IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.1

Error Message Reference Guide

GC14-7624-02

IBM® Security Access Manager for Enterprise Single Sign-On
Version 8.2.1

Error Message Reference Guide

GC14-7624-02

Note
Before using this information and the product it supports, read the information in "Notices" on page 49.

Edition notice

Note: This edition applies to version 8.2.1 of IBM Security Access Manager for Enterprise Single Sign-On, (product number 5724–V67) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide describes all the informational, warning, and error messages that are associated with IBM® Security Access Manager for Enterprise Single Sign-On.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Access Manager for Enterprise Single Sign-On library."
- Links to "Online publications" on page viii.
- A link to the "IBM Terminology website" on page viii.

IBM Security Access Manager for Enterprise Single Sign-On library

The following documents are available in the IBM Security Access Manager for Enterprise Single Sign-On library:

- *IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide*, CF3T3ML

  IBM Security Access Manager for Enterprise Single Sign-On Quick Start Guide provides a quick start on the main installation and configuration tasks to deploy and use IBM Security Access Manager for Enterprise Single Sign-On.
- *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*, SC23995206

  IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide contains information about planning your deployment and preparing your environment. It provides an overview of the product features and components, the required installation and configuration, and the different deployment scenarios. It also describes how to achieve high availability and disaster recovery. Read this guide before you do any installation or configuration tasks.
- *IBM Security Access Manager for Enterprise Single Sign-On Installation Guide*, GI11930904

  IBM Security Access Manager for Enterprise Single Sign-On Installation Guide provides detailed procedures on installation, upgrade, or uninstallation of IBM Security Access Manager for Enterprise Single Sign-On.

  This guide helps you to install the different product components and their required middleware. It also includes the initial configurations that are required to complete the product deployment. It covers procedures for using virtual appliance, WebSphere® Application Server Base editions, and Network Deployment.
- *IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide*, GC23969204

  IBM Security Access Manager for Enterprise Single Sign-On Configuration Guide provides information about configuring the IMS Server settings, the AccessAgent user interface, and its behavior.
- *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*, SC23995105

This guide is intended for the Administrators. It covers the different Administrator tasks. *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide* provides procedures for creating and assigning policy templates, editing policy values, generating logs and reports, and backing up the IMS Server and its database. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide*, SC23969404

  IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide provides detailed descriptions of the different user, machine, and system policies that Administrators can configure in AccessAdmin. Use this guide along with the IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide*, SC23995304

  This guide is intended for Help desk officers. *IBM Security Access Manager for Enterprise Single Sign-On Help Desk Guide* provides Help desk officers information about managing queries and requests from users usually about their authentication factors. Use this guide together with the IBM Security Access Manager for Enterprise Single Sign-On Policies Definition Guide.

- *IBM Security Access Manager for Enterprise Single Sign-On User Guide*, SC23995005

  This guide is intended for the users. *IBM Security Access Manager for Enterprise Single Sign-On User Guide* provides instructions for using AccessAgent and Web Workplace.

- *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*, GC23969303

  IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide provides information about issues with regards to installation, upgrade, and product usage. This guide covers the known issues and limitations of the product. It helps you determine the symptoms and workaround for the problem. It also provides information about fixes, knowledge bases, and support.

- *IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide*, GC14762402

  IBM Security Access Manager for Enterprise Single Sign-On Error Message Reference Guide describes all the informational, warning, and error messages that are associated with IBM Security Access Manager for Enterprise Single Sign-On.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide*, SC23995605

  IBM Security Access Manager for Enterprise Single Sign-On AccessStudio Guide provides information about creating and using AccessProfiles. This guide provides procedures for creating and editing standard and advanced AccessProfiles for different application types. It also covers information about managing authentication services and application objects, and information about other functions and features of AccessStudio.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide*, SC27444401

  IBM Security Access Manager for Enterprise Single Sign-On AccessProfile Widgets Guide provides information about creating and using widgets.

- *IBM Security Access Manager for Enterprise Single Sign-On Tivoli® Endpoint Manager Integration Guide*, SC27562000

IBM Security Access Manager for Enterprise Single Sign-On Tivoli Endpoint Manager Integration Guide provides information about how to create and deploy Fixlets for AccessAgent installation, upgrade or patch management. It also includes topics about using and customizing the dashboard to view information about AccessAgent deployment on the endpoints.

- *IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide*, SC23995704

  IBM Security Access Manager for Enterprise Single Sign-On Provisioning Integration Guide provides information about the different Java™ and SOAP API for provisioning. It also covers procedures for installing and configuring the Provisioning Agent.

- *IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide*, SC14764601

  IBM Security Access Manager for Enterprise Single Sign-On Web API for Credential Management Guide provides information about installing and configuring the Web API for credential management.

- *IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide*, SC14762601

  IBM Security Access Manager for Enterprise Single Sign-On Serial ID SPI Guide describes how to integrate any device with serial numbers and use it as a second authentication factor with AccessAgent.

- *IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide*, SC27562300

  IBM Security Access Manager for Enterprise Single Sign-On Epic Integration Guide provides information about the IBM Security Access Manager for Enterprise Single Sign-On and Epic integration, including supported workflows, configurations, and deployment.

- *IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide*, SC23995404

  IBM Security Access Manager for Enterprise Single Sign-On Context Management Integration Guide provides information about installing, configuring, and testing the Context Management integrated solution in each client workstation.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide*, SC27562101

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Mobile Guide provides information about the deployment and use of single sign-on on mobile devices.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide*, SC27562201

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Virtual Desktop Infrastructure Guide provides information about setting up single sign-on support on a Virtual Desktop Infrastructure, and the different user workflows for accessing the virtual desktop.

- *IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide*, SC27566801

  IBM Security Access Manager for Enterprise Single Sign-On AccessAgent on Terminal Server and Citrix Server Guide provides information about the required configurations and supported workflows in the Terminal and Citrix Servers.

Online publications

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

IBM Security Access Manager for Enterprise Single Sign-On library
The product documentation site (http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc_8.2.1/kc-homepage.html) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
IBM Publications Center offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

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

For additional information, see "Accessibility features" in the *IBM Security Access Manager for Enterprise Single Sign-On Planning and Deployment Guide*.

Technical training

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

Support information

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

IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Message overview

Messages indicate events that occur during the operation of the system.

Depending on their purpose, messages might be displayed on the screen. By default, all informational, warning, and error messages are written to the message logs.

The logs can be reviewed later to determine what events occurred, to see what corrective actions were taken, and to audit all the actions you complete. For more information about message logs, see the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

Chapter 2. Message format

Messages that are generated by IBM Security Access Manager for Enterprise Single Sign-On contain messages that are based both on standard and non-standard format messages. Standard messages consist of a message identifier (ID) and message text. Non-standard messages do not contain message identifiers.

Standard message format

A message ID consists of 10 alphanumeric characters that uniquely identify the message.

Messages are in the format `CTG`*`ccnnnns`*.

IBM Security Access Manager for Enterprise Single Sign-On messages have the following format:

CTG The three-character IBM product prefix.

cc The two-character component or subsystem identifier for IBM Security Access Manager for Enterprise Single Sign-On.

nnnn A three-digit or four-digit serial that uniquely identifies each message.

s A one-character identifier that describes the message severity.

- **I** Informational. The message requires no user action.
- **E** Error. A user action is required.
- **W** Warning. The message might require a user action.

Component identifiers

The component identifier indicates which component or subsystem produced the message.

AM IMS Server

AN AccessAssistant or WebWorkplace

Message text

The text of the message is recorded in the log file in the system locale. If the message text is not available in the local language, the message text is stored in English in the log file.

```
CTGAM0102E Unable to verify your credentials because ISAM ESSO
server cannot connect to enterprise directory.
Explanation:
This error can occur if there is no connectivity between the
ISAM ESSO Server and the enterprise directory.
```

Non-standard message format

A non-standard formatted message does not contain a message identifier.

Chapter 3. IMS Server messages

The following messages contain information about IMS Server.

CTGAM0001E Update error.

Explanation: This error is displayed with saved searches in AccessAdmin.

CTGAM0002E Value must be within the specified range.

Explanation: This error is displayed when you provide a value beyond an acceptable range of values.

User response: Specify a value that is in the specified range.

CTGAM0003E Datatype is not correct.

Explanation: The datatype of the input value is not correct.

User response: Verify and enter a value using the appropriate datatype.

CTGAM0004E The value must be an integer.

Explanation: This error is displayed when you specify a value other than an integer.

User response: Specify an integer value.

CTGAM0005E The value must be a positive integer.

Explanation: This error is displayed when you enter a value that is not a positive integer.

User response: Enter a positive integer.

CTGAM0006E An error occurs when updating the authentication service.

Explanation: This error is displayed when you attempt to update an authentication service.

User response: See the log file.

CTGAM0007E An error occurs when you add the new authentication service.

Explanation: This error is displayed when you attempt to add an authentication service.

User response: Check whether the new authentication service follows all the required criteria.

CTGAM0008E An authentication service with this ID exists.

Explanation: This error is displayed when you attempt to create an ID. The new ID exists.

User response: Create an authentication service with a new ID.

CTGAM0009E The value cannot contain spaces.

Explanation: This error is displayed when you attempt to create an ID and the new ID name contains a space character.

User response: Remove the space characters in the new ID.

CTGAM0010E Error writing value to disk.

Explanation: This error is displayed when you write a value to the disk.

User response: See the log file.

CTGAM0011E The password entries do not match.

Explanation: This error is displayed when you enter two different passwords.

User response: Enter the same password in both text boxes.

CTGAM0012E An error occurs when updating some configuration keys.

Explanation: See message.

User response: See the log file.

CTGAM0013E Due to a connection error the configuration cannot be verified.

Explanation: This error is displayed when you verify the configuration and the system cannot verify the configuration.

User response: See the network connectivity. Check whether your browser is set to work in offline mode.

CTGAM0014E The configuration group with the specified name already exists.

Explanation: This error is displayed when you specify the configuration group name that exists.

User response: Enter a new configuration group name.

CTGAM0015E The configuration group with the specified name already exists.

Explanation: This error is displayed when you specify the configuration group name that exists.

User response: Enter a new configuration group name.

CTGAM0016E The policy value is not valid.

Explanation: This error is displayed when you specify a policy value that is not valid.

User response: Enter a valid policy value. See the *IBM Security Access Manager for Enterprise Single Sign On Configuration Guide* for more details about the policy.

CTGAM0017E The value is not valid or there was an error updating the value.

Explanation: This error is displayed when you provide a value that is not valid or there was an error while updating the value.

User response: Enter a valid value.

CTGAM0018E A user with this value is already existing.

Explanation: This error is displayed when you specify the same value for an existing user.

User response: Enter a new value for the new user.

CTGAM0019E The date is not valid.

Explanation: This error is displayed when you specify the date in a wrong format.

User response: Enter the date in the accepted standard format.

CTGAM0020E The search from date must be earlier than the search to date.

Explanation: This error is displayed when you provide a **search from** date later than the **search to** date.

User response: Enter a **search from** date earlier than **search to** date.

CTGAM0021E A search with that name already exists.

Explanation: This error is displayed when you specify the same search name as the existing one.

User response: Enter a new name for the search.

CTGAM0022E A policy template with the specified name already exists.

Explanation: This error is displayed when you specify the same name as the existing policy template name.

User response: Enter a new value for the policy template.

CTGAM0023E The name can only contain these characters: alphabets, digits, spaces, underscores(_), and dashes(-).

Explanation: This error is displayed when you specify a special character other than those specified in the error message.

User response: Enter a new name that contains only the permitted characters.

CTGAM0024E The name can only contain these characters: alphabets, digits, spaces, commas, underscore(_), and dashes(-).

Explanation: This error is displayed when you specify a special character other than those specified in the error message.

User response: Enter a new name that contains only the permitted characters.

CTGAM0025E The value cannot be empty.

Explanation: This error is displayed when you do not specify a value.

User response: Enter a value.

CTGAM0026E The specified value is not a valid integer.

Explanation: This error is displayed when you specify a value that is not a valid integer.

User response: Enter a new value that is a valid integer.

CTGAM0027E The specified value is not a valid long integer.

Explanation: This error is displayed when you specify a value that is not a valid long integer.

User response: Enter a new value that is a valid long integer.

CTGAM0028E The specified value is not a valid short integer.

Explanation: This error is displayed when you specify a value that is not a valid short integer.

User response: Enter a new value that is a valid short integer.

CTGAM0029E The specified value is not a valid number.

Explanation: This error is displayed when you specify a value that is not a valid number.

User response: Enter a new value that is a valid number.

CTGAM0030E The specified value is not a valid floating point number.

Explanation: This error is displayed when you specify a value that is not a valid floating point number.

User response: Enter a new value that is a valid floating point number.

CTGAM0031E The specified value is not a valid double floating point number.

Explanation: This error is displayed when you specify a value that is not a valid double floating point number.

User response: Enter a new value that is a valid double floating point number.

CTGAM0032E The specified value (*VALUE_0*) is not valid.

Explanation: This error is displayed when you specify a value that is not a valid.

User response: Enter a new value that is a valid.

CTGAM0033E An error occurred when processing your request.

Explanation: This error is displayed while processing your request. There can be several reasons that cause this error.

User response: See the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

CTGAM0034E No results were found matching your search criteria.

Explanation: This error is displayed when there are no results that match your search criteria.

User response: Enter a new search criteria.

CTGAM0035E The maximum number of results allowed were exceeded. Refine your search criteria.

Explanation: This error is displayed when the number of results exceed the permitted number of results.

