Security
Technical White Paper

March 2017

An integrated approach to insider threat mitigation and risk management

Detect, prevent and mitigate insider threats with a comprehensive solution from IBM

Highlights

- Extend privileged identity management with additional security controls to improve control and reduce security risks
- Govern privileged users and their access; monitor their activity and their access to sensitive data
- Protect enterprise data resources and enable timely detection of anomalous activity
- Address key privacy and regulatory mandates
- Facilitate implementation of a multi-disciplinary program to mitigate insider threats

Counter to the usual portrayal of computer security threats, the risks to your enterprise data don't all come from distant, shadowy intruders—or even from outside your firewall. Organizations rely on the actions and decisions made every day by users with legitimate authorization to access crucial systems, sometimes several of them. These privileged insiders' access to IT resources is critical, but it can be risky.

A 2016 report based on IBM® X-Force® security research found that 60 percent of vulnerabilities are actually linked to insiders,[1] rather than being purely the work of outside attackers. One reason for this sobering figure is that organizations very often apply appropriate, layered security measures to traffic that reaches their networks from the outside, or to data being uploaded from within the organization—but give lighter scrutiny to internal traffic and their own users. This means that, while malware and phishing attempts may be blocked, the privileged insiders with the greatest access aren't just trusted—they are essentially unsupervised.

Such a situation might have been acceptable decades ago or even now in very small organizations, but today's enterprise networks are unavoidably complex, and their legitimate users have a complicated mix of access needs. Some users also have heightened privileges, with access to a mix of resources that may cross departmental divisions or job-function lines. These privileged users may need to reach websites, offline records, remote data stores and applications. Insiders with elevated access to crucial data stores, in other words, can be just as big a threat as attackers from the outside.

Whether inadvertently or intentionally, privileged insiders can expose or damage crucial data, or infect systems with malware. Proactively managing their access to systems and keeping records to help roll back damage resulting from a breach or other data loss is essential.

An introduction to IBM Security Privileged Identity Manager

To counter the risks to data that trusted insiders pose, IBM Security Privileged Identity Manager centrally manages privileged access credentials across systems, applications and platforms. To reduce costs and provide faster time to value, the solution is available as a virtual appliance.

Centralizing credential access allows IBM Security Privileged Identity Manager to provide audit logs for later analysis. These core features—access control and audit-suitable logging—help address compliance, regulatory and privacy requirements that enterprises face.

Rather than relying on a patchwork of disparate access methods and tracing access only with after-the-fact log examination (if at all), security administrators can rely on IBM Security Privileged Identity Manager to coordinate and track access in real time. Its capabilities can also be extended through integration with existing enterprise security tools and with dedicated extensions.

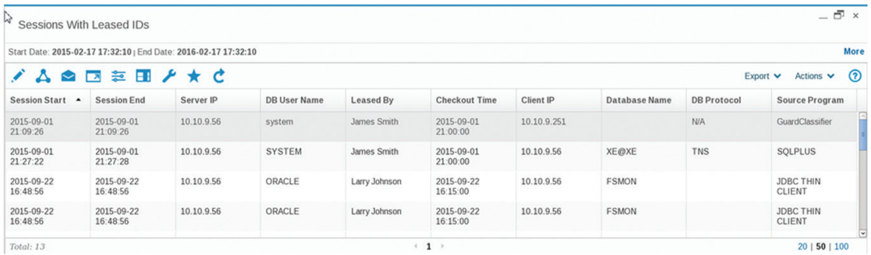
Besides the existing agent-based and manual credential access that IBM Security Privileged Identity Manager offers, the optional Privileged Session Gateway function supports agent-less access to shared credentials, providing users with greater flexibility in deploying the solution and in reducing the maintenance overhead of installing and maintaining the agents.

Another optional component, IBM Security Privileged Identity Manager for Applications, eliminates the use of hard-coded, clear text passwords in applications to help secure databases, applications and scripts. Privileged user endpoint activities can also be permanently recorded with a Privileged Session Recorder tool for improved visibility and security compliance.

