

IBM Security Identity Manager
Version 7.0.0.2

Troubleshooting Topics



IBM Security Identity Manager
Version 7.0.0.2

Troubleshooting Topics



Table of contents

Table list	v
----------------------	---

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	6
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 13

Logs	13
Installation and initial configuration logs	13
IBM Security Identity Manager operational logs	14
Prerequisite product logs	19
Traces	21
Server tracing	21
Applet tracing	25
Identity Service Center tracing	25
Performance and availability	27

Chapter 4. Troubleshooting installation and configuration problems 29

Firewalls can block the IBM Security Identity Manager Server installation	29
User IDs must be in the administrator group to start an installation	29
Middleware configuration utility fails to catalog LDAP database instance node	30
Entries in the services file prevent reinstalling the DB2 Universal Database	30
LDAP port value is already in use for an initial installation of IBM Security Identity Manager	31
Messaging engines do not start after installation	31
The temp directory is not deleted after installation (Microsoft Windows only)	32
Cannot uninstall interim fixes or fix packs	32
Cannot log on to the IBM Security Identity Manager Console	32

Chapter 5. Troubleshooting IBM Security Identity Manager Server problems 33

In SUSE Linux, the design forms applet fails to load, or takes a long time to load	33
A blank page is displayed when a customized person profile user logs in to Identity Service Center	33
Identity Service Center view options are displayed even though it is not installed with the fix pack	33
Date format does not display correctly in the Self-Service User Interface	33
Text search does not consider the language sensitivity in the user interfaces	34
Forgotten password problems in Turkish	34
Identity Service Center search control and sub form limitations	34
ACI filter not working correctly when an account is created	35
User accounts are included when performing a suspend, restore, or delete task	35
Warning messages not displayed during identity feed or reconciliation	35
Changing the service name prevents viewing and performing actions on service requests	36
Identity feed operation fails and returns an LDAP error	36
A request fails because one or more values cannot be changed	37
Concurrent usage of IBM Security Identity Manager Server can affect changes to data	37
All results from a large search operation are not displayed	37
Users are deleted from default groups in identity feeds	38
Restoring the system administrator account	38
Do not change the date and time while users are logged in to IBM Security Identity Manager	39
Presentation problems	39
Data problems	42
Workflow problems	45
Usage problems	48
Customization problems	51
Manager group is not updated when using custom person entity	52
IBM Security Identity Manager applets do not work	52
Limitation in access catalog search when intersection or custom join enabled	53
Ignorable warnings occur for new access types	53

Chapter 6. Troubleshooting database problems 55

Passwords are changed or expired	55
Creation of DB2 schema fails during middleware configuration	55
Database update fails with an SQL error	56

Error occurs during recovery of Oracle database transactions	57
System failure causes data synchronization problem	58
Cannot connect to the database after running the Middleware Configuration program	58
Default multi-threaded DBPURGE operation on IBM DB2 database might not always work in a large environment	59
Error message CTGIMI094E when searching for access in Identity Service Center	60

Chapter 7. Troubleshooting IBM Security Directory Server problems . . . 61

User modifications fail with ObjectClassViolation errors in IBM Security Directory Server	61
Preventing connection problems with multiple LDAP sessions	62
Changing from a Sun ONE Directory Server causes index loss	62

Chapter 8. Troubleshooting email problems. 65

Cannot send email from IBM Security Identity Manager Server	65
Cannot send email to external mail addresses	65
No information provided when email notifications are not delivered	65
Email searches can slow performance when you are provisioning many accounts	66
Email notification template for canceling requests is not applied after installing Fix Pack 6.0.0.3	66

Chapter 9. Troubleshooting browser problems. 69

Subform does not start when the same browser instance is shared by multiple users	69
Page help does not display	69
Identity Service Center login orientation error in Internet Explorer 10.0	69
Administrator Console does not display correctly on Internet Explorer 10.0 in bidirectional mode	70
Mozilla Firefox web browser truncates double-byte characters in text fields	70
Enabling Microsoft Internet Explorer active scripting	71
Update issues in the Administrator Console on Internet Explorer, version 10.0, native mode	71
Cannot initiate a session with IBM Security Identity Manager Server	71
Table columns truncate entries that exceed 50 characters (Mozilla Firefox only)	71
Drop-down lists and pop-up menus do not display (Mozilla Firefox only)	72
Mozilla Firefox does not wrap text in a table column	72
Window does not resize properly (Mozilla Firefox only)	72
Inconsistent tab order between supported web browsers	72

Mozilla Firefox browser overwrites the session management behavior	72
--	----

Chapter 10. Troubleshooting report problems. 75

Orphan accounts are not displayed on the dashboard report	77
Filters on each individual chart do not refresh in the dashboard report	77
Dashboard report fails to show the aggregate values or measures on the chart	77
Provisioning policy membership chart takes a long time to load in the dashboard report	78
Best practices to run the Cognos reports in a large data deployment scenario	78
Web session does not time out when the provisioning policy change preview is in progress	78
Report data synchronization fails intermittently	79

Chapter 11. Troubleshooting virtual appliance problems 81

Clearing the transaction logs.	81
Handling local management interface restart issues	82
Middleware configuration utility might not support your IBM Security Directory Server version.	83
Log messages are not displayed when the virtual appliance is restarted	84
IBM Security Identity Manager Server does not start on the new primary or backup node	84
Service type description is not displayed in the IBM Security Identity Manager Console from the virtual appliance	85
Find bootstrap port information in the IBM Security Identity Manager virtual appliance	86
Unable to access Identity administration console after Identity external user registry configuration.	86
Common issues	87
Limitations	89
Restrict operations for a member node	89
Cluster bootstrap process.	90
Changing host name of the IBM Security Identity Manager virtual appliance	91
Troubleshooting dashboard panel widget display issues on Microsoft Internet Explorer 10	91
Startup problems with the IBM Security Identity Manager virtual appliance Dashboard	92
IBM Security Identity Manager virtual appliance Dashboard displays notifications about snapshots	92
LDAP Server must run when IBM Security Identity Manager virtual appliance servers are restarted after LDAP configuration	93
Bulkload command errors	93

Index 95

Table list

1.	Installation log file names and directories	13	5.	Logging components	22
2.	Default property values	16	6.	Tuning the DB2 statement heap attribute	45
3.	Pattern letters for the formatter.dateFormat and formatter.timeFormat log properties	16	7.	Configuration options from the Configure menu and the Manage menu	89
4.	Sample patterns for timestamps by using the US locale	18			

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 in 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, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Are multiple users or applications encountering the same type of problem?
- Can the problem be re-created 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 IBM Security Identity Manager documentation. However, sometimes you need to look beyond the documentation 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:
 - IBM Security Identity Manager Support website.

- IBM support communities (forums and newsgroups).
- Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the **Search** field at the top of any ibm.com® page.
- Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include “IBM” and the name of the product in your search if you are looking for information about an IBM product.

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 provided by IBM Support for various 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. Download them from Fix Central. This site provides download, installation, and configuration instructions.
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 you download 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. Follow the instructions in the “Installation Instructions” section of the download document.
 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:





1. Subscribe to My Notifications by going to the IBM Support Portal and click **My Notifications** in the **Notifications** portlet.
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](#)
-  [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

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and explain how to resolve the problem. Problem determination is the process of determining why a product does not function as it is designed to function.

The following information is an introduction to the general troubleshooting process. It provides troubleshooting guidelines for the problems that you might experience with IBM Security Identity Manager:

- Resources and techniques for identifying and resolving problems with IBM Security Identity Manager deployments.
- Information about how to resolve errors that are 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

There can be some conditions that can cause errors and unanticipated results.

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 documentation* 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 *Security Identity Manager documentation* 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 documentation:
 - 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 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 documentation* that lists the supported components.
- Review the “Troubleshooting” topics that describe the known problems for these components:
 - Application server, such as the WebSphere® Application Server
 - IBM Security Identity Manager Server
 - Database server

- Directory server and directory integrator, such as the IBM Security Directory Integrator Server
- Adapters
- See the online user assistance for field descriptions, concepts, and task-related questions about user interface.
The documentation provides helpful information about the following tasks:
 - Activity administration
 - Login administration
 - Organization administration
 - Password administration
 - Policy administration
 - Report administration
 - Request administration
 - Role administration
 - Security administration
 - Services administration
 - User administration
 - Workflow management

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 documentation 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.

Database errors

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

Database installation and configuration processing messages are logged in the database log file that is listed in Table 1 on page 13.

For more information, see Installing.

Directory server errors

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

Directory server installation and configuration processing information is logged in the directory server log file that is listed in Table 1 on page 13.

For more information, see Installing.

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 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 Security Identity Manager problems, see Chapter 3, “Diagnostic tools,” on page 13.

Chapter 3. Diagnostic tools

This chapter describes the diagnostic tools that capture and record details about how the program operates. The records help locate the product or component from which an error originates.

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.

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 Security Identity Manager.

Installation and initial configuration logs

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

Table 1 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 Security Identity Manager uninstallation program.
- Installing required middleware products:
 - A directory server, such as IBM Security Directory Server
 - A database, such as DB2 Universal Database™
- Running the middleware configuration utility.
- Installing Security Identity Manager, which also includes:
 - IBM Security Identity Manager Server
 - Security Identity Manager IBM Security Directory Server-based *posix* adapter profiles
 - Database configuration
 - Directory server configuration

Table 1. Installation log file names and directories

File names	Description and location
log.txt	Installation log file for IBM Security Identity Manager.
<ul style="list-style-type: none">• isim_install.stdout• isim_install.stderr	Standard out and error log files for Security Identity Manager.

Table 1. Installation log file names and directories (continued)

File names	Description and location
<ul style="list-style-type: none"> • dbConfig.stdout • ldapConfig.stdout • itim_installer_debug.txt • runConfigFirstTime.stdout • runConfig.stdout • setupEnrole.stdout • StartStopWas.stdout • itim_install_activity.log 	Install log files for Security Identity Manager.
<ul style="list-style-type: none"> • trace.log • msg.log 	<p>The Tivoli® Common Directory is the central location for all serviceability-related files, such as log files and first-failure capture data.</p> <p>Trace or message log files for Security Identity Manager.</p> <p>Location: <i>TIVOLI_COMMON_DIRECTORY\CTGIM\logs\</i></p>
cfg_itim_mw.log	The middleware configuration utility log file.

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 Security Identity Manager operations.
- Logging options. You can set logging options for all Security Identity Manager logs. You can also set options for each type of logging activity.

You can configure different options to manage the quantity and size of the log files. See [Configuring logs](#).

Log format

The message, security, and trace logs are formatted in XML. 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](#).

Application 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. 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*.

You can view the application message log file in the IBM Security Identity Manager virtual appliance to troubleshoot any virtual appliance related issues better. See Managing the log configuration.

