Note

Before using this information and the product it supports, read the information in "Notices" on page 103.

Edition notice

Note: This edition applies to version 6.0 of IBM Security Identity Manager (product number 5724-C34) and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright IBM Corporation 2012.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
Table of contents

Table list ........................................ V

About this publication .................. vii
Access to publications and terminology .......... vii
Accessibility ................................ viii
Technical training ........................ viii
Support information .................. viii

Chapter 1. Troubleshooting and support for IBM Security Identity Manager ........ 1
Techniques for troubleshooting problems .... 1
Searching knowledge bases ................ 3
Getting fixes ................................. 4
  Getting fixes from Fix Central ............... 4
Contacting IBM Support .................. 5
Exchanging information with IBM .......... 6
  Sending information to IBM Support .... 6
  Receiving information from IBM Support ... 7
Subscribing to Support updates .............. 7

Chapter 2. Introduction to troubleshooting .......... 9
Minimizing error conditions ................ 9
  Minimizing installation and configuration errors . 9
Minimizing product operation errors ....... 10
Troubleshooting installation problems ...... 11
  Installation errors .......................... 11
  Troubleshooting operational problems ...... 12

Chapter 3. Diagnostic tools .............. 15
Logs ........................................ 15
  Installation and initial configuration logs .. 15
  IBM Security Identity Manager operational logs 16
  Prerequisite product logs .................. 22
Traces ...................................... 24
  Server tracing ................................ 24
  Applet tracing ................................ 28
Diagnostic utilities .................. 29
  Diagnosing completed requests with the audit log .......... 29
  Viewing log file data ....................... 29
Performance and availability ........ 33
Forwarding IBM Security Identity Manager logging and tracing to WebSphere Application Server .... 34
Retrieving and analyzing problem determination data remotely .................. 35

Chapter 4. Troubleshooting installation and configuration problems ........ 37
Firewalls can block the IBM Security Identity Manager Server installation .......... 37
User IDs must be in the administrator group to start an installation ............... 37
Microsoft Windows Terminal Server License server prevents an IBM Security Identity Manager installation .................................................. 38
Middleware configuration utility fails to catalog LDAP database instance node ........ 38
Entries in the services file prevent reinstalling the DB2 Universal Database .......... 38
LDAP port value is already in use for an initial installation of IBM Security Identity Manager .......................... 39
Backspace key deletes characters (SUSE Linux only) .................. 39
Error messages do not display when using an emulator program to install IBM Security Identity Manager ............... 39
tzmappings: illegal format at near line 11 error message .................................. 40
Messaging engines do not start after installation ........................................ 40
The temp directory is not deleted after installation (Microsoft Windows only) ........ 40
A java.lang. exception occurs in a cluster environment .................................. 41
Cannot uninstall interim fixes or fix packs ........................................ 41
Cannot log on to the IBM Security Identity Manager Console .......................... 41

Chapter 5. Troubleshooting operating system problems ........ 43
Too many files open (UNIX and Linux) ........ 43

Chapter 6. Troubleshooting IBM Security Identity Manager Server problems ........ 45
ACI filter not working correctly when an account is created .................. 45
User accounts are included when performing a suspend, restore, or delete task .... 45
Warning messages not displayed during identity feed or reconciliation ........ 45
Changing the service name prevents viewing and performing actions on service requests .......... 46
Identity feed operation fails and returns an LDAP error .................. 46
Reconciliation operation fails with an out-of-memory error .......... 47
A request fails because one or more values cannot be changed ........ 47
Concurrent usage of IBM Security Identity Manager Server can affect changes to data .......... 48
All results from a large search operation are not displayed ................ 48
Users are deleted from default groups in identity feeds .......... 49
Restoring the system administrator account ........ 49
Logging on to IBM Security Identity Manager after stopping and starting the WebSphere Application Server Administrative Console .......... 49

© Copyright IBM Corp. 2012
### Table list

1. Installation log file names and directories .................................................. 16
2. Default property values ................................................................................. 19
3. Pattern letters for the formatter.dateFormat and formatter.timeFormat log properties ......................................................................................................................... 19
4. Sample patterns for timestamps by using the US locale ................................. 20
5. Logging components ....................................................................................... 26
6. Column names for query strings ..................................................................... 31
7. JLog levels ...................................................................................................... 34
8. Tuning the DB2 statement heap attribute ....................................................... 58
9. Running SAConfig .......................................................................................... 82
10. Credential vault server files to copy .............................................................. 84
11. Running SAConfig ....................................................................................... 92
12. Running SAConfig ....................................................................................... 92
13. Running SAConfig ....................................................................................... 93
14. Running SAConfig ....................................................................................... 93
15. Credential vault server files to copy .............................................................. 95
About this publication

*IBM Security Identity Manager Troubleshooting Guide* helps you understand, isolate, and resolve problems with IBM Security Identity Manager. The support section provides information about the tools and options that you can use to connect to the service and support organization. It includes general information about searching knowledge bases, getting fixes, and contacting IBM® support. The troubleshooting section describes the events that generate the problems, symptoms, environment, possible causes, and suggestions for recovery actions. It also contains information about where logs are stored and how to run traces.

Access to publications and terminology

This section provides:
- A list of publications in the IBM Security Identity Manager library
- Links to “Online publications.”
- A link to the “IBM Terminology website” on page viii.

IBM Security Identity Manager library

The following documents are available in the IBM Security Identity Manager library:

- *IBM Security Identity Manager Quick Start Guide*, CF3L2ML
- *IBM Security Identity Manager Product Overview Guide*, GC14-7692
- *IBM Security Identity Manager Planning Guide*, GC14-7694
- *IBM Security Identity Manager Installation Guide*, GC14-7695
- *IBM Security Identity Manager Configuration Guide*, SC14-7696
- *IBM Security Identity Manager Administration Guide*, SC14-7701
- *IBM Security Identity Manager Troubleshooting Guide*, GC14-7702
- *IBM Security Identity Manager Error Message Reference*, GC14-7393
- *IBM Security Identity Manager Database and Directory Server Schema Reference*, SC14-7395
- *IBM Security Identity Manager Glossary*, SC14-7397

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager Information Center

IBM Security Information Center
The http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp site displays an alphabetical list of and general information about all IBM Security product documentation.

IBM Publications Center
The http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss site offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

Accessibility
Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the topic "Accessibility features for IBM Security Identity Manager" in the IBM Security Identity Manager Reference Guide.

Technical training
For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information
IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

IBM Security Identity Manager Troubleshooting Guide provides details about:
• What information to collect before contacting IBM Support.
• The various methods for contacting IBM Support.
• How to use IBM Support Assistant.
• Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The Community and Support tab on the product information center can provide additional support resources.
Chapter 1. Troubleshooting and support for IBM Security Identity Manager

To isolate and resolve problems with your IBM products, you can use the troubleshooting and support information. This information contains instructions for using the problem-determination resources that are provided with your IBM products.

This section includes the following topics.
- How to identify the source of a problem.
- How to gather diagnostic information.
- Where to get fixes.
- Which knowledge bases to search, so you can resolve problems.
- What diagnostic information the service technicians need to address a problem when you contact IBM Support.

Techniques for troubleshooting problems

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. Certain common techniques can help with the task of troubleshooting.

The first step in the troubleshooting process is to describe the problem completely. Problem descriptions help you and the IBM technical-support representative know where to start to find the cause of the problem. This step includes asking yourself basic questions:
- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When starting to describe a problem, the most obvious question is “What is the problem?” This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:
- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?
Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one platform or operating system, or is it common across multiple platforms or operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multisite installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration; many problems can be traced back to incompatible levels of software that are not intended to run together or have not been fully tested together.

When does the problem occur?

Develop a detailed timeline of events leading up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you need to look only as far as the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being performed?
- Does a certain sequence of events need to happen for the problem to occur?
- Do any other applications fail at the same time?
Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might have occurred around the same time, the problems are not necessarily related.

**Can the problem be reproduced?**

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Consequently, problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, recreate the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be recreated on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be recreated by running a single command, a set of commands, or a particular application?

**Searching knowledge bases**

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

**About this task**

You can find useful information by searching the information center for IBM Security Identity Manager. However, sometimes you need to look beyond the information center to answer your questions or resolve problems.

**Procedure**

To search knowledge bases for information that you need, use one or more of the following approaches:

- **Search for content by using the IBM Support Assistant (ISA).**
  ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the [ISA website](#).

- **Find the content that you need by using the IBM Support Portal.**
  The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the [demo videos](#) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.

- **Search for content about IBM Security Identity Manager by using one of the following additional technical resources:**
Getting fixes

A product fix might be available to resolve your problem.

**About this task**

**Procedure**

To find and install fixes:
1. Obtain the tools required to get the fix.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.
5. Subscribe to receive weekly email notifications about fixes and other IBM Support information.

**Getting fixes from Fix Central**

You can use Fix Central to find the fixes that are recommended by IBM Support for a variety of products, including IBM Security Identity Manager. With Fix Central, you can search, select, order, and download fixes for your system with a choice of delivery options. A IBM Security Identity Manager product fix might be available to resolve your problem.

**About this task**

**Procedure**

To find and install fixes:
1. Obtain the tools that are required to get the fix. If it is not installed, obtain your product update installer. You can download the installer from Fix Central. This site provides download, installation, and configuration instructions for the update installer.
2. Select IBM Security Identity Manager as the product, and select one or more check boxes that are relevant to the problem that you want to resolve. For details, see: http://www.ibm.com/systems/support/fixes/en/fixcentral/help/faq_sw.html.

3. Identify and select the fix that is required.

4. Download the fix.
   a. Open the download document and follow the link in the “Download Package” section.
   b. When downloading the file, ensure that the name of the maintenance file is not changed. This change might be intentional, or it might be an inadvertent change that is caused by certain web browsers or download utilities.

5. Apply the fix.
   a. Follow the instructions in the “Installation Instructions” section of the download document.
   b. For more information, see the “Installing fixes with the Update Installer” topic in the product documentation.

6. Optional: Subscribe to receive weekly email notifications about fixes and other IBM Support updates. See “Subscribing to Support updates” on page 7.

**Contacting IBM Support**

IBM Support provides assistance with product defects, answers FAQs, and helps users resolve problems with the product.

**Before you begin**

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM maintenance contract name, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the “Software Support Handbook”.

For information about the types of available support, see the Support portfolio topic in the Software Support Handbook.

**Procedure**

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. See the Contacting IBM Support topic in the Software Support Handbook. For more information, see the Getting IBM support topic in the Software Support Handbook.

2. Gather diagnostic information.

3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):
     a. Download and install the ISA tool from the ISA website. See www.ibm.com/software/support/isa/.
     b. Open ISA.
     c. Click Collection and Send Data.
     d. Click the Service Requests tab.
e. Click **Open a New Service Request**.

Using ISA in this way can expedite the analysis and reduce the time to resolution.

- Online through the **IBM Support Portal**. You can open, update, and view all of your service requests from the **Service Request** portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the **Directory of worldwide contacts** web page. You can also see the **Contacts** page in the **Software Support Handbook**.

**Results**

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution. See “Exchanging information with IBM.”

**Exchanging information with IBM**

To diagnose or identify a problem, you might need to provide IBM Support with data and information from your system. In other cases, IBM Support might provide you with tools or utilities to use for problem determination.

**Sending information to IBM Support**

To reduce the time that is required to resolve your problem, you can send trace and diagnostic information to IBM Support.

**Procedure**

To submit diagnostic information to IBM Support:

1. Open a problem management record (PMR).
2. Collect the diagnostic data that you need. Diagnostic data helps reduce the time that it takes to resolve your PMR. You can collect the diagnostic data manually or automatically:
   - Collect the data manually.
   - Collect the data automatically.
3. Compress the files by using the .zip or .tar file format.
4. Transfer the files to IBM. You can use one of the following methods to transfer the files to IBM:
   - **IBM Support Assistant**
   - **The Service Request tool**
   - Standard data upload methods: FTP, HTTP
   - Secure data upload methods: FTPS, SFTP, HTTPS
   - Email

All of these data exchange methods are explained on the **IBM Support website**.
Receiving information from IBM Support

Occasionally an IBM technical-support representative might ask you to download diagnostic tools or other files. You can use FTP to download these files.

Before you begin

Ensure that your IBM technical-support representative provided you with the preferred server to use for downloading the files and the exact directory and file names to access.

Procedure

To download files from IBM Support:

1. Use FTP to connect to the site that your IBM technical-support representative provided and log in as anonymous. Use your email address as the password.
2. Change to the appropriate directory:
   a. Change to the /fromibm directory.
      
   
   cd fromibm
   b. Change to the directory that your IBM technical-support representative provided.
      
   cd nameofdirectory
3. Enable binary mode for your session.

   binary
4. Use the get command to download the file that your IBM technical-support representative specified.

   get filename.extension
5. End your FTP session.

   quit

Subscribing to Support updates

To stay informed of important information about the IBM products that you use, you can subscribe to updates.

About this task

By subscribing to receive updates about IBM Security Identity Manager, you can receive important technical information and updates for specific IBM Support tools and resources. You can subscribe to updates by using one of two approaches:

RSS feeds

For information about RSS, including steps for getting started and a list of RSS-enabled IBM web pages, visit the IBM Software Support RSS feeds site.

My Notifications

With My Notifications, you can subscribe to Support updates for any IBM product. My Notifications replaces My Support, which is a similar tool that you might have used in the past. With My Notifications, you can specify that you want to receive daily or weekly email announcements.

You can specify what type of information you want to receive (such as publications, hints and tips, product flashes (also known as alerts), downloads, and drivers). My Notifications enables you to customize and
categorize the products about which you want to be informed and the delivery methods that best suit your needs.

**Procedure**

To subscribe to Support updates:

2. Sign in using your IBM ID and password, and click Submit.
3. Identify what and how you want to receive updates.
   a. Click the **Subscribe** tab.
   b. Select the appropriate software brand or type of hardware.
   c. Select one or more products by name and click **Continue**.
   d. Select your preferences for how to receive updates, whether by email, online in a designated folder, or as an RSS or Atom feed.
   e. Select the types of documentation updates that you want to receive, for example, new information about product downloads and discussion group comments.
   f. Click **Submit**.

**Results**

Until you modify your **RSS feeds** and **My Notifications** preferences, you receive notifications of updates that you have requested. You can modify your preferences when needed (for example, if you stop using one product and begin using another product).

**Related information**

- [IBM Software Support RSS feeds](https://www.ibm.com)
- Subscribe to My Notifications support content updates
- My Notifications for IBM technical support
- My Notifications for IBM technical support overview
Chapter 2. Introduction to troubleshooting

Problem determination is the process of determining why a product does not function as it is designed to function.

This guide provides the following information:
- Resources and techniques for identifying and resolving problems with IBM Security Identity Manager deployments.
- Information about how to resolve errors caused by improper setup, installation, configuration, and operation procedures.
- Steps and tools for gathering detailed trace information for determining the source of problems that cannot be resolved through routine investigation.

To resolve a problem with IBM Security Identity Manager, distinguish between the expected product response and the actual response.

Most problems are preceded by symptoms, such as:
- An error message that is logged during installation
- An unanticipated error message that is displayed in the console
- Slow response intervals during normal processing

When you see a symptom, you might take one or both of the following actions to isolate the symptom and resolve the problem:
- Interpret a message about the symptom and make a minor adjustment
- Use special tools to isolate the symptom

Minimizing error conditions

The following conditions can cause errors and unanticipated results.
- Product prerequisites that are not installed or used
- Installation and configuration steps that are not followed
- Product usage guidelines and procedures that are not followed

These errors and unanticipated results occur primarily when the product is installed, configured, and used for the first time. As you become familiar with the features and behavior of the product, such errors can be reduced. The following sections make reference to information in the product library that help minimize errors and ensure successful installation, configuration, and operation of the software.

Minimizing installation and configuration errors

This section summarizes steps you can take before installing the product that minimize errors.

Checking product requirements

Ensure that you meet hardware and software requirements before you begin the installation prevents many errors. The IBM Security Identity Manager Information Center lists the requirements.

Confirm the following information before you begin the installation:
• Ensure that the system meets the minimum hardware requirements.
• Consider a system that meets the higher hardware requirements when using the product to manage thousands of users. See the Performance Tuning Guide.
• Review the Before you begin section in the Installation and Configuration Guide. The guide provides tips that can help you avoid problems during the installation and configuration process.
• Minimize product operation errors. For more information, see “Minimizing product operation errors.”

Checking requirements when installing IBM Security Identity Manager Server and one or more middleware products
You must meet hardware and software requirements for IBM Security Identity Manager Server and associated middleware products to prevent errors. The IBM Security Identity Manager Information Center lists the requirements.

Before you install IBM Security Identity Manager Server and one or more required middleware products:
• Find the following information in the product information center:
  – Product and prerequisite software requirements. Some required fix packs are in the IBM Security Identity Manager Server installation package.
  – Product limitations and workarounds.
  – Latest information about known problems.
  – Changes to information in the product library.
• Review the Installation and Configuration Guide. The guide provides tips that can help you avoid problems during the installation and configuration process.

Errors can occur for the following reasons:
• User error in specifying values during the installation and configuration process.
• Preinstalled middleware might not be configured for IBM Security Identity Manager Server.
• Existing settings might conflict with IBM Security Identity Manager requirements. Settings include items such as administrator IDs and port values.

Minimizing product operation errors
Preventing product operation errors contributes to a successful and more efficient installation.

To prevent product operation errors, use the following resources:
• Review the IBM Security Identity Manager Information Center that lists the supported components.
• Review the “Troubleshooting” topics that describe the known problems for these components:
  – Operating system
  – Application server, such as the WebSphere® Application Server
  – IBM Security Identity Manager Server
  – Database server
  – Directory server and directory integrator, such as the IBM Tivoli® Directory Integrator Server
  – Adapters
Troubleshooting installation problems

This section describes basic steps for troubleshooting the various stages of installation and configuration.

Installation errors

Use the installation package to selectively install the IBM Security Identity Manager Server and the required middleware. You also can use it to install the fix packs, which upgrade the associated product to the required software level.

To install one or more products selectively, you must run the installation program for each product you are installing.

*IBM Security Identity Manager Information Center* provides websites for accessing the libraries of associated products. For more information about any failures with those products, see the installation, configuration, and troubleshooting guides that are associated with them.

Deployment and configuration errors

This section describes how to respond to errors that occur during installation.

Do the following actions to respond to errors that occur during installation.

* Read the message text to determine the source of the problem. Depending on the type of error, the error message might be posted in the installation program window or in a command window. If the error is severe, detailed information is entered in a log file. See [Logs](#) for information about the logs created during installation.

* Correct the cause of any errors described in the error message information and try the installation again. Installation errors are also described in the *IBM Security Identity Manager Server Installation and Configuration Guide*.

* If you cannot resolve all the errors, see [Chapter 1, “Troubleshooting and support for IBM Security Identity Manager,”](#) on page 1 for instructions on obtaining help.
WebSphere Application Server deployment and configuration errors
Use the WebSphere log file to view deployment and configuration errors for the administrative console.

IBM Security Identity Manager is deployed and configured as a WebSphere enterprise application. Deployment and configuration messages are written to the WebSphere Application Server Administrative Console. The administrative console logs installation information in the WebSphere log file listed in Table 1 on page 16.

Database errors
You must create a database, such as example, DB2®, before you start the IBM Security Identity Manager installation program.

The DBConfig utility configures the IBM Security Identity Manager database and tables. You can run this utility as part of the installation program or as a stand-alone program after the installation. If you run DBConfig as a stand-alone program, you must start the IBM Security Identity Manager Server again.

Database installation and configuration processing messages are logged in the database log file that is listed in Table 1 on page 16.

For more information, see the IBM Security Identity Manager Server Installation Guide.

Directory server errors
A directory server, for example, IBM Tivoli Directory Server, stores current information that is used by IBM Security Identity Manager to manage identities. IBM Tivoli Directory Server must be installed and operational before the IBM Security Identity Manager schema can be set up.

The ldapConfig utility sets up the schema and default data entries for IBM Security Identity Manager. You can run this utility as part of the installation program or as a stand-alone program after the installation. If you run ldapConfig as a stand-alone program, you must start the IBM Security Identity Manager Server again.

Directory server installation and configuration processing information is logged in the directory server log file that is listed in Table 1 on page 16.

For additional information, see the IBM Security Identity Manager Server Installation Guide.

Troubleshooting operational problems
Information about the various components that process requests and operations is in the log files for the IBM Security Identity Manager Server.

You can use the information in the various logs to determine how a request was handled. In addition, if backend processing occurs in the database or directory server that is related to the problem, the logs associated with these servers can also contain important diagnostic information. Messages are logged by the IBM Security Identity Manager Server components while handling a task. The IBM Security Identity Manager messages include the CTGIM prefix. For more information about messages, see the IBM Security Identity Manager Messages Guide.
For information about the various log files and available tools for diagnosing IBM Security Identity Manager problems, see Chapter 3, “Diagnostic tools,” on page 15.
Chapter 3. Diagnostic tools

This chapter describes the log, trace, and other diagnostic utilities that capture and record details about how the program operates. The records help locate the product or component from which an error originates. Trace information can isolate the entry and exit points of interfaces in a specific product.

Logs

IBM Security Identity Manager logs system events during specific transactions. Log files contain levels of information about the product processes. Log files also include information about other software that is used to complete a task. Use the information in log files to facilitate isolating and debugging system problems.

IBM Security Identity Manager uses the IBM Logging Toolkit for Java™ or JLog libraries for message logging and trace facilities. JLog is a set of Java packages for incorporating message logging in Java applications. JLog can extend the logging functions to suit your needs. You can also use JLog to set logging configuration by using the enRoleLogging.properties file instead of programming it. You can change the logging configuration without stopping IBM Security Identity Manager.

