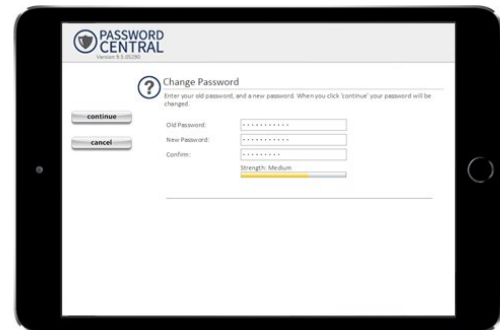


# Ivanti Password Central

Ivanti® Password Central provides fast, secure, automated self-service password reset for end users 24/7, password synchronization, and password policy enforcement tied to service desk process for zero-call resolution. Increase end-user productivity and satisfaction, gain control of the service desk operation, and optimize IT operations



## Integrate with Ivanti® Service Desk

Ivanti Password Central helps service desks refocus and align with the expectations of today's users for self-sufficiency. The solution enables end users to reset and synchronize their own passwords securely and unlock accounts themselves, at the same time eliminating calls to the service desk in peak periods. Through simple integration with Ivanti® Service Desk, end users can request a password reset from a self service portal that initiates a password reset process in Ivanti Service Desk.\* Reduce support costs by opening and closing incidents automatically in Service Desk. When a reset is complete, store the information in Service Desk for tracking and auditing purposes.

## Provide the Option of Multi-Access Self Service

Ivanti Password Central offers users secure access 24/7 to a number of reset options and provides you the flexibility to accommodate end user preferences. Let them choose from web, touch-tone phone PIN, voice recognition, SMS text messages, or biometric access to reset passwords.

## Eliminate End User Frustration with Active Directory Pre-Login

Enable end users to reset passwords from the log-in screen of their workstation prior to logging in, improving their experience. For Active Directory password resets, Microsoft credentials provide support for Microsoft Windows Credential Provider for Windows 7 and 8 and Microsoft

GINA supports Windows 2000 and XP. Maintain end-user productivity with fast, secure resets, no matter what.

## Coach End Users through Password Policies

The Reset Policy Checker in Ivanti Password Central assesses the strength of end user passwords against corporate policies and shows the password conditions they failed to meet. It recommends how susceptible a password is to brute force attacks. Combine this with automatic policy enforcement and a Hacker Dictionary that performs pattern checking and word list substitutions. You can be confident knowing your end users employ passwords that align with IT policy.

\* Requires Ivanti® Event Manager

## Enforce Authentication Questions for End Users

With Password Central you can force users to refresh authentication questions to maintain a high level of security. In addition, you can employ semi-private questions revealed in sequence to add another security layer to verify end users when they reset passwords.

## Simplify Password Maintenance

Synchronize passwords to one login for all systems and applications assigned to a user's identity or role. End users need only remember one password, expiration time of one password, and one set of password rules. Having to remember multiple passwords becomes passé. In addition, synchronization of network passwords with those stored

locally keeps both in sync. The solution stores the authentication credentials on mobile devices, computers, and servers. Security audit controls protect the passwords from compromise.

### Enforce Password Policies

IT administrators can use the Policy Enforcer capability to deploy password rules to all domain controllers on a network or in the cloud. Policy Enforcer pushes policies down a hierarchy through domains and sub-domains automatically. What's more, it checks for new domains, enables complex rules, and notifies administrators of status, reducing vulnerabilities associated with password management.

### Increase Enrollment Efficiency

Ivanti Password Central enables IT administrators to mass-enroll end users, reducing enrollment time and cost.

Enabling all end users to reset passwords immediately speeds adoption. Mass enrollment lets administrators auto-populate information about trusted business users so that they can be enrolled automatically. On first login attempt, end users are prompted to set up their security authentication questions, ensuring security is maintained as end users adopt the solution.



[www.ivanti.com](http://www.ivanti.com)



1.800.982.2130



[sales@ivanti.com](mailto:sales@ivanti.com)

Copyright © 2017, Ivanti. All rights reserved. IVI-1357 03/17 MK/BB/DR