User response: Refine your search criteria.

CTGAM0036E There was a problem performing the search. Verify your search attribute configuration and try again.

Explanation: This error is displayed when a problem occurs when performing a search.

User response: Verify your search attribute configuration and try again.

CTGAM0037E No authentication services are selected.

Explanation: This error is displayed when an authentication service is not selected.

User response: Select an authentication service.

CTGAM0038E An Active Directory account is not selected.

CTGAM0039E Unable to add user application binding because the application binding: (*VALUE_0*,*VALUE_1*) belongs to user:

Explanation: This error is displayed when the application cannot add a user application binding.

User response: See the log file.

CTGAM0040E Unable to add user application binding: (*VALUE_0*,*VALUE_1*)

Explanation: This error is displayed when the application cannot add a user application binding.

User response: See the log file.

CTGAM0041E The value *VALUE_0* has already been assigned to the user:

Explanation: This error is displayed when the binding value is already assigned to another user.

User response: Change the binding value and try again.

CTGAM0042E There was an error updating attribute: *VALUE_0* with value: *VALUE_1*, Error message: *VALUE_2*

Explanation: This error is displayed when the binding value is already assigned to another user.

User response: Change the binding value and try again.

CTGAM0043E There is an error when updating attribute, Error message: *VALUE_0*

Explanation: See message.

User response: See the log file.

CTGAM0044E This authorization code has already been used. Generate a new authorization code.

Explanation: This error is displayed when the authorization code provided is already used.

User response: Generate a new authorization code.

CTGAM0046E The software key is locked. Unlock the software key and try again.

Explanation: The software key might get locked because of various reasons.

User response: Unlock the user Wallet from AccessAdmin.

CTGAM0047E The secret question cannot be found.

Explanation: This error is displayed when IMS Server cannot find the secret question.

User response: Check with the system administrator.

CTGAM0033E An error occurred when processing your request.

Explanation: This error is displayed while processing your request. There can be several reasons that cause this error.

User response: See the *IBM Security Access Manager for Enterprise Single Sign-On Troubleshooting and Support Guide*.

CTGAM0049E The OTP token cannot be reset. Enter *VALUE_0* **consecutive OTPs and try again.**

Explanation: This error is displayed when the OTP token cannot be reset.

User response: Try to enter the last *number* of consecutive OTPs.

CTGAM0050E The OTP token cannot be reset. Try again.

Explanation: This is displayed when the OTP token cannot be reset.

User response: Try to enter the OTP token again.

CTGAM0051E The wallet was locked due to the number of incorrect attempts was exceeded.

Explanation: This error is displayed when you exceed the allowed number of failed logon attempts to the Wallet.

User response: Contact your Administrator.

CTGAM0052E The user cannot perform self-service registration and bypass of second factor because of too many failed login attempts.

Explanation: This error is displayed when the logon attempts exceeded the number of permitted attempts.

User response: Try to enter the last *number* of consecutive OTPs.

CTGAM0053E The policy values are not valid. Load this policy again.

Explanation: See message.

User response: Load this policy again.

CTGAM0054E Your search query has exceeded the configured limit. Refine your search criteria.

Explanation: This error is displayed when the search query exceeds the configured limit. This limit is configured by your Administrator.

User response: Refine your search criteria.

CTGAM0055E Attribute look-up configuration is not correct

Explanation: This error is displayed when the attribute look-up configuration is not correct.

User response: See the logs for details. See the IMS Server `SystemOut.log` file for more details.

CTGAM0056E No user is found matching to the criteria.

Explanation: This error is displayed when there is no user matching the criteria.

User response: Enter a new search criteria to find the user who matches the conditions.

CTGAM0057E Configure ActiveCode-enabled authentication services for adding application bindings.

Explanation: This error is displayed when the ActiveCode-enabled authentication services are not configured for adding application bindings.

User response: Configure the ActiveCode-enabled authentication services.

CTGAM0058E There was an error when updating the enterprise directory. The configuration might be wrong.

Explanation: This error is displayed when you attempt to update the enterprise directory by using a wrong configuration.

User response: Correct the configuration before you attempt to update the enterprise directory.

CTGAM0060E There was an error when obtaining NetBIOS domain name. This might be due to incorrect Active Directory configuration in the corporate network. Logins that use a NetBIOS domain name are not supported for this domain.

Explanation: This error is displayed when the Active Directory configuration is wrong.

User response: Update the logins that use NetBIOS domain names.

CTGAM0061E There is an error obtaining a DNS domain name for the domain.

CTGAM0062E There is an error deleting the generated authentication services.

Explanation: This error is displayed when you attempt to delete a generated authentication service.

User response: Stop the authentication service before deleting the generated authentication service.

CTGAM0063E There is an error testing the connector.

CTGAM0064E There is an error saving the configuration keys.

Explanation: This error is displayed when you attempt to save the configuration keys.

User response: See the log files.

CTGAM0065E There is error deleting the current configuration.

Explanation: This error is displayed when you attempt to delete a configuration.

User response: See the log files.

CTGAM0066E There is an error deleting the forest configuration.

Explanation: This error is displayed when you attempt to delete a forest configuration.

User response: See the log files.

CTGAM0071E The enterprise directory ID already exists.

Explanation: This error is displayed when you attempt to create an enterprise directory using the enterprise directory ID that exists.

User response: Use a new enterprise directory ID.

CTGAM0072E The ActiveDirectory server name or domain name is empty.

Explanation: See message.

User response: Specify the ActiveDirectory server name or the domain name.

CTGAM0073E An error occurred when trying to reload the IMS Server. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons.

User response: See the IMS Server logs for details.

CTGAM0074E An error occurred when trying to start the IMS Server. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons.

User response: See the IMS Server logs for details.

CTGAM0075E An error occurred when trying to stop the IMS Server. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons.

User response: See the IMS Server logs for details.

CTGAM0076E There is an error provisioning the user. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons.

User response: Verify the IMS Server logs for details.

CTGAM0077E The user name or password is incorrect.

Explanation: This error is displayed when you enter a wrong user name or password.

User response: Specify the correct user name or password.

CTGAM0078E There is an error configuring the Active Directory. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons when configuring the Active Directory.

User response: See the IMS Server logs for details.

CTGAM0079E There is an error provisioning the initial Administrator. Verify the IMS Server logs for details.

Explanation: This error is displayed because of several reasons when trying to provision the initial Administrator.

User response: See the IMS Server logs for details.

CTGAM0080E The domain cannot be resolved.

Explanation: The domain name cannot be resolved.

User response: Specify the domain name again or verify the IMS Server logs for details.

CTGAM0080E The domain cannot be resolved.

Explanation: The domain name cannot be resolved.

User response: Specify the domain name again or verify the IMS Server logs for details.

CTGAM0082E This user has already been registered. Provide a different user name.

Explanation: This error is displayed when you attempt to register a new user. The user name exists.

User response: Provide a new user name.

CTGAM0085E Unable to verify the user registration status.

Explanation: This error is displayed when the registration status of a user cannot be verified.

User response: Try again or request Administrator to verify the IMS Server logs for details.

CTGAM0086E Unable to initialize IMS connectors.

CTGAM0087E There is a problem while fetching the enterprise directory for verifying user credentials. Try again.

Explanation: This error is displayed when the IMS Server cannot fetch the user credentials.

User response: Try again later.

CTGAM0088E Either the user name and password do not match, or the user does not have sufficient privileges.

Explanation: This error is displayed because of several reasons.

User response: Check for the user privileges or enter the username and password.

CTGAM0089E There was a problem performing the search. Verify your search attribute configuration and try again.

Explanation: This error is displayed when the application cannot perform a search.

User response: Verify your search attribute configuration and try again.

CTGAM0090E No results were found matching your search criteria.

Explanation: This error is displayed when your search does not yield any results.

User response: Specify a different search criteria.

CTGAM0091E The user policy template cannot be applied to all the selected users. Try again.

Explanation: This error is displayed when your search does not yield any results.

User response: Specify a different search criteria.

CTGAM0092E No users are selected. Select users and try again.

Explanation: This error is displayed when you want to perform an operation without selecting any users.

User response: Select users and try again.

CTGAM0093E A user policy template is not selected. Select a template and try again.

Explanation: This error is displayed when you want to perform an operation on a policy template without selecting a policy template.

User response: Select user policy template and try again.

CTGAM0094E No User Policy is selected. Select a User Policy and try again.

Explanation: This error is displayed when you want to perform an operation on a user policy without selecting a user policy.

User response: Select a user policy and try again.

CTGAM0095E Error in applying policies to user(s).

Explanation: This error is displayed when you cannot apply policies to users.

User response: See the IMS Server logs for details.

CTGAM0096E No Machine Policy Template has been selected.

Explanation: This error is displayed when you want to perform an operation without selecting a Machine Policy Template.

User response: Select a Machine Policy Template and try again.

CTGAM0097E There is a problem when fetching the details for the selected machine.

Explanation: This error is displayed because of several reasons.

User response: See the IMS Server logs for details.

CTGAM0098E The template name already exists.

Explanation: This error is displayed when you want to create a template name that already exists.

User response: Specify a new template name.

CTGAM0099E A machine policy template was not selected. Select a machine policy template and try again.

Explanation: This error is displayed when you want to perform an operation on a machine policy template but you did not selected any machine policy template.

User response: Select machine policy template and try again.

CTGAM0095E Error in applying policies to user(s).

Explanation: This error is displayed when you cannot apply policies to users.

User response: See the IMS Server logs for details.

CTGAM0101E No machines were selected. Select machines and try again.

Explanation: This error is displayed when you want to perform an operation on machines, however you have not selected any machines.

User response: Select machines and try again.

CTGAM0102E The machine cannot be deleted. See the IMS Server log for details.

Explanation: This error is displayed when you want to delete a machine.

User response: See the IMS Server logs for details.

CTGAM0103E The machine policy template cannot be created. See the log for more details.

Explanation: This error is displayed when you want to delete a machine policy template.

User response: See the IMS Server logs for details.

CTGAM0104E The machine policy template cannot be updated. See the log for more details.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0105E The machine policy template cannot be deleted. See the log for more details.

Explanation: This error is displayed when you want to delete a machine policy template.

User response: See the log for more details.

CTGAM0106E The log-signing feature is not enabled. See the IMS Configuration Utility.

Explanation: See message.

User response: See the IMS Configuration Utility.

CTGAM0107E The IMS Server configuration file (IMS.xml) does not exist in the specified path.

Explanation: This error is displayed when the *IMS.xml* file is not found in the `<WAS_Profile>/config/tamesso/config` directory.

User response: Check if the *IMS.xml* file exists in the `<WAS_Profile>/config/tamesso/config` directory.

CTGAM0108E The AccessAssistant/WebWorkPlace configuration file (*accessAnywhere.properties*) does not exist in the specified path.

Explanation: This error is displayed when the *accessAnywhere.properties* file is not found in the specified path.

User response: See the <*file*> and specify the correct location for the *accessAnywhere.properties* file or copy the *accessAnywhere.properties* to the correct location.

CTGAM0109E The IMS Server already uses the specified transformation string, and re-encryption is not required.

CTGAM0110E AccessAssistant/WebWorkPlace already uses the specified transformation string, and re-encryption is not required.

CTGAM0111E Incorrect master password.

Explanation: This error is displayed when the master password provided is wrong.

User response: Provide the correct master password.

CTGAM0112E Validation error

Explanation: The information you provided is not valid during validation.

User response: Provide the valid inputs.

CTGAM0113E Unable to create the new enterprise directory: *VALUE_0*

Explanation: This error is displayed when you attempt to create a new enterprise directory.

User response: See the documentation for the enterprise directory by using the reference number displayed.

CTGAM0114E Unable to create a new enterprise directory.

Explanation: This error is displayed when you attempt to create a new enterprise directory.

User response: See the documentation for the enterprise directory and resolve the issue.

CTGAM0118E Unable to update the connector information for: *VALUE_0*: *VALUE_1*

Explanation: This error is displayed when you cannot update the connector information.

User response: See the IMS Server logs for details.

CTGAM0119E Unable to create the authentication services for: *VALUE_0*: *VALUE_1*

Explanation: This error is displayed when you cannot create authentication services..

User response: See the IMS Server logs for details.

CTGAM0120E Unable to update the enterprise directory: *VALUE_0*: *VALUE_1*

Explanation: This error is displayed when you attempt to delete the Active Directory domain.

User response: Contact Administrator.

CTGAM0121E Unable to set the Application Deployment Type: *VALUE_0*

Explanation: This error appears when you cannot set the Application Deployment Type.

User response: Contact Administrator.

CTGAM0122E Unable to obtain a NetBIOS domain for the DNS domain: *VALUE_0*, **Error message:** *VALUE_1*

Explanation: This error is displayed when you cannot obtain the NetBIOS domain for the DNS domain < *domain name*>.

User response: See message.

CTGAM0123E Unable to initialize the AD connector: *VALUE_0*

CTGAM0125E Select an authentication service.

Explanation: This error is displayed to prompt you to select an authentication service.

User response: See message.

CTGAM0126E Enter a user name.

Explanation: This error is displayed when you forget to enter the user name.

User response: Enter the user name.

CTGAM0130E Unable to provision initial administrator:

Explanation: This error is displayed when you cannot provision initial administrator.

User response: See the IMS Server logs for details.

CTGAM0131E The submitted authorization request code is not valid. Verify and submit again.

Explanation: This error is displayed when the authorization request code is not valid.

User response: Verify the authorization request code and submit again.