Installation and initial configuration logs

This section describes IBM Security Identity Manager Server installation and initial configuration logs.

Table 1 on page 16 contains a list of the log files that are created during the installation and configuration of the IBM Security Identity Manager Server and the prerequisite products.

Log files are created for the following tasks:

- Running the product installation program.
- Installing the IBM Security Identity Manager uninstallation program.
- Installing required middleware products:
  - WebSphere Application Server
  - A directory server, such as IBM Tivoli Directory Server
  - A database, such as DB2 Universal Database™
- Running the middleware configuration utility.
- Installing IBM Security Identity Manager, which also includes:
  - IBM Security Identity Manager Server
  - IBM Security Identity Manager IBM Tivoli Directory Server-based posix adapter profiles
  - Database configuration program, such as DBConfig
  - Directory server configuration program, such as ldapConfig

In Table 1 on page 16, the system temp directory is designated with the TEMP environment variable. The TEMP variable is either %temp% or %tmp% for Microsoft Windows systems. UNIX and Linux use /tmp as the temp directory.
Table 1. Installation log file names and directories

<table>
<thead>
<tr>
<th>File names</th>
<th>Description and location</th>
</tr>
</thead>
<tbody>
<tr>
<td>log.txt</td>
<td>Installation log file for WebSphere Application Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Location:</strong> The system temp directory.</td>
</tr>
<tr>
<td>isim_install.stdout</td>
<td>Standard out and error log files for IBM Security Identity Manager.</td>
</tr>
<tr>
<td>isim_install.stderr</td>
<td><strong>Location:</strong> The system root directory.</td>
</tr>
<tr>
<td>dbConfig.stdout</td>
<td>Install log files for IBM Security Identity Manager.</td>
</tr>
<tr>
<td>ldapConfig.stdout</td>
<td><strong>Location:</strong> ISIM_HOME\install_logs.</td>
</tr>
<tr>
<td>itim_installer_debug.txt</td>
<td>Install log files for IBM Security Identity Manager.</td>
</tr>
<tr>
<td>runConfigFirstTime.stdout</td>
<td><strong>Location:</strong> ISIM_HOME\install_logs.</td>
</tr>
<tr>
<td>runConfig.stdout</td>
<td></td>
</tr>
<tr>
<td>setupEnrole.stdout</td>
<td></td>
</tr>
<tr>
<td>StartStopWas.stdout</td>
<td></td>
</tr>
<tr>
<td>itim_install_activity.log</td>
<td>The Tivoli Common Directory is the central location for all serviceability-related files, such as log files and first-failure capture data.</td>
</tr>
<tr>
<td></td>
<td><strong>Location:</strong> ISIM_HOME\install_logs.</td>
</tr>
<tr>
<td>trace.log</td>
<td>Trace or message log files for IBM Security Identity Manager.</td>
</tr>
<tr>
<td>msg.log</td>
<td><strong>Location:</strong> TIVOLI_COMMON_DIRECTORY\CTGIM\logs\</td>
</tr>
<tr>
<td>cfg_itim_mw.log</td>
<td>The middleware configuration utility log file.</td>
</tr>
<tr>
<td></td>
<td><strong>Location:</strong> The system temp directory.</td>
</tr>
</tbody>
</table>

**IBM Security Identity Manager operational logs**

Operational log files contain information about processing activities. These activities are associated with the communication between the IBM Security Identity Manager Server and other applications.

This section describes:
- Message, security, and trace logs. Use these logs to troubleshoot errors that occur during IBM Security Identity Manager operations.
- Logging options. You can set logging options for all IBM Security Identity Manager logs. You can also set options for each type of logging activity.

**Default location of operational logs**

The operational log files are in subdirectories of the TIVOLI_COMMON_DIRECTORY\CTGIM directory. The default location of the log files depends on the operating system.

**Microsoft Windows systems**

C:\Program Files\IBM\tivo...\common\CTGIM\logs

**UNIX and Linux systems**

/opt/IBM/tivo.../common/CTGIM/logs
You can change the default location of the log files during the initial installation and configuration. After installation and configuration, you can edit the enRoleLogging.properties file to change the location. The default location of the enRoleLogging.properties file depends on the operating system.

**Microsoft Windows systems**
C:\Program Files\IBM\isim\data

**UNIX and Linux systems**
/opt/IBM/isim/data

IBM Security Identity Manager logging properties describes the general logging options and the options for each type of logging activity.

**Management of size and number of files**

You can configure the size and number of log files in the enRoleLogging.properties file. The handler.file.maxFileSize property changes the size of all files. The handler.file.log_type.maxFiles property sets the number of files that are maintained for each type of log before discarding records.

After a set of log files reaches the specified capacity for a single file, the newest data replaces the oldest log data. To maintain a longer activity history, you can specify the number of multiple log files to keep before data is discarded. The following algorithm manages the number of log files:

1. If the log_type.log file reaches 100 KB, the data is moved to the log_type1.log file.
2. If the size of log_type.log reaches 100 KB again:
   - Data from log_type1.log is moved to log_type2.log
   - Data from log_type.log is moved to log_type1.log
3. The next time log_type.log reaches a size of 100 KB, step 2 is repeated until the maximum number of specified files is reached. If the maximum file limit is reached before the last set of data is moved, the data from log_typeX.log is discarded.

**Log format**

The message, security, and trace logs are formatted in XML. IBM Security Identity Manager provides a viewer for viewing the log contents. You can view them as plain text or as formatted HTML. See Viewing log file data.

**Message log (msg.log)**

The message log contains IBM Security Identity Manager messages. The product generates messages during processing. Messages are presented when you log on to the IBM Security Identity Manager Server and perform operations. IBM Security Identity Manager messages are identified by the CTGIM prefix.

The message log is turned on by default. You can configure:
- When message collection starts and stops.
- The level of data that is collected
- The log file size.
After the message log file reaches its capacity, data is overwritten. The newest data replaces the oldest log data. To maintain a longer history of messages, you can create multiple message log files. When the msg.log file is full, data is moved to another file.

For information about message descriptions and configuring the message log, see the Messages Guide.

**Security log (access.log)**
The security log contains information about authentication requests, also called attempts.

The security log is turned on by default.

You can configure:
- When to start and stop collecting security data.
- The level of data that is collected.
- The log file size.

For information about configuring the size and contents of the security log, see "IBM Security Identity Manager logging properties."

**Trace log (trace.log)**
Trace logs capture information about the operating environment when the software fails to operate as intended.

For more information about capturing trace data, see "Traces" on page 24.

For information about configuring the size and contents of the trace log, see "Configuring the server trace log" on page 24.

**Adapter logs**
Adapters provide an interface between a managed resource and the IBM Security Identity Manager Server.

The adapter logs and log locations depend on the type of adapter. IBM Security Identity Manager has the following types of adapters:

**Adapter Development Kit (ADK)-based adapters**
Each ADK adapter has its own log file. The log file is in the adapter log directory. The log file name is `adapternameAgent.log`. For example, the Microsoft Windows Local adapter is `WinLocalAgent.log`.

**IBM Tivoli Directory Integrator Server-based adapters**
There is a log file for all adapters that are installed on one instance. The log file is in the log directory of the adapters solution directory. The log file name is `ibmdi.log`.

For more information about adapters and adapter log configuration and settings, see the “Installation Guide” and the “Configuration Guide” on the IBM Security Identity Manager Information Center.

**IBM Security Identity Manager logging properties**
Use a text editor to set logging properties in the `enRoleLogging.properties` file.
The default location of the enRoleLogging.properties file depends on the operating system.

**Microsoft Windows systems**

    C:\Program Files\IBM\isim\data

**UNIX and Linux systems**

    /opt/IBM/isim/data

**Global logging properties:**

The global logging properties apply to all IBM Security Identity Manager logs.

The following values are the default property values:

**Table 2. Default property values**

<table>
<thead>
<tr>
<th>Property value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logger.refreshInterval=300000</td>
<td>Specifies the number of milliseconds between checking for updates to enRoleLogging.properties. The default value is 5 minutes (300,000 milliseconds).</td>
</tr>
<tr>
<td>handler.file.fileDir=</td>
<td>Specifies the location of the log files. The default location of the log files depends on the operating system. Microsoft Windows systems: C:\Program Files\IBM\tivo....\common\CTGIM\logs UNIX and Linux systems: /opt/IBM/tivo../../common/CTGIM/logs</td>
</tr>
<tr>
<td>handler.file.maxFileSize=1024</td>
<td>Specifies the maximum size for each log file in KB.</td>
</tr>
<tr>
<td>formatter.dateFormat=&quot;yyyy.MM.dd&quot;</td>
<td>Specifies the date and time formats for the timestamps in the log records.</td>
</tr>
<tr>
<td>formatter.timeFormat=&quot;HH:mm:ss:SSS&quot;</td>
<td>Specifies the date and time formats for the timestamps in the log records.</td>
</tr>
</tbody>
</table>

Use the ASCII letters described in **Table 3** to specify a different date and time format.

**Table 3. Pattern letters for the formatter.dateFormat and formatter.timeFormat log properties**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Presentation type*</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>G (uppercase)</td>
<td>Era designator</td>
<td>Text</td>
<td>AD</td>
</tr>
<tr>
<td>y (lowercase)</td>
<td>Year</td>
<td>Number</td>
<td>1996</td>
</tr>
<tr>
<td>M</td>
<td>Month in the year</td>
<td>Text and number</td>
<td>July and 07</td>
</tr>
<tr>
<td>d</td>
<td>Day in the month</td>
<td>Number</td>
<td>10</td>
</tr>
<tr>
<td>E</td>
<td>Day of the week</td>
<td>Text</td>
<td>Tuesday</td>
</tr>
<tr>
<td>D</td>
<td>Day in the year</td>
<td>Number</td>
<td>189</td>
</tr>
<tr>
<td>F</td>
<td>Day of the week in the month</td>
<td>Number</td>
<td>2 (second Wednesday in July)</td>
</tr>
<tr>
<td>w</td>
<td>Week in the year</td>
<td>Number</td>
<td>27</td>
</tr>
<tr>
<td>W</td>
<td>Week in the month</td>
<td>Number</td>
<td>2</td>
</tr>
<tr>
<td>h</td>
<td>Hour in AM or PM</td>
<td>Number (1-12)</td>
<td>12</td>
</tr>
</tbody>
</table>
Table 3. Pattern letters for the formatter.dateFormat and formatter.timeFormat log properties (continued)

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
<th>Presentation type*</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>Hour in the day</td>
<td>Number (0-23)</td>
<td>0</td>
</tr>
<tr>
<td>m</td>
<td>Minute in the hour</td>
<td>Number</td>
<td>30</td>
</tr>
<tr>
<td>s</td>
<td>Second of the minute</td>
<td>Number</td>
<td>55</td>
</tr>
<tr>
<td>S</td>
<td>Millisecond</td>
<td>Number</td>
<td>987</td>
</tr>
<tr>
<td>a</td>
<td>AM or PM marker</td>
<td>Text</td>
<td>PM</td>
</tr>
<tr>
<td>k</td>
<td>Hour in the day</td>
<td>Number (1-24)</td>
<td>24</td>
</tr>
<tr>
<td>K</td>
<td>Hour in AM or PM</td>
<td>Number (0-11)</td>
<td>0</td>
</tr>
<tr>
<td>z</td>
<td>Time zone</td>
<td>Text</td>
<td>Pacific Standard Time</td>
</tr>
<tr>
<td>'</td>
<td>(single quotation mark)</td>
<td>Escape for text</td>
<td>Delimiter</td>
</tr>
<tr>
<td>&quot;</td>
<td>(2 single quotation marks)</td>
<td>Single quotation mark</td>
<td>Literal</td>
</tr>
</tbody>
</table>

* The number of pattern letters that are specified determines whether a short form or long form is used in the timestamp.

The number of pattern letters determines the format.

**Text**

Specifies whether to use full or short form. If four or more pattern letters are specified, the full form is used. If less than four letters are specified, the short form is used if a short form exists.

**Number**

Specifies the minimum number of digits to be included. Shorter numbers are padded with zeros to the specified number of digits. Year (y) is handled differently; if 2 y's are specified, the year is shortened to two digits.

**Text and number**

Specifies whether to use text or a number. If 3 or more pattern letters are specified, text is used, otherwise a number is used. Any characters in the pattern that are not in the ranges of a through z and A through Z are treated as quoted text. For example, characters such as the semicolon (:), period (.), blank space, number sign (#), and at sign (@) are included in the output text even though they are not delimited with single quotation marks.

A pattern that contains an invalid pattern letter generates an error during formatting or parsing.

Table 4 provides examples of user-defined date and time patterns.

Table 4. Sample patterns for timestamps by using the US locale

<table>
<thead>
<tr>
<th>Sample pattern</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>formatter.dateFormat=&quot;yyyy.MM.dd G&quot;</td>
<td>1996.07.10 AD at 15:08:56 PDT</td>
</tr>
<tr>
<td>formatter.timeFormat=&quot;'at' hh:mm:ss z&quot;</td>
<td></td>
</tr>
<tr>
<td>formatter.dateFormat=&quot;EEE, MMM d, &quot;yy&quot;</td>
<td>Wed, July 10, '96</td>
</tr>
<tr>
<td>formatter.timeFormat=&quot;h:mm a&quot;</td>
<td>12:08 PM</td>
</tr>
<tr>
<td>formatter.timeFormat=&quot;hh 'o'clock' a, zzzz&quot;</td>
<td>12 o'clock PM, Pacific Daylight Time</td>
</tr>
</tbody>
</table>
Table 4. Sample patterns for timestamps by using the US locale (continued)

<table>
<thead>
<tr>
<th>Sample pattern</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>formatter.timeFormat=&quot;K:mm a, z&quot;</td>
<td>0:00 PM, PST</td>
</tr>
<tr>
<td>formatter.dateFormat=&quot;yyyyy.MMMMM.dd GGG&quot;</td>
<td></td>
</tr>
<tr>
<td>formatter.timeFormat=&quot;hh:mm aaa&quot;</td>
<td>1996.July.10 AD 12:08 PM</td>
</tr>
</tbody>
</table>

Message logging options:

The properties in this section apply to IBM Security Identity Manager messages.

The property values are the defaults:

**logger.msg.logging=true**
- Turns message logging on or off.
  - true  Turns on message logging.
  - false Turns off message logging.

**handler.file.msg.fileName=msg.log**
- Specifies the name of the message log file.

**logger.msg.level=INFO**
- Specifies the message logging level.
  - INFO  Captures all message types such as informational, warning, and error messages.
  - WARN  Captures warning and error messages.
  - ERROR Captures only error messages.

**handler.file.msg.maxFiles=5**
- Specifies the maximum number of message log files to keep before log records start to be discarded.

Security logging options:

The properties in this section apply to attempts to authenticate with IBM Security Identity Manager Server.

The property values are the defaults:

**logger.msg.com.ibm.itim.security.logging=true**
- Turns security logging on or off.
  - true  Turns on security logging.
  - false Turns off security logging.

**handler.file.security.fileName=access.log**
- Specifies the name of the security log file. The default location of the log files depends on the operating system.

**Microsoft Windows systems**
- handler.file.security.fileDir=C:\Program Files\IBM\tivo..\.\common\CTGIM\logs
- Specifies the location of the security log file.
UNIX and Linux systems

    handler.file.security.fileDir=/opt/IBM/tivo../../common/CTGIM/logs

Specifies the location of the security log file.

**logger.msg.com.ibm.itim.security.logChoice=failure**

Specifies the types of attempts that are logged.

- **failure**
  - Log only failed attempts.
- **success**
  - Log only successful attempts.
- **both**
  - Log both failed and successful attempts.

**handler.file.security.maxFiles=10**

Specifies the maximum number of security log files to keep before log records are discarded.

Displaying the logged data in Common Base Event format:

The JLog toolkit provides a Common Base Event (CBE) formatter.

To show the logged data in CBE format, modify the property value.

In `formatter.PDXML.className=com.ibm.itim.logging.LogXMLFormatter` file:

<table>
<thead>
<tr>
<th>Change this value</th>
<th>com.ibm.itim.logging.LogXMLFormatter</th>
</tr>
</thead>
<tbody>
<tr>
<td>To this value</td>
<td>com.ibm.log.CBE101Formatter</td>
</tr>
</tbody>
</table>

The updated logged data in CBE format is `formatter.PDXML.className=com.ibm.log.CBE101Formatter`.

**Prerequisite product logs**

This section describes logging for the middleware products. It also provides links to websites for more information about logging.

**WebSphere Application Server logs**

These log files provide troubleshooting information about communication between the IBM Security Identity Manager Server and WebSphere Application Server.

The default directory location of the WebSphere Application Server log files depends on the operating system.

**Microsoft Windows systems**

    WAS_HOME\profiles\default\logs\server_name

For example: `C:\Program Files\IBM\WebSphere\AppServer\profiles\default\logs\server1`

**UNIX and Linux systems**

    WAS_HOME/profiles/default/logs/server_name

For example: `/opt/IBM/WebSphere/AppServer/profiles/default/logs/server1`
IBM Tivoli Directory Server logs
These logs provide information about the installation and communications between the IBM Security Identity Manager Server and the IBM Tivoli Directory Server.

Note: If you use a directory server other than IBM Tivoli Directory Server, see its product documentation for logging information.

The IBM Tivoli Directory Server documentation provides more information about IBM Tivoli Directory Server logs.

The default directory location of the installation logs depends on the operating system.

Microsoft Windows systems

\texttt{ITDS\_HOME\var}

For example: \texttt{C:\Program Files\IBM\LDAP\V6.3\var}

UNIX and Linux systems

\texttt{ITDS\_HOME\var}

For example: \texttt{/opt/ibm/ldap/V6.3}

The default directory location of the operational logs depends on the operating system.

Microsoft Windows systems

\texttt{ITDS\_instance\_HOME\logs}

For example: \texttt{C:\idsslapd-ldapdb2\logs}

UNIX and Linux systems

\texttt{ITDS\_instance\_HOME\logs}

For example: \texttt{/home/ldapdb2/idsslapd-ldapdb2/logs}

IBM Tivoli Directory Integrator log
The \texttt{ibmdi.log} file reports information about the communications between the IBM Security Identity Manager Server and the agentless adapters. The IBM Security Identity Manager Server UNIX and Linux adapter and the IBM Security Identity Manager Server LDAP adapter are agentless adapters.

The default directory location of these log files depends on the operating system.

Microsoft Windows systems

\texttt{ITDI\_HOME\solDir}

For example: \texttt{C:\Program Files\IBM\isim\itdi\home\solDir}

UNIX and Linux systems

The solution directory for IBM Tivoli Directory Integrator

For example: \texttt{/opt/IBM/isim/itdi/solDir}

You can specify logging properties for IBM Tivoli Directory Integrator.

For more information about the agentless adapters and about setting logging properties, see the installation and configuration guides on the \textit{IBM Security Identity Manager Information Center}.

Database server logs
DB2 Universal Database records database requests in its own log files.
Note: If you use a database server other than DB2 Universal Database, see its product documentation for logging information.

You specify the location of these files when you install the database server.

By default, the DB2 Universal Database log files are in the DB_INSTANCE_HOME directory.

**Microsoft Windows systems**

C:\Program Files\IBM\SQLLIB\DB2

**UNIX and Linux systems**

/home/db2inst1

---

## Traces

Trace data provides in-depth processing information to help you focus on a particular area that you suspect is causing a problem. Trace data is more complex and detailed than message data.

By default, the trace log is set on to collect the minimum amount of information. The minimum level reduces the impact of capturing and recording data on the overall performance of IBM Security Identity Manager. The higher the level of tracing, the greater the potential impact on server performance.

IBM Security Identity Manager Server provides both [Server trace](#) and [Applet trace](#).

You can configure the following items:

- When to start and stop collecting data
- The level of detailed data that is collected
- The log file size

You can also use the `runConfig` configuration tool to change the level of the trace logging. For more information about the `runConfig` tool, see the installation and configuration guides on the [IBM Security Identity Manager Information Center](#).

### Server tracing

The trace facility provides methods to capture information about the IBM Security Identity Manager Server internal operations. The trace log information is designed so support personnel can trace a problem to its source and determine why an error occurred.

### Configuring the server trace log

Configuration properties for the server trace log are stored in the `enRoleLogging.properties` file. The default directory location of `enRoleLogging.properties` depends on the operating system.

**Microsoft Windows systems**

C:\Program Files\IBM\isim\data

**UNIX and Linux systems**

/opt/IBM/isim/data

Changes take effect when the IBM Security Identity Manager Server checks for updates. You can specify the update interval in the properties file. The following properties values are the defaults:
logger.trace.logging=true
  Turns trace logging on or off.
  true  Turns on trace logging.
  false Turns off trace logging.

logger.trace.level=DEBUG_MIN
  Specifies the trace logging level.
  DEBUG_MIN
    Records the least amount of information. (Default)
  DEBUG_MID
    Records a greater amount of trace information for debugging.
  DEBUG_MAX
    Records the maximum amount of trace information. This level has
    the greatest impact on server performance. Use this level only to
    narrow down a problem to a specific component. Then reset this
    parameter back to DEBUG_MIN or DEBUG_MID.

  Note: Use the runConfig command to also change the trace logging level.

handler.file.trace.maxFiles=10
  Specifies the maximum number of trace log files to keep before log records
  are discarded.

logger.trace.com.ibm.itim.component_name
  Defines the IBM Security Identity Manager component you want to trace.
  For information about this property, see "Specifying trace contents."