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.

To configure the security log, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Manage > Maintenance > Log Retrieval and Configuration**.
3. On the Log Retrieval and Configuration page, select the **Identity** tab.
4. Select **Application access**.
5. Click **Configure**. For more information, see Managing the log configuration.

For information about configuring the size and contents of the security log, see “IBM Security Identity Manager logging properties” on page 16.

Application 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 21.

For information about configuring the size and contents of the trace log, see “Configuring the server trace log” on page 21.

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 Security 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 documentation*.

IBM Security Identity Manager logging properties

Use the **Appliance Dashboard** from the IBM Security Identity Manager virtual appliance console to set logging properties in the *enRoleLogging.properties* file.

Log on to the IBM Security Identity Manager virtual appliance console. From the **Appliance Dashboard**, use the Update Property page to work with the *enRoleLogging.properties*. See Managing the server properties.

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

Property value	Description
<code>logger.refreshInterval=300000</code>	Specifies the number of milliseconds between checking for updates to <i>enRoleLogging.properties</i> . The default value is 5 minutes (300,000 milliseconds).
<code>handler.file.fileDir=</code>	Specifies the location of the log files. Do not change the default path value for the <i>handler.file.fileDir</i> property in the IBM Security Identity Manager virtual appliance.
<code>handler.file.maxFileSize=1024</code>	Specifies the maximum size for each log file in KB.
<code>formatter.dateFormat="yyyy.MM.dd"</code> <code>formatter.timeFormat="HH:mm:ss:SSS"</code>	Specifies the date and time formats for the timestamps in the log records.

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

Symbol	Description	Presentation type*	Example
G (uppercase)	Era designator	Text	AD
y (lowercase)	Year	Number	1996

Table 3. Pattern letters for the `formatter.dateFormat` and `formatter.timeFormat` log properties (continued)

Symbol	Description	Presentation type*	Example
M	Month in the year	Text and number	July and 07
d	Day in the month	Number	10
E	Day of the week	Text	Tuesday
D	Day in the year	Number	189
F	Day of the week in the month	Number	2 (second Wednesday in July)
w	Week in the year	Number	27
W	Week in the month	Number	2
h	Hour in AM or PM	Number (1-12)	12
H	Hour in the day	Number (0-23)	0
m	Minute in the hour	Number	30
s	Second of the minute	Number	55
S	millisecond	Number	987
a	AM or PM marker	Text	PM
k	Hour in the day	Number (1-24)	24
K	Hour in AM or PM	Number (0-11)	0
z	Time zone	Text	Pacific Standard Time
' (single quotation mark)	Escape for text	Delimiter	
" (2 single quotation marks)	Single quotation mark	Literal	
* 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

Sample pattern	Result
formatter.dateFormat="yyyy.MM.dd G" formatter.timeFormat=" 'at' hh:mm:ss z"	1996.07.10 AD at 15:08:56 PDT
formatter.dateFormat="EEE, MMM d, 'yy"	Wed, July 10, '96
formatter.timeFormat="h:mm a"	12:08 PM
formatter.timeFormat="hh 'o''clock' a, zzzz"	12 o'clock PM, Pacific Daylight Time
formatter.timeFormat="K:mm a, z"	0:00 PM, PST
formatter.dateFormat="yyyyy.MMMMM.dd GGG" formatter.timeFormat="hh:mm aaa"	1996.July.10 AD 12:08 PM

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.

Do not change the default path value for the `handler.file.security.fileDir` property in the IBM Security Identity Manager virtual appliance.

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.

Do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. Click the **All properties** tab and select **Identity server property files**.
4. Select the `enRoleLogging.properties` file.
5. Select `formatter.PDXML.className`.
6. Click **Edit**.
7. Change the property value.

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

Change this value	<code>com.ibm.itim.logging.LogXMLFormatter</code>
To this value	<code>com.ibm.log.CBE101Formatter</code>

For more information, see [Managing the server properties](#).

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.

IBM Security Directory Server logs

These logs provide information about the installation and communications between the IBM Security Identity Manager Server and the IBM Security Directory Server.

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

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

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

Microsoft Windows systems

ITDS_HOME\var

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

UNIX and Linux systems

ITDS_HOME/var

For example: /opt/ibm/ldap/V6.3

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

Microsoft Windows systems

ITDS_instance_HOME\logs

For example: C:\idsslapd-ldapdb2\logs

UNIX and Linux systems

ITDS_instance_HOME/logs

For example: /home/ldapdb2/idsslapd-ldapdb2/logs

IBM Security Directory Integrator log

The *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.

IBM Security Directory Integrator logs are available in the support file. Do these steps:

1. From the top-level menu of the **Appliance Dashboard**, click **Manage > System Settings > Support Files**. The Support Files page is displayed.
2. On the Support Files page, work with the support files. For more information, see *Managing the support files*.

You can specify logging properties for IBM Security Directory Integrator.

For more information about the agentless adapters and about setting logging properties, see the *Installation and Configuration Guides on the IBM Security Identity Manager documentation*.

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

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.

Log on to the IBM Security Identity Manager virtual appliance console. From the **Appliance Dashboard**, use the Update Property page to work with the `enRoleLogging.properties`. See *Managing the server properties*.

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_MIN

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_MIN`.

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 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

From the **Appliance Dashboard**, use the Update Property page to work with the `enRoleLogging.properties`. See *Managing the server properties*.

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 shows logging components and descriptions.

Table 5. Logging components

Component	To troubleshoot problems related to:
<code>logger.trace.com.ibm.itim.adhocreport.level</code>	Running operations under the Report tab. For example, synchronizing data or designing and running reports.
<code>logger.trace.com.ibm.itim.adhocreport.changelog.level</code>	Synchronizing data incrementally.
<code>logger.trace.com.ibm.itim.apps.level</code>	Validating business logic. For example, password synchronization and account compliance about provisioning policy.
<code>logger.trace.com.ibm.itim.apps.ejb.adhocreport.level</code>	Synchronizing data. For example, retrieving data from Security Identity Manager LDAP and storing it in a database.
<code>logger.trace.com.ibm.itim.authentication.level</code>	Logging on to or authenticating with Security Identity Manager.

Table 5. Logging components (continued)

Component	To troubleshoot problems related to:
logger.trace.com.ibm.itim.authorization.level	Validating and checking of ACIs for a logged-in user.
logger.trace.com.ibm.itim.common.level	Validating input per defined FORM constraints or schema.
logger.com.ibm.itim.script.level	Evaluating the scriptframework, which replaces FESI. For example, the workflow engine script node and service selection policy script.
logger.trace.com.ibm.itim.fesiextensions.level	Evaluating a FESI script. For example, the workflow engine script node and service selection policy script.
logger.trace.com.ibm.itim.mail.level	Sending mail from Security Identity Manager. For example, notifications.
logger.trace.com.ibm.itim.messaging.level	Sending messages to queues.
logger.trace.com.ibm.itim.dataservices.model.level	Performing LDAP Directory server operations. For example, updating a person.
logger.trace.com.ibm.itim.passworddelivery.level	Clearing expired password transactions.
logger.trace.com.ibm.itim.policy.level	Running and validating policies. For example, password and provisioning policies.
logger.trace.com.ibm.itim.remoteservices.level	Running operations for remote resources and interpreting the response. For example, HR feed, reconciliation and account operations.
logger.trace.com.ibm.itim.report.level	Not used.
logger.trace.com.ibm.itim.security.level	Not used.
logger.trace.com.ibm.itim.scheduling.level	Running scheduled operations such as those that the user scheduled to run at a later date.
logger.trace.com.ibm.itim.systemConfig.level	Running LDAP\DB upgrade\config utilities.

Table 5. Logging components (continued)

Component	To troubleshoot problems related to:
<code>logger.trace.com.ibm.itim.util.level</code>	Sharing utility classes across various components. For example, acquiring and releasing database connections from the WebSphere Application Server Java Database Connectivity (JDBC) connection pool.
<code>logger.trace.com.ibm.itim.webclient.level</code>	Navigating from one page to another, input validation, or display problems.
<code>logger.trace.com.ibm.itim.workflow.level</code>	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.
<code>logger.trace.com.ibm.dam1.level</code>	Communication between IBM Security Identity Manager Server and remote agent.
<code>logger.trace.com.ibm.erma.level</code>	Communication between IBM Security Identity Manager Server and remote agent by using an FTP protocol like RACF®.

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.itim.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 the Update Property page to work with the `enRoleLogging.properties`. See Managing the server properties.
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**.

Identity Service Center tracing

The Identity Service Center tracing is separate from other IBM Security Identity Manager tracing. All Identity Service Center tracing goes to a separate browser window on the client.

Starting the Identity Service Center tracing

Identity Service Center tracing can be started for individual users, with little or no impact to other users of the Identity Service Center. You can view the Identity Service Center trace data in a separate browser window.

Procedure

Log in to the Identity Service Center by using a modified URL, as shown here:

```
http://[host]:[port]/itim/ui?isimPath=debug&isimTrace=[logger]:[level]<,...>
```

Where:

[host] Is the host name of the IBM Security Identity Manager server.

[port] Is the port number of the IBM Security Identity Manager server application.

[logger]

Is the name of a specific Identity Service Center logger to start, or all to specify the logging level for all other loggers.

[level] Is the logging level to be activated for the [logger]

<...> Indicates you can define multiple [logger]:[level] combinations, to start different levels of logging for different loggers.

The following Identity Service Center logger names are supported:

- com.ibm.security.ui.util.store
- com.ibm.isim.ui.control.nav
- com.ibm.isim.ui.util.api
- com.ibm.isim.ui.util.factory
- all

The following Identity Service Center logging levels are support, in ascending order, which is based on importance or severity:

- all
- trace
- debug
- info
- warn
- error
- fatal
- none

Starting logging at a specific level causes trace records for that level and all higher levels to be collected.

For example, starting logging at the debug level collects trace data for debug, info, warn, error, and fatal trace records. If no level is specified for a logger, all is assumed.

The following URLs are equivalent and start all levels of logging for all loggers:

```
http://[host]:[port]/itim/ui?isimPath=debug&isimTrace=all
```

```
http://[host]:[port]/itim/ui?isimPath=debug&isimTrace=all:all
```

The following URLs are equivalent and start all logging for one logger and warn logging for all other loggers:

```
http://[host]:[port]/itim/ui?isimPath=debug&
isimTrace=com.ibm.isim.ui.util.api:all,all:warn
http://[host]:[port]/itim/ui?isimPath=debug&
all:warn,com.ibm.security.ui.util.store:all
```

Stopping the Identity Service Center tracing

You can stop the Identity Service Center trace process when you are done collecting the information that you need to investigate an issue.

