TECH BRIEF

Integration with Change Management Systems

Safeguard for Privileged Sessions Use Case

The Challenge

Today, many enterprises use ticketing or issue tracking systems to automate change management processes in IT infrastructures. Regardless if it's a planned server maintenance, a system upgrade, or an unplanned network outage, a typical change management workflow is as follows:

- The IT operator submits a change management request by specifying the details of the issue (description of the issue, proposed resolution, planned maintenance window, etc.)
- The authorizer approves (or rejects) the change management request
- In case of approval, a change management ticket is issued for the operator, who does the job on the problematic system and closes the ticket.

Monitoring the work of operators is a great challenge in ticketing systems, however. As ticketing systems are not enforcement points, they aren't capable of controlling the real activities of operators in IT systems. Without using an activity monitoring solution, you can't verify:

- If the task was successfully completed or not
- If the task was completed in the requested maintenance window, or some other time
- Who performed the actual work
- The quality of the work done

Change management is often associated with ITIL, a set of practices for IT service management that focuses on aligning IT services with the needs of business. Among others, ITIL recommends best practices for IT operation management, configuration management, incident management, root cause analysis and identity management. One Identity Safeguard for Privileged Sessions provides a best-of-breed activity monitoring solution which helps enterprises comply with the above ITIL requirements

Learn more

- Safeguard homepage
- Request callback

Currently, Safeguard for Privileged Sessions offers plugin support for: **BMC Remedy** and **ServiceNow**.

(To request a plugin that interoperates with your ticketing system, contact the One Identity Support Team.)

The Solution

Safeguard for Privileged Sessions is an activity monitoring appliance that controls privileged access to remote IT systems, records activities in searchable movie-like audit trails, and prevents malicious actions. Safeguard for Privileged Sessions is a quickly deployable enterprise tool with the widest platform coverage on the market. It's completely independent from clients and servers - integrating seamlessly into existing infrastructures.

Safeguard for Privileged Sessions provides a plugin framework to integrate with external ticketing (or issue tracking) systems, allowing you to request a ticket ID from the operator before authenticating on the target server. That way, Safeguard for Privileged Sessions can verify that the user has a valid reason to access the server — and optionally terminate the connection if they don't.

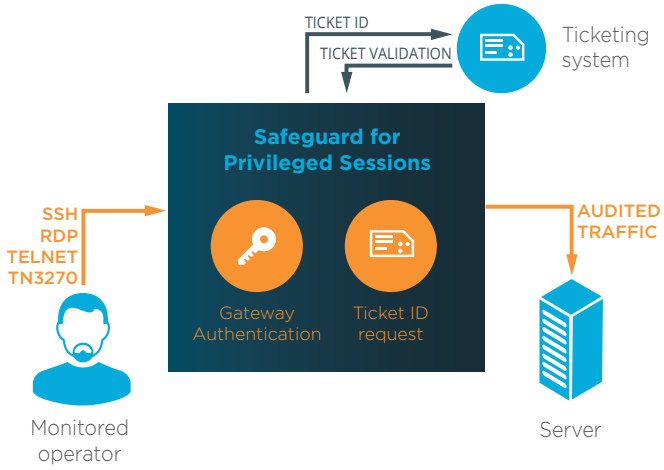
- Safeguard for Privileged Sessions can also enforce strong authentication which is completely independent from the authentication that the operator performs on the remote server.
- To avoid accidental misconfiguration and other human errors, Safeguard for Privileged Sessions supports the 4-eyes authorization principle: the authorizer can allow/deny, track, and instantly terminate the operator's access to the server.
- Safeguard for Privileged Sessions monitors operator's activity in real-time and detects anomalies as they occur. Upon detection of a suspicious user action (for example, entering a destructive command, such as "delete"), Safeguard for Privileged Sessions can send you an alert or immediately terminate the connection.
- Safeguard for Privileged Sessions records all working sessions into searchable audit trails, making it easy to find relevant information in forensics or troubleshooting situations. This way, you can conduct fast post-mortem analysis of operators' activities.

Benefits

Integrating Safeguard for Privileged Sessions with change management systems can provide

- Granular access control for operators to enforce company policies
- Real-time monitoring of sessions to mitigate the risk of human errors (or cyber-attacks)
- Tamper-proof auditing of sessions to provide strong evidence in legal proceedings
- Quick ROI – IT troubleshooting and forensics investigations in minutes instead of days
- Activity reporting to meet compliance requirements

Safeguard for Privileged Sessions has a flexible plugin framework to integrate with any custom-built or commercial ticketing systems. You can even use multiple plugins. So, for example, if system operators use one ticketing system and another department uses a different one, you can have plugins for both, even if the two departments access the same servers.



Safeguard for Privileged Sessions integration with Ticketing System

About One Identity

One Identity helps organizations get identity and access management (IAM) right. With our unique combination of offerings, including a portfolio of identity governance, access management, privileged management and identity as a service solutions, organizations can achieve their full potential – unimpeded by security, yet safeguarded against threats. Learn more at OneIdentity.com