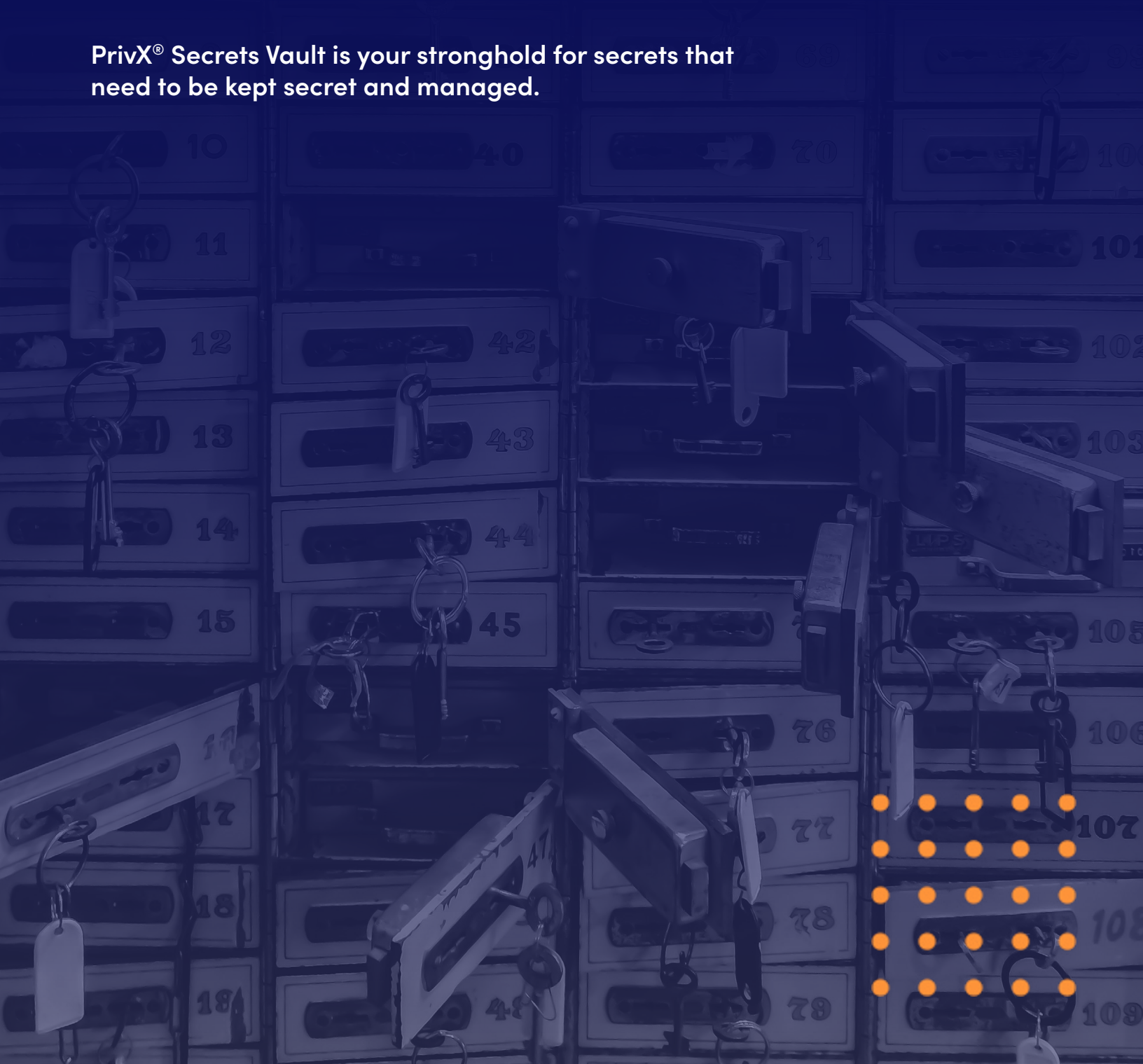
Secrets Vault

PrivX® Secrets Vault is your stronghold for secrets that need to be kept secret and managed.



Contents

SSH

Secrets are easy to create but hard to keep safe

IT environments are full of secrets, including tokens, passwords, certificates, and encryption keys. These secrets open access to mission-critical information, which makes secrets management and security organizations' top priorities.

At the same time, IT environments consist of a mix of technologies, and every organization's environment is at a different stage of maturity. Some are much further along the way toward cloudification or even containerization, whereas others are run mainly by physical servers. Most IT environments are somewhere in between, in a hybrid stage.

Unfortunately, there is no silver bullet method for securing access secrets. The best approach depends on the use case. In this article, we explore and summarize the best practices of secrets vaulting.