Specifying trace contents

You can specify the level of trace data that is collected either during installation or
at a later time. The enRoleLogging.properties file contains properties that are
related to what data to collect and the level of collection.

About this task

The default directory location of enRoleLogging.properties depends on the
operating system.

Microsoft Windows systems
  C:\Program Files\IBM\isim\data

UNIX and Linux systems
  /opt/IBM/isim/data

The setting of these values is suggested by support personnel when debugging a
problem. Under normal operating conditions, the default settings are appropriate.
The more data that is collected, the greater the impact is to system performance.

Table 5 on page 26 shows logging components and descriptions.
<table>
<thead>
<tr>
<th>Component</th>
<th>To troubleshoot problems related to:</th>
</tr>
</thead>
<tbody>
<tr>
<td>logger.trace.com.ibm.itim.adhocreport.level</td>
<td>Running operations under the Report tab. For example, synchronizing data or designing and running reports.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.adhocreport.changelog.level</td>
<td>Synchronizing data incrementally.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.apps.level</td>
<td>Validating business logic. For example, password synchronization and account compliance about provisioning policy.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.apps.ejb.adhocreport.level</td>
<td>Synchronizing data. For example, retrieving data from IBM Security Identity Manager LDAP and storing it in a database.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.authentication.level</td>
<td>Logging on to or authenticating with IBM Security Identity Manager.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.authorization.level</td>
<td>Validating and checking of ACIs for a logged-in user.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.common.level</td>
<td>Validating input per defined FORM constraints or schema.</td>
</tr>
<tr>
<td>logger.com.ibm.itim.script.level</td>
<td>Evaluating the scriptframework, which replaces FESI. For example, the workflow engine script node and service selection policy script.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.fesixtensions.level</td>
<td>Evaluating a FESI script. For example, the workflow engine script node and service selection policy script.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.mail.level</td>
<td>Sending mail from IBM Security Identity Manager. For example, notifications.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.messaging.level</td>
<td>Sending messages to queues.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.dataservices.model.level</td>
<td>Performing LDAP Directory server operations. For example, updating a person.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.passworddelivery.level</td>
<td>Clearing expired password transactions.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.policy.level</td>
<td>Running and validating policies. For example, password and provisioning policies.</td>
</tr>
<tr>
<td>Component</td>
<td>To troubleshoot problems related to:</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.remoteservices.level</td>
<td>Running operations for remote resources and interpreting the response. For example, HR feed, reconciliation and account operations.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.report.level</td>
<td>Not used.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.security.level</td>
<td>Not used.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.scheduling.level</td>
<td>Running scheduled operations such as those that the user scheduled to run at a later date.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.systemConfig.level</td>
<td>Running LDAP/DB upgrade/config utilities.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.util.level</td>
<td>Sharing utility classes across various components. For example, acquiring and releasing database connections from the WebSphere Application Server Java Database Connectivity (JDBC) connection pool.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.webclient.level</td>
<td>Navigating from one page to another, input validation, or display problems.</td>
</tr>
<tr>
<td>logger.trace.com.ibm.itim.workflow.level</td>
<td>Running workflows. This operation includes providing information about running a specific node in the workflow definition. For example, the input and output of a node and the transition from one node to the other.</td>
</tr>
</tbody>
</table>

JLog supports a hierarchical set of named objects that inherit properties from their ancestors. A period (.) separates each level of the hierarchy. The highest level of the hierarchy is shown first. For example, the logger.trace.com.ibm.itim.workflow object in the workflow inherits properties that are not explicitly defined at the workflow level from logger.trace.com.ibm.itim, logger.trace.com.ibm,
logger.trace.com, and logger.trace. Because of the inheritance characteristic, the default tracing level can be defined at the top of the hierarchy, which is logger.trace.

The following definition sets a specific level of tracing for a component:

```
logger.trace.com.ibm.itim.component_name.level=tracing_level
```

where `component_name` is the name of the component and `tracing_level` is the level of tracing to use for that component.

Setting a tracing level for a component overrides the inherited level of tracing. For example, `logger.trace.com.ibm.tim.workflow.level=DEBUG_MAX` traces the workflow component at the maximum level of detail, that is, DEBUG_MAX. This setting continues tracing all other levels at the minimum level, that is, DEBUG_MIN.

**Procedure**

1. Open the `enRoleLogging.properties` file.
2. Locate the section that contains the `logger.trace.com.ibm.itim.component_name` property.
   Use this property to define each component. The following statement defines tracing for the workflow component:
   ```
   # logger.trace.com.ibm.itim.workflow.level=DEBUG_MIN
   ```
3. To start tracing for a component, remove the comment characters (#) from the appropriate statement.
4. Set the level of tracing as DEBUG_MIN, DEBUG_MID, or DEBUG_MAX.

**Applet tracing**

The applet tracing is separate from IBM Security Identity Manager Server tracing. All applet tracing information goes to the applet console window on the client.

**Viewing applet tracing**

You can view the applet trace data on the IBM Security Identity Manager Console.

Two properties in the `enRoleLogging.properties` file control applet tracing.

```
logger.trace.com.ibm.itim.applet.logging
```

Starts and stops applet tracing.
```
true  Turns on trace logging.
false Turns off trace logging.
```

```
logger.trace.com.ibm.itim.applet.level=DEBUG_MIN
```

Specifies the trace logging level.
```
DEBUG_MIN  Records the least amount of information. (Default)
DEBUG_MID  Records a greater amount of trace information for debugging.
DEBUG_MAX  Records the maximum amount of trace information. This level has the greatest impact on server performance. Use this level only to narrow down a problem to a specific component. Then reset this parameter back to DEBUG_MIN or DEBUG_MID.
```
Procedure
1. Open the Java plug-in control panel while the applet is being loaded on the client browser.
2. Click Show Console.

Diagnostic utilities
This section describes tools that assist with diagnosing problems.

Diagnosing completed requests with the audit log
Use the audit log to diagnose completed requests with adapter communication, policy enforcement, and request approval. For example, you request a new account on a service, but the related adapter is not running. Then the audit log shows that the connection was refused.

About this task
A user in the IBM Security Identity Manager administrator group can view all available audit records on the system.

For information about setting the audit log option, see the IBM Security Identity Manager Information Center.

Procedure
1. From the navigation tree, click Home to display the Home page.
2. Take one of the following actions to display the View All Requests page:
   • Under Common Tasks, click View All Requests.
   • From the navigation tree, select View Requests > View All Requests.
3. On the View All Requests page, select a request type from the list.
4. Select a time interval.
5. Optional: Click the icon next to More Search Criteria to filter by status, date request was completed or submitted, service, user, or request ID.
6. Click Search Requests after you specify the search criteria.
7. To view the details of a request, click the request type. The information about the request is read-only.
8. On the View All Requests page, complete these steps:
   a. View the submitted details of the request in the Process Details section.
   b. Click the icon next to the data type in the Process Data section to view current data or changes.
   c. Click to expand the root structure to view additional details about the request type.
9. Click Close to close the View All Requests page.
10. Click Close when you are done reviewing the requests.

Viewing log file data
IBM Security Identity Manager provides a viewer for formatting and viewing logs. The logs are formatted in XML, but the viewer displays the files in HTML or plain text. The viewer can filter message and trace records for various fields in the records. For example, you can filter for timestamp, severity, thread identifier, and component ID. You can combine different types of logs and view them together.
To create a single file for presentation, run the `viewer` command from a command-line window. The filepath of the `viewer` command depends on the operating system.

**Microsoft Windows systems**

   `ISIM_HOME\bin\logviewer\viewer.bat`

**UNIX and Linux systems**

   `ISIM_HOME/bin/logviewer/viewer.sh`

The `viewer` command uses the following syntax and parameters:

`viewer [{-qstring | -f filename}] [-soutput_type] [-h] input_data`

- **-qstring**
  Defines a string that determines the content and format of the output. You can define this string on the command line or in a file. For more information, see "Query strings."

- **-f filename**
  Defines a file that contains a string and determines the content and format of the output. You can define this string on the command line or in a file. For more information, see "Query strings."

- **soutput_type**
  Specifies that the output format of the data is in plain text or HTML. The default value is HTML. The HTML output is in UTF-8 encoding. The text format is in the default encoding of the console where the command is issued. Specify text or HTML. Use the standard redirection symbol (>) to direct the output to a file instead of `stdout`. See "Generating the contents of the access.log in HTML format" on page 32.

- **-h**
  Prints the usage statement, which is the command syntax.

- **input_data**
  Specifies one or more input files to be viewed. If you specify multiple input files, the log and trace records are merged based on the timestamp of each record.

**Query strings**

The query string has the following format. If you do not specify a query string, the default query string is "select default where true". This section describes these values.

"select column_name [,column_name]
where filter_predicate"

- **column_name**
  Specify one or more column headers for the trace output. A timestamp is displayed in the output for each record.

  - **all**
    Includes all columns.

  - **default**
    Specifies to include the default columns. The default columns are Time, Severity, MessageId, LogText, Server, ProductID, Component, and ProductInstance.

**Names of columns**

[Table 6 on page 31] lists the valid column names. The column names are not case-sensitive. Some column names might not apply to a particular log.
If a description or example is not listed, review the actual log to determine whether the column applies to the troubleshooting task.

Table 6. Column names for query strings

<table>
<thead>
<tr>
<th>Column name</th>
<th>Column type</th>
<th>Description or example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client</td>
<td>String</td>
<td>Client identifier</td>
</tr>
<tr>
<td>Component</td>
<td>String</td>
<td>Component identifier</td>
</tr>
<tr>
<td>CorrelationId</td>
<td>String</td>
<td>Correlation identifier</td>
</tr>
<tr>
<td>Element</td>
<td>String</td>
<td>Message or trace</td>
</tr>
<tr>
<td>Exception</td>
<td>String</td>
<td>Error identifier</td>
</tr>
<tr>
<td>LogAttribs</td>
<td>Key value pairs</td>
<td>The attributes of a log</td>
</tr>
<tr>
<td>LogText</td>
<td>String</td>
<td>The description of the log attribute</td>
</tr>
<tr>
<td>MessageId</td>
<td>String</td>
<td>Unique identifier of the message</td>
</tr>
<tr>
<td>Millis</td>
<td>Long integer</td>
<td>Time in milliseconds</td>
</tr>
<tr>
<td>Principal</td>
<td>String</td>
<td>An ID that has the necessary permissions. For example, server1.</td>
</tr>
<tr>
<td>Process</td>
<td>String</td>
<td>The process number.</td>
</tr>
<tr>
<td>ProductId</td>
<td>String</td>
<td>The three-letter identifier</td>
</tr>
<tr>
<td>ProductInstance</td>
<td>String</td>
<td>The installed server instance name</td>
</tr>
<tr>
<td>Server</td>
<td>String</td>
<td>Name or IP address</td>
</tr>
<tr>
<td>ServerFormat</td>
<td>String</td>
<td>For example, TCP/IP</td>
</tr>
<tr>
<td>Severity</td>
<td>String</td>
<td>Severity level of the log record</td>
</tr>
<tr>
<td>SourceFile</td>
<td>String</td>
<td>Name of the source file where the event was generated</td>
</tr>
<tr>
<td>SourceLine</td>
<td>String</td>
<td>Line number where the event was generated</td>
</tr>
<tr>
<td>SourceMethod</td>
<td>String</td>
<td>Name of the method that generated the event</td>
</tr>
<tr>
<td>Thread</td>
<td>String</td>
<td>The thread number. For example, 3928.</td>
</tr>
<tr>
<td>Time</td>
<td>String</td>
<td>Localized time. For example,</td>
</tr>
<tr>
<td>TraceLevel</td>
<td>String</td>
<td>Trace level of the log file. For example, MIN.</td>
</tr>
</tbody>
</table>

*filter Predicate*

Determines which records are in the output. The *filter Predicate* value can contain conditional operators, pattern operators, Boolean operators, or the true keyword.

The true keyword indicates that filtering is disabled and all log records are included in the output.
Conditional operators include:
• = (equal)
• > (greater than)
• < (less than)
• >= (greater than or equal to)
• <= (less than or equal to)
• <> (not equal to)

You can also use the MATCH pattern operator in the conditional selection of the where clause. Use MATCH to select log or trace records with regular expression syntax. Put strings with special characters in the regular expression in quotation marks.

Boolean operators include the following operators in the format of (expression) operator (expression):
• OR
• AND

"Displaying only the server and productID columns of the log records" on page 33 includes a Boolean expression with the MATCH pattern operator and the AND and OR Boolean operators.

Log viewer syntax examples

The examples show various uses of the viewer command:

**Generating the contents of the access.log in HTML format**

It uses the default columns. It redirects the output to the logout.html file in the local directory.

**Microsoft Windows systems**
viewer -shtml "C:\Program Files\IBM\tivo..\.\common\CTGIM\logs\access.log" > logout.html

**UNIX and Linux systems**
./viewer.sh -shtml "/opt/IBM/tivo../../common/CTGIM/logs/access.log" > logout.html

**Displaying the filtered contents of the trace.log file in text format**

It displays all fields with a correlation identifier of 12. The output goes to stdout.

**Microsoft Windows systems**
viewer -q"select all where CorrelationId = 12" -stext "C:\Program Files\IBM\tivo..\.\common\CTGIM\logs\trace.log"

**UNIX and Linux systems**
./viewer.sh -q"select all where CorrelationId = 12" -stext "/opt/IBM/tivo../../common/CTGIM/logs/trace.log"

**Displaying the filtered contents of the trace.log file in text format**

It displays all records with a timestamp less than 1007067881373. The output goes to stdout.
Microsoft Windows systems
viewe-r q"select all where Millis < 1007067881373" -stext
"C:\Program Files\IBM\tivo...\..\common\CTGIM\logs\trace.log"

UNIX and Linux systems
./viewer.sh -q"select all where Millis < 1007067881373" -stext
"/opt/IBM/tivo...\..\common/CTGIM/logs/trace.log"

Displaying only the server and productID columns of the log records

Records are displayed only if the Boolean expression evaluates to TRUE. The output is sent to stdout. You must use parentheses with Boolean operators to indicate the order of operator evaluation. Input is merged from the specified files: msg1.log, msg2.log, and msg3.log.

Note: Parentheses determine how the Boolean expression is evaluated. The Boolean expression evaluates to TRUE only if both of these statements are true:

- The text in the messageid column contains message IDs in the range CTGIMA010 to CTGIMA045
- The Server column contains the string test1, or the severity column contains the string ERROR.

Microsoft Windows systems
viewe-r q"select server,ProductId where
(messageid MATCH 'CTGIMA0[10-45]' )
AND ((server = 'test1')
OR (severity = 'ERROR'))"
"C:\Program Files\IBM\tivo...\..\common\CTGIM\logs\msg1.log
C:\Program Files\IBM\tivo...\..\common\CTGIM\logs\msg2.log
C:\Program Files\IBM\tivo...\..\common\CTGIM\logs\msg3.log"

UNIX and Linux systems
./viewer.sh -q"select server,ProductId where
(messageid MATCH 'CTGIMA0[10-45]' )
AND ((server = 'test1')
OR (severity = 'ERROR'))"
"/opt/IBM/tivo...\..\common/CTGIM/logs/msg1.log
/opt/IBM/tivo...\..\common/CTGIM/logs/msg2.log
/opt/IBM/tivo...\..\common/CTGIM/logs/msg3.log"

Filtering with a log attribute

You can filter with a log attribute that has the name FNG and a value of 123. The output is sent to stdout.

Microsoft Windows systems
viewe-r q"select default where LogAttribs MATCH 'FNG=123''
"C:\Program Files\IBM\tivo...\..\common\CTGIM\logs\trace.log"

UNIX and Linux systems
./viewer.sh -q"select default where LogAttribs MATCH 'FNG=123''
"/opt/IBM/tivo...\..\common/CTGIM/logs\trace.log"

Performance and availability

The Performance Tuning Guide provides information about setting the parameters used to tune IBM Security Identity Manager, IBM Tivoli Directory Server, and database servers. These parameters can improve the performance of your environment.
**Forwarding IBM Security Identity Manager logging and tracing to WebSphere Application Server**

You can optionally forward IBM Security Identity Manager logging and tracing to WebSphere Application Server.

**About this task**

You can forward the logging and tracing information to the WebSphere Application Server by changing the `enRoleLogging.properties` file. The JLog levels are mapped to WebSphere Application Server logging levels or Java logging levels. The following table shows this mapping.

<table>
<thead>
<tr>
<th>JLog levels</th>
<th>Maps to...</th>
<th>Java logging levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERROR</td>
<td>=&gt;</td>
<td>SEVERE</td>
</tr>
<tr>
<td>WARN</td>
<td>=&gt;</td>
<td>WARNING</td>
</tr>
<tr>
<td>INFO</td>
<td>=&gt;</td>
<td>INFO</td>
</tr>
<tr>
<td>DEBUG_MIN</td>
<td>=&gt;</td>
<td>FINE</td>
</tr>
<tr>
<td>DEBUG_MID</td>
<td>=&gt;</td>
<td>FINER</td>
</tr>
<tr>
<td>DEBUG_MAX</td>
<td>=&gt;</td>
<td>FINEST</td>
</tr>
</tbody>
</table>

**Procedure**

1. Add the `logger.forwardToWAS=true` property in `enRoleLogging.properties`.

   **Note:** This property is for UI-tier logging. UI-tier uses Java logging API directly. When this property does not exist or is set to `false`, UI-tier attaches a custom handler to route the UI-tier logging to JLog. Otherwise, the logging is routed to the WebSphere Application Server automatically because it has a handler attached to the Java root logger.

2. Modify the `handler.file.className=com.ibm.log.FileHandler` property in `enRoleLogging.properties` as follows:

   ```
   handler.file.className=com.ibm.itim.logging.JSR47Handler
   ```

   **Note:** After the handler is set to use the `JSR47Handler`, any format settings in `enRoleLogging.properties` are ignored. The formatting uses the WebSphere Application Server logging and tracing settings.

3. Turn on the fine-level tracing for IBM Security Identity Manager components.

   a. Access the WebSphere Application Server Administrative Console.
   b. Navigate to Troubleshooting > Logging and Tracing > server name > Diagnostic Trace > Change Log Detail Levels.
   c. Click the Runtime tab so that you do not need to restart the WebSphere Application Server or clusters.
   d. Add `com.ibm.itim.*=fine` to the Components field:

      ```
      *=info: com.ibm.itim.*=fine
      ```
   e. Restart the IBM Security Identity Manager application. Use the WebSphere Application Server Administrative Console.
Results

IBM Security Identity Manager now forwards logging and tracing information to the WebSphere Application Server.

- $WAS_HOME/profiles/profilename/logs/activity.log contains all the runtime messages in CBE binary format.
- $WAS_HOME/profiles/profilename/logs/server name/trace.log contains trace information.

What to do next

View the run time messages stored in the activity.log on the WebSphere Application Server Administrative Console. Select Troubleshooting > Runtime Messages.

Viewing the trace file on the WebSphere Application Server Administrative Console

You can view the trace file on the WebSphere Application Server Administrative Console.

Procedure

1. Select Troubleshooting > Logging and Tracing > server name > Diagnostic Trace Service.
2. Select the Runtime tab.
3. Select View.

What to do next

After the initial setup, you can change trace levels for any component. Change the enRoleLogging.properties file and WebSphere Application Server. For example, the following changes enable FINER tracing on the workflow component:

- For the IBM Security Identity Manager enRoleLogging.properties file:
  
  logger.trace.com.ibm.itim.workflow.level=DEBUG_MID

- For the WebSphere Application Server Administrative Console:
  
  **info:com.ibm.itim.**fine:com.ibm.itim.workflow.**finer

Retrieving and analyzing problem determination data remotely

You can see tracing and logging information from a remote system by setting up and using remote retrieval.

About this task

If logging or tracing is forwarded to the WebSphere Application Server, you can view the information from the administrative console. You can start the administrative console from any remote system.

If logging and tracing uses the default setting, you can use the IBM HTTP server. IBM Security Identity Manager uses this server to publish the tracing and logging information in the Tivoli Common Directory.

Procedure
1. Define the logging directory as an alias on the IBM HTTP server.
   The logging directory is \textit{tivoli\_common\_directory}/CTGIM. All directories and files are under CTGIM.
   a. Open \texttt{HTTP\_SERVER\_HOME/conf/httpd.config} in edit mode.
   b. Search for \texttt{Aliases}.
   c. In the \texttt{Aliases} section, add an alias. For example:
      \begin{verbatim}
      Alias /CTGIM tivoli_common_directory/CTGIM
      \end{verbatim}
   d. Restart the IBM HTTP server.

2. From any remote system, open the web browser and type the URL:
   \texttt{http://hostName/CTGIM}.

   \textbf{Note:} When you use this URL, the default IBM HTTP server listening port is 80. If it listens at a different port, you must include that port in the URL.
Chapter 4. Troubleshooting installation and configuration problems

This section describes solutions for installation and configuration problems.

Before you install IBM Security Identity Manager Server:

- Read the troubleshooting tips in the “Installation Guide” and the “Configuration Guide”.
- Review the known problems and solutions in the IBM Security Identity Manager Information Center. Some of the topics in the “Installation Guide” and the “Configuration Guide” are repeated in this section.
- Configure IBM Tivoli Common Reporting to run on non-default ports if it is installed on the same system as IBM Security Identity Manager version 6.0 prerequisites. The default ports of IBM Tivoli Common Reporting are likely to conflict with ports of the installed products, which causes the IBM Tivoli Common Reporting installation to fail.

