iManage

Making knowledge work

iManage SQL Agent for iManage Security Policy Manager Installation Guide

Publication date: October 2023

Product version: 10.3.1.1

Document revision: 0

Notice

This documentation is a proprietary product of **iManage LLC** and is protected by copyright laws and international treaty. Information in this documentation is subject to change without notice and does not represent a commitment on the part of iManage. While reasonable efforts have been made to ensure the accuracy of the information contained herein, iManage assumes no liability for errors or omissions. No liability is assumed for direct, incidental, or consequential damages resulting from the use of the information contained in this documentation.

The copyrighted software that accompanies this documentation is licensed to the End User for use only in strict accordance with the End User License Agreement, which the Licensee should read carefully before commencing use of the software. No part of this publication may be reproduced, transmitted, stored in a retrieval system, nor translated into any human or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of the copyright owner. This documentation may use fictitious names for purposes of demonstration; references to actual persons, companies, or organizations are strictly coincidental.

Trademarks and Copyrights

Notice to Government End Users

If this product is acquired under the terms of a

- **DoD contract**: Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of 252.227-7013.
- **Civilian agency contract**: Use, reproduction or disclosure is subject to 52.227-19 (a) through (d) and restrictions set forth in the accompanying end user agreement.

Unpublished-rights reserved under the copyright laws of the United States. **iManage,71 S. Wacker Drive, Suite 400, Chicago, IL 60606, US**.

Acknowledgements

RSA Data Security, Inc. MD5 Message-Digest Algorithm; zlib general purpose compression library, Jean-loup Gailly and Mark Adler; Info-ZIP, more information at ftp://ftp.info-zip.org/pub/infozip/license.html; HTML-to-RTF Pro DLL 1.8 © 2002-2007 SautinSoft.

Contents

Preface

This document provides the essential information required for the installation, application and upgrade of iManage SQL Agent. It is relevant to 3rd Parties who have opted to integrate with SPM using MS SQL Server.

Alternate integration mechanisms include:

- iManage SPM REST
- a custom iManage SPM Agent

About agents in iManage Security Policy Manager

When your organization stores sensitive client and matter material across multiple locations, systems, and file shares, it is imperative that security policies can be applied across these systems and repositories consistently and performantly. With iManage Security Policy Manager (iManage SPM), you can apply your organizational security policies across a wide range of systems.

To do this, iManage SPM supports the connection of multiple "agents": exclusive services that apply iManage SPM security to the systems to be secured (target systems). Each iManage SPM agent is installed separately and secures a single system or location type. Multiple agents of the same type can also be installed; such as when securing file shares in different geographical locations.

For example, if your organization has client and matter content stored in various geographical locations across iManage Work, Microsoft Windows File Shares, and Linux file shares, you can secure each of these with the corresponding agent.

When agents are connected to iManage SPM, security policy is applied via the agents to the target systems automatically, and the agents can be monitored and managed centrally from within the iManage SPM Administration Console.

The installation and configuration of each agent is performed separately. For more information about individual agents, see their corresponding guides.

iManage Security Policy Manager currently has 11 agents that can be installed to apply security to specific systems:

- iManage Work agent
- iManage Records Manager agent
- Elite Enterprise agent
- iManage Elite 3E agent
- iManage Aderant Agent
- iManage SharePoint Agent
- Generic File System agent
- Windows File System agent
- Intapp Time agent
- Intapp Open agent
- Carpe Diem agent
- iManage Teams Agent

There are also four specialized agents that can be used for specific purposes:

- SQL Server agent
- iManage HR agent
- iManage Custom agent
- iManage Policy Cache agent