The virtual appliance platform and extensibility of IBM Security Privileged Identity Manager make the solution simple to install and easy to manage, yet powerful.

Integration with IBM Security Guardium

IBM Security Privileged Identity Manager integrates smoothly with IBM Security Guardium®, which monitors and audits privileged user access to sensitive database objects, and which can send alerts or block access on unauthorized access. When the two solutions are operating in concert, Guardium offers protection for data and databases, and access and session audit logging, while IBM Security Privileged Identity Manager enables management of shared privileged accounts, enables users to check out and check in stored passwords, and tracks use of shared credentials.



Sessions With Leased IDs

Start Date: **2015-02-17 17:32:10** | End Date: **2016-02-17 17:32:10**

Session Start ▲	Session End	Server IP	DB User Name	Leased By	Checkout Time	Client IP	Database Name	DB Protocol	Source Program
2015-09-01 21:09:26	2015-09-01 21:09:26	10.10.9.56	system	James Smith	2015-09-01 21:00:00	10.10.9.251		N/A	GuardClassifier
2015-09-01 21:27:22	2015-09-01 21:27:28	10.10.9.56	SYSTEM	James Smith	2015-09-01 21:00:00	10.10.9.56	XE@XE	TNS	SQLPLUS
2015-09-22 16:48:56	2015-09-22 16:48:56	10.10.9.56	ORACLE	Larry Johnson	2015-09-22 16:15:00	10.10.9.56	FSMON		JDBC THIN CLIENT
2015-09-22 16:48:56	2015-09-22 16:48:56	10.10.9.56	ORACLE	Larry Johnson	2015-09-22 16:15:00	10.10.9.56	FSMON		JDBC THIN CLIENT

Total: 13

Guardium report showing the privileged activity sessions initiated using shared IDs with real user names received from IBM Security Privileged Identity Manager.

When these two solutions are integrated, IBM Security Privileged Identity Manager shares check-in / check-out audit records and Guardium cross references information with its auditing of data access activity. Integration with Guardium provides the Guardium platform with visibility into data, including credentials and leased IDs, stored by IBM Security Privileged Identity Manager.

Guardium session logs can be correlated with IBM Security Privileged Identity Manager check-out activity logs, allowing Guardium to display a consolidated view of user activity and database access. This enables security administrators to track individual users' access to sensitive data even when individuals are using commonly employed (and commonly shared) account names to identify privileged user accounts, such as "Administrator," "SA" or "admin."

Use-case scenario:

When user Jennifer Lee logs into a database containing sensitive records regarding an ongoing business proposal, she does so using an administrator account, called "Admin," to which she and several others have access. When security administrators suspect that some of these records have been leaked to a competitor, they seek to discover who accessed these records, and when. They can correlate the times that the Admin account has been used to access the database with the times individual users such as Jennifer checked out the credentials to use that account.

Solution deployment overview

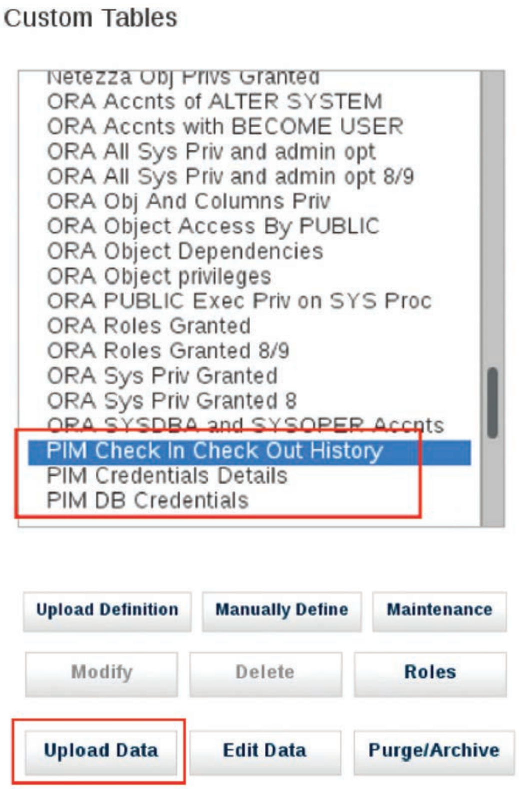
Integrating Guardium with IBM Security Privileged Identity Manager is a simple four-step process:

1. Add the IBM Security Privileged Identity Manager database to Guardium, using the Datasource Definitions tool.

2. Upload IBM Security Privileged Identity Manager data, using the Custom Tables tool. Three tables (IBM Security Privileged Identity Manager Check-in / Check-out History, IBM Security Privileged Identity Manager Credentials Details and IBM Security Privileged Identity Manager DB Credentials) need to be uploaded. Because the information contained in these tables will be updated over time, it is highly recommended that administrators schedule regular uploads for all three of these tables.

3. Correlate the uploaded data by running the IBM Security Privileged Identity Manager Data Correlation tool (added to Guardium). This will examine the data that has been uploaded into the IBM Security Privileged Identity Manager Custom Tables and reconcile that data with the Guardium session logs, saving the results in a database. This job can be manually executed or automated.

4. Create a custom report that includes IBM Security Privileged Identity Manager fields to display the correlated information. This report is the goal of the integration, and gives fine-grained insight into data access history, by user and by resource.



Custom table creation is an integral step in correlating data between IBM Security Privileged Identity Manager and Guardium.

Integration with IBM QRadar

IBM Security Privileged Identity Manager can be integrated with IBM QRadar® Security Intelligence Platform to take advantage of a two-way information flow between the two solutions. QRadar analyzes both IBM Security Privileged Identity Manager credentials and Guardium activities to detect anomalies and trigger targeted alerts so administrators can take corrective action.

With this combination, it is possible to suspend access for specific IBM Security Privileged Identity Manager users, or to suspend all shared credentials associated with a shared resource, automatically and nearly in real time, in response to security intelligence events from QRadar.

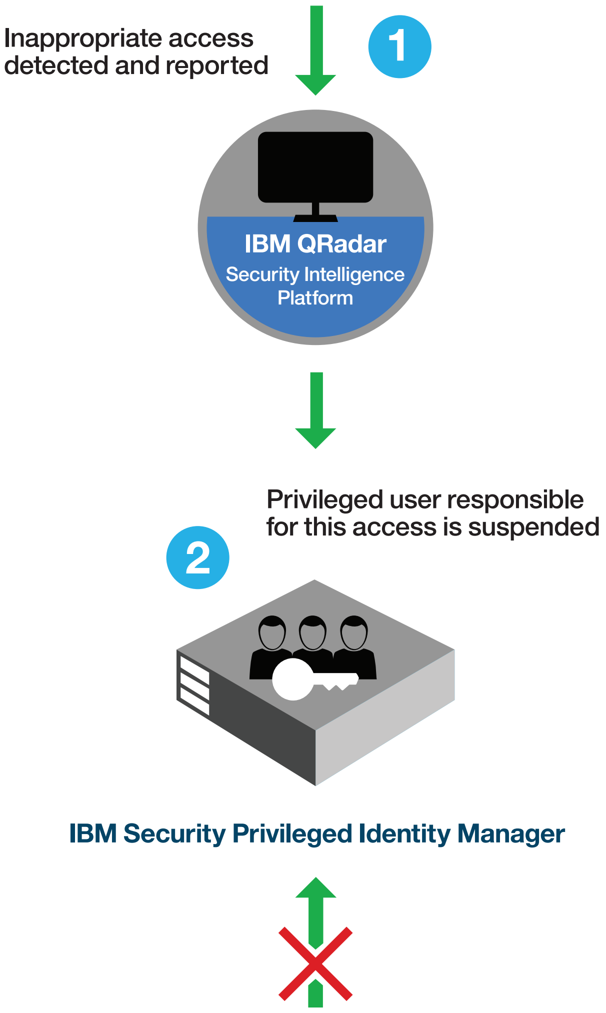
When QRadar identifies a suspicious action, it forwards an event notification to a connector tool, called QRPIM. Events from QRadar are tied to actions in QRPIM through event-action rules. QRPIM uses the details associated with the forwarded event notification to identify either the resource or the user to suspend, based on a pre-populated event-action rules file which pairs anticipated security events to appropriate actions.