Firewalls can block the IBM Security Identity Manager Server installation

Stop all firewalls before initiating the product installation and configuration to prevent problems.

A firewall on the computer where IBM Security Identity Manager Server is installed might cause the installation to fail. For example, the middleware configuration component initiates LDAP commands. The firewall blocks the LDAP port, that is, port 389, which blocks LDAP commands from running. LDAP commands include `ldapsearch` and `ldapadd`.

User IDs must be in the administrator group to start an installation

The DB2 Universal Database configuration can fail due to restrictions on the privileges of and the characters in the user ID.

The installation can fail under the following conditions:

- You run the IBM Security Identity Manager installation program when a user ID is not in the administrator group.
- You install and configure DB2 Universal Database separately. The user ID is not in the administrator group.
- You use an ID containing reserved characters.

Install IBM Security Identity Manager and prerequisite products with a user ID in the administrator group. You cannot use any of these administrator user IDs:

- USERS
- ADMINS
- GUESTS
- PUBLIC
- LOCAL
The user ID cannot begin with any of the following letters, either lowercase or uppercase:
- IBM
- SQL
- SYS

**Microsoft Windows Terminal Server License server prevents an IBM Security Identity Manager installation**

Do not install the product with a DB2 Universal Database on a workstation with a Microsoft Windows Terminal Server License server installation.

If Microsoft Windows Terminal Server is on the system, uninstall it. Select **Control Panel > Add or Remove Programs > Add/Remove Windows Components.**

**Middleware configuration utility fails to catalog LDAP database instance node**

If the middleware configuration utility fails to configure the LDAP instance for IBM Security Identity Manager, check the error messages in the `cfg_itim_mw.log` file.

If you see the following messages in the `cfg_itim_mw.log` file, add `TDS_HOME/sbin` to the system path. Run the middleware configuration utility again.

```
GLPCTL017I Cataloging database instance node: 'itimldap'.
GLPCTL019E Failed to catalog database instance node: 'itimldap'.
The failure might have occurred because the system was not set up correctly before using the tool.
GLPCTL005I Removing database instance: 'itimldap'.
GLPIDP002I Deleting directory server instance: 'itimldap'.
```

**Entries in the services file prevent reinstalling the DB2 Universal Database**

When you uninstall DB2 Universal Database, some port entries are not deleted. If you attempt to reinstall the database, the installation fails.

This situation and the solution apply in all the following situations:
- To all supported versions of DB2 Universal Database
- To manual installation and configuration of DB2 Universal Database
- To the IBM Security Identity Manager installation program

The DB2 Universal Database uninstallation does not delete corresponding DB2 port entries from the system services file. The default location of the file depends on the operating system.

**Microsoft Windows systems**

```bash
%SystemRoot%\System32\drivers\etc\services
```

For example:
```
C:\WINDOWS\system32\driver\etc
```
UNIX and Linux systems

/etc/services

The following example shows the default service name entries and corresponding port values that remain in the file:

db2cdb2admin 50000/tcp
db2cdb2admini 50002/tcp

Note: If you specify a different DB2 administrator user ID during installation, the service uses the specified names. For example:

Microsoft Windows systems
db2cinstanceowner and db2cinstanceowner

UNIX and Linux, and DB2

instanceowner and DB2_instanceowner

When you try to reinstall, the services file is searched to determine whether DB2 port entries are present. If DB2 finds the port entries in the services file, the installation fails and returns the following message:

SQL5043N Support for one or more communications protocols failed to start successfully.

The core database manager functionality started successfully. This message is generated when the middleware configuration utility issues a db2start command to start the database.

Because the uninstall operation did not remove the entries, you must manually edit the services file and remove them before installing again.

LDAP port value is already in use for an initial installation of IBM Security Identity Manager

IBM Tivoli Directory Server uses the default port value 389.

Other directory servers and applications, such as Microsoft Windows Active Directory, also use this value.

If another directory server or directory application is installed on the same system as IBM Security Identity Manager, specify a different port value for IBM Tivoli Directory Server.

Backspace key deletes characters (SUSE Linux only)

The Backspace key might work like a Delete key on SUSE Linux systems when you use the user interface for installation, uninstallation, or middleware configuration tasks.

Error messages do not display when using an emulator program to install IBM Security Identity Manager

If you use an emulator program such as the X Window System server or Virtual network computing (VNC) to access a remote computer to perform a separate installation of middleware or IBM Security Identity Manager Server, you might not see all the error messages that an installation problem can generate.
If the installation fails without a message, install the application directly on the target system.

### tz mappings: illegal format at near line 11 error message

The tz mappings: Illegal format at near line 11 message might be displayed during installation and configuration. You can ignore it.

The error message might be displayed in any log file from InstallAnywhere, such as a server installation, DBConfig, runConfig, ldapConfig, and others.

### Messaging engines do not start after installation

On systems that run DB2 Universal Database, the IBM Security Identity Manager messaging engines might not start.

The SystemOut.log file in the WebSphere Application Server contains a message like the following one:

```
4/19/07 9:06:03:421 IST] 00000014 SibMessage E
[itim_bus:64ibm2Node01.server1-itim_bus]
CWSIS0002E: The messaging engine encountered an exception while starting.
Exception: com.ibm.ws.sib.msgstore.PersistenceException:
CWSIS1501E: The data source has produced an unexpected exception:
com.ibm.db2.jcc.b.SqlException:
DB2 SQL error: SQLCODE: -443, SQLSTATE: 38553,
SQLERRMC: SYSIBM.SQLTABLES;TABLES;SYSIBM:CLI:-80
```

A DB2 Universal Database fix pack installation is incomplete. Complete these steps:

1. Stop the WebSphere Application Server that hosts the IBM Security Identity Manager Server.
3. Follow the required procedure for your platform in the post-installation instructions.
4. Restart the WebSphere Application Server.

### The temp directory is not deleted after installation (Microsoft Windows only)

The temp directory is not deleted after the installation. You must manually delete it.

The installation process might create a temp directory at the root of the disk if:

- You installed the product on the Microsoft Windows operating system.
- You installed on a disk drive other than the C:\ drive.
- The temp directory does not exist.
A java.lang exception occurs in a cluster environment

A java.lang exception occurs during installation in a cluster environment. You can ignore the exception. It does not affect the IBM Security Identity Manager installation or operation.

This exception occurs when you install IBM Security Identity Manager:
  OR
- On a IBM Security Identity Manager cluster member.

Part of the exception includes this line:
## ZG6fxUtil.loadImage: image loading failed for:
com/zerog/ia/installer/images/introImage.png

Cannot uninstall interim fixes or fix packs

IBM Security Identity Manager cannot uninstall interim fixes or fix packs.

Cannot log on to the IBM Security Identity Manager Console

You cannot log on to the IBM Security Identity Manager Console. This problem occurs if you rerun the runConfig utility on IBM Security Identity Manager that is configured to access LDAP server with SSL.

If you rerun the runConfig utility, it overwrites the java.naming.provider.url property in the enRoleLDAPConnection.properties file.

<table>
<thead>
<tr>
<th>Before reconfiguration</th>
<th>After reconfiguration</th>
</tr>
</thead>
<tbody>
<tr>
<td>java.naming.provider.url=ldaps://Host_IP:secure_port</td>
<td>java.naming.provider.url=ldap://Host_IP:secure_port</td>
</tr>
</tbody>
</table>

To fix the problem, complete these steps:
1. Open the enRoleLDAPConnection.properties file. The default directory location of the file depends on the operating system:
   - **Microsoft Windows systems**
     C:\Program Files\IBM\isim\data
   - **UNIX and Linux systems**
     /opt/IBM/isim/data
2. Go to the java.naming.provider.url property in the enRoleLDAPConnection.properties file.
3. Modify the java.naming.provider.url property to
   - java.naming.provider.url=ldaps://Host_IP:secure_port
5. Log on to the IBM Security Identity Manager Console.
Too many files open (UNIX and Linux)

The Too many open files message occurs on UNIX and Linux operating systems. The default setting for the maximum number of open files might be too low.

To avoid this condition, increase the maximum open files to 8000:
1. Edit the /etc/security/limit.conf file.
2. Change the statement that specifies the value of nofiles to 8000.
3. Optional: If you want the change to take effect in the current session, type ulimit -n 8000.
Chapter 6. Troubleshooting IBM Security Identity Manager Server problems

This section describes solutions for IBM Security Identity Manager Server problems.

**ACI filter not working correctly when an account is created**

Access control item (ACI) object filters for the Add Entity operation are ignored.

If an ACI contains a filter that defines the scope of its target entities, the filter in the ACI is ignored when an add operation performed. Instead, the filter is considered a wildcard filter while displaying the form for that particular entity, and the target filter is evaluated only when the request is submitted.

**User accounts are included when performing a suspend, restore, or delete task**

User accounts are included for suspend, restore, or delete tasks.

**Problem**

The current default value includes user accounts when suspending, restoring, or deleting users.

**Solution**

When you use the Manage Users window in the IBM Security Identity Manager Console to suspend, restore, or delete user accounts, clear the **Include accounts when suspending, restoring, or deleting users** check box.

When you suspend users during an identity feed, edit the **enRole.properties** file. The default value of this property is true. Set the **enrole.suspend.accounts.identity.feed** property to false. For example:

```
enrole.suspend.accounts.identity.feed=false
```

**Warning messages not displayed during identity feed or reconciliation**

The identity feed or a reconciliation operation does not display warning messages if account or user attributes are not successfully updated.

**Problem**

The operation displays a warning message only if a user or an account update fails. Reconciliation can return a successful status under the following conditions:

- All users or accounts are updated.
- One or more attributes associated with the users or accounts are not successfully updated.
Solution

Review the IBM Security Identity Manager log files. The logs record updates and changes to account and user attributes. See "Logs" on page 15 for more information.

Changing the service name prevents viewing and performing actions on service requests

Changing the name of a service prevents you from viewing and performing actions on service requests that applied to the service before the name change.

Keep in mind the following considerations:
• Carefully consider the name of a new service before you name it.
• Do not change the name of the service after requests are made to create accounts on the service.

Follow this process if the software prevents you from acting on a service request after changing a service name:
1. Change the name back to the original name.
2. View and perform actions on requests that occurred before the service was renamed.
3. Change the name of the service to the new name.
4. View and perform actions on requests that occurred after the service was renamed.

Identity feed operation fails and returns an LDAP error

The installation program sets a maximum of 500 search operations per application task. If you set up an identity feed for more than 500 to populate the IBM Security Identity Manager Server, the operation fails. You must configure the LDAP server that is supplying the user data for the number of users in the feed.

Setting the maximum number of search entries

If the IBM Tivoli Directory Server is the source of user data:
1. Use the IBM Tivoli Directory Server Administration Console.
2. Edit the ibm-slapdSizeLimit variable in the ibmslapd.conf configuration file.

The default directory of ibmslapd.conf depends on the operating system.

Microsoft Windows systems
C:\idssldap-ldapdb2\etc

UNIX and Linux systems
/home/ldapdb2/idsslapd-ldapdb2/etc

Increasing the number of results in the user interface
1. Edit the enrole.ui.maxSearchResults property in the ui.properties file.
2. Increase the limit on the number of results that are displayed for a search.

The default directory of enRoleLogging.properties depends on the operating system.
Reconciliation operation fails with an out-of-memory error

The reconciliation operation fails with an out-of-memory error. You can increase the Java Virtual Machine (JVM) heap size limit in the WebSphere Application Server. Try the reconciliation again.

About this task

If the system on which the IBM Security Identity Manager Server is installed has the suggested amount of physical memory (2 GB), you can set the maximum JVM heap size to 1 GB (1024 KB). You can set the maximum heap size higher if the physical memory exceeds 2 GB.

Procedure

1. Open the WebSphere Application Server Administrative Console.
2. Log in to the server with the following URL: http://machine:port_number/ibm/console/
   For example, the local host is localhost. The connection port is 9060. The URL is http://localhost:9060/ibm/console/.
3. Select Servers > Application Servers > server1. Use the equivalent name if you are not using the default server name.
5. Go to the Maximum Heap Size parameter.
6. Set the heap size value to 1024 or higher. If the physical memory is greater, you can set the maximum heap size higher.
7. Save the configuration.
8. Restart the IBM Security Identity Manager Server.
   a. Access the WebSphere Application Server Administrative Console main window.
   b. Select Applications > Enterprise Applications.
   c. Select the check box next to the ITIM application.
   d. Click Stop.
   e. Wait for the following message:
      Application ITIM on server server_name and node node_name stopped successfully.
   f. Select the check box next to the ITIM application.
   g. Click Start.
   h. Wait for the following message:
      Application ITIM on server server_name and node node_name started successfully.
   i. You can now run reconciliation.

A request fails because one or more values cannot be changed

If you submit a request to change a user, account, or service, the entire request fails if any single value cannot be changed.
A potential scenario that causes a failure includes two users using separate browsers, concurrently attempting to add or remove the same value.

- You submit a request to change the given name and family name of a user.
- The family name cannot be changed.
- Neither change is made.
- The entire request fails.

A request can also fail when an inconsistent value that is not part of the current change task is already populated for one of the attributes in LDAP. For example, set the manager attribute of a person to a value similar to `erglobalid:7654212221212, ou=users...` in IBM Tivoli Directory Integrator. Because all IBM Tivoli Directory Integrator-based changes are submitted to IBM Security Identity Manager with `System` as the requestor, the change is accepted. However, if an administrator makes a change to the email address or any other field for the same person, the change user task fails until you manually correct the manager attribute in LDAP to a value such as `erglobalid=7654212221212, ou=users...`.

Concurrent usage of IBM Security Identity Manager Server can affect changes to data

Certain conditions apply to how changes are made to data as a result of concurrency. An example of concurrency is when two or more users access the same data through the user interface using separate sessions on separate computers.

**Single-value attributes**

- When you run the **ADD** operation to change an attribute from null to a value, only the first request succeeds. All other concurrent requests fail because multiple values cannot be added to a single-value attribute.
- When you run the **REMOVE** operation to change an attribute from a value to null, only the first request succeeds. All other concurrent requests fail because there is only one value to remove.
- When you change an attribute from one value to another, the last value submitted overrides any other changes.

**Multi-value attributes**

The last values submitted override all existing values.

All results from a large search operation are not displayed

By default, the user interface can display a maximum of 1000 search entries. If your search returns more than 1000 entries, you can change the maximum amount.

Typically, you perform a search operation to locate and select specific users. For operations such as reconciliations, you might want to view all entries associated with the operation. This type of search operation might return more than 1000 entries. You can change the default maximum number with the `enrole.ui.maxSearchResults` property in the `ui.properties` file. The default directory of `ui.properties` depends on the operating system.

The default location of the directory depends on the operating system.
Microsoft Windows systems
   C:\Program Files\IBM\isim\data

UNIX and Linux systems
   /opt/IBM/isim/data

Setting this value higher consumes more physical memory. Dedicating a large amount of memory to a single operation can deteriorate the overall performance of the IBM Security Identity Manager Server. Do not change the amount for systems configured with the minimum amount of physical memory (2 GB).

---

**Users are deleted from default groups in identity feeds**

During an identity feed, users can be inadvertently deleted from the default groups that are associated with the customized groups.

When performing an identity feed, always specify that a user has membership in both a customized group and the default group of the same category. For example, a user who is a member of a customized group must also be a member of the default group of the same category or processing results are unpredictable. If the incoming identity record for a user initially indicates membership in a customized group, the product includes the user as a member of both the customized group and the default group of the same category. IBM Security Identity Manager interprets a subsequent identity feed that includes the same user as a modification of the existing user. If the subsequent identity feed specifies the user has membership in the customized group, but not in the default group of the same category, the software removes the user from membership in the default group.

---

**Restoring the system administrator account**

Incorrectly modifying a provisioning policy can deprovision all accounts except the built-in system administrator account. If you suspend or deprovision all IBM Security Identity Manager accounts, including the system administrator account, you can restore the system administrator account through the IBM Tivoli Directory Server.

The following process restores the itim_manager account. You can then restore other accounts using the manager account.

1. Access the IBM Tivoli Directory Server Administration Console.
   The dc=com value was specified for the Identity Manager DN Location field in the Directory Configuration during installation.
3. Change the eraccountstatus value from 1 to 0.

---

**Logging on to IBM Security Identity Manager after stopping and starting the WebSphere Application Server Administrative Console**

When you stop and restart the IBM Security Identity Manager Server using the WebSphere Application Server Administrative Console, subsequent attempts to log in to IBM Security Identity Manager fail.

An error is entered in the trace.log file. The error depends on the operating system.
Microsoft Windows systems
java.lang.UnsatisfiedLinkError: Native Library
C:\Program Files\IBM\isim\lib\nt\i4clntjni.dll
already loaded in another classloader

UNIX and Linux systems
java.lang.UnsatisfiedLinkError: Native Library/opt/IBM/isim/lib/unix/libi4clntjni.so
already loaded in another classloader

To resolve this problem, restart the WebSphere Application Server.

Tip: To prevent this error from occurring, stop and restart the WebSphere Application Server each time you restart IBM Security Identity Manager from the WebSphere Application Server Administrative Console.

Do not change the date and time while users are logged in to IBM Security Identity Manager

If you change the date and time while users are logged on, unpredictable behavior might occur.

If you change the date and time on the operating system on which IBM Security Identity Manager is installed, make sure that no users are logged on.

A Java core dump occurs while performing a search from an applet

A Java core dump occurs in WebSphere Application Server during a search from an applet when the Java Virtual Machine (JVM) heap size is too small.

About this task

The core dump contains the following message:

NULL ------------------------------------------------------------------------
0SECTION TITLE subcomponent dump routine
NULL = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
1TISIGINFO OUTOFMEMORY received

To prevent this problem, increase the JVM heap size limit.

Procedure

1. Open the WebSphere Application Server Administrative Console.
2. Log in to the server using the following URL:
   http://machine name:port_number/ibm/console/
   Example: The local host is localhost. The connection port is 9060. Log in to the local host with http://localhost:9060/ibm/console/.
3. Select Servers > Application Servers > server1. Use an equivalent name, if you are not using the default server name.
5. Navigate to the Maximum Heap Size parameter.
6. Set the value to 1024 or higher. If the physical memory is greater, you can set the maximum heap size higher.
7. Save the configuration.
8. Restart the IBM Security Identity Manager Server.
a. Access the WebSphere Application Server Administrative Console main window.
b. Select Applications > Enterprise Applications.
c. Select the check box next to the ITIM application.
d. Click Stop.
e. Wait for the following message:
   Application ITIM on server server_name and node node_name stopped successfully.
f. Select the check box next to the ITIM application.
g. Click Start.
h. Wait for the following message:
   Application ITIM on server server_name and node node_name started successfully.

Presentation problems

This section describes solutions to information presentation problems.

Incorrect display of multiple tasks in the administration console

If you rapidly open multiple tasks in the administration console, sometimes the tasks open in the same tab rather than in separate tabs. To prevent this problem, wait until one task is loaded by the browser before you start the next task.

If multiple tasks get loaded on the same tab, you can correct the problem by refreshing the page. To refresh the page, press F5 on your keyboard or click the refresh button on your web browser.

Blank spaces do not differentiate user-defined identifiers

Do not use blank spaces to differentiate user-defined identifiers such as the names of users or other objects. The user interface contracts two or more consecutive blank spaces into a single blank space. Example:

- You create two users: j doe and j doe.
- The first j doe has one space between the given and family names.
- The second j doe has three spaces between the given and family names.
- The user interface displays both names as j doe.

Attribute deleted from service profile is still displayed in the form designer

You delete an attribute from a service profile. The form designer continues to display the attribute, even though the attribute no longer exists in the LDAP directory.

You must delete the same attribute in the form designer. If you close and open the form designer after deleting the attribute, it is no longer included in the list of attributes for the service.
Creating or modifying a form, a workflow design, or a policy might be hindered by timeout

Creating or modifying a form, a workflow design, or configuring policy join behaviors might take longer than the session timeout interval. To avoid interruption, the session never times out while the Form Designer, Workflow Designer, or Policy join applet is running.

Exit the task if you want the session timeout interval to take effect.

LDAP attributes are not displayed

The following attributes are not included in the searchable attributes menu in the user interface:
- erpersonstatus
- eraccountstatus
- erorgstatus
- erbporgstatus
- eraccountcompliance

These attributes are hidden and not searchable. Hidden attributes are specified in the ISIM_HOME\data\enRoleHiddenAttributes.properties file. To make these attributes searchable, comment out the attributes in the file.

Note: Many hidden attributes are system-managed attributes. Do not modify system-managed attributes. Determine the impact when making a previously hidden attribute visible.

New attributes do not display on a form

If new attributes are added to a form and are not displayed, they might be in the enRoleHiddenAttributes.properties file. Attributes listed in this file are not displayed on the forms. To display these attributes on the form, comment out the lines for these attributes.

The default directory of enRoleHiddenAttributes.properties depends on the operating system.

Microsoft Windows systems
C:\Program Files\IBM\isim\data

UNIX and Linux systems
/opt/IBM/isim/data

If the attributes are not marked as hidden in the enRoleHiddenAttributes.properties file, you might need to update the IBM Security Identity Manager Server cache. This situation typically occurs when a new attribute was added to an object class.

To update the cache, stop and start the IBM Security Identity Manager Server.
1. Open the WebSphere Application Server Administrative Console.
2. Log on to the server by using the following URL:
   http://machine name:port_number/ibm/console/
   Example: The local host is localhost. The connection port is 9060. Log on to the local host by using http://localhost:9060/ibm/console/.
3. Select Applications > Enterprise Applications.
4. Select the check box next to the ITIM application.
5. Click Stop.
6. Wait for the following message:
   Application ISIM on server server_name and node node_name stopped successfully.
7. Select the check box next to the ITIM application.
8. Click Start.
9. Wait for the following message:
   Application ISIM on server server_name and node node_name started successfully.