Related Documents

- iManage Security Policy Manager Installation Guide
- iManage Security Policy Manager Administration Guide
- iManage Work Agent for SPM and Preparation of iManage Work for SPM Integration
- iManage Records Manager (IRM) Agent for SPM and Preparation of IRM for SPM Integration
- Elite Agent for iManage Security Policy Manager Installation Guide
- File System Agent for iManage Security Policy Manager Installation Guide
- HR Agent for iManage Security Policy Manager Installation Guide
- Intapp Time Agent for iManage Security Policy Manager Installation Guide
- Carpe Diem Agent for iManage Security Policy Manager Installation Guide
- Custom Agent for iManage Security Policy Manager Installation Guide
- iManage Policy Cache Agent Installation Guide
- iManage Aderant Agent Installation Guide
- iManage SharePoint Agent Installation and SharePoint Integration Guide
- iManage Teams Agent for Security Policy Manager Installation Guide

Compatibility

- Latest software recommended - SPM 10..3.1
- Compatibility exists with SPM Server 10.3.1 and the following:

Compatibility
SQL agent for iManage Security Policy Manager 1.4.x or later

Navigating this Document

This document is designed to provide quick access to the information you may require for this product. For easy navigation, the following options are provided:

- **Principal table of contents**
  - Located at the beginning of the document, this option lists all sections and main headings of the document along with the page numbers. All items are selectable (linked).
- **Sectional tables of contents**
  - Longer sections may include a sectional table of contents for ease of navigation within those sections.
- **Collapsible bookmarks**

  - A bookmarks panel is displayed by default upon opening the document. This contains a nested list of all headings within the document.
- **Selectable links**
  - Selectable links, presented with blue text, enable you to jump to other relevant parts within the document (or to pertinent websites, when applicable). To make full use of this functionality, iManage recommends that you configure reverse navigation in your PDF reading software.
    - For example, in Adobe Acrobat software, go to: **View** > **Show/Hide** > **Toolbar Items** > **Show Page Navigation Tools**. Select **Previous View**. When you select an internal link, the linked page opens. You can see the **Previous View** button on the toolbar. Select this button to return to the page from which you selected the link. If you are using a device with keyboard, you can also use shortcut "**alt+Left Arrow**" to return to previous view.
- **External referencing**
  - References to other documents are displayed in the following manner: Refer to *iManage Work Server Installation Guide 10.2*.

Conventions

The following conventions are used in this document.

Notational Conventions

This guide uses the following conventions:

Convention	Usage
Bold	User-interface elements such as a menu item or button. For example: Click **Cancel** to halt the operation.
Italics	Document titles and new terms. For example: • For more information, refer to *iManage Security Policy Manager Administration Guide*. • An *action command* is a request, such as a query or indexing instruction, sent to IDOL Server.

Notices

NOTE:

A note provides information that emphasizes or supplements important points of the main text. A note supplies information that may apply only in special cases. For example, memory limitations, equipment configurations, or details that apply to specific versions of the software.

CAUTION:

A caution indicates an action that can result in the loss of data.

TIP:

A tip provides additional information that makes a task easier or more productive.

Documentation Updates and Support

iManage Support provides prompt and accurate support to help you resolve issues you may encounter or questions you may have while using iManage products. Support services include access to the Help Center for online answers, expert service by iManage support engineers, and software maintenance to ensure you have the most up-to-date technology.

To access the iManage Help Center, visit https://help.imanage.com

Help Center provides access to:

- **Knowledge base and production documentation:** The Help Center Knowledge Base and Documentation sections contain an extensive library of technote articles, FAQs, and product documentation.
- **Releases and release notes:** The Help Center Releases section contains iManage product installer downloads, release notes, and links to available patch releases.
- **Community:** The Help Center Community section allows you to interact with other iManage Community members and iManage Support engineers in order to seek answers to your questions or help provide answers to others' questions.
- **Podcasts and videos:** The Podcasts and Videos sections offer a library of audio and video reference materials to help you learn more about implementing, using, and maintaining iManage products.
- **Announcements:** Receive announcement notifications by following the announcement sections you find most relevant to your needs for information such as: support news, new releases and resources, and technical updates.
- **Case portal:** The Help Center also includes your iManage Support case portal where you can submit and manage all your support cases.