Procedure

Stop the trace process by reloading the Identity Service Center using this URL:

```
http://[host]:[port]/itim/ui?isimPath=dist&isimTrace=all:none.
```

Alternatively, you can log off from Identity Service Center. Then, close all browser windows to clear all the Identity Service Center trace settings.

Viewing the Identity Service Center trace data

The Identity Service Center trace data is viewed in a separate browser window.

Procedure

Start the Identity Service Center tracing for one or more loggers, as described earlier.

As trace data is collected, a new browser window automatically opens to display the trace data.

The new browser window has a control panel where you can search, filter, and navigate the collected trace data.

What to do next

1. Send the trace data to IBM support. Highlight the relevant trace records in the trace browser window and copy or paste the trace records to a separate file.
2. Stop the trace process.
3. Reload the Identity Service Center using the URL to stop tracing, as described earlier, and close the browser window that contains the collected trace data.

Performance and availability

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

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 “Installing” and the “Configuring” sections.
- Review the known problems and solutions in the *IBM Security Identity Manager Knowledge Center*. Some of the topics in the “Installing” and the “Configuring” sections are repeated in this section.

Firewalls can block the IBM Security Identity Manager Server installation

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

A firewall on the computer where IBM Security Identity Manager Server is being 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 install and configure DB2 Universal Database separately. The user ID is not in the administrator group.
- You use an ID containing reserved characters.

Install 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

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'.
GLPCTL006I Removed database instance: 'itimldap'.
GLPICR033E Failed to add database instance 'itimldap' to directory server
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

`%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 Security 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 Security Identity Manager, specify a different port value for IBM Security Directory Server.

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 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
```

To view the message, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Manage > Maintenance > Log Retrieval and Configuration**
3. From the Log Retrieval and Configuration table of the **Appliance** tab, select a log file.
4. Click **View** to display the contents of the selected log file in the **Log file** field of the Log Content window.

For more information, see *Managing the log configuration*.

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

1. From the **Server Control** widget on the **Appliance Dashboard**, select **Identity Manager Server** and click **Stop**.

2. Review the DB2 Universal Database fix pack installation instructions in the DB2 Universal Database product documentation at <http://www-01.ibm.com/support/docview.wss?uid=swg27023554>.
3. Follow the required procedure for your platform in the post-installation instructions.
4. From the **Server Control** widget on the **Appliance Dashboard**, select **Identity Manager Server** and click **Start**.

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.

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.

To fix the problem, complete these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Directory Server Configuration**.
3. On the Directory Server Configuration page, select **IBM Security Identity Manager User Registry**.
4. Click **Reconfigure**.
5. In the Edit directory server configuration details window, edit the configuration variables.
For more information, see [Managing the directory server configuration](#).
6. Click **Save Configuration**.

Chapter 5. Troubleshooting IBM Security Identity Manager Server problems

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

In SUSE Linux, the design forms applet fails to load, or takes a long time to load

When you run the IBM Security Identity Manager on SUSE Linux kernel-smp-2.6.16.6.0-0.85.1, and use the Java plug-in version 1.7.0_55, the design forms applet fails to load. When you use Java plug-in version 1.7.0_51, the design forms applet takes up to 10 minutes to load.

The failure to load or delay is caused by the specific releases of Java plug-in 1.7.0_55 or 1.7.0_51.

To resolve the problem, upgrade or downgrade the Java plug-in release. The problem is not experienced with the higher or lower Java levels. For example, 1.7.0_60 or 1.7.0_45.

A blank page is displayed when a customized person profile user logs in to Identity Service Center

In the Identity Service Center, a person profile that is created by using a customized schema can have either of the following problems.

- User cannot log in to Identity Service Center.
- User can log in to Identity Service Center, but a blank page is displayed.

The cause of the problem is that the Access Control Items (ACIs) are not defined for a customized person profile.

To resolve the problem, write a new ACI that grants appropriate privileges to the customized person profile.

Identity Service Center view options are displayed even though it is not installed with the fix pack

Install the Security Identity Manager fix packs 6.0.0.x without installing the Identity Service Center. The Identity Service Center view options are displayed when an administrator configures a view definition on the server.

It is a known limitation. No action is necessary. If the Identity Service Center is not installed, the Identity Service Center view definitions do not take effect.

Date format does not display correctly in the Self-Service User Interface

Some of the pages display incorrect date formats in the Self-Service User Interface.

In the Self-Service User Interface, some of the pages display the date in the international date format. For example, 2014 05 06 17:01:15. The international date format does not match with the regional date format that corresponds to the locale in which the user interface is started.

It is a known limitation.

Text search does not consider the language sensitivity in the user interfaces

In IBM Security Identity Manager user interfaces, text search does consider the language sensitivity.

In IBM Security Identity Manager user interfaces, text search does not return any results when the search string contains:

- Umlaut characters. For example, the search strings **Müller** and **Mueller** do not return any results.
- Dotted or dotless **İ**. For example, **ıı** or **İİ**.

It is a known limitation.

Forgotten password problems in Turkish

The forgotten password challenge response might not work with the Turkish language because of case sensitivity issues.

Because of the language sensitivity of the Turkish language, the forgotten password challenge response information must be case-sensitive. Turkish users must remember the case that was used for any challenge response information that they entered.

Ensure that the `enrole.properties` file has the following setting.

```
#####  
## Challenge Response Encoding Information  
#####  
# Controls how CR responses are encoded before being stored  
# in the directory.  
# Values are:  
# lower (DEFAULT)  
# upper  
# none (Case-sensitive responses)  
enrole.challengeresponse.responseConvertCase=none
```

Identity Service Center search control and sub form limitations

IBM Security Identity Manager supports various controls to customize the account form and other forms. The Search control, Search match control, and the Sub Form in a customized account form can have certain limitations when you use the Identity Service Center to request an account in a service that contains these controls.

By using the search control or search match control options, you cannot do a compliance check on attributes until the request is submitted. For non-compliance in account forms that are caused by the selections in search control or search match control, the submit request results in an error.

The Identity Service Center does not display any attributes if you configure them to use sub forms in the Form designer. Therefore, you cannot select any value for the attributes that are configured as a sub form. If the attribute is mandatory, then the submit request results in an error.

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 is 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 13 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 Security Directory Server is the source of user data:

1. Use the IBM Security Directory Server Administration Console.
2. Edit the `ibm-slappedSizeLimit` variable in the `ibmslapd.conf` configuration file.

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

Microsoft Windows systems

`C:\idsslapped-ldapdb2\etc`

UNIX and Linux systems

`/home/ldapdb2/idsslapped-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.

To access the `enRoleLogging.properties` file, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. In the Update Property page, do these steps.
 - a. In the **All properties** tab, click **Identity server property files**.

- b. Select `enRoleLogging.properties` and view the property names and their value in the right pane.

For more information, see *Managing the server properties*.

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:76542121221212,ou=users...` in IBM Security Directory Integrator. Because all IBM Security Directory Integrator-based changes are submitted to IBM Security Identity Manager with System as the requester, 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=765421221212,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.

To access the `ui.properties` file, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. In the Update Property page, do these steps.
 - a. In the **All properties** tab, click **Identity server property files**.
 - b. Select `ui.properties` and view the property names and their value in the right pane.

For more information, see [Managing the server properties](#).

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. 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 Security Directory Server.

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

1. Access the IBM Security Directory Server Administration Console.
2. Navigate to `ou=SystemUser,ou=itim,ou=tim,dc=com`.

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.

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 from the IBM Security Identity Manager virtual appliance console, make sure that no users are logged on.

Presentation problems

This section describes solutions to information presentation problems.

Incorrect displays after running DBConfig

After you run the DBConfig command in either a single-server or a clustered environment, the following problems occur:

- During service creation, the account form labels are displayed incorrectly in the administrative console and Identity Service Center user interfaces. The `ldapAttributes` are displayed instead of the actual account form labels.
- In the administrative console, the service type descriptions do not display in the Configure System > Manage Service Types.

To resolve the problem, reimport the Security Directory Integrator profile JAR files from `ITIM_HOME/config/adapters`.

Search returns no results in Identity Service Center

When a search string is added on the Search User page, no results are returned, even though the list of users was shown before.

Resolution: check permissions. The search operation returns the results only if a user is granted read permissions on all of the default search attributes in the search filter: Full Name, Title, Image Uniform Resource Identifier, and Email address.

Validation error icons do not display in form view when reviewing edited changes in Identity Service Center

Modification details in the form view display only the noncompliant error icons. Validation error icons do not display in the form view for any fields except for the field User ID.

Workaround: Use the table view to review the changes.

This is a known limitation.

Headers in the Identity Service Center do not disappear upon log out from Self-Service user interface

This problem occurs when tasks in the Identity Service Center user interface start in the Self-Service user interface.

After you complete the activity and log out of the Self-Service user interface, though you can see the Identity Service Center login window, the headers do not disappear.

This is a known limitation.

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.

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 recognize 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**.

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 %*##abc".
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 Security 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

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, 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 Security 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, stop and start the IBM Security Identity Manager. If it does not correct the problem, ensure that both IBM Security Identity Manager and the DB2 Universal Database servers are running. To stop and start the IBM Security Identity Manager, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the **Server Control** widget on the **Appliance Dashboard**, do these steps:
 - a. Select **Security Identity Manager server** and click **Stop**.
 - b. Select **Security Identity Manager server** and click **Start**.

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 Security 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:

```
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.

Cannot save workflows

If you cannot save or modify a workflow, you might need to modify your Java security settings. High Java security setting might prevent you from saving changes to workflows.

Symptoms:

- The administration console indicates a successful operation, but the changes are not saved when the workflow designer closes.
- An error message is issued that a Java security setting prevented the workflow from being saved.

Workaround:

If this problem occurs:

1. Install the Java 1.7 plug-in.
2. Change or save your new workflow definition.

This problem is a known limitation.

Activities might be delayed when submitted in a batch through Identity Service Center

The Identity Service Center workflows process requests serially. After you submit a batch request, a particular request might not be displayed because it must wait until another request in the batch is completed. For example, a high priority role request might be delayed by a low priority account or group approval.

This condition is a known limitation.

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 `stmtheap` attribute for the maximum number of service instances. This table provides guidelines:

Table 6. Tuning the DB2 statement heap attribute

Maximum service instances	Statement heap size attribute value
12	4096
17	8192
24	16384

Change the statement heap size with the DB2 **update** command.