Use-case scenario 1: Suspending a resource

QRadar identifies anomalous access to a server containing sensitive information and issues a security alert. QRadar forwards that alert to IBM Security Privileged Identity Manager, which then suspends credential check-out for this resource for further investigation. Endpoints that have been blocked can be reinstated at administrator discretion when the underlying security concern has been addressed.

Use-case scenario 2: Suspending a user

QRadar identifies that user Jason Jones started to access certain servers and databases more frequently and outside of his working hours. This inappropriate access triggers QRadar to send an alert to IBM Security Privileged Identity Manager, which can temporarily suspend or revoke this user's access to these resources for further investigation. The incident response team will review session recordings captured for this user and the resources in question to determine what activities were performed on these resources.


Inappropriate access detected and reported
1
IBM QRadar
Security Intelligence Platform
Privileged user responsible for this access is suspended
2
IBM Security Privileged Identity Manager

IBM Security Privileged Identity Manager and QRadar work together to identify and act when credentials must be revoked for better security.

QRadar can link IBM Security Privileged Identity Manager event data with events from protected systems. On spotting suspicious activity of "root" on a sensitive server, QRadar can tie it to IBM Security Privileged Identity Manager user "james," notify James' manager, and (via QRPIM) suspend his account. And QRadar admins can correlate security incidents involving shared credentials with IBM Security Privileged Identity Manager or AccessAgent check-out events, then (with the Privileged Session Recorder console) actually watch a recording of sessions where the credentials were used.

Solution deployment overview

When QRadar detects a relevant anomaly, QRadar Event Rule dispatches JSON alerts via TCP to a designated forwarding address monitored by QRPIM.

QRPIM receives and parses the event data, then dispatches it to a highly configurable, extremely compact workflow (also known as a “microflow”) describing the action to be taken based on the details of QRadar alerts received. These microflows invoke IBM Security Privileged Identity Manager REST calls to suspend a resource or a user. Microflows can easily be customized, extended or created from scratch using simple editing tools. Integrating QRadar with IBM Security Privileged Identity Manager requires five steps:

1. Ensure that resources are well-defined, so they can be correlated with event data.

2. Secure credentials to the IBM Security Privileged Identity Manager REST API, sufficient to modify credentials, access privileges and users, and to read resources.

3. Within QRadar, configure a forwarding destination (using JSON over TCP to the IBM Security Privileged Identity Manager solution), and define event rules that dispatch events to the forwarding destination.

4. Install IBM Security Directory Integrator, then copy the solution files (4 text files). Configure the eventAction.rules file to assign actions to QRadar events.

5. Activate the integration by navigating to the IBM Security Directory Integrator installation directory (in Linux/UNIX or Microsoft Windows) and executing the command *ibmdisrv –c configs/QRTrigger.xml –d*

Integration with IBM Security Identity Governance and Intelligence

IBM Security Identity Governance and Intelligence is an identity governance platform that lets IT managers and business owners set policies to manage access and ensure regulatory compliance. This solution provides enterprises with capabilities for end-to-end user lifecycle management, including intelligence-driven access risk assessment and mitigation using business-driven identity governance and workflows to coordinate repeated management tasks.

It features user lifecycle management tools for provisioning, modifying and deprovisioning accounts, along with capabilities to consolidate access entitlements from target applications and employ sophisticated algorithms for role mining, modeling and optimization.