CTGAM0132E The time period submitted is not a valid value. Verify and submit again.

Explanation: This error is displayed when the time period you submitted is not valid.

User response: Verify the time period and submit again.

CTGAM0133E The operation failed due to bad input parameters. Verify the parameters and try again.

Explanation: This error is displayed when the authorization request code you submitted is not valid.

User response: Verify the authorization request code and submit again.

CTGAM0134E The authorization code cannot be generated because of invalid data entry.

Explanation: This error is displayed when the authorization request code you submitted is not valid.

User response: Verify the authorization request code and submit again.

CTGAM0135E The operation failed because your session has timed out. Try again.

Explanation: This error is displayed when you take more time or your connection time out setting is too low.

User response: Try again or increase the connection time out setting.

CTGAM0136E Enter a valid email address.

Explanation: You submitted an email address that is not valid.

User response: Enter a valid mail address.

CTGAM0137E No unassigned tokens available

Explanation: This error is displayed when all the tokens are assigned and no new tokens are available.

User response: Contact your Administrator.

CTGAM0138E The JDBC provider name already exists

Explanation: The JDBC provider name that you are trying to create already exists.

User response: Create a new JDBC connection with a different name.

CTGAM0139E The data source name already exists

Explanation: The data source name that you are trying to create already exists.

User response: Create a new data source with a different name.

CTGAM0140E The JNDI name already exists

Explanation: The JNDI name that you are trying to create already exists.

User response: Create a new JNDI connection with a different name.

CTGAM0141E The AAS - J2C authentication data alias already exists

Explanation: The AAS - J2C authentication data alias that you are trying to create already exists.

User response: Create a AAS - J2C authentication data alias source with a different name.

CTGAM0142E Unable to access the specified Root CA

Explanation: The AAS - J2C authentication data alias that you are trying to create already exists.

User response: Create a AAS - J2C authentication data alias source with a different name.

CTGAM0143E Values for HTTP and HTTPS port number are required

Explanation: You have not specified the values for the HTTP and HTTPS port numbers.

User response: Specify the values for the HTTP and HTTPS port numbers.

CTGAM0144E Unable to See the specified HTTP and HTTPS port

Explanation: The HTTP and HTTPS port numbers specified cannot be checked.

User response: Verify the values for the HTTP and HTTPS port numbers. Check if these ports are already assigned to a different application.

CTGAM0145E The HTTP and HTTPS port specified already exists

Explanation: The HTTP and HTTPS port numbers specified already exist.

User response: Specify new values for the HTTP and HTTPS port numbers.

CTGAM0146E Invalid port number

Explanation: The specified HTTP and HTTPS port numbers are not valid.

User response: Specify valid values for the HTTP and HTTPS port numbers.

CTGAM0147E Port number for HTTP and HTTPS cannot be the same

Explanation: You cannot specify the same number for the HTTP and HTTPS ports.

User response: Specify different values for the HTTP and HTTPS ports.

CTGAM0148E The port number specified does not exist on WAS

Explanation: You have specified the HTTP and HTTPS port numbers that do not exist on the WebSphere Application Server.

User response: The specified HTTP and HTTPS port numbers do not exist on the WebSphere Application Server.

CTGAM0149E An error occurred when creating WAS data source.

Explanation: This error message is displayed because of several reasons.

User response: See the IMS Server logs for details.

CTGAM0150E An error occurred when creating the database and user.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0151E An error occurred when generating the new database user.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0152E An error occurred when copying configuration files.

Explanation: Some of the reasons include insufficient file permissions and low disk space.

User response: See the IMS Server `SystemOut.log` file for more details.

CTGAM0153E Connection Failed! The connection settings cannot be verified. Try again.

Explanation: See message.

User response: Try again or contact administrator.

CTGAM0154E Database already exists! The specified database already exists. Provide a new database name that does not exist.

Explanation: The database was not created because the name you specified exists.

User response: Provide a new database name.

CTGAM0155E Provide an entry for Database name.

Explanation: The error message is displayed when you have not specified the Database name.

User response: See message.

CTGAM0156E Provide an entry for Database hostname.

Explanation: This message is displayed when there is no value specified for the Database hostname.

User response: Specify the value for the Database hostname.

CTGAM0157E Provide an entry for Database instance.

Explanation: This message is displayed when there is no value specified for the Database instance.

User response: Specify the value for the Database instance.

CTGAM0158E Provide an entry for Database port.

Explanation: This message is displayed when there is no value specified for the Database port.

User response: Specify the value for the Database port.

CTGAM0159E Provide an entry for Administrator password.

Explanation: This message is displayed when there is no value specified for the Administrator password.

User response: Specify the value for the Administrator password.

CTGAM0160E Provide an entry for Administrator user name.

Explanation: This message is displayed when there is no value specified for the Administrator user name.

User response: Specify the value for the Administrator user name.

CTGAM0161E Incorrect Database Collation! The database must use a case-sensitive collation (such as SQL_Latin1_General_CP1_CS_AS).

Explanation: This message is displayed when the Database collation is not correct.

User response: Ensure that the database has correct collation.

CTGAM0162E Insufficient Privilege! The user name does not have the privilege to create the database. Provide a database administrator username and password.

Explanation: This message is displayed when you do not have the sufficient privileges to create the database.

User response: Contact your Administrator and request for the required privilege and create a database.

CTGAM0163E Database name contains an invalid character '.'.

Explanation: The message is displayed when there is no value specified for the Database instance.

User response: Specify the value for the Database instance.

CTGAM0164E Username and password cannot be verified. Log in to the database server failed, provide a valid database host name, administrator user name and password.

Explanation: This message is displayed when the user name and password cannot be verified.

User response: Specify a valid database host name, administrator user name, and password.

CTGAM0165E Database hostname must be the actual hostname and not the IP address of the database.

Explanation: This message is displayed when the IP address of the database is specified instead of the actual hostname value.

User response: Specify the actual host name instead of the IP address of the database.

CTGAM0166E Database port number must be an integer.

Explanation: This message is displayed when the value specified for the Database port number is not an integer.

User response: Specify an integer value for the database port number.

CTGAM0167E IMS Server KeyStore already exists, but some certificates are missing.

Explanation: This message is displayed when configuring the IMS Server. It occurs when the certificates are missing although the IMS Server keystore is available.

User response: Contact your Administrator.

CTGAM0168E An error occurred when accessing the IMS Server KeyStore.

Explanation: This message is displayed when the IMS Server keystore is not accessible.

User response: See the IMS Server `SystemOut.log` file.

CTGAM0169E IMS Server KeyStore setup failed.

Explanation: The message is displayed when the IMS Server cannot set up the keystore.

User response: See the `SystemOut.log` file.

CTGAM0170E Adding ports to WAS failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0171E Failed to set the IMS Server runtime URL

Explanation: This message is displayed when the IMS Server cannot set the runtime URL.

User response: See the IMS Server logs for details.

CTGAM0172E Failed to upload IMS Server Soft CA

Explanation: This message is displayed when the IMS Server Soft Certificate Authority cannot be uploaded.

User response: See the IMS Server logs for details.

CTGAM0176E At least one user DN must be defined

Explanation: This message is displayed when DN values are not specified.

User response: Specify at least one user DN value.

CTGAM0177E Error in uploading system data.

Explanation: This message is displayed when an error occurs while uploading the system data.

User response: See the IMS Server logs for details.

CTGAM0178E System data must be in XML format.

Explanation: This message is displayed when the system data is specified in a non-XML format.

User response: See message.

CTGAM0179E An error occurred during upgrade. Verify the log for details about the error.

Explanation: This message is displayed because of several reasons during an IMS Server upgrade.

User response: See the log file.

CTGAM0200E The previous installation is not valid.

Explanation: This message is displayed when the previous installation is not valid.

User response: Ensure that you are pointing the IMS Server to a valid previous installation folder.

CTGAM0201E An error occurred during configuration. Verify the log for details about the error.

Explanation: This message is displayed when there is an unknown error while configuring the IMS Server.

User response: See the log file.

CTGAM0202E Domain name cannot be empty.

Explanation: This message is displayed when you have not specified the domain name value.

User response: Specify a domain name value.

CTGAM0203E User name cannot be empty.

Explanation: This message is displayed when the user name value is not specified.

User response: Specify a user name.

CTGAM0204E Do not leave the fields blank. Enter a value.

Explanation: This message is displayed when some fields are empty.

User response: Specify a value.

CTGAM0205E There are too many results to display. Provide specific search criteria to narrow down the search results.

Explanation: This message is displayed when the search criteria displays more results than the permitted number of values.

User response: Enter a specific search criteria to narrow down the search.

CTGAM0206E The input file is not valid.

Explanation: This message is displayed when you provide an input file that is not valid.

User response: Provide a valid input file.

CTGAM0207E IMS data source JNDI key is missing in ims.xml.

Explanation: This message is displayed when the IMS data source JNDI key is missing in the `ims.xml` file.

User response: Specify the IMS data source JNDI key in the `ims.xml` file.

CTGAM0208E IMS data source JNDI key does not exist in WAS.

Explanation: This message is displayed when the IMS data source JNDI key does not exist in the WebSphere Application Server.

User response: Ensure that the IMS Server is configured successfully and the IMS data source JNDI key is created.

CTGAM0209E Exporting IMS configuration files failed.

Explanation: This message is displayed when the IMS Server cannot export the IMS Server configuration files. For example, the disk space might not be sufficient.

User response: See the `SystemOut.log` file for the exception details.

CTGAM0210E IMS data source cleanup failed.

Explanation: This message is displayed when the IMS Server cannot clean up the data source.

User response: See the `SystemOut.log` file for more details.

CTGAM0211E Importing IMS configuration files failed.

Explanation: This message is displayed when the IMS Server cannot import the IMS Server configuration files. This might be caused by insufficient disk space or insufficient disk privileges.

User response: See the `SystemOut.log` file for more details.

CTGAM0212E Saving ims.properties failed.

Explanation: This message is displayed when the IMS Server cannot save the `ims.properties` file.

User response: See the IMS Server logs for details.

CTGAM0213E Unable to see the SSL Certificate in the exported keystore

Explanation: This message is displayed when the IMS Server cannot see the SSL Certificate in the exported KeyStore.

User response: See the `SystemOut.log` file for more details.

CTGAM0214E Unable to find the SSL Certificate in the exported keystore

Explanation: This message is displayed when the IMS Server cannot locate the SSL Certificate in the exported KeyStore.

User response: You can export from the original IMS Server and import to the target IMS Server again.

CTGAM0215E Unable to delete existing IMS KeyStore

Explanation: This message is displayed when the IMS Server cannot delete the existing IMS KeyStore.

User response: See the `SystemOut.log` file for more details.

CTGAM0216E Unable to get the IHS keystore scope.

Explanation: This message is displayed when the IMS Server cannot get the IBM HTTP Server keystore scope.

User response: See the `SystemOut.log` file for more details.

CTGAM0217E Failed to export the SSL Certificate

Explanation: This message is displayed when the IMS Server cannot export the SSL Certificate.

User response: See the IMS Server logs for details.

CTGAM0218E Failed to export IMS Certificates

Explanation: This message is displayed when the IMS Server fails to export the IMS Certificates.

User response: See the IMS Server logs for details.

CTGAM0219E Failed to store the keystore in the archive

Explanation: This message is displayed when the IMS Server fails to store the keystore in the archive.

User response: See the IMS Server logs for details.

CTGAM0220E Unable to export the Root CA

Explanation: This message is displayed when the IMS Server cannot export the Root Certificate Authority.

User response: See the IMS Server logs for details.

CTGAM0221E Failed to import the SSL certificate

Explanation: This message is displayed when the IMS Server fails to import the SSL Certificate.

User response: See the IMS Server `SystemOut.log` file.

CTGAM0222E Failed to import IMS Certificates

Explanation: This message is displayed when the IMS Server fails to import the IMS Server certificates.

User response: See the IMS Server `SystemOut.log` file.

CTGAM0223E Failed to import the Root CA

Explanation: This message is displayed when the IMS Server fails to import the Root CA.

User response: See the IMS Server `SystemOut.log` file.

CTGAM0224E Unable to update client keystore or truststore

Explanation: This message is displayed when the IMS Server cannot update the client keystore or truststore.

User response: See the IMS Server logs for details.

CTGAM0226E Failed to initialize the keystore import operations

Explanation: This message is displayed when the IMS Server fails to initialize the keystore import operation.

User response: See the `SystemOut.log` file.

CTGAM0227E Failed creating repository:

Explanation: This message is displayed when the IMS Server fails to create a repository.

User response: See the `SystemOut.log` file for more details.

CTGAM0228E Failed updating repository

Explanation: This message is displayed when the IMS Server fails to update the repository.

User response: See the `SystemOut.log` file for more details.

CTGAM0229E Repository already exists

Explanation: This message is displayed when the IMS Server attempts to create a repository configuration but the repository exists.

User response: Use the IMS Configuration Utility to see the list of configured enterprise directory repositories. If a similar repository exists, delete the repository configuration. You can also see the WebSphere Application Server administrative console if there are additional similar repositories. If there is another repository with similar details, delete the repository configuration.

CTGAM0230E Bind user name or password not valid

Explanation: This message is displayed when the IMS Server attempts to bind user name and password that are not valid.

User response: Specify a valid user name or password for the bind.

CTGAM0231E Unable to resolve host specified

Explanation: This message is displayed when the IMS Server cannot resolve the host specified.

User response: Ensure that the host name resolution is set up through a DNS or a hosts file correctly.

CTGAM0232E Connection refused, host, or port not valid

Explanation: This message is displayed when the IMS Server connection fails either because of a wrong host or port name.

