DATASHEET

Password Manager

Empower users, reduce support costs and strengthen security

Benefits

- Reduces help-desk and IT involvement in routine password management
- Dramatically reduces user downtime
- Provides immediate return on investment
- Improves user and IT satisfaction due to ease of use and simple deployment
- Increases network security
- Allows for synchronization of passwords between disparate systems
- Integrates with Defender multifactor authentication for increased security
- Integrates with One Identity single sign-on solutions for a complete password management solution

Overview

Most requests for help-desk assistance are for password resets. And as organizations strive for stronger security policies, the pain of password management is becoming more pervasive. Requiring more complex passwords that must be changed more frequently increases the likelihood that users will forget them and place a call to support. The problem is magnified as organizations apply passwords to multiple, disparate systems and applications. As a result, many organizations are caught between increasing security and reducing user support costs.

Password Manager provides a simple, secure, self-service solution that allows end users to reset forgotten passwords and unlock their accounts. It permits administrators to implement stronger password policies while reducing the help-desk workload. Organizations no longer have to sacrifice security to reduce costs.

Features

Enhance security

Password Manager enables organizations to adopt more secure data-access policies beyond the control offered natively in Microsoft® Active Directory®. It increases security by eliminating help-desk errors, reducing the need for users to write down their passwords and making password guessing and break-ins more difficult. Built-in data encryption supports global access while maintaining data security.

User participation secures your return on investment

Password Manager empowers users to handle the most basic password tasks on their own, allowing you to save your IT budget and realize a fast return on your investment.

Make a smart investment

Password Manager is a long-term solution to a growing problem. It is a smart investment for any enterprise seeking to increase IT operational efficiency and improve security.

- Cost-effectiveness in using existing Active Directory infrastructure—Password Manager allows you to get more from your existing Active Directory infrastructure. You can also quickly deploy it and realize

immediate ROI. Plus, it provides a more granular, group-based password policy than Windows Server 2008 does.

- Reduced help-desk workload and cost, and increased user productivity—With Password Manager, users can reset their own passwords and unlock their own accounts without involving the help desk or administrative support.
- On-demand user help—Password Manager provides online password policy explanations. In addition, it delivers feedback to the users automatically if password setup rules are not met, and can generate compliant passwords for users without help-desk assistance.
- GINA extensions for the Windows log-on dialog box—To simplify password resets for users, administrators can make the Windows log-on screen display a button for resetting passwords prior to log on. This eliminates the need to configure public kiosks or expensive telephone-based systems.

Enforce organizational standards

Password Manager accommodates the widest possible range of organizational policies and data security standards.

- Strict policy enforcement—Password Manager enforces administrator-defined standards, logs unsuccessful authentication attempts, and locks the corresponding accounts if necessary.
- Enforced enrollment—Password Manager provides several mechanisms that ensure that users enroll and use the software, guaranteeing its effectiveness.
- Reliable authentication—The personal Q&A profiles for users contain questions with unique answers that are easy for users to remember but hard for others to guess. In addition, Password Manager can be implemented with Defender to require a more secure one-time-password (OTP) authentication in conjunction with—or as a replacement to—the Q&A profile.
- Security and simplicity—Password Manager seamlessly integrates with Windows, allowing you to serve users from multiple domains, with or without trusts. Strong data encryption and secure communication are provided through support for leading technologies such as 3DES, MD5, SSL and Microsoft's CryptoAPI.

Monitor system activity

Password Manager provides administrators with robust logging and reporting features, making it easy to monitor system activity and correct any abnormalities.

Support identity management initiatives

Password Manager supports multiple web browsers and provides password management for any system connected to Microsoft Identity Integration Server (MIIS). It also extends to non-Microsoft operating systems, such as Unix and Linux, through Authentication Services; the addition of two-factor authentication through Defender; and integration with an enterprise-wide single sign-on initiative through integration with Enterprise Single Sign-on and Cloud Access Manager.

One Identity Hybrid Subscription

Expand the capabilities of Password Manager with the One Identity Hybrid Subscription which offers a myriad of additional cloud-delivered features and services. Gain access to all-you-can-eat Starling Two-Factor Authentication to protect administrative and end-user access in Password Manager replacing Telephone Verification Add-On. This offering can also be extended to additional target systems and use cases. A single subscription enables all One Identity solution deployments.

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