1. Set `db2instance` to one of these instances:
 - `db2admin`
 - IBM Security 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 STMHEAP size`

4. Stop and start IBM Security Directory Server.

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 Security 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=org,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 `erglobalid=0000000000000000000000000000000022,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=00000000000000000000000000000000, tenant,root suffix`

Example: The tenant is `ou=org`. The root suffix is `dc=com`. The workflow definitions are in:

`DN:ou=workflow,erglobalid=00000000000000000000000000000000,ou=org,dc=com`

2. 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>=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:

```
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

Search limit exceeded

The `ui.properties` file 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 virtual appliance console.
2. From the **Quick Links** widget on the **Appliance Dashboard**, click **Identity Administration Console**.
3. Log on to the IBM Security Identity Manager Console.
4. Click **Configure System > Design Forms**.
5. Click **Accounts**.
6. Double-click the account you want to modify.
7. Double-click the attribute on which you are searching on. It is identified as `[ListBox]`.
8. Specify the object class.
9. Select the **Show Query UI** check box and click **OK**.
10. Click **Save**.
11. Click **OK**.

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.

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 `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}`.

To update the `reportingLabels.properties` file, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. In the Update Property page, do these steps.
 - a. In the **All properties** tab, click **Identity server property files**.
 - b. Select `reportingLabels.properties`.
 - c. Select `accessControlInformation` in the right pane and click **Edit**.

For more information, see *Managing the server properties*.

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 `UnsupportedOperationException` error

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

The message is:

CTGIM0002E. 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 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.

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.

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 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 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*)))
```

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.

To access the `CustomLabels.properties` file, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. In the Update Property page, do these steps.
 - a. In the **All properties** tab, click **Identity server property files**.
 - b. Select `CustomLabels.properties` to view the property names and its values.

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 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.

```
reversePasswordSynchron.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 a 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 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 Security Identity Manager.

Problem

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

- Set `pass-http-only-cookie-attr=yes` in the WebSEAL configuration file.
- Set the `HttpOnly` attribute to `JSESSIONID` 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 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
```

Limitation in access catalog search when intersection or custom join enabled

Initially, the access catalog search in IBM Security Identity Manager does not support intersection and custom join for group access. There is a limitation in the search when the intersection or custom join is enabled. To make the search work correctly, you must change properties in the `enRole.properties` file.

If you have groups that are defined as access and the join directive is intersection or custom, these groups are not found in an access catalog search. To enable them, use the `com.ibm.itim.accesscatalog.groupIntersectionJoin.enabled` and `com.ibm.itim.accesscatalog.groupCustomJoin.enabled` properties that are defined in the `enRole.properties` file. Set these properties to false.

```
#####  
## Access Catalog Properties  
# com.ibm.itim.accesscatalog.groupIntersectionJoin.enabled -- This will enable  
# support to search group access when requesting access in Service Center in case that  
# Intersection Join director is used for the group attribute. Default = false  
# com.ibm.itim.accesscatalog.groupCustomJoin.enabled -- This will enable support to  
# search group access when requesting access in Service Center in case that  
# Custom Join director is used for the group attribute. Default = false  
#####  
com.ibm.itim.accesscatalog.groupIntersectionJoin.enabled=false  
com.ibm.itim.accesscatalog.groupCustomJoin.enabled=false
```

See “Access catalog properties” in the *Reference Guide* in the IBM Security Identity Manager product documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0.0.2/kc-homepage.htm.

Ignorable warnings occur for new access types

After you specify a new access type, ignorable warnings can occur because an icon file is not found, but is associated with the access type.

There are also cases in which real errors occur for a request for a custom file that does not exist. You must determine which requests for nonexistent files are harmless and which require correction.

A harmless error can occur when you define new access types, but do not explicitly define a URL to an existing icon file name. The result is that a new access is implicitly associated with an icon file name pattern for a file that does not exist. Subsequently, when entitled users request access, ignorable warning messages are written to the log. For example:

```
[3/11/14 9:12:16:788 EDT] 0000022b SystemOut      0 CTGIMW001W  
File not found: /ui/images/access/iconAccessRoleApplicationAccess.gif
```

Chapter 6. Troubleshooting database problems

This section describes solutions for potential database problems.

Passwords are changed or expired

The product installation creates three system users to enable communication between the database and IBM Security 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 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:

```
Filename  Type      Size  Used  Priority
/dev/sda3 partition 522104 315540 -1
```

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:

```
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:

```
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:

```
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:

```
/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 c.

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

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.c.jb.1(jb.java(Compiled Code))
  at com.ibm.db2.jcc.c.jb.a(jb.java(Compiled Code))
  at com.ibm.db2.jcc.c.w.a(w.java(Inlined Compiled Code))
  at com.ibm.db2.jcc.c.dc.c(dc.java(Compiled Code))
  at com.ibm.db2.jcc.a.id.cb(id.java(Inlined Compiled Code))
  at com.ibm.db2.jcc.a.id.d(id.java(Compiled Code))
  at com.ibm.db2.jcc.a.id.Y(id.java(Compiled Code))
  at com.ibm.db2.jcc.a.id.executeUpdate(id.java(Compiled Code))
  at com.ibm.ws.rsadapter.jdbc.WSJdbcPreparedStatement.
    pmiExecuteUpdate(WSJdbcPreparedStatement.java(Compiled Code))
  at com.ibm.ws.rsadapter.jdbc.WSJdbcPreparedStatement.
    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 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.

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 **SYS**.
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 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. 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 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.

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 suggested size.

Log file size (4KB) (LOGFILSIZ) = 10000

Increase the disk space in the logging partition in the home directory of the DB2 instance. For example, `/home/db2admin`.

Default multi-threaded DBPURGE operation on IBM DB2 database might not always work in a large environment

Multi-threaded **DBPurge** operation might fail with deadlock in database systems even though all optimization steps are followed.

Note: This scenario and the workaround apply to IBM Tivoli Identity Manager, version 5.1 and later versions of IBM Security Identity Manager.

The IBM Security Identity Manager **DBPurge** operation, by default, uses four threads for the IBM DB2 database. You can run the **DBPurge** operation with one thread by specifying the `-threads 1` argument in the **DBPurge** command.

If you run the **DBPurge** operation without the `-threads 1` option, the operation might fail with errors similar to the following one:

```
DB2 SQL Error: SQLCODE=-1476, SQLSTATE=40506,SQLERRMC=-911
```

The error indicates that either a database timeout or deadlock occurred.

The issue resulted from a deadlock condition between the multiple threads of the **DBPurge** operation. Tables that have defined foreign key constraint and have no defined index on the foreign key column might cause a deadlock or a lock timeout in the database system.

See the IBM DB2 documentation (<http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.admin.perf.doc/doc/c0004121.html>) for this scenario.

Example:

The **ACTIVITY_LOCK** table has a foreign key constraint that is defined with the **PROCESS_ID** and **ACTIVITY_ID** fields of the **PROCESS** and **ACTIVITY** tables. The **ACTIVITY_LOCK** table does not have an index for a foreign key **ACTIVITY_ID** column.

The **DBPurge** utility refers to the following tables which have no index entries that are defined in foreign key column:

- The **ACTIVITY_LOCK** table does not have an index entry for the foreign key **ACTIVITY_ID** column.
- The **PENDING** and **PENDING_REQUESTS** tables do not have index entries that are defined on the foreign key column. However, this table has the foreign key and primary key that is defined on the same column, **PROCESS_ID**. The database creates the index internally for the **PROCESS_ID** column.
- The **PROCESSDATA** and **RECONCILIATION_INFO** tables have index entries that include the foreign key column. However, the tables do not have index that contains only the foreign key columns. The DB2 documentation specifies that you must create an index that contains only the foreign key columns, to resolve the deadlock issue.

You can resolve this problem by creating the following extra index entries in the IBM Security Identity Manager database:

- `CREATE INDEX ENROLE.ACTIVITY_LOCK_AIDX ON ENROLE.ACTIVITY_LOCK (ACTIVITY_ID ASC) MINPCTUSED 10 ALLOW REVERSE SCANS;`
- `CREATE INDEX ENROLE.PROCESSDATA_PIDX ON ENROLE.PROCESSDATA (PROCESS_ID ASC) MINPCTUSED 10 ALLOW REVERSE SCANS;`

- CREATE INDEX ENROLE.RECONCILIATION_INFO_RIDX ON ENROLE.RECONCILIATION_INFO (RECONID ASC) MINPCTUSED 10 ALLOW REVERSE SCANS;

Creating the additional index entries ensures that **DBPurge** operation completes without a deadlock on a DB2 database when multiple threads of **DBPurge** operation run simultaneously.

Error message CTGIMI094E when searching for access in Identity Service Center

When a regular expression is used in the provisioning policy to grant group entitlement, you must be sure that the Java class to support regular expressions is loaded on the database server correctly.

Be sure to follow the steps to configure the Java class to support regular expressions for your database. See “Regular expressions for access requests” in the *Installation Guide* in the IBM Security Identity Manager product documentation website at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0.0.2/kc-homepage.htm

If the Java class for regular expression support is not configured, you receive an internal server error when you search for access for a user during Request Access in the Identity Service Center. The error message with ID=CTGIMI094E is logged in the message log.

Chapter 7. Troubleshooting IBM Security Directory Server problems

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

User modifications fail with ObjectClassViolation errors in IBM Security 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 Security 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:

```
CTGIM0017E: 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 Security Directory Server `ibmslapd.log` file contains an error similar to the following:

```
GLPRDB069E: Attribute EMPLOYEEENUNBER has a maximum value length of 20.  
Current attribute value is of length 27.
```

The `ibmslapd.log` log file is produced by IBM Security 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 Security 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 Security 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 Security 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
```

index erenabled eq
 index errolename pres,eq
 index eraliases eq,sub
 index erservicename pres,eq,sub
 index erobjectprofilename pres,eq
 index ercustomclass eq
 index eroid eq
 index erisdeleted pres
 index erpolicyitemname pres,eq,sub
 index erlabel eq,sub
 index erkeywords eq,sub
 index erpolicytarget eq,sub
 index erreppolicytarget eq,sub
 index erpolicymembership eq,sub
 index eroverride eq
 index eruserclass eq
 index erprocessname pres,eq
 index eracl pres
 index eruid eq,sub
 index erdraft eq
 index erscope pres
 index ersystemrolecategory eq
 index erversionid eq
 index erglobalid eq
 index eradministrator eq
 index ercategory eq
 index erformname eq
 index erpersonstatus eq
 index eraccessdescription eq
 index eraccessname eq
 index ertype eq
 index erword eq
 index o eq,sub
 index ou eq,sub
 index owner eq
 index l eq,sub
 index manager eq
 index description eq,sub
 index ergroupdescription 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 8. 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.

Take these actions:

- Log on to the IBM Security Identity Manager virtual appliance console.
- From the top-level menu of the **Appliance Dashboard**, select **Configure > Manage Server Setting > Mail Server Configuration**.
- Use the Mail Server Configuration page to check the mail server properties. For more information, see *Managing the mail server configuration*.
- 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 **tools** command.
 3. 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.

