What's New in Centrify Privilege Service

Centrify Identity Platform 15.4

Centrify Privilege Service

Centrify Privilege Service™ is a cloud-based password and access management solution. Privilege Service combines shared account password management with the ability to securely manage and audit access by internal and outsourced IT. The net result is increased security when sharing privileged accounts, simplified compliance, and secure remote access to on-premises and cloud-based infrastructure.

Privilege Service is built on the Centrify Identity Platform and delivered as Software-as-a-Service (SaaS) from the Centrify Cloud. In addition to its powerful features for password and access management, Privilege Service includes all the features and functionality of Centrify Identity Service App+ Edition.

Privilege Service complements Centrify Server Suite™, which combines comprehensive bridging of Linux and UNIX systems to Active Directory with powerful privilege management and session monitoring across Windows, Linux and UNIX systems.

Built on the 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.

Privilege Service leverages the Identity Platform and adds features that enable authorized access to your infrastructure regardless of where it's deployed — on-premises or in the cloud — and control and management of shared accounts and passwords. Privilege Service is delivered from the Centrify Cloud through your Web browser, and is secure, simple to use, and easy to deploy.

Secure Data Storage

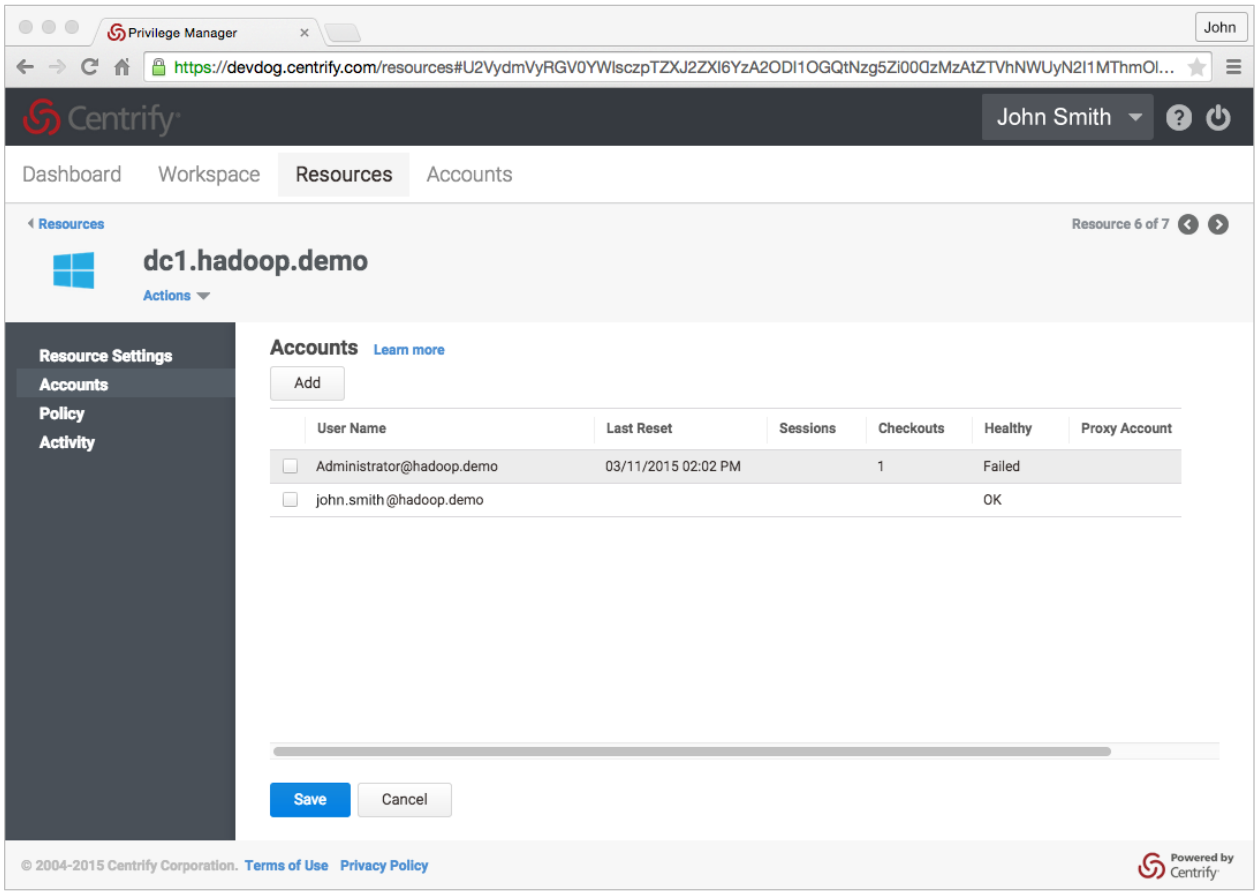
Your data is protected in the Centrify Cloud. Privilege Service uses the secure data store of the Centrify Identity Platform to protect all user, resource, account, and password information, at-rest and in-motion. Depending on your needs, you can choose from additional options for different levels of data and compute isolation in the Centrify Cloud hosted on Microsoft Azure.