You can retrieve the latest available product documentation from iManage’s Knowledge Base in the iManage Help Center. A document in the Knowledge Base has a *version number* (for example, version 1.4.1) and may also have a *revision number* (for example, revision 3). The version number applies to the product that the document describes. The revision number applies to the document. The Knowledge Base contains the latest available revision of any document.

You can submit a support request or manage existing requests online, by selecting **Submit a request** on the top navigation menu in Help Center.

You can also submit a new support case to iManage Support by email: contact us at support@imanage.com.

To contact iManage Support by phone, please refer to the iManage Support FAQ knowledge base article in Help Center for contact information by region.

Changes in this document version

This page provides a changelog for versions and revisions of this guide.

Changes in document version 10.3.1.1

- Updates to .NET framework prerequisites. See Prerequisites.

Changes in document version 10.3.1

- Update of .NET and Java prerequisites. See Prerequisites.

Prerequisites

The prerequisites for installing this agent are listed below. Note that if you are connecting the agent to SPM Service in the Cloud, these prerequisites are already met and you can proceed to Overview of iManage SQL Agent and SPM Compliance.

- Java 17 must be installed on the server.

  NOTE:

  SPM supports both Oracle and OpenJDK implementations of the Java platform.

- The .NET Framework version installed on the server must be compatible with a target framework of 4.0. For more information about .NET framework version compatibility, go to https://learn.microsoft.com/en-us/dotnet/framework/migration-guide/version-compatibility.
- iManage Security Policy Manager Server services must be running for the agent to operate: but are not required during installation.

Also refer to the *Certificate requirements* section in Installation.

Overview of iManage SQL Agent and SPM Compliance

This section details the following:

About iManage SQL Agent

iManage SQL Agent provides access to the latest iManage Security Policy Manager (SPM) Policy definitions and a Changes Log capturing policy change events.

The installation process for iManage SQL Agent (as detailed in this guide) includes the creation of a SQL database "SPMAgentSecurity".

NOTE:

For installation instructions, see Installation of iManage SQL Agent.

iManage SQL Agent and SPM Compliance

For a 3rd Party application to be considered compliant with SPM, the following must be in place:

- Searching for items will never return results that violate SPM Policy.
- Browsing for items will never return results that violate SPM Policy.
- Any newly introduced or renamed or moved client/matter should adhere to SPM Policy immediately.
- Any newly introduced or renamed user account should adhere to SPM Policy immediately.
- Product security can be more restrictive than SPM policy. Product security should never be more open than SPM policy.

Policy Definition

Policy is captured into the following tables:

- governacl - identifies the SPM Policy impacting the client and/or matter.
  - When matterId is blank, it is a client policy.
  - When matterId is '_default_', it is a matter policy impacting those matters within the client that do not have their own policy
  - When matterId is not blank and not '_default_', it is a matter policy impacting the specified matter.
  - When defaultAllowAcces is 'T', then all users in the system should be given access access unless they have been denied (refer to governace)
  - When defaultAllowAcces is 'F', then all users in the system should be denied access access unless they have been allowed (refer to governace)

- governovr - identifies the set of users that should always have access unless they have been denied access by policy (refer to governace)
- governeu - identifies the set of users that should only have access to a client/matter if they are specifically listed on that client/matter (refer to governace)
- governace - on a per policy basis, lists users that should have access (allowaccess = 'T') and those users that should not have access (allowaccess = 'F')

Change Log Event Processing

The Change Log event list is available using view_govern_changeevent. The Change Log will record changes by ascending identifier.

Polling for changes by Id is recommended. For example, if Events with Id 1 through 10 have been processed, then processing should continue with the next batch of changes where the Id is greater than 10.

An Event will provide Id, EventDateTime, EventType, EventDescription, ClientId, and MatterId.

The following event types exist:

Event Type	Description
PA	Policy Add
PR	Policy Remove
PU	Policy Update - defaultallowaccess
EL	External User list has changed
OL	Over the Wall list has changed
UL	Policy User list has changed
SU	System User list has changed. This event is only generated for those integrations that are populating the Users table. Populating this table is a prerequisite for Index integration.