To view the trace entries, do these steps:

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. From the top-level menu of the **Appliance Dashboard**, select **Manage > Maintenance > Log Retrieval and Configuration**.
3. On the Log Retrieval and Configuration page, click the **Identity** tab.
4. Select **Application trace**.
5. Click **View**.

For more information, see Managing the log configuration.

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.
3. Select **Workflow Notification Properties**.
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.

Email notification template for canceling requests is not applied after installing Fix Pack 6.0.0.3

IBM Security Identity Manager Fix Pack 6.0.0.3 includes support for entering the reason for canceling a request. With Fix Pack 6.0.0.3, the **Process Completion Template** includes information about who canceled the request, why the request was canceled, and when the request was canceled.

You can use the Workflow Notification Properties page to manually add information about canceling a request to the email notification template. When you install the IBM Security Identity Manager Fix Pack 6.0.0.3, the email notification template content that includes information about canceling a request is not automatically applied. The template changes that are available with Fix Pack 6.0.0.3 are not automatically applied so that the installation process does not overwrite any custom changes that you might have made to the email templates.

1. From the navigation tree, select **Configure System > Workflow Notification Properties**.
2. On the Workflow Notification Properties page, in the **E-mail Notification Templates** table, select **Process Completion Template**. Then, click **Change**.
3. In the Notification Template page, modify the **Plaintext body** field by adding this code to the end of the existing code:

```
<JS> if (process.canceledBy != null) { '<RE key="CanceledBy"/>: ' + process.canceledBy; }</JS>
<JS> if (process.canceledBy != null) { '<RE key="DateCanceled"/>: '; }</JS> <RE key="readOnlyDateFormat"><PARM>
<JS> if (process.canceledDate != null) return process.canceledDate.getTime(); else return '';</JS></PARM></RE>
<JS> if (process.canceledBy != null) { '<RE key="CanceledReason"/>:
<JS> (process.canceledJustification == null)? '': process.canceledJustification;</JS>'; }</JS>
```

4. In the Notification Template page, modify the **XHTML body** field by adding this code inside the table:

```
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledBy"/></td><td width="773" class="text-description" bgcolor="white">
  <JS>process.canceledBy;</JS></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="DateCanceled"/></td><td width="773" class="text-description" bgcolor="white">
  <RE key="readOnlyDateFormat"><PARM>
  <JS>if (process.canceledDate != null) return process.canceledDate.getTime();
  else return '';</JS>
  </PARM></RE></td></tr>
<tr align="left" valign="middle"><td class="text-description" bgcolor="EBEDF3">
  <RE key="CanceledReason"/></td><td width="773" class="text-description" bgcolor="white">
  <JS>process.canceledJustification;</JS></td></tr>
```

Place the new code inside the table between these two sets of existing code:

```
<pre><JS>Enrole.localize(process.resultDetail, "$LOCALE");</JS></pre></td></tr>
```

and

```
</table>
</td>
<!-- End Of Notification body -->
```

5. To save the changes, click **OK**.
6. On the Workflow Notification Properties page, click **OK**. On the Success page, click **Close**.

Related tasks:

Manually applying the email notification template changes for canceling a request in the *Administration Guide*

Chapter 9. Troubleshooting browser problems

The following section describes solutions for problems that involve a web server and a web browser.

Subform does not start when the same browser instance is shared by multiple users

The problem occurs when IBM WebSphere Application Server security integration check is enabled for the Identity Service Center and multiple users open the subform using the same browser instance.

To avoid the problem, close all browser windows after you log out of the Identity Service Center. Start a new browser session when you next log in to the Identity Service Center

Page help does not display

In some browsers, the page helps for the IBM Security Identity Manager administration console might generate a Java 404 error.

The page help file is loaded after the console page load is completed. This loading might take a second or more depending on your computer. If you open the page help before it is loaded, the 404 error is generated. If you click the help icon again after the file is loaded, the help file opens.

Identity Service Center login orientation error in Internet Explorer 10.0

The Identity Service Center login information incorrectly displays on the right side of the panel when it is viewed in Internet Explorer, version 10.0.

Problem

After the IBM Security Identity Manager 6.0 was installed, the developer accessed the Identity Service Center in Microsoft Internet Explorer, version 10. The login orientation was different and the information were incorrectly flushed on the right side of the panel.

Solution

The default setting for Microsoft Internet Explorer, version 10 is **Browser mode: IE10**.

The issue occurs only if the user sets the browser to Microsoft Internet Explorer, version 10 browser to **Compatibility View**.

To fix the issue, start the Identity Service Center in the Internet Explorer browser mode or native mode.

1. To set the native mode, press **F12** to open the Microsoft Internet Explorer developer tools.

If the Microsoft Internet Explorer is in compatibility view, which is the case for this issue, then **Browser Mode: IE 10 Compat view** displays in the developer tools.

2. Select **Browser Mode: IE 10 Compat View**.
3. From the drop-down menu, select **Internet Explorer 10**. Your screen is automatically refreshed.

Administrator Console does not display correctly on Internet Explorer 10.0 in bidirectional mode

Problem

Unable to render IBM Security Identity Manager 6.0 Administrator Console correctly on Microsoft Internet Explorer, version 10, in bidirectional mode.

Solution

To fix the issue, start the IBM Security Identity Manager 6.0 Administrator Console in the Internet Explorer, version 10, browser.

1. To set the browser to **Compatibility View**, go to the toolbar and select **Browser Mode: IE10**.
2. From the drop-down menu, select **Internet Explorer 10 Compatibility View**. Your screen is automatically refreshed.

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**.

Update issues in the Administrator Console on Internet Explorer, version 10.0, native mode

Problem

The following IBM Security Identity Manager 6.0 Administrator Console pages are not updated when you click the **OK**, **Apply**, or **Cancel** buttons in an Internet Explorer, version 10 native mode environment:

- Manage Account Workflows
- Manage Operations

Solution

To fix the issue:

1. Start the IBM Security Identity Manager 6.0 Administrator Console in the Internet Explorer, version 10 browser.
2. Set the browser to **Compatibility View**.

To set the browser to **Compatibility View**, go to the Address bar and check if the **Compatibility View** button is available.

- Click the **Compatibility View** button if it is available.
- If you do not see the **Compatibility View** button in the Address bar, then you do not have to turn it on.

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 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.

Chapter 10. Troubleshooting report problems

The following section describes solutions for the IBM Security Identity Manager Cognos® report problems.

Problems and their solutions

Viewing a report in Turkish locale shows characters that are not translated as '#'.

The PDF report by default is unable to render some Turkish characters. This issue is a known limitation.

IBM Cognos audit history report does not show the audit of an account that is provisioned on the managed resource

IBM Cognos audit history for an account does not show the audit of the account that is provisioned on the managed resource when "Default Account Request Workflow" is configured with the entitlements that are associated with the provisioning policy.

Solution

To generate the audit history reports for the accounts with the default workflow, clear the **Approval Start Date** and **Approval End Date** check boxes, and then run the report.

IBM Security Identity Manager Cognos report execution fails on Oracle data source

During the report generation on Oracle data source, if you select more than 1000 filter values on the prompt page, the report execution fails.

Solution

1. Open the report in IBM Cognos Report Studio.
2. Open the prompt page and edit the property **Rows Per Page** for all input widgets.
3. Set the value to less than or equal to 1000.

The scope for the default provisioning policy is shown as blank on Oracle database.

When you generate the customized IBM Cognos report that includes provisioning policy scope in it, the scope for the default provisioning policy is shown as blank. This issue is specific to Oracle database.

Solution

If the scope for the default provisioning policy is shown as blank on Oracle database, then, interpret the scope of a provisioning policy as Subtree.

No data is displayed in the IBM Security Identity Manager Cognos audit history report

Account audit is not supported for an account that is added and does not have a defined workflow. To audit the accounts for an audit history report, the default workflow or custom workflow must be attached to the provisioning policy that is created.

Long filter values are not shown completely on the prompt pages

Follow the technote link <http://www.ibm.com/support/docview.wss?uid=swg21341018> to resolve this issue. The information in the technote also applies to IBM Cognos Business Intelligence 10.2.1 version.

Known limitations

IBM Security Identity Manager administrative console reports do not display information about accounts that are requested through the Identity Service Center

Solution

Operations that are performed in the Identity Service Center do not generate audit records. They generate access records in IBM Cognos. Use IBM Cognos audit history report to view them.

User entitlements are not displayed in Legacy Administrator console reports and in BIRT reports

Both the Legacy Administrator console reports and BIRT reports do not show the entitlements granted to an individual when the provisioning policy membership is set to "All Other Users". To resolve the problem, use Cognos-based entitlements granted to an individual report to get the entitlement details.

IBM Cognos entitlements report shows the provisioning policy data that is in the draft state

The IBM Cognos entitlements report shows the entitlements that are granted to an individual. It lists all the users and the items for which they are entitled. The report also shows the provisioning policy information that includes the policies that are saved in the draft state.

Cannot truncate the length of the text in the pie charts

An option or a property that can be set to truncate the length of the text is not available for the pie charts. You cannot truncate the length of the text in the pie charts.

Unable to interpret the date in the separation of duty policy violation report

The date value in the Separation of duty policy violation report shows the numbers only. This value is the time in the seconds since the Epoch date.

Languages that are not supported by the IBM Cognos Business Intelligence Server 10.2.1

IBM Cognos Business Intelligence Server 10.2.1 does not support the following languages:

- ar=Arabic
- iw=Hebrew

It provides partial support for the following language:

- el=Greek

The IBM Cognos Business Intelligence Server 10.2.1 is not fully translated into the Greek language. Only components like Cognos Viewer, Cognos Connection, Cognos Administration, and Cognos Workspace support translation in the Greek language.

Note: The unsupported languages are not in the **Product Language** list, although they are displayed in the **Content Language** list in the Cognos configuration of IBM Cognos Business Intelligence Server.

Duplicate entries of the account add operation are observed when you run the account audit report

Duplicate entries of the account add operation are observed if the provisioning policy is configured with the default workflow and an extra

custom workflow is created in IBM Security Identity Manager Console under **Configure System > Manage Operations**.

Solution

Remove the default workflow that is defined in the provisioning policy. Therefore, only the custom workflow that is defined would be effective, which would be captured in the account audit report.

Custom workflows that are defined in IBM Security Identity Manager are not supported for the following type of actions on an account

Only the default workflows are supported for the following actions on an account.

- Restore
- Suspend

Audit of the custom access type is not supported in the access audit history report Any custom access type that is defined as access for a role, service, or group cannot be audited in the access audit history report.

Orphan accounts are not displayed on the dashboard report

When an initial account status view is displayed for the orphan accounts on the IBM Security Identity Manager Cognos dashboard report, orphan accounts are not found.