Features and Benefits

Manage Passwords for Local and Service Accounts

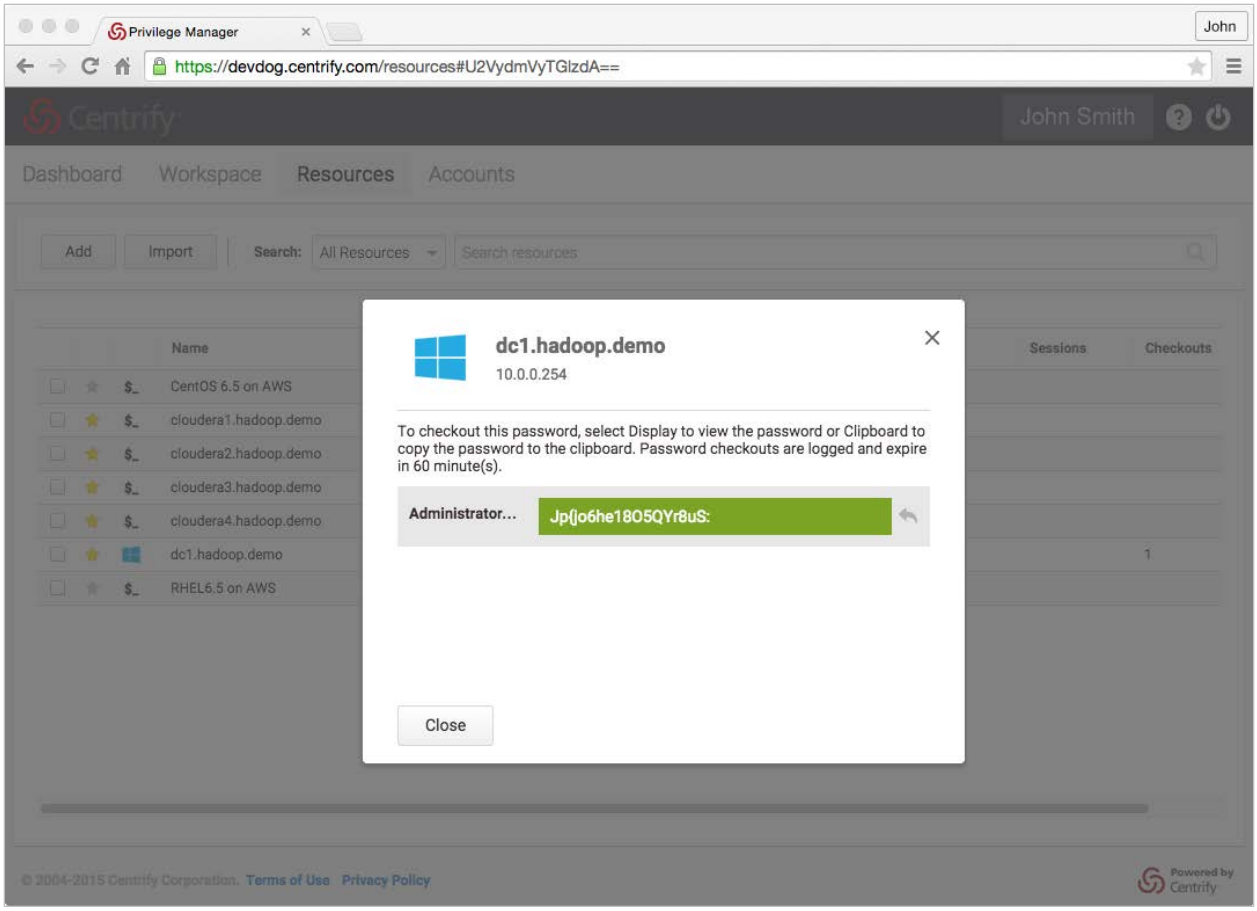
Privilege Service can manage passwords for local and service accounts on servers and network hardware. Managed passwords are automatically changed as soon as the account is added to Privilege Service. From that time forward, only Privilege Service will know the password. Admins can't share the password, and unauthorized users can't login with that account.