IBM Security Identity Governance and Intelligence relies on the notion that users have particular duties based on their job functions, and that access to data resources should be based on each user’s actual needs. It checks for segregation-of-duties violations across enterprise applications, including SAP, and coordinates certification and recertification campaigns to ensure the validity of privileged access rights.

The solution’s flexible architecture allows for coordination with both IBM and third-party tools, and lets administrators take advantage of integration with IBM Security Privileged Identity Manager. With the IBM Security Directory Integrator-based IBM Security Privileged Identity Manager adapter, an administrator can bulk load privileged users’ access entitlements into IBM Security Identity Governance and Intelligence.

By integrating IBM Security Identity Governance and Intelligence with IBM Security Privileged Identity Manager, security administrators can reconcile users and access entitlements, and selectively assign and revoke user access based on policy.

In coordination with IBM Security Privileged Identity Manager, this solution can correlate current permissions and roles with actual business needs as they evolve, for IT planning, security and regulatory compliance purposes. It enables visibility and sophisticated user access control by consolidating access entitlements from target applications, and through the use of sophisticated algorithms for role mining, modeling and optimization.

Use-case scenario

XYZ Corporation has a list of employees with elevated access rights and privileged access to servers or databases. Periodically, the managers of XYZ augment and review this list with the aid of IBM Security Privileged Identity Manager, to assure that these users still need these elevated privileges and these privileges are properly assigned. To execute such a recertification campaign, IT personnel use the capabilities of both IBM Security Privileged Identity Manager and IBM Security Identity Governance and Intelligence solutions. A list of privileged users and their access permissions is imported into IBM Security Identity Governance and Intelligence, and these permissions are reconciled with the existing users in the system and their access privileges. Then the recertification campaign is configured and launched to certify these elevated privileges for these users.

A reviewer, having received an email notice about the new campaign, logs into the IBM Security Identity Governance and Intelligence Service Center. She sees that she has been assigned a recertification task, and proceeds to review the items presented. Noticing that an employee has two access entitlements assigned, one of which is no longer necessary, she proceeds to approve one and revoke the other.

She can skip individual reviews as needed, while continuing to process and review others, and can examine the approval history for any item if needed.

Next, the campaign supervisor logs into the IBM Security Identity Governance and Intelligence Service Center to check on the progress of the campaign, where he can check on the progress both for the users and for the reviewers, until the campaign is complete.

Deployment overview

IBM Security Identity Governance and Intelligence provides identity management and advanced user-permission auditing capabilities. IBM Security Privileged Identity Manager essentially manages shared privileged user accounts, allowing clients to audit actual usage of shared privileged credentials such as root, admin or domain administrator. Audit accuracy is achieved by storing shared-account passwords in a credential vault that requires a checkout process before using a shared credential.

This integration is made possible by an identity adapter that allows comprehensive two-way reconciliation between the IBM Security Privileged Identity Manager and IBM Security Identity Governance and Intelligence platforms. This adapter allows IBM Security Identity Governance and Intelligence to audit IBM Security Privileged Identity Manager user-access permissions, and allows users to request new access to (or recertification for) IBM Security Privileged Identity Manager using IBM Security Identity Governance and Intelligence workflows. Supervisors can also revoke user's access to IBM Security Privileged Identity Manager credentials using IBM Security Identity Governance and Intelligence tools.

Prerequisites

To get started, you should have working deployments of IBM Security Identity Governance and Intelligence and IBM Security Privileged Identity Manager, and you should have enabled Identity Brokerage Providers in IBM Security Identity Governance and Intelligence. Download the following files:

- IBM Security Identity Governance and Intelligence Adapter v7.1.1 for IBM Privileged Identity Manager 2.1, Multiplatform, Multilingual (CNH0AML)
- IBM Security Identity Adapter RMI Dispatcher v7.1.36 for Tivoli Directory Integrator v7.x, Multiplatform, Multilingual (CNH08ML)
- httpclient-4.0.1.jar

For more information regarding the use of this identity adapter, refer to the "SDI-based IBM Security Privileged Identity Manager adapter Installation and Configuration Guide" (available in HTML or PDF format via a simple online search for this title).