Orphan accounts are not displayed during the initial account status view and the following message is displayed. No orphan account found on managed resource.

To resolve the problem, reselect the filters that are displayed in the left pane of the dashboard, and then click OK.

Filters on each individual chart do not refresh in the dashboard report

In the IBM Security Identity Manager Cognos dashboard report, filters that are applied on each individual chart do not refresh based on the global filter value that is provided in the dashboard.

To resolve the problem, refresh the workspace. Click **Refresh Workspace** in the workspace toolbar.

Dashboard report fails to show the aggregate values or measures on the chart

When the IBM Security Identity Manager entities such as business unit, provisioning policy, or service are duplicate, the IBM Security Identity Manager Cognos dashboard report does not display the aggregate values on the chart.

To resolve the problem, ensure that the entity names that are defined in the IBM Security Identity Manager are prefixed to make them unique.

Provisioning policy membership chart takes a long time to load in the dashboard report

In a large deployment scenario, the query takes a long time to render the data on the IBM Security Identity Manager Cognos dashboard report for the provisioning policy membership chart.

To resolve the problem:

- Hide the Provisioning Policy Membership chart.
 1. Right-click the Provisioning Policy Membership chart.
 2. Select **Remove from Workspace**.
- Display the reports.
 1. Click **My preferences**.
 2. Select the **Show hidden entries** check box in the IBM Cognos Connection.
- If the data is not displayed in the provisioning policy membership chart, edit the query that is associated with the chart to provide the required filters. Then, start the dashboard report.

Note: The required chart and its query are available in the report name **Workspace Tab Report** that is hidden under the package **ISIMReportingModel_6.0.0.3** in the IBM Cognos Connection portal.

Best practices to run the Cognos reports in a large data deployment scenario

Follow the best practices when you run IBM Security Identity Manager or IBM Security Privileged Identity Manager Cognos reports in a large data deployment scenario.

Use parameters or filters when you run PDF report

When you run the reports with the default report parameters, all the records rendered. Use the reporting parameters or filters to scope down the records.

Prefer HTML format

IBM Security Identity Manager Cognos reports in the HTML format support pagination. When you run the report in HTML format, it renders one page at a time. Click the page down link on the report to display the next page.

Tune the database

See the *Performance* section at <http://www.ibm.com/support/knowledgecenter/SSRMWJ/welcome>.

Web session does not time out when the provisioning policy change preview is in progress

If the provisioning policy preview is in progress, the web session does not time out.

The provisioning policy change preview automatically refreshes the IBM Security Identity Manager user interface every 10 seconds to update the preview status. It does not acknowledge the default web session idle timeout (10 minutes).

It is a known limitation.

Report data synchronization fails intermittently

When you run the report data synchronization, it might fail with an exception `com.sun.jndi.ldap.Ber$DecodeException`.

One of the causes of the problem might be the absence of database tuning.

To resolve the problem, set the value of the property `accountSynchronizationStrategy` to `new`. Complete the following steps:

1. Open the `ITIM_HOME/data/ReportDataSynchronization.properties` property file.
2. Set the value of the property `accountSynchronizationStrategy=new`.
3. Try the data synchronization operation again.

The new synchronization strategy is also designed to improve the performance of the data synchronization.

Chapter 11. Troubleshooting virtual appliance problems

The following topics describe solutions for problems that involve the virtual appliance.

Clearing the transaction logs

A transactional log is simply a binary file where transactions are written. Transaction logging keeps a sequential record of every operation that occurs to your data. If a database becomes corrupted, you can "roll back" the database to a point before it was corrupted and replay the changes from the transaction log.

About this task

Do not to delete these files as this action might cause application server function failure.

Procedure

1. From the top-level menu of the **Appliance Dashboard**, locate the **Server Control** widget.
2. From the **Server Control** widget, select **Application server**.
3. Click **Stop**.
4. Access the command-line interface (CLI) of the virtual appliance by using either an ssh session or the console.
5. From the command-line interface, log on to the IBM Security Identity Manager virtual appliance. The following message is displayed:

```
Welcome to the IBM Security Identity Manager appliance
Enter "help" for a list of available commands
```

6. Enter the help command at the `isimvasrv` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
firmware           Work with firmware images.
fixpacks           Work with fix packs.
isim                Work with the ISIM settings.
license            Work with licenses.
management         Work with management settings.
snapshots          Work with policy snapshot files.
support            Work with support information files.
tools              Work with network diagnostic tools.
updates            Work with firmware and security updates.
Global commands:
back               Return to the previous command mode.
exit               Log off from the appliance.
help               Display information for using the specified command.
reboot             Reboot the appliance.
shutdown           End system operation and turn off the power.
top                Return to the top level.
```

7. Enter the `isim` command at the `isimvasrv` prompt.
8. Enter the help command at the `isimvasrv:isim` prompt for a list of available commands. The following result is displayed:

```
Current mode commands:
firmware_update    Work with the ISIM Appliance firmware settings.
keystore_password  Work with the middleware keystore.
logs               Work with the ISIM log files.
```

```

service_trace      Work with the ISIM trace settings.
Global commands:
back              Return to the previous command mode.
exit             Log off from the appliance.
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.

```

9. Enter the logs command at the isimvasrv:isim prompt.
10. Enter the help command at the isimvasrv:isim:logs prompt for a list of available commands. The following result is displayed:

```

Current mode commands:
clear_ffdc       Clear all FFDC log files on the system.
clear_tranlog   Clearing transaction logs for application server.
monitor         Monitor log files on the system.
Global commands:
back              Return to the previous command mode.
exit             Log off from the appliance.
help            Display information for using the specified command.
reboot          Reboot the appliance.
shutdown        End system operation and turn off the power.
top             Return to the top level.

```

11. Enter the clear_tranlog command at the isimvasrv:isim:logs prompt.

Results

This command clears transaction logs for the Application server.

Handling local management interface restart issues

Sometimes the **Appliance Dashboard** widgets on the IBM Security Identity Manager virtual appliance continue to show progress endlessly.

About this task

To overcome such situations, run the **lmi restart** CLI command.

Procedure

1. Access the command-line interface (CLI) of the virtual appliance by using either an ssh session or the console.
2. From the command-line interface, log on to the IBM Security Identity Manager virtual appliance. The following message is displayed:

```

Welcome to the IBM Security Identity Manager appliance
Enter "help" for a list of available commands

```

3. Enter the help command at the isimvasrv prompt for a list of available commands. The following result is displayed.

```

Current mode commands:
firmware        Work with firmware images.
fixpacks       Work with fix packs.
isim           Work with the ISIM settings.
license        Work with licenses.
lmi            Work with the local management interface.
management     Work with management settings.
snapshots      Work with policy snapshot files.
support        Work with support information files.
tools          Work with network diagnostic tools.
updates        Work with firmware and security updates.
Global commands:
back           Return to the previous command mode.

```

```

exit          Log off from the appliance.
help         Display information for using the specified command.
reboot       Reboot the appliance.
shutdown     End system operation and turn off the power.
top          Return to the top level.

```

4. Enter the `lmi` command at the `isimvasrv` prompt.
5. Enter the `help` command at the `isimvasrv:lmi` prompt for a list of available commands. The following result is displayed:

```

Current mode commands:
reset_lmi_cert  Reset the server certificate for the local management interface to a self-signed certificate.
restart        Restart the local management interface.
Global commands:
back          Return to the previous command mode.
exit          Log off from the appliance.
help         Display information for using the specified command.
reboot       Reboot the appliance.
shutdown     End system operation and turn off the power.
top          Return to the top level.

```

6. Enter the `restart` command at the `isimvasrv:lmi` prompt. This action restarts the local management interface.
7. Log on to the IBM Security Identity Manager virtual appliance to view the **Appliance Dashboard**.

Results

All the widgets on **Appliance Dashboard** are updated.

Middleware configuration utility might not support your IBM Security Directory Server version

The middleware configuration utility might not recognize or support your version of the IBM Security Directory Server, which generates error messages.

If you continue to use the middleware configuration utility to configure with any missing or unsupported version of the IBM Security Directory Server, you might encounter configuration problems.

The middleware configuration utility does not support the use of IBM Security Identity Manager with any missing or incorrect versions of the IBM Security Directory Server.

Resolving the problem

Do these steps:

For UNIX

When you start the middleware configuration utility, use the following command-line argument:

```
-W ITIMRSP.idsInstalledDir=sds_install_location
```

sds_install_location is the IBM Security Directory Server installation directory.

For Windows

Manually configure the IBM Security Directory Server. See *Configuring IBM Security Directory Server manually*.

Important: When you want to manage the virtual appliance for networking, use only a static IP address to map with a valid host name.

Log messages are not displayed when the virtual appliance is restarted

Log messages are not displayed on the IBM Security Identity Manager virtual appliance console when the virtual appliance is restarted.

Problem

After you deploy the ISO and restart the virtual appliance, log messages are not displayed on the virtual appliance console.

Similarly, after you complete the first steps and when you restart the virtual appliance, log messages are not displayed on the virtual appliance console.

Diagnosing the problem

1. Map the ISO of the virtual appliance to the CD drive of the virtual machine.
2. Connect the CD drive to the virtual machine.
3. Start from the ISO and install the image.
4. After the installation is complete, restart the virtual appliance.

Resolving the problem

Wait until you see a login prompt so you can proceed with the other operations.

IBM Security Identity Manager Server does not start on the new primary or backup node

IBM Security Identity Manager Server does not start on the new primary or backup node, which was made by applying a snapshot of the primary node.

Problem

After you apply the snapshot of the primary node on the backup node, the IBM Security Identity Manager Server on the new primary node does not start.

Symptom

When you log on to the new primary or backup node, the **Server Control** widget displays the status of the IBM Security Identity Manager Server as Stopped.

Diagnosing the problem

1. Set up a primary node and make sure that its activation is completed.
2. Set up another node as a backup of the primary node. The backup node must be in a different subnet than the primary node.
3. After you create the snapshot of the primary node on the backup node, apply the snapshot on the new primary or backup node.
4. Restart the new primary node.
5. Observe that the IBM Security Identity Manager Server is not running on the new primary node.
6. From the **Server Control** widget on the **Appliance Dashboard**, click **Start** to start the Security Identity Manager Server on the new primary node.

The IBM Security Identity Manager Server does not start.

Resolving the problem

Make sure that the backup node is in the same subnet as the primary node. For subnet information, see [Setting up the initial IBM Security Identity Manager virtual appliance](#).

Service type description is not displayed in the IBM Security Identity Manager Console from the virtual appliance

When you unconfigure an Identity record from the virtual appliance, it does not display the Service type description in the IBM Security Identity Manager Console.

Problem

After you unconfigure an Identity record from the **Database Server Configuration** menu on the **Appliance Dashboard** of the virtual appliance, the Service type description is not displayed on the **Configure System > Manage Service Types** page of the IBM Security Identity Manager Console.

Symptom

The Service type description does not display on the **Configure System > Manage Service Types** page of the IBM Security Identity Manager Console.

Diagnosing the problem

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Database Server Configuration** to display the Database Server Configuration page.
2. From the Database Server Configuration table, select a record. For example, **Identity data store**.
3. Click **Unconfigure**.
4. Click **Yes** to confirm.
5. On the **Appliance Dashboard**, go to the **Quick Links** widget and click the **Identity Administration console** link.
6. Log on to the IBM Security Identity Manager Console

The result is that you cannot log on to the administrative console.

Resolving the problem

1. From the top-level menu of the **Appliance Dashboard**, click **Configure > Manage External Entities > Database Server Configuration** to display the Database Server Configuration page.
2. Click **Configure**.
3. In the Database Server Configuration Details window, specify the expected variable values.
4. Click **Save Configuration** to complete this task.
5. On the **Appliance Dashboard**, go to the **Quick Links** widget and click the **Identity Administration console** link.
6. Log on to the IBM Security Identity Manager Console
7. Go to **Configure System > Manage Service Types**.
8. Click **Import**.

9. Select the IBM Security Directory Integrator profile JAR files from the directory where the files are placed.
10. Click **OK**.

The Service type description now displays on the **Configure System > Manage Service Types** page.

Find bootstrap port information in the IBM Security Identity Manager virtual appliance

You must know the bootstrap port value to access IBM Security Identity Manager.

Problem

To access IBM Security Identity Manager, the bootstrap port value is required.

Diagnosing the problem

You must find the bootstrap port value from the IBM Security Identity Manager virtual appliance.

Resolving the problem

Do these steps to identify the bootstrap port value from the IBM Security Identity Manager virtual appliance console.

1. Log on to the IBM Security Identity Manager virtual appliance console to display the **Appliance Dashboard**.
2. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
3. In the Update Property page, click the **All properties** tab.
4. Click **Identity server property files** to display a list of properties.
5. Select `enRole.properties`.
6. Select `enrole.appServer.url` in the property table.

Note: To search a property name, use the search box. Type a name or a character string to help you narrow your search. For more information, see [Managing the server properties](#).

7. View the value in the **Property value** column for the selected property name.
8. See the host name:port value pair to identify the bootstrap value.

Unable to access Identity administration console after Identity external user registry configuration

You might encounter problems when you access the IBM Security Identity Manager Console from the **Quick Links** widget after the Identity external user registry configuration.

Symptom

After the Identity external user registry configuration, you might not be able to access the **Identity administration console** in the IBM Security Identity Manager virtual appliance, and the following error is displayed:

```
"Error 404: javax.servlet.ServletException: java.io.FileNotFoundException: SRVE0190E: File not found  
console/main"
```

Resolving the problem

To open the IBM Security Identity Manager Console properly, you must restart these servers from the **Server Control** widget on the **Appliance Dashboard**:

- **Cluster Manager server**
- **Security Identity Manager server**

Do these steps.

1. On the **Appliance Dashboard**, locate the **Server Control** widget. The **Server name** column displays a list of servers.
2. Select **Cluster Manager server**.
3. Click **Restart**.
4. Select **Security Identity Manager server**.
5. Click **Restart**.

For more information, see Viewing the Server Control widget.

Common issues

You might encounter common issues during the deployment and usage of IBM Security Identity Manager in the IBM Security Identity Manager virtual appliance. For more information, see the following common issues and workaround sections.

Data store configuration fails

Check the configuration of the database system.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the Identity data store configuration, server system out, and server messages.

If your configuration is not successful, try to configure again. In case of any problems, you might want use a previously taken snapshot to restore the virtual appliance to its previous state.

Directory server configuration fails

Check the configuration of the directory server.

On the Log Retrieval and Configuration page, click the **Appliance** tab and check the directory server configuration, server system out, and server messages.

If your configuration is not successful, try to configure again. In case of any problems, you might want use a previously taken snapshot to restore the virtual appliance to its previous state.

Unable to access the IBM Security Identity Manager virtual appliance console

View to make sure that the network configuration link IP, Subnet Mast, DNS, and Gateway are correct.

High disk usage notification on the dashboard

Reduce the setting for the **Maximum size for log file rotation** and **Maximum number of historical log files**.

Reduce the trace level from the command-line interface.

Clean the log files from **Manage > Maintenance > Log Retrieval and Configuration**.

For any other unrecoverable issues

Generate a support file by using the command-line interface or the IBM Security Identity Manager virtual appliance console for the IBM Support Team.

CLI

```
isimva.example.com> support
isimva.example.com:support> create
isimva.example.com:support> download
1: isim_1.0.1.1_20130925-014609_isimva.example.com.zip
2: isim_1.0.1.1_20130925-015645_isimva.example.com.zip
Enter index: 1
Insert a USB drive into the USB port on the appliance.
Enter 'YES' to confirm: YES
```

Console

1. Log on to the IBM Security Identity Manager virtual appliance console.
2. Select **Manage > System Settings > Support Files**.
3. Click **New** to create a new file.
4. Click **download** to save a copy of the support file.

Unable to connect the IBM Security Identity Manager Server even with the correct host name

To resolve this issue, add the certificate to the client.

1. Log on with Administrator privileges on the client computer.
2. Start a web browser and go to the HTTPS URL for the IBM Security Identity Manager Server `https://hostname` where host name is the name of the computer that has the IBM Security Identity Manager virtual appliance Server.
3. In the web browser, export the security certificates to a file.
4. Complete the following instructions:
 - a. On the Microsoft Internet Explorer, click **File > Properties**.
 - b. Click **Certificates**.
 - c. Click the **Certification Path** tab.
 - d. Click the **Details** tab.
 - e. For each certificate marked with a red X in the certificate hierarchy, do the following actions:
 - 1) Click **View Certificate**.
 - 2) Click **Details**.
 - 3) Click **Copy to File**.
 - 4) Follow the instructions in the wizard with the following considerations:
 - When the Export format page is displayed, select the **DER encode binary x.509 (CER) format**.

- Save the certificates on your local computer. For example: `webhost.cer`.
5. Restart the computer.

Limitations

Security Identity Manager limitations can affect how the IBM Security Identity Manager virtual appliance behaves or processes information that is received from Security Identity Manager. In the same way, Security Identity Manager limitations can affect how the IBM Security Identity Manager virtual appliance capabilities work.

IBM Security Identity Manager virtual appliance limitations

- Characters other than English are not supported in the **Comment** fields of the following IBM Security Identity Manager virtual appliance pages:
 - Snapshot
 - Firmware Settings
 - Support Files
- The following file name display issues occur in several languages when a snapshot with a long file name is uploaded in the IBM Security Identity Manager virtual appliance:
 - The text in the **Comment** field is truncated.
 - The file name gets truncated in the **Snapshot** table.

Security Identity Manager limitations

- Data Tier and Reporting components

The Data Tier and Reporting components must be installed separately or must be outside the IBM Security Identity Manager virtual appliance.

 - IBM Cognos reporting components are outside of the IBM Security Identity Manager virtual appliance.
 - Supports DB2, IBM Security Directory Server, and Oracle as the Security Identity Manager data store on the external data tier.
- Three network adapters can be used.
- Custom adapters are supported on external Security Directory Integrator.
- Security Identity Manager mobile is supported.

Restrict operations for a member node

The IBM Security Identity Manager virtual appliance cluster is composed of one primary node and other nodes that are called as member nodes. To configure the virtual appliance, you must work from the primary node.

The configuration options from the **Configure** menu and the **Manage** menu on the **Appliance Dashboard** are listed in Table 7.

*Table 7. Configuration options from the **Configure** menu and the **Manage** menu*

Configure	Manage
Directory Server Configuration	Update History
Database Server Configuration	Licensing
Directory Integrator Configuration	Firmware Settings
Mail Server Configuration	Fix Packs

Table 7. Configuration options from the **Configure** menu and the **Manage** menu (continued)

Configure	Manage
Upload Feed File	Log Retrieval and Configuration
Identity External User Registry Configuration	About
Single Sign-On Configuration	Memory
Custom File Management	CPU
Library and Workflow Extension	Storage
Update Property	Application
Application Server Certificate Management	Date/Time
	Administrator Settings
	Snapshots
	Support Files
	Restart or Shut down

The operations for any of the configuration options from the **Configure** menu are restricted from being done on a member node. All these options are available in read-only mode on a member node. You can work with these options only from a primary node. But you can work with the manage options from the **Manage** menu from both, primary and member node.

If you open any configuration page from the **Configure** menu on the member node to modify any configuration information, a warning message is displayed.

If you ignore the warning message and continue to modify any of the configuration information from the **Configure** menu, a warning message indicates that you cannot complete the operation.

The restriction exists because the IBM Security Identity Manager virtual appliance is a member of a cluster, which does not contain the role of a primary node.

Cluster bootstrap process

Bootstrapping refers to getting a cluster node up and running. When a cluster node recovers from failure, checks are made to keep the node state consistent with the rest of the nodes in the cluster.

When you encounter an unresponsive primary node or member node, take following actions:

- You troubleshoot or fix the errors by using the various methods that are documented in this IBM Knowledge Center.
- Restart the primary node or the member node virtual appliance.
 - Synchronize the member node with the primary node to update the node with any virtual appliance configuration changes in the cluster.
 - This node becomes stand-alone node if this node is removed from the cluster definition.

The following actions are done by the cluster bootstrap process:

- When a primary node recovers from a failure and detects that there are no changes in the cluster, the primary node does not display any notifications.
- When a member node recovers from a failure, and detects that it continues to be part of the original cluster, synchronization might be needed if the virtual appliance configuration changes were made.
- When a primary node or a member node recovers from a failure and cannot connect with any of the previously known cluster members because the virtual appliance password changed or the primary node is down, the current node is made stand-alone node. A reconnect notification is set.

Changing host name of the IBM Security Identity Manager virtual appliance

You can change the host name of the virtual appliance to meet your server requirements. Use the CLI command to change the host name, and then use the IBM Security Identity Manager virtual appliance console to update the server properties.

Procedure

1. From a command line, log in to the virtual appliance with the Administrator credentials. For example:
 - **User name:** admin
 - **Password:** admin
2. Type the following command in a command line to set the new host name for the virtual appliance.