Complex, high-entropy passwords are created for Privilege Service at run-time by Microsoft .NET cryptography libraries.



Password Checkout

Authorized users can checkout account passwords for a limited duration, displaying them in plain text or copying them to the system clipboard. All password checkouts are audited and associated with the user who logged into Privilege Service and performed the checkout.



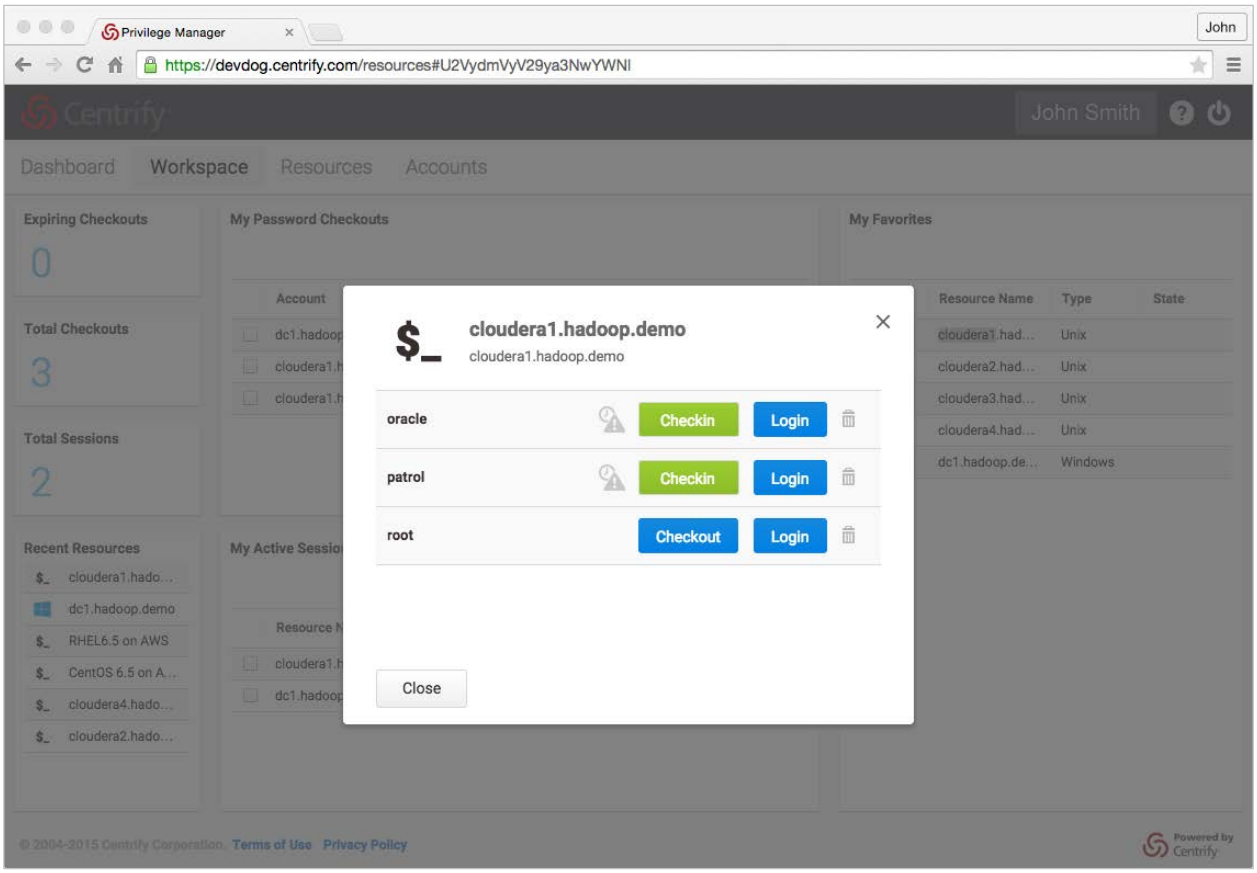
Automatic Password Reset

For managed passwords, Privilege Service automatically generates a new password and changes the password:

- When the account is added to Privilege Service
- When the password's checkout interval expires

Remote Management Sessions

Privilege Service enables authorized users to launch management sessions for resources directly from the Privilege Service portal within the user's browser. Sessions use standard HTTPS, SSH and RDP protocols to connect to resources, and are always protected end-to-end.



Use Shared Accounts without Disclosing Passwords

Authorized users can login to resources using shared accounts without knowing the passwords, and without Privilege Service disclosing the passwords to them. This enables IT admins to use accounts that must be shared for routine management, while stopping password sharing and unauthorized access.

Limit Access to Resources

Unlike a VPN that gives users visibility to the entire network, Privilege Service enables you to grant access to resources on a per-resource basis. This means that you can easily give your most privileged 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 requires.