Integration configuration

The first step of this integration is to export the Local Management Interface (LMI) certificate from IBM Security Privileged Identity Manager. Since the adapter is installed to IBM Security Identity Governance and Intelligence, the LMI SSL certificate is required for the adapter to establish a secure connection to the IBM Security Privileged Identity Manager platform. Steps 2 through 4 will get the adapter installed and configured. Once Step 4 is complete, reconciliation will be working between IBM Security Privileged Identity Manager and IBM Security Identity Governance and Intelligence. At this point, experienced IBM Security Identity Governance and Intelligence administrators will be up and running and the rest of the guide is unnecessary. Later steps demonstrate the capabilities of the integration adapter and give some basic guidance regarding IBM Security Identity Governance and Intelligence and adapter functionality.

Step 1: Export the LMI Certificate from IBM Security Privileged Identity Manager

Using Microsoft Internet Explorer:

See page 9 in the "SDI-based IBM Security Privileged Identity Manager adapter Installation and Configuration Guide" (available in HTML or PDF format via a simple online search for this title).

Using Mozilla Firefox:

1. Browse to the IBM Security Privileged Identity Manager LMI in Firefox.
2. Click SSL Lock icon (to the left of the address bar), and choose **More Information...**
3. Click the **View Certificate** button, and select the **Details** tab.
4. In the Certificate Hierarchy box, select the hostname of your IBM Security Privileged Identity Manager appliance, then click **Export...**
5. Choose file type: **X.509 Certificate (PEM)**; name the file **IBM Security Privileged Identity Manager.cer**, then click **Save**.

Using Google Chrome:

1. Browse to the IBM Security Privileged Identity Manager LMI in Firefox.
2. With the IBM Security Privileged Identity Manager LMI as the active Window, press **Control+Shift+I** to open the **Developer Tools** pane.
3. Select the **Security** tab in the **Developer Tools** pane.
4. Click the **View certificate** button, then select the **Details** tab.
5. In the Certificate Hierarchy box, select the hostname of your IBM Security Privileged Identity Manager appliance, then click **Export...**
6. Choose filter: **DER/PEM/Netscape-encoded X.509 certificate** and name the file **IBM Security Privileged Identity Manager.cer**, then click **Save**.

Step 2: Install the IBM Security Privileged Identity Manager Adapter

1. Extract Adapter ZIP file locally.
2. Connect to IBM Security Identity Governance and Intelligence LMI.
3. Browse to **Configure** > **SDI Management**; Select **SDI1** and choose **Manage** > **SDI Adapters**.
4. Click **Install** in the toolbar, browse to the adapter zipfile and click **OK**.
5. When prompted for Prerequisite files, click the **Select Files** button and browse to the previously downloaded copy of **httpclient-4.0.1.jar** and click **OK**.
6. Click the **Close** button to leave the **SDI Adapters** window.
7. Ensure SDI1 is still selected and click **Edit** in the toolbar.
8. Check **Enable SSL** and click **Save Configuration**.
9. While SDI1 is still selected, choose **Manage** > **Certificates** from the toolbar.
10. Select the **Signer** tab and click **Upload** in the toolbar.
11. Browse to the **IBM Security Privileged Identity Manager.cer** file that was exported in the previous section and click **Open**.
12. Set the Label to IBM Security Privileged Identity Manager and click Save.
13. Wait about 20 seconds for the certificate list to refresh; confirm that the IBM Security Privileged Identity Manager certificate was added to the list.
14. Again, browse to **Configure** > **SDI Management**.
15. Select **SDI1** and click **Restart** in the toolbar; you should see **True** in the **Changes are Active** column.