**Browser limitation when displaying home page**

The home page might require too much time to display with the Mozilla Firefox web browser. The home page might be displayed without GUI labels.

If the network.http.pipelining property is set to true, the home page might load slowly. This enablement multiplies the number of HTTP requests that are sent to the server and might overload it and the Mozilla Firefox web browser.

**Browser limitation when setting row or column restraints**

If you specify row or column constraints for a text area with the Form Designer applet, Mozilla Firefox web browser might not recognise them. The browser might display more rows or columns than you specified.

Example: You change the number of rows in the Properties pane to 2. You expect that only two visible lines are displayed. Mozilla Firefox web browser displays more than two rows.

Microsoft Internet Explorer web browser adheres to the column and row attributes on a text area.

**Browser limitation when selecting multiple image controls with the Shift key**

You cannot select multiple image controls in the Mozilla Firefox web browser by pressing Shift and Click simultaneously. If you try to select multiple image controls, another browser opens. Radio buttons are an example of multiple image controls.

**JAWS reader interprets symbol as greater than**

The JAWS reader interprets the > symbol as greater than. The greater than phrase might confuse a visually impaired user, because one piece of text cannot be greater or less than another piece of text.

The JAWS reader also reads the > symbol as greater than for all pages in the console application that contain the symbol. For example: breadcrumbs, Next, and Back.
Form designer: no morning or afternoon indicator on 12-hour format

In the form designer, if the dateinput mode is in read-only mode, you see the time displayed in 12-hour format. There is no indicator for morning (a.m.) or afternoon (p.m.).

Set the dateinput mode field to read-write mode. The time is displayed in 24-hour format and is correctly understood.

1. Click Configure System > Design Forms. The form designer is displayed.
2. Double-click Identity Manager User in the left column.
3. Double-click ITIM account.
4. Click erchangepswrequired on the panel.
5. In the Format tab of the Properties section, ensure that the Read-Only on Modify field is not checked.
6. Save the changes.

If the dateinput field is in read-only mode, change the following line in the Labels.properties file in the ISIM_HOME\data directory from:

readOnlyDateFormat=MMM dd, yyyy hh:mm:ss z

to:

readOnlyDateFormat=MMM dd, yyyy hh:mm:ss a z

For Arabic locales, English numbers are displayed for calendar and date widgets

To change the numbers to Arabic in the regional setting of the operating system, change the Digit substitution field from Context to National.

Twistie next to node names with special characters in a tree widget might not display correctly in bidirectional mode

You might encounter a display problem when you work in bidirectional mode.

In the IBM Security Identity Manager Console, the position of the twistie (•) next to a node or nodes in the tree widget might not display correctly. The display problem can occur when you do the following actions:
1. You create and name the node in a tree widget with a combination of text, numbers, and special characters. For example, "abc ½abc".
2. You view the IBM Security Identity Manager Console in bidirectional mode.

The cause of this problem is that the special characters are misinterpreted as Arabic characters. Therefore, the web browser renders a mix of English and Arabic characters. However, this problem does not affect the strings of text and are considered for all other processing actions.

This problem is only related to the display of the nodes and does not affect any operation.

Data problems

This section describes solutions to problems with data.
Error message: An integer field contains a non-integer value

You cannot enter a value greater than 2147483647 in the UID number field of the Account information window. This problem is a Java limitation. The following message is displayed:

CTGIMU656E: An integer field contains a non-integer value.

The message can be misleading when you enter an integer greater than 2147483647.

Cannot read library files

If the IBM Security Identity Manager Server does not have permission to read library files, verify that the files have the correct permission. If necessary, make the appropriate changes to the file permission.

Data input problems

Data input problems typically occur when users define custom data structures, such as new service types, in the directory structure, or when users install new adapters. If you cannot enter data for a custom class such as a service type, check the IBM Security Identity Manager Server and the IBM Tivoli Directory Server logs. LDAP messages such as object error 32 are typical. They indicate missing data for required fields or problems interpreting the schema.

Passwords cannot contain leading or trailing spaces

IBM Security Identity Manager trims leading and trailing spaces for passwords. If the root user password for a managed resource includes a leading or trailing space, IBM Security Identity Manager cannot connect to it.

The root password to access the associated managed resource must not have any leading or trailing spaces. The password cannot be a single blank space.

Cannot delete an organizational unit (OU)

When deleting an organizational unit (any unit in the organization), you must delete all dependent units before deleting the OU. Sometimes, dependent units might exist even though they are not displayed in the organizational tree. If you do not delete the dependent units, the system displays the following message:

Dependent Unit(s) exists. Remove all dependent Unit(s) first, then Delete.

Complete these steps:
1. Search the IBM Tivoli Directory Server for dependencies using the following command:
   erparent=OU-DN

   where OU-DN is the distinguished name (DN) of the OU.
2. Remove any discovered dependencies.
3. Delete the OU using the user interface.

Users cannot obtain their new passwords

If the following settings and conditions apply, the affected users cannot receive passwords reset by an administrator in the user interface:
Some users and their supervisors do not have email addresses.
Users cannot change their passwords.
Challenge-response authentication is enabled.

If these conditions apply and a user clicks the Forgot your password? link to reset a password:
- The user cannot obtain the password through email or from the help desk assistant.
- The help desk assistant can reset the password, but the password cannot be delivered to the recipient.
- The user must contact the help desk to obtain the new password.

To avoid this problem, ensure that the email notification function is working and that all affected users and their supervisors have email addresses. As an alternative, users can change their passwords according to the applicable password policy.

User cannot change a password and the TRANSACTION_ROLLEDBACK error is displayed

If a user receives the TRANSACTION_ROLLEDBACK error when changing a reset password, restart the WebSphere Application Server. If the server restart does not correct the problem, ensure that both WebSphere Application Server and the DB2 Universal Database servers are running.

Cannot determine if data synchronization is running or the status of the last synchronization

You cannot determine if data synchronization is running or determine the status of the last synchronization.

When you select a report type in the administrative console, the status is displayed as the Data Validity field in the Options window. The following possible values determine the state of the data synchronization:
- No Data synchronized
- In progress
- Invalid
- Date and time when last synchronization completed

Importing backup directory information with LDIF fails

Using LDAP Data Interchange Format (LDIF) files to import backup directory information can experience problems if the system is not stopped or workflows are incomplete.

When you use LDIF files to import backup directory information, stop the application servers. If the LDIF import modifies workflows or operations, complete all workflows before you perform an LDIF import.

For more information about LDIF files, see the IBM Tivoli Directory Server documentation.
Multiple access control items are ignored if the first 255 characters are the same

If you define more than one access control item (ACI) on the same target and at the same organizational level and the first 255 characters of every ACI name are identical, only one ACI is staged into the ACI table.

Reporting ignores the remainder of the ACIs. An ACI report shows only one ACI. The trace.log file displays the following error message:

com.ibm.websphere.ce.cm.DuplicateKeyException: ORA-00001: unique constraint (ENROLE.SYS_C003110) violated

Do not define multiple ACIs with the same first 255 characters on the same target and at the same organizational level.

The Requestee column displays an unexpected value of the common name in a person during self registration

During self registration, the Requestee column of the common name in a person does not display an expected value.

To correct this problem, complete these steps:

Note: The value of Name Attribute in Configuration > Entities > Person must be set to sn. If the value of Name Attribute is changed back to cn, remove the script node.

1. Log on as itim manager.
2. Click Configuration.
3. Click Entity Type.
4. Select Person in the menu.
5. Click selfRegister as the operation.
6. On the selfRegister workflow, insert a uniquely named script node between the Start and the selfRegister Approval nodes.
7. Double-click the new script node to display Properties: Script Node window.
8. Enter the following Java script:
   ```java
   var personData = person.get();
   var snValue = personData.getProperty("sn")[0];
   process.setRequesteeData(snValue);
   ```
9. Click OK.

Workflow problems

This section describes problems with workflow processes.

Creating nine or more service instances for a password policy causes an error condition

An error occurs after nine or more service instances are associated with a password policy. Tune the DB2 stmheap attribute for the maximum number of service instances. This table provides guidelines:
### Change the statement heap size with the DB2 `update` command.

1. Set `db2instance` to one of these instances:
   - `db2admin`
   - IBM Tivoli Directory Server instance
2. Run `db2` from a command line to start the DB2 command-line interface.
3. Run an `update` command and specify the appropriate value as the `size` variable:
   ```
   update db cfg for db_name using STMTHEAP size
   ```

### Requests timeout before reaching the escalation period

One or more pending requests timeout before completion. The timeout stamp indicates that the escalation period was not reached. Modify the LIMIT values for requests in the IBM Tivoli Directory Server operation objects. Specify a value of `-1` to set the operation to unlimited.

#### Set the LIMIT value for operation objects corresponding to operations, such as adding an account

1. Ensure that the user ID for connecting to the directory server has the necessary permissions to modify LDAP entries.
2. Using an LDAP client, connect to the directory server with the IBM Security Identity Manager data.
3. Browse to the appropriate operation definition. The operation definitions are located under this Distinguished Name:
   ```
   DN: ou=operations, ou=itim, tenant, root suffix
   ```

   Example: The tenant is `ou=org`. The root suffix is `dc=com`. The operations are in `ou=operations, ou=itim, ou=organ, dc=com`.

4. Edit and set LIMIT to the appropriate value in the tag of the `erXml` attribute of the process definition entry. For example:
   - To set the timeout of the account add operation to four days, edit the `erXml` attribute on
     ```
     <PROCESSDEFINITION...>
     ```
     `erglobalid=0000000000000000000022, ou=operations, ou=itim, ou=tenant, root suffix`
   - Change `LIMIT="43200000"` to `LIMIT="345600000"` in the `<PROCESSDEFINITION...>` tag.
   - To set LIMIT to unlimited, specify `LIMIT="-1"`.

#### Set the LIMIT value for operation objects for workflows

1. Browse to the appropriate workflow definition. All the operation definitions for workflows are under this DN:
   ```
   DN: ou=workflow, erglobalid=00000000000000000000, tenant, root suffix
   ```

   Example: The tenant is `ou=org`. The root suffix is `dc=com`. The workflow definitions are in:
Select the workflow entry under the Distinguished Name that you want to change.

3. Set the LIMIT value for changing the LIMIT value for operations. See Set the LIMIT value for operation objects corresponding to operations, such as adding an account.

Creating or modifying a workflow design, a form, or a policy takes longer than the timeout interval

Creating or modifying a workflow design, a form, or a policy might take longer than the session timeout interval. To avoid interruption, the timeout value in the web.xml file is ignored. The session never times out while the Workflow Designer, Form Designer, or Policy applet is running.

Ensure that you complete each activity to create or modify a workflow design, a form, or a policy.

A workflow UNTIL loop behaves like a DO...WHILE loop

A workflow UNTIL loop behaves like a DO...WHILE loop. Instead of ending when a specified loop condition is met, the loop continues until a specified condition fails. You must restate the condition as the negative of the specified loop condition.

For example, this condition requires restating as follows:

\[ a<b \]

Needs to be restated as:

\[ a\geq b \]

Approval workflow not initiating

You defined an access with an approval workflow for a group. The workflow is not initiated when you add members to the group with the group management function.

Therefore, it is possible for unauthorized users to gain access to groups.

Workflow or operation cannot be created or updated

You created or updated a workflow or operation, but the changes did not take effect. The administration console indicates a successful operation, but the changes were not saved when the workflow designer exited.

This problem occurs only when you are running the administration console on localhost. For example:

http://localhost:9080/isim/console

When the problem occurs, check to see whether this exception is shown in the Java console window:

java.security.AccessControlException: access denied
  (java.net.SocketPermission 127.0.0.1:9080 connect,resolve)

Note: If you do not see the Java console window on your desktop when the browser loads the workflow designer applet, configure it from the Java control panel.
Workaround:

Select one of these workarounds:

- Do not use localhost. Instead, use the actual IP address or the host name to access the console. When you use an IP address or host name, the problem does not occur. For example:
  http://testserver.subnet.example.com:9080/isim/console
  http://1.1.1.1:9080/isim/console

- Modify a policy file to enable localhost. You can successfully use localhost by specifying a grant statement in a .java.policy file in your home directory. If you do not have an existing .java.policy file, create a text file. Add this statement:

```java
grant {
    permission java.net.SocketPermission
    "127.0.0.1:9080", "connect,resolve";
};
```

Note: You must restart your browser after you create or modify the .java.policy file.

Usage problems

This section describes problems with using the product.

Search limit exceeded

The $ISIM_HOME$/data/ui.properties limits the number of results for accounts with default group attribute widget of the type search filter list box. The limit is 1000. The search returns only the first 1000 entries.

To access the remaining entries you must modify the account form to include a filter field so that you can narrow the search.

1. Log on to the IBM Security Identity Manager Console.
2. Click Configure System > Design Forms.
3. Click Accounts.
4. Double-click the account you want to modify.
5. Double-click the attribute on which you are searching on. It is identified as [ListBox].
6. Specify the object class.
7. Select the Show Query UI check box and click OK.
8. Click Save.
9. Click OK.

Error page displays as blank during uninstallation

The uninstaller program stops abruptly when you run the uninstaller.exe program and click the upper right X in the frame of the uninstaller window.

The program loses the Java Virtual Machine (JVM) and cannot generate a correct error message.

To avoid this situation, wait for all panels to display and close them with Close or Cancel.
Out-of-memory error occurs while generating a report in PDF

An out-of-memory error occurs while generating a report in portable document format (PDF). This error is unlikely to occur when generating comma-separated value (CSV) reports.

This error can occur if the JVM heap does not have enough available space to transform the XML to PDF format. In addition, the error can occur for double byte character set (DBCS) languages that have larger space requirements.

Use this procedure to increase the JVM heap size maximum:
1. Access the WebSphere Application Server Administrative Console.
2. Use the following URL to log on to the WebSphere Application Server:
   ```
   http://machine_name:port_number/ibm/console/
   ```
   Example: The local host is localhost. The connection port is 9060. Use http://localhost:9060/ibm/console/ to log on to the local host.
3. Select Servers > Application Servers > server1. Use an equivalent name if you are not using the default server name.
5. Go to the Maximum Heap Size parameter and set this value to 1024 or higher.
   If the physical memory is greater, the maximum heap size can be set higher.
6. Save the configuration.
   a. Access the WebSphere Application Server Administrative Console main window.
   b. Select Applications > Enterprise Applications.
   c. Select the check box next to the ITIM application.
   d. Click Stop.
   e. Wait for the following message:
      ```
      Application ITIM on server server_name and node node_name stopped successfully.
      ```
   f. Select the check box next to the ITIM application.
   g. Click Start.
   h. Wait for the following message:
      ```
      Application ITIM on server server_name and node node_name started successfully.
      ```
8. Run the PDF report again.

Information is garbled in a CSV-formatted report

If you save or view a report in CSV format, UTF-8 encoding is used to format the output file. This format is supported by most CSV-compatible applications for viewing or manipulating CSV information. Some viewers might not support UTF-8 encoding or might not be set to open UTF-8 formatted files.

If the information in a CSV report does not render successfully, ensure that the application supports UTF-8 encoding and is set to use UTF-8 encoding.

Out-of-memory error causes server failure

IBM Security Identity Manager fails with an out-of-memory condition when the following conditions exist:
Many concurrent users exit the software without properly logging out in a 10-minute window.

Example: Several concurrent users close their web browsers by clicking X, the Close icon, while logged on to IBM Security Identity Manager.

The amount of physical memory and the JVM heap size settings are not high enough.
An out-of-memory condition occurs when the memory used by the total number of sessions exceeds the amount of memory allocated for the server.

If this problem occurs, complete one or more of the following tuning tasks:

Limit the number of in-memory sessions that WebSphere Application Server provides.

1. Access the WebSphere Application Server Administrative Console.
2. Click Applications > Enterprise Applications > ITIM > Web Module > app_web.war > Session Management.
3. Select Override session management.
4. Clear the Allow overflow check box.
5. Reduce the value in the Maximum in-memory session count field. This value depends on the amount of memory allocated to your servers.
   This value specifies the maximum number of concurrent live web browser sessions for IBM Security Identity Manager.
6. Reduce the value in the Set timeout field from 30 minutes to a smaller value.
7. Click OK and save the changes to the master configuration.

Restart the IBM Security Identity Manager Server.

1. Access the WebSphere Application Server Administrative Console main window.
2. Select Applications > Enterprise Applications.
3. Select the check box next to the ITIM application.
4. Click Stop.
5. Wait for the following message:
   Application ITIM on server server_name and node node_name stopped successfully.
6. Select the check box next to the ITIM application.
7. Click Start.
8. Wait for the following message:
   Application ITIM on server server_name and node node_name started successfully.

Generating large CSV reports results in out of memory errors

Generating a large CSV report might result in an out of memory error. Adjust the value of the reportBatchSize property in the adhocreporting.properties file to avoid Java OutOfMemory errors for large reports.

The reportBatchSize property specifies number of items requested from the reporting tables at one time. If no value is set or the line is commented out, all items are retrieved.

1. Access the adhocreporting.properties file.
2. Change the reportBatchSize property to 10000, as follows:
   reportBatchSize=10000
3. Make sure that the line is not commented out.
4. Change all nodes in a clustered environment.
5. Restart the IBM Security Identity Manager application for the change to take effect.

**Note:** If you use Microsoft Internet Explorer to generate the report, enable **Automatic prompting for file downloads** in the web browser security setting.

**Generating a PDF report with an active report file open fails**

You generated a report output file as a Portable Document Format (PDF) file and either minimized the displayed information or left the file open.

You cannot generate another report until you close the active report file.

**Report has Deprecated label Access Control Information**

The report feature uses a deprecated label called Access Control Information. The new label is **Access Control Item (ACI)**.

You might see the deprecated label if you:
- View the **Access Control Information {ACIs}** report builder.
- Click **Run report > Access Reports > Access Control Information {ACIs}** on the **Reports** tab.

Edit the `ISIM_HOME/data/reportingLabels.properties` file and manually change the value for `accessControlInformation`. For example, the deprecated value is `accessControlInformation=Access Control Information {ACIs}`, and the correct value is `accessControlInformation=Access Control Item {ACIs}`.

**The font in a report is too small**

If the font in the report is too small to read, save the report in PDF format or in CSV format and print the report.

To save the report, complete these steps:
1. Select **File > Save As** from the report output window.
2. Browse to the directory where you want to save the file.
3. Enter a valid file name.
4. Save the document.

You can print both PDF and CSV format reports. You can print PDF reports in portrait or landscape modes. CSV can print reports that do not fit on a single page horizontally.

To print a CSV report, complete these steps:
1. Select the **CSV** report format when generating the report.
2. Select the **Save As** option in the dialog box.
3. Provide a valid location and file name for saving the report.
4. Use Microsoft Excel or any other CSV file reader to open the report.
5. Use the print option to print the document.
Adding the owner attribute causes an IllegalStateException error

Adding the owner attribute on an account form might cause a java.lang.UnsupportedOperationException error.

The message is:
CTGIMO002E. An unhandled exception occurred.
Error: java.lang.UnsupportedOperationException: the owner and (or) service
or an account cannot be changed.

Do not use the Form Designer to add the owner attribute to an account form.

Use the IBM Security Identity Manager account adoption and orphan operations to set or clear the owner of an account.

An organizational unit name with more than 128 characters is not created

If the organizational unit name exceeds 128 characters, the name is not created. Do not enter a value greater than 128 characters for the organizational unit name.

Note: A long name within the 128-character limit does not wrap when displayed.

IBM Security Identity Manager fails because of an out of memory condition

IBM Security Identity Manager can fail with an out of memory condition when the following conditions occur simultaneously:

Many concurrent users quit without properly logging out in a 30-minute window.
Example: All the concurrent users close their web browsers by clicking X, the Close icon, while remaining logged on.

The IBM Security Identity Manager Server physical memory and Java heap size settings are not high enough.
An out of memory condition occurs when the memory used by the total number of sessions exceeds the amount of memory allocated for the server.

To correct this problem, do either one or both of the following tuning tasks:

Limit the number of in-memory sessions for WebSphere Application Server.
1. Access the WebSphere Application Server Administrative Console.
2. Click Applications > Enterprise Applications > ITIM > Manage Modules > ITIM Console > Session Management.
3. Select Override session management.
5. Reduce the value in the Maximum in memory session count field. The value limits the number of concurrent web browser sessions. This value depends on the amount of memory allocated to your servers and the number of WebSphere clustered nodes used by IBM Security Identity Manager.
6. Click OK and save the changes to the master configuration.
7. Repeat the previous steps from Step 2 but select the module ITIM Self Service in Step 2.
Reduce the session inactivity time to less than 30 minutes.

1. Click Applications > Enterprise Applications > ITIM > Manage Modules > ITIM Console > Session Management.
2. Select Override session management.
3. Select Set timeout.
4. Reduce the value of the timeout to less than 30 minutes.
5. Click OK and save the changes to the master configuration.
6. Repeat the previous steps. But select the module ITIM Self Service in Step 1.

The authenticated token can call only the SelfPasswordManager.resetPassword() API after authentication by using the challenge-response authentication system

If the system configuration property Lost password question behavior is set to Reset Password, the authenticated token can call only the SelfPasswordManager.resetPassword() API after the challenge-response authentication system authenticates a user.

Set the system configuration property Lost password question behavior to Direct Entry, so that the authenticated token can be used to call any API.

