, you should know about the following details:

- Account data template
- Authentication service (auth info)
- Account data bag (identified by an ID)

The account data bag is a container for account data and authentication identified by a name. The content of the credential (account data) that contains the account data items, and authentication service information is contained in a virtual bag identified by an identifier. The account data bag is analogous to a property ID value pair, where the value is not a string but the entire *account data object and authentication service blob*.

The idea of capture is to fill the bag with the value for account data items and authentication service. After you fill the bag with the values, the bag is ready to be saved to the Wallet.

Note: The value of key fields and auth info *cannot* be empty.

Two types of account data bags exist:

- Local bag

  A local bag is generated by default and only exists within the life of the application.

- Global bag

  A global bag can be accessible even after the application is closed and by other application.

3.3 Web Workplace

The Web Workplace component provides a Web-based interface that enables the user to log on to enterprise Web applications by simply clicking on links, without having to remember the passwords for individual applications. Users can also access applications hosted on Citrix MetaFrame or Terminal Servers through the Web Workplace without further logins. Web Workplace is especially useful when you cannot install AccessAgent (for example, users who have to access enterprise applications through SSL VPN from home computers or cyber cafes). It can be integrated with the existing portal. This feature allows users to perform automatic sign-on to a Web application through Web Workplace from a link in the enterprise portal. To securely implement this functionality, you should use SSL VPN connections.

Similar to signing up through AccessAgent, users have to authenticate themselves by providing their enterprise directory password (for example, Active Directory password) first, then specify the password and secret. Users can also specify more secret questions and answers, which can be used by the self-service feature for password resets.

You can also enable two-factor authentication for Web Workplace, which requires you to provide either of the following to log on, in addition to your password:

- Authorization code issued by the Help desk officer.
- Mobile active code (MAC), which can be sent to user via mobile phone or e-mail.
- One-time password (OTP) provided by an OTP token (for example, VASCO Digipass).

For each user, the same Wallet can be accessed through AccessAgent, AccessAssistant, or Web Workplace. The contents are fully synchronized across the user interfaces. System, machine, and user policies are all configured through AccessAdmin, enabling administrators to more easily configure all user interfaces from one central console.

Note: For more information about all the policies relevant to AccessAssistant and Web Workplace using AccessAdmin, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952

An administrator can author and manage Web AccessProfiles from AccessAssistant or Web Workplace.

The following additional options are available for administrators:

- Manage AccessProfiles

  Use this profile to view, add, modify, or test Web AccessProfiles.

- Synchronize system data with IMS Server:

  Use to synchronize AccessProfiles and system policies with the IMS Server.

4

Configuration

In this chapter, we discuss various configuration and customization tasks that are optional or mandatory after the installation and initial configuration of the Tivoli Access Manager for Enterprise Single Sign-On environment. Depending on your particular implementation, various configuration steps can be performed, including enabling strong authentication with a USB Key, OTP token, mobile active code (MAC), RFID, fingerprint reader, and so on.

Depending on your environment, various user, machine, and system policies can be implemented. Besides AccessAgent, Tivoli Access Manager for Enterprise Single Sign-On supports secure remote access that provides browser-based single sign-on to all applications (for example, traditional, desktop, and Web) from outside the company firewall.

These configuration tasks and other advanced configurations and concepts are discussed in this chapter, along with auditing and reporting features.

4.1 IMS configuration steps after installation

After a new installation, the IMS Server uses the base connector for Tivoli Access Manager for Enterprise Single Sign-On user validation. Any user can sign up as a new Tivoli Access Manager for Enterprise Single Sign-On user without providing validation credentials.

To use Active Directory or other enterprise authentication services to validate users during sign up, configure the authentication service for user validation. After you have installed the IMS Server you select Setup Assistant from the IMS Configuration Utility. This step also provisions an initial administrator account. The initial administrator account is then subsequently used for logging on AccessAdmin. This step should be complete before the IMS Server becomes available for users to sign up.

Now, you may add or delete policy templates with the system, machine, or user scope.

Note: Specifying information or settings using the IMS Configuration Utility involves manipulating the configuration file (`ims.xml`). Because the IMS Server loads the configuration keys on startup, it is necessary to restart the IMS Server after any configuration is done through the Configuration Utility, so that the changes can take effect.

4.2 Enterprise directory

An enterprise can have numerous applications deployed throughout their network with as many directories to hold user accounts. An infrastructure of that complexity causes difficulty in controlling audits, enforcing policies, and de-provision at the enterprise level. All of these tasks are possible if the enterprise has a single point for collating user accounts. An enterprise must identify which applications are considered enterprise applications.

Enterprise applications are specific to the business of an enterprise and controlled by an administrator, for example, Microsoft Windows, Lotus Notes, Active Directory, SAP®, PeopleSoft®, and Oracle.

One of the enterprise applications is used for *enterprise identity binding*. This application is required to verify the identities of users who log on to their Wallet. It also allows for linking the IMS Server with the directory that the enterprise uses to manage their users.

For example, an enterprise has identified Active Directory for enterprise identity binding as all user account information is stored in Active Directory.

When users register their USB Keys for the first time, they must enter their user name and password for Windows. The IMS Server verifies the identities of users by checking with Active Directory. After the server receives confirmation, the users can proceed with the registration. This process is possible because certain configurations were made during the installation of the IMS Server, allowing it to communicate with the enterprise's Active Directory.

Currently, the IMS Server supports the following types of enterprise directories:

- Active Directory
- LDAP directories

The integration of organization directories

An organization directory is an entity that validates user credentials for Tivoli Access Manager for Enterprise Single Sign-On users. It can be used for validating users during sign-up and also during logon, if the password is set up to synchronize with the enterprise directory password. In short, it can be a directory of user accounts that define Tivoli Access Manager for Enterprise Single Sign-On users. An example for an enterprise directory can be an Active Directory forest, as depicted in Figure 4-1.

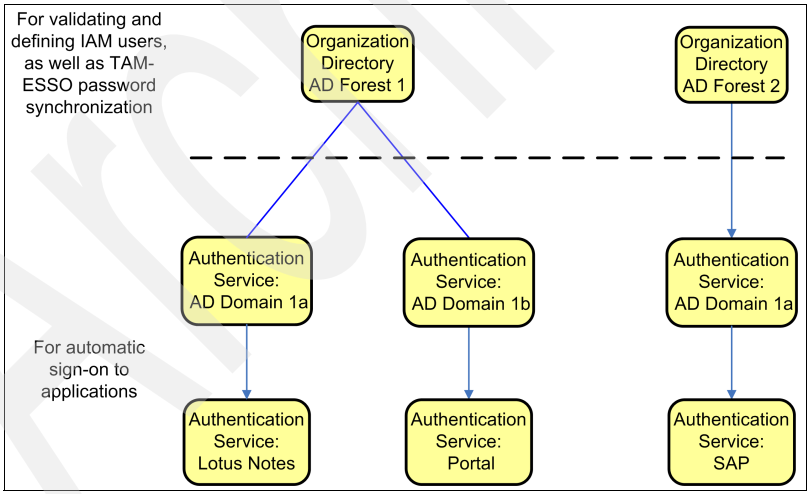

Figure 4-1 Organization directory integration

An organization directory may contain several authentication services, or none at all. An Active Directory forest with multiple domains can be an enterprise directory that contains multiple authentication services, with each authentication

service representing one domain. Such a definition, coupled with the password synchronization feature, allows enterprise directory passwords to be used for both logon to the Tivoli Access Manager for Enterprise Single Sign-On Wallet and automatic sign-on to applications.

Use of existing user registries

Tivoli Access Manager for Enterprise Single Sign-On uses existing user registries (for example, Microsoft Active Directory or IBM Tivoli Directory Server) to identify and validate a user when they register or sign up.

Note: Currently, only one enterprise directory is allowed for validating Tivoli Access Manager for Enterprise Single Sign-On users.

After this step, it creates an account for this user in its own user repository (stored on the IMS database), and thereafter only this database is consulted during runtime when the user accesses the Tivoli Access Manager for Enterprise Single Sign-On functions. Additionally, user accounts can be provisioned into Tivoli Access Manager for Enterprise Single Sign-On using user provisioning products such as Tivoli Identity Manager as described in 4.3, “IMS Provisioning Bridge” on page 115.

For deployments where the IMS Server is configured to use Microsoft Active Directory as its user repository, Tivoli Access Manager for Enterprise Single Sign-On can be configured to perform password synchronization with Active Directory. In this configuration, users can always log on to the AccessAgent with their latest Active Directory credentials; if this Active Directory password is reset out-of-band, the AccessAgent and IMS Server will verify the new Active Directory password against the Active Directory server, and re-sync the Tivoli Access Manager for Enterprise Single Sign-On password to this new value.

Additionally, for Active Directory deployments, the IMS Server can look up the directory for attributes of Windows workstations joined to the domain, and use these attributes to select a machine group policy template to apply onto the machine.

To facilitate validating of user credentials and searching for users and their attributes, the credentials of a lookup-user are stored on the IMS Server. The lookup-user is a valid domain user but does not have to have administrator rights. The password for this account should not expire.

For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951

4.3 IMS Provisioning Bridge

The Tivoli Access Manager for Enterprise Single Sign-On *Provisioning Bridge* extends the benefits generated by Tivoli Access Manager for Enterprise Single Sign-On through the automation of the credential distribution process. The *provisioning bridge* automates the user credential distribution process by using its API libraries (SOAP interface) to allow identity management solutions such as Tivoli Identity Manager to provision and remove user involvement in the credential provisioning and management process. It enables end-to-end identity life cycle management. New employees, partners, or contractors get fast and easy access to corporate information upon being provisioned. An administrator can automatically provision Tivoli Access Manager for Enterprise Single Sign-On with a user's ID and password by using an external provisioning system. An administrator is able to *add*, *modify*, and *delete* IDs and passwords for particular applications within the provisioning system and have the changes reflected in Tivoli Access Manager for Enterprise Single Sign-On.

From the provisioning system, all user names and passwords in Tivoli Access Manager for Enterprise Single Sign-On can also be deleted so that a user's access to all protected applications is revoked. Figure 4-2 illustrates the provisioning bridge architecture.

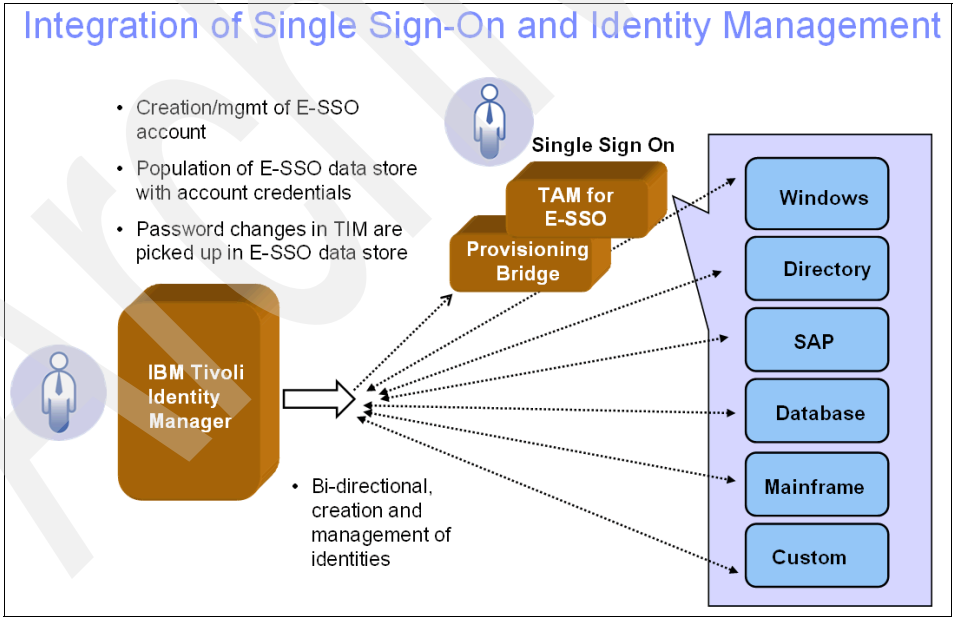

Figure 4-2 Provisioning bridge architecture

In most organizations, 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 the Tivoli Access Manager for Enterprise Single Sign-On provisioning bridge, application credential provisioning and de-provisioning between the identity management system such as Tivoli Identity Manager and Tivoli Access Manager for Enterprise Single Sign-On are automated. Consequently, organizations no longer have to physically distribute credentials to 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 the identity management system such as Tivoli Identity Manager. Users can enjoy single sign-on from day one and are no longer responsible for keeping track of their own application credentials, while helping to maximize security. When users no longer need access to systems, the integration between the Tivoli applications enables Tivoli Identity Manager to remove or revoke the users' systems and application access and also delete their credentials automatically 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.

Note: In this context, a best practice is to always *revoke* a Tivoli Access Manager for Enterprise Single Sign-On account instead of *deleting* it. The reason for this is to keep the audit log information available for later audits. After a Tivoli Access Manager for Enterprise Single Sign-On account has been revoked, it cannot be re-activated.

By integrating with an identity management system users never have to know their user name or password for their applications because it can be managed transparently to them.

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

Furthermore, the Tivoli Access Manager for Enterprise Single Sign-On provisioning bridge 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. The provisioning bridge 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.

The provisioning bridge offers a Java interface to the identity provisioning system to communicate with the IMS Server. If using the Java interface is not possible, a Tivoli Access Manager for Enterprise Single Sign-On IMS Bridge that communicates directly with the IMS Server using SOAP will have to be developed for the identity provisioning system.

Communications between the identity provisioning system and the IMS Server are done using Simple Object Access Protocol (SOAP) over HTTPS using one-way SSL. When the identity provisioning system provisions new users or new accounts for a user application, resets application passwords for users, de-provisions an enterprise user or an application account, it makes appropriate SOAP calls to the IMS Server with relevant account data information.

The provisioning bridge is configured with a simple XLM file. For the IMS Bridge configuration file parameter descriptions (Java Provisioning API), refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Integration Guide Version 8.0.1*, SC23-9957

4.4 Provisioning Agent

The Provisioning Agent is an application that monitors an Active Directory periodically for deletion of users to trigger a corresponding deletion or evocation of the user's account or Wallet on the IMS Server. This application is intended for deployments in which a user provisioning system (like Tivoli Identity Manager) is not deployed, because it helps save the administrator from having to separately revoke a user's Tivoli Access Manager for Enterprise Single Sign-On account when the administrator deletes the user from Active Directory. Typically, the

Active Directory management console is used for user management, to set user attributes, disable accounts, and de-provision accounts.

Note: No policy settings are required for the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent.

However, after deploying Tivoli Access Manager for Enterprise Single Sign-On, the organization potentially has to manage users from the IMS Server's administrative user interface (AccessAdmin), because the IMS Server manages the users' Wallets containing all application credentials, audit logs, and policies.

Note: The Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent can support up to a maximum number of 2,000 users. Performance tests should be done before deploying it for more than 2,000 users.

The IMS Server can be configured as the central administration server so that when an IMS user is de-provisioned using the AccessAdmin interface, the IMS Server can delete the user's Active Directory account from Active Directory using a connector. However, many organizations might not want to change their existing business and help desk processes of de-provisioning users through the Active Directory management console. In such cases, the Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent can be used. With the Provisioning Agent, the administrator or help desk employee can de-provision users from the Active Directory management console. The Provisioning Agent then automatically de-provisions the corresponding IMS users from the IMS Server.

Note: Although the component is named *Provisioning Agent*, it can only de-provision IMS users when the users have been de-provisioned in Active Directory. If necessary, other provisioning features can be added in the future.

Currently, the product only supports the de-provisioning of an IMS user when the Active Directory account is de-provisioned.

The administrator or help desk employee can de-provision a user from the Active Directory management console, as follows:

1. In the Active Directory management console, de-provision the user.
2. The Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent detects (through periodic polling) that a user has been de-provisioned on Active Directory.

3. The Provisioning Agent invokes the IMS Server's provisioning API to de-provision the IMS user.
4. The user's authentication factors are automatically revoked.
5. During the user's next logon attempt through AccessAgent, the user is informed that the account has been revoked.

Note: The Provisioning Agent polls Active Directory or Active Directory Application Mode (ADAM) periodically for recently de-provisioned users and performs the de-provisioning actions on the IMS Server accordingly. This implies that the de-provisioning of IMS users might not happen immediately after an Active Directory user is de-provisioned.

A good practice is to install the Provisioning Agent on the same machine as the Active Directory Application Mode (ADAM). In that case, the search functions are faster as ADAM has its own cached copy of the user directory. However, the Provisioning Agent can also be configured to directly communicate with Active Directory.

An organization might have deployed one or more ADAMs. If multiple ADAMs are supporting multiple domains, each ADAM machine would host one Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent.

When you install the Provisioning Agent, an IMS Server must already be installed and configured. Before you begin installation:

1. Set up a new IMS Bridge by using the IMS Configuration Utility (IMS Bridges Configure) on the IMS Server that will connect to the Provisioning Agent:
   - Specify the IP address (IMS Bridge IP Addresses) of the machine where the Provisioning Agent will be installed.
   - Create a new user name (Name) and password (IMS Bridge password) for the IMS Bridge. These will be used later in the Provisioning Agent configuration.
2. Extract the distributable archive to a directory (for example, `C:\Encentuate`), making sure to maintain the directory structure in the archive.
3. The Provisioning Agent uses one-way SSL to communicate with the IMS Server. This means that the IMS Server SSL certificate must be trusted by importing it into a trust store. The trust store can either be a pre-existing store that is used by other applications, or it can be the trust store provided in `config\truststore.jks`. To import the Base-64 certificate to a trust store, use the Java `keytool.exe` command line tool.

4.5 Remote Access Integration solution

The Tivoli Access Manager for Enterprise Single Sign-On *Remote Access Integration* provides browser-based single sign-on to all applications (for example, traditional, desktop, and Web) from outside the firewall. Organizations can effectively and quickly enable secure remote access combined with two-factor authentication for their mobile workforce without installing any desktop software or modifying application servers.

Users can access the Web, desktop, and traditional applications using an SSL VPN appliance and ensure two-factor authentication through the use of a one-time Tivoli Access Manager for Enterprise Single Sign-On mobile active code (MAC) password delivered to smartphones, PDAs, pagers, fax, or other mobile devices. Organizations can also leverage Tivoli Access Manager for Enterprise Single Sign-On to provide single sign-on functionality to applications that are accessible over an SSL VPN appliance.

Organizations can enable secure remote access for their mobile workforce with the highest levels of security, without the inconvenience and cost of implementing and administering separate authentication tokens. Users can leverage existing personal devices to secure access to corporate networks without extensive training.

The Tivoli Access Manager for Enterprise Single Sign-On Remote Access Integration provides the following benefits:

- Easy to use

  Users can leverage existing devices (for example, smartphones, PDAs, or pagers) to ensure two-factor authentication and secure remote access to corporate networks over an SSL VPN appliance.

- No extra tokens to manage

  Users can leverage their e-mail and personal mobile devices. No tokens to deploy, replace, or administer.