Step 3: Create a service account in IBM Security Privileged Identity Manager for the IBM Security Identity Governance and Intelligence adapter to use

1. Connect to the **Identity and Credential Vault Administration** tool using the IBM Security Privileged Identity Manager **manager user**. This page can be found in the **Quick Links** pane on the IBM Security Privileged Identity Manager **Home** section.
2. Once authenticated, click the **Manage Users** link in the left pane.
3. Click the **Refresh** button, then click the **Create** button.
4. In the **Create User** tool, choose an appropriate Business Unit for this service account and click **Continue**.
5. For Last Name, use **IGI Service Account**. For Full Name and Preferred User ID, use **igiadmin**, then click **Continue**.
6. Select **Allow me to type a password**, enter a new password for the igiadmin account, then click **Submit**.
7. Click the **Manage Groups** link in the left pane, then click the **Refresh** button to get a list of groups.
8. Click the arrow icon by the System Administrator group and select **Add Members**.
9. Click the **Search** button.

10. Select the **igiadmin** user that was previously created; click **OK**, then **Submit**, then **Close**.

11. Browse to **View Requests** > **View All Requests** and click the **Refresh** button to confirm that the new account was created without errors.

Step 4: Create the IBM Security Privileged Identity Manager target in IBM Security Identity Governance and Intelligence

1. Connect to the **IGI Administration Console** as the admin user.

2. Select the **Target Administration** category.

3. Click the **Manage Target Types** link in the pane on the left, then click the **Browse** button.

4. Browse to the folder where the SDI Adapter was previously extracted. In this folder, choose **ISPIMProfile.jar** and click **Open**, then click the **OK** button.

5. Click the **Manage Target** Types link.

6. Click the arrow icon at ISPIM Profile and select **Attribute Mapping. Note:** If ISPIMProfile does not exist in the list, wait a few minutes, then click Refresh. Click the **Browse** button.

7. Select the **ISPIMProfileMapping.def** and click the **Open** button; click **OK**, then **Close**.

8. Click the **Manage Targets** link on the left.

9. Click the **Refresh** button, then click the **Create** button.

10. Select **ISPIM Profile** and click **Next**.

11. Service Name should be ISPIM, and server URL should be https://ispim_ip_or_hostname

12. Tivoli Directory Integrator Location **rmi://localhost:1099/ITDIDispatcher**.

13. Click the **Next** button.

14. Enter the details for the **igiadmin** account that was created in IBM Security Privileged Identity Manager in the previous section of this guide.

15. Click **Test Connection** button and wait for the test to complete, then click the **Next** button.

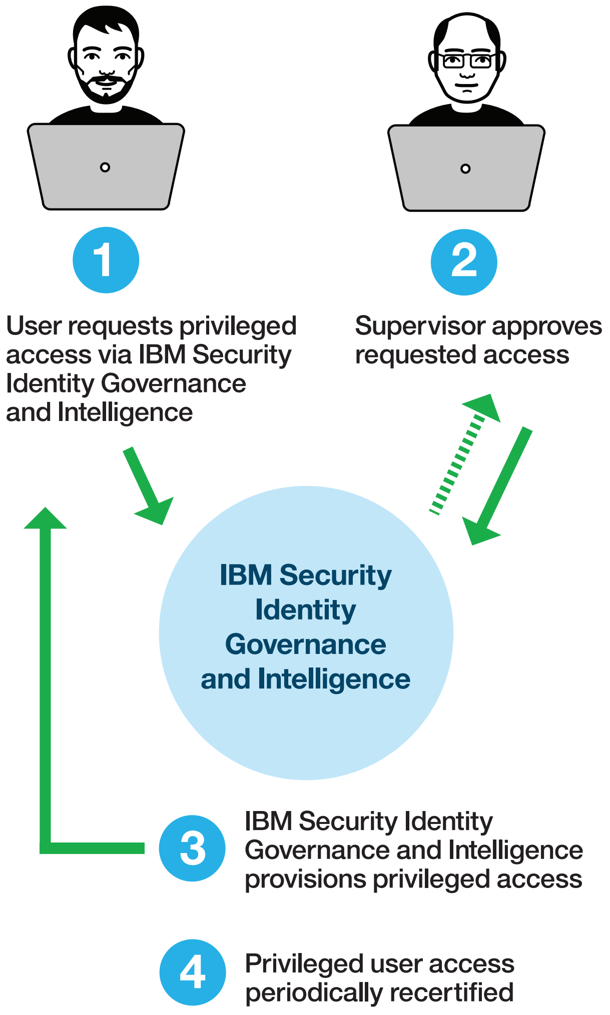
16. Application Name should be **ISPIM**.