To vault or not to vault your secrets, that is the question

The easiest way to manage secrets is when they don't have to be managed at all. That is why our solution PrivX is built around just-in-time access tokens and ephemeral certificates that are created at the time of establishing a connection and then expire automatically after authorization. Like this, users never see or handle any secrets during the process, which improves an organization's security posture even further.

Temporary access tokens and ephemeral access tokens are a great fit for multi-cloud and hybrid environments. They allow enterprises to align their operations with Zero Trust and Zero Standing Privileges frameworks where you keep your environment free from credentials, reduce the complexity of managing them, and adopt passwordless and credential-less paradigms.

This approach leaves no secrets behind to vault or manage, freeing companies from traditional secrets management altogether.

In fact, PrivX turns privileged access management (PAM) passwordless for many use cases: by integrating PrivX with identity and access management systems (IAM), users log in via single-sign-on (SSO) to their targets without worrying about credentials. This is not only a security boost, but it also saves time and makes day-to-day operations run smoother.

It might seem contradictory that when we talk about secrets vaulting, we recommend going vault-less and passwordless. The truth is: not all IT environments or use cases support this approach. That is why PrivX also offers other options, such as Secrets Vault, where access secrets can be stored, secured, and retrieved when needed.

So, when should you vault your secrets instead of using just-in-time access tokens that leave no secrets behind?

An example case of secrets vaulting: Automated access

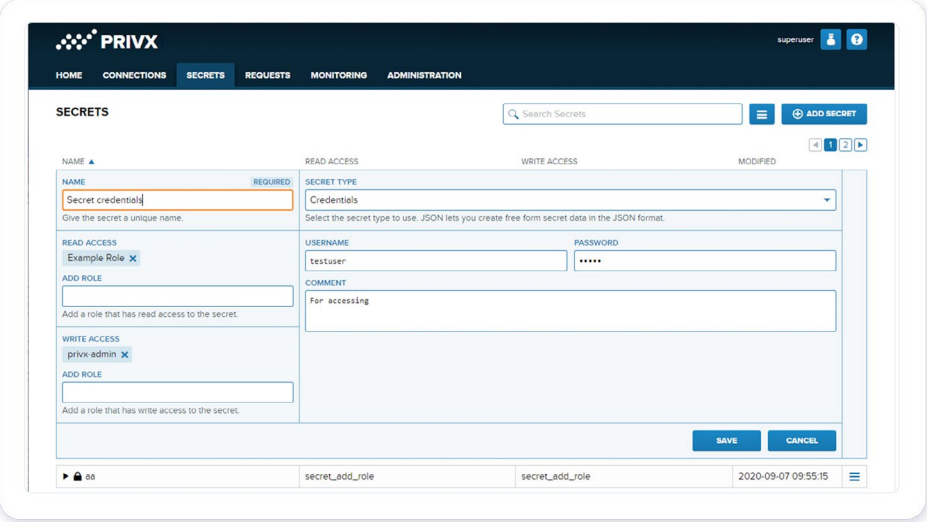
Typically, storing secrets has been associated with interactive access and privileged access management (PAM). However, automated connections - like application-to-application (A2A), machine-to-machine (M2M), or robotic process automation (RPA) communications - easily outnumber those made by humans.

For example, let's take a closer look at applications. Applications have identities, but their access credentials and privileges are often all over the place, and they typically exist outside IAM or directory services, like Active Directory (AD). Moreover, automated applications might be generating thousands of requests per second, as opposed to interactive sessions where the rate is often significantly lower.

Some of the key points to consider include:

- How many applications (e. g. web servers) can or should you connect to your databases?
- What level of access privilege do those applications need?
- Is it a read, use, or write type of access? (If it's another type of target, like the Amazon Simple Storage Service Amazon S3 object storage service.)
- What types of secrets grant access to the targets?
- Can you track and audit their sessions if needed?

For database access, your application needs a username and a password. For S3 access, it needs an API token. If you are dealing with server-to-server access, it might need an SSH key. That is a wide variety of secrets already, just based on the target.



PrivX Secrets Vault

Why do application secrets need vaulting?

In the past, the common practice was to create high-trust environments. An IT team would set up a security perimeter, inside which automated file transfers would run without interruptions. The required credentials were usually kept in plain-text format, hardcoded in the application, embedded in configuration files, part of configuration management, or integrated with version control.

Even back in the day, this was a dubious approach, since valuable secrets were basically up for grabs inside the high-trust security perimeter. But organizations were able to get away with it since only the initiated got access to the high-trust network.

Nowadays, enterprises are connected in various ways, and we live in the age of Zero Trust where no connection should be trusted by default. Instead, it should be verified every time it is established. The traditional security perimeter is gone - many critical maintenance, upgrade, and update tasks are outsourced, and applications are in contact with each other globally.

There is a clear need for a solution that manages all credentials and secrets, ensures that they are used securely, puts them under proper access controls, and ensures the right level of privilege per application access – typically a minimal amount of privilege to get the job done.

