DATASHEET

Centrify Privilege Service

Cloud-based Password and Access Management

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 a password and access 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. The proliferation of privileged accounts beyond the data center to cloud-based infrastructure 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.

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.

Easy import of resources, accounts and passwords

A simple wizard guides you through adding new servers and network hardware, accounts, and passwords to Privilege Service. You can also import from an Excel or CSV file.

Secure checkout of account passwords

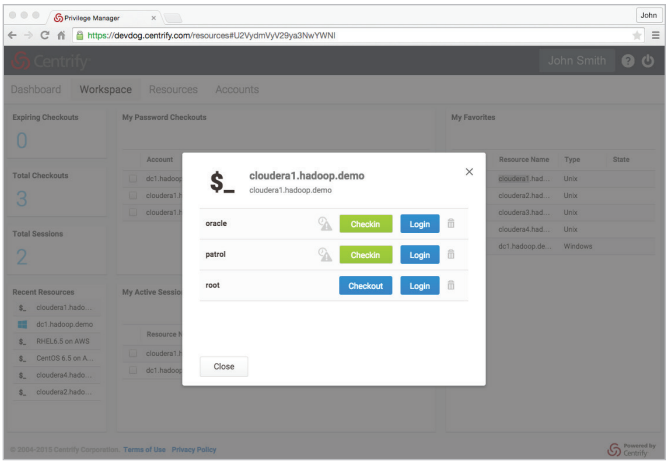
Authorized IT users can checkout passwords for accounts for a limited duration, displaying them or copying to the clipboard.

Automatic password resets

Privilege Service generates a new password and changes the password on the target system when a checkout expires. Complex, high-entropy passwords are created at run-time by Microsoft .NET cryptography libraries.

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.



Authorized users can checkout account passwords or initiate sessions without knowing the password.

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.

Managed and unmanaged passwords

Privilege Service gives you the option to take passwords under its full control — called managed passwords — and only Privilege Service will know the actual password until a user checks it out. Unmanaged passwords will never be updated or changed by Privilege Service, but they can still be used for checkout and remote sessions.

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 Centrify Cloud Directory. You can use one or any combination of these identity stores to grant granular access to employees, business partners and outside vendors.

Limit access to 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

Because Privilege Service is delivered as Software-as-a-Service (SaaS), your IT admins can log in and securely access resources from any location that can reach the Centrify Cloud. 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.

Monitor Privileged Sessions

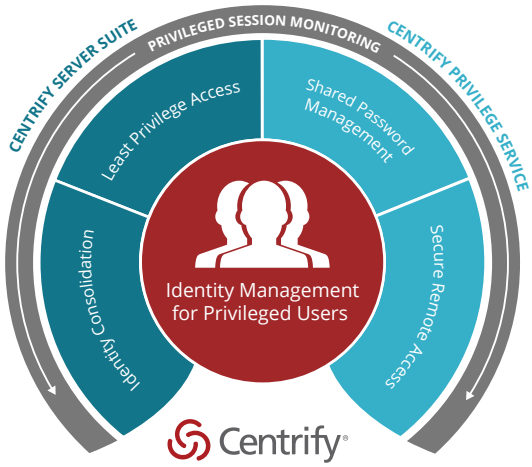
Consistently monitor privileged sessions, whether using shared accounts or user accounts with privilege elevation, for servers and network devices, both on-premises and cloud-based. An audit add-on to Privilege Service provides gateway-based session auditing, search capabilities and session reporting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

Benefits

- Minimize risk of security breach when sharing privileged accounts
- Enforce centralized control over privileged accounts
- Increase access security
- Enable effective compliance and audits for privileged accounts
- Future-proof your identity and access management (IAM) strategy

Identity Management for Privileged Users

Centrify Privilege Service extends Centrify Server Suite by delivering shared account password management and secure managed access to 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.



Centrify Identity Platform

The foundation for Privilege Service is the Centrify Identity Platform, the industry's first cloud-based platform built from the ground up to provide secure, always-on identity management services for end users and privileged users. The Identity Platform provides core services for secure data storage, directories for users, resources and applications, authentication services (both single and multi-factor), and reporting.

Secure, encrypted storage of your data

Your data is secure in the Centrify Cloud. Privilege Service uses the secure data store of the Centrify Identity Platform to store all user, resource, account, and password information.

Platform Support

Privilege Service supports over 450 versions of Windows, Linux and UNIX operating systems. In addition, Privilege Service supports leading network hardware operating systems.

- Microsoft Windows Server
- Red Hat Enterprise Linux
- Oracle Solaris
- Cisco IOS, NX-OS
- HP ProCurve, Comware
- Juniper JUNOS

Centrify

Centrify delivers secure and unified identity management for end users and privileged users across cloud, mobile and data center environments. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, shared account password management, auditing for compliance and enterprise mobility management.

SANTA CLARA, CALIFORNIA	+1 (669) 444 5200
EMEA	+44 (0) 1344 317950
ASIA PACIFIC	+61 1300 795 789
BRAZIL	+55 11 3958 4876
LATIN AMERICA	+1 305 900 5354
EMAIL	sales@centrify.com
WEB	www.centrify.com

DSH001579EN-04212015