Perform either of these tasks after upgrading to IBM Security Identity Manager Version 6.0:
- Use only the SelfPasswordManager.resetPassword() API to reset a password after authentication by using the challenge-response authentication system.
- Make any API call valid by changing the Lost password question behavior system configuration property to Direct Entry.

Forms generate an authorization exception

A user without attribute-level permission to read or write for a field tries to set a value for a drop-down list or plain list box. The form designer generates an authorization exception. When the field value is not set, the form viewer sets the value to the first item in the list.

Take one of the following actions:
- Designate a user with the appropriate attribute-level permission to set the value of the problem field. After the field is set to any value, the user without read and write permissions can modify the entity without authorization violations.
- Add a blank value to the top of the list. If the form viewer selects the blank value, no authorization violation occurs because a blank value and no selection are treated as the same condition.
- Check the Use Blank Row check box on all drop-down lists that use Form Customization.
- If the data is not sensitive, grant both read and write permissions for this attribute to the user.
Making multiple modifications to a IBM Security Identity Manager object gives an unexpected outcome or failure with warning messages

A concurrent operation on the same object causes a trace condition that makes the outcome unpredictable. This problem occurs when using the APIs, such as submitting multiple requests to modify the same object in a while-for loop.

To ensure that all pending actions complete successfully, pause for an interval, such as a minute, before making a second modification to the same object. Alternatively, collect all the attribute changes on the same object and submit the changes as a single modify request. When you use IBM Security Identity Manager APIs, consider collecting all your attribute changes to the object in the while-for loop. Then submit the changes as a single modify request.

LDAP version 3 filters cause adapter problems

Using LDAP Version 3 filters causes inconsistent results from an adapter, or might not be accepted by the adapter as input. Using more than two arguments in a reconciliation filter might cause an error unless multiple operators are used.

For example, the following filter causes a FilterException error:
(& (eruid=a*) (ersql2000defdatabase=i*) (ersql2000deflanguage=E*))

Use filters that are compliant with LDAP Version 2.
(& ((eruid=a*) (ersql2000defdatabase=i*)) (ersql2000deflanguage=E*))

Cleaning up the database with the DBPurge script

Keeping the IBM Security Identity Manager Server database a manageable size is a good maintenance practice. You can use the DBPurge script to clean up the audit trail in the database by removing records that are related to completed workflow processes. The script handles only removal, not archiving, of these records. Use the script sparingly in order to avoid any unforeseen problems.

Command syntax

Use the following command to delete historical workflow audit data, non-workflow audit events, and reconciliation reporting entries from the database.

```
DBPurge.[sh|cmd] -age num_days [ -date yyyy-mm-dd[HH:mm] ]
   [ -grouping group_size ]
   [ -workflow wf_flag [-process_type proc_type] ]
   [ -audit audit_flag ] [ -recon recon_flag ]
```

Depending on your operating system, the command is located in one of the following directories:

- `ISIM_HOME\bin\win`
- `ISIM_HOME/bin/unix`

`-age num_days`

Specifies the age by the number of days of the records you want to remove. Records that were completed more than or equal to `num_days` ago are eligible for cleanup. The value must be greater than or equal to zero. A value of zero removes all data that is currently in the system.
-date date
  Specifies the deletion date and optional time in an alternative way. For example, '2010-08-15-22:00'. All records created on this date or earlier are deleted, based on the server timezone.

-grouping group_size
  Optional: Specifies the number of deleted entries in a single commit. The group size must be between 1 - 100 inclusive, where 50 is the default value.

-workflow wf_flag
  Optional: Determines whether workflow data is removed. The flag is Boolean, and its default setting is true.

-process_type proc_type
  Optional: Specifies a two-character parameter, which restricts the deletion of processes to the specified type.

  For example, 'AP' removes only processes of type Account Password Change. This parameter is relevant only when workflow data is removed. If you do not specify this parameter, then processes of any type are removed if they match the other parameters. For more information about the valid values, see the TYPE column description in the “Database and Directory > Server Schema Reference > Database tables reference > Workflow tables > PROCESS table” section on the IBM Security Identity Manager Information Center.

-audit audit_flag
  Optional: Determines whether non-workflow data is removed. The flag is Boolean, and its default setting is true.

-recon recon_flag
  Optional: Determines whether historical reconciliation data is removed. The flag is Boolean, and its default setting is true.

Note: You must set at least one of the data types such as workflow, audit, or reconciliation to true.

After you run the command, it reports the number of primary workflow, audit-based records, and reconciliation data that were removed. It also shows any errors or warnings.

Processing description

The following description illustrates the cleanup processing that occurs when you run DBPurge. Additional archive utilities can be built and run before running DBPurge. The exact implementation might vary.

DBPurge runs the following queries to locate the primary records to remove:

1. SELECT ID FROM PROCESS WHERE COMPLETED <= timestamp
2. SELECT ID FROM AUDIT_EVENT WHERE TIMESTAMP <= timestamp AND WORKFLOW_PROCESS_ID IS NULL
3. SELECT RECONID, ACCOUNTID FROM RECONCILIATION_INFO WHERE RECONID IN (SELECT RECONID FROM RECONCILIATION WHERE COMPLETED <= timestamp)
4. SELECT RECONID FROM RECONCILIATION WHERE COMPLETED <= timestamp

The value of timestamp is based on the specified -age parameter and uses the IBM Security Identity Manager date format yyyy-MM-dd HH:mm:ss:SSS GMT. As the primary records are selected, the data is removed along with data from the secondary, dependent tables that reference these identifiers. The deletion is done in groups.
An adjusted age specification supports consistency so that the record age accurately reflects the time zone of the record time stamps. This strategy supports consistent handling of record time zones. The following values are valid:

0 Deletes any records that completed before the current time.
1 Deletes any records completed before exactly 24 hours ago.

This utility includes multi-threaded deletion. For all databases, separate threads and database connections to read record identifiers and to carry out deletions. For DB2 databases, multiple threads carry out the deletion and improve performance. Each thread requires its own database connection. The utility fails if the appropriate number of database connections is not available. For DB2 databases, DBPurge requires five connections; for other databases, it requires only two.

The following example is a high-level version of the statements for each table, and it illustrates the rows that are removed from each table.

**Example**

The following delete statements remove rows that reference identifiers from query (1) and from the PROCESS table:

```
DELETE FROM WORKITEM WHERE PROCESS_ID = ?
DELETE FROM ACTIVITY_LOCK WHERE PROCESS_ID = ?
DELETE FROM PROCESSLOG WHERE PROCESS_ID = ?
DELETE FROM PROCESSDATA WHERE PROCESS_ID = ?
DELETE FROM PENDING WHERE PROCESS_ID = ?
DELETE FROM PASSWORD_TRANSACTION WHERE PROCESS_ID = ?
DELETE FROM ACTIVITY WHERE PROCESS_ID = ?
DELETE FROM WORKFLOW_CALLBACK WHERE PROCESS_ID = ?
DELETE FROM SYCH_POINT WHERE PROCESS_ID = ?
DELETE FROM AUDIT_MGMT_PROVISIONING WHERE EVENT_ID IN
  (SELECT ID FROM AUDIT_EVENT WHERE WORKFLOW_PROCESS_ID = ?)
DELETE FROM AUDIT_MGMT_TARGET WHERE EVENT_ID IN
  (SELECT ID FROM AUDIT_EVENT WHERE WORKFLOW_PROCESS_ID = ?)
DELETE FROM AUDIT_MGMT_DELEGATE WHERE EVENT_ID IN
  (SELECT ID FROM AUDIT_EVENT WHERE WORKFLOW_PROCESS_ID = ?)
DELETE FROM SCHEDULED_MESSAGE WHERE REFERENCE_ID = ?
DELETE FROM LCR_INPROGRESS_TABLE WHERE CHILD_ID = ?
DELETE FROM PROCESS WHERE ID = ?
```

The following delete statements remove rows that reference identifiers from query (2) and from the AUDIT_EVENT table:

```
DELETE FROM AUDIT_MGMT_PROVISIONING WHERE EVENT_ID = ?
DELETE FROM AUDIT_MGMT_TARGET WHERE EVENT_ID = ?
DELETE FROM AUDIT_MGMT_DELEGATE WHERE EVENT_ID = ?
DELETE FROM AUDIT_EVENT WHERE WORKFLOW_PROCESS_ID = ?
DELETE FROM SCHEDULED_MESSAGE WHERE REFERENCE_ID = ?
DELETE FROM LCR_INPROGRESS_TABLE WHERE CHILD_ID = ?
DELETE FROM PROCESS WHERE ID = ?
```

The following delete statements remove rows that reference identifiers from query (3) and from the RECONCILIATION_INFO table:

```
DELETE FROM RECONCILIATION_INFO WHERE RECONID = ? AND ACCOUNTID = ?
```

The following delete statements remove rows that reference identifiers from query (4) and from the RECONCILIATION table:

```
DELETE FROM RECONCILIATION WHERE RECONID = ?
```

**Customization problems**

This section describes solutions for problems with customization.
Do not use the er prefix in label names

If you create a schema attribute label in the CustomLabels.properties file when you create a manual service definition, do not begin the name of the label with the characters er. This prefix is reserved by IBM Security Identity Manager.

The CustomLabels.properties file is placed in this default directory:

**Microsoft Windows systems**

C:\Program Files\IBM\isim\data

**UNIX and Linux systems**

/opt/IBM/isim/data

IBM Security Identity Manager does not provide a method to create an outer join in the custom report designer

Create an outer join in the custom report designer by designing a hooked report that is a custom servlet. Put logic for an outer join of database tables in the custom servlet itself. The custom servlet, registered with the report.xml file, is run like a typical report from the IBM Security Identity Manager reporting engine.

Adapter request fails on an orphan account

You might need to bypass the password validation on an orphan account when a request is submitted from an adapter. The enRole.properties file contains the following property to bypass the password validation on an orphan account when a request is submitted from an adapter.

reversePasswordSynch.bypassPwdValidationOnOrphanAccount

Set this value to true to bypass the password validation.

Manager group is not updated when using custom person entity

If you use a custom person entity and want the accounts automatically added to the service manager group, the schema must be mapped correctly.

The automatic population of managers into the manager group uses the ersupervisor attribute in the user profile schema. The ersupervisor attribute is an IBM Security Identity Manager attribute and must be mapped to the attribute in the schema that stores the manager relationship. For the ready-to-use Person profile, ersupervisor is mapped to the manager attribute in the inetOrgPerson objectclass. The mapping of ersupervisor to manager is appropriate for a custom user profile based on an objectclass that extends inetOrgPerson.

**Mapping the ersupervisor attribute**

1. Select **Configure System** > **Manage Entities**.
2. Click the name of the custom user profile.
3. Click the **Attribute Mapping** tab.
4. Select ersupervisor as the IBM Security Identity Manager attribute.
5. Select the appropriate Custom LDAP attribute, such as manager.
6. Click **Map** to map the attribute.
7. Click **OK** to save your changes.
IBM Security Identity Manager applets do not work

WebSEAL file and WebSphere Application Server configuration causes function problems with the applets in IBM Security Identity Manager.

Problem

A IBM Security Identity Manager applet, such as the workflow designer, does not work. It does not provide support when you do the following changes:

- Set as pass-http-only-cookie-attr=yes in the WebSEAL configuration file.
- Set the HttpOnly attribute to JESSIONID in WebSphere Application Server.
- Set the HttpOnly attribute to PD-S-SESSION-ID cookie in WebSphere Application Server.

An error can occur with these settings.

The cookie does not supply information to the applet with these settings. As a result, you cannot use the IBM Security Identity Manager applet through WebSEAL.

Solution

The WebSEAL does not pass the HttpOnly attribute in the cookie. You can access the cookie information from the applet with the following setting in the WebSEAL configuration file:

pass-http-only-cookie-attr=no
Chapter 7. Troubleshooting WebSphere Application Server problems

This section describes solutions for potential WebSphere Application Server problems.

The following links can help you to identify the problem, find the appropriate troubleshooting information, and then collect any necessary information about WebSphere Application Server:


For more information, see the WebSphere Application Server Information Center.

Installing IBM Security Identity Manager on an operating system with the Turkish language setting

To install IBM Security Identity Manager on an operating system with the Turkish language setting, change the Java Virtual Machine (JVM) settings before you run the IBM Security Identity Manager installer.

1. Log on to the WebSphere Application Server Administrative Console.
2. Select Servers > Application Servers > serverName > Process Definition > Java Virtual Machine.

   Note: serverName is the name of the server. For example, server1.

3. In the Generic JVM parameters field, add the following JVM parameter:
   `Duser.language=en -Duser.region=US`

4. Click Apply.
5. Click the Save link in the Messages box.
6. Restart the WebSphere Application Server.

Ignoring exceptions in WebSphere Application Server logs

Some exceptions might occur during the IBM Security Identity Manager installation. You can ignore these exceptions after the installation. It does not affect the IBM Security Identity Manager installation or operation.

The WebSphere Application Server SystemOut.log file can contain the following messages:

```
PrivExAction E   J2CA0044E: The Connection Manager failed to get a Subject from the security service associated with ConnectionFactory itimBusDataSource.
   Received exception javax.security.auth.login.LoginException:
   Incorrect authDataEntry and alias is: itim_init
ConnectionMan E   J2CA0060E: PrivilegedActionException calling doPrivileged:
   java.security.PrivilegedActionException:
   javax.resource.ResourceException: LoginException getting Subject
```

© Copyright IBM Corp. 2012
IBM Security Identity Manager uninstallation or reinstallation might create bus error messages

Bus error messages might be logged in the SystemOut logs during the IBM Security Identity Manager uninstallation or reinstallation.

The error messages can be as follows:

00000013 XARecoveryDat W  WTRN0005W: The XAResource for a transaction participant could not be recreated and transaction recovery may not be able to complete properly.
The resource was [com.ibm.ws.sib.ra.recovery.impl.SibRaXaResourceInfo@1562336543
busName=itim_bus meName=timperf04_AppServCluster.000-itim_bus
meUuid=8A1304029A6B5E5A xaRecoveryAlias=itim_jms useServerSubject=false
providerEndpoints=null]
The exception stack trace follows: com.ibm.ws.Transaction.XAResourceNotAvailableException: com.ibm.websphere.sib.exception.SIResourceException: CWSIT0019E: No suitable messaging engine is available on bus itim_bus that matched the specified connection properties {connectionMode=Recovery, targetType=MEUuid, busName=itim_bus, providerEndpoints=null, targetGroup=8A1304029A6B5E5A}.
Reason for failure: CWSIT0103E: No messaging engine was found that matched the following parameters: bus=itim_bus, targetGroup=8A1304029A6B5E5A, targetType=MEUuid, targetSignificance=Required, transportChain=InboundSecureMessaging, proximity=Bus.

Caused by: com.ibm.websphere.sib.exception.SIResourceException: CWSIT0019E: No suitable messaging engine is available on bus itim_bus that matched the specified connection properties {connectionMode=Recovery, targetType=MEUuid, busName=itim_bus, providerEndpoints=null, targetGroup=8A1304029A6B5E5A}.
Reason for failure: CWSIT0103E: No messaging engine was found that matched the following parameters: bus=itim_bus, targetGroup=8A1304029A6B5E5A, targetType=MEUuid, targetSignificance=Required, transportChain=InboundSecureMessaging, proximity=Bus.

The errors are logged due to the WebSphere XA recovery messaging engines and does not affect the IBM Security Identity Manager installation or operation.

To prevent the errors, complete these steps:
1. Uninstall the IBM Security Identity Manager application.
2. Stop the WebSphere Application Server.
3. Delete the content in the transaction logs from WAS_HOME/profiles/profilename/tranlog/.

Note: Stop the WebSphere Application Server before deleting the transaction log contents. This operation might affect other non-erroneous transactions.

If you continue to see XAER or recovery errors, review the database for in-doubt transactions.

For more information about these errors, see:

Chapter 8. Troubleshooting WebSphere Application Server authentication problems

This section describes solutions for potential WebSphere Application Server authentication problems.

IBM Security Identity Manager does not authenticate with WebSphere Application Server

IBM Security Identity Manager does not establish an authentication with WebSphere Application Server.

Problem

IBM Security Identity Manager does not start. The WebSphere Application Server systemOut.log file contains the following error message:

```
J2CA0138E: The Message Endpoint activation failed for  
ActivationSpec policySimulationActivationSpec  
(com.ibm.ws.sib.api.jmsra.impl.JmsJcaActivationSpecImpl) and MDB application  
ITIMmdb_ejb.jar#enroleejb.PolicySimulationMDB due to the following exception:  
javax.resource.ResourceException:  
CWSIV0954E: The authentication exception  
com.ibm.wsspi.sib.core.exception.SIAuthenticationException:  
CWSIP0301E: Unable to authenticate user isimsystem when creating  
a connection to secure messaging engine  
sabresNode01.server1-itim_bus on bus itim_bus. was thrown while attempting  
to create a connection on factory  
com.ibm.ws.sib.processor.impl.MessageProcessor@20e420e4.
```

The J2C authentication alias used for the itim_bus service integration bus is not configured correctly. The user specified in this J2C alias cannot authenticate to connect to the secure messaging engine.

Solution

To configure the J2C authentication alias correctly for the itim_bus service integration bus, complete these steps:

1. Log on to the WebSphere Application Server Administrative Console.
2. From the navigation tree, click Security > Bus security to open the Buses page.
3. Click the itim_bus link to open the Security for bus itim_bus page.
4. Ensure that the security status of the itim_bus link is set to Enabled before you click the link.
5. Ensure that the following options are listed:
   a. The itim.jms option in the Inter-engine authentication alias list from the General Properties section.
   b. The security domain option that the itim_bus uses in the Use the selected domain list from the Bus security domain section.

If you select the security domain that the IBM Security Identity Manager installer created, then the Use the selected domain list shows the ISIMSecurityDomain option. This option is the default name for the security domain.
6. Click the **JAAS – J2C authentication data** link from the **Related Items** section to open the **JAAS – J2C authentication data** page.

7. Click the **itim_jms** authentication alias link.

8. Ensure that the correct user ID and the password are set for the **itim_jms** authentication alias.

   The **itim_jms** alias user ID and the enrole.appServer.ejbuser.principal property user ID must be the same. The user ID is in the ISIM_HOME/data/enRole.properties file. ISIM_HOME is the directory where IBM Security Identity Manager is installed.

9. In the **User ID** field, type the user ID that you specified in the enRole.properties file.

   **Note:** The user ID is case-sensitive.

   For example, if the user ID is isimsystem in the enRole.properties file, then set the user ID for the **itim_jms** alias to isimsystem, not isimSystem.

10. Retype the password and click **OK** or **Apply**.

11. Click **Save**.

12. Restart the WebSphere Application Server.
Chapter 9. Adapter problems

If you encounter communication problems between an adapter and IBM Security Identity Manager Server, see “IBM Security Identity Manager Adapters” on the IBM Security Identity Manager Information Center.

The “IBM Security Identity Manager Adapters” section contains adapters-specific installation and configuration guides.
Chapter 10. Troubleshooting database problems

This section describes solutions for potential database problems.

Generating reports is slow and causes timeouts

You might encounter slow performance or transaction time-outs during report generation for certain reports against large data sets.

To improve performance and reduce time-outs, see the IBM Security Identity Manager Performance Tuning Guide for suggested indexes to set on columns in Report DB tables.

Passwords are changed or expired

The product installation creates three system users to enable communication between the database and IBM Tivoli Directory Server. The default users are itimuser, db2admin, and ldapdb2.

The db2admin user is created with a password that never expires.

Passwords for ldapdb2 and itimuser expire based on the password policy of your system. If these passwords expire or are changed, reconfigure IBM Security Identity Manager and its associated middleware to use the new passwords. For example, if the itimuser user password expires, database access fails unexpectedly. For more information, see the Installation and Configuration Guide.

Creation of DB2 schema fails during middleware configuration

If the IBM Security Identity Manager installation program or the middleware configuration utility fails to set up the DB2 database schema after you specified DB2 parameters, check the DB2 configuration log. The log is cgf_itim_mw.log or dbConfig.stdout. Check it to determine the source of the error.

The problem might be a lack of allocated swap space.

For example, if the configuration log indicates that the DB2 buffer pools for IBM Security Identity Manager (ENROLEBP) cannot be created immediately, increase the swap space. Then try the configuration again.

The following procedure describes creating an auxiliary swap file for extra swap space on an existing partition:

1. Back up all important data before you start this procedure.
2. Log on as root (type su - and enter your root password).
3. Determine how much existing swap space you have and how much is already in use. At a command prompt, type swapon -s:
   
   Output like the following is displayed, where Size and Used are in KB:

<table>
<thead>
<tr>
<th>Filename</th>
<th>Type</th>
<th>Size</th>
<th>Used</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda3</td>
<td>partition</td>
<td>522104</td>
<td>315540</td>
<td>-1</td>
</tr>
</tbody>
</table>
If the total swap space is less than 512 MB or if the available swap space is less than 512 MB, you must create and configure an auxiliary file as swap space by following the remaining steps.

4. Determine where to put the auxiliary file. At a command line, type `df -m`  
   
   `df` specifies the disk free command.  
   `-m` specifies to show the value in megabytes.  
   
   The following output is displayed:  
   
   ```  
   Filesystem  1M-blocks Used Available Use% Mounted on  
   /dev/sda2 24607 7617 15741 33% /  
   /dev/sda1 99 10 85 10% /  
   ```  
   
   The `Available` column indicates the amount of free space on the partitions, beginning with the root partition. If plenty of disk space is available, the swap space equals twice the amount of memory installed on the system.

