ServiceNow Secrets Management

The business challenge

Organizations today depend on cloud applications to manage their critical business processes, deliver new services to their end user customers, and gain an edge over their competition. While cloud solutions offer significant benefits, they also present challenges with respect to compliance and governance, including the complexity of managing digital credentials, also known as secrets, across a vast number of applications and enterprise clouds.

Secrets are used by users and machines for authentication and include things like passwords, encryption keys, certificates, and tokens. According to Cyber Ventures, the number of passwords used by users machines was expected to exceed 300 billion in 2020.   The ever-growing number of secrets are used in many different contexts, making them extremely difficult to track and apply consistently across the enterprise.

Organizations need a well thought through centralized secrets management strategy with strong protection and access control to prevent cybersecurity issues including unauthorized access to critical data and data losses and breaches.

The ServiceNow solution

ServiceNow Secrets Management is a centrally managed secrets solution and a key component of the ServiceNow Vault offering. It provides granular management of access to passwords, digital certificates, and application programming interface (API) tokens using secret groups that can be defined to fit an organization's business needs.

Secrets are stored in a secret group which is a container that encrypts the secrets using a common key. A secret group can store many secrets and uses cryptographic modules to store the encryption/decryption keys for individual secrets. Each secret group maps to a single cryptographic module.

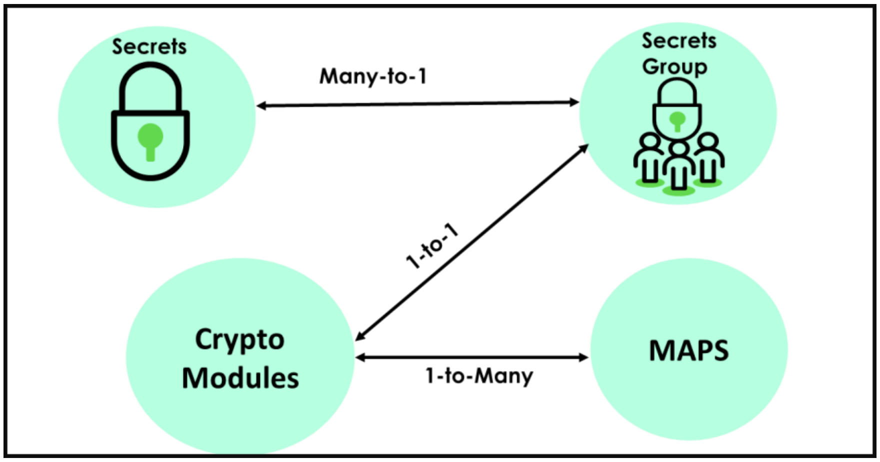


Figure 1: ServiceNow Secrets Management

Benefits

Granular access control to access credentials on a per record basis

Secure storage with innovative client-side encryption for secrets

Enhance the underlying architecture by enabling organizations to ship granular access policies on PW2 fields

Compliance: Using FIPS 140-2 Level 3 HSMs to ensure encryption keys are stored securely

Cryptographic modules are associated with one or many module access policies (MAP). These MAPs are applied to cryptographic modules and provide the access control mechanisms that defines who is allowed to access a given secret.

Secrets Management Dashboard

Organizations can monitor security issues related to their secrets management or review their security groups configured on their respective instances using the Secrets Management Dashboard. The out-of-the-box dashboard enables administrators to analyze information quickly and easily about configured secret groups such as the number of dedicated secrets, secret groups by type, and inactive security groups.

Use Cases

Ensuring secure ITOM Discovery

Figure 2 shows a simplified reference architecture of how ServiceNow IT Operations Management (ITOM) Discovery can be deployed by organizations. As shown in figure 2, multiple Windows and Linux servers connect to the MID server and several MID server agents enable the discovery process to update the CMDB. Every MID server transaction requires a secure authentication, hence managing the authentication credentials is critical from a security perspective.

Accelerating workflow connectivity with Integration Hub securely

Organizations use ServiceNow's Integration Hub to connect to different systems using automated application programming interface (APIs). Each time Integration Hub connects to a system using an API, an authentication credential is required to establish connectivity. As organizations manage a multitude of applications and APIs for connectivity they will require a secrets management solution.

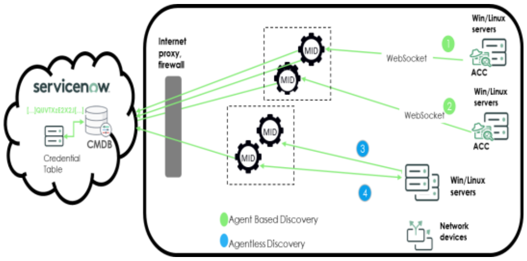
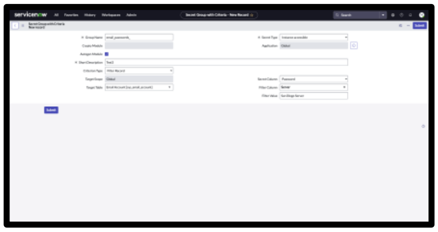


Figure 2: Secrets Management for ITOM Discovery

Secrets management is a key part of ensuring an organization's cybersecurity. It covers all processes and tools related to the creation, storage, transmission, and management of digital credentials such as encryption keys, API tokens, and passwords. To manage secrets both securely and effectively, organizations should build a core secrets management policy that establishes standard rules and procedures for all phases of a secret's lifecycle. With ServiceNow Secrets Management organizations can secure their credentials with confidence for all applications and users.



Group Name: email_passwords_
Crypto Module:
Autogen Module: ☑
Short Description: Test3
Criterion Type: Filter Record
Target Scope: Global
Target Table: Email Account [sys_email_account]
Secret Type: Instance accessible
Application: Global
Secret Column: Password
Filter Column: Server
Filter Value: [illegible]

Figure 3: Secret group detail page with Criteria

Find out more

servicenow.com/products/vault.html