User response: Specify valid host or port information.

CTGAM0233E Base entry already exists in other repository

Explanation: This message is displayed when the IMS Server attempts to create a base entry that exists in another repository.

User response: Check whether the base distinguished name is already used in another configured repository.

CTGAM0234E Attribute name is not supported

Explanation: This message is displayed when an Attribute name not supported by the IMS Server is used.

User response: Specify a supported attribute name.

CTGAM0235E Unknown error, see log for details

Explanation: This message is displayed when the reason for the error is not known.

User response: See the log file to determine more details about the error.

CTGAM0236E The value entered is not a valid LDAP name

Explanation: This message is displayed when the LDAP name entered is not valid.

User response: Specify a valid LDAP name.

CTGAM0237E Unable to connect to host specified

Explanation: This message is displayed when the IMS Server cannot connect to the specified host.

User response: Ensure that the host name resolution is set up correctly. Test the connection between the host. You can also ensure that the firewall is configured correctly and is not blocking any connections.

CTGAM0238E At least one user attribute name must be provided

Explanation: This message is displayed when there are no user attributes are provided.

User response: Specify at least one attribute name.

CTGAM0239E At least one base user distinguished name must be provided

Explanation: This message is displayed when the IMS Server base user distinguished names are not provided.

User response: Specify at least one base user distinguished name.

CTGAM0240E Cannot construct base distinguished name from bind distinguished name, please go to the advanced view to edit

Explanation: This message is displayed when the IMS Server cannot connect to the specified host.

User response: Edit the base distinguished name from advanced view.

CTGAM0241E Cannot write enterprise directory entries to database

Explanation: This message is displayed when the IMS Server cannot write enterprise directory entries into the database.

User response: See the IMS Server logs to see whether the database connection is available.

CTGAM0242E Not a valid domain name

Explanation: This message is displayed when the domain name specified is not valid.

User response: Specify a valid domain name.

CTGAM0243E User exists but verification fail, either password is wrong, password expired, or user is disabled

Explanation: This message is displayed when the user credentials are wrong for an existing user.

User response: Check whether the user is disabled or the password has expired. Check whether you entered the correct password.

CTGAM0244E User does not exists

Explanation: This message is displayed when the specified user does not exist.

User response: Contact your Administrator.

CTGAM0245E Multiple user found

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0246E Code format is not valid

Explanation: See message.

User response: Specify a valid code format.

CTGAM0247E Failed to create a local data source for uploading.

Explanation: See message.

User response: See the `SystemOut.log` file for more details.

CTGAM0248E Error cleanup enterprise directory db entry

Explanation: See message.

User response: Contact your Administrator.

CTGAM0249E Error uploading IMS configuration file.

Explanation: See message.

User response: See the `SystemOut.log` file for more details.

CTGAM0250E Path to client keystore/truststore is invalid.

Explanation: This message is displayed when you provide a wrong path to the keystore or truststore is provided.

User response: Specify a valid path to the client keystore or truststore.

CTGAM0251E Failed to import enterprise directories.

Explanation: This message is displayed when the IMS Server fails to import the enterprise directories.

User response: Contact your Administrator.

CTGAM0252E Failed to export enterprise directories.

Explanation: This message is displayed when the IMS Server cannot export enterprise directories.

User response: See the IMS Server logs for details.

CTGAM0253E Unable to access the specified IHS SSL key.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM0254E Failed to upgrade IMS database.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0255E Unable to backup database information.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0256E Unable to backup keystore information.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0257E Unable to sync nodes. Check if node agents are running.

Explanation: See message.

User response: Verify if the node agents are running.

CTGAM0258E User name cannot contain ".

Explanation: See message.

User response: Remove the quotes (") from the user name.

CTGAM0259E User name cannot start with number.

Explanation: See message.

User response: Specify another username that does not start with a number.

CTGAM0260E The installation directory is not valid.

Explanation: See message.

User response: Specify a valid installation directory.

CTGAM0261E An error occurred while deleting IHS information.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0262E An error occurred while adding IHS information.

Explanation: See message.

User response: Contact your System Administrator.

CTGAM0263E The IMS configuration JAR file provided is not valid or corrupted.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0264E The specified database does not meet all the ISAM ESSO database requirements.

Explanation: See message.

User response: Contact your Administrator.

CTGAM0265E The base distinguished name entry is not valid. Please go to advanced view to fix this.

Explanation: This message is displayed when you specify a wrong base distinguished name entry.

User response: Edit the base distinguished name entry in the advanced view.

CTGAM0266E The database server is not reachable.

Explanation: This message is displayed when the database server is not reachable.

User response: Contact your Administrator.

CTGAM0267E The enterprise directory server is not reachable.

Explanation: This message is displayed when the enterprise directory server is not reachable.

User response: Contact your Administrator.

CTGAM0268E Cannot find IBM HTTP server. Please configure webserver and try again.

Explanation: This message is displayed when the IMS Server cannot detect the IBM HTTP Server.

User response: See message.

CTGAM0269E Connection to 'TIM AD Adapter' refused by the server. Host or port information is not valid.

Explanation: This message is displayed when the IMS Server connection to a TIM AD Adapter fails because the host or port information is not valid.

User response: Specify valid host or port information.

CTGAM0270E Simple authentication to TIM AD Adapter failed. User name or password is wrong.

Explanation: This message is displayed when the simple authentication to TIM AD Adapter fails because of wrong user name or password.

User response: Specify the correct user name and password.

CTGAM0271E Specify the Domain Name and NetBIOS Name.

Explanation: This message is displayed when the Domain name and the NetBIOS Name are not specified.

User response: Provide the Domain name and the NetBIOS Name.

CTGAM0272E Verification failed: User exists but the password is wrong.

CTGAM0273E Verification failed: User exists but account is disabled.

CTGAM0274E Verification failed: User exists but account is locked.

CTGAM0275E Verification failed: User exists but password must be changed on next login.

CTGAM0276E Verification failed: User exists but password expired.

CTGAM5003E Pending SOCI is renewable.

Explanation: See message.

User response: Contact your Administrator.

CTGAM5004E Unexpected fatal error occurred.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5005E Unexpected warning occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5006E Transient failure occured on server.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5007E Not initialized.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5008E Bad configuration occurred.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5009E Mail System error occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5010E The session is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5011E The session is not valid: IP address has changed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5012E The session is not valid: inactivity timeout.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5013E The session is not valid: forced timeout.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5014E Access denied.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5015E The attribute name is not valid.

Explanation: See message.

User response: Specify a valid value for attribute name.

CTGAM5016E Login is not valid: Bad login ID or password.

Explanation: See message.

User response: Specify a valid login ID and password.

CTGAM5017E Login is not valid: IMS certificate is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5018E Login is not valid: Certificate cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5019E Login is not valid: Bad authentication code.

Explanation: See message.

User response: Specify the correct authentication code. Verify the IMS Server logs for details.

CTGAM5020E Login is not valid: Clients IP address is missing.

Explanation: See message.

User response: Specify the correct value for the client IP address. See the IMS Server logs for details.

CTGAM5021E Login is not valid: Bad access code.

Explanation: See message.

User response: Provide the correct access code. See the IMS Server logs for details.

CTGAM5023E Passcode login is incorrect.

Explanation: See message.

User response: Specify the correct passcode login. See the IMS Server logs for details.

CTGAM5024E Certificate is not renewable.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5025E User is revoked.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5026E Incorrect login: account is disabled.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5027E User is disabled.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5028E User is registered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5029E User is not registered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5030E The user role is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5031E Passcode synchronization is not enabled.

Explanation: See message.

User response: Enable passcode synchronization. See the IMS Server logs for details.

CTGAM5032E The SOCI ID is not valid.

Explanation: See message.

User response: Specify a valid SOCI ID. See the IMS Server logs for details.

CTGAM5034E Wrong passcode.

Explanation: See message.

User response: Specify the correct passcode. See the IMS Server logs for details.

CTGAM5035E The SOCI type is not valid.

Explanation: See message.

User response: Specify a valid SOCI type. See the IMS Server logs for details.

CTGAM5036E Duplicate is not allowed by MN policy.

Explanation: See message.

User response: Remove the duplicate value. See the IMS Server logs for details.

CTGAM5040E Application user name is already bound.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5041E SOCI has already been registered: certificate found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5042E SOCI has already been registered: no certificate found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5043E SOCI type has already been registered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5044E Application binding is disabled.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5045E The application binding status is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5046E The session property is not valid.

Explanation: See message.

User response: Specify a valid session property. See the IMS Server logs for details.

CTGAM5047E The session is not valid: unknown error occurred.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5048E Service is not supported.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5049E Bad input parameters.

Explanation: See message.

User response: Specify valid input parameters. See the IMS Server logs for details.

CTGAM5050E Data cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5051E No record is deleted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5056E Contract is not known.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5057E Contract is not specified.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5058E Contract version is not supported.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5059E The user data format is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5060E CSK cannot be interpreted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5061E CSK decryption error occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5062E CSK cannnot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5063E Access is not sufficient.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5064E Certificate cannot be issued successfully.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5065E Biometric shared secret between IMS Server and AccessAgent is not initialized.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5066E No biometric authentication providers is configured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5067E Unexpected error occurred.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5068E Biometric template data is corrupted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5069E Illegal biometric data item.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5070E Biometric authentication name is corrupted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5071E The biometric login is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5072E Missing biometric shared key.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5073E Biometric signature has already been registered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5074E The fingerprint login is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5075E Datastore exception occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5076E Datastore entry is corrupted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5077E SQL query is not correct.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5078E RDB exception occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5079E Duplicate key found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5080E Value is too large.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5081E Entry cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5082E Foreign key conflict occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5084E The ActiveCode is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5085E The password is not valid.

Explanation: See message.

User response: Set a valid password.

CTGAM5086E The IP address of the client computer is not valid.

Explanation: See message.

User response: Specify a valid IP address for the client computer

CTGAM5087E Server to server authentication failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5088E The user name is not valid.

Explanation: See message.

User response: Provide a valid user name.

CTGAM5089E Key index out of bounds.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5090E User name is not unique.

Explanation: See message.

User response: Specify a unique user name.

CTGAM5091E ActiveCode initialization failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5092E ActiveCode initialization failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5093E Secure channel is required but not available.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5094E The ActiveCode is not valid.

Explanation: See message.

User response: Specify a valid ActiveCode.

CTGAM5095E The user name is not valid.

Explanation: See message.

User response: Specify a valid user name.

CTGAM5096E ActiveCode data decryption failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5097E ActiveCode data encryption failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5098E The ActiveCode account is locked.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5099E Unable to determine when ActiveCode account was locked.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5100E Database error.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5101E The Mobile ActiveCode preference is not valid.

Explanation: See message.

User response: Specify a valid mobile ActiveCode preference.

CTGAM5102E Mobile ActiveCode expired.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5103E The application password is not valid.

Explanation: See message.

User response: Specify a valid application password.

CTGAM5104E The Mobile ActiveCode request method is not valid.

Explanation: See message.

User response: Use a valid Mobile ActiveCode request method.

CTGAM5105E The Network Access Server ID is not valid.

Explanation: See message.

User response: Specify a valid Network Access Server ID.

CTGAM5106E ActiveCode character sets not found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5107E ActiveCode algorithm not supported.

Explanation: See message.

User response: Use an ActiveCode algorithm that is supported.

CTGAM5108E ActiveCode is not enabled for authentication service.

Explanation: See message.

User response: Contact your Administrator

CTGAM5109E ActiveCode is disabled.

Explanation: See message.

User response: Contact your System Administrator.

CTGAM5110E The user secret is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5111E ActiveCode bypass failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5112E Error parsing ActiveCode.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5115E LDAP exception occured.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5116E The Connector is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5117E Access denied to connector.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5118E Connector failed to connect to external application.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5119E Deprovisioning is not supported.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5120E Deprovisioning action is not supported.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5121E The Deprovisioning status is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5122E Search count limit exceeded.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5123E Policy data cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5124E Policy data is corrupted.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5125E Policy is not defined.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5126E The policy value is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5127E The Policy value storage type is not valid.

Explanation: See message.

User response: Set a valid policy value storage type.

CTGAM5128E The policy definition is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5129E The policy is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5130E Policy template is not defined.

Explanation: See message.

User response: Define the policy template.

CTGAM5131E The policy template is not valid.

Explanation: See message.

User response: Use a valid policy template.

CTGAM5132E Default policy template cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5133E Policy template assignment cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5134E The policy resolution query is not valid.

Explanation: See message.

User response: Use a valid policy resolution query.

CTGAM5136E Unknown policy definition.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5137E The backup key activation request code is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5138E Multiple backup secrets found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5139E The Mobile ActiveCode message is not valid.

Explanation: See message.

User response: Specify a valid Mobile ActiveCode message.

CTGAM5140E The message connector is not valid.

Explanation: See message.

User response: Use a valid message connector.

CTGAM5141E Message connector disabled.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5142E Message connector failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5143E Message connector configuration is not valid.

Explanation: See message.

User response: Provide the valid Message connector configuration.

CTGAM5144E The email or phone number is not valid.

Explanation: See message.

User response: Specify a valid email or phone number.

CTGAM5145E Metadata parsing exception occurred.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5146E Metadata cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5147E Metadata snapshot cannot be obtained.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5148E Metadata key cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5149E Metadata section cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5150E Metadata group cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5151E Metadata group does not have keys.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5152E The metadata key value is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5153E Metadata attribute cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5154E Login to syslog failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5155E Log files have been tampered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5156E Log files might be tampered.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5157E The keystore is not valid.