- Convenience of multiple channels

  Users can choose to receive OTPs over a channel of their choice: mobile phone, e-mail, or fax.

- Easy secure remote access from anywhere

  Users receive highly-secure transparent access to all network resources from any network environment or device.

- Easy remote access control

  Managers can set up and deploy a single secure access gateway for all users, internal and external, to all network resources with full control.

- Security of one time passwords

  All one-time passwords are generated upon successful verification of a user's identity. The passwords expire after a preset period or upon usage.

- No installation of client software

  No need to install client software.

- Extensible, scalable solution

  The solution can be extended to support other identity and access management features, such as single sign-on and user provisioning.

4.6 AccessAgent for Citrix

Citrix MetaFrame provides a thin-client architecture to run and manage applications centrally on Windows 2000 or 2003 Server.

Tivoli Access Manager for Enterprise Single Sign-On can integrate the AccessAgent with the Citrix MetaFrame product suite to provide sign-on automation to applications running on Citrix servers. In the integrated solution, AccessAgent runs within a Citrix MetaFrame session remotely on the Citrix MetaFrame server, and provides auto-capture and auto-fill of passwords. The remote AccessAgent runs on the Citrix server, independent of whether a local AccessAgent is running on the user's workstation. Both the local and remote versions of AccessAgent synchronize credentials directly with the IMS Server.

For older installations of the Citrix MetaFrame Server, turn on password encryption so that clear text passwords will not be sent over the ICA channel. By default, newer installations of the Citrix MetaFrame Server already have password encryption enabled.

AccessAgent uses an IMS client certificate for authentication when connecting to the IMS Server. That certificate is stored in a USB Key.

Install AccessAgent on each Windows Terminal Server or Citrix, if used in the Remote Access Integration deployment.

Standard AccessAgent can be installed on the Citrix client. The installer automatically installs the Citrix related components and configures certain Citrix settings, if the computer has a Citrix client (for example, ICA client) installed.

To allow AccessAgent to run on the Citrix or Terminal Server that your system supports, you have to configure your IMS Server settings. Use the Setup Assistant (AccessAdmin) to mark the *Enable AccessAgent for Citrix or Terminal Server* check box.

For more information, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

4.7 User role assignment

By default, all new users are assigned *user* roles. To re-assign roles to either help desk personnel or an administrator, you have to use either the AccessAdmin or IMS Configuration Utility, depending on the number of users to be re-assigned at that certain time.

To re-assign one user at a time, usually from a user role to a help desk role, use AccessAdmin and refer to 4.7.1, “Re-assigning roles for help desk users” on page 122.

To reassign multiple users at a time, use the IMS Configuration Utility and refer to 4.7.2, “Automatic role assignment for large deployments” on page 123.

4.7.1 Re-assigning roles for help desk users

Use AccessAdmin to change the role of the user. By default, when users sign up, all users are automatically assigned the role *user*, except for those who have been predefined as administrators during IMS Server installation. Administrators are automatically assigned the *administrator* role during sign-up.

Using AccessAdmin, a user can be assigned to a help desk role manually. However, it becomes tedious if the administrator must reassign hundreds of users. Therefore, an automatic role assignment feature must be provided.

You can assign one or more existing help desk employees to a policy template. However, the problem arises when a new help desk user signs up, and this new person must be added to the template manually.

If each new help desk user is allowed to manage all users, enable the feature for automatic assignment of all policy templates and users to the new help desk user by selecting: **AccessAdmin** → **User Attributes** → **Automatic assignment of all policy templates and users to new Help desk user**.

4.7.2 Automatic role assignment for large deployments

For larger deployments, if a large number of help desk users and administrators exist, manually assigning roles to them through AccessAdmin might be too tedious. An Active Directory attribute can be used to distinguish between users, help desk personnel, and administrators.

The automatic role assignment feature in Tivoli Access Manager for Enterprise Single Sign-On allows users to assign the appropriate roles (for example, user, help desk, administrator) automatically during sign up, based on a particular Active Directory attribute.

Consider the following information about the automatic role assignment feature:

- Automatic role assignment does not apply to existing users.

  Automatic role assignment is used only when a user signs up or is provisioned. It does not apply to existing Tivoli Access Manager for Enterprise Single Sign-On users. The roles of existing users will not change when the automatic role assignment configuration is modified, or when a user's Active Directory attribute for role assignment is modified.

- The Active Directory attribute for role assignment must not be nested.

  Certain Active Directory attributes may be nested. For example, the *memberOf* attribute specifies a user's direct Active Directory group membership. However, because groups can be members of other groups, this nested relationship among groups also applies to users. In the current implementation, the IMS Server does not traverse the nested relationship among groups, and cannot properly handle Active Directory attributes (for example, memberOf). If memberOf is used, users must be *direct members* of the groups to be used for role assignment.

- The automatic assignment of existing policy templates and users to new help desk user is limited to either of these listed settings:
  - The *Enabled* setting assigns all existing policy templates and users to a new help desk user. The assumption is that each help desk user should be allowed to manage all Tivoli Access Manager for Enterprise Single Sign-On users.
  - The *Disabled* setting does not assign any policy template or user to a new help desk user. The administrator must manually assign the appropriate policy templates and users to each new help desk user.

The role assignment feature must be enabled using the IMS Configuration Utility, as follows:

1. Launch the IMS Configuration Utility.
2. Ensure that the automatic role assignment bind task is in the bind task list (select **IMS Server** → **Miscellaneous** → **Application Binding Tasks**).
3. Specify the Active Directory attribute for automatic role assignment (select **AccessAdmin** → **User Attributes** → **Role assignment attribute**).

   Note: The usual Active Directory attributes that may be used are *memberOf, title, description*, and *department*. The Active Directory attribute for role assignment can be multi-valued (for example, *memberOf*). For multi-valued Active Directory attributes, all the values are considered. An attribute search will be treated as a match, if one of the values matches what is configured for the role assignment.

4. Define the mapping between Active Directory attribute values and roles (select **AccessAdmin** → **User Attributes** → **Role assignment mapping**).

Note: Users in the list of predefined administrators (defined during IMS Server installation) are assigned the administrator role regardless of their Active Directory attribute value for automatic role assignment.

4.8 Managing policies

Tivoli Access Manager for Enterprise Single Sign-On uses policies to control the behavior of its components. These policies are configurable through various means, so Tivoli Access Manager for Enterprise Single Sign-On can meet specific organizational requirements. Policies have different visibilities and scopes, and are managed by different roles.

Policies can be applicable system-wide, or only to certain groups of users or machines. The applicability of a policy is determined by its scope, which can be system, user, or machine:

- The *system* policy is system-wide.
- The *user* policy affects only a specific user.
- The *Machine* policy affects only a specific machine.

System, machine, and user policies are configured with AccessAdmin. Changes to these policies are propagated to clients the next time that AccessAgent synchronizes with the IMS Server (for example, usually in 30 minutes).

Note: Periodic synchronization intervals can be changed. The IMS Server policies only accept non-negative integers for time values.

The IMS applies machine policies to machines after they join the IMS Server, and which are then automatically synchronized with AccessAgent. Multiple machine policy templates can be defined in IMS; only one of these templates is set as the default.

Administrators have full control over policies, and users assigned to the help desk role have more limited control over policies. Refer to Table 4-1.

Table 4-1 Policies and their scopes

Policy type	Administrator permission	Help desk permission	Policy scope
System policies	Full read/write	Read only	System-wide
Machine policies	Full read/write	Read only	Machines
User policies	Full read/write	Full read/write	Users

System, machine, and user policies each have unique and overlapping policy parameters and therefore some groups of policies have overlapping scopes. For example, these policies have a system scope, but the range of entities that they affect is different:

- Wallet inject password entry option default policy

  (`pid_wallet_inject_pwd_entry_option_default`)

  This policy defines the default password entry option for all authentication services and applications.

- Authentication inject password entry option default policy

  (`pid_auth_inject_pwd_entry_option_default`)

  This policy defines the default password entry option for a specific authentication service.

- Application inject password entry option default policy

  (`pid_app_inject_pwd_entry_option_default`)

  This policy defines the default password entry option for a specific application.

A policy may be defined for different scopes. For example, the desktop inactivity policy may define the desktop inactivity time-out duration for one machine or for the entire system. If this policy is defined for both scopes, a priority is defined, in case the time-out value is different for the machine and for the entire system. In this case, use the `managepolicypriority.bat` command-line utility to manage policy priorities. For more information, refer to the discussion about setting policy priorities in *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

Policies are created and modified to enforce the rules set by the business. Prior to production deployment, you should have all of your policies clearly defined as direct translations of the business security requirements. Modifying policy after deployment might be unavoidable, but best effort should be made to define policies before deployment to production.

For more information about setting policies, refer to the discussion about policy management in *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

4.8.1 Policy template

A policy template is a set of predefined user or machine policies that can be applied to IMS users or machines.

AccessAdmin supports dynamic non-hierarchical groups, collapsible sections, and the setting of policies for groups and users. Attributes that define logical groups (for example, department) can be obtained directly from the corporate directory. When the user signs up or a machine joins the IMS Server, policies are initially assigned based on the attributes of the machine/user that match the policy template.

User groups are dynamic because membership depends on the user's policies. For example, a user may belong to the RFID user group if assigned with a *Password + RFID* authentication policy. By changing the authentication policy for the user to *USB Key*, the user becomes a member of the USB Key users group.

User policy modifications may be performed on each user or on groups of users. The user may belong to the group of USB Key users and the group of AccessAssistant users. Groups are based on search criteria, so the associations are virtual and overlapping.

User policy templates can be defined for specific groups of users to facilitate policy setting. For example, a template can be defined for the Finance

department. Any new user with a department attribute of Finance will have policies initialized with the template settings.

Machine policy templates are defined for each machine that joins the IMS Server. These policies are under `scope:machine(scp_machine)`, and keyed on the machine name. The machine policies are synchronized through incremental synchronization and based on the machine name.

Machines can be assigned to an existing machine policy template based on one or more of the following attributes:

- Host name
- IP address
- AccessAgent version
- Active Directory security group
- Machine Tag

System, machine, and user policies are configured with AccessAdmin. The two ways to log on to AccessAdmin are as follows:

- Go to the console of the machine where the IMS Server is installed, access `https://imsservername`, and a logon prompt is displayed.
- Log on to AccessAgent on any machine as an administrator, and then launch `https://imsservername`.

Note: If the IMS Server is accessed without using the fully-qualified domain name, AccessAgent cannot perform automatic logons to a search page.

User policies can also be modified for an entire group of users by using the Search Users feature. System policies may be defined for authentication services, applications, or a combination of authentication service and application.

The help desk role can be defined for different groups of users. The help desk user associated with a group can manage (for example, authorize and revoke) users only for that group. Help desk officers may manage overlapping groups of users.

Administrators can view, modify, create, and delete policy templates.

User policy template

The administrator can specify the policy templates to apply to users according to certain attributes. For example, if the administrator chooses department as the

attribute, IMS can apply a specific template to all users in the Engineering department, and another template to all users in the Sales department.

By default, the user attribute value is matched with the values specified in policy template assignments. Note that values are case-sensitive.

If the user attribute value does not have an exact match, IMS determines whether the suffix of the user attribute value matches any assignments. If the suffix of a user attribute value matches two or more assignments, IMS applies the first template that matches the user attribute value.

IMS automatically applies policy templates to users during sign-up. Each IMS can have several defined policy templates, but one policy template is set as the default policy template.

When a user signs up, IMS checks the user attributes and assigns the policy template. If no policy template matches the attributes of a new user, the default policy template is applied.

For unusual cases, where no policy template is defined in IMS, IMS will not set any user policies during sign-up.

A policy template can also be applied to a single user or to a group of users by using the user's or group's profile page in AccessAdmin.

Use AccessAdmin and the IMS Configuration Utility to assign policy templates to new users during sign-up, as follows:

1. Modify the IMS configuration file using the following entry:

   `encentuate.ims.ui.templateAsgAttribute`

   This enter is the name of the user attribute in the enterprise directory whose value determines the policy template for each user.

   Note: To configure the attribute using the IMS Configuration Utility:

   a. Go to **Advanced Settings** → **AccessAdmin** → **User Interface** → **Policy assignment attribute**.

   b. Restart IMS after modifying the configuration.

2. Configure the mapping between the user attribute values and the policy template names using AccessAdmin. Go to **AccessAdmin** → **User Policy Templates** → **Template assignments**.

Machine policy template

IMS automatically applies policy templates to machines after they join the IMS Server, which are then automatically synchronized with AccessAgent. Multiple machine policy templates can be defined in IMS. One of these templates is set as the default.

After a machine joins the IMS, IMS checks the machine's attributes against the specified criteria and assigns the matching machine policy template.

If the machine matches two or more machine policy templates, IMS assigns the first matching policy template from the list of templates. If no policy template matches the attributes of a new machine, the default machine policy template is applied.

If a policy within a machine policy template is modified, all machines assigned to the machine policy template will receive the new value. However, if the criteria for machine policy template assignments are changed, existing assignments of machines to machine policy templates does not change.

One way to group a machine is to use the MachineGroup registry setting in the `DeploymentOptions.reg` file. It allows machines to be grouped according to which machine policy templates should be assigned to the machines.

For example, if a deployment can be set up to use machine group tags, it will be possible to prepare different installation packages (for example, one for personal workstations, one for shared desktops, one for private desktops) and use the appropriate one to install on each workstation. It will also be possible to use WMI scripts to push out the machine group tag through AD GPO, so that machine policy templates can be assigned accordingly.

4.9 Usage workflows

Tivoli Access Manager for Enterprise Single Sign-On supports two main usage configurations for *personal workstations* and *shared workstations*.

The personal workstation configuration is used in typical enterprise setups where users are assigned their own workstations. A good practice is to use the USB Key as the authentication factor for these configurations.

The most prevalent shared workstation configuration can be found in health care organizations, where doctors and nurses use any shared workstation that is available in the room they are currently assigned to.

Such a usage scenario requires efficient switching of users on the shared workstation. Any other authentication factor other than the USB Key is suggested for the shared workstation configuration.

For both scenarios, Tivoli Access Manager for Enterprise Single Sign-On can be configured to allow users to log on or unlock a computer without password by using either a fingerprint or RFID authentication factor.

4.9.1 Personal workstation

The personal workstation configuration is more applicable for organizations where users are assigned their own workstations. The USB Key is the common authentication factor for this type of usage configuration. The setup procedure and workflow are the same, regardless of the selected authentication factor.

The user signs up from EnGINA, a desktop, or a locked computer at startup, and inserts the USB Key.

The user can also sign up without the USB Key and register later. Signing up without the USB Key allows the user to log on to AccessAgent subsequently with just a password, if it is set in the authentication policy.

To lock the computer, the user has to simply remove the USB Key. To unlock the computer, reinsert the USB Key.

For more information about managing workflows for personal workstations, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

4.9.2 Shared workstation configuration

The shared workstation configuration is for organizations where users share common workstations. In a working environment, such as in a hospital, doctors and nurses have to share computers. They usually move from one workstation to another for their work. This results in frequent *Switch User* tasks for each workstation. Ideally, the switching of users should be fast and easy so that precious time can be saved.

Tivoli Access Manager for Enterprise Single Sign-On supports fast user switching through the following desktop schemes:

- Shared desktops
- Private desktops
- Roaming desktops

Note: These schemes do not use the Windows XP Fast User Switching feature.

When selecting which shared desktop scheme to deploy, consider the following details:

- Customer requirements
- Customer budget
- Limitations of each scheme
- Supported applications
- Authentication factors

Shared desktops

Shared desktops allow multiple users to share a generic Windows desktop. Because each user does not have to log on to Windows, switching of users can be done quickly and efficiently. However, after switching from User A to User B, the applications contexts of User A are lost. When the workstation switches back to User A, the applications must be re-launched. For the scheme, AccessProfiles must be created to automatically log off enterprise applications when user switching occurs.

RFID is the authentication factor for this usage configuration.

Users can sign up from EnGINA, from their desktop, or from a locked computer. Users have to tap their RFID cards during sign up, but they can initially sign up without RFID cards, then register the RFID cards later when the cards are available. After completing the sign-up process, the user is then logged on to AccessAgent.

When a different user taps the RFID card, switching is invoked, either from the desktop or from the locked computer screen.

After the new user supplies a valid password, AccessAgent unlocks the computer (if locked), logs off the previous user, and then logs on the new user to the Wallet. If the user has logged on to other computers with the same *RFID + Password* in a set time range during the day, the user might not be required to enter a password.

For more information about workflows for shared desktops, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

Private desktops

Private desktops allow users to have their own Windows desktops in a workstation. The scheme uses the Local User Session Management feature of AccessAgent, which allows users to retain the existing user's desktop session during switching of users. When a User A returns to the workstation to unlock it, AccessAgent switches to User A's earlier desktop session, allowing User A to resume the previously incomplete or interrupted work. However, an existing desktop has to be logged off if the workstation runs out of resources (for example, memory) to accept a new user logon.

If the user logs on at another workstation, the user still has to restart the application.

To manage multiple desktops on a single workstation, the private desktop scheme uses the Local User Session Management (LUSM) feature of AccessAgent that uses a component called Tivoli Access Manager for Enterprise Single Sign-On Desktop Manager.

Logging on from the EnGINA welcome screen is not supported by Local User Session Management. Workstations have to be configured to automatically log on to a generic Windows account upon startup, and then lock the computer.

Note: The generic Windows account for Auto-Logon to the Windows machine must not be a registered Tivoli Access Manager for Enterprise Single Sign-On user. Use a local machine user account. The generic Windows account should also be given *interactive logon* rights so administrators can connect to the machine that is running private desktop by using the Remote Desktop Protocol (RDP).

All users log on to the workstation from the locked screen, for example, users tap their RFID cards during sign-up. They can also sign up without the RFID cards and register these later. After completing the sign-up process, the user is logged on to AccessAgent.

Note: AccessAgent is not logged on if you are using an auto-admin account.

When another user taps the RFID card to switch to another desktop, this user logs on (if the user does not have an existing invisible session) or unlocks the workstation (if the user has an existing invisible session).

The following Wallet authentication options are currently supported:

- Password
- RFID + password
- Active proximity badge + password
- Fingerprint

For more information about workflows for private desktops, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

Roaming desktops

Roaming desktops allow users' Windows desktops to *roam* to the users' points of access, from workstation to workstation. A user can disconnect from a desktop or application session at one client, log on to another client, and continue a desktop or application session at the new client. Roaming desktops give users the ability to access and preserve their desktops, regardless of which computer they use.

This scheme requires a Windows Terminal Server or Citrix MetaFrame Server, which is usually more costly to deploy. This setup is especially useful for a shared workstation environment where users roam from one workstation to another, depending on the user's current location.

For more information about workflows for roaming desktops, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

4.10 Thin client solution

Thin clients are becoming more common in hospitals. Administrators usually run applications on Terminal Servers (TS) or Citrix MetaFrame Servers. Thin clients are used as kiosk workstations. Users log on to TS or Citrix using thin clients.