The following Installation section provides instruction on the installation and upgrade of iManage SQL Agent. If you require any assistance or additional information regarding the installation, for example on the modifiable settings of the .cfg file, contact iManage Support – see Preface for details.

Installation

This section details how to install and start the iManage SQL Agent for Security Policy Manager.

Certificate requirements

- About certificates for agents
- Obtaining the certificate
- Installing the certificate

About certificates for agents

An SSL certificate is a digital certificate that enables an encrypted connection between the agent and SPM, by authenticating the identity of the SPM Server that the agent is connecting to.

When SSL is enabled in SPM Server, you must import the full chain of trust of the SPM Server SSL certificate to the Java truststore of the system where you are installing this agent. Details on how you can do this are provided in the subsections below.

NOTE:

SPM Service in the Cloud is SSL-enabled, You need to perform the steps in this section when installing this agent, to ensure a valid certificate is installed.

Obtaining the certificate

Whether you are connecting the agent to SPM Service in the Cloud, or SPM on-premises, you can use similar steps to obtain the full chain of trust of the SPM Server SSL certificate, in PEM format.

The steps below show how to do this using Mozilla® Firefox®, but similar steps can be performed in other browsers - refer to the relevant browser product documentation for more information.

1. Log in to SPM Administration Console using Mozilla® Firefox®.
2. Select the padlock symbol 🔒 beside the address bar. Connection security information is displayed.
3. Select **More Information**. The **Page Info** dialog opens at the **Security** tab.
4. Select **View Certificate**. The certificate information is displayed.
5. Under **Miscellaneous**, select (Download) **PEM (chain)**.
6. Select ⤓ to view the downloaded PEM file.

   TIP:

   To check the certificate downloaded is in the correct (PEM, Base64) format, you can open the file in a text editor. PEM files are displayed as follows:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate information>
   -----END CERTIFICATE-----
   ```

   where `<certificate information>` is the certificate content, comprising alphanumeric and special characters.

7. Save the file, noting its location. You will need this when installing the certificate.

Installing the certificate

Copy/Install the certificate onto the machine where you are installing the agent. The following steps describe how to do this:

1. Open the command line interface as a user with administrator access.
2. Import the certificate into the java truststore using a command similar to:

   ```
   <keytool.exe location> -importcert -file <certificate location> -alias <cert
   alias> -keystore "<truststore location>"
   ```

   Where:

   - `<keytool.exe location>` is the location of the Java Keytool EXE. This EXE is included within standard JDK or JRE distributions, for example: `"%JAVA_HOME%\bin\keytool"`.
   - `<certificate location>` is the filepath to the certificate including the certificate name.
   - `<truststore location>` is the location of the cacerts truststore file, for example `C:\Program Files\Java\<JAVA_VERSION>\lib\security\cacerts`
   - `<cert alias>` is the optional alias of the certificate.

3. Enter the truststore password when prompted. (The default truststore password is `changeit`.)

The certificate is now in place to enable the agent to connect to SPM in production.

Installation of iManage SQL Agent

Installation Overview

Follow the numbered steps below to install iManage SQL Agent, referring to the linked sections (below) for additional configuration information

1. Extract the installation package files to a destination folder of your choice.
2. The installation package folder contains the `aclapplier_setup.sql` file. Run this script using MS SQL Enterprise Studio to establish a database SPMAgentSecurity.
3. Edit `iManage SQL Agent.cfg`. Review the default settings and adjust where necessary. See iManage SQL Agent Configuration Settings.
   a. Service Account
   b. SPM Settings
   c. ACL Applier Settings
   d. Optional configuration for client ID and matter ID padding
4. Right-click `iManage SQL Agent Setup.cmd`, and select **Run as Administrator**.
5. Follow the instructions provided in the setup wizard. iManage SQL Agent is now installed.

NOTE:

If there is a need to adjust configuration post installation, simply repeat steps 2 through 5 above.

iManage SQL Agent Configuration Settings

Service Account

When installation completes, a new service is installed, namely, the SPM SQL Agent service.

service.user identifies the user that this service logs on as.

If the value is left blank, then the currently logged in user is assumed.

SPM Settings

These are the configurations that the agent uses to connect to SPM server.

1. In the `securityPolicyManager.server` field, enter the host name or the IP address for iManage SPM Server. By default, this is `localhost`.

   NOTE:

   For iManage Security Policy Manager hosted in the Cloud, enter the relevant hostname component of the URL (as supplied by iManage).
   For example, for URL https://*<OrganizationID>*-spm.imanage.work/, where "*<OrganizationID>*" is your customer ID or the vanity URL of your organization, as supplied by iManage, enter `<OrganizationID>-spm.imanage.work.`

2. In the `securityPolicyManager.port` field:

a. for iManage Security Policy Manager installed on-premises, enter the port number for iManage SPM Server. The default value is `8080`.

b. for iManage Security Policy Manager hosted in the Cloud, this setting should be deleted or commented out.

> **NOTE:**
>
> To comment this setting out, add a `#` directly before the setting. That is:
>
> ```
> #securityPolicyManager.port=8080
> ```

3. In the `securityPolicyManager.useSSL` field, keep the default value of `true` if iManage SPM Server has been configured for SSL, otherwise, enter `false.`
4. In the `securityPolicyManager.username` field, enter the iManage SPM server account that this iManage SPM Agent should use. By default, this is `SPMAGENT`.
5. You are prompted to provide a password during the installation process if `securityPolicyManager.encodedPassword` is left in its default state of `<passwordprompt>`. `<passwordprompt>` is recommended.

ACL Applier Settings

These are located in the [SQL_1] section.

1. SPM tracks security applied based on `uniqueAgentIdentifier`. In the `uniqueAgentIdentifier` field, enter a name/value that uniquely identifies the agent to SPM. iManage recommends that you choose a name that reflects the target system, so that multiple agents do not attempt to manage a single target system. This ensures that when the agent is upgraded/moved/replaced, the security does not get re-applied on to the target system unless deemed necessary by SPM Server.
2. `applysecurity.enabled` is set to `true`, by default. This field must be left unchanged.
3. In the `jdbcConnectionString` field, enter the database connection URL for the SPMAgentSecurity database. The URL is based on the authentication method used.
4. `acceptExternalUsers` is set to `true`, by default. This default setting implies that the 'External User' role in SPM is recognized by the target system, and hence prevents access of all users to open clients and matters, unless specifically included. It is recommended that the ACL Applier flag to enable external user support is left in the default `true` setting.
5. Optional parameters

   a. `dbSchema` is the database schema to use. Default is `dbo`.

   b. `dbTimeout` refers to the database connection timeout in seconds. Default is `600` seconds (10 minutes).

   c. `connectionPoolSize` refers to the maximum number of available database connections. Default is `2`.