Explanation: See message.

User response: Specify a valid keystore.

CTGAM5158E Cryptographic failed.

Explanation: This error is displayed because of an unsupported encoding.

User response: See the `SystemOut.log` file.

CTGAM5159E Encryption failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5160E Decryption failed.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5161E Missing reset symmetric key.

Explanation: The error is displayed when the system reset key is not specified in the `ims.xml` file.

User response: See the `SystemOut.log` file.

CTGAM5162E SOCI is not revoked.

Explanation: See message.

User response: See the `SystemOut.log` file.

CTGAM5163E Unknown authentication service.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5164E Unknown account data template.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5165E Unknown account data item template.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5166E Authentication service has already been defined.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5167E The authentication service is not valid.

Explanation: See message.

User response: Provide a valid authentication service.

CTGAM5168E The account data template is not valid.

Explanation: See message.

User response: Provide a valid account data template.

CTGAM5169E The account data item template is not valid.

Explanation: See message.

User response: Enter a valid account data item template.

CTGAM5170E Mismatched account data template.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5171E Unknown authentication mechanism.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5172E Unsupported authentication mechanism.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5173E Unknown data storage template.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5174E Provisioning certificate already exists.

Explanation: This message is displayed when a provisioning certificate exists for a registered user.

User response: No action is required.

CTGAM5175E Wallet ID already exists.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5176E Account already exists.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5177E Account cannot be found.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5178E User name is not valid.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5179E Too many unsuccessful attempts when entering your credentials. Contact Helpdesk.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAM5180E Unable to connect to the Active Directory domain.

CTGAN0001E Enter your user name.

Explanation: See message.

User response: See message.

CTGAN0002E The user name you entered is already registered with the IMS Server. Enter a different user name or contact your Helpdesk.

Explanation: You entered a user name that is already registered with the IMS Server.

User response: Specify a different user name or contact your Helpdesk.

CTGAN0003E The information you entered for identity verification was rejected. Before you try again, See the status of Caps Lock key. Ensure that the characters are entered in the correct case.

Explanation: You have entered information that is not valid for verifying your identity.

User response: Specify the characters in the correct case.

CTGAN0004E Select a question.

Explanation: See message.

User response: See message.

CTGAN0005E Answer the mandatory question.

Explanation: You have not answered a mandatory question.

User response: Review the form and answer the mandatory question.

CTGAN0006E Answer all the questions.

Explanation: You have not answered all the questions.

User response: Provide answers for all the questions.

CTGAN0007E Do not select the same question twice.

Explanation: You have selected the same question twice.

User response: See message.

CTGAN0008E Enter an answer for the question you selected.

Explanation: See message.

User response: See message.

CTGAN0009E Enter your ISAM ESSO password.

Explanation: See message.

User response: See message.

CTGAN0010E The new passwords you entered does not match. Enter same password in both the fields.

Explanation: You entered two different passwords.

User response: See message.

CTGAN0011E Enter a new password that satisfies all the password policy requirements.

Explanation: The password that you provided does not meet the password policy requirements.

User response: Specify a new password.

CTGAN0012E Enter a new answer that meets all the policy requirements.

Explanation: The current answer you provided does not meet the policy requirements.

User response: Read the policy requirements and specify a new answer that satisfies the policy requirements.

CTGAN0013E The user name you entered is not registered with the IMS Server. Enter a different user name or contact your Helpdesk.

Explanation: The user name is not registered with the IMS Server.

User response: Specify a different user name or contact your Helpdesk.

CTGAN0014E Your account has been disabled or revoked.

Explanation: This error message can be displayed because of several reasons.

User response: Contact your Administrator or Helpdesk.

CTGAN0015E Enter your authorization code.

Explanation: See message.

User response: Specify your authorization code. You can get your authorization code from your Administrator.

CTGAN0017E Your secret answer is not correct. Enter the correct answer. If you cannot provide the correct answer, select another question and provide the correct answer.

Explanation: This message is displayed when you provided a wrong answer for the question.

User response: Select another question and provide the correct answer.

CTGAN0018E Some of your answers are not correct. Make sure you enter the correct answer for each question.

Explanation: You have not provided the correct answers for all the questions.

User response: Ensure that you provide the correct answers for all the questions.

CTGAN0019E You cannot reset your ISAM ESSO password using secrets.

Explanation: See message.

User response: You need an authorization code to reset the IBM Security Access Manager for Enterprise Single Sign-On password.

CTGAN0020E You cannot change your password. Contact your Helpdesk.

Explanation: This error message is displayed because of several reasons.

User response: Contact your Helpdesk.

CTGAN0021E *VALUE_0* **was unable to retrieve password for logon. Try again. If the problem persists, contact your Helpdesk.**

Explanation: The IMS Server cannot retrieve password for the specific logon.

User response: Contact your Helpdesk to retrieve the password for logon.

CTGAN0022E *AccessAgent* **is currently unable to contact the application you specified. Try again. If the problem persists, contact your Helpdesk.**

Explanation: AccessAgent cannot contact the application you specified.

User response: Try again or contact your Helpdesk.

CTGAN0023E *VALUE_0* **was unable to enter your user name and password on the application. Try again. If the problem persists, contact your Helpdesk.**

Explanation: AccessAgent cannot inject your credentials into the application.

User response: Try again or contact your Helpdesk.

CTGAN0024E Your password cannot be changed. Contact your Helpdesk.

Explanation: Your attempt to change the password failed.

User response: Contact your Helpdesk.

CTGAN0025E *VALUE_0* **was unable to store your user name and password. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

CTGAN0026E You do not have permission to use *VALUE_0***. Contact your Helpdesk to enable this service.**

Explanation: See message.

User response: Contact Helpdesk to enable this service.

CTGAN0027E You have not signed up with ISAM ESSO, or you might have entered a wrong password. Sign up now or login again. Contact your Helpdesk.

Explanation: See message.

User response: Contact Helpdesk if you cannot sign up or log on to IBM Security Access Manager for Enterprise Single Sign-On.

CTGAN0028E Enter the recovery code you entered when you signed up.

Explanation: See message.

User response: See message.

CTGAN0029E Your account has been locked because you exceeded the maximum permitted login attempts. Contact your Helpdesk.

Explanation: You exceeded the maximum permitted login attempts and your account is locked.

User response: Contact your Helpdesk to unlock your account.

CTGAN0030E Mobile ActiveCodes are currently not available for your account. (Error Message : *VALUE_0***). Contact your Helpdesk.**

Explanation: One Time Passwords are not available for your account.

User response: Contact your Helpdesk.

CTGAN0031E The OTP you entered cannot be verified because the settings are not correct. (Error Message : *VALUE_0***). Contact your Helpdesk.**

Explanation: See message.

User response: Verify your settings or contact your Helpdesk.

CTGAN0032E The OTP you entered is not valid. Try again.

Explanation: The OTP you have entered has expired or is not valid.

User response: Enter the OTP again.

CTGAN0034E The authentication service cannot be created in the IMS Server. Contact your Helpdesk. (Error Message : *error number***)**

Explanation: See message.

User response: Contact your Helpdesk to create an authentication service in the IMS Server.

CTGAN0035E The authentication service cannot be created in the IMS Server. Contact your Helpdesk.

Explanation: See message.

User response: Contact your Helpdesk.

CTGAN0036E The application cannot be created in the IMS Server. Contact your Helpdesk.(Error Message : *VALUE_0***)**

Explanation: See message.

User response: See message.

CTGAN0037E The application cannot be created in the IMS Server. Contact your Helpdesk.

Explanation: See message.

User response: See message.

CTGAN0038E The AccessProfile cannot be created in the IMS Server. Contact your Helpdesk.

Explanation: See message.

User response: Contact your Helpdesk.

CTGAN0039E Messaging connectors have not yet been configured. Contact your Helpdesk.

Explanation: See message.

User response: Contact your Helpdesk.

CTGAN0040E Your password has expired. Enter a new password to change your Windows and ISAM ESSO password.

Explanation: You password has expired.

User response: Specify the new password to replace the Windows and ISAM ESSO password.

CTGAN0041E Your ISAM ESSO password does not match the password you have entered. It updates after you provide the answer to your secret question.

Explanation: The password stored in your ISAM ESSO Wallet is different from the password you are entering.

User response: Provide the correct answer to the secret question to update the ISAM ESSO Wallet.

CTGAN0042E The user name and password does not match. Try again.

Explanation: Either your user name or password is wrong.

User response: Try to enter the user name and password again.

CTGAN0043E Your account has been locked due to too many unsuccessful attempts to enter a password. Contact your Helpdesk.

Explanation: The account is locked because of several unsuccessful attempts to enter a password.

User response: Contact your Helpdesk.

CTGAN0044E Your rights to log on with this user name have been revoked. Contact your Helpdesk.

Explanation: You cannot log on using this user name. The privileges have been revoked.

User response: Contact your Helpdesk.

CTGAN0045E The authorization code you entered is not valid. Contact your Helpdesk.

Explanation: You have entered an authorization code that is not valid.

User response: Enter a valid authorization code. Contact the Helpdesk if the problem persists.

CTGAN0046E The unlock account is disabled. Contact your Helpdesk.

Explanation: You have exceeded the maximum number of attempts to unlock your account.

User response: Contact your Helpdesk.

CTGAN0047E You failed to answer the following questions:

CTGAN0048E Your enterprise account cannot be unlocked due to a temporary problem. However, your ISAM ESSO wallet was unlocked successfully.

Explanation: See message.

User response: See message.

CTGAN0049E The unlock account failed. Ensure that you provided the secret answer.

Explanation: Your attempt to unlock the account is not successful.

User response: Provide the secret answer to unlock the account.

CTGAN0050E Your Wallet cannot be updated with the latest Windows password due to a temporary problem. It is updated automatically at your next logon to *VALUE_0* **or** *VALUE_1***.**

Explanation: The Windows password that you have updated is included in your Wallet on your next logon.

User response: No action is required.

CTGAN0051E The user name field cannot be empty.

Explanation: A value is required for the user name field. This field cannot be empty.

User response: Specify a value for the user name field.

CTGAN0052E The password field cannot be empty.

Explanation: A value is required for the password field. This field cannot be empty.

User response: Specify a value for the password field.

CTGAN0053E Your password entries do not match.

Explanation: The passwords that you specified in the password and confirm password field do not match.

User response: Specify the correct password.

CTGAN0054E The display name cannot be empty. Enter a valid display name.

Explanation: A value is required for the display name field. This field cannot be empty.

User response: Specify a valid display name.

CTGAN0055E You cannot access the page directly.

Explanation: You are attempting to access a page directly. This page can be accessed only through the application.

User response: Log on to the application and access the page through the application.

CTGAN0056E You must specify your recovery code.

Explanation: Answer the secret questions.

User response: Answer the secret questions to register yourself.

CTGAN0057E Your browser does not support this method to view passwords.

Explanation: See message.

User response: See the IMS Server logs for details.

CTGAN0058E There are no application passwords to be edited.

Explanation: See message.

User response: See message.

CTGAN0059E Select the application that requires an edited password.

Explanation: See message.

User response: See message.

CTGAN0060E You can edit only one application password at a time. Select an application.

Explanation: The password can be edited only after you select the application.

User response: Select the password of the application that must be edited.

CTGAN0061E There are no application user names to be deleted.

Explanation: You are attempting to delete the application user name. However, there are no user names to be deleted.

User response: See the IMS Server logs for details.

CTGAN0062E Select the application whose user name must be deleted.

CTGAN0063E The *VALUE_0* you entered is not valid. Try again or contact your Helpdesk.

Explanation: The value you have provided is not valid anymore.

User response: Try again or contact your Helpdesk.

CTGAN0064E The *VALUE_0*/*VALUE_1* you entered is not valid. Try again or contact your Helpdesk.

Explanation: The values you have specified are not valid anymore.

User response: Try again or contact your Helpdesk.

CTGAN0065E The *VALUE_0* you entered is no longer valid. Try again or contact the help desk.

Explanation: You have entered a value that is not valid anymore.

User response: Try again to enter the value or contact your Helpdesk.

CTGAN0066E The *VALUE_0*/*VALUE_1* you entered is no longer valid. Try again or contact your Helpdesk.

Explanation: The values you have specified are not valid anymore.

User response: Provide the values again or contact your Helpdesk.

CTGAN0067E The password cannot be reset due to a temporary problem. However, you can use *VALUE_0* and the new password you just entered to log on. *VALUE_1* completes the password reset automatically at the next logon.

Explanation: See message.

User response: See message.

CTGAN0068E The password cannot be reset due to a temporary problem. Try again later. If the problem persists, contact your Helpdesk.

Explanation: This error message is displayed because of several reasons.

User response: Try again later or contact your Helpdesk.

CTGAN0069E The authorization code you entered is not valid. Try again.

Explanation: You have entered an authorization code that is not valid.

User response: Try to enter the authorization code again or contact Helpdesk to request for a new authorization code.

CTGAN0071E SSO Site cannot be added: *VALUE_0*

Explanation: See message.

User response: See message.

CTGAN0072E Enter a valid logon page URL.

Explanation: The logon page URL that you have specified is not valid.

User response: Specify a valid logon page URL.

CTGAN0073E The secret you entered is not valid. Try again.

Explanation: The secret you have entered is not valid.

User response: Enter a valid secret. See the *IBM Security Access Manager for Enterprise Single Sign-On User Guide* for more information about setting secrets.

CTGAN0074E An error occurred when verifying user secret.

