Centrify Privilege Service
Access and Password Management for the Modern Enterprise

IT organizations are increasingly required to manage hybrid deployments that combine cloud-based and data center infrastructure. IT admins, both internal and outsourced, need to login from inside and outside of the corporate perimeter. In order to meet these challenges, IT organizations that share privileged accounts need an access and password management solution built for the modern enterprise to increase security, simplify compliance and control remote access to servers and network equipment.

Privileged Accounts Hold the Keys to the Kingdom
Security breaches are all over the news. Caused by both malicious insiders as well as hackers, they use Advanced Persistent Threats (APTs) to take advantage of poorly managed privileged accounts and a lack of additional security measures such as multi-factor authentication. The proliferation of privileged accounts beyond the data center to cloud-based infrastructure further amplifies the complexities of securing privileged access to critical servers and network equipment.

Organizations need to control and monitor privileged accounts and access while improving IT productivity for both internal and outsourced IT in today's modern enterprise.

Implementing a least privilege access model, auditing and associating privileged activity to an individual, securely managing shared privileges and providing comprehensive regulatory compliance reporting are at the root of reducing threats, intentional or not. Cost-effectively meeting regulatory mandates as a part of doing business.

Granular Control without a VPN
Centrify Privilege Service provides all of your IT administration teams with secure, granular access to infrastructure regardless of location, and without the hassles of a VPN.

Secure browser-based access
Authorized IT users launch management sessions for resources directly from the Privilege Service portal. Sessions use SSH and RDP protocols, and are always protected end-to-end.

Access across organizational boundaries
Privilege Service enables you to authenticate your IT users through Active Directory, LDAP and the Cloud Directory. You can use one or any combination of these identity stores to grant granular access to employees, business partners and outside vendors.

Grant access to specific resources
Unlike a VPN, Privilege Service enables you to grant access to resources on a on a per-resource basis. This means that you can easily give your internal IT admins access to as much of your infrastructure as necessary, while limiting access by an outsourced team to only the servers and network hardware their business role or IT function requires.

Access from any location
Your IT admins can log in and securely access resources from any location that can reach the Privilege Service. For user logins outside the corporate network, you can require Centrify's built-in multi-factor authentication for security stronger than a user name and password.

Control Shared Access to Privileged Accounts
Centrify Privilege Service gives you control over shared accounts. Regardless of where your server and network infrastructure is located — on-premises or in the cloud — Privilege Service gives your IT admins secure, always-on access to critical shared account passwords, while giving you control over who has access, which account passwords they have access to, and how those passwords are managed.

Reduce deployment and management costs
Simplify and automate shared account password management for super-user and service accounts with flexible deployment options such as leveraging a cloud service or manage the solution entirely within your own data center or Infrastructure-as-a-Service (IaaS) deployment.

Secure checkout of account passwords
Authorized IT users can checkout passwords for accounts for a limited duration, displaying them or copying to the clipboard. Privilege Service delivers “break-glass access to passwords from mobile devices enrolled in the Centrify Cloud. Secured password checkout requires a PIN or fingerprint validation.

Automatic password resets
Privilege Service generates a new password and changes the password on
Remote sessions using shared accounts

In combination with the secure remote access features, authorized users log in to resources using shared accounts without Privilege Service disclosing the passwords to them.

Control access globally, per-resource, and per-account

Privilege Service provides you with both global and granular control of permissions for accounts and passwords. You have full control over who can access which resources, and which accounts they can use.

Reinforce Secure Access to Critical Systems

Privilege Service works with Centrify Server Suite® to provide an extra layer of security to protect against hackers by configuring multi-factor authentication (MFA) for IT administrators who access UNIX and Linux systems and require elevated privileges.

Self-service Privileged Access Request

Minimize your attack surface with governed access to privileged account credentials and remote sessions. Keep control with request and approval workflows, time-bound access and privileged session monitoring. Capture who requested access and who approved it, and easily reconcile approved access with actual access for privileged access governance.

Secure, Encrypt and Manage Application Passwords

Prevent cyberattacks that target privileged account credentials and streamline operations by eliminating hard-coded, plain text account passwords from scripts and applications. Applications and scripts authenticate and retrieve passwords securely without human intervention, enabling organizations to meet compliance and security policies.

Monitor Privileged Sessions

Consistently monitor privileged sessions, whether using shared accounts or user accounts with privilege elevation, for servers and network devices, both on-premises and cloud-based. An audit add-on to Privilege Service provides gateway-based session monitoring, the ability to watch and terminate suspicious sessions and session reporting while Server Suite offers full host-based privileged session monitoring for additional security.

Secure, encrypted storage for your data

Privilege Service securely stores all your user, resource, account, and password information. Privilege Service also offers integrated support for customers using Gemalto’s SafeNet KeySecure key management appliances to secure and encrypted storage of account passwords.

Identity Management for Privileged Users

Privilege Service complements Server Suite by delivering secure managed access and shared account password management for on-premises servers and network equipment as well as Infrastructure-as-a-Service (IaaS). Together they constitute Centrify’s identity management for privileged users solution, which reduces the risk of security breaches by minimizing the attack surface and auditing all privileged sessions.

Benefits

• Eliminate identity-related risks associated with shared accounts
• Flexible deployment choices include a cloud service, or managing the solution entirely within your own data center or IaaS deployment.
• Mitigate the risks of granting full VPN access
• Secure privileged access for outsourced IT
• Lower TCO with a single, integrated solution