However, thin clients do not have as much RAM or disk space as standard computers and software such as AccessAgent are usually not installed. Upgrading the software on a thin client is more difficult.

In hospitals, thin clients (WinCE or WinXPe) from vendors such as Neoware and Wyse are used as shared terminals. Because no local AccessAgent is running on the thin clients, the server-side AccessAgent has to detect and verify authenticators, such as RFID cards, fingerprints, and smart cards.

Supported thin clients for Tivoli Access Manager for Enterprise Single Sign-On include.

- Neoware and Wyse thin clients:
  - Microsoft Windows CE: 4.20
  - Microsoft Windows XP Embedded
  - RDP connections (to Windows 2003 Server and also RDP to Citrix server installed on Windows 2003 Server), and ICA connections (to Citrix MetaFrame Server on Windows 2003 Servers)
  - RFIDeas pcProx serial reader (model BSE-PCPRXH-232 connected to the thin client)

The thin client setup is related to roaming sessions. AccessAgent is integrated with the RDP client, Terminal Server, ICA client, and Citrix server to provide sign-on automation to applications running on Terminal Servers or Citrix servers. In the integrated solution, the AccessAgent runs remotely within a Windows session on the Terminal Server or Citrix server, and auto-captures and auto-fills passwords.

AccessAgent supports roaming session from thin clients by using an RFID card, as follows.

1. From a thin client, a shared desktop is automatically launched as an application through Citrix/Terminal Server. This shared desktop serves as the default shared desktop for users on a thin client. Use the thin client's Windows credentials to create the Windows session on Citrix/Terminal Server that hosts this desktop.

   Note: Assign a unique Windows user for each thin client.

2. Configure the shared desktop (using Windows logon script defined through AD GPO) to lock the screen immediately after logon to display EnGINA. The user can then tap the RFID card at the thin client and log on to AccessAgent in the shared desktop.
3. AccessAgent should automatically launch a Citrix/RDP session (user desktop) from the shared desktop through an AccessAgent logon script. AccessAgent in the shared desktop injects the user's own Windows credentials in the Citrix/RDP client. This user desktop can be hosted on the same or different Citrix/Terminal Server.

4. When the user finishes work on the user desktop, the user can lock the screen or log off AccessAgent on the shared desktop. AccessAgent can be configured to close the user desktop. The Citrix/RDP session hosting the user desktop is now disconnected.
5. The user can log on to a shared desktop at another thin client and reconnect to the disconnected Citrix/RDP session.

For more information about thin clients and roaming sessions, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

4.11 Using the IMS Configuration Utility

The IMS Configuration Utility is used to control the behavior of the IMS Server. The IMS Server configuration is different for every organization. The configuration is predetermined before full deployment takes place.

The IMS Configuration Utility provides professional services with a user interface for configuring the IMS configuration keys (in the following location:

```
<IMS Installation Folder>\ims\config\ims.xml
```

The IMS configuration keys are grouped according to complexity, either basic or advanced.

Basic settings refer to the settings that govern the general behavior of the IMS Server, such as the types of authentication services or connectors used, the housekeeping schedule, support for biometrics, and all settings related to ActiveCode deployment.

In the advanced settings section, you can modify configuration keys relating to the more advanced level of behavior of Tivoli Access Manager for Enterprise Single Sign-On, such as:

- AccessAdmin configurations (for example, change the User Interface by enabling the Delete user button in AccessAdmin)
- IMS Server configurations (for example, assigning user roles automatically based on a particular Active Directory attribute)
- Data source configurations (for example, modify the maximum database connection pool sizes and connection timeout values)
- Message connector configuration (for example, add SMPP Messaging Connector or add SMTP[1] Messaging Connector)

[1] Short Message Peer-to-Peer (SMPP); Simple Mail Transfer Protocol (SMTP)

- IMS bridge configuration (for example, specify the IP addresses from which the IMS Bridge can access the IMS Server).
- User authentication configuration (for example, specify whether authorization code authentication is allowed by the IMS Server).
- De-provisioning configuration (for example, setup automatic de-provisioning).

By default, the utility is installed on port 8080, and can only be accessed locally from the server console for security reasons (`http://<servername>:8080/`). It can be accessed from the Start Menu through **Start** → **All Programs** → **TAM E-SSO IMS Server** → **TAM E-SSO IMS Configuration Utility**. Unlike AccessAdmin, the utility does not authenticate users.

The IMS Configuration Utility is only available when the IMS Server is running. Because the IMS Server loads the configuration keys on startup, you must restart the IMS Server after any configuration is done through the utility, so that the configuration can take effect.

4.12 Using AccessAdmin

The IMS Server provides an administrative interface called AccessAdmin, which is consistent with the interface of AccessAgent. Different access rights are given to the administrator and help desk roles.

Logging on to AccessAdmin requires certificate authentication. The user must be logged on to a cached Wallet that has either an administrator or a help desk role. Certain configurations (for example, system policies and machine policies) can only be viewed but not modified by a help desk user.

As with the AccessAgent interface, AccessAdmin has a navigation panel for accessing various functions, such as:

- User search and administration (to modify user policies, issue authorization code, unlock a locked Wallet, revoke user, and so on)
- Machine search and maintaining machine policy templates
- Creating and maintaining policy templates (can only be created and maintained by the administrator, but help desk can view and apply)
- Setting system and application policies (can only be modified by the administrator, but help desk can view)
- Accessing logs and status information

From the IMS Server machine, you can log on to AccessAdmin by providing a user name and password, without installing AccessAgent. If required, use the

IMS Configuration Utility (select **Advanced Settings** → **AccessAdmin** → **Login** → **Allow form-based login to AccessAdmin from remote machine**) to allow user name and password login from any machine.

AccessAdmin supports dynamic non-hierarchical groups, collapsible sections, and the setting of policies for groups and users. Attributes that define logical groups (for example, department) can be obtained directly from the corporate directory. When the user signs up or a machine joins the IMS Server, policies are initially assigned based on the machine's/user's attributes that match the policy template.

Subsequently, user groups are dynamic because membership depends on the user's policies. For example, a user may belong to the group of RFID users because the authentication policy is *Password + RFID*. By changing the authentication policy for the user to *USB Key*, the user becomes a member of the group of USB Key users.

User policy modifications can be performed on individual users or on entire groups of users. A user may belong to the group of all USB Key users, and to the group of all AccessAssistant users. Because groups are based on search criteria, they are virtual and they overlap.

User policy templates can be defined for specific groups of users to facilitate policy setting. For example, a template can be defined for the Finance department. Any new user whose department attribute is Finance will have the policies initialized with the template settings.

Machine policy templates are defined for each machine that joins the IMS Server. These policies are under `scope:machine(scp_machine)`, and keyed on the machine name. The machine policies are synchronized incrementally based on the machine name.

Machines can be assigned to an existing machine policy template based on one or all of the following attributes:

- Host name
- IP address
- AccessAgent version
- Active Directory security group
- Machine tag

All policies with system, machine, or user scope can be modified through AccessAdmin. User policies can also be modified for an entire group of users by using the Search Users feature. System policies may be defined for

authentication services, applications, or a combination of an authentication service and application.

The help desk role can be defined for different groups of users. A user taking on the help desk role associated with a group can manage (for example, authorize and revoke) users only for that group. Help desks may manage overlapping groups of users.

AccessAdmin is also used to issue authorization codes to users. Each authorization code has a selectable life span.

4.13 Using AccessAssistant

With AccessAssistant and Web Workplace, organizations can enjoy single sign-on without the hassle of deploying AccessAgent to client PCs, if enterprise applications are all Web-based.

The AccessAssistant is a Web-based interface that enables users to manage their Wallets. They can reset their Tivoli Access Manager for Enterprise Single Sign-On passwords, change the reset questions and answers, and view, add, edit, or delete user names and passwords inside their Wallets. Use AccessAssistant to get the latest credentials and log on to applications. The Web automatic sign-on feature allows users to log on to enterprise Web applications by clicking on links from AccessAssistant, Web Workplace, or enterprise portals, without entering each application password. Users just need to remember one password to log on to all applications. Combined with the reverse proxy feature, Web automatic sign-on can support a large variety of Web applications.

If AccessAgent is not deployed, users must sign up through other means. The enterprise can integrate an identity provisioning system with Tivoli Access Manager for Enterprise Single Sign-On and use the system to provision its users. Alternatively, users can sign up with Tivoli Access Manager for Enterprise Single Sign-On through AccessAssistant or Web Workplace.

Similar to signing up through AccessAgent, users must authenticate themselves by providing their enterprise directory password (for example, Active Directory password) first, then specifying the password and secret. Users can also choose to specify more secret questions and answers, which can be used by the self-service feature for password resets.

AccessAssistant and Web Workplace offer a host of self-service capabilities to its users. Users who use AccessAgent to log on to enterprise applications have to know their application passwords when they use PCs that do not have

AccessAgent installed. AccessAssistant allows users to view their application passwords or copy them to the computer's clipboard.

Users can also reset their secret questions and answers with AccessAssistant or Web Workplace. Instead of calling the help desk for an authorization code, the self-service feature allows users to reset their passwords by providing a subset of the secrets that they have previously specified.

Users of AccessAgent appreciate the similar user interfaces of AccessAssistant and Web Workplace.

For each user, the same Wallet can be accessed through AccessAgent, AccessAssistant, or Web Workplace. The contents are fully synchronized across the user interfaces. System, machine, and user policies are all configured through AccessAdmin, making it easy for administrators to configure all user interfaces from one central console.

AccessAssistant enables users to view application passwords, unlike Web Workplace. AccessAssistant is designed to facilitate the viewing of application passwords. However, Web Workplace is designed to look like a typical portal page, which facilitates logging on to enterprise Web applications. Web Workplace can be integrated with the customer's existing portal or SSL VPN, and AccessAssistant will perform such an integration.

AccessAssistant and Web Workplace support the following second factors:

- One-time mobile active code (MAC) password delivered to smartphones, PDAs, pagers, fax, or other mobile devices.
- OTP tokens, such as:
  - Authenex A-Key OATH-only token (OATH-based OTP)
  - VASCO Digipass GO 3 (time-based OTP)

For specific settings of AccessAssistant and Web Workspace, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

4.14 Strong authentication

Tivoli Access Manager for Enterprise Single Sign-On provides *strong authentication* for all user groups (inside and outside the corporate perimeter) to prevent unauthorized access to confidential corporate information and IT networks. The solution leverages multi-factor authentication devices, such as

USB smart card tokens, building access badges, proximity cards, mobile devices, photo badges, biometrics, and one-time password (OTP) tokens.

In addition to comprehensive support for authentication devices, Tivoli Access Manager for Enterprise Single Sign-On focuses on leveraging existing identification devices and technologies for authentication. Tivoli Access Manager for Enterprise Single Sign-On also provides iTag, a patent-pending technology that can convert any photo badge or personal object into a proximity device, which can be used for strong authentication.

AccessAgent can support sign-up, logon, and lock/unlock by using several authentication factors, from simple passwords to proximity cards, smart cards, USB Keys, and biometrics. The authorization code is treated like a special authentication factor issued by the IMS Server.

For the distribution and adoption of second factors, users can perform an initial sign-up with only one factor (password), and an optional second factor. Administrators can implement a grace period, during which users can register their selected second factor. Registration of second factors after the initial sign-up requires the authorization code issued by the administrator or help desk with AccessAdmin. Second factors can only be registered if AccessAgent is connected to the IMS Server.

To configure user authentication, select **Advanced Settings** → **User Authentication** from the IMS Configuration Utility navigation panel.

When a user signs up for a new Wallet or registers a second authentication factor, the information is synchronized with the IMS Server. An entry with the corresponding second authentication factor is added under the user's settings. This approach allows you to view the user's various types of second authentication factors.

You can revoke a second authentication factor or Wallet when the user leaves the company or when a second authentication factor is reported as lost or stolen.

For more information about supported authentication factors, refer to:

- 4.14.1, "USB Key authentication" on page 141
- 4.14.2, "OTP token authentication" on page 142
- 4.14.3, "RFID authentication" on page 142
- 4.14.4, "Active RFID authentication" on page 144
- 4.14.5, "Fingerprint authentication" on page 144
- 4.14.6, "Authorization code authentication" on page 145
- 4.14.7, "Mobile active code authentication" on page 148

4.14.1 USB Key authentication

The USB Key is a customized and removable USB drive that combines the utility and storage capacity of Flash RAM, the security of a smart card, and the universal connectivity of Universal Serial Bus (USB) in one package. The USB Key can store user names, passwords, certificates, encryption keys, and other security credentials.

The USB form factor is cost-effective. No additional hardware is required for the key to work, and USB ports are available on various platforms. The USB Key stores more passwords and certificates than any other authentication device in the market. The size of the memory can vary according to the needs of your organization. Depending on company policy, users can store passwords for personal applications and Web sites.

Internally, the USB Key stores the following information:

- Serial number

  The serial number is a unique number embedded in the USB Key during manufacturing. It is also printed on the casing of the USB Key. The number is unique for each USB Key and cannot be changed.

- Common Symmetric Key

  The Common Symmetric Key (CSK) is used to encrypt information that is communicated to the IMS Server for backup. Each user has a unique CSK.

- Digital certificates for each certificate-enabled application
- Driver for the USB Key and installation files for AccessAgent

  Your computer cannot communicate with a device until a program or driver is installed. The USB Key might require a driver for it to work with your computer. The required drivers can be found in the USB Key, and are detected and installed automatically.

  The files required for installing AccessAgent on your computer are also available in the USB Key.

The authentication policy always allows USB Keys to be used as a second factor (the USB Key option in the user's authentication policy cannot be disabled). The USB Key password is required when logging on to the USB Key.

The supported USB Keys are:

- USB Key 2.5
- USB Key 3.0
- DigiSAFE KeyCrypt
- Charismathics keys

USB Keys do not work on Windows 2000 machines with USB 2.0 hubs (internal or external). USB Key is the recommended second factor for personal workstations and set at default.

4.14.2 OTP token authentication

A one-time password (OTP) can also be used as a second authentication factor. An OTP is a randomly-generated password, intended only for one specific user for a specific time or purpose. For most systems, the OTP can be sent to an OTP token or another mobile device.

Tivoli Access Manager for Enterprise Single Sign-On support for both time-based OTP (VASCO Digipass) and OATH-based OTP (Authenex A-Key) tokens adds to the list of OTP ActiveCode options.

The OTP displayed on the LCD of an OTP token can be used as an authentication factor to log on to AccessAssistant, Web Workplace, or any application configured to use IMS Server as authentication server through RADIUS. Currently, the only supported OTP tokens are VASCO Digipass GO 3 and Authenex A-Key.

To support the use of OTP token for authentication, an application must be configured to use IMS Server as the RADIUS authentication server. This is similar to configuring an application to use MAC (mobile active code) or other forms of OTP for authentication.

For the second factor, the enterprise application can be configured to authenticate users with:

- Only OTP provided by token
- Either OTP provided by token, or MAC

Before an OTP token can be used and appear in the list of unassigned tokens on AccessAdmin, you should upload the corresponding OTP data file to IMS Server first. This data file contains the OTP data and secrets for one token or an entire batch of tokens.

4.14.3 RFID authentication

The RFID card is an electronic device that uses radio frequency signals to read identification information stored within. Radio frequency identification (RFID) works on the concept of proximity; the user needs to tap the RFID card on the RFID reader to gain access to credentials. The wireless technology in RFID

cards transmits product serial numbers from tags to a scanner, without human intervention.

The RFID reader is an additional hardware component that must be installed on every machine where the RFID card is used for authentication.

RFID is one of the second factors used for shared workstations; all the shared workstation workflows are supported. RFID can also be used for personal workstations.

Currently, the RFID must be used with a password, except for the RFID-only logon and RFID-only unlock scenarios. This is specified as Password + RFID in the user's authentication policy.

AccessAdmin automatically enables Password + RFID authentication if password authentication is allowed for the user.

Important: Plug in the RFID device to your machine before starting up. If the device is not detected upon startup, restart your machine. Do not unplug and re-plug the RFID reader while AccessAgent is still running.

Different versions of RFID cards are available; some might require different readers and configurations, as indicated in this section. In particular, iTag, which is a Tivoli Access Manager for Enterprise Single Sign-On branded RFID smart label, is a Mifare card.

The supported cards include:

- HID 125 kHz Proximity Card
- HID iCLASS
- Mifare (Ultralight, 1 K, 4 K)

Note: This class of cards includes iTag.

The supported readers include:

- RF IDeas pcProx Readers (for 125 kHz cards)
- RF IDeas AIR ID Contactless Smart Card Readers (for iCLASS and Mifare cards)
- GIGA-TMS Proximity Reader MFR135 (PCMCIA reader for Mifare cards)
- Altrus Mifare Desktop Reader Writer A1 (USB reader for Mifare cards)

Important: The GIGA-TMS Proximity Reader MFR135 is not supported on Microsoft Windows Vista.

Currently, only one of the following three types of RFID cards is supported per deployment:

- Mifare card with 32-bit CSN
- Mifare card with greater than 32-bit CSN
- Other RFID cards

An RFID card can also be used for unified access, so users can access a computer and also have access doors or elevators

4.14.4 Active RFID authentication

An active RFID (ARFID) is also termed an *active proximity badge*. This is the term that appears on AccessAgent. The active proximity badge works almost the same way as a regular RFID card. The active proximity badge has an RFID, and works with a proximity reader. However, the active proximity badge differs in its proximity range.

With a regular RFID card, the card must be in close proximity with the reader. With an active proximity badge, the organization can set the distance for detection. For example, the active proximity badge can be two meters away from the reader, and it will be detected from that distance.

ARFID is one of the second factors for shared workstations, as all the shared workstation workflows are supported. ARFID can also be used for personal workstations.

ARFID must be used in conjunction with the password, except for the RFID-only unlock scenario. This is specified as Password + RFID in the user's authentication policy. AccessAdmin automatically enables Password + RFID authentication if Password authentication is allowed for the user. Supported are:

- The currently supported *card* is the Ensure Technologies XyLoc Key XC-2.
- The currently supported *reader* is the Ensure Technologies XyLoc Lock NL-2.

4.14.5 Fingerprint authentication

The fingerprint identification system recognizes the user's fingerprint as an authentication factor. The fingerprint reader translates the fingerprint into encrypted codes, which logs on the user to AccessAgent.

Fingerprint is one of the authentication factors used for shared workstations; all the shared workstation workflows are supported. Fingerprint can also be used for personal workstations.

A user can log on or unlock a computer by simply tapping a finger on the sensor (without password) if the user's cached Wallet is present in the hard drive. If the cached Wallet is absent, the user has to supply the user name (also without password), because the IMS Server can compare a supplied fingerprint with existing fingerprints in the database one at a time, for performance reasons.

Currently, only one-factor authentication is supported for fingerprint. This is specified as Fingerprint in the user's authentication policy.

Note: Automatic sign-up is not supported for fingerprint.