Explanation: There is an error when verifying the user secret. This error is generated because of several reasons.

User response: Provide the user secret again.

CTGAN0075E The Authentication Service ID cannot be empty. Enter a valid ID.

Explanation: A value is required for the Authentication Service ID field. This field cannot be empty.

User response: Provide a valid Authentication Service ID.

CTGAN0076E Application ID cannot be empty. Enter a valid ID.

Explanation: A value is required for the Application ID field. This field cannot be empty.

User response: Provide a valid Application ID.

CTGAN0077E There was an error obtaining your current email address.

Explanation: This error message is displayed when the email address you have entered is not in a valid format.

User response: Specify the email address again.

CTGAN0078E There was an error while obtaining your current mobile phone number.

Explanation: This error message is displayed because of several reasons.

User response: Provide your mobile number again.

CTGAN0079E The default user name for the auto-logon cannot be set.

Explanation: This error message is displayed because of several reasons.

User response: Set another username as a default for auto-logon.

CTGAN0080E The default user name for the auto-logon cannot be deleted.

Explanation: You are attempting to delete the default user name for auto-logon. The default user name for auto-logon cannot be deleted.

User response: Set another user name as default user name before you delete this user name.

CTGAN0081E Deleting the application user name failed. Try again.

Explanation: Cannot delete the application user name.

User response: See the log files or try again to delete the application user name.

CTGAN0082E Updating the user name for auto-logon failed. Try again.

Explanation: This error message is displayed because of several reasons.

User response: See the log files or try again to update the user name for auto-logon.

CTGAN0083E The AccessProfile cannot be updated in the IMS Server. Error Message: *<error number>*

Explanation: See message.

User response: See message.

CTGAN0084E The *<value>* **you entered is not valid. Try again or contact your Helpdesk.**

Explanation: This error message indicates that the value you have entered is not valid.

User response: Enter a valid value. Contact your Helpdesk.

CTGAN0085E The ISAM ESSO password cannot be empty.

Explanation: A value is required for the ISAM ESSO password field. This field cannot be empty.

User response: Specify the ISAM ESSO password.

CTGAN0091E The secret answer cannot be empty.

Explanation: A value is required for the secret answer field. This field cannot be empty.

User response: Specify a value for the secret answer field.

CTGAN0092E Your OTP token cannot be reset.

Explanation: This error message is displayed because of several reasons.

User response: Contact your Helpdesk.

CTGAN0093E Try again. If the problem persists, contact your Helpdesk.

Explanation: This error message is displayed because of several reasons.

User response: Contact your Helpdesk.

CTGAN0094E You have not been assigned any OTP Tokens. Contact your Helpdesk.

Explanation: This error message is displayed because of several reasons.

User response: Contact your Helpdesk.

CTGAN0095E If you do not receive a *VALUE_0***, click the appropriate link below to get another** *VALUE_1* **in your registered** *VALUE_2* **or** *VALUE_3***.**

Explanation: This message is displayed to initiate the IMS Server to send the OTP to the registered mobile device.

User response: Click the appropriate link to receive another OTP. See the log file for more details or contact your Helpdesk.

CTGAN0096E *VALUE_0* **cannot synchronize AccessProfiles and system policies with the IMS Server. (Error Message :** *<error number>***)**

Explanation: See message.

User response: Contact your Administrator.

CTGAN0097E Try again. If the problem persists, contact your Helpdesk.

Explanation: This error message is displayed because of several reasons.

User response: See the log file for more details or contact your Helpdesk.

CTGAN0098E Unable to copy the password to the clipboard.

CTGAN0099E User name cannot contain ".

Explanation: Quotes (") is a special character that cannot be used in a user name.

User response: Provide a user name without the quotes (") character.

CTGAN0100E The email address you entered is not valid.

Explanation: The email address you entered is not valid.

User response: Specify a valid email address.

CTGAN0101E Please enter your comments.

Explanation: You are required to enter comments in this field.

User response: Provide your comments.

CTGAN0102E Unable to verify your credentials because ISAM ESSO server cannot connect to enterprise directory.

Explanation: Your credentials cannot be verified. The IMS Server cannot connect to the enterprise directory.

User response: See the connection between the IMS Server and the enterprise directory.

Chapter 4. AccessAgent messages

These messages contain information about AccessAgent.

This section provides information about the following error messages:

RFID messages

These messages contain information about RFID.

Message **AccessAgent is unable to contact the IMS Server. Try again later.**

Explanation: This message is displayed because of several reasons.

User response: Try again later or contact your Helpdesk.

Message **Either your user name and RFID do not match or you do not have privileges to login to your ISAM ESSO Wallet.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Your RFID card cannot be registered with the IMS Server. The card might be registered to some other user. Use another card.**

Explanation: See message.

User response: Use a different card. If the problem persists, contact your Helpdesk.

Message **The RFID card you have cannot be registered with the IMS Server. The card might have been registered to some other user. Contact your Helpdesk.**

Explanation: See message.

User response: Use a different card. If the problem persists, contact your Helpdesk.

Password management messages

These messages contain information about password management.

Message **Your ISAM ESSO Wallet has been locked because there have been too many unsuccessful attempts to enter its password. Log on to Windows selecting Go to Windows to log on.**

Explanation: See message.

User response: See message.

Message **Either your authorization code or password is not correct. Enter the right credentials and try again. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **The password you entered does not match the one in your Wallet. Before you try again, see the Caps Lock key. Ensure that the letters are entered in the correct case.**

Explanation: See message.

User response: See message.

Message

Message **Your Wallet has been locked due to too many unsuccessful attempts to enter its password. Click Reset password option to reset it or contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **There is a problem logging you on to the computer because either your Wallet cannot be accessed or your Windows password cannot be retrieved or verified. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Enter the password for your Wallet to store your Windows user account information:**

Explanation: See message.

User response: See message.

Message **There have been too many unsuccessful attempts to enter the password or recovery code. You need to get a new authorization code from your Helpdesk and try again.**

Explanation: See message.

User response: See message.

Message **You have already registered a ISAM ESSO Wallet and cannot register another Wallet. Log on using your password. If you cannot remember your password, use the Reset password option or log on to Windows yourself.**

Explanation: See message.

User response: See message.

Message **Unable to verify the user name and password that you provided. Check your computer's network connectivity, and then try to enter your user name and password again. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: See message.

Message **You must be connected to the IMS Server to change the password of your ISAM ESSO Wallet. Check network connections settings and try again.**

Explanation: See message.

User response: See message.

Message **The old password you entered does not match the one in your Wallet. Before you try again, See the Caps Lock key, and make sure that letters are entered in the correct case.**

Explanation: See message.

User response: See message.

Smartcard messages

These messages contain information about smartcards.

Message **You cannot register your smart card since IMS server is not available. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **The system cannot read the smart card. Remove the smart card and insert it again. If the problem persists, contact your Administrator.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **The IMS server you are using does not support smart card login. Contact your Helpdesk**

Explanation: See message.

User response: Contact your Helpdesk.

Message **The smart card certificate cannot be authenticated. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Multiple smart cards are detected. AccessAgent can read only one smart card at a time to proceed with the smart card logon.**

Explanation: See message.

User response: Tap only one smart card on the card reader.

Message **The system cannot read the smart card. Make sure that the support for smart card is properly configured. Contact your Administrator.**

Explanation: See message.

User response: Contact your Administrator.

Message **Login failed. Make sure that the support for smart card is properly configured. Contact your Administrator.**

Explanation: See message.

User response: Contact your Administrator.

Message **Your smart card was previously registered using a different certificate. Remove your card and try again. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent needs to read your hybrid smart card. Remove the card and tap it on the reader before inserting it.**

Explanation: See message.

User response: See message.

Message **Your smart card was not registered correctly. Contact your Administrator to revoke the smart card from IMS Server and register the card again**

Explanation: See message.

User response: Contact your Administrator.

Fingerprint messages

The following messages contain information about fingerprint support.

Messages **You need an Administrator privilege for this computer to perform this operation. Contact your Administrator for assistance**

Explanation: You do not have Administrator privileges on this computer to perform this operation.

User response: Contact your Administrator.

Message **Your fingerprint is required for identity verification. Use a computer with a fingerprint reader to recover your Software Key.**

Explanation: See message.

User response: See message.

Message **There is no fingerprint reader present currently. You need fingerprint authentication to log in to your Software Key.**

Explanation: See message.

User response: See message.

Message **There was error reading your fingerprint from the reader. Make sure that you use the same finger throughout the process. Try again.**

Explanation: This error is displayed if different fingers are used for successive scans during the fingerprint registration process.

User response: Use the same finger during registration.

Message **Your fingerprint does not match with the one stored in your Software Key. Try again.**

Explanation: See message.

User response: Use the registered finger to log on.

Message **The finger you are using is not registered to you. You require fingerprint authentication to unlock this machine.**

Explanation: See message.

User response: Use the registered finger to log on.

Message **Ensure that you have entered the correct user name and tapped the correct finger.**

Explanation: See message.

User response: See message.

Message **Either your user name and fingerprint do not match or you do not have privileges to log in to your ISAM ESSO Wallet.**

Explanation: See message.

User response: Contact your Administrator.

Message **Your Wallet has been locked because of too many unsuccessful attempts to log in using fingerprint. Contact your Helpdesk.**

Explanation: See message

User response: Contact your Helpdesk.

Message **You need to register a fingerprint to sign up with AccessAgent. However, AccessAgent is unable to detect a fingerprint reader. Contact your Helpdesk.**

Explanation: See message.

User response: Connect your fingerprint reader again or contact your Helpdesk.

Message **Your fingerprint registered earlier cannot be identified and will be replaced with the new one. Use your <*finger name*> to log on from now on.**

Explanation: See message.

User response: Use the newly registered finger to log on.

Message **AccessAgent is unable to detect a fingerprint reader. If you have a reader plugged in, unplug it and plug it back again.**

Explanation: See message.

User response: Unplug the reader and plug it back again.

Message **You have already registered the <*number of fingers*> finger(s) that you are allowed. Do you want to delete one?**

Explanation: See message.

User response: Click **Yes** to delete the finger print that you have scanned earlier.

Message **AccessAgent was unable to delete your fingerprint. Try again. If this problem persists, contact the Administrator.**

Explanation: See message.

User response: Contact Administrator.

Message **You can only delete an already registered fingerprint.**

Explanation: See message.

User response: See the log files.

Message **Your fingerprint does not match any of those stored on server. Click retry to try a different user name and fingerprint or register a new finger.**

Explanation: See message.

User response: Click **Retry** to try a different user name and fingerprint or register a new finger.

Installation messages

These messages contain information about installation.

Message **You need an Administrator privilege for this computer to perform this operation. Contact your Administrator for assistance**

Explanation: You do not have Administrator privileges on this computer to perform this operation.

User response: Contact your Administrator.

Message **setStringValue for previous GINA dll failed**

Explanation: Unable to write into the registry during GINA update.

User response: Verify if you have Administrator privileges when installing AccessAgent on this computer.

Message **setStringValue for GinaDLL failed**

Explanation: AccessAgent failed to write into registry during GINA update.

User response: Check whether any other software is preventing the installer from writing into the registry. Check if you have Administrator privileges to install AccessAgent.

Message **SetStringValue for PrevGINA failed**

Explanation: Unable to write into the registry during GINA update.

User response: Verify if you have Administrator privileges when installing AccessAgent on this computer.

Message **SetStringValue for engina.dll failed**

Explanation: AccessAgent cannot write into registry during GINA update.

User response: Verify if you have Administrator privileges when installing AccessAgent on this computer.

Message **The setup is exiting because installation of a required driver [Smart card reader] failed. Failed Operation: Pre-installation.**

Explanation: See message.

User response: Install the driver for the smart card reader. Run the setup again.

Message **Your system has not been modified. To complete installation at another time, run setup again.**

Explanation: This message indicates that the installation has not modified any files on your computer. The installation has failed.

User response: Run the setup again at a later time.

Message **The setup is exiting because installation of a required driver [Smart card reader] failed.**

Explanation: See message.

User response: Exit the current installation. Install the driver for the smart card reader. Run the setup again.

Message **Sorry, this OS is currently not supported in this release. Windows 2000 with Service pack 3, or Windows XP is required, along with Internet Explorer 6.0 or above.**

Explanation: See message.

User response: Do not install AccessAgent on the machine.

Message

Message **The setup cannot progress because it requires Windows XP service pack 1 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Internet Explorer 5.0 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Windows XP service pack 1 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*> You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Internet Explorer 5.0 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*> You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Windows 2000 service pack 3 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Internet Explorer 5.0 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **If you intend to use a Software Key or the black colored USB key, click Yes to continue. If you are going to use a blue or green colored USB Key you need Service Pack 3 which is currently not installed on your machine. To download the pack go to *url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The setup cannot progress because it requires Windows 2000 service pack 3 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your

browser before the setup exits.

Message **The setup cannot progress because it requires Internet Explorer 5.0 or above to be installed on your computer. Start the setup again after upgrading your machine. You can download the required files from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The installer is unable to find a IMS Server on its own. Your system administrator should have provided you with server's location. Enter the server location and click OK.**

Explanation: See message.

User response: Enter a valid IMS Server name. If required, contact your Administrator.

Message **The setup cannot progress because a required dependency 'Windows High Encryption pack' is missing on your computer. Run the setup again after installing this dependency. This dependency can be installed from <*url*>. You will need to run the setup again after installing the dependencies. Would you like the setup to open the URL in your browser before it exits?**

Explanation: See message.

User response: Click **Yes** to open the URL in your browser before the setup exits.