6. In the **combineMatterAlias** field, enter **true** if the client identifier is prepended to the matter identifier in the target system, for example: "1080.1000". Setting this to true has the effect that "clientId.matterId" in

SPM will be applied to "clientId.clientId<separator>matterId" in the target system, with <separator> being the Installation (SQL Agent)#separ defined in the step below.

7. If you have set Installation (SQL Agent)#combi above to **true**, specify the **clientMatterSeparator** used between the client identifier and matter identifier (in the target system). This property is ignored if combineMatterAlias is false. The default is . and the supported values are . - + :

NOTE:

iManage SQL Agent logs can be found in the installation directory in the following files:

- `spm-agent-service-sql.out.log`
- `spm-agent-service-sql.err.log`
- `spm-agent-service-sql.wrapper.log`

Optional configuration for client ID and matter ID padding

If the client and matter IDs in SPM differ from those in the target system (that is, the system the agent will apply security to) by character padding, you can configure the agent to pad (and/or strip) the client and matter IDs to match the way they are named in the target system, in order to apply SPM security.

For example, if you have clientID.matterID **123.456** in SPM (and a source system importing client and matter definitions), but **000123.000456** for that clientID.matterID in the target system, you can configure the agent to pad the SPM client IDs and matter IDs with a "0" character, for a length of 6 characters each.

Conversely, if you have, for example, clientID.matterID **0456.0789** in SPM and clientID.matterID **456.789** in the target system, you can configure the agent to strip the SPM client IDs and matter IDs (of the "0" character), to give a length of 3 characters each, as in the target system.

To configure padding/stripping in the agent, **add** and set the relevant parameters, as described below, to the CFG file. You only need to specify the parameters that you will use; for example if you do not want to strip characters, or only want to pad client IDs, you can leave out the configuration related to stripping and matter IDs respectively.

These settings are fully compatible with the `combineMatterAlias` and `clientMatterSeparator` parameters.

1. **clientPaddingSize -** use this to specify the minimum size of the client ID in the target system, in characters.
   - When required, the agent will prefix the client ID with the configured client padding character to ensure the correct length. The default value is `0`.
   - If stripping is enabled, for example to remove padding applied in a source system that is not required in the target system, this value represents the minimum size of the client ID in the target system, below which stripping will not occur.
2. **matterPaddingSize** - use this to specify the minimum size of the matter ID in the target system, in characters.
   - When required, the agent will prefix the matter ID with the configured matter padding character to ensure the correct length. The default value is `0`.
   - If stripping is enabled, for example to remove padding applied in a source system that is not required in the target system, this value represents the minimum size of the matter ID in the target system, below which stripping will not occur.

3. **stripClientPaddingCharacters** - set this to `true` to strip padding characters from the client ID. The default value is false.
4. **stripMatterPaddingCharacters** - set this to `true` to strip padding characters from the matter ID. The default value is false.
5. **clientPaddingCharacter** - set the character used as padding for client IDs. The default is `0`.

   > **NOTE:**
   >
   > The character specified here is also the one considered for stripping, when stripping is enabled.

6. **matterPaddingCharacter** - set the character used as padding for matter IDs. The default is `0`.

   > **NOTE:**
   >
   > The character specified here is also the one considered for stripping, when stripping is enabled.

Example

To convert 345.123, per SPM, to 000345.00123, per target system, add these values to the CFG:

- `clientPaddingSize=6`
- `matterPaddingSize=5`

The default values imply padding with 0s, and no stripping.

Starting iManage SQL Agent for Security Policy Manager

After installation, the agent service should be started manually.

Starting the Service

1. Go to **Control Panel** > **All Control Panel Items** > **Administrative Tools** > **Services**.
2. Scroll down to the iManage SQL Agent.
3. Select **iManage SQL Agent**, and click **Start Service**.

Stopping the Service

If you wish to stop the agent service, perform the following steps:

1. Go to **Control Panel** > **All Control Panel Items** > **Administrative Tools** > **Services**.
2. Scroll down to the iManage SQL Agent.
3. Select **iManage SQL Agent**, and click **Stop Service**.

Upgrading

This section explains the process of upgrading the iManage SQL Agent for Security Policy Manager from version 1.3.x or later, to the current version.

Upgrade Steps

1. Stop the iManage SQL Agent for iManage Security Policy Manager service.
2. Open command prompt as a Windows Administrator.
3. Run the following command: `sc delete imanage-agent-SQL`, and press **Enter**.

   > **NOTE:**
   >
   > Note that if you are upgrading more than one agent, you have to run the command one time for each agent. In such case, replace '- `SQL` ' in the command above with one of ' `-Custom` ', ' `-Elite` ', ' `-Work` ', `'-HR','-Filesystem', '-IntappTime'`, and so on, as required.

4. Refresh Windows Services to confirm removal of the service.
5. Download the new agent installation package.
6. Make the necessary configuration changes in the `iManage SQL Agent.cfg` file. For more information about the configuration changes, see Installation.
7. Right-click `iManage SQL Agent Setup.cmd`, and select **Run as Administrator**.
8. Follow the instructions provided in the setup wizard. The iManage SQL Agent for iManage Security Policy Manager is now installed.