Supported readers include:

- DigitalPersona U.are.U 4000B Fingerprint Reader
- UPEK TouchStrip Fingerprint Sensor TFRZ3 (built-in reader on Lenovo ThinkPad)
- UPEK TouchStrip USB Reader TCRZ3
- UPEK Eikon USB Fingerprint Reader TCRE3C

4.14.6 Authorization code authentication

The authorization code is a system-generated code that can be used as a special authentication factor in certain user scenarios.

The two types of authorization codes are:

- Online authorization code, which is used when AccessAgent can connect to the IMS Server. This is used for password resets, registration of authentication factors, or temporary bypass of authentication factor.
- Offline authorization code, which is used when AccessAgent cannot connect to the IMS Server. A request code will be shown on AccessAgent. This is used for temporary password-reset or temporary bypass of an authentication factor.

The administrator or help desk can issue authorization codes by using AccessAdmin. The self-service authorization code feature, if deployed, allows users to request for and obtain an authorization code by using a mobile phone (SMS).

Note: Although the last-issued authorization code for a user can be revoked by the administrator or help desk using AccessAdmin, the revocation only prevents the user from reusing same authorization code. Any temporary locks created by the authorization code remain valid until the original validity period of the authorization code expires.

Online authorization code

Online authorization codes can be used when AccessAgent can connect to IMS Server. They are required in the following user scenarios:

- Password reset (online)

  The user has forgotten the password and has to reset it. AccessAgent asks for an authorization code and a secret.

- Registration of authentication factors

  The user wants to register a new second factor for the Wallet. AccessAgent asks for authorization code and password. The second factor must not have been previously registered.

- Temporary bypass of authentication factor (online)

  The user has lost the second factor and the Wallet authentication policy requires it. AccessAgent asks the user to present the second factor after entering the user name and password. If the user clicks the **...but I do not have** link, AccessAgent asks for an authorization code as a temporary replacement for the second factor.

  A temporary password-only lock (expires when authorization code expires) will be created for the Wallet on the machine. Subsequently, the user can log on to the Wallet on this machine by supplying the user name and password, until the authorization code expires.

  Note: A USB Key password cannot be reset using this scenario; the user should not insert the USB Key when performing this operation.

Note the following information about online authorization code properties:

- They can be used multiple times for multiple purposes until it expires.
- Length of the authorization code can be configured using the IMS Configuration Utility. It should have a minimum of one character and a maximum of 32 characters.
- Character set is 0123456789ABCDEF. It is case-insensitive and any hyphens entered are ignored.

Note: The choices for a validity period can be configured by using the IMS Configuration Utility (minimum of one day, maximum of 31 days, with a granularity of one day). One month is the period from the issue date to the same day of the next month, thus the exact number of days depends on the month of issue (for example, from 26 August 2008, 3 p.m. to 26 September 2008, 3 p.m.).

Offline authorization code

Offline authorization codes can be used when AccessAgent cannot connect to the IMS Server.

They are required in the following user scenarios:

- Password reset (offline)

  The user has forgotten the password and has to reset it temporarily. AccessAgent asks for an authorization code and a secret.

- Temporary bypass of authentication factor (offline)

  The user has lost the second factor and it is required by the Wallet authentication policy. AccessAgent asks the user to present the second factor after entering the user name and password. If the user clicks the **...but I do not have** link, AccessAgent asks for the authorization code as a temporary replacement for the second factor.

In both user scenarios, a temporary password-only lock (which expires when the authorization code expires) will be created for the Wallet on the machine. Subsequently, the user can log on to the Wallet on this machine by supplying the user name and password, until the authorization code expires.

Note: A USB Key passwords cannot be reset using this method, the user should not insert the USB Key when performing this operation.

Note the following information about offline authorization code properties:

- They can only be used once, because they are issued based on the request code that is displayed on AccessAgent.
- Request codes are eight characters long and they change every minute.
- Period of validity is specified by the administrator or help desk on AccessAdmin as and when the authorization code is issued.
- Offline authorization codes are 16 characters long.
- Default character set for both the request code and authorization code Z3467ACEFHJKRWXY. It is case-insensitive and any entered hyphens are

ignored. Supported character sets can be configured by using the IMS Configuration Utility.

Note: The choices for a validity period can be configured using the IMS Configuration Utility (minimum of one day, maximum of 31 days, with a granularity of one day). One month is the period from the issue date to the same day of the next month, thus the exact number of days depends on the month of issue (for example, from 26 August 2008, 3 p.m. to 26 September 2008, 3 p.m.).

4.14.7 Mobile active code authentication

A Tivoli Access Manager for Enterprise Single Sign-On mobile active code (MAC) is a one-time password that is randomly-generated and event-based. A MAC is generated on the IMS Server and delivered through a secure second channel, such as text services (SMS) on mobile phones. It is used for strong authentication.

Using MACs enhances the security of traditional password-based authentication for applications, because a MAC is a random password that can only be used once by an authorized user. Combined with alternative channels and devices, MACs provide effective second factor authentication.

For a typical logon to an application, the user launches the application logon interface. The user then enters the application user name and password. For example, if the application is authenticated against Active Directory, the user enters an Active Directory user name and password.

The authentication request is redirected to the IMS Server. The IMS Server verifies the logon credentials and delivers an MAC to the user's pre-registered e-mail or mobile phone. The application returns a screen to the user, to enter the MAC.

After receiving the MAC, the user enters the MAC on the application logon interface. Upon submission, the MAC verification request is redirected to the IMS Server. The user can access the application after successful MAC verification.

If the logon interface is customizable, the user can also choose a preferred channel from the logon interface to send the MAC.

The solution provides two-factor authentication by delivering one-time passwords (OTPs) through SMS on mobile phones and other channels (for example, pagers, e-mail, fax, and IVR (Interactive Voice Response) systems).

The central components of MAC are:

- IMS Server

  The server provides centralized management of users and security polices. It provides the following capabilities:

  - Centralized management and de-provisioning of users

    The IMS Server allows administrators to manage users individually or by AD groups. The console can be used to revoke users and immediately deny access to corporate networks over the SSL VPN appliance.

  - Secure one-time passwords

    The passwords comply with FIPS 140-2 requirements.

- Tivoli Access Manager for Enterprise Single Sign-On mobile active code service module

  The service module determines if the user is authorized to remotely access the corporate network. The component is integrated with the IMS Server and generates active codes (OTPs) for authorized users.

- Multiple Channels for receiving active code

  The solution supports a variety of channels for receiving the OTP, including SMS on mobile phones and devices, pagers, e-mail, fax, and IVR systems. The user profiles and policies defined in the IMS Server govern the use of these channels.

To deploy the Tivoli Access Manager for Enterprise Single Sign-On mobile active code solution, perform the following steps (IMS Server is already installed):

1. Use the IMS Configuration Utility to configure the MAC settings for the IMS Server.
2. Use the IMS Configuration Utility to set up and list the parameters to configure the message connector for sending MACs.
3. Provision users at the IMS Server by using the AccessAdmin interface.
4. Use the IMS Configuration Utility and Access Admin to enable MAC settings for applications and users.

For information about Remote Access Integration deployment and installation, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Remote Access Integration Guide Version 8.0.1*, SC23-9955.

4.15 Password self-service

The Tivoli Access Manager for Enterprise Single Sign-On password self-service enables users to reset their primary authentication (Tivoli Access Manager for Enterprise Single Sign-On password or desktop password) from any workstation based on a challenge-response process. All questions are customizable and configurable. When the Tivoli Access Manager for Enterprise Single Sign-On password self-service is configured (no additional components must be installed), calling the help desk or technical support is not necessary, and no waiting for an administrator to reset the password. Instead, the users have to provide second secrets that they have set up during the sign-up phase of the AccessAgent.

When you use the Tivoli Access Manager for Enterprise Single Sign-On password self-service, different workflows can occur. Depending on whether the IMS Server is available for executing the password self-service request, the workflow differs. When the password self-service feature is disabled but the user still wants to reset the password, another workflow is triggered.

When the user wants to use the password self-service function, a series of questions must be answered in preparation. The questions are predefined and managed by the administrator using the AccessAdmin console.

A list of predefined questions is part of the standard installation of IMS Server:

- What's your favorite color?
- What's your favorite fruit?
- What's your mother's maiden name?
- Who's your favorite author?
- Who's your favorite composer?
- Who's your favorite person from history?

Challenge-response questions are prepared by the administrator. When you have determined the set of questions, you have to configure them into Tivoli Access Manager for Enterprise Single Sign-On using AccessAdmin.

The password self-service can be disabled or enabled by system policy using the AccessAdmin GUI. Depending on the status of the self-service feature, the password workflow is different.

As we have mentioned before, several different workflows can occur during a password self-service situation. If the user has a user name and password for primary authentication, the two resulting workflows for password reset are:

- Online access to the IMS Server exists and password self-service enabled

  If the AccessAgent can contact the IMS Server and the password self-service function is enabled, the user can process a password-reset without contacting the help desk staff by providing the self-service credentials. Because the IMS Server can be contacted by the AccessAgent, a password-reset also updates the Wallet in the IMS Server.

- No access to the IMS Server, or password self-service disabled

  If the AccessAgent cannot contact the IMS Server to process a password self-service request, the user has to contact the help desk to get an authorization code. There is no difference whether the password self-service is enabled or not. In offline mode, the AccessAgent can access only local computer resources, in our case, the locally cached identity wallet of the user. Because your AccessAgent has no connection to the IMS Server, any password change is only temporary.

4.16 Auditing and reporting

With Tivoli Access Manager for Enterprise Single Sign-On's audit and compliance functionality, organizations can consolidate data, manage user-centric, secure, and tamper-evident audit capabilities across all endpoints (for example, personal or shared workstations, Citrix, Windows Terminal Services, or browsers).

When combined with Tivoli Access Manager for Enterprise Single Sign-On's strong authentication capabilities, the user-centric audit logs ensure secure access to confidential corporate information and accountability at all times. The logs provide the meta-information that can guide compliance and IT administrators to a more detailed analysis (by user, by application, or by endpoint). These audit logs can be viewed only by the administrator through AccessAdmin.

In addition, this information is collated in a central relational database facilitating real-time monitoring and separate reporting with third party reporting tools.

The identity information and events captured in the database by Tivoli Access Manager for Enterprise Single Sign-On's comprehensive identity auditing

framework allow administrators to generate useful reports for identity auditing, such as:

- List of application accounts for a user
- Policy changes performed on a user by an administrator or help desk
- Successful and failed application logons and logoffs
- Summary table of the number of times each user logs on to each application within a period of time

Organizations can also leverage the endpoint automation framework to audit custom access events for any application, without modifying the application or leveraging the native audit functionalities. The product ships with several included reports, but custom reports are easily generated because all audit data resides in single database. Custom events can be created to track events specific to the application, such as:

- Access to confidential data
- Attempted unauthorized access to application features
- Access to an application outside office hours

To use custom events, you have to modify the *System Policies - AccessAudit Policies* and add each pair of event code and display text to the list of custom audit event codes and their corresponding display names.

Note: Users also have the option to disable the audit log features of AccessAgent to reduce network clutter and IMS Server load.

You cannot track audit events if AccessAgent is not connected to the IMS Server.

The two ways to maintain your audit logs (also known as housekeeping), and determine when to prune logs and free disk space are:

- Run a maintenance batch file `imsserver/bin/hskpLogs.bat`.
- Schedule the IMS Server housekeeping activity by using the IMS Configuration Utility.

4.16.1 IMS Server housekeeping

To perform IMS Server housekeeping tasks, select **Basic Settings** → **IMS Server Housekeeping** from the IMS Configuration Utility navigation panel. You can perform a general, daily, weekly, or monthly housekeeping.

Note: When specifying the directory where RDB (Relational Database) backup files will be stored, ensure that this directory exists and has three subdirectories: daily, weekly, and monthly. This directory is created on the database server, not the IMS Server. The daily, weekly, and monthly subdirectories must also be created.

IMS Server housekeeping supports the following tasks:

- The `cleanupRdbLogs` task cleans up database logs every day.
- The `backupRdb` task creates a back up of the database every day.
- The `backupImsFiles` task creates a back up of the IMS files every day.

You can also specify the number of days to keep logs during log housekeeping.

For more information about IMS Server housekeeping, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Administration Guide Version 8.0.1*, SC23-9951.

4.16.2 Tamper-evident audit logs

The IMS Server logs various types of activities, such as Web service invocation, user administration activities, and user AccessAgent activities. Audit logs are susceptible to tampering, but you can protect them by turning on the hashing of the log, also known as log-signing.

To turn on hashing, modify a configuration key in the `ims.xml` file by using the IMS Configuration Utility. Enable only those activities that you want to set as tamper-evident.

You can set the following activity logs to be tamper-evident by log-signing:

- System management activity
- System operations
- User administration activity
- User activity
- User service

To ensure the integrity of an audit log, run the following checking batch file (log verifier batch file):

`imsserver\ims\bin\vrfyLogs.bat.`

5

Administration

In this chapter, we discuss various administration tasks that are necessary after the installation and initial configuration. We describe how to perform regular administrative tasks and how to best administer the Tivoli Access Manager for Enterprise Single Sign-On environment.

We cover the following topics:

- Managing AccessProfiles using AccessStudio
- IMS Server configuration and maintenance
- AccessAdmin user search and maintenance
- Policy management
- Reports and audit logs
- Migration strategy and considerations

5.1 Managing AccessProfiles using AccessStudio

AccessStudio is the component that is used to create and manage AccessProfiles and enable single sign-on, sign-off, and workflow automation.

Each application is represented by an AccessProfile, which is a set of instructions that define the automatic logon mechanism for that particular application. An application, in AccessStudio, is a logical grouping of AccessProfiles for a business application.

After defined by AccessStudio, AccessAgent reads the AccessProfiles created and performs workflow automation such as sign-on and sign-off.

AccessStudio offers the following features:

- Standard and advanced modes of AccessProfiles that support requirements of varying complexity
- Multiple ways of editing by using GUI-based and XML editors
- Flexibility in editing AccessProfiles stored in any location, including those existing in the IMS Server
- The ability to import existing AccessProfiles from a local installation of AccessAgent or from the IMS Server
- Automatic validation of user-configured AccessProfile data to minimize errors
- The ability to test and debug AccessProfiles

5.1.1 How AccessStudio works

You can create AccessProfile data and save it to a file using AccessStudio. You can also download and modify AccessProfiles and their associated data from either the IMS Server or the local installation of an AccessAgent.

After creating or modifying an AccessProfile and its associated data, use the *Upload to IMS* option to publish the data to the IMS Server. After the IMS Server receives the update, the data is downloaded by the AccessAgents associated with the IMS Server. Any changes or newly created AccessProfiles are applied to the applications in the users' systems.

5.1.2 AccessStudio basic concepts

Let us review several basic concepts we discussed earlier:

- AccessProfile

  An AccessProfile contains instructions for handling automation for an application. An application can be an executable file (`.exe`) or a Web page.

- Authentication service

  An authentication service is a verification entity that validates application logon information. All AccessProfiles are associated with an authentication service.

  Note: You can associate multiple AccessProfiles with a single authentication service.

- Application

  An application is a logical representation of a set of executable files (`.exe`) or Web pages.

5.1.3 AccessStudio advanced concepts

To work with advanced AccessProfiles, an administrator should understand the following concepts:

- Standard AccessProfile (simple SSO support)

  A standard AccessProfile contains all logon, password, and logoff information.

- Advanced AccessProfile (state engine SSO support)

  An advanced AccessProfile can automate operations based on various conditions.

  - State

    The state indicates the current condition or status of an application with a user-defined unique ID.

  - Trigger

    A trigger represents an event that causes transitions between states in a state engine.

– Action

  An action is the process performed in response to a trigger, such as when the software automatically fills in the user name and password details.

– Account data

  Account data contains logon information required for verification against an authentication service.

For more information, refer to 3.2, “AccessProfile configuration” on page 88.

5.1.4 AccessStudio interface

The four main parts to the AccessStudio interface are:

- Menu bar

  The menu bar contains functions for managing AccessProfiles,

- Data type pane

  This pane displays AccessProfiles and their associated data.

- Details pane

  This pane is used to view and edit information associated with a list item from the data type pane.

- Message pane

  This pane is used to view real-time information about the currently active task.

5.1.5 Managing authentication services

Most applications require validation of logon information by a verification entity. In AccessStudio, a reference is created to these entities through *authentication services*. AccessProfiles associated with the same authentication service belong to the same verification entity. Changes made to the logon information in one AccessProfile are reflected across all others associated with the authentication service.

All these applications must share the same set of credentials. If you associate applications with different sets of credentials with the same authentication service, an error can result for the specific AccessProfiles. User credentials are stored in the Wallet according to the authentication service and not the application.

This information is helpful to those using the Form Editor tab or XML Editor tab to create AccessProfiles.

Associating authentication services with AccessProfiles

You can define authentication services in AccessStudio by using the Authentication Services function in the View menu. At a minimum, you provide an ID and a display name for the authentication service. Additional information has to be specified depending on your requirements. Authentication services can be associated with AccessProfiles in two ways: directly and indirectly.

- Direct auth-info

  Direct auth-info is a direct reference to an existing authentication service configured using the Authentication Services function in AccessStudio. When you configure an authentication service as a direct reference, specify the authentication service ID and display name.

- Indirect auth-info

  Indirect auth-info is used when you do not know which authentication service to select at the time of creating an AccessProfile. It is an indirect reference to an existing authentication service. When you configure an authentication service as an indirect reference, in addition to the ID and display name, you must provide information about the server locators.

Managing authentication service groups and group links

Associating AccessProfiles with independent authentication services is usually sufficient. However, there are rare cases where even the user interface of an application cannot identify the authentication service. In such cases, you can create an *authentication service group*, and associate multiple authentication services with this group.

Use the Authentication Service Groups function in AccessStudio to configure an authentication service group.

Note: You can associate authentication service groups only with advanced AccessProfiles.

5.1.6 Managing application objects

An *application object* in AccessStudio is a logical representation of a set of executable files (`.exe`) or Web pages. It provides you with tighter control to apply policies on a group of AccessProfiles. Each AccessProfile must be associated with an application object. Many AccessProfiles can be associated with the same application object.

5.1.7 Account data items and templates

Account data represents a user's logon information in AccessStudio. This consists of the user name and password. The account data for an AccessProfile is stored in a specific format defined in the account data templates.

Account data templates include individual account data items. The properties of these items are defined in the account data item templates. These templates are accessible in AccessStudio through the account data templates and account data item template functions. The templates are predefined in AccessStudio. You can view using the respective functions, but you cannot modify the template.

5.1.8 Signatures

AccessStudio extends the users' capability of editing the application's advanced AccessProfiles using *signatures* containing *XPaths*. Signatures contain XPath (XML Path Language), which is a language that facilitates XML document navigation to select elements and attributes. The XPath language has a hierarchical structure or a tree representation of a given XML document. It provides the ability to navigate around and select list items by a variety of criteria. From this tree, you can access the elements, attributes, and list items of your XML document.

5.1.9 Validating functions

AccessStudio allows you to validate the accuracy or completeness of the functions you configure. These include AccessProfiles, authentication services, applications, and advanced data functions such as account data templates. A red exclamation point displays beside a node that has an error in a function.

