DATASHEET

One Identity Safeguard for Privileged Passwords

Take the risk out of shared privileged credentials

Benefits

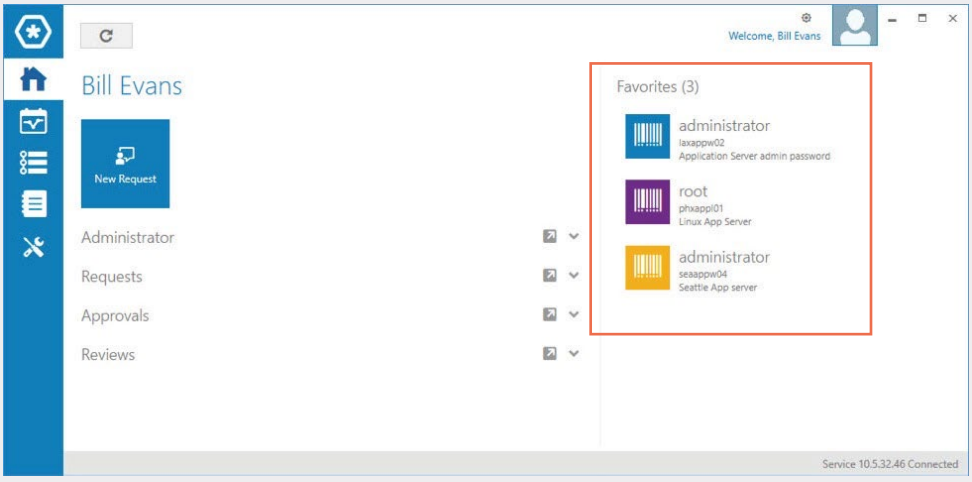
- Mitigate the damage of a security breach by controlling access to privilege accounts
- Easily meet compliance requirements for privileged accounts
- Get value faster with simplified deployment and ongoing management
- Maximize productivity with a small learning curve and elegant UI design
- Simplified and faster audit report creation

Introduction

Time and time again, recent incidents have shown that the most vulnerable – and potentially the most devastating – element of systems security is privileged account passwords. These passwords are the keys to the kingdom. Once hackers obtain them, they have unlimited access to your systems and data. And, as you've seen, the cost to an impacted organization's reputation and lost intellectual property can be immense.

Traditionally, securing privileged credentials has created friction and slowed productivity for both daily and long-term operations. This conundrum often puts IT managers and security officers in the unfortunate position of weighing security against ease of use. Until now. With One Identity Safeguard for Privileged Passwords, you can have both.

One Identity Safeguard for Privileged Passwords automates, controls and secures the process of granting privileged credentials with role- based access management and automated work flows. It can be deployed as a hardened appliance, which eliminates concerns about securing access to the solution itself. This also helps to acellerate integration with your systems and IT strategies. Plus, its usercentered design means a small learning curve and the ability to manage passwords from anywhere and using nearly any device. The result is a solution that secures your enterprise and enables your privileged users with a new level of freedom and functionality.



Quick access to your passwords

Favorites enable you to quickly access the passwords that you use the most right from the login screen.

Features

Release control

Manages password requests from authorized users for the accounts they are entitled to access via a secure web browser connection with support for mobile devices.

Workflow Engine

A work low engine that supports time restrictions, reviewers, multiple approvers, emergency access, and expiration of policy. It also includes the ability to input reason codes and/or integrate directly with ticketing systems. A password request can be automatically approved or require multiple levels of approvals.

Discovery

Quickly discover any privileged account or system on your network with host, directory and network-discovery options.

Approval Anywhere

Leveraging One Identity Starling, you can approve or deny any request anywhere without being on the VPN.

Favorites

Quickly access the passwords that you use the most right from the login screen.

Always online

You get true high availability as this solution was built for distributed clustering. Plus, with load balancing capabilities, you get faster throughput and shorter response times as you request passwords and sessions from any appliance.

RESTful API

Safeguard uses a modernized API based on REST to connect with other applications and systems. Every function is exposed through the API to enable quick and easy integration regardless of what want to do or which language your applications are written.

Activity Center

You can quickly and easily view all activity with a query builder. Depending on who requested a report — such as IT operations or executives — you can add and remove data to get the information you need. In addition, you can schedule queries, and save or export the data in a variety of formats.

Two-factor authentication support

Protecting access to passwords with another password isn't enough. Enhance security by requiring two-factor authentication to Safeguard. Safeguard supports any RADIUS-based 2FA solution and includes unlimited two-factor authentication with the One Identity Hybrid Subscription.

One Identity Hybrid Subscription

Expand the capabilities of Safeguard with the One Identity Hybrid Subscription, which offers immediate access to cloud delivered features and services. These include all-you-can eat Starling Two-Factor Authentication to protect Safeguard access and Starling Access Certification for Safeguard to certify privileged access rights and ensure compliance. A single subscription enables all One Identity solution deployments

Smartcard support

Use your strong authentication methods to keep access to your vault buttoned down.

The One Identity approach to privileged access management

The One Identity portfolio includes the industry's most comprehensive set of privileged access management solutions. You can build on the capabilities of One Identity Safeguard withsolutions for granular delegation of the UNIX root account and the Active Directory administrator account; add-ons to make open source sudo enterprise-ready; and keystroke logging for UNIX root activities – all tightly integrated with the industry's leading Active Directory bridge solution.

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

Datasheet_2019-Safeguard-PrivPass_RS_41020