ServiceNow Password Reset

Benefits

- **Reduce IT Service Requests**
  Apply self-service and automation to manual password reset processes to give IT more time to work on high priority requests.
- **Ensure a Consistent User Experience**
  Provide end users with the same, streamlined process for verifying their identities and resetting passwords across ServiceNow, Active Directory, and other credential stores.
- **Improve Password Management Processes**
  Leverage the ServiceNow single data model for detailed usage and enrollment reporting to monitor for compliance with corporate password security policies and identify potential security threats.

The IT Challenge

Password resets are estimated to represent around 20 percent of all service desk calls, and manually resetting passwords can be costly and slow. Password reset requests can cost anywhere from $10-$25 each to resolve, so an enterprise with thousands of end users who need to reset their passwords may find that manually resetting passwords is inordinately expensive. Moreover, manual password reset processes typically involve governance challenges associated with the service desk being given access to privileged password management tools. These processes need to be fully integrated with an IT single system of record so that governance, security, and process usage can be managed. Finally, end users requesting password resets are accustomed to the password reset experience of the internet and have come to expect a fast, consistent experience across all password reset processes.

The ServiceNow Solution

ServiceNow Password Reset significantly reduces the overall volume of IT service requests by enabling end users to reset their own passwords using self-service and automation. This application takes the familiar consumer internet password reset experience and applies it to enterprise IT. The Service desk-assisted password reset feature is an alternative approach that provides a streamlined and automated process for the service desk to quickly and consistently fulfill password reset requests without having to access password management tools. ServiceNow Password Reset supports all credential stores, including ServiceNow, Microsoft Active Directory, and more. It also supports a variety of identity verification methods, such as security questions, SMS text, and CAPTCHA, which may be used across all credential stores for a consistent and simplified user experience. End users may enroll in password reset by configuring their identity verification methods, or they may be automatically enrolled through user data already existing in ServiceNow. Extensive reporting based on the ServiceNow single system of record provides high-level and drill-down views of password reset processes, users, problems, and potential security threats.

ServiceNow Password Reset takes the familiar consumer internet password reset experience and applies it to enterprise IT

Self-Service Process

ServiceNow Password Reset provides a self-service process that is the password reset experience of the internet brought to enterprise IT. End users may request automated password resets from their web browsers by clicking a password reset link. They will then be asked to provide information to verify their identities. Once verified, users are either given a new password or allowed to enter a new, one-time password for use during their next login attempt.

Service Desk-assisted Process

An alternative to self-service, the service desk-assisted password reset process scripts, streamlines, and automates the interaction between end users and the service desk. The scripted process ensures a consistent, streamlined experience for end users and eliminates the need for the service desk to have access to private data or password management tools. When end users call the service desk to reset their passwords, the service desk can launch the password reset process from users' records in the ServiceNow Configuration Management Database (CMDB) and can select from the different password reset processes users have enrolled in. The service desk is then prompted with the steps required to verify users' identities. Once identities are verified, the service desk is given one-time passwords to read back to users. Phonetic readings of passwords are included as part of the scripted process.

All Credential Stores Supported

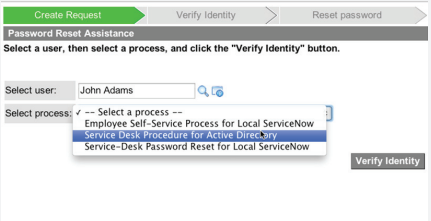
ServiceNow Password Reset supports all types of passwords the service desk may need to reset, including ServiceNow, Microsoft Active Directory, and other credentials. The application provides out-of-the-box support for ServiceNow and Microsoft Active Directory, while support for other types of credentials is a simple matter of creating custom credential stores as application extensions. Regardless of the credential store where users' passwords are housed, ServiceNow Password Reset provides a consistent user experience for self-service or service desk-assisted password reset.

Strong Identity Verification

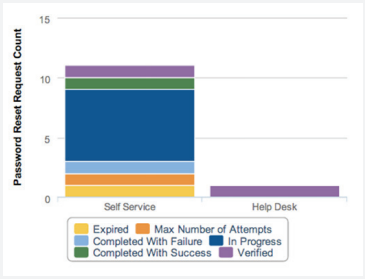
A range of methods can be used to verify the identities of users prior to allowing them to reset their passwords. Verification methods include login ID, employee ID, email address, SMS text sent to phones, security questions, and CAPTCHA to verify that requests originate from users and not malicious software. Security questions may be selected from a list of recommended, best practice questions. Other custom verification methods may be created as application extensions. Users configure their verification methods, such as selecting and answering security questions and verifying ownership of mobile devices to receive SMS text, when they enroll in password reset. They can enroll manually through the ServiceNow Service Catalog, or they can be automatically enrolled using already-existing user data in ServiceNow to set security questions. Once verification methods have been configured, ServiceNow Password Reset leverages the same methods across all credential stores. As a result, users do not need to configure and remember unique identity verification data and processes for every set of credentials.

Built-in Governance of Password Resets

ServiceNow Password Reset includes detailed reporting required to govern password reset processes. A dashboard provides at-a-glance views of password reset requests, locked-out users, users who frequently change their passwords, usage of each password reset process, and failed verifications. Use the dashboard to track enrollment and drive users to set up their verification methods. Look for potential overuse or abuse scenarios such as excessive guessing and denial of service attacks and adjust lockout policies as appropriate. Reporting can drill down to the level of detailed activity logs for tracking requests and troubleshooting problems. Review all password resets and how far they were processed. See who is locked out and unlock them if appropriate.



Service desk-assisted password reset provides a streamlined and automated process that does not require access to password management tools



Detailed reporting enables governance of password reset processes

servicenow

www.servicenow.com