Message **The installer was unable to find an IMS Server at the location you provided. Check it again, or contact your helpdesk.**

Explanation: See message.

User response: Verify the IMS Server location that you provided or contact your Helpdesk.

Message **An error occurred while applying security settings. <*user or group*> is not a valid user or group. This problem is caused due to the package, or a problem connecting to a domain controller on the network. Check your network connection and click Retry, or Cancel to end the installation. Unable to locate the user's SID, system error <*error number*>.**

Explanation: See message.

User response: See message.

Message **Cannot install AccessAgent because the Windows Scripting Host on this computer is not installed or is corrupted. Contact your Administrator for assistance.**

Explanation: See message.

User response: Contact your Administrator.

Message **This is a x86 version of AccesAgent, install x64 version of AccessAgent instead.**

Explanation: This AccessAgent version is not suitable for your operating system.

User response: Use the x64 version of the AccessAgent installer.

Message **Cannot install AccessAgent because the Windows Scripting Host on this computer is disabled. Contact your Administrator.**

Explanation: Windows Scripting Host is required for installing AccessAgent.

User response: Enable Windows Scripting Host on this computer.

Chapter 5. Observer messages

These messages contain information about the Observer component.

Message **A component of AccessAgent [Sync.exe] may be compromised. Contact your administrator.**

Explanation: See message.

User response: Contact your Administrator.

Message **AccessAgent is unable to verify your Wallet password at the moment. Try again later.**

Explanation: See message.

User response: Try again later.

Message **The password you entered does not match your Wallet password. Before you try again, see the Caps Lock key, and make sure that letters are entered in the correct case.**

Explanation: See message.

User response: See message.

Message **AccessAgent is unable to carry out de-provisioning on this machine. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to de-provision** *<user name>* **for the** *<application name>***. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to de-provision** *<user name>* **on the IMS Server. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to de-provision** *<user name>* **for** *<application name>* **because this user does not exist for the application.**

Explanation: See message.

User response: Check whether the user name is entered correctly.

Message **AccessAgent is unable to de-provision** *<user name>* **for** *<application name>* **because de-provisioning is not supported for this server.**

Explanation: See message.

User response: Check with your application Administrator on how to deprovision a user.

Message **AccessAgent is unable to de-provision** *<user name>* **for** *<application name>* **on this server as the IMS Server does not have access privilege to de-provision an account.**

Explanation: See message.

User response: Contact your Administrator to request for appropriate privileges to access the IMS Server.

Message **User** *<user name>* **has been de-provisioned on the IMS Server.**

Explanation: See message.

User response: Contact your Administrator.

Message **AccessAgent is unable to generate an OTP ActiveCode. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **The new passwords you have entered do not match. Enter the same password in both fields.**

Explanation: See message.

User response: Enter the same password in both password fields.

Message **AccessAgent is unable to provision** *<user name>* **because a password has not been created for the user. Reprovision the user.**

Message

Explanation: See message.

User response: Provision the user again.

Message **AccessAgent is unable to carry out provisioning on this machine. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to provision** *<user name>* **for the IMS Server. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>***. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>***. Reprovision the user.**

Explanation: See message.

User response: Provision the user again.

Message **The user name** *<user name>* **exists on the IMS Server. You cannot provision the same user twice. Use another user name.**

Explanation: See message.

User response: Use another user name.

Message **The user name** *<user name>* **exists for** *<application name>***. You cannot provision the same user for an application twice. Use another user name.**

Explanation: See message.

User response: Use another user name.

Message **AccessAgent is unable to provision** *<user name>* **because the user ID does not meet the password policy requirements for** *<application name>***. Ensure that the application password policies are consistent, and then reprovision the user.**

Explanation: See message.

User response: Provision the user again.

Message **AccessAgent is unable to provision** *<user name>* **because the user password does not meet the password policy requirements for** *<application name>***. Ensure that the application password policies are consistent, and then reprovision the user.**

Explanation: See message.

User response: Provision the user again.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>* **because the value of the user attribute on the Active Directory Server is not valid. Contact your Administrator.**

Explanation: See message.

User response: Contact your Administrator.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>* **because of incompatible user attribute settings on the Active Directory Server. Contact your Administrator.**

Explanation: See message.

User response: Contact your Administrator.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>* **because provisioning is not supported for this server.**

Explanation: See message.

User response: Provision the user again.

Message **AccessAgent is unable to provision** *<user name>* **for** *<application name>* **on this server as the IMS Server does not have access privilege to provision an account.**

Explanation: See message.

User response: Contact the Administrator.

Message **Do you want the password you entered for** *<user name>* **to be stored and entered when you log on to** *<application name>***?**

Explanation: See message.

User response: Click **Yes** to store the password for the *<user name>* when you log on to *<application name>*.

Message **Do you want the password you entered to be stored and entered when you log on to <*application name*>?**

Explanation: See message.

User response: Click **Yes** to store the password for the <*user name*>.

Message **Do you want the password you entered for <*user name*> to be stored and entered when you log on to this application?**

Explanation: See message.

User response: Click **Yes** to store the password for the <*user name*>.

Message **You have a different password stored for the user name <*user name*> on <*application name*> in your Wallet. Do you want to replace it with the one you just entered?**

Explanation: See message.

User response: Click **Yes** to replace the old password with the new password on the Wallet.

Message **You have a different password stored for the user name <*user name*> on this application in your Wallet. Do you want to replace it with the one you just entered?**

Explanation: See message.

User response: Click **Yes** to replace the old password with the new password on the Wallet.

Message **The password does not match your Wallet password. Before you try again, see the Caps Lock key, and make sure that letters are entered in the correct case.**

Explanation: See message.

User response: See message.

Message **Your Wallet has been locked due to too many unsuccessful attempts to enter its password. Log out and log on to try again.**

Explanation: See message.

User response: Log off and log on to try again.

Message **AccessAgent is unable to verify your Wallet password at the moment. Try again later.**

Explanation: See message.

User response: Log off and log on to try again.

Message **AccessAgent is unable to add a user. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to display application settings. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to delete the user account. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to edit password. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to change the password entry option. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **You do not have sufficient access privileges to view password. Contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Unable to export your application passwords because you do not have the access privilege to save a file in this folder. Select an alternative folder. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Unable to export your application passwords because your destination drive might not have sufficient space for the exported file. Free some disk space, and try again. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Unable to export your application passwords because some unexpected error occurs. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **Unable to export your application passwords because some unexpected error occurs (error code is <*error number*>). If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to refresh your wallet display. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **AccessAgent is unable to change the password entry option. If the problem persists, contact your Helpdesk.**

Explanation: See message.

User response: Contact your Helpdesk.

Message **You cannot add any more user account for <*application name*> because you reached the authorized limit. To add an account, delete some of the existing accounts.**

Explanation: See message.

User response: Delete some of the existing accounts.

Message **The file name is not complete. Enter a complete path and file name.**

Explanation: See message.

User response: Enter the complete file path and file name.

Message **Unable to export your application passwords because the file name is not valid.**

Explanation: See message.

User response: Check whether the specified path or file name is valid. Check whether you have permission to create or write to the file or folder. Check whether the file is marked as read-only.

Message **Unable to verify Wallet password.**

Explanation: See message.

User response: Make sure that the password is correct.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

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

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

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

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

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

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration or other usage tracking or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

Glossary

This glossary includes terms and definitions for IBM Security Access Manager for Enterprise Single Sign-On.

The following cross-references are used in this glossary:

- See refers you from a term to a preferred synonym, or from an acronym or abbreviation to the defined full form.
- See also refers you to a related or contrasting term.

To view glossaries for other IBM products, go to www.ibm.com/software/globalization/terminology (opens in new window).

A

account data
The logon information required to verify an authentication service. It can be the user name, password, and the authentication service which the logon information is stored.

account data bag
A data structure that holds user credentials in memory while single sign-on is performed on an application.

account data item
The user credentials required for logon.

account data item template
A template that defines the properties of an account data item.

account data template
A template that defines the format of account data to be stored for credentials captured using a specific AccessProfile.

action In profiling, an act that can be performed in response to a trigger. For example, automatic filling of user name and password details as soon as a sign-on window displays.

Active Directory (AD)
A hierarchical directory service that enables centralized, secure management of an entire network, which is a central component of the Microsoft Windows platform.

Active Directory credential
The Active Directory user name and password.

Active Directory password synchronization
An IBM Security Access Manager for Enterprise Single Sign-On feature that synchronizes the ISAM ESSO password with the Active Directory password.

active radio frequency identification (active RFID) A second authentication factor and presence detector. See also radio frequency identification.

active RFID
See active radio frequency identification.

AD See Active Directory.

administrator
A person responsible for administrative tasks such as access authorization and content management. Administrators can also grant levels of authority to users.

API See application programming interface.

application
A system that provides the user interface for reading or entering the authentication credentials.

application policy
A collection of policies and attributes governing access to applications.

application programming interface (API)
An interface that allows an application program that is written in a high-level language to use specific data or functions of the operating system or another program.

audit A process that logs the user, Administrator, and Helpdesk activities.

authentication factor
The device, biometrics, or secrets required as a credentials for validating digital identities. Examples of authentication

factors are passwords, smart card, RFID, biometrics, and one-time password tokens.

authentication service
A service that verifies the validity of an account; applications authenticate against their own user store or against a corporate directory.

authorization code
An alphanumeric code generated for administrative functions, such as password resets or two-factor authentication bypass.

auto-capture
A process that allows a system to collect and reuse user credentials for different applications. These credentials are captured when the user enters information for the first time, and then stored and secured for future use.

automatic sign-on
A feature where users can log on to the sign-on automation system and the system logs on the user to all other applications.

B

base distinguished name
A name that indicates the starting point for searches in the directory server.

base image
A template for a virtual desktop.

bidirectional language
A language that uses a script, such as Arabic and Hebrew, whose general flow of text proceeds horizontally from right to left, but numbers, English, and other left-to-right language text are written from left to right.

bind distinguished name
A name that specifies the credentials for the application server to use when connecting to a directory service. The distinguished name uniquely identifies an entry in a directory.

biometrics
The identification of a user based on a physical characteristic of the user, such as a fingerprint, iris, face, voice, or handwriting.

C

CA See certificate authority.

CAPI See cryptographic application programming interface.

Card Serial Number (CSN)
A unique data item that identifies a hybrid smart card. It has no relation to the certificates installed in the smart card

CCOW
See Clinical Context Object Workgroup.

cell A group of managed processes that are federated to the same deployment manager and can include high-availability core groups.

certificate
In computer security, a digital document that binds a public key to the identity of the certificate owner, thereby enabling the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority. See also certificate authority.

certificate authority (CA)
A trusted third-party organization or company that issues the digital certificates. The certificate authority typically verifies the identity of the individuals who are granted the unique certificate. See also certificate.

CLI See command-line interface.

Clinical Context Object Workgroup (CCOW)
A vendor independent standard, for the interchange of information between clinical applications in the healthcare industry.

cluster
A group of application servers that collaborate for the purposes of workload balancing and failover.

command-line interface (CLI)
A computer interface in which the input and output are text based.

credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a

user ID and password are credentials that allow access to network and system resources.

cryptographic application programming interface (CAPI)
An application programming interface that provides services to enable developers to secure applications using cryptography. It is a set of dynamically-linked libraries that provides an abstraction layer which isolates programmers from the code used to encrypt the data.

cryptographic service provider (CSP)
A feature of the i5/OS™ operating system that provides APIs. The CCA Cryptographic Service Provider enables a user to run functions on the 4758 Coprocessor.

CSN See Card Serial Number.

CSP See cryptographic service provider.

D

dashboard
An interface that integrates data from a variety of sources and provides a unified display of relevant and in-context information.

database server
A software program that uses a database manager to provide database services to other software programs or computers.

data source
The means by which an application accesses data from a database.

deployment manager
A server that manages and configures operations for a logical group or cell of other servers.

deployment manager profile
A WebSphere Application Server runtime environment that manages operations for a logical group, or cell, of other servers.

deprovision
To remove a service or component. For example, to deprovision an account means to delete an account from a resource. See also provision.

desktop pool
A collection of virtual desktops of similar configuration intended to be used by a designated group of users.

directory
A file that contains the names and controlling information for objects or other directories.

directory service
A directory of names, profile information, and machine addresses of every user and resource on the network. It manages user accounts and network permissions. When a user name is sent, it returns the attributes of that individual, which might include a telephone number, as well as an email address. Directory services use highly specialized databases that are typically hierarchical in design and provide fast lookups.

disaster recovery
The process of restoring a database, system, policies after a partial or complete site failure that was caused by a catastrophic event such as an earthquake or fire. Typically, disaster recovery requires a full backup at another location.

disaster recovery site
A secondary location for the production environment in case of a disaster.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute:value pairs, separated by commas. For example, CN=person name and C=country or region.

DLL See dynamic link library.

DN See distinguished name.

DNS See domain name server.

domain name server (DNS)
A server program that supplies name-to-address conversion by mapping domain names to IP addresses.

dynamic link library (DLL)
A file containing executable code and data bound to a program at load time or run time, rather than during linking. The code and data in a DLL can be shared by several applications simultaneously.

E

enterprise directory
A directory of user accounts that define IBM Security Access Manager for Enterprise Single Sign-On users. It validates user credentials during sign-up and logon, if the password is synchronized with the enterprise directory password. An example of an enterprise directory is Active Directory.

enterprise single sign-on (ESSO)
A mechanism that allows users to log on to all applications deployed in the enterprise by entering a user ID and other credentials, such as a password.