By default, the Messages pane displays at the bottom of AccessStudio. The pane displays the nature of the problem (a trigger or action) with an error.

5.1.10 AccessProfile testing

Use AccessStudio's Test function to perform real-time tests on AccessProfiles. This function is either accessible from either the Test menu (**Test** → **Start**) or the Test icon on the tool bar. The results of the test are provided in the Messages pane. A tab with the process name on it displays the logs of all active applications that have AccessProfiles defined for them. New tabs are created for each process ID.

When you start your test, launch the applications with the configured AccessProfiles in AccessStudio. The test will be executed for all AccessProfiles whose corresponding applications are active on the computer. A log is created for each one of these applications in addition to the existing logs.

For example, the *Real-Time Logs* pane displays four logs: Patient Information Manager, IBM Lotus Sametime, messaging software, and E-mail software. The first two are for AccessProfiles running on your AccessAgent. The last two are for those that you are testing with AccessStudio. You can close any of these by clicking the **Close** button at the corner on the right side of the pane.

Note: When you start a test using AccessStudio, the AccessAgent Wallet is temporarily cleared until the test is stopped. This means that logon automation on your computer will not work until after the test is stopped.

5.1.11 Downloading, uploading, and saving information

AccessStudio enables you to download AccessProfiles and associated information (which includes application objects, authentication services, authentication service groups, and authentication service group links) from either the IMS Server or from the AccessAgent installed on your computer.

When you create information (like a new authentication service) or modify it, you must upload it to the IMS Server to be available to all AccessStudio users. AccessStudio also enables you to save the AccessProfiles and additional information you configure in a separate file.

You can upload AccessProfiles, application objects, authentication services, authentication service groups, and authentication service group links to the IMS Server after you have created or modified them.

5.1.12 Backing up IMS Server data

AccessStudio allows you to take a backup of AccessProfiles and associated information existing on your IMS Server. When you use this option, AccessStudio downloads all the information and saves it in a custom AccessStudio `.eas` file or `.xml` file, depending on your preference.

For more details, refer to the *IBM Tivoli Access Manager for Enterprise Single Sign-On Administrator Guide Version 8.0.1*, SC23-9951.

5.2 IMS Server configuration and maintenance

The IMS Server is an integrated management system that provides a central point of secure access administration for an enterprise. It enables centralized management of user identities, AccessProfiles, authentication policies, provides loss management, certificate management, and audit management for the enterprise.

5.2.1 Configuring the IMS Server

Before you can add or delete policy templates within the system, machine, or user scope, you must set up the IMS Server in AccessAdmin by:

1. Specifying IMS Server settings in the Setup Assistant (AccessAdmin)

   Use AccessAdmin's Setup Assistant to configure IMS Server settings.

2. Configuring policy templates in Setup Assistant (AccessAdmin)

   Use AccessAdmin's Setup Assistant to set up user and machine policy templates. The policy templates in this wizard are auto-generated based on previously selected options in Setup Assistant.

5.2.2 IMS Server maintenance

The administrator maintains the IMS Server periodically to ensure that data is backed up, logs are created, and that the IMS Server is running smoothly. This set of topics contains procedures for backing up the IMS Server database, viewing logs, and performing system diagnostics.

The IMS Server is designed to require minimal management or maintenance. Any maintenance efforts can be done using AccessAdmin or the IMS Configuration Utility.

Also refer to 4.16.1, “IMS Server housekeeping” on page 152.

5.2.3 Backing up the database

Data is essential for an enterprise's day-to-day operations, and there should be backup and recovery plans in place. Data loss can occur in several possible ways (for example, accidental deletion of important data, corruption of data critical to daily operations).

Backup and recovery plans allow users to recover data and minimize business and operation downtime. Without implementing backup and recovery plans, critical data may not be retrieved.

Backup and recovery plans must be based on the importance of data, how often data is used and updated, how fast data should be restored, the equipment that will be used to perform backup, and similar factors.

Determine the appropriate backup and recovery plans after careful planning and after considering the impact of data in your enterprise. The database administrator should be responsible for overlooking the whole operation.

The plans should dictate the backup frequency and the media to be used for backup. Back up the entire IMS Server database rather than specific tables.

5.2.4 Viewing logs

The three types of logs available in the IMS Server are *user*, *system*, and *administrator*. The user log contains information about actions performed by the user. The system log provides information related to the IMS Server. The administrator log lists help desk employee and administrator actions.

User logs are available to both help desk employee and administrator, although the help desk employee likely will be going through these logs. Only the administrator has access to both the system and administrator logs.

The events in AccessAdmin are specified in the configuration file and can be modified as needed using the IMS Configuration Utility.

5.3 AccessAdmin user search and maintenance

In this section we discuss how to manage users with AccessAdmin.

The two ways to log on to AccessAdmin are:

- From the console of the machine where the IMS Server is installed, access the following address and then a logon prompt is displayed:

  `https://imsservername`

- Log on to AccessAgent on any machine as Administrator, and then launch:

  `https://imsservername`

When logging on to AccessAdmin, enter the fully-qualified domain name (for example, `https://ims.ibm.com`).

Note: If the IMS Server is accessed without using the fully-qualified domain name, AccessAgent cannot perform logons to the search page automatically.

The IMS Server location should be set during the typical setup period, which is done by setting the ImsServerName key in the `SetupHlp.ini` file appropriately. The AccessAgent installer will automatically download the IMS Server certificate from the IMS Server.

In the main user interface, you can find links to all the available administrative functions. The main link, AccessAdmin, should be visible at all times. Click on the link to view the AccessAdmin user interface.

As an Administrator, you can *search for users*, and *view* and *edit user settings* by using AccessAdmin.

5.4 Policy management

Policies control the behavior of Tivoli Access Manager for Enterprise Single Sign-On components and facilitate configurability of the product to meet specific requirements.

Use AccessAdmin to view system, machine, and user policies. All policies with system, machine, or user scopes can be modified through AccessAdmin. User policies can also be modified for an entire group of users using the Search Users feature. System policies may be defined for authentication services, applications, or a combination of an authentication service and an application.

5.4.1 Defining policies

Use this procedure to define a Tivoli Access Manager for Enterprise Single Sign-On policy. You have to determine the policy scope and its relationship and dependency on other policies, such as:

- Setting administrative policies

  Use AccessAdmin to set the *promotion level* of the user. The three roles within Tivoli Access Manager for Enterprise Single Sign-On are: *user*, *help desk*, and *administrator*. An administrator can promote the user or a help desk user, and also demote a help desk user.

- Setting authentication policies

  Use AccessAdmin to set the *Wallet authentication policies* for each user to enforce the combinations of authentication factors that can be used to log on.

- Setting password policies

  Use AccessAdmin to set the *password policies* for each user.

- Setting Wallet policies

  Use AccessAdmin to set *Wallet policies* for a user.

- Setting AccessAgent policies

  Use AccessAdmin to set *AccessAgent policies* for a user. AccessAgent policies consists of all the policies that define the behavioral patterns of AccessAgent on one computer when the user is logged on.

- Setting authentication service policies

  Use AccessAdmin to modify the *authentication service policies* of each enterprise authentication service.

5.4.2 Viewing and setting system policies

Use the AccessAdmin navigation panel to view, create and modify system policies. These policies are used to report, track or audit any application-specific custom event. Custom events are created as a list of event code and display text pairs.

You create custom events to track application-specific events such as:

- Access to confidential data
- Attempted access to application features that a user is not authorized to use
- Access to applications outside office hours

For example, you can define an AccessAudit policy to create an AccessProfile that tracks an event and submits an audit log.

5.4.3 Viewing and setting policy priorities

If a policy is defined for two scopes (for example, machine and system, user and system, or machine and user), you can define a priority in case the time-out value is different for the scopes. For example, if the policy priority is machine, then only the machine policy would be effective.

Policies can only be modified by help desk employees and administrators. These policies affect the behavior of the entire system and should only be modified when absolutely necessary.

These policies should be set at deployment and followed through. Changes to these policies are propagated to clients the next time the AccessAgent synchronizes with the IMS Server.

5.5 Reports and audit logs

Reports and audit logs are an essential element in any product administration for viewing and properly managing critical system properties. In this section, we describe the Tivoli Access Manager for Enterprise Single Sign-On reporting and auditing capabilities.

5.5.1 Viewing and printing audit logs

Use AccessAdmin to generate audit logs on one or more selected activities (for example, authentication factor verification, authorization code issuance) within a specified time period. The audit logs display the details of each activity, such as the user who performed the activity, the date and time of the activity, and the result of the activity.

5.5.2 Viewing and printing audit reports

Use AccessAdmin to generate audit reports that display a summary of user information, token information, application usage, and help desk activity within a specified time period. Actions performed by users, help desk officers, and administrators are all logged in audit reports with a comprehensive audit trail.

- Generating and printing user information reports

  The user information report contains the activity of one or more users, sorted by event, result, and time. The report also displays the machine IP address and the full name of users (not just the user name).

- Generating and printing token information reports

  A token information report contains the activity of one or more users, sorted by token type, event, and time. The report also displays the machine IP address and full name of users.

- Generating and printing application usage reports

  An application usage report contains the authentication service activity of one or more users, sorted by event and time. The report also displays the machine IP address and the full name of users.

- Generating and printing Help desk activity reports

  A help desk activity report contains the activity of one or more help desk users, sorted by event and time. The report also displays the machine IP address, token type, token ID, and the full name of each help desk user. Token type and token ID information are displayed only if they are available.

Note: You can specify the number of matching results to display by per page by marking the appropriate **Page size** button.

5.5.3 Integrating an audit log with a commercial reporting tool

The Tivoli Access Manager for Enterprise Single Sign-On audit log database can be integrated with third- party commercial reporting tools, such as Crystal Reports or Eclipse.

5.5.4 Maintaining audit logs

You can maintain your audit logs (also known as housekeeping), and determine when to prune logs and free disk space. The two ways to maintain your audit logs are:

- Run a maintenance batch file.
- Schedule the housekeeping activity using the IMS Configuration Utility.

5.6 Migration strategy and considerations

The process of migrating data across environments consists of searching for and exporting configured entities from a source server and importing them into a target server. This can be used between development environments, from development to test, from test to production, from production to a disaster recovery site, and so on. In a majority of cases, the most crucial part of migrating or promoting policies and business logic between environments is when moving between the staging and production environments.

In this section, we provide an overview of the migration scenarios and provide configuration tips.

5.6.1 Switching to another IMS Server

To switch to another IMS Server on the client machine, use the following steps:

1. Set the machine policy `pid_ims_server_name` by editing the registry value:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\IMSService\DefaultIMSService]"ImsSe
   rverName"
   ```

2. Download the IMS Server certificate by running:

   ```
   C:\Program Files\Encentuate\SetupCertDlg.exe
   ```

3. Log off AccessAgent (if logged on).
4. Kill the AccessAgent processes: `AATray.exe`, `DataProvider.exe`, and `Sync.exe`.
5. Stop the SOCIAccess service by issuing the following command:

   ```
   net stop sociaccess
   ```

6. Delete the entire `C:\Program Files\Encentuate\Cryptoboxes` folder (back up the existing folders to another location to switch back to the original IMS Server).
7. Restart the machine.

> **Note:** Restarting the machine with a missing machine Wallet forces AccessAgent to re-create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

To switch to a different IMS Server with no Cryptoboxes backed up, use the following steps:

1. Log off AccessAgent (if logged on).
2. Kill the AccessAgent processes: `AATray.exe`, `DataProvider.exe`, and `Sync.exe`.
3. Stop the SOCIAccess service by issuing the following command:

   ```
   net stop sociaccess
   ```

4. Restore the Cryptoboxes folder for the IMS Server (back up the existing ones to another location to switch back to the original IMS Server).
5. Start the SOCIAccess service by issuing the following command:

   ```
   net start sociaccess
   ```

6. Run the following command:

   ```
   C:\Program Files\Encentuate\AATray.exe
   ```

5.6.2 Copying AccessProfiles between IMS Servers

Use the following steps to copy AccessProfiles between IMS Servers:

1. Set the machine policy `pid_ims_server_name` to the IMS Server that will contain the copied AccessProfiles.
2. Run AccessStudio.
3. Perform a *download from IMS Server*.
4. Save to a file (`.eas`) and exit from AccessStudio.

5. Set the machine policy `pid_ims_server_name` to the target IMS Server.
6. Run AccessStudio.
7. Open the saved file.
8. Perform an *upload all to IMS Server*.

5.6.3 Configuration tips

The following list contains helpful configuration tips:

- Deleting a user without revoking

  When a user is revoked through AccessAdmin, the user name can no longer be used. To prevent a user name from being reused, delete the user without revoking the user name.

- Promoting a user to administrator

  After signing up, a user is not assigned an administrator or help desk role unless previously configured as an administrator during an IMS Server installation. A new user is usually promoted to an administrator role by existing administrators through AccessAdmin.

- Enabling and disabling autoplay for removable drives

  When an older version of AccessAgent (before version 3.3.2.6) is installed, the installer sets a Windows registry entry named `NoDriveTypeAutoRun` to a value of `4`, which disables autoplay when a removable drive is connected to the machine. If autoplay is enabled, Windows activates autoplay every time a USB key is inserted, which might not be a desired behavior.

- Improving AccessAgent performance

  The AccessProfiles can become very large data objects when they are parsed by the DataProvider process of AccessAgent. These data objects must be kept in memory. Removing unused AccessProfiles can speed up AccessAgent performance. To remove unused data objects, right-click on each unused AccessProfile and click **Delete**.

- Specifying the IMS database user account

  Installation can fail if you specify the SA account as the IMS database user account. The IMS database user account should be different from the SA account.

- Configuring the ADAM Server

  For detailed configuration instructions, refer to the *ADAM Step-by-Step Guide* from the Microsoft Download Center.

- Turning off authentication for AccessAdmin

  By default, AccessAdmin is protected by a certificate-based authentication mechanism supported by AccessAgent. An administrator must first log on to AccessAgent before accessing AccessAdmin.

- Configuring the IMS Server download port

  If Microsoft IIS (Internet Information Server) or other Web servers are installed on the same machine as the IMS Server, it may be necessary to use a download port other than the default port 80. Configuration changes must be done on both the IMS Server and AccessAgent.

- Enabling RFID readers for AccessAgent running in VMware®

  Since the RFID reader is actually a Human Interface Device (HID), the following line should be added to the VMware image's VMX file:

  ```
  usb.generic.allowHID = "TRUE"
  ```

- Modifying AccessAdmin Web pages

  Starting from IMS Server 3.5.0, `.jsp` files are precompiled when an IMS Server is installed or upgraded. This improves the loading speed of IMS Server pages (AccessAdmin and IMS Configuration Utility) on first access.

5.6.4 Preparing the IMS database

The IMS database can be separately installed and prepared, or installed as part of the IMS installer after version 3.4.0.0.

On a manually prepared IMS database, the installation instance must satisfy the database vendor specific prerequisites for IMS Server version above 3.4.0.0.

Note: If the IMS database and IMS Server are running on different machines, the system clocks must be synchronized. Use the time synchronization feature of Microsoft Windows and that is based on Network Time Protocol (NTP) to synchronize the system clocks

6

Performance tuning and problem determination

In this chapter, we discuss basic performance tuning for a Tivoli Access Manager for Enterprise Single Sign-On environment.

We also look at problem determination, focusing on explanations and actions.

6.1 Optimizing IMS Server performance

The IMS Server (and its underlying Apache Tomcat and JVM environment) is optimized to support large deployments. It is possible to setup a single server machine hosting IMS and database server or a distributed or highly available solution. When installing IMS, the default parameters used for the database pool and for the underlying Tomcat application server and JVM assumes a server-class host machine with a SpecIntRate2006 greater than 30 and at least 1 GB of RAM. Usually, adjusting these parameters is not necessary unless the server machine is of lower-end specification (for example, a low-end machine with 512 MB RAM).

You may further optimize the various IMS, Tomcat, and JVM parameters for specific scenarios where the default configuration is found to be sub-optimal. Because IMS is processor-bound, setting the JVM maximum heap size, for example, greater than 512 M might not have significant performance improvements in some scenarios. However, a best practice is for tuning to be accompanied by a round of load or stress-testing to verify the performance gains and to ensure the system remains stable under load.

The IMS installer always sets the memory allocation and connection parameters to default values on the first installation. During upgrades, the memory setting is overwritten, while the database connection setting parameter remains the same. You have to optimize the number of concurrent threads after every upgrade. For specific steps, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

The IMS Server performance tuning parameters can be classified in four types:

- Memory allocation, which is the amount of RAM allocated to IMS Server

  These parameters specify the amount of memory allocated to the JVM.

- Connection parameters, which are the number of concurrent connections to be accepted or processed

  These parameters control the number of concurrent AccessAgent connections that the IMS Server can handle.

- Database parameters, which is the database pool size and timeout values

Note: There are separate configurations for connections to the IMS database (which stores system data, user passwords, and more) and the IMS log database (which stores audit logs), although most of the time, the IMS database and log database reside on the same database server.

- RADIUS parameters: The number of concurrent RADIUS requests to be accepted

> **Note:** This setting is only required if the RADIUS authentication feature of IMS Server is used.

The optimal values of these parameters depend on many external factors, which vary across deployments:

- Number of concurrent AccessAgent connections to IMS Server
- Whether IMS Servers are load-balanced
- Tasks performed on IMS Server (for example, a deployment using OTP authentication may require more processor power)
- Processor speed of IMS Server
- Amount of physical RAM that can be allocated to IMS Server
- Whether the database server is sharing the same machine with IMS Server
- Processor speed of database server
- Amount of physical RAM allocated to database server
- Capability of the database server (for example, number of concurrent connections it can handle)
- Quality of the network (for example, slow network requires higher timeout thresholds for database connections)

Refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952 for more information about IMS Server performance tuning parameters.

6.1.1 Improving server scalability and availability

Let us take a look at two different deployments: small scale and typical.

Small-scale deployment

The IMS and database server can be hosted on a single machine, which is sufficient for small-scale deployments. This configuration can be scaled-up in the following ways:

- Enhance the processor hardware (faster processor or multi-processor).
- Add more RAM.
- Upgrade the disk sub-system (more disks, faster disks) and optimize the database file layout on these disks.

A single server configuration can be made highly-available by adding a second server and setting up an *active-passive* cluster over the two servers. Such a configuration typically involves:

- Use of Microsoft Cluster Service (or equivalent)
- Use of an external disk array shared by both server machines
- Use of a cluster-aware edition of the database server
- Configuring the cluster service to recognize IMS and the database as resources to be managed under the cluster

In such a configuration, the cluster service monitors the following elements:

- Host machines
- Health of the IMS Server
- Database services

The cluster service can trigger a failover from one machine to another if any of the elements fail.

Typical deployment

For most deployments, a two-tier architecture is good practice, with a tier of IMS Servers fronting a shared database server.

In this configuration, a hardware or software-based load-balancing solution should be used to distribute the incoming traffic from various AccessAgent installations into multiple IMS Servers. The load-balancing solution should support *session affinity*, where each client's request is consistently routed to the same IMS Server (until the server goes down, and the requests are then re-routed to another server). Such load balancers inspect each packet's IP headers and route it to one of the IMS Server farm members based on some rule (for example, client IP address, destination port, and so on).

The load balancers automatically re-balances incoming traffic when a member of the server farm goes up or down. Some load balancers also support continuous monitoring of application or service status based on custom scripts (for example, pinging a certain URL), so that traffic can be re-routed if a certain application or service on a server machine fails to respond.

An example software-based load balancing solution is the Microsoft Network Load Balancing (NLB) solution, which is packaged with the Windows Server platform. In a Microsoft NLB setup, all member servers share the same DNS name and virtual IP address. Each server has its own private IP address, for heartbeat checks and administration purposes. Incoming traffic is routed to all servers but only one server accepts and processes the request. NLB can be

configured to support session affinity, where the client's IP address is used to determine which member server to accept the request.

A load balancing solution is also often used to provide High Availability. Refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952 for details.

You scale up the database server if performance measurements indicate that its processor, RAM, or disk is a bottleneck. As such, the methods for scaling up the database server includes:

- Enhance the processor hardware (faster processor or multi- processor).
- Add more RAM.
- Upgrade the disk sub-system (more disks, faster disks) and optimize the database file layout on these disks.

Solutions for scaling out the database server across multiple machines are typically vendor-dependent (for example, Oracle RAC, IBM DB2 DPF, and so on) and might require customization to the IMS installation process to interoperate with such solutions.

6.1.2 Distributed IMS using replicated databases

A previous limitation of the IMS architecture was that all IMS Servers had to share a single database instance. This precluded large enterprises from deploying IMS in a distributed fashion. Even if the IMS Servers can be distributed in multiple sites (for example, one in New York, one in Los Angeles, and one in Singapore), they must ultimately connect back to the single IMS DB server installed at one site.

This single database instance limitation is an issue for large customers, for reasons such as:

- The IMS site (and the IMS database) becomes a single point of failure.
- A lot of unnecessary cross-site traffic might occur between AccessAgent and IMS, because AccessAgent systems will not be in the same site as IMS.
- Scaling the IMS database might be I difficult and expensive because the only way to handle higher load volumes is by upgrading the DB server hardware.

For some large customers, the workaround is to set up separate logical IMS Servers for each region. Each region's users will have a separate IMS setup (one IMS and one DB), with its own set of users, profiles, and policies. However, this solution has limitations because AccessAgent can only support one IMS at a time. A user from one site cannot log in to AccessAgent from a machine

configured at another site. You can have an architectural solution that allows each major geographic region and site to host its own set of IMS and IMS DB servers (service AccessAgent systems in its respective region), while allowing users to occasionally roam from one site to another.

Database replication is a solution that allows IMS databases to replicate with across sites reliably and quickly. Because database replication technologies vary for each vendor, Tivoli Access Manager for Enterprise Single Sign-On supports only database replication for DB2 for this release.

For more information about distributed IMS, refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952.

6.2 Improve AccessAgent performance

Improving AccessAgent performance, the AccessProfiles can become very large data objects when they are parsed by the DataProvider process of AccessAgent. These data objects must be kept in memory. Removing unused AccessProfiles can speed up AccessAgent performance. To remove unused data objects, right-click on each unused AccessProfile and then click **Delete**.

During login or unlock, AccessAgent performs SOAP calls to IMS, password verification, and writing logs. One of the things that contributes to timings is logs, because of disk access. To improve AccessAgent performance, you can reduce the LogLevel in the Windows registry.

Another way to improve logon performance is to limit the maximum number of cached Wallets for a shared workstation, especially in deployments where fingerprint readers are used for authentication.

To improve AccessAgent performance in a Citrix deployment with Active Directory password synchronization enabled, the machine policy `pid_ts_wallet_cahing_option` for remote AccessAgent should be set to `2`, so remote AccessAgent can cache the user's Wallet on the hard disk.

6.3 Microsoft Operations Manager

Microsoft Operations Manager (MOM) is the event and performance management element of the Microsoft Windows Server System™. The product allows monitoring of numerous computers interconnected by one or more communications networks. Microsoft server products, such as Active Directory,

Microsoft SQL Server, Microsoft Exchange Server, and MOM itself can be monitored through MOM.

Integrating the IMS Server with MOM provides customers with a unified monitoring and management solution across the entire corporate platform. MOM allows administrators to examine the health status of the IMS Server and trigger alerts when certain important events occur.

MOM depends on agents to manage computers. An agent is a piece of software running on managed computers that monitor system resources, for example, a Windows event log. Specific events or alerts can be generated by applications running on the monitored computer. Upon event occurrence and detection, MOM agents forward the event to a central MOM server.

The MOM server maintains a history of events in a database by applying filtering rules to all incoming events and generating the necessary notifications. A notification can take the form of an e-mail, a pager message, a network support ticket, or some other workflow intended to correct the problem that triggered the notifications.

Several MOM servers can be aggregated to monitor multiple networks across logical Windows domains and physical network boundaries. Through a connector framework scheme employing Web services, individual MOM servers can exchange alerts with other network management applications.

Although Microsoft and other software vendors make Management Packs available for their products, MOM also provides facilities for authoring custom Management Packs. A MOM Management Pack for the IMS Server (in `.AKM` file format) has been developed to help administrators with the integration of the IMS Server with MOM.

The integration of Tivoli Access Manager for Enterprise Single Sign-On (TAM E-SSO) with MOM allows administrators to monitor the health status of the IMS Server and to examine TAM E-SSO event logs through the MOM console. The IMS Server has to be set up to transmit event logs to an MOM agent (running on the same server machine) through a Syslog protocol.

In turn, the MOM agent filters the received logs based on predefined rules and sends the filtered events to the MOM server for storage. The MOM agent also monitors the system resources (for example, Windows event log, memory, and processor) and notifies the MOM Server, based on the defined rules.

The MOM server maintains a history of events in a database by applying filtering rules to all incoming events and generating notifications whenever necessary. A notification can be sent through e-mail, a pager message, a network support ticket, or another workflow.

The main features of MOM include the capability to:

- Monitor the IMS Server health status

  Using the MOM Operator console, administrators can monitor the health status of each IMS Server, and check whether the server is operational. The console can also show performance monitoring graphs for various health parameters of the IMS Server, including:

  - Processor utilization
  - Memory utilization
  - Disk utilization
  - Page file utilization
  - Context switches per second
  - Processor queue length

- Start or stop the IMS Server from the MOM console

  The administrator can start or stop the IMS Server by using the MOM Operator console.

- Store audit logs in the MOM server

  The administrator chooses which IMS Server log tables (user activity, system management activity, and so on) are exported to the MOM server through the Syslog protocol.

  To reduce the size of the IMS Server database, the administrator can also set the IMS Server to export the logs to the MOM server without storing them in the IMS Server database. This approach can improve the performance of the IMS Server.

  Note: At present, logs sent to external entities through the Syslog protocol are not tamper-evident. When administrators abort the IMS Server database logging in favor of MOM-managed audit logging and reporting, reporting log tampering is effectively lost.

- Trigger alerts based on rules

  The MOM server can generate alerts or notifications based on rules applied to IMS Server health information, including audit logs received from the IMS Server.

- Audit reports using MOM reporting tools

  The MOM server uses two databases (DB) – one for live operations, and the other for archival. Activity events are transferred from the live DB to the archival DB every night. Reports can be generated from:

  - Reporting console, using SQL Reporting Services, based on archival data
  - Operator console based on live data

Data sources cannot be combined to produce reports.

The MOM Management Pack for IMS Server includes XML schemas for SQL Reporting Services, so standard reports can be generated from the MOM reporting console.

Note: At present, logs sent to external entities through the Syslog protocol are not tamper-evident. When administrators abort the IMS Server database logging in favor of MOM-managed audit logging and reporting, reporting log tampering is effectively lost.

6.4 Problem determination

Problem determination, or troubleshooting, is a process of determining why a product is not functioning in the expected manner. This section provides information to help you identify and resolve problems that you might encounter while deploying Tivoli Access Manager for Enterprise Single Sign-On.

Refer to the following sections for more information:

- 6.4.1, “Installation issues” on page 179
- 6.4.2, “IMS Server issues” on page 184
- 6.4.3, “AccessAgent issues” on page 186
- 6.4.4, “Other issues” on page 194
- 6.4.5, “Documenting a PMR” on page 197

6.4.1 Installation issues

In this section, we discuss installation issues.

Anti-virus software can interfere with AccessAgent or IMS Server

Certain anti-virus software has been observed to interfere with AccessAgent or IMS Server, causing the following symptoms:

- AccessAgent (on user’s PC, Terminal Server, or Citrix server) can become very slow.
- AccessAgent (on user’s PC, Terminal Server, or Citrix server) can fail to start.
- Logging on to AccessAgent (on Terminal Server or Citrix server) can fail intermittently.
- The IMS Server can become very slow.

These problems have been observed at deployments that use McAfee anti-virus. To resolve the problem, store the following frequently changing Tivoli Access Manager for Enterprise Single Sign-On folders in the anti-virus software's exclusion list:

- For AccessAgent

  ```
  C:\Program Files\Encentuate\logs for AccessAgent
  ```

- For IMS Server

  ```
  C:\Encentuate for IMS Server
  ```

For the particular McAfee example refer to "Configuration for McAfee antivirus" on page 180.

Configuration for McAfee antivirus

To include Tivoli Access Manager for Enterprise Single Sign-On folders in the McAfee anti-virus software's exclusion list, performing the following steps:

1. Open the scanner's property pages.
2. On the Detection tab, under *What not to scan*, use the *exclusions* feature.
3. Click **Exclusions** to open the Set Exclusions dialog box.
4. Add files, folders, or drives, or edit an item in the list.
5. To add an item, click **Add**. The Add Exclusion Item dialog box opens.
6. Under *What* to exclude, select the folder using By name/location.
7. Under *When* to exclude, specify all options.
8. Click **OK** to save these settings and return to the Set Exclusions dialog box.
9. Click **OK** to save these settings and return to the Detection tab.
10. Click **Apply** to save these settings.

MSDE installation problem

If a previous version of MSDE[1] (before Service Pack 3) is installed on Windows XP (Service Pack 2), there may be no errors during installation. However, because of a security vulnerability in older versions of MSDE, Windows disallows the SQL server to use port 1433. Windows disallows the SQL server to use port 1433, which can result in disconnections to the database during IMS Server installation.

Use the Event Viewer in the Applications category to find the logs generated by SQL server. Older versions of MSDE should indicate that port 1433 cannot be used because of a vulnerability in the current version of MSDE.

[1] Microsoft SQL Server Desktop Engine (MSDE)

To resolve this issue, apply MSDE 2000 Service Pack 3 (or a newer version), or simply download the latest release of MSDE installer from the Microsoft Support Web site.

IMS Server installation problem as a result of database configuration

The IMS Server installation can fail if the database server has been configured to return *No Count*. Because the IMS Server uses these counts to determine the success or failure of database operations, this database feature must be disabled

To disable the database feature, perform the following steps:

1. From Enterprise Manager, right-click the database server and select **Properties**.
2. Go to **Connection** → **No Count**, and disable it.

The IMS Server installation can also fail if the database has incorrect user privileges. The database user should have public, db_owner rights for the IMS database. The user should not be a DB administrator account.

To check whether the database user has the correct privileges, perform the following steps:

1. Select **DB Server** → **Security** → **Logins**.
2. Right-click **DB login** and select **Properties**.
3. Click on the **Server Roles** tab.
4. Privileges are *incorrect* if the *System Administrators* and *Database Creators* roles are *marked*. If incorrect, manually prepare the IMS database and refer to the instructions for preparing the IMS database in *IBM Tivoli Access Manager for Enterprise Single Sign-On Administrator Guide Version 8.0*, SC23-9951.

Failure to connect to named instance of SQL Server 2000 database

If an earlier version of IMS Server is upgraded to version 3.3.1.4 or later, the upgrade might fail if the IMS database is a named instance of an SQL Server 2000 database. The following error message occurs:

"`There was a problem uploading all_storage_templates.xml`**"** `is displayed, since the IMS Server cannot connect to the database.`

This problem is the result of a problem in a Microsoft's SQL Server 2000 JDBC driver that was used prior to IMS Server version 3.3.1.4, which ignores the database port number field if a named instance is used. In the new SQL Server

2005 JDBC driver used in IMS Server version 3.3.1.4 and later, the port number field is not ignored, and the database connection can fail if the port number is incorrect.

To fix this problem during an IMS Server upgrade, modify the IMS Server configuration file to the correct the port number:

1. Provide the correct port number in the following keys in the `ims.xml` file (found in `<IMS Installation Folder>\ims\config`):

   ```
   ds.ims.rdb.uri
   ds.ims_log.rdb.uri
   ```

   For example, if the correct port number is 1074, select the following line:

   ```
   jdbc:microsoft:sqlserver://serverName\instanceName:1433
   ```

   Replace the line with:

   ```
   jdbc:microsoft:sqlserver://serverName\instanceName:1074
   ```

2. To find the port number that is running the instance:
   a. Select **Start** → **Programs** → **Microsoft SQL Server** → **Server Network Utility**. Then choose **TCP/IP**.
   b. Click **Properties**.
   c. Right-click **database server** and select **Properties**.
3. For a fresh IMS Server installation, make sure that the port number in the installation wizard is correct.

RFID reader RDR-7172AKU problem

If you are using RFID reader RDR-7172AKU, card detection issues might be caused by putting a machine into standby or hibernation mode and then resuming from it. This recurring issue is the result of problems with the RFID reader drivers. To fix this problem unplug and re-plug the RFID reader.

AccessAgent displays incorrect icons after an installation upgrade

After an upgrade from a previous version of AccessAgent to AccessAgent 8.0, the program icons are not updated and continue to display the icons used in the previous version of AccessAgent.

This is a Microsoft Windows icon cache problem. For Windows 2000, the system caches the older icons and re-uses them during an AccessAgent upgrade. To correct the problem, rebuild the Windows icon cache.

Refer to the Microsoft knowledge base (KB) item 199152 at:

http://support.microsoft.com/kb/Q199152/

AccessAgent fails to install

If AccessAgent fails to install, check the following items:

- Windows Scripting Host 5.6 and later should be installed.
- Windows Management Instrumentation (WMI) has to be functional. To verify its functionality:

  a. Go to **Computer Management** → **Services and Applications** → **WMI Control**.

  b. Right-click **Properties** and verify whether the following message is displayed:

  ```
  Successfully Connected to: <local computer>
  ```

  If no message is displayed, AccessAgent does not install.

Issues concerning Microsoft Operations Manager

Various messages can display when you install MOM components:

- The following message is displayed when you install Microsoft Operations Manager (MOM) 2005:

  ```
  Microsoft SQL Server 2000 SP3a or above required
  ```

  Refer to Microsoft KB 902803:

  http://support.microsoft.com/kb/902803

- The following message is displayed when you install Microsoft Operations Manager Reporting:

  ```
  Failed to create data source for data warehouse
  ```

  Refer to Microsoft KB 555533:

  http://support.microsoft.com/kb/555533

- The following message is displayed when you install the MOM Agent:

  ```
  The MOM Server detected that DCOM was disabled on the remote
  computer
  ```

  To resolve the problem:

  a. Open **dcomcnfg** in **Start** → **Run**.

  b. Go to **Console Root** → **Component Services** → **My Computer**.

  c. Right-click **My Computer** and select **Properties**.

d. In the My Computer Properties dialog, select the Default Properties tab.

e. Make sure the **Enable Distributed COM on this computer** option is marked.

6.4.2 IMS Server issues

In this section, we discuss IMS Server issues.

IMS Server logs

A useful approach for troubleshooting IMS Server problems is to view the log files in:

```
C:\Encentuate\IMSServerx.x.x.x\ims\logs
```

In general, the `stdout.log` and `stderr.log` files are most useful.

You should understand that the `stdout.log` and `stderr.log` are overwritten when the IMS Server starts up. Therefore, if you have a problem and you want to provide the IMS Server log files, collect them *before you restart the IMS Server*. Otherwise, the log files get lost during the next restart of the IMS Server.

IMS Configuration Utility cannot be accessed

If the IP address of the IMS Server has changed, the IMS Configuration Utility is inaccessible from the following URL unless the new IP address is included in the *RemoteAddrValve* configuration key of the `<IMS Installation Folder>\conf\server.xml` file:

```
http://imsservername:8080/
```

Restart the IMS Server after the configuration key is modified.

Alternatively, to retain the original configuration key, you can still access the IMS Configuration Utility from:

```
http://localhost:8080/
```

IMS Server cannot issue certificate for an application

A known bug is that subject fields of IMS certificates must not contain the underscore character (_). This character can cause problems at deployments that use certificate-based authentication for applications.

The result is that the IMS Server cannot issue SCR or CAPI certificates for an authentication service with an ID that contains the underscore character. The workaround is to remove all underscore characters from the IDs of authentication services that use certificate-based authentication.

IMS Server diagnostic information

To obtain IMS Server diagnostic information:

1. Log on to AccessAdmin.
2. Navigate to the following address:

   `https://imsserver/ims/ui/diagnostics`

The site contains the list of SOAP services, IMS configuration information, test facilities for IMS Connectors, and descriptions of event and result codes.

IMS Server console startup

By default, the IMS Server runs automatically as a service *IMSService* when the machine starts up. When in this mode, troubleshooting any problem with the IMS Server might be difficult. Alternatively, the IMS Server can be run in console mode, so that any error messages are displayed in real-time.

To run the IMS Server in console mode, perform the following steps:

1. Stop the IMSService using the **`net stop IMSService`** command.
2. Run the batch file: `<IMS Installation Folder>\ims\bin\runserver.bat`.

IMS Server database housekeeping problems

For normal database backup operations, the IMS database user must have backup permissions on the IMS database. However, if the Housekeeping RDB System Backup Flag is set to `true`, the IMS database user also has administrative privileges, otherwise the following exception appears in the IMS Server standard error logs:

```
java.sql.SQLException: [Microsoft][SQLServer 2000 Driver for
JDBC][SQLServer]BACKUP DATABASE permission denied in database 'master'.
```

If cleanupRdbLogs is enabled (that is, log table pruning), a log directory should exist in the `<IMS Installation Folder>\bin` directory, otherwise the following exception appears in the IMS Server standard error logs:

```
java.io.FileNotFoundException: logs\rdbLogCleanup.log (The system
cannot find the path specified)
```

6.4.3 AccessAgent issues

In this first section, we focus on issues concerning the AccessAgent.

AccessAgent logs

To help you with troubleshooting AccessAgent problems, view the log files in the `C:\Program Files\Encentuate\logs` folder. The XML files indicate communications with the IMS Server and are useful for troubleshooting failure because of AccessAgent-IMS Server interaction. The `AccessAgent.log` records internal AccessAgent processes and is useful for troubleshooting internal failure within AccessAgent. The `aa_observer.log` records observations of applications for automatic sign-on.

For installation problems, the AccessAgent installer logs can be found in the `C:\AAInstaller.log` file.

When reporting a problem, including a `.zip` file that contains the entire `C:\Program Files\Encentuate\logs` folder is helpful. You should also provide the approximate local time when the events occurred.

AccessAgent log level

Also useful when you troubleshoot AccessAgent problems is to increase the log level so that more debugging information can be produced.The log level is specified by the machine policy `pid_log_level`, which can be set through the registry entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\DeploymentOptions]"LogLevel"
```

Log level 3 is usually enough for most debugging purposes. If more detailed logs are required, the log level can be set to 4.