```
isimva> management hostname set
```
3. Enter the value for the new host name.
4. Restart the virtual appliance. See Restarting or shutting down.
5. Log on to the IBM Security Identity Manager virtual appliance console to open the **Appliance Dashboard**.
6. From the top-level menu of the **Appliance Dashboard**, select **Configure > Advanced Configuration > Update Property** to display the Update Property page.
7. In the Update Property page, edit the following property files with the new host name.
 - enrole.appServer.url from enRole.properties
 - enrole.appServer.url from com_ibm_itim_isimm.properties

See ../configuring/tsk/t_managing_prop.dita.

Troubleshooting dashboard panel widget display issues on Microsoft Internet Explorer 10

The **Appliance Dashboard** might not display when you view it in the Microsoft Internet Explorer 10 web browser. The web browser shows browser not supported message for any appliance panel.

About this task

An attempt to view the IBM Security Identity Manager Console or activation wizard in a Microsoft Internet Explorer, version 10 browser shows browser not supported message.

To solve the issue, complete these steps as a workaround:

Procedure

1. Open the Microsoft Internet Explorer 10 web browser.
2. After the activation steps are completed, change the browser setting:
 - a. Click **Tools**.
 - b. Clear the **Compatibility View** option.
 - c. Open **Compatibility View Settings**.
 - d. Clear the **Download updated compatibility lists from Microsoft** option.
3. Access the IBM Security Identity Manager Console.

Startup problems with the IBM Security Identity Manager virtual appliance Dashboard

You might encounter some problems when you start the IBM Security Identity Manager virtual appliance Dashboard.

The possible startup problems are as follows:

- Startup or loading delays for several seconds or minutes.
- A notification prompts for a required restart.
- A component status prompts as started, but is not available.

Symptom

You might experience some delays or other startup problems with the IBM Security Identity Manager virtual appliance Dashboard due to these conditions:

- The virtual appliance dashboard starts for the first time after configuration.
- All the widgets are not loaded.

Resolving the problem

Wait for some time and refresh the widget to check the most recent status of the virtual appliance.

IBM Security Identity Manager virtual appliance Dashboard displays notifications about snapshots

The IBM Security Identity Manager virtual appliance Dashboard displays notifications that a snapshot is being applied.

Symptom

Notifications about snapshots that are being applied are displayed by the IBM Security Identity Manager virtual appliance Dashboard.

Resolving the problem

Snapshots might also change the network settings of the virtual appliance. When you apply a snapshot from the management interface of the virtual appliance, you are directed to a window. The window notifies you to go to the virtual appliance by using the IP or the host name that is specified in the snapshot.

If you log on to the virtual appliance while the snapshot process is in progress, in the **Notifications** widget, you might see a notification such as 'Snapshot is getting applied'. Since the snapshot process takes some time, wait until the process completes. Refresh the **Notifications** widget to retrieve the recent notifications.

LDAP Server must run when IBM Security Identity Manager virtual appliance servers are restarted after LDAP configuration

The LDAP Server must be running when you restart the IBM Security Identity Manager virtual appliance servers after an LDAP configuration.

Symptom

When the IBM Security Identity Manager virtual appliance servers are restarted after an LDAP configuration, the LDAP Server must be in a running state.

Resolving the problem

Some of the post-configuration tasks start running after an LDAP configuration and when you start the IBM Security Identity Manager virtual appliance server. This task requires the LDAP Server to be in running state. Therefore, it is required that the LDAP Server is running.

Bulkload command errors

When running the bulkload command, some errors might occur. The bulkload utility fails if any of the entries in the input LDIF file exist in LDAP.

This error might occur if the suffix you defined exists as an entry in the directory server. It might be necessary to delete all entries in the suffix (but leave the suffix) from LDAP before running the command. You can use the `ldapsearch` commands to check for existence of entries, and the `ldapdelete` command to remove these entries.

Error codes:

GLPCRY007E The directory key stash file is inconsistent with the associated encrypted data.

GLPBLK071E Bulkload is unable to run because of an initialization error.

GLPBLK030E Run DB2CMD.EXE first, and then run bulkload within the "DB2 CMD" command interpreter.

To correct these errors, you must know the encryption seed and salt values of the target instance. The target instance is the directory server instance where you are running the bulkload.

1. To determine the salt value of target instance, run the following command from `TDS_HOME/bin`:

```
ldapsearch -D bind DN -w password -h hostname -p port -s base -b cn=crypto,cn=localhost cn=*
```

where:
bind DN is the distinguished name (DN) of the directory server.

password is the DN password.

hostname is the name of the computer where IBM Security Directory Server is installed.

port is the port number on which IBM Security Directory Server is listening.

2. Replace the value of `ibm-slapdCryptoSync`, `ibm-slapdCryptoSalt` with the values returned by the **ldapsearch** command in the `ldap_output_file` file. This file is generated as output of the **db2ldif** command, for example `old_ldif_data.ldif`.
3. Run the **bulkload** command again.

Note: You can use the **-W OUT_FILE_NAME** option with the **bulkload** command. This option places the output from the command into the specified file. The **bulkload** command runs several instances of a DB2 command to load data. Each one has its own success, error, or warning messages. Without the **-W** option to save the output, it is difficult to check the result.

Index

A

- access catalog search limitation 53
- access.log 15
- aci filter 35
- active scripting 71
- adapters
 - ADK adapter logs 15
 - IBM Tivoli Directory Integrator adapter logs 15
- administration console
 - helptroubleshooting 69
- Administrator Console
 - orientation display error 70
 - update issues 71
- administrator group installation prerequisite 29
- applets
 - not working 52
 - troubleshooting 52

B

- browsers
 - active scripting 71
 - Administrator console update issues 71
 - bidirectional mode issue 70
 - font size limitation 70
 - inconsistent tab order 72
 - Internet Explorer 10 69, 70, 71
 - Internet Explorer 9 71
 - list and menu problems 72
 - orientation display error 69, 70
 - session issues 71
 - session management behavior 73
 - text wrapping issue in tables 72
 - troubleshooting 69
 - truncated entries 71
 - window resizing issue 72
- bulkload command errors 93

C

- cancel request email template 66
- Common Base Event (CBE) 19
- common issues 87
- configuration
 - minimize errors 10
 - troubleshooting 29
- custom person entity 52
- customization issues 51

D

- data
 - invalid object names 42
- database
 - server logs 20
 - troubleshooting 55, 58

DB2

- connectivity issue,
 - post-configuration 58
- DBPurge 59
- password, changed or expired 55
- reinstallation issue, service file entries 30
- schema creation failure 55
- update failure 57

DBPurge

- multi-threaded operation 59

diagnostic tools

 13

E

- email
 - failure to send to external addresses 65
 - failure to send to IBM Security Identity Manager Server 65
 - no delivery failure notification 65
 - search slows down performance 66
 - troubleshooting 65
- errors, minimizing 9

F

- firewall block 29
- forgotten password
 - language considerations 34

G

- global logging properties 16

H

- help file, not displaying 69

I

- IBM Security Identity Manager
 - Cognos reports troubleshooting 75
 - console login problems 32
 - installation and configuration errors 10
 - operation errors 10
 - requirements 10
- IBM Security Identity Manager Server
 - concurrent usage 37
 - date and time change 39
 - system administrator account restoration 38
 - troubleshooting 33, 36
 - users, deleted from default groups 38
 - warning message during identity feed 35
- IBM Support contact details 5

- IBM Tivoli Directory Integrator logs 20

- IBM Tivoli Directory Server
 - connectivity problems 62
 - index loss 62
 - logs 20
 - troubleshooting 61
 - user modification failure 61

- identity feed failure 36
- Identity Service Center
 - security integration check 69
 - starting trace process 26
 - stopping trace process 27
 - tracing 26, 27
 - viewing trace data 27

- installation

- messaging engine problems 31
- minimize errors 10
- temp directory not deleted 32
- troubleshooting 29
- interim fix issues 32

J

- JLog 13

K

- knowledge bases 3
- known issues and workaround
 - browser issues 91
 - dashboard panel widget display issues 91
 - Microsoft Internet Explorer 10 91

L

- language considerations, Turkish 34
- large search operation, result display issue 38

- LDAP

- identity feed failure 36
- initial installation port value 31
- instance error on middleware configuration utility 30
- port value initial installation 31
- ldapConfig utility 12
- limitations
 - IBM Security Identity Manager 89
- logging options
 - messages 18
 - security 18
- logging properties 16
- Logging Toolkit for Java 13
- login problems, IBM Security Identity Manager Console 32
- logs 13
 - database server 20
 - IBM Tivoli Directory Integrator 20
 - IBM Tivoli Directory Server 20
 - installation 13

logs (*continued*)
message 14
operational 14
security 15
trace 15

M

messaging engine start problems 31
middleware configuration utility, LDAP
error 30
msg.log 14

N

new account, aci filter issue 35

O

Oracle database
troubleshooting 58

P

presentation issues 39
problem determination
exchanging information with IBM
support 6
product requirements 10
production, minimize errors 10

R

regular expression for granting group
entitlement 60
request failure
unchangable value 37
requirements 10
resources to minimize errors 10
restrict operations
member node 89
results not displayed, search issue 38
runConfig 21

S

services file entries, DB2 reinstall
issue 30
subforms 69

T

temp directory 32
trace.log 15
traces 21
applet 25
server 21
troubleshooting
applet tracing 25
applets 52
bootstrap port 86
browsers 69, 70, 71, 72, 73
cluster bootstrap process 90
custom person entity 52

troubleshooting (*continued*)
customization 51
data problems 42
DB2 55, 57
deployment and configuration
errors 11
diagnostic tools 13
directory server errors 12
email 65, 66
email notification template
cancel request email template 66
help file does not display 69
IBM Security Identity Manager 52
IBM Security Identity Manager
Cognos reports 75
IBM Security Identity Manager
Server 33, 35, 36, 37, 38, 39
IBM Tivoli Directory Integrator
logs 20
IBM Tivoli Directory Server 61, 62
IBM Tivoli Directory Server logs 20
knowledge bases, searching 3
LDAP Server running 93
logs 14
no log messages 84
operational 12, 14
Oracle database 58
presentation problems 39
problems 12
security logs 15
server tracing 21
service type description 85
trace logs 15
traces 21
usage problems 48
virtual appliance
middleware problems 83
startup problems 92
virtual appliance snapshots 92
workflow problems 45
troubleshooting and support
contact details 5
exchanging information 6
Fix Central 4
IBM Security Identity Manager 1
IBM Support 4
support updates 7
techniques 1
troubleshooting databases
DB2 55, 57, 58
errors 58
Oracle 58
troubleshooting installation
errors 11
logs 13
problems 29
troubleshooting logs
database server 20
displaying in CBE format 19
general 13
global logging properties 16
IBM Tivoli Directory Integrator 20
message 14, 18
security 15
trace logs 15

Turkish language
considerations for forgotten
password 34

U

usage troubleshooting 48
user account issues 35
user accounts, multiple tasks 35
User IDs 29

V

virtual appliance
change host name 91

W

warning
ignorable 53
new access type icon, ignorable 53
workflow troubleshooting 45



Printed in USA