17. Click **Finish**, and then **Close**.

18. In the Manage Targets pane, click **Refresh**, then click the arrow icon by the new ISPIM Target.

19. Choose **Reconcile Now**, then verify that reconciliation is successful.

Following initial reconciliation, review orphaned accounts and match them to existing IBM Security Identity Governance and Intelligence users if necessary. This process is the same by any adapter. (https://www.ibm.com/support/knowledgecenter/en/SSGHJR_5.2.2/com.ibm.igi.doc/CrossIdeas_Topics/ACCM/Introduction_to_Account_Matching.html)


1
User requests privileged access via IBM Security Identity Governance and Intelligence
2
Supervisor approves requested access
IBM Security Identity Governance and Intelligence
3
IBM Security Identity Governance and Intelligence provisions privileged access
4
Privileged user access periodically recertified

IBM Security Identity Governance and Intelligence enables an efficient, user-friendly system for requesting and granting privileged access to the users who need it.

Deep integration for deeper security

Any one of the integrations described above can give security personnel increased visibility into the workings of the data environment they are responsible for managing and protecting. However, more complex integrations can extend the advantages even further. A system equipped with all four of these technologies—IBM Security Privileged Identity Manager, Guardium, QRadar and IBM Security Identity Governance and Intelligence—can form a coherent authorization, tracking and auditing system. Such a system can amplify the strength of each tool and simplify authorization, tracking, audit-ready logging and forensic investigation in the event of a breach.

A holistic multi-disciplinary approach is needed

Security controls are only one aspect of a comprehensive multi-disciplinary approach to insider threat mitigation. An enterprise-level program should also implement corporate policies and processes to detect and respond to insider threats to limit the risks associated with them. Such a program should include, in addition to cybersecurity experts, risk managers, IT leaders and representatives from individual departments as well as human resources.

IBM recommends that such a program should include the following components:

1. Polices to govern privileged access and manage security risks (including insider risk)

2. Department-level collection of insider-risk data and aggregation of this data on the corporate level

3. A working committee responsible for education and implementation of insider threat programs in each department

4. Standardized processes to review threat intelligence and identify internal risks

5. A corporate insider-threat awareness employee training program

6. Oversight of employee access lifecycle in the organization, including on-boarding, off-boarding, individual access risk assessment and background checks

Today's organizations must govern and enforce user access across multiple channels, including mobile, social and cloud. At the same time, they must address business needs such as role management, compliance and audit reporting, and the integration of various user populations, both external and internal.

IBM Security identity and access management solutions help strengthen compliance and reduce risk by protecting and monitoring user access in today's multi-perimeter environments.

For more information

To learn more about IBM Privileged Identity Manager, please contact your IBM representative or IBM Business Partner, or visit http://www-03.ibm.com/software/products/en/pim

Additionally, IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. We provide full lifecycle management of IT products and services, from acquisition to disposition. For more information, visit: **ibm.com**/financing

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 lawful, 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.

IBM Corporation
IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
March 2017

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

♻ Please Recycle

[1] "2016 Cyber Security Intelligence Index," *IBM X-Force Research*, April 2016. http://www-03.ibm.com/security/data-breach/cyber-security-index.html