AccessAgent cryptoboxes

AccessAgent stores user and machine Wallets as hidden files in the `C:\Program Files\Encentuate\Cryptoboxes` folder. The machine Wallet at `C:\Program Files\Cryptoboxes\Wallets\machine.wlt` contains system policies and AccessProfiles downloaded from the current IMS Server. To view the Wallet files, make sure that Windows Explorer has been configured to *show hidden files and folders*. To refresh the user Wallets during testing or troubleshooting, delete the corresponding Wallet files in the folder `C:\Program Files\Encentuate\Cryptoboxes\Wallets`.

In the following steps that refresh the machine Wallet, the SOCIAccess service automatically replaces any deleted machine Wallet file, so deleting a folder (as with user Wallets) does not achieve the same result.

To refresh the machine Wallet, perform the following steps.

1. Log off AccessAgent (if logged on).
2. Kill AccessAgent processes: `AATray.exe`, `DataProvider.exe`, and `Sync.exe`.
3. Stop the SOCIAccess service by using the **`net stop sociaccess`** command.
4. Delete the machine Wallet.
5. Restart the machine.

Restarting the machine with a missing machine Wallet prompts AccessAgent to re-create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server.

Machine Wallet download problem

When a machine starts up with a missing machine Wallet, AccessAgent attempts to create the machine Wallet by downloading the latest policies and AccessProfiles from the current IMS Server. However, if the IMS Server is inaccessible, AccessAgent uses the policies and AccessProfiles specified in the following file:

`C:\Program Files\Encentuate\all_sync_data.xml.`

To confirm whether the machine Wallet has been downloaded correctly:

1. Run AccessStudio.
2. Load AccessProfiles from AccessAgent.
3. Click **sso_site_web_ims_admin** under AccessProfiles.

The machine Wallet is correct if the @domain field on the right panel is set to the IMS Server name. If the @domain field is `$hostname`, the machine Wallet has not been downloaded properly.

If AccessAgent cannot successfully download the policies and AccessProfiles from the IMS Server despite several manual synchronization attempts, you can edit the policies and AccessProfiles directly in the `all_sync_data.xml` file.

To refresh the machine Wallet, follow the steps in “AccessAgent cryptoboxes” on page 186.

For certain deployments, workstations can connect to the network only after a user logs on to Windows. Because AccessAgent has to download system data from the IMS Server during first startup after installation, other workstations will be unsuccessful in connecting at that time. For this reason, AccessAgent is inaccessible on first startup.

A workaround is for the first user to bypass the Tivoli Access Manager for Enterprise Single Sign-On logon process and log on to Windows directly. After that, subsequent users can log on normally by using the Tivoli Access Manager

for Enterprise Single Sign-On logon process. Another alternative is to include the IMS Server's latest `all_sync_data.xml` file in the installation package.

To include the `all_sync_data.xml` file in the installation package:

1. Launch AccessStudio.
2. Select **Tools** → **Backup System Data from IMS to File**.
3. Click **Backup**, and save it as `all_sync_data.xml` file.
4. Place `all_sync_data.xml` file in the `Config` folder of the AccessAgent installer package.

Synchronization with IMS Server

AccessAgent performs synchronization with the IMS Server periodically, according to the frequency specified by `pid_wallet_sync_mins`. Sometimes, invoking synchronization manually so the latest policies or AccessProfiles can be downloaded is useful, and is especially useful during troubleshooting or demonstrations.

To enable the AccessAgent, perform the following steps:

1. Right-click the option for **Synchronize with IMS**.
2. Set machine policy `pid_wallet_manual_sync_enabled` to 1, which can be set through the registry entry:

   ```
   [HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp]"WalletManualSyncEnabled"
   ```

Logon user interface failed to load

Upon startup, instead of EnGINA[2], the following error message appears:

```
Caption: User Interface Failure
Message: The Logon User Interface DLL xxx.dll failed to load…..
```

Either EnGINA has not been properly installed or the Winlogon GINA registry entry was not set correctly after AccessAgent was uninstalled.

To resolve the problem perform the following steps:

1. Restart the computer.
2. Go to Safe Mode by pressing F8 before Windows starts up.
3. Log on as an administrator.

[2] EnGINA is the Tivoli Access Manager for Enterprise Single Sign-On logon user interface.

4. Modify the following Windows registry value:

   `[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]"GinaDLL".`

5. If the value was `engina.dll`, EnGINA was probably not installed correctly and could not load. Change the value to `msgina.dll`. The default Windows Logon prompt will be displayed on the next startup.

   To use EnGINA again after fixing the problem, change the value to `engina.dll`.

AccessAgent does not display the correct domain

For this problem, we look at two separate cases:

- For IMS Server version 2.x

  When a user logs on, AccessAgent shows the display name of the authentication service specified by `pid_bind_auth_list` in the Domain field. To modify the displayed domain, use AccessStudio or the IMS Configuration Utility to modify the display name of the appropriate authentication service.

- For IMS Server version 3.x and later

  The policy `pid_bind_edir_list` replaces `pid_bind_auth_list`. AccessAgent shows the domains specified in the enterprise directory listed in `pid_bind_edir_list`.

Cannot return to EnGINA from Windows GINA

Users cannot return to EnGINA from Windows GINA by clicking **Cancel** if the following domain group policy is set to `Enabled`:

```
[Computer Configuration\Windows Settings\Security Settings\Local
Policies\Security Options]
   "Disable CTRL+ALT+DEL requirement for logon".
```

To fix this problem, set the value to `Disabled` or `Not Defined`.

Web automatic sign-on fails on Internet Explorer settings

Because of a Microsoft problem, Internet Explorer 5.5 with Service Pack 2 and Internet Explorer 6.0 without a Service Pack cannot be used with AccessAgent. Information is located at:

`http://support.microsoft.com/kb/316593`

Users have to upgrade their Internet Explorer to at least 6.0 with Service Pack 1.

Web automatic sign-on also fails if Internet Explorer has been configured to disable third-party browser extensions. To enable third-party browser extensions in Internet Explorer:

1. Go to **Tools** → **Internet Options** → **Advanced**.
2. Under the Browsing category, look for *Enable third-party browser extensions (requires restart)*. Mark the option and click **OK**.
3. Exit Internet Explorer and try Web automatic sign-on again.

Also possible is for certain spyware to automatically remove the Tivoli Access Manager for Enterprise Single Sign-On Browser Helper Object. For such cases, Web automatic sign-on might initially work, but subsequently it does not work. Install and run an anti-spyware software to clear all spyware in your machine before re-installing AccessAgent.

Automatic sign-on does not work properly for Windows applications

The required services might not have been registered properly during the AccessAgent installation. To register the required services:

1. Launch a command prompt.
2. Go to the Tivoli Access Manager for Enterprise Single Sign-On program directory:

   ```
   cd C:\Program Files\Encentuate
   ```

3. Execute the following commands:

   ```
   obsservice -service
   regsvr32 -i winssoagent.dll
   net start obsservice
   ```

Automatic sign-on does not work properly for Microsoft GINA

For IMS Server versions in the range of 3.1.1.6 - 3.1.7.1, the domain name must be regenerated for the authentication service representing the Windows credentials. When you configure an enterprise directory for an Active Directory server, the IMS Server automatically generates authentication services, one for each Active Directory domain.

To view the auto-generated authentication services in the IMS Configuration Utility, click **Authentication Services** in the left panel and select the authentication service from the drop-down list.

For an authentication service representing an Active Directory domain, two domain names are included in the Server locators to be used during injection:

- DNS domain name (for example, `test.ibm.com`)
- NETBIOS domain name (for example, `ibm_test`)

To perform automatic sign-on using the Microsoft GINA, ensure that the NETBIOS domain is the first item in the list.

Modification to Winlogon AccessProfile does not take effect

The latest AccessProfile of an application is loaded when the application process starts. Because the Winlogon process is only started on machine startup, restart the machine for the new Winlogon AccessProfile to take effect.

Application does not work properly after AccessAgent is installed

Certain Microsoft DLLs are used by AccessAgent when observing applications. If the DLL versions conflict with those used by an application, the application might not work correctly. To check for DLL conflicts:

1. Launch a command prompt.
2. Execute the following command:

   ```
   net stop obsservice
   ```

3. Launch the application and check whether the application is working properly.

You can check the application folder to see if it is carrying any Microsoft DLLs, which are usually named `ms*.dll` (for example, `msvcr70.dll`, `msvcp70.dll`).

A fix for the problem is to use the DLL redirection configuration suggested by Microsoft Dynamic-Link Library Redirection:

`http://msdn2.microsoft.com/en-us/library/ms682600.aspx`

Another possible fix is to replace the DLL carried by the application with a DLL that is compatible with AccessAgent. However, the application must also be compatible with the same DLL.

Cannot log on to Wallet after AccessAgent is installed

If you are using a version of AccessAgent earlier than 3.3.1.4, a problem prevents users from logging on if the machine Wallet is larger than 2 MB. This problem can happen if a large number of AccessProfiles exist.

When a user attempts to log on, the following error message is displayed:

```
You do not have a Wallet stored on this computer. However, you
cannot download your Wallet from IMS Server because network
connectivity is currently unavailable. Please try again later.
```

To resolve this problem, upgrade to AccessAgent version 3.3.1.4 or later. You can also reduce the number of AccessProfiles so the machine Wallet is smaller than 2 MB.

Note that the inability to log on may also be because of any of the problems listed in “Unable to connect to the IMS Server” on page 192.

Cannot log on to cached Wallets

If AccessAgent can log on when the IMS Server is online, but cannot log on to cached Wallets while the IMS Server is offline, the cached Wallets might be corrupted. For such cases, delete all cached user Wallets and try to log on again.

Enable the AccessAgent right-click option for Delete, which can be set through the registry entry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate\Temp]"WalletDeleteEnabled"
```

Downloading the IMS Server certificate

If configured properly, the AccessAgent installer should download the IMS Server certificate to the client PC. However, this download can fail if the client PC is offline or the IMS Server is not available at that time. The server certificate can be downloaded after installation through either of the following methods:

- Select **Start** → **All Programs** → **TAM E-SSO AccessAgent** → **Set IMS Server Location**.
- Run the following executable file:

  ```
  C:\Program Files\Encentuate\SetupCertDlg.exe executable.
  ```

Unable to connect to the IMS Server

If AccessAgent cannot connect to the IMS Server, it cannot perform certain operations, such as:

- Logging on to AccessAgent when no cached Wallet exists for the user
- Changing a Tivoli Access Manager for Enterprise Single Sign-On or USB Key password
- Registering a second factor
- Signing up users

The following situations can prevent AccessAgent from connecting to the IMS Server:

- The client machine is not connected to the network.
- The client machine has no network connectivity (or has lost connectivity) to the IMS Server. This could be because of an intervening firewall between the client machine and the IMS Server, or because of network configuration issues, such as DNS problems.
- The client machine has a personal firewall or anti-spyware that is blocking traffic from AccessAgent. To allow AccessAgent to contact the IMS Server while computer is locked, the personal firewall or anti-spyware must also not be blocking traffic from the `winlogon.exe` and `aatray.exe` files.
- The client machine does not have the IMS Server certificates installed, possibly because the client machine was offline during AccessAgent installation (see “Downloading the IMS Server certificate” on page 192).
- AccessAgent registry settings are corrupted or misconfigured (for example, AccessAgent is pointing to the wrong IMS Server).

Spontaneous termination of sync.exe

The following symptoms might show a problem with `sync.exe`:

- After the first reboot, EnGINA does not show up. Instead, it bypasses to Microsoft GINA.
- When logged on to Windows, the PC appears to be very slow. Stopping ObsService restores the computer to its original speed.
- The `sync.exe` file does not show up in the Windows Task Manager.
- After starting `sync.exe` manually, it shuts down within milliseconds.

These symptoms can be caused by anti-spyware, such as the LanDesk software monitoring tool (`SoftMon.exe`), which might have identified the process `sync.exe` to be a spyware or malware. The anti-spyware shuts down the process when it is detected. In the AccessAgent logs, `sync.exe` appears to be failing at different instances.

To remedy this problem, add `sync.exe` to the LanDesk software monitoring tool’s exclusion list. After making the settings, LanDesk ignores `sync.exe` and does not shut down the process. For other anti-spyware products, make the same changes to their exclusion lists.

Personal firewalls on private desktops

For AccessAgent installations on private desktops, personal firewalls can prevent users from logging on, and can cause slower Windows desktop

performance. If the user presses Ctrl+Alt+Del, the lock screen for private desktop might not appear and the computer may fail.

To resolve the problem, be sure that the personal firewall is configured properly before AccessAgent is installed. Set up the personal firewall to include AccessAgent components (for example, `SOCIAccess.exe`, `aatray.exe`) in the trust list. Refer to your personal firewall's documentation on including applications or components into the trust list.

6.4.4 Other issues

In this section, we describe problems that cannot be grouped into any of the previous sections.

AccessStudio logs

To troubleshoot AccessStudio problems, a useful approach is to view the log files in `C:\Program Files\Encentuate\AccessStudio\logs` folder. When reporting a problem, including a `.zip` file that contains the entire `C:\Program Files\Encentuate\AccessStudio\logs` folder is helpful. Provide the approximate local times when the events occurred.

Unable to log on to AccessAdmin

If a user cannot log on to AccessAdmin, check the following information:

- Make sure that the user has an administrator or help desk role.
- If the user is not using a USB Key, ensure that the user's Wallet is cached.
- Make sure that the machine Wallet has been downloaded properly (refer to "Machine Wallet download problem" on page 187).
- Make sure that the DNS name of the IMS Server does not contain the underscore character (see "Machine Wallet download problem" on page 187).
- Make sure that the URL of AccessAdmin is the same URL specified during IMS installation. To check the setting, go to the IMS Server page and double-click the lock icon to view the SSL certificate. The SSL certificate should list the exact host name that you have to use.

If you are using Windows 2003 Server and the home page of Internet Explorer starts up with the page `res://../hardAdmin.htm`, the Advanced Security Option might be enabled.

To set the home page to `res://../softAdmin.htm`, go to the Add/Remove programs menu in the Windows Control Panel and select to Add/remove Windows components. Remove the Internet Explorer *Enhanced Security Configuration*.

SOCIAccess.exe crash caused by RFID readers

Restart the machine if you experience a `SOCIAccess.exe` crash when unplugging and re-plugging RFID readers from RF Ideas. This issue is the result of some problems with the RFID reader drivers.

Do not unplug and re-plug the RFID reader while AccessAgent is still running.

Application is slower when automatic sign-on is enabled.

Certain applications might respond slower when automatic sign-on is enabled, or noticeable delays can occur before credentials are auto-filled or auto-captured. The reason might be because of the use of an inefficient signature comparison in the AccessProfile for the affected application. If a signature where `@title` is the only predicate checked for top level window (as shown in the following example), AccessAgent tries to retrieve the title of each top level window using Windows messages:

```
/child::wnd[@title="Logon"]
```

However, for some applications, many hidden top-level windows might be created during logon, and might take at least 0.5 seconds to respond to Windows messages. The response time in fetching the title of each window adds to the delay. For such cases, use more specific signatures to reduce the number of matching windows. For example, the `@class_name` predicate can be used in the signature to filter only windows of a certain class so that the title is fetched for fewer windows (fetching of class name does not require Windows messaging).

Missing labels in state engine view of AccessStudio

In some Windows 2000 machines, the state engine view of AccessStudio might show a graph with the states and connections without any labels. The names of the states, triggers, and actions appear to be missing. The reason is because of the Arial font not being supported on the machine. The workaround is to install the Arial font.

Back button does not work for AccessAdmin, AccessAssistant, and Web Workplace

The browser's Back button cannot be used when accessing AccessAdmin, AccessAssistant, and Web Workplace. AccessAssistant and Web Workplace are designed this way for security reasons, whereas AccessAdmin is designed this way because of certain implementation constraints.

GINA conflict with ThinkPad fingerprint software

On an IBM/Lenovo ThinkPad with a built-in fingerprint reader, EnGINA is not displayed during startup. Instead, the system fails. The reason might be because

the ThinkPad ThinkVantage fingerprint GINA (`vrlogin.dll`) conflicts with EnGINA.

As a solution, disable the ThinkVantage fingerprint GINA (**Start** → **ThinkVantage fingerprint** → **Control Center**) before installing AccessAgent. If AccessAgent is already installed, make sure that the following registry entry is set to blank:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Encentuate]"PrevGINA"
```

Performance data is not available in MOM reports

To resolve the problem of performance data not being available:

1. Open the MOM Administrator console.
2. Go to **Console Root** → **Microsoft Operations Manager** (**SERVER_NAME**) → **Administration** → **Computers** → **Agent-managed Computers**.
3. Right-click on the computer with the MOM agent installed, then select **Run** → **Attribute Discovery Now**.

Security logs are full

If the *security logs* are full, problems can occur both in RDP[3] connections to a private desktop machine, and also during the start-up of any shared workstation (shared desktop, private desktop, roaming desktop), if the auto-admin logon account is not an administrator account.

The security logs being full is a limitation that Windows imposes during logon and unlock.

Recovery workflows

Tivoli Access Manager for Enterprise Single Sign-On addresses various operational problems and their associated recovery workflows. The recovery scenarios especially address allowing access to their computer and applications when operational problems are encountered.

Note: The workflows might depend on whether IMS Server is accessible from AccessAgent (indicated as *online* or *offline*).

[3] Remote Desktop Protocol (RDP)

Refer to *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952 for the following topics:

- Recovery workflows for user issues, such as:
  - Forgotten password
  - Forgotten USB Key password
  - Forgotten or lost USB Key
  - Forgotten or lost RFID car
- Recovery workflows for computer issues
- Recovery workflows for server issues, such as:
  - IMS Server is unavailable
  - The IMS Server has crashed
  - The database server has crashed
- IMS keystore recovery

6.4.5 Documenting a PMR

This section provides instructions with check lists when a Problem Management Record (PMR) for IBM Tivoli Access Manager for Enterprise Single Sign-On must be opened. Depending on whether the problem exists in the AccessAgent of IMS Server site, different tasks should be performed.

Documentation of AccessAgent errors

The tasks differ slightly, depending on whether the error is reproducible or not.

Error is reproducible

If the error is reproducible, perform all of the tasks in the check list:

- ☐ Record the system time and date when the problem happened or when it is reproduced (very important).
- ☐ Take screen captures or record the exact text of any related error messages.
- ☐ Document the issue and steps to reproduce it and its effects upon the organization.
- ☐ Back up or delete all the logs in the AccessAgent directory (usually `C:\Program Files\Encentuate\logs`). For most development and testing, you may delete the logs. However, check with management if you are unsure.
- ☐ Reproduce the problem, documenting the exact actions taken.
- ☐ Compress all the logs in the AccessAgent directory immediately after the test is finished.