5. Use the data dump (`dd`) command to create an auxiliary file that is used as a swap space:  
   ```bash  
   dd if=/dev/zero of=/swap_space_name bs=1M count=swap_file_size  
   ```  
   
   `-if=/dev/zero` input file. The `/dev/zero` device file provides zeros that are written to the output file.  
   `-of=/swap_space_name` output file. Defines the path and name of the output file. In this case, the output file is used as the swap space partition that receives the data; for example, `of=/aux_swap_space`.  
   `-bs=1M` specifies the unit type. In this case, the unit of 1 MB per digit is specified.  
   `-count=swap_file_size` specifies the size of the partition; for example, `count=1536` and `bs=1M` defines a partition with a capacity of 1536 MB (1.5 GB).

6. Set up the new partition for a swap file. Type the following command:  
   ```bash  
   mkswap /swap_space_name  
   ```  
   For example, if you used the `dd` command to specify a partition named `aux_swap_space`, type `mkswap /aux_swap_space`.  

7. Use the `swapon` command to turn on the swap file; for example, type the following command at the command prompt:  
   ```bash  
   swapon /aux_swap_space  
   ```

8. Verify the size of the new swap file. Type `swapon -s` again to view the existing swap partition and the new swap file you created.

9. If you restart the computer, the new swap file is not active. To make the swap file active, run the `swapon /swap_space_name` command. For example, `swapon /aux_swap_space`.

10. Make the auxiliary file a permanent swap file by editing the `/etc/fstab` file:  
    a. Back up the `/etc/fstab` file.  
    
    **Attention:** If you manually edit `/etc/fstab`, then your system might not reboot if you edit other than the one described in these steps.  
    b. Locate the permanent swap partition entry, which looks like the following entry:  
       ```bash  
       /dev/sda3 swap swap defaults 0 0  
       ```
c. Immediately after this line entry, add an entry for the new swap space file. For example:

```
/aux_swap_space none swap defaults 0 0
```

d. Save the file.

e. Run the `diff` command to ensure that the only change you made was the addition of a single-line entry from Step 3.

f. If you made other changes accidentally, restore the backup file and repeat these steps. Begin with Step 4.

---

**Database update fails with an SQL error**

The following example shows an error that can occur during database update operations. You might receive similar errors.

```
com.ibm.db2.jcc.a.SqlException: DB2 SQL error:
  SQLCODE: -964, SQLSTATE: 57011, SQLERRMC: null
at com.ibm.db2.jcc.a.hd.d(hd.java(Compiled Code))
at com.ibm.db2.jcc.a.db.ha{dba.java(Compiled Code)}
at com.ibm.db2.jcc.a.db.ha{db.a.java(Compiled Code)}
at com.ibm.db2.jcc.c.w.a{w.java(Inlined Compiled Code)}
at com.ibm.db2.jcc.c.w.a{w.java(Inlined Compiled Code)}
at com.ibm.db2.jcc.a.id.cb{ia.java(Inlined Compiled Code)}
at com.ibm.db2.jcc.a.id.d{ia.java(Compiled Code)}
at com.ibm.db2.jcc.a.id.d{ia.java(Compiled Code)}
at com.ibm.db2.jcc.a.id.executeUpdate{ia.java(Compiled Code)}
  executeUpdate(WSJdbcPreparedStatement.java(Compiled Code))
  executeUpdate(WSJdbcPreparedStatement.java(Compiled Code))
```

The `SQLCODE: -964, SQLSTATE: 57011` error occurs when the transaction log space is depleted. This problem can occur because of a temporary increase in the number of active transactions.

1. Open a DB2 command window.
2. Run the following command:

```
db2 get snapshot for all on itimdb
```

3. Examine the values of the following entries to determine if the database is running low on available log space:
   - Log space available to the database
   - Log space used by the database
   - Secondary logs allocated currently

4. Increase the number of secondary log files available to the database by 12 to provide additional log file space:
   a. From the DB2 command window, run the following command:

```
db2 update db cfg for itimdb using logsecond
```
   b. Specify a value of `logsecond` plus 12 for `x`.

If the problem reoccurs, DB2 UDB in-doubt transactions might be the cause. In-doubt transactions result in transaction log space shortage. Previous server failures or crashes cause the transaction log to become full when transactions are performed. To correct this problem, complete these steps:

**CAUTION:**
If IBM Security Identity Manager Server is running, changing transactions with timestamps close to the current time can cause server failures.
1. From a DB2 command window, connect to the IBM Security Identity Manager database.
2. Run the following command:
   ```
   db2 list indoubt transactions with prompting
   ```
3. Roll back any transactions with a timestamp near the time of the server crash.

### Error occurs during recovery of Oracle database transactions

The WTRN0037: The transaction service encountered an error on an xa_recover operation error occurs during automatic generation of IBM Security Identity Manager accounts.

WebSphere Application Server attempted to recover Oracle database transactions. Oracle requires special permissions for recovery. You can correct this problem by running the following command to grant permissions:

1. Log in as the user SY$.
2. Run the following commands:
   ```
   grant select on pending_trans$ to public;
   grant select on dba_2pc_pending to public;
   grant select on dba_pending_transactions to public;
   grant execute on dbms_system to <user>;
   ```

The default IBM Security Identity Manager database user is itimuser.

#### System failure causes data synchronization problem

If a system fails during data synchronization, you might not be able to run data synchronization after a system restore. WebSphere Application Server and database failures can cause this problem.

When data synchronization starts, IBM Security Identity Manager sets the STATUS column to Started in the ITIMDB.SYNCHRONIZATION_HISTORY table. When the system fails, the status is not updated to Failure. You must set data synchronization status correctly in the SYNCHRONIZATION_HISTORY table. Complete these steps:

1. Connect to the IBM Security Identity Manager database.
2. Open the SYNCHRONIZATION_HISTORY table.
3. Locate the entry for data synchronization that reads Started in the STATUS column.

   **Note:** Only one Started entry is displayed.
4. Change the value of Started to Failure.
5. Commit the change to the database.
6. Run data synchronization.

#### Oracle database fails to create enrole_data_001.dbf data file

You might receive an error message that enrole_data_001.dbf exists. This error occurs during IBM Security Identity Manager installation. It also occurs after running the DBConfig command.
You can point several instances of IBM Security Identity Manager to multiple databases on the same Oracle server. Complete these steps:

1. Copy and modify this code example in the $ISIM_home/config/rdbms/oracle/enrole_admin.sql file. The bold highlighting shows the two lines to modify.

   **Note:** The value enrole_data_001.dbf was changed to enrole_data_002.dbf. Increment this value for each additional instance on the same Oracle server.

   ```
   # pwd
   /u02/enrole/config/rdbms/oracle
   # more enrole_admin.sql
   CREATE TABLESPACE enrole_data
   DATAFILE 'enrole1_data_002.dbf'
   SIZE 160M
   AUTOEXTEND ON
   NEXT 20M
   MAXSIZE 1024M
   DEFAULT STORAGE (INITIAL 10M
   NEXT 1M
   PCTINCREASE 10)
   PERMANENT
   ONLINE
   LOGGING;
   
   CREATE TABLESPACE enrole_indexes
   DATAFILE 'enrole1_idx_002.dbf'
   SIZE 160M
   AUTOEXTEND ON
   NEXT 20M
   MAXSIZE 1024M
   DEFAULT STORAGE (INITIAL 10M
   NEXT 1M
   PCTINCREASE 10)
   PERMANENT
   ONLINE
   LOGGING;
   
   CREATE USER itimuser IDENTIFIED BY itimuserPwd
   DEFAULT TABLESPACE enrole_data
   QUOTA UNLIMITED ON enrole_data
   QUOTA UNLIMITED ON enrole_indexes;
   GRANT CREATE SESSION TO enrole;
   GRANT CREATE TABLE to enrole;
   #
   ```

2. Add the code to create the $ISIM_home/config/rdbms/oracle/enrole_admin.sql file.

   **Note:** Add the code after you start the IBM Security Identity Manager installation, and before you submit the DBConfig portion of the installation.

---

### Cannot connect to the database after running the Middleware Configuration program

You cannot connect to the database after running the Middleware Configuration program on DB2. You might see this error message: SQL1762N Unable to connect to database because there is not enough space to allocate active log files. SQLSTATE=08004.

This message indicates that the logging size setting might be too large to create when you reconnect. Tuning IBM Security Identity Manager sets logging to the recommended size.
Fixing data replication errors for invalid object names

Data replication errors can occur in a cluster environment if the shared access configuration utility was not run.

**About this task**

When IBM Security Identity Manager is deployed in a cluster environment, and shared access is configured, data replication can report errors. The errors indicate that an invalid object name was found. The pattern of the error is:

Invalid object name itimuser.isim_object_name

For example:

Invalid object name 'itimuser.erAccountItem'
Invalid object name 'itimuser.erServiceItem'
Invalid object name 'itimuser.errSystemUser'

In this case, data replication fails if you run **DBConfig** to drop all database tables but do not run **SAConfig** to repopulate the tables that are specific to the shared access module.

The file `ISIM_HOME/data/dataSynchronization.properties` contains entries that are configured to replicate, such as `erAccountItem` or `erServiceItem`. However, the replication component cannot find the target replication table that is specified in `DB_REPLICATION_CONFIG`. In this case, the component defaults to the class name.

To fix this problem, complete the steps in the following procedure.

**Procedure**

1. On the deployment manager, change directory to the bin directory in IBM Security Identity Manager installation location and run the **SAConfig** utility.

   For example:

   **Table 9. Running SAConfig**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>In C:\Program Files\IBM\isim\bin, either click SAConfig or open a command window and enter <strong>SAConfig</strong>.</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>In /opt/IBM/isim/bin, enter ./SAConfig.</td>
</tr>
</tbody>
</table>

2. Update the clipassword property in the `ISIM_HOME/data/KMIPServer.properties` file.

   You can specify any string value. For example:

   `clipassword=test`

   **Note:** Edit this file only on the deployment manager.

3. Configure the keystore files for the credential vault server.

   **Note:** Complete this step only on the deployment manager. You do not need to complete it on the cluster members.
In the following command, ensure that the value of the -p parameter matches the value you specified for clipassword in the ISIM_HOME/data/KMIPServer.properties file.

Use the command for your operating system:

- On the Windows operating systems, enter:
  ```
  cd /d "ISIM_HOME\lib"
  From the ISIM_HOME\lib directory, run the following command:
  "ISIM_HOME\jre\jre\bin\java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar;
  com.ibm.sec.authz.xacml4j_7.3.1.jar;
  j2ee.jar;
 ojdbc.jar;
  db2jcc.jar;
  db2jcc_license_cu.jar;
  sqljdbc.jar;
  com.ibm.tklm.kmip.jar;
  CVCommon.jar;
  CVCore.jar;
  CVCli.jar;
  com.ibm.tklm.credvault.common.jar;
  commons-cli.jar;
  com.ibm.cv.kmip.ext.jar
  -DKMIPConfigProperties="$USER_INSTALL_DIR$\data$\KMIPServer.properties"
  -Djava.security.auth.login.config=login.config
  -Djava.security.auth.policy=jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

- On the UNIX or Linux operating systems, enter:
  ```
  cd "ISIM_HOME/lib"
  From the ISIM_HOME/lib directory, run the following command:
  "ISIM_HOME/jre/jre/bin/java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar;
  com.ibm.sec.authz.xacml4j_7.3.1.jar;
  j2ee.jar;
  ojdbc.jar;
  db2jcc.jar;
  db2jcc_license_cu.jar;
  sqljdbc.jar;
  com.ibm.tklm.kmip.jar;
  CVCommon.jar;
  CVCore.jar;
  CVCli.jar;
  com.ibm.tklm.credvault.common.jar;
  commons-cli.jar;
  com.ibm.cv.kmip.ext.jar
  -DKMIPConfigProperties="$USER_INSTALL_DIR$\data$\KMIPServer.properties"
  -Djava.security.auth.login.config=login.config
  -Djava.security.auth.policy=jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

The command generates two credential vault keystore files, cvKeystore.jceks and pwdEncKeystore.jceks, under the ISIM_HOME/data/keystore directory. It updates the credential vault database data entry and the encryption key in ISIM_HOME/data/KMIPServer.properties.

4. Copy the generated keystore files and KMIPServer.properties to the WAS_DM_profile_path/config/cells/cellName/itim directory.

   **Note:** Complete this step only on the deployment manager. You do not need to complete it on the cluster members.

5. Manually synchronize the nodes from the WebSphere Application Server Deployment Manager console.
6. On each cluster member, copy the following credential vault files from the WebSphere profile directory hierarchy to the IBM Security Identity Manager data directory hierarchy:

Table 10. Credential vault server files to copy

<table>
<thead>
<tr>
<th>Copy this file:</th>
<th>To this location:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS_PROFILE_PATH/config/cells/cellName/itim/cvKeystore.jceks</td>
<td>ISIM_HOME/data/keystore/cvKeystore.jceks</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH/config/cells/cellName/itim/pwdEncKeystore.jceks</td>
<td>ISIM_HOME/data/keystore/pwdEncKeystore.jceks</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH/config/cells/cellName/itim/KMIPServer.properties</td>
<td>ISIM_HOME/data/KMIPServer.properties</td>
</tr>
</tbody>
</table>

7. Restart the WebSphere Application Server cluster.
Chapter 11. Troubleshooting IBM Tivoli Directory Server problems

This section describes solutions for potential problems using IBM Tivoli Directory Server.

User modifications fail with ObjectClassViolation errors in IBM Tivoli Directory Server

The requests to create or modify a user fail when using the default Person user profile. Length restrictions for certain user attributes cause this failure.

Problem

The IBM Tivoli Directory Server schema imposes length restrictions on several attributes in the inetOrgPerson object class such as initials, employeeNumber, and telephoneNumber.

The following errors can help you determine if a user-related request fails due to a length restriction:

- The audit trail request for IBM Security Identity Manager displays the following error in the process result:
  
  CTGIMO017E: The following directory server schema violation occurred. Error: [LDAP: error code 65 - Object Class Violation]

  You can observe this error message by viewing the failed request in the View Requests console.

- The IBM Tivoli Directory Server ibmslapd.log file contains an error similar to the following:
  
  GLPRDB069E: Attribute EMPLOYEE NUMBER has a maximum value length of 20. Current attribute value is of length 27.

  The ibmslapd.log log file is produced by IBM Tivoli Directory Server.

Solution

You can prevent request failures due to length violations with one of the following actions:

- Customize the Person form with the necessary field constraints. Customizing the Person form with the necessary field constraints prevents user errors and ensures that values conform to the requirements.

- Increase the maximum length of the attributes in the directory server schema.

Note: IBM Tivoli Directory Server specifies each schema length constraint in number of bytes. Certain character sets require multiple bytes to represent a single character. When customizing the form or changing the schema length constraints, it is important to consider whether or not attribute values are specified using a multibyte character set.
Preventing connection problems with multiple LDAP sessions

On the Microsoft Windows operating system, the IBM Tivoli Directory Server supports a default of 64 concurrent connections.

Connection attempts beyond 64 connections from the IBM Security Identity Manager Server fail and display a Directory Server not available error message like this example:
Connection pool exceeded: directory server not available

To limit connection problems, define the value of SLAPD_OCHANDLERS to increase the available connections.

1. Locate the following stanza in the ibmslapd.conf file:
   dn: cn=Front End, cn=Configuration
   The default directory of the ibmslapd.conf file depends on the operating system.

   **Microsoft Windows systems**
   C:\idssldap-ldapdb2\etc

   **UNIX and Linux systems**
   /home/ldapdb2/idsslapd-ldapdb2/etc

2. Add the following line to this stanza:
   `ibm-slapdsetenv: SLAPD_OCHANDLERS=number-of-threads`
   One thread supports 64 connections. If there are multiple instances of the IBM Security Identity Manager Server, increase this value. If there are two instances of the server, each requiring a minimum of 50 simultaneous LDAP connections, specify a value of 2 or larger. For example, add this line to the following stanza:
   `ibm-slapdsetenv: SLAPD_OCHANDLERS=4`

3. Save the changes.
4. Restart the IBM Tivoli Directory Server so that the changes take effect.

Changing from a Sun ONE Directory Server causes index loss

After an initial installation that uses the Sun ONE Directory Server, changing to another LDAP server causes the loss of certain indexes.

You must add the missing indexes manually to the new LDAP server from the er-indexes.conf file on the initial LDAP server.

Complete these tasks from the Sun ONE Directory Server administration console:
1. Navigate to `Data=itim_suffix`. For example, `itim_suffix` is a value such as `dc=com`. `dc` denotes Domain Component.
2. Click **Add attributes**.
3. Add the following attributes:
   - `index erparent eq`
   - `index erroles eq`
   - `index erservice eq`
   - `index ersupervisor eq`
   - `index ersponsor eq`
   - `index erhost eq`
   - `index erauthorizationowner eq`
   - `index erprerequisite eq`
4. Save the attributes.
5. Add the rules that are specified next to the attribute name.
6. Navigate to Data=itim_suffix and right-click itim_suffix.
7. Select the Re-index option.
Chapter 12. Troubleshooting Shared Access Module problems

This section describes the solutions for potential Shared Access Module problems. You can enable Shared Access Module during installation or after installation with the `SAConfig` utility. The utility is in the `ISIM_HOME/bin` directory.

Adding a credential to the vault fails with error CTGIMO003E

An administrative request to add a credential to the credential vault fails with error CTGIMO003E.

**Symptoms**

An error occurs when a request to add a credential to vault fails. The following error message is logged in the `msg.log` file:

```
CTGIMO003E The c:cvserverCVClient.properties
(The system cannot find the file specified.)
```

Also, the `trace.log` file contains the following exception:

```
java.io.FileNotFoundException: c:cvserverCVClient.properties
(The system cannot find the file specified.)
at java.io.FileInputStream.open(Native Method)
```

**Solution**

This problem can occur on Microsoft Windows systems because the operating system uses backslashes "\" in file paths.

To solve the problem, examine the contents of the `ISIM_HOME\cvserver.properties` file. For example:

```
KMIPConfigProperties=c:\cvserver\CVClient.properties
javax.net.ssl.trustStore=c:\cvserver\myClientTrust.jks
javax.net.ssl.trustStorePassword=password
javax.net.ssl.keyStore=c:\cvserver\myClientStore.jks
javax.net.ssl.keyStorePassword=password
javax.net.ssl.keyStoreType=jks
javax.net.ssl.trustStoreType=jks
```

In the example, notice that the path names are separated by a single backslash "\" mark. This use of a single backslash causes the problem. To fix the problem, replace the single slash mark with double backslash "\\". For example:

```
KMIPConfigProperties=c:\\cvserver\\CVClient.properties
javax.net.ssl.trustStore=c\\\cvserver\\myClientTrust.jks
javax.net.ssl.trustStorePassword=password
javax.net.ssl.keyStore=c\\\cvserver\\myClientStore.jks
javax.net.ssl.keyStorePassword=password
javax.net.ssl.keyStoreType=jks
javax.net.ssl.trustStoreType=jks
```

Adding a credential to the vault fails with error CTGIMO242E

An administrative request to add a credential to the vault fails with error CTGIMO242E.
Symptoms

An error occurs when a request to add a credential to vault fails. The following error message is logged in the msg.log file:

CTGIMO242E The following credential vault error occurred.
Error:
CTGIMO242E The c:cvserverCVClient.properties
(The system cannot find the file specified.)

Also, the following exception is logged in the trace.log file:

com.ibm.cv.CVProxyException: KMIPProxy Exception:
Unrecognized exception reason
CTGKP4025E Error connecting to the remote server.
Error is Connection refused: connect.
Exception: java.net.ConnectException:
Connection refused: connect

The following properties are present in the tklm_debug.log file:
ALL: Connecting to http://localhost:8080/WebUI/kmip.html

Solution

There is a problem with the formatting of the settings in the kmip.html file. Examine the settings and look for leading or trailing spaces. Remove any leading or trailing spaces.

Following is an example of a file with the properties formatted correctly:

```
protocol=ssl
host=localhost
port=9696
path=/cvsvc/kmip.html
```

An authorized credential does not show in the Self Service user interface checkout page

The shared access policy entitlement preview shows that a credential is included by the entitlement. But that credential does not show up in the Self Service user interface (SSUI) checkout page to a user who is entitled to the credential. This behavior indicates that the problem is most likely caused by inappropriate credential setting.

Before you begin


Depending on how your system administrator customized your system, you might not have access to this task. To obtain access to this task or to have someone complete it for you, contact your system administrator.

Ensure that you created an ACI for the protection category of Credential.
About this task

The IBM Security Identity Manager Console supports the addition of user credentials into a credential vault. When you add a credential to the vault, you can apply values for each of the credential settings. Use this task to fix the credential configuration settings.

Procedure

1. From the navigation tree, select Manage Shared Access > Manage Credential Vault > Select a Credential.
2. On the Select a Credential page, click Refresh under Credentials.
3. Click the credential from the results to open the Change Configuration Settings page.
4. Under Credential Settings, verify that you selected these settings:
   - The Require the checkin and checkout process for the shared IDs option to specify the checkin and checkout process for the accounts.
   - The Enable checkout search check box to enable the credentials for a checkout search. The accounts are searched for the checkout process on the Self Service user interface.
5. Click Submit to save the configuration settings.

What to do next

Log on to the Self Service user interface to verify that the credential is listed under My Shared Access > Check out Credential.

Fixing problems when LDAP is reconfigured after installation

If LDAP is configured again after the IBM Security Identity Manager installation, you must run the SAConfig utility.

When LDAP is reconfigured again after the completion of the IBM Security Identity Manager installation, all the default data for the shared access module is lost. This reconfiguration can cause problem with actions that require access to LDAP data.