PrivX Secrets Vault does exactly that.

When to vault interactive session secrets?

Again, our recommendation is rather simple: if possible, organizations should use automatically expiring and just-in-time generated ephemeral certificates. If it is not possible right now, PrivX Secrets Vault is the secure access stronghold for managing secrets for tools that are used in software and infrastructure deployment, testing, orchestration, and configuration.

PrivX allows your organization to decide their own path toward modern secrets management. As an organization's environment and technologies evolve, PrivX enables migrating from a vault-based approach to a passwordless and vault-less paradigm.

When you modernize your environment and when you are ready for it, PrivX offers exactly that - a migration path to the passwordless world at your own pace.

Benefits of PrivX Secrets Vault

No exposed secrets left behind

Many critical tasks, like automated file transfers or DevOps development cycles, still operate outside proper identity governance and administration (IGA), leaving secrets non-compliant or exposed for misuse. With PrivX Secrets Vault, you can onboard those secrets into a vault and mitigate risks.

Protect all types of secrets

PrivX helps you secure, protect, and control access to:

- Tokens
- Certificates
- Passwords
- Encryption keys
- Pieces of code

Basically, all secrets that are used through a UI, CLI, or HTTP API to access sensitive or mission-critical data.

Manage non-interactive access with proper levels of granularity

Bring automated connections, like application-to-application (A2A), machine-to-machine (M2M), and Robotic Process Automation (RPA), under role-based access controls (RBAC). Make access lifecycle management fast and easy by associating non-human identities with a role. Manage their access and their level of privilege based on a small number of roles instead of identities, which can be counted in thousands.

Keep your identities and roles in sync automatically

Integrate machine identities and human identities alike to the trusted identity provider of your choice. PrivX Secrets Vault automatically stays in sync with any changes to identities, making sure that the right identity is associated with the right role, or that access rights are revoked automatically - and almost in real time - if the identity is removed from your IAM.

Audit and track sessions

Stay in control of all activities in your environment by auditing and tracking each session whether they are interactive or non-interactive.

Centralize access and workflow processes

Put your access management under a single pane of glass with PrivX's multi-tenant vault. Use consistent, centralized, and well-defined workflows to manage secrets and access that they enable.

Use cases

Personal password manager

Allow your privileged users to store their own secrets in the vault, using it as their secure personal password manager for highly valuable secrets.

Enable collaborative secrets management

Enable collaborative secrets management based on a role for privileged users, instead of them sharing secrets or using hard-coded credentials. PrivX Secrets Vault contains ready-made templates to help you get started.

1 Interactive UI access for environments that do not support certificates

PrivX Secrets Vault is based on role-based access controls (RBAC). The user logs into PrivX and always sees an up-to-date list of accessible targets based on their role. If the target requires a password, the user retrieves the masked password from the vault and enters it into PrivX when prompted. The secrets available to the user are always limited by the role and the level of privilege associated with that role.

2 Interactive command line interface (CLI) access in DevOps

For those contexts where a CLI is needed, PrivX Secrets Vault ensures that secrets are accessible through an easy-to-use CLI tool. For example, for DevOps teams, this means that instead of the DevOps team sharing or using hard-coded secrets assigned to individual users, they can use a centralized vault where these secrets are stored.