- ☐ Export the profiles through the **File** → **Save As** feature of AccessStudio.
- ☐ Export the system data from IMS through the **Tools** → **Backup System data to file** feature of AccessStudio, if applicable.
- ☐ Save Windows Event logs, if applicable.
- ☐ Open a PMR.
- ☐ Send all pertinent information to your IBM Support contact.

Error is not reproducible

If the error is not reproducible, perform all tasks in the following check list:

- ☐ Record the system time and date when the problem happened (very important).
- ☐ Take screen captures or record the exact text of any related error messages.
- ☐ Document the issue, the steps leading to the failure and its effects upon the organization.
- ☐ Compress all the logs in the AccessAgent directory (usually `C:\Program Files\Encentuate\logs`).
- ☐ Export the profiles through the **File** → **Save As** feature of AccessStudio.
- ☐ Export the system data from IMS through the **Tools** → **Backup System data to file** feature of AccessStudio, if applicable.
- ☐ Save Windows Event logs, if applicable.
- ☐ Open a PMR.
- ☐ Send all pertinent information to your IBM Support contact.

Documentation of IMS Server errors

Perform the following tasks if a problem exists with the IMS Server.

- ☐ Record the system time and date when the problem happened or when it is reproduced (very important).
- ☐ Take screen captures of any related error messages.
- ☐ Document the issue, the steps leading to the failure and its effects upon the organization.
- ☐ Compress all logs in the IMS Server Directory:

  ```
  C:\Encentuate\IMSServer.x.x.x\logs
  C:\Encentuate\IMSServer.x.x.x\ims\logs
  ```

- ☐ Export the profiles through the **File** → **Save As** feature of AccessStudio if applicable.

- ☐ Export the system data from IMS through the **Tools** → **Backup System data to file** feature of AccessStudio if applicable.
- ☐ Save Windows Event logs, if applicable.
- ☐ Open a PMR.
- ☐ Send all pertinent information to your IBM Support contact.

A

Sample questions

In this appendix, we provides sample questions for Test 000-020.

This appendix contains:

- “Questions” on page 202
- “Answers” on page 206

Questions

The following questions can assist you in studying for the certification test:

1. A customer has a Microsoft SQL Server 2005 database server and Windows 2003 Enterprise as their application server's operating system.

   Which task would be outside the scope of IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server's housekeeping functionality?

   a. Backup of the IMS database

   b. Periodic pruning of the Audit Logs in the database

   c. Backup of the operating system security event logs

   d. Backup of the IMS Configuration files located on the server

2. In which policy scope is the maximum number of concurrent users on a shared workstation defined?

   a. AD

   b. User

   c. System

   d. Machine

3. Which statement is true about a SQL Server database if it is to be used as the database for IBM Tivoli Access Manager for Enterprise Single Sign-On IMS Server?

   a. The database must be configured to use Case Sensitive collation and the SQL Server must be configured to use SQL Server Authentication.

   b. The database must be configured to use Case Insensitive collation and the SQL Server must be configured to use SQL Server Authentication.

   c. The IMS user for the database must be created before installation of IMS and the SQL Server must be configured to use Windows authentication only.

   d. The IMS user for the database must not be created before installation of IMS and the SQL Server must be configured to use Windows authentication only.

4. Which object does an authentication-service-group-link object connect an authentication-service-group to?
   a. An application
   b. A policy object
   c. An AccessProfile
   d. An authentication service
5. What is the main function of Web Workplace?
   a. To allow users to perform password self-service activities
   b. To enable single sign-on to applications through a Web browser
   c. To enable users to securely connect to a corporate network without requiring AccessAgent
   d. To provision credentials for Web applications, to enable single sign-on through AccessAgent
6. Which incoming ports must be opened on the IMS Server host for it to function properly if the default ports are used by the IMS Server?
   a. Port 80 only
   b. Port 443 only
   c. Port 80 and 443 only
   d. Port 25, 80, and 443 only
7. Which requirement can be met by setting up the IBM Tivoli Access Manager for Enterprise Single Sign-On Provisioning Agent?
   a. Provision an IBM Tivoli Access Manager for Enterprise Single Sign-On user account automatically when a corresponding account is created in AD.
   b. Revoke an IBM Tivoli Access Manager for Enterprise Single Sign-On user account when the corresponding account is deprovisioned in Active Directory (AD).
   c. Create or revoke an IBM Tivoli Access Manager for Enterprise Single Sign-On user account automatically when the corresponding AD account is provisioned or deprovisioned, respectively.
   d. Create or revoke an AD account automatically when the corresponding IBM Tivoli Access Manager for Enterprise Single Sign-On user account is provisioned or deprovisioned, respectively.

8. Which two groups of policies have machine policy scope? (Choose two.)
   a. Wallet policies
   b. Password policies
   c. AccessAudit policies
   d. Shared Workstation policies
   e. AccessAssistant and Web Workplace policies
9. The IBM Tivoli Access Manager for Enterprise Single Sign-On Help Desk role provides users that are assigned to this role the ability to perform help desk duties. What are these duties?
   a. View system and user logs, view system and machine policies, and modify user policies.
   b. Only revoke users signed up to the IBM Tivoli Access Manager for Enterprise Single Sign-On system.
   c. Perform password reset operations on behalf of a user, view system and machine policies, and modify user policies.
   d. Provide authorization codes for a user while the user is offline, view system and machine policies, and modify user policies.
10. What must an administrator consider if the IMS Server certificate is required to be recreated?
   a. The key length of the private key must be at least 1024 bytes.
   b. For security the certificate must not be a self-signed certificate.
   c. The certificate must be signed by a well-known Certificate Authority.
   d. The Common Name field of the certificate must match the fully qualified host name of the IMS Server.
11. An administrator has changed the IP address of the machine where the IMS is installed. Which file has to be modified to access the configuration utility as http://imsservername:8080/?
   a. ims.xml
   b. event.xml
   c. server.xml
   d. as_sync_data.xml

12. A workstation with radio frequency identification (RFID) authentication enabled is at the IBM Tivoli Access Manager for Enterprise Single Sign-On Graphical Identification and Authentication (GINA) screen; the machine is online. A user wants to log on but has forgotten his RFID card at home. Which three statements are true about recovery workflows for the user? (Choose three.)

    a. If password-only authentication is not allowed, the user answers previously set challenge questions to bypass the second factor requirement, given that self-service bypass of second factors is enabled.

    b. If password-only authentication is not allowed, the user calls help desk for an authorization code which is used to bypass the second factor requirement, but only if self-service bypass of second factors is enabled.

    c. If password-only authentication is not allowed, the user calls help desk for an authorization code which is used to bypass the second factor requirement, given that self-service bypass of second factors is disabled.

    d. If password-only authentication is not allowed, user answers previously set challenge questions to bypass the second factor requirement, irrespective of whether self-service bypass of second factors is enabled or disabled.

    e. If password-only authentication is allowed, the user logs on with user name and password only without using the user's RFID badge or having to bypass it by other means of authentication and irrespective of whether self-service bypass of second factors is enabled or disabled.

    f. If password-only authentication is allowed, the user logs on with user name and password only without using the user's RFID badge but only after correctly answering previously set challenge questions and given that self-service bypass of second factors is enabled.

Answers

The correct answers to the sample questions in this appendix are:

1. c
2. d
3. a
4. d
5. b
6. c
7. b
8. a, d
9. d
10. d
11. c
12. a, c, e

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this book.

IBM Redbooks

For information about ordering these publications, see “How to get Redbooks” on page 208. Note that some of the documents referenced here may be available in softcopy only.

- *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350
- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*, SG24-6014

Other publications

These publications are also relevant as further information sources:

- *IBM Tivoli Access Manager for Enterprise Single Sign-On User Guide Version 8.0.1*, SC23-9950
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Administrator Guide Version 8.0.1*, SC23-9951
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Deployment Guide Version 8.0.1*, SC23-9952
- *IBM Tivoli Access Manager for Enterprise Single Sign-On Help Desk Guide Version 8.0.1*, SC23-9953

Online resources

These Web sites are also relevant as further information sources:

- The IBM Tivoli Access Manager for Enterprise Single Sign-On Wiki provides best practices, education materials, example AccessProfiles, and other documents to enable and support IBM sales, Business Partners, practitioners and customers with developing AccessProfiles, deploying the product, and learning about the many capabilities of this solution.

  http://www.ibm.com/developerworks/wikis/display/tivoliaccessmanagerforesso/Home

- IBM Tivoli Access Manager for Enterprise Single Sign-On Information Center, (only available online as HTML version, either on the Tivoli publications Web site or through your local installation)

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/welcome.htm

How to get Redbooks

You can search for, view, or download Redbooks, Redpapers, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this Web site:

ibm.com/redbooks

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

Index

A

access control
  customization 46
AccessAdmin 35, 47, 50, 136
  challenge-response questions 150
  IMS Server configuration 83
  password self-service 150
  policy management 63
  troubleshooting 194
AccessAgent 34, 39, 57, 77–78
  architecture 42
  cached Wallet troubleshooting 192
  cryptobox 53, 186
  DLL version conflict 191
  installation 85
  local user session management 46
  log files 186
  log level 186
  observer agent 44
  observer module 43
  performance tuning 176
  Plug-In 45
  policy 165
  secure storage 53
  server mode 47
  SOAP API 58
  synchronization 78
  troubleshooting
    automatic sign-on 190
    domain name 189
    Internet Explorer 189
    machine Wallet 191
    upgrade 182
  unable to connect to IMS Server 192
  Wallet 78
AccessAssistant 138
AccessProfile 39, 44, 78, 157
  action 105
  advanced 89, 101, 157
  central administration 47
  configuration 88
  creating of 50
  machine Wallet 186
  shared desktop 46
  standard 89–90, 157
  state 104
  storage 58
  testing 160
  trigger 104
  Winlogon 191
AccessStudio 50, 77–78
  account data 107
  concepts 156
  data backup 161
  installation 87
  logging 194
  profiling 60
account
  data 106, 160
  data bag 108
action 105
Active Directory
  lookup-user 79
  Provisioning Agent 117
active proximity badge 144
ActiveCode 49
administration 25
Administrative Console
  installation 80
administrative user
  create 79
administrator log 163
advanced AccessProfile 89, 101, 157
  action 105
  state 104
  trigger 104
all_sync_data.xml 187
application object 159
ARFID
  authentication 144
audit 49, 151
  Identity Manager credentials 117
  log 166
  log file hashing 153
  management 47
  report 166
  security 52, 54

authentication 63
ActiveCode 49
ARFID 144
authorization code 145
central administration 47
customization 46
device manager 43, 64
factor 39, 54, 64
fingerprint 144
mobile active code 148
OTP token 142
RFID 142
security 52
service 107, 157–158
configuration 88
service group 108, 159
service policy 165
USB key 141
authorization code 64
authentication 145
automatic sign-on performance 195
availability 173

B

backup
database 162
backup password 64
behavioral state 44

C

CAPI certificate 184
certificate management 47
certification
benefits 3
checklist 5
IBM Professional Certification 2
Certified Deployment Professional 7
challenge-response questions 150
Citrix MetaFrame 121, 133
Citrix MetaFrame Presentation Server 39, 47
client-side components 78
communication
security 52–53
compliance
de-provisioning credentials 116
configuration 16
AccessProfile 88
authentication service 88
IMS Server 82–83
corporate security policy 35
credential
distribution 49–50, 115
process 67, 115
security 51
cryptobox 53, 186

D

data
expected volume 59
secure processing 52
synchronization 43
database 50
administrator 79
deployment 15
architecture 77
stages 37
directory 76
Directory Integrator 66
Directory Server
organization directory 114

E

education
for users 34
educational resources 28
enterprise authentication services 88
enterprise identity binding 112
expected data volume 59

F

fast user switching 46, 56
fingerprint authentication 144

G

GINA 39
Graphical Identification and Authentication
See GINA

H

hashing of log files 153
high availability 68, 70
housekeeping 152

I

IBM Certified Deployment Professional 7
IBM Professional Certification 2
IBM Tivoli Directory Integrator
  See Directory Integrator
IBM Tivoli Directory Server
  See Directory Server
IBM Tivoli Identity Manager
  See Identity Manager
identity binding 112
identity management 48
Identity Manager
  credential distribution 49–50, 115
  password updates 117
  workflow
    extension 65
identity wallet
  See Wallet
IMS
  auditing 49
  authentication 49
  Configuration Utility 135
    troubleshooting 184
  connector 47
  database 50, 58, 77–78
    backup 162
    housekeeping problems 185
    preparation 170
  identity management 48
  policy 49
  provisioning bridge 47
  Server 40, 47, 77–78
    AccessAdmin 136
    application certificate 184
    certificate download 192
    configuration 82–83, 112, 162
    console mode 185
    data backup 161
    diagnostics 185
    housekeeping 152
    installation
      troubleshooting 181
    logging 163, 184
    maintenance 162
    migration 167
    performance tuning 172
    policy synchronization 43
    secure storage 53
    synchronization troubleshooting 188
    system policy 186
    time synchronization 81
    troubleshooting 184
    unable to connect to AccessAgent 192
  SOAP API 47
installation 14
  AccessAgent 85
  AccessStudio 87
  Administrative Console 80
  troubleshooting 179

J

Java
  Observer module 86

K

key field 107

L

local user session management 46
log file hashing 153
log table pruning 185
logging
  AccessAgent 186
  IMS Server 163
logical components
  AccessAdmin 50
  AccessAgent 42
  AccessAgent Observer module 43
  AccessStudio 50
  auditing 49
  authentication 49, 63
  data synchronization 43
  identity management 48
  IMS database 50
  IMS Server 47
  provisioning bridge 50, 115
  self-service GUI 43
  session management 46
  Wallet Manager GUI 43
logon
  Mainframe/Host application 45
  Web application 45
  Windows application 45
logon user interface
  troubleshooting 188
log-signing 153

lookup-user 79, 82
password 80
loss management 47

M

machine policy 124
template 129, 137
machine Wallet 186
troubleshooting 187
Mainframe/Host application
logon 45
Microsoft Windows Server Terminal Services 39, 47
migration 167
mobile active code
authentication 148

N

Network Time Protocol 81

O

objectives
administration 25
configuration 16
deployment 15
for Test 934 9
installation 14
performance tuning 26
planning 9
problem determination 26
organization directory 113
OTP token
authentication 142
overview diagram 39

P

password 64
ActiveCode mechanism 49
backup 64
policy 54, 165
reset 64
reset strategy 35
self-service 150
challenge-response questions 150
synchronization 82, 114
updates by Identity Manager 117
performance
AccessAgent 176
IMS Server 172
performance tuning 26
personal authentication services 89
personal desktop 61
personal workstation 129
physical components
AccessAgent 57
IMS database 58
organization directory 113
pid_wallet_sync_mins 188
planning 9
policy
machine template 129, 137
management 83, 124, 164
password 54
priorities 165
storage 58, 77
synchronization 78
template 126
user template 127, 137
post-logon 44
pre-logon 44
prerequisites 8
private desktop 46, 61, 132
security 46
problem determination 26, 179
Problem Management Record
creation of 197
provisioning
credential distribution 49–50, 115
Provisioning Agent 117
provisioning bridge 47, 50, 67, 115
Java API 49

R

RADIUS API 58
Redbooks Web site 208
Contact us xi
remote access integration 120
reporting 151
repository 76
RFID
authentication 142
troubleshooting 182, 195
roaming desktop 46, 133
role assignment 122

S

scalability 68, 173
scenario
  deployment architecture 77
SCR certificate 184
second authentication factors 64
secret 64
secure storage 52
security
  AccessAgent 53
  audit 54
  authentication factors 54
  communication 53
  de-provisioning credentials 116
  IMS Server 53
  policy 35
security log
  troubleshooting 196
self-service
  challenge-response questions 150
  user interface 43
server-side components 78
session management 46
  for local user 46
SetupHlp.ini 85
shared desktop 46, 131
shared workstation 46, 61, 130
signature 91, 102, 160
site signature 102
SOAP API 47, 58
solution
  overview 35
solution design 36
standard AccessProfile 89–90, 157
state 104
state engine
  trigger 45
state machine 44
strong authentication 139
strong password 54
sync.exe
  program termination troubleshooting 193
synchronization
  of time 81
system log 163
system policy 124, 165, 186

T

target
  application 79
  audience 7
Test 934
  objectives 9
thin client 133
Tivoli Software Professional Certification 4
training information 29
trigger 104
troubleshooting 179
  AccessAdmin 194
  AccessAgent 186
    automatic sign-on 190
    cached Wallet 192
    DLL version conflict 191
    domain name 189
    Internet Explorer 189
    machine Wallet 191
    upgrade 182
  application certificate 184
  automatic sign-on performance 195
  IMS Configuration Utility 184
  IMS database 185
  IMS Server 184
    certificate download 192
    console mode 185
    synchronization 188
  installation 179
  logon user interface 188
  machine Wallet 187
  Problem Management Record 197
  RFID 182, 195
  security log 196
  sync.exe termination 193
  Winlogon AccessProfile 191

U

USB key
  authentication 141
user
  central administration 47
  credentials 40
  data storage 77
  education 34
  log 163
  policy template 127, 137
  repository 76

User Interface Failure 188
user policy 124

W

Wallet 40, 78, 116
  authentication policy 164
  cryptobox 186
  data synchronization 43
  Manager GUI 43
  policy 165
  secret 64
  troubleshooting 191–192
Web application
  logon 45
Web Workplace 109, 138
Windows
  application logon 45
  Graphical Identification and Authentication
    See GINA
  Terminal Services 39, 47
Winlogon AccessProfile 191
workflow
  action 45
  automation 46, 50
  custom action 45
  extension 65

X

XML
  Path Language 160
XPath 160

(0.2”spine)
0.17”<->0.473”
90<->249 pages

Certification Study Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0

Helps you achieve Tivoli Access Manager for Enterprise Single Sign-On certification

Explains the certification path and prerequisites

Includes sample test questions and answers

This IBM Redbooks publication is a study guide for the "IBM Certified Deployment Professional - IBM Tivoli Access Manager for Enterprise Single Sign-On V8.0" certification test, test number 000-020, and is meant for those who want to achieve IBM Certifications for this specific product.

The IBM Tivoli Access Manager for Enterprise Single Sign-On Certification, offered through the Professional Certification Program from IBM, is designed to validate the skills required of technical professionals who work with the implementation of the IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.0 product.

This book provides a combination of theory and practical experience needed for a general understanding of the subject matter. It also provides sample questions that will help in the evaluation of personal progress and provide familiarity with the types of questions that will be encountered in the exam.

This publication does not replace practical experience, and it is not designed to be a stand-alone guide for any subject. Instead, it is an effective tool which, when combined with education activities and experience, can be a very useful preparation guide for the exam.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks

SG24-7784-00 ISBN 0738433217