To fix the problems, run the SAConfig utility. This utility repopulates the default data for the shared access module.

The steps differ depending on whether your deployment is on a WebSphere single server or in a WebSphere cluster. Use the instructions for your deployment:

- Configuring shared access on a single server after LDAP reconfiguration
- Configuring shared access on a WebSphere cluster after LDAP reconfiguration

Configuring shared access on a WebSphere single server after LDAP reconfiguration

When LDAP is reconfigured after the IBM Security Identity Manager installation, you must run the SAConfig utility again.

Procedure

1. Change to the bin directory in IBM Security Identity Manager installation location and run the utility.
For example:

Table 11. Running SAConfig

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>In C:\Program Files\IBM\isim\bin, either click SAConfig or open a command window and enter <strong>SAConfig</strong>.</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>In /opt/IBM/isim/bin, enter <strong>./SAConfig</strong>.</td>
</tr>
</tbody>
</table>

2. Restart WebSphere Application Server.

**Configuring shared access on a WebSphere cluster after LDAP reconfiguration**

When LDAP is reconfigured after the IBM Security Identity Manager installation, you must run the **SAConfig** utility again.

**Procedure**

1. On the WebSphere deployment manager, change to the bin directory in IBM Security Identity Manager installation location and run the utility.
   
   For example:

   Table 12. Running SAConfig

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>In C:\Program Files\IBM\isim\bin, either click SAConfig or open a command window and enter <strong>SAConfig</strong>.</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>In /opt/IBM/isim/bin, enter <strong>./SAConfig</strong>.</td>
</tr>
</tbody>
</table>

2. Restart the WebSphere Application Server cluster.

**Fixing problems when the database is reconfigured after installation**

If the IBM Security Identity Manager database is reconfigured after the IBM Security Identity Manager installation, you must run the **SAConfig** utility.

When the database is reconfigured again after the completion of the IBM Security Identity Manager installation, all the default data for the shared access module is lost. This reconfiguration can cause problem with actions that require access to the database.

To fix the problems, run the **SAConfig** utility. This utility repopulates the default data for the shared access module.

The steps differ depending on whether your deployment is on a WebSphere single server or in a WebSphere cluster. Use the instructions for your deployment:

- **Configuring shared access on a WebSphere single server after database reconfiguration**
- **Configuring shared access on a WebSphere cluster after database reconfiguration** on page 93

**Configuring shared access on a WebSphere single server after database reconfiguration**

When the database reconfigured after the IBM Security Identity Manager installation, you must run the **SAConfig** utility again.
Procedure

1. Change to the bin directory in IBM Security Identity Manager installation location and run the utility.
   For example:

   **Table 13. Running SAConfig**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>In C:\Program Files\IBM\isim\bin, either click SAConfig or open a command window and enter <strong>SAConfig</strong>.</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>In /opt/IBM/isim/bin, enter <strong>./SAConfig</strong>.</td>
</tr>
</tbody>
</table>

2. Remove the following files from the ISIM_HOME/data/keystore directory:
   - cvKeystore.jceks
   - pwdEncKeystore.jceks

   where ISIM_HOME is IBM Security Identity Manager installation directory.

3. Remove the cv.encryption.password property from the ISIM_HOME/data/KMIPServer.properties file.

4. Restart WebSphere Application Server.

Configuring shared access on a WebSphere cluster after database reconfiguration

When the database is reconfigured after the IBM Security Identity Manager installation, you must run the **SAConfig** utility again.

Procedure

1. Change to the bin directory in IBM Security Identity Manager installation location and run the utility.

   **Note:** You must run this command on the deployment manager and on each cluster member.
   For example:

   **Table 14. Running SAConfig**

<table>
<thead>
<tr>
<th>Operating system</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows</td>
<td>In C:\Program Files\IBM\isim\bin, either click SAConfig or open a command window and enter <strong>SAConfig</strong>.</td>
</tr>
<tr>
<td>UNIX or Linux</td>
<td>In /opt/IBM/isim/bin, enter <strong>./SAConfig</strong>.</td>
</tr>
</tbody>
</table>

2. Remove the following files from the ISIM_HOME/data/keystore directory:
   - cvKeystore.jceks
   - pwdEncKeystore.jceks

   where ISIM_HOME is IBM Security Identity Manager installation directory.

3. Remove the cv.encryption.password property from the ISIM_HOME/data/KMIPServer.properties file.

4. Update the clipassword property in the ISIM_HOME/data/KMIPServer.properties file:
   You can specify any string value. For example:
   clipassword=test
5. Configure the keystore files for the credential vault server.

**Note:** Complete this step only on the deployment manager. You do not need to complete it on the cluster members.

In the following command, ensure that the value of the `-p` parameter matches the value you specified for clipassword in the `ISIM_HOME/data/KMIPServer.properties` file.

Use the command for your operating system:

- On Microsoft Windows operating systems, enter:
  ```bash
  cd /d "ISIM_HOME\lib"
  From the ISIM_HOME\lib directory, run the following command:
  
  "ISIM_HOME\jre\jre\bin\java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar;
  com.ibm.sec.authz.xacml4j_7.3.1.jar;
  j2ee.jar;
  ojdbc.jar;
  db2jcc.jar;
  db2jcc_license_cu.jar;
  sqljdbc.jar;
  com.ibm.tklm.kmip.jar;
  CVCommon.jar;
  CVCore.jar;
  CVCli.jar;
  com.ibm.tklm.credvault.common.jar;
  commons-cli.jar;
  com.ibm.cv.kmip.ext.jar
  -DKMIPConfigProperties="$USER_INSTALL_DIR$$\data$$KMIPServer.properties"
  -Djava.security.auth.login.config==login.config
  -Djava.security.auth.policy==jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

- On the UNIX or Linux operating systems, enter:
  ```bash
  cd "ISIM_HOME/lib"
  From the ISIM_HOME/lib directory, run the following command:
  
  "ISIM_HOME/jre/jre/bin/java"-cp
  com.ibm.sec.authz.jaccplus_7.3.1.jar;
  com.ibm.sec.authz.xacml4j_7.3.1.jar;
  j2ee.jar;
  ojdbc.jar;
  db2jcc.jar;
  db2jcc_license_cu.jar;
  sqljdbc.jar;
  com.ibm.tklm.kmip.jar;
  CVCommon.jar;
  CVCore.jar;
  CVCli.jar;
  com.ibm.tklm.credvault.common.jar;
  commons-cli.jar;
  com.ibm.cv.kmip.ext.jar
  -DKMIPConfigProperties="$USER_INSTALL_DIR$/data/$KMIPServer.properties"
  -Djava.security.auth.login.config=login.config
  -Djava.security.auth.policy=jaas.policy
  com.ibm.cv.cli.CVShell -u test -p test
  ```

The command generates two credential vault keystore files, `cvKeystore.jceks` and `pwdEncKeystore.jceks`, under the `ISIM_HOME/data/keystore` directory. It updates the credential vault database data entry and the encryption key in `ISIM_HOME/data/KMIPServer.properties`.

6. Copy the generated keystore files and KMIPServer.properties to the `WAS_DM_profile_path/config/cells/cellName/itim` directory.
Note: Complete this step only on the deployment manager. You do not need to complete it on the cluster members.

7. Manually synchronize the nodes from the WebSphere Application Server deployment manager console.

8. On each cluster member, copy the following credential vault files from the WebSphere profile directory hierarchy to the IBM Security Identity Manager data directory hierarchy:

   Table 15. Credential vault server files to copy

<table>
<thead>
<tr>
<th>Copy this file:</th>
<th>To this location:</th>
</tr>
</thead>
<tbody>
<tr>
<td>WAS_PROFILE_PATH/config/cells/cellName/itim/cvKeystore.jceks</td>
<td>ISIM_HOME/data/keystore/cvKeystore.jceks</td>
</tr>
<tr>
<td>WASPROFILE_PATH/config/cells/cellName/itim/pwdEncKeystore.jceks</td>
<td>ISIM_HOME/data/keystore/pwdEncKeystore.jceks</td>
</tr>
<tr>
<td>WAS_PROFILE_PATH/config/cells/cellName/itim/KMIPServer.properties</td>
<td>ISIM_HOME/data/KMIPServer.properties</td>
</tr>
</tbody>
</table>

9. Restart the WebSphere Application Server cluster.
Chapter 13. Troubleshooting email problems

This section describes solutions for email problems.

Cannot send email from IBM Security Identity Manager Server

If you cannot send an email, check the mail server properties. For example, you might not be able to send an email notification of a password change.

The properties are in the enRoleMail.properties file. The following list shows the default directory for the file:

Microsoft Windows systems
C:\Program Files\IBM\isim\data

UNIX or Linux systems
/opt/IBM/isim/data

Take these actions:

- Verify that the mailing protocol and host are correct. SMTP is the most commonly used protocol.
- Check the server log for mail-related messages.
- Check the host server name. Use the nslookup command to list the mail server name and IP address for a specific domain.
  1. Access the command prompt.
  2. Enter the nslookup commands as follows:
     
     nslookup
     > set type=MX
     > domain-name

     where domain-name is the Internet domain name of the email addresses of your organization. For example, us.yourcompany.com.

Cannot send email to external mail addresses

You might not be able to send email to external email addresses.

This problem might be caused by the relay permission on your mail server.

Your mail server must be set up for relaying from the machine that runs the IBM Security Identity Manager Server.

No information provided when email notifications are not delivered

When email notifications are not delivered through the IBM Security Identity Manager Server, there is no information to determine the cause of the problem. The information provided by the user to create and send the email notifications probably contains errors that can cause delivery failures.

Enable tracing and perform a task that generates an email notification. Examine the trace.log file to determine what errors occur.
Note: The trace.log file entries are saved in English only.

Email searches can slow performance when you are provisioning many accounts

When you provision accounts to users without email addresses, you might experience slow performance. For large populations, the LDAP search for system administrators can slow down provisioning. To avoid this issue, ensure that user records have email addresses if you want email notifications. If you do not want email notifications, disable them to avoid the lookup.

The product is configured to send an email for an action, such as the creation of a new account. IBM Security Identity Manager follows this process:

1. Checks if the user has an email address on the person record.
2. Checks the manager of the user if no email address is found.
3. Sends an email to the system administrators, if the manager does not have an email address or the user does not have a manager.

To disable email notifications for a specific activity, such as new account creation, complete these steps:

1. Log in as a system administrator.
2. Expand Configure System in the navigation pane.
4. In the E-mail Notification Templates section, locate the notification you want to disable.
5. In the Status column, hover over the menu and click Disable.
6. Click OK.

The change takes effect immediately.
Chapter 14. Browser problems

This section describes solutions for problems that involve a web server and a web browser.

Mozilla Firefox web browser truncates double-byte characters in text fields

The Mozilla Firefox web browser truncates double-byte text characters in an input field. This problem is a browser limitation related to the font size.

Problem

Text fields that contain double-byte characters appear to vertically truncate the text when viewed at certain font sizes. The text appears to move down in the input field. The characters at the bottom are truncated. This problem does not occur with Microsoft Internet Explorer.

Solution

You can prevent the truncation with one of the following actions:
- Use the Microsoft Internet Explorer web browser.
- Decrease the font size in the Mozilla Firefox web browser. Complete one of the following actions:
  - Simultaneously press the Ctrl key and the - key.
  - Select View > Zoom > Zoom Out from the browser menu bar.

Enabling Microsoft Internet Explorer active scripting

For Microsoft Internet Explorer, ensure that the Active scripting item is enabled in the Scripting section of the web browser. If you disable active scripting, some websites might not function properly, or can cause online security problems.

Complete these steps to enable active scripting:
1. Click Tools > Internet Options on the browser menu bar.
2. Click the Security tab.
3. Click the Internet icon.
4. Click Custom Level.
5. Click the Scripting > Active Scripting list item.
6. Click Enable.

Increasing the web session timeout interval

A web session might timeout before a form customization is complete. For example, a session interval can expire while a form customization task is in progress, but the session does not time out until the task finishes. The default timeout interval is 30 minutes.
About this task

If the web session times out unexpectedly, you can increase the web session timeout interval.

Note: Increasing the web session timeout interval can affect performance if multiple users have active sessions.

Procedure

1. On the WebSphere Application Server Administrative Console, click Enterprise Applications > ITIM > Web modules > app_web.war > Session Management.
2. In the Session timeout field, increment the interval. For example, 60 minutes.

Cannot initiate a session with IBM Security Identity Manager Server

Enable cookies in the browser to establish a session with the IBM Security Identity Manager Server.

Do not start two or more separate browser sessions from the same client computer. Consider the two sessions as one session that yields unpredictable results.

Table columns truncate entries that exceed 50 characters (Mozilla Firefox only)

Mozilla Firefox truncates some table column entries that exceed 50 characters.

This browser limitation can cause a problem when two or more items have the same 50 characters at the beginning. The entry looks identical to the user.

If possible, use naming conventions that ensure uniqueness up to 50 characters. If it is not possible to ensure uniqueness in a 50-character range, use Microsoft Internet Explorer to do certain tasks.

Drop-down lists and pop-up menus do not display (Mozilla Firefox only)

Mozilla Firefox web browser might not display drop-down lists and pop-up menus.

Mozilla Firefox web browser does not display the entire list of tasks because of these reasons:

• If you select the icon next to a user name in a list
• The name is at the bottom of the window

To view a complete list of tasks, use the ↓ key to scroll through the entire list.

Mozilla Firefox does not wrap text in a table column

The text does not fit in a table column and does not wrap in a Mozilla Firefox browser.

Text that does not fit inside a table column does not wrap. For example, an email address might not fit inside the E-Mail Address column. Use the mouse to
highlight the text and drag it toward the edge of the column. This action scrolls
the text in the direction of the mouse movement.

**Window does not resize properly (Mozilla Firefox only)**

The Mozilla Firefox web browser window does not resize properly.

If a window does not fill the web browser space after a resizing operation, resize
the window again. This error can happen the first time that you resize the window.

**Inconsistent tab order between supported web browsers**

For the Mozilla Firefox web browser, the tab order is inconsistent between
supported web browsers.

In windows that display the Password Rules table, for example, if you select
Allow me to type a password in the Confirm Password window, you enable the
other fields. You can then use the Tab key to navigate to the Password and
Confirm Password fields.

In the Mozilla Firefox web browser, however, the cursor moves from the Confirm
Password field to the Password Rule column of the Password Rules table, instead
of moving directly to the Submit button.

Use the mouse rather than the Tab key to select the Submit button.

**Mozilla Firefox browser overwrites the session management behavior**

Some unexpected session management behaviors occur when the Startup mode is
set to Show my windows and tabs from last time in the Mozilla Firefox web
browser.

With this setting, the session is not terminated. The web browser also does not
clear cookies from the previous session, including the LTPA token, even after you
close or reopen the web browser. This setting causes unexpected behavior in IBM
Security Identity Manager because the IBM Security Identity Manager expects the
following behaviors when the web browser is closed:

- The session to be terminated
- The session cookies to be cleared.

Do not use this setting in the Mozilla Firefox web browser because it is not
supported. If required, clear all cookies or use another web browser like Microsoft
Internet Explorer to carry out certain tasks.

**Reports show erroneous characters after a Japanese language pack installation**

You can encounter an IBM Security Identity Manager report problem after you
install Japanese from the language pack.

**Problem:** After you install Japanese from the language pack, viewing a report
shows erroneous characters if you select English at the IBM Security Identity
Manager logon. However, if you select Japanese as the language at the logon, the
report is displayed correctly.
**Workaround:** This problem occurs if you run a Japanese language report and set the locale to English, because the default English font does not support DBCS characters. To view reports generated in a double-byte character set (DBCS) language, specify a font that can display DBCS characters. This workaround applies for locales other than English when DBCS characters are not supported by the respective font.

Complete these steps:
1. Open the `ISIM_HOME/data/enRoleFonts.properties` file.
2. Comment out the `$LOCALE=`font_name line for the English font. For example, if characters in the report are Japanese, and `$LOCALE = en`, comment out `en=sans-serif`.
3. Add a line for the `$LOCALE=DBCS_character_support_font_name`. The following language fonts are supported:
   - Japanese
   - Simplified_Chinese
   - Traditional_Chinese
   - Korean
4. Configure the web browser.
   a. Choose your preferred language from the Language list.
   b. Use **Move Up** to place your language at the top of the list.

   **Note:** Your preferences for that language must always be ordered from most to least specific, top to bottom.
Notices

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

IBM may not offer the products, services, or features contained 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 might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant 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.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

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 might 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.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003
U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

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.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

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 that conform 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. The sample
programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows: © (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. 2004, 2012. All rights reserved.

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

**Trademarks**

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: [http://www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

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

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

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

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

A
access.log 18
accessibility viii
aci filter not working
new account 45
adapter logs
  ADK adapters 18
  IBM Tivoli Directory Integrator
    adapters 18
  adapters troubleshooting 75
    adding credential to vault 89, 90
    administrator group troubleshooting 37
    applets 70
    troubleshooting 70
    authentication troubleshooting 73
    WebSphere Application Server 73
    authorized credential 90

B
backspace key
  deletes characters 39
Browser
  browsers 99
  browsers troubleshooting 99, 100, 101
bus errors
  SystemOut logs 72
  troubleshooting 72

C
Cannot uninstall interim fixes 41
check out page authorized credential 90
  self service 90
cluster environment java.lang exception 41
  Common Base Event (CBE) 22
configuration troubleshooting 37
  custom person entity troubleshooting 69
customization troubleshooting 69

data
  troubleshooting 55
data replication errors 82
database
  troubleshooting 77, 80
database reconfiguration (continued)
    Shared Access Module 93
database server
  logs 24
DB2
  troubleshooting 77, 79, 81
DBPurge 66
deletes characters
  backspace key 39
diagnostic tools 15

E
education viii
email
  troubleshooting 97, 98
errors
  minimizing 9

F
firewall block
  troubleshooting 37
forwarding logging and tracing
  logs
    JLog 34
    WebSphere, forwarding 34

I
IBM
  Software Support viii
  Support Assistant viii
IBM Security Identity Manager 72
  installation 71
  troubleshooting 49
IBM Security Identity Manager Console
  login problems 41
IBM Security Identity Manager Server
  troubleshooting 45, 46, 48, 49, 50
IBM Tivoli Directory Integrator
  logs 23
IBM Tivoli Directory Server
  logs 23
  troubleshooting 85, 86
identity feed fails
  ldap error 46
ignoring exceptions
  WebSphere Application Server 71
illegal format message
tz mappings 40
initial installation
  LDAP port value 39
installation
  IBM Security Identity Manager 71
  troubleshooting 37
  Turkish language setting 71
  installation problems
    messaging engine starting problems 40
installation problems (continued)
  temp directory not deleted 40
  interim fixes
    Cannot uninstall 41
    invalid object names 82

J
text
  java.lang exception
    cluster environment 41
  JLog 15
  java.lang exception
    java.lang exception
    cluster environment 41
  JLog 15

K
knowledge bases 3

L
large search operation results not displayed 48
ldap error
  identity feed fails 46
LDAP instance error
  middleware configuration utility 38
LDAP port value
  initial installation 39
LDAP reconfiguration
  SAConfig 91, 92
  Shared Access Module 91, 92
ldapConfig 12
logging options
  messages 21
  security 21
logging properties 19
  global 19
Logging Toolkit for Java 15
login problems
  IBM Security Identity Manager
    Console 41
logs 15, 35
  audit 29
  database server 24
  IBM Tivoli Directory Integrator 23
  IBM Tivoli Directory Server 23
  installation 15
  message 17
  operational 16
  security 18
  trace 18
  viewing 30
WebSphere Application Server 22
many files open
operating system problems 43
messaging engine starting problems installation problems 40

© Copyright IBM Corp. 2012
middleware configuration utility
LDAP instance error 38
msg.log 17
multiple tasks
user accounts included 45

new account
aci filter not working 45
no error messages
using emulator program 40

online
publications vii
terminology vii
operating system troubleshooting 43
operating system problems many files open 43
Oracle database troubleshooting 80, 81
out-of-memory error reconciliation 47

presentation
troubleshooting 51
prevent DB2 reinstall
services file entries 38
problem determination exchanging information with IBM support 6
problem-determination viii
publications accessing online vii
list of for this product vii

reconciliation
out-of-memory error 47
remotely retrieving data 35
request fails
values not changed 48
results not displayed
large search operation 48
runConfig 24

SAConfig 91, 92, 93
self service 90
services file entries
prevent DB2 reinstall 38
Shared Access Module 91, 92, 93
CV keystore files 92
database reconfiguration 92
SAConfig 92
troubleshooting 89
troubleshooting (continued)
viewing log file data 30
WebSphere Application Server 71
WebSphere Application Server authentication 73
WebSphere Application Server errors 12
WebSphere Application Server logs 22
workflow problems 57
troubleshooting and support contacting IBM support 5
exchange information with IBM support 6
Fix Central getting fixes with 4
fixes getting 4
getting fixes 4
IBM Security Identity Manager overview 1
subscribing to Support updates 7
troubleshooting identifying problems, techniques for 1
troubleshooting techniques 1
troubleshooting and support fixes getting 4
generating fixes 4
tzMappings illegal format message 40

usage
troubleshooting 60
user accounts included
multiple tasks 45
User IDs 37
using emulator program no error messages 40

values not changed
request fails 48

WebSphere Application Server 73
ignoring exceptions 71
logs 22
troubleshooting 71
WebSphere Application Server authentication troubleshooting 73
Windows Terminal Server License
troubleshooting 38
workflow troubleshooting 57