3 Application-to-application (A2A), machine-to-machine (M2M), and Robotic Process Automation (RBA) access

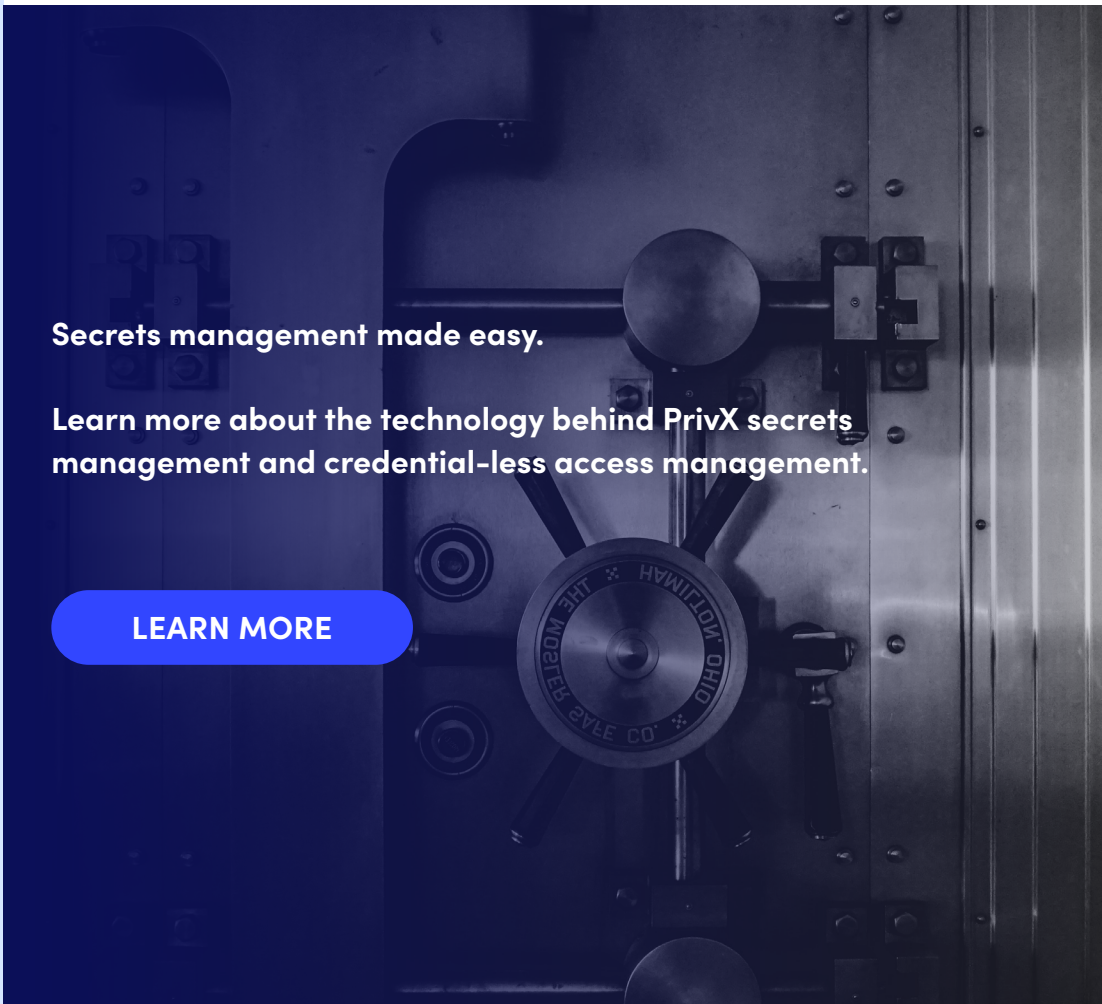
PrivX Secrets Vault enables A2A, M2M, and RPA communication without risky, hard-coded target system credentials or credentials embedded in the code. Instead, these credentials are stored in the vault, which the non-human identities then access through a REST API to enable their automated connections. With the vault, you can centrally manage, control, track, and audit these processes and their secrets as needed.

4 Collaborative admin secrets management for critical IT infrastructure access

Use PrivX Secrets Vault as a centralized safe for a team of administrators to store encryption keys, access tokens, or break glass credentials. These can be used to access web applications, network devices, databases, or servers. No need to share secrets, the vault is the only location where a secret has to be updated.

5 Digital safe for break glass credentials

Use a single PrivX Secrets Vault instance as a centralized safe for critical secrets to be handled with extraordinary care, like break glass credentials. You can isolate the instance from your IAM integrations and set specific rules (like firewall or VPN configurations) on how these secrets can be accessed even if network connections are down.



SSH

Key features of PrivX Secrets Vault

FEATURES	
Secrets vault as a microservice	The vault stores the secret data in encrypted format along with the metadata in the database. Internally, it uses the key vault API for performing secret encryption and decryption.
Role-based access control to target hosts	Users can be dynamically mapped to roles. You can view hosts that are accessible by specific roles.
Context-based roles	Restrict access based on the day of the week, time of the day, or IP addresses for specific roles.
Restrictions based on access groups	Restrict access based on access groups that can be, for example, departments or functions inside an organization. Even as an admin, you only get access to the area of the network your department is entitled to access.
Directory service integration	Users and groups can be synced with Microsoft AD, Azure AD via Graph API, Google G Suite, LDAP, and OpenID Connect providers (e.g. AWS Cognito, Okta, Ubisecure).
Sign-in and access control to PrivX	• Single sign-on (SSO) through directory service applications via Kerberos • Username & password for local users • Multi-factor authentication (MFA), time-based one-time password (TOTP), e.g. Google Authenticator, Duo, Authy
Authentication to target hosts	• OpenSSH certificate • Virtual Smart Card for RDP • Stored, vaulted credentials • Username & password
Supported protocols	SSH (v2), RDP, HTTP(S), and SFTP
Fast and responsive user experience	HTML5 single page UI over REST APIs
Complete HTTP REST API	Anything the UI does can be executed via the API
Support for Thales Vormetric Data Security Manager (DSM)	Integrate with a centralized security management solution

Let’s get to know each other

Want to find out more about how we safeguard mission-critical access for leading organizations around the world? We’d love to hear from you.

REQUEST A DEMO

SSH