



Syssero[®] Solution Packet

Personal Information Changes Post Security Alert



Solution Overview

Solution Overview

We conducted a comprehensive security audit to evaluate activity within an employee's account. Given the significant volume of personal changes, the audit also served to verify that no unauthorized modifications occurred.

Audit Process

A series of detailed reports and dashboards were utilized to scrutinize the employee's account activity.

1. User Activity

This report details every action taken by a specific user over a set date range. It logs the request time, the IP address used, and the type of action (READ, WRITE). In some cases, it even includes a link to the associated Workday event or object.

View User Activity [X]

From Moment * 01/17/2025 11:14:02 AM

To Moment * 01/20/2025 11:14:02 AM

System Accounts [Hernandez]

Tasks []

Cancel OK



View User Activity ... 01/19/2025

From Moment 01/17/2025 11:14:02.000 AM System Accounts [REDACTED]

To Moment 01/20/2025 11:14:02.000 AM

2583 items

Request Time	System Account	IP Address	User Agent	Task	Target	Activity Category
01/19/2025 01:03:31.274 PM	[REDACTED]	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/121.0.2277.128	Change My Personal Information	Personal Information Change:	WRITE
01/19/2025 01:06:32.394 PM	[REDACTED]	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/121.0.2277.128	Search in Main Page (Web Service)		READ
01/19/2025 01:06:32.616 PM	[REDACTED]	[REDACTED]	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/121.0.2277.128	Change My Personal Information	Personal Information Change:	WRITE

2. Sign-ons and Attempted Sign-ons

This report details every sign-on attempt for a given Workday account. It aids in diagnosing issues such as incorrect passwords or authentication policy errors and can highlight any suspicious activity from unfamiliar IP addresses.

Signons and Attempted Signons 01/17/2025 10:10

From Moment 01/17/2025 11:17:56.000 AM

To Moment 01/20/2025 11:17:56.000 AM

Select Workday Accounts [REDACTED]

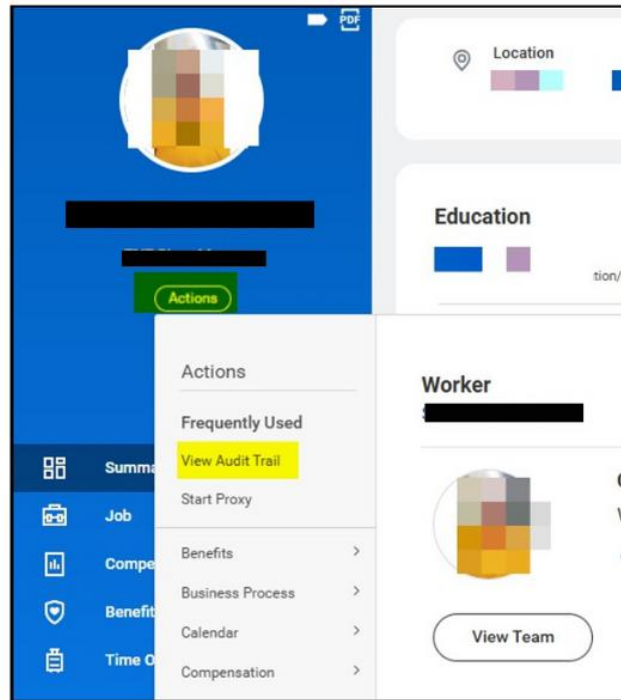
Signons 13 items

Signon	Session Start	Workday Account	Session End	Active Session	Device Type	Authentication Type for Signon	SAML Identity Provider	Authentication Channel
Q	01/19/2025 08:15:58 AM	[REDACTED]	01/19/2025 10:06:40 AM		Desktop	SAML	Azure PROD SSO	UI
Q	01/19/2025 06:08:27 AM	[REDACTED]	01/19/2025 07:39:41 AM			Trusted		Web Services
Q	01/18/2025 05:14:13 PM	[REDACTED]	01/18/2025 06:44:13 PM			Trusted		Web Services
Q	01/18/2025 01:53:39 PM	[REDACTED]	01/18/2025 03:27:23 PM		Phone	Mobile PIN		UI
Q	01/18/2025 01:52:57 PM	[REDACTED]	01/18/2025 03:22:57 PM			Trusted		Web Services



3. Audit Trail

Every object in Workday is auditable, allowing you to easily track who made changes and when. To get to the audit trail, go to the object's related actions:



Transaction	Entered On	Effective Date	Attribute	User Language	New Value	Prior Value	Changed Relationship	Added	Removed	By User
01/20/2023, 7:57:45 6911 AM CST	01/20/2023, 07:57:45 6911 AM						Event Target for Event	Time Ent. [REDACTED] 59 833034 hours from 01/11/2023 to 01/18/2023		[REDACTED]
							Worker subject of Worker Event	Time Ent. [REDACTED] 59 833034 hours from 01/11/2023 to 01/18/2023		
01/19/2023, 1:52:02 035 PM CST	01/19/2023, 01:52:02 035 PM						Worker subject of Worker Event	Personal Information Chang (United States of America) [REDACTED]	Personal Information Chang (United States of America) [REDACTED]	[REDACTED]
01/19/2023, 1:49:20 973 PM CST	01/19/2023, 01:49:20 973 PM						Worker subject of Worker Event	Personal Information Chang (United States of America) [REDACTED]	Personal Information Chang (United States of America) [REDACTED]	[REDACTED]
01/19/2023, 1:45:59 904 PM CST	01/19/2023, 01:45:59 904 PM						Worker subject of Worker Event	Personal Information Chang (United States of America) [REDACTED]	Personal Information Chang (United States of America) [REDACTED]	[REDACTED]



4. Worker History

A worker's Worker History tab displays every business process associated with that worker. This dashboard provides details on each process, including its effective date, completion date, and current status—whether it was successfully completed, rescinded, canceled, or is still in progress. You can also click into any business process event to view additional details if needed.

Business Process	Effective Date	Initiated On	Due Date	Completed On	Status
Payment Election [redacted] on 01/19/2025	01/19/2025	01/19/2025 08:36:02 AM	01/20/2025	01/19/2025 08:36:02 AM	Successfully Completed
Payment Election [redacted] on 01/18/2025	01/18/2025	01/18/2025 01:52:46 PM	01/19/2025	01/18/2025 01:52:46 PM	Successfully Completed
Payment Election [redacted] on 01/17/2025	01/17/2025	01/17/2025 09:42:58 AM	01/18/2025	01/17/2025 09:42:58 AM	Successfully Completed
Team Member Handbook-Sandra [redacted]		01/13/2025 09:21:23 AM	01/15/2025	01/13/2025 04:21:58 PM	Successfully Completed
Convenience Store, Kitchen, & Mitchs		01/13/2025 02:57:09	01/15/2025	01/13/2025 03:31:06	Successfully Completed

These steps are critical for maintaining the security and integrity of your Workday environment. In summary:

- **Security Assurance:** Auditing user activity and object changes helps verify that only authorized modifications are made, reducing the risk of data breaches or malicious activity.
 - **Issue Diagnosis:** Detailed reports on sign-on attempts and business processes assist in quickly identifying and resolving technical issues, such as authentication errors or system misconfigurations.
 - **Accountability and Transparency:** By tracking who made which changes and when, these processes establish clear accountability, which is essential for both compliance and internal governance.
 - **Operational Insight:** The comprehensive view provided by tools like the Worker History tab ensures that all business processes are tracked and understood, enabling proactive management and troubleshooting of any anomalies.
- Overall, these steps create a robust framework for monitoring system activity, safeguarding sensitive data, and ensuring smooth operations.