ESSO See enterprise single sign-on.

event code
A code that represents a specific event that is tracked and logged into the audit log tables.

F

failover
An automatic operation that switches to a redundant or standby system or node in the event of a software, hardware, or network interruption.

fast user switching
A feature that allows users to switch between user accounts on a single workstation without quitting and logging out of applications.

Federal Information Processing Standard (FIPS)
A standard produced by the National Institute of Standards and Technology when national and international standards are nonexistent or inadequate to satisfy the U.S. government requirements.

FIPS See Federal Information Processing Standard.

fix pack
A cumulative collection of fixes that is released between scheduled refresh packs, manufacturing refreshes, or releases. A fix pack updates the system to a specific maintenance level.

FQDN
See fully qualified domain name.

fully qualified domain name (FQDN)
In Internet communications, the name of a host system that includes all of the subnames of the domain name. An example of a fully qualified domain name is rchland.vnet.ibm.com. See also host name.

G

GINA See graphical identification and authentication.

GPO See group policy object.

graphical identification and authentication (GINA)
A dynamic link library that provides a user interface that is tightly integrated with authentication factors and provides password resets and second factor bypass options.

group policy object (GPO)
A collection of group policy settings. Group policy objects are the documents created by the group policy snap-in. Group policy objects are stored at the domain level, and they affect users and computers contained in sites, domains, and organizational units.

H

HA See high availability.

high availability (HA)
The ability of IT services to withstand all outages and continue providing processing capability according to some predefined service level. Covered outages include both planned events, such as maintenance and backups, and unplanned events, such as software failures, hardware failures, power failures, and disasters.

host name
In Internet communication, the name given to a computer. The host name might be a fully qualified domain name such as mycomputer.city.company.com, or it might be a specific subname such as mycomputer. See also fully qualified domain name, IP address.

hot key
A key sequence used to shift operations

between different applications or between different functions of an application.

hybrid smart card
An ISO-7816 compliant smart card which contains a public key cryptography chip and an RFID chip. The cryptographic chip is accessible through contact interface. The RFID chip is accessible through contactless (RF) interface.

I

interactive graphical mode
A series of panels that prompts for information to complete the installation.

IP address
A unique address for a device or logical unit on a network that uses the Internet Protocol standard. See also host name.

J

Java Management Extensions (JMX)
A means of doing management of and through Java technology. JMX is a universal, open extension of the Java programming language for management that can be deployed across all industries, wherever management is needed.

Java runtime environment (JRE)
A subset of a Java developer kit that contains the core executable programs and files that constitute the standard Java platform. The JRE includes the Java virtual machine (JVM), core classes, and supporting files.

Java virtual machine (JVM)
A software implementation of a processor that runs compiled Java code (applets and applications).

JMX See Java Management Extensions.

JRE See Java runtime environment.

JVM See Java virtual machine.

K

keystore
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted or public keys. See also truststore.

L

LDAP See Lightweight Directory Access Protocol.

Lightweight Directory Access Protocol (LDAP)
An open protocol that uses TCP/IP to provide access to directories that support an X.500 model. An LDAP can be used to locate people, organizations, and other resources in an Internet or intranet directory.

lightweight mode
A Server AccessAgent mode. Running in lightweight mode reduces the memory footprint of AccessAgent on a Terminal or Citrix Server and improves the single sign-on startup duration.

linked clone
A copy of a virtual machine that shares virtual disks with the parent virtual machine in an ongoing manner.

load balancing
The monitoring of application servers and management of the workload on servers. If one server exceeds its workload, requests are forwarded to another server with more capacity.

lookup user
A user who is authenticated in the Enterprise Directory and searches for other users. IBM Security Access Manager for Enterprise Single Sign-On uses the lookup user to retrieve user attributes from the Active Directory or LDAP enterprise repository.

M

managed node
A node that is federated to a deployment manager and contains a node agent and can contain managed servers. See also node.

mobile authentication
An authentication factor which allows mobile users to sign-on securely to corporate resources from anywhere on the network.

N

network deployment
The deployment of an IMS™ Server on a WebSphere Application Server cluster.

node A logical group of managed servers. See also managed node.

node agent
An administrative agent that manages all application servers on a node and represents the node in the management cell.

O

one-time password (OTP)
A one-use password that is generated for an authentication event, and is sometimes communicated between the client and the server through a secure channel.

OTP See one-time password.

OTP token
A small, highly portable hardware device that the owner carries to authorize access to digital systems and physical assets, or both.

P

password aging
A security feature by which the superuser can specify how often users must change their passwords.

password complexity policy
A policy that specifies the minimum and maximum length of the password, the minimum number of numeric and alphabetic characters, and whether to allow mixed uppercase and lowercase characters.

personal identification number (PIN)
In Cryptographic Support, a unique number assigned by an organization to an individual and used as proof of identity. PINs are commonly assigned by financial institutions to their customers.

PIN See personal identification number.

pinnable state
A state from an AccessProfile widget that can be combined to the main AccessProfile to reuse the AccessProfile widget function.

PKCS See Public Key Cryptography Standards.

policy template
A predefined policy form that helps users define a policy by providing the fixed policy elements that cannot be changed and the variable policy elements that can be changed.

portal A single, secure point of access to diverse information, applications, and people that can be customized and personalized.

presence detector
A device that, when fixed to a computer, detects when a person moves away from it. This device eliminates manually locking the computer upon leaving it for a short time.

primary authentication factor
The IBM Security Access Manager for Enterprise Single Sign-On password or directory server credentials.

private key
In computer security, the secret half of a cryptographic key pair that is used with a public key algorithm. The private key is known only to its owner. Private keys are typically used to digitally sign data and to decrypt data that has been encrypted with the corresponding public key.

provision
To provide, deploy, and track a service, component, application, or resource. See also deprovision.

provisioning API
An interface that allows IBM Security Access Manager for Enterprise Single Sign-On to integrate with user provisioning systems.

provisioning bridge
An automatic IMS Server credential distribution process with third party provisioning systems that uses API libraries with a SOAP connection.

provisioning system
A system that provides identity lifecycle management for application users in enterprises and manages their credentials.

Public Key Cryptography Standards (PKCS)
A set of industry-standard protocols used for secure information exchange on the Internet. Domino® Certificate Authority and Server Certificate Administration applications can accept certificates in PKCS format.

published application
An application installed on Citrix XenApp server that can be accessed from Citrix ICA Clients.

published desktop
A Citrix XenApp feature where users have remote access to a full Windows desktop from any device, anywhere, at any time.

R

radio frequency identification (RFID)
An automatic identification and data capture technology that identifies unique items and transmits data using radio waves. See also active radio frequency identification.

RADIUS
See remote authentication dial-in user service.

random password
An arbitrarily generated password used to increase authentication security between clients and servers.

RDP See remote desktop protocol.

registry
A repository that contains access and configuration information for users, systems, and software.

registry hive
In Windows systems, the structure of the data stored in the registry.

remote authentication dial-in user service (RADIUS)
An authentication and accounting system that uses access servers to provide centralized management of access to large networks.

remote desktop protocol (RDP)
A protocol that facilitates remote display and input over network connections for Windows-based server applications. RDP supports different network topologies and multiple connections.

replication
The process of maintaining a defined set of data in more than one location. Replication involves copying designated changes for one location (a source) to another (a target) and synchronizing the data in both locations.

revoke
To remove a privilege or an authority from an authorization identifier.

RFID See radio frequency identification.

root CA
See root certificate authority.

root certificate authority (root CA)
The certificate authority at the top of the hierarchy of authorities by which the identity of a certificate holder can be verified.

S

scope A reference to the applicability of a policy, at the system, user, or machine level.

secret question
A question whose answer is known only to the user. A secret question is used as a security feature to verify the identity of a user.

secure remote access
The solution that provides web browser-based single sign-on to all applications from outside the firewall.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. With SSL, client/server applications can communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

Secure Sockets Layer virtual private network (SSL VPN)
A form of VPN that can be used with a standard web browser.

Security Token Service (STS)
A web service that is used for issuing and exchanging security tokens.

security trust service chain
A group of module instances that are

configured for use together. Each module instance in the chain is called in turn to perform a specific function as part of the overall processing of a request.

serial ID service provider interface
A programmatic interface intended for integrating AccessAgent with third-party Serial ID devices used for two-factor authentication.

serial number
A unique number embedded in the IBM Security Access Manager for Enterprise Single Sign-On keys, which is unique to each key and cannot be changed.

server locator
A locator that groups a related set of web applications that require authentication by the same authentication service. In AccessStudio, server locators identify the authentication service with which an application screen is associated.

service provider interface (SPI)
An interface through which vendors can integrate any device with serial numbers with IBM Security Access Manager for Enterprise Single Sign-On and use the device as a second factor in AccessAgent.

signature
In profiling, unique identification information for any application, window, or field.

sign-on automation
A technology that works with application user interfaces to automate the sign-on process for users.

sign up
To request a resource.

silent mode
A method for installing or uninstalling a product component from the command line with no GUI display. When using silent mode, you specify the data required by the installation or uninstallation program directly on the command line or in a file (called an option file or response file).

Simple Mail Transfer Protocol (SMTP)
An Internet application protocol for transferring mail among users of the Internet.

single sign-on (SSO)
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

smart card
An intelligent token that is embedded with an integrated circuit chip that provides memory capacity and computational capabilities.

smart card middleware
Software that acts as an interface between smart card applications and the smart card hardware. Typically the software consists of libraries that implement PKCS#11 and CAPI interfaces to smart cards.

SMTP See Simple Mail Transfer Protocol.

snapshot
A captured state, data, and hardware configuration of a running virtual machine.

SOAP A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and invoke services across the Internet. See also web service.

SPI See service provider interface.

SSL See Secure Sockets Layer.

SSL VPN
See Secure Sockets Layer virtual private network.

SSO See single sign-on.

stand-alone deployment
A deployment where the IMS Server is deployed on an independent WebSphere Application Server profile.

stand-alone server
A fully operational server that is managed independently of all other servers, using its own administrative console.

strong authentication
A solution that uses multifactor authentication devices to prevent unauthorized access to confidential corporate information and IT networks, both inside and outside the corporate perimeter.

strong digital identity
An online persona that is difficult to impersonate, possibly secured by private keys on a smart card.

STS See Security Token Service.

system modal message
A system dialog box that is typically used to display important messages. When a system modal message is displayed, nothing else can be selected on the screen until the message is closed.

T

terminal emulator
A program that allows a device such as a microcomputer or personal computer to enter and receive data from a computer system as if it were a particular type of attached terminal.

terminal type (tty)
A generic device driver for a text display. A tty typically performs input and output on a character-by-character basis.

thin client
A client that has little or no installed software but has access to software that is managed and delivered by network servers that are attached to it. A thin client is an alternative to a full-function client such as a workstation.

transparent screen lock
An feature that, when enabled, permits users to lock their desktop screens but still see the contents of their desktop.

trigger
In profiling, an event that causes transitions between states in a states engine, such as, the loading of a web page or the appearance of a window on the desktop.

trust service chain
A chain of modules that operate in different modes such as validate, map, and issue truststore.

truststore
In security, a storage object, either a file or a hardware cryptographic card, where public keys are stored in the form of trusted certificates, for authentication purposes in web transactions. In some applications, these trusted certificates are moved into the application keystore to be stored with the private keys. See also keystore.

tty See terminal type.

two-factor authentication
The use of two factors to authenticate a user. For example, the use of password and an RFID card to log on to AccessAgent.

U

uniform resource identifier
A compact string of characters for identifying an abstract or physical resource.

user credential
Information acquired during authentication that describes a user, group associations, or other security-related identity attributes, and that is used to perform services such as authorization, auditing, or delegation. For example, a user ID and password are credentials that allow access to network and system resources.

user deprovisioning
The process of removing a user account from IBM Security Access Manager for Enterprise Single Sign-On.

user provisioning
The process of signing up a user to use IBM Security Access Manager for Enterprise Single Sign-On.

V

VB See Visual Basic.

virtual appliance
A virtual machine image with a specific application purpose that is deployed to virtualization platforms.

virtual channel connector
A connector that is used in a terminal services environment. The virtual channel connector establishes a virtual communication channel to manage the remote sessions between the Client AccessAgent component and the Server AccessAgent.

virtual desktop
A user interface in a virtualized environment, stored on a remote server.

virtual desktop infrastructure
An infrastructure that consists of desktop operating systems hosted within virtual machines on a centralized server.

Virtual Member Manager (VMM)
A WebSphere Application Server component that provides applications with a secure facility to access basic organizational entity data such as people, logon accounts, and security roles.

virtual private network (VPN)
An extension of a company intranet over the existing framework of either a public or private network. A VPN ensures that the data that is sent between the two endpoints of its connection remains secure.

Visual Basic (VB)
An event-driven programming language and integrated development environment (IDE) from Microsoft.

VMM See Virtual Member Manager.

VPN See virtual private network.

W

wallet A secured data store of access credentials of a user and related information, which includes user IDs, passwords, certificates, encryption keys.

wallet caching
The process during single sign-on for an application whereby AccessAgent retrieves the logon credentials from the user credential wallet. The user credential wallet is downloaded on the user machine and stored securely on the IMS Server.

wallet manager
The IBM Security Access Manager for Enterprise Single Sign-On GUI component that lets users manage application credentials in the personal identity wallet.

web server
A software program that is capable of servicing Hypertext Transfer Protocol (HTTP) requests.

web service
A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available. See also SOAP.

WS-Trust
A web services security specification that defines a framework for trust models to establish trust between web services.

Index

Printed in USA

GC14-7624-02