Access from any Location

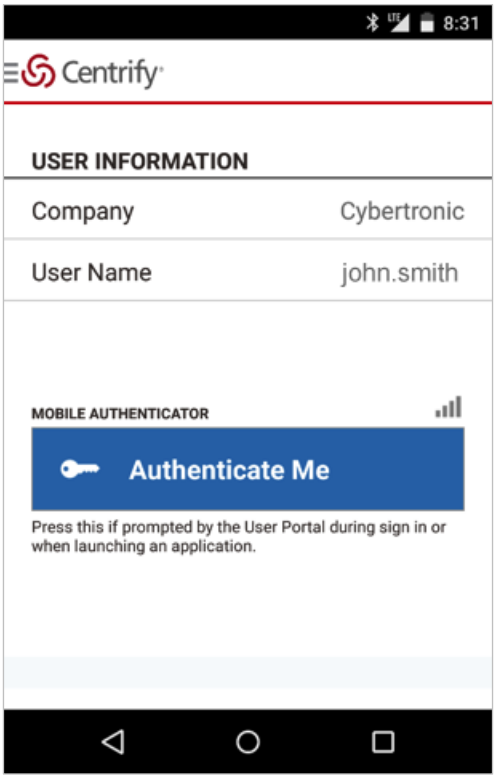
Privilege Service is delivered as Software-as-a-Service (SaaS) to the user's browser. Authorized users can log in from any location that can reach the Centrify Cloud, and user login is context aware. For example, when users log in from outside the corporate network, you can require Centrify's multi-factor authentication for security stronger than a user name and password.

Audit and Report User Activity

Privilege Service automatically audits and keeps a record of all user and administrative activity in the portal. Password checkouts and remote management sessions are always associated with the user account that logged into Privilege Service and performed the activity. Simple reporting is provided through the user interface, and users can create and share their own custom reports for more complex queries.

Optional Gateway-based Session Monitoring

Privilege Service can optionally capture screen activity for remote management sessions, giving supervisors and auditors a record of the actions taken by a user on a server or network device. Session monitoring is integrated with the DirectAudit feature set of Centrify Server Suite, Enterprise Edition. You can use a Centrify audit installation independently with Privilege Service, or leverage an existing Server Suite, Enterprise Edition installation and combine both Privilege Service and Server Suite session monitoring in one database, leveraging a single set of query and management tools.



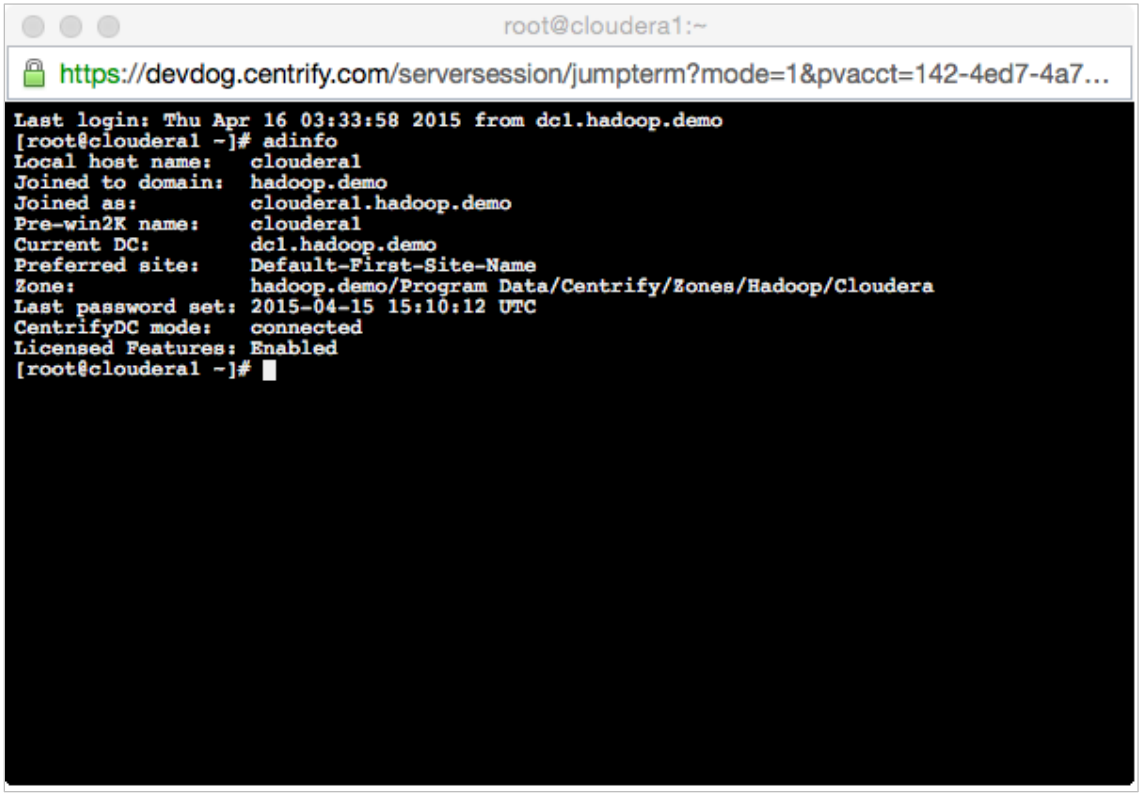
Centrify Mobile Authenticator lets you do multi-factor authentication from any device.

Securely Store Static Passwords

Privilege Service can optionally store an account password without managing it. The password will be securely stored and can be checked out or used for remote management sessions, but will not be changed automatically by Privilege Service.

SSH Proxy

A common scenario for Privilege Service is management of the UNIX or Linux `root` account. If the computer is configured to prevent the `root` user from opening a Secure Shell (SSH) session, you can tell Privilege Service to use a proxy account on that computer to open the SSH sessions necessary for password and remote management.



Platform Support

Privilege Service supports local and service password management on the same set of Windows, UNIX and Linux server operating systems as Centrify Server Suite 2015. In addition, Privilege Server supports five network hardware operating systems for secure storage and use of account passwords for checkout and remote management sessions.

- Cisco IOS
- Cisco NX-OS
- Juniper JUNOS
- HP ProCurve
- HP Comware

Contact 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. Centrify customers can typically reduce their total cost of identity management and compliance by more than 50 percent, while improving business agility and overall security. Centrify is used by more than 5,000 customers worldwide, including nearly half of the Fortune 50 and more than 60 Federal agencies.

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