

New features

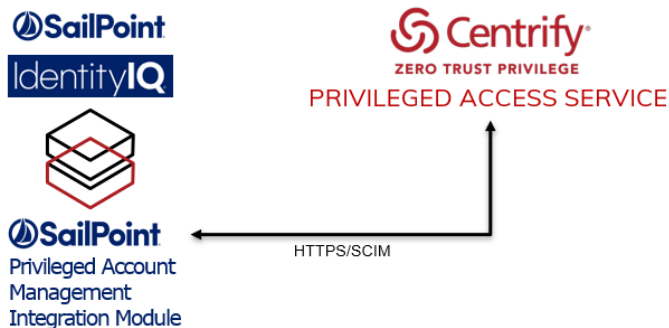
PAS integration with SailPoint IdentityIQ PAM Module

Combining role-based access control with attestation and remediation from the industry leaders – Centrify and SailPoint

SailPoint IdentityIQ is the industry-leading IAM application focusing on attestation and remediation, access request, and user provisioning.

Centrify's integration with SailPoint enables organizations to accelerate the adoption of crucial governance and compliance processes for identity and access management.

- Provisioning users into Centrify PAS Roles or Sets
- SailPoint PAM Module containers map to Centrify PAS Roles and Sets
 - Provision users into Centrify PAS Roles
 - Grant user permissions on Centrify PAS Sets
- Attestation of user rights and permissions from PAS



Use and manage secrets in an RBAC hierarchy

Role-based access control is the proven methodology for managing distributed access to critical information. Centrify adds an RBAC hierarchy to file and text secrets.

- Define who can edit and use Secrets within a Secret and folder hierarchy
- You control:
 - The hierarchy ('Secret and folder')
 - Who can edit/use Secrets in which folder
 - Who can create/delete new folders in the hierarchy
 - Who can move Secrets and folders
- Virtually unlimited namespace for Secrets
- Standard for managing Secrets in DevOps
 - Secure API access to hierarchy and Secrets

FolderD

Secrets / FolderA / FolderX / FolderD

	Name	Type	Filename	Path	Created
<input type="checkbox"/>	SubFolderA				05/27/2018 04:21 PM
<input type="checkbox"/>	SubFolderB				05/27/2018 04:21 PM
<input type="checkbox"/>	SecretA	File	File-A.docx	FolderD/FolderB/	05/27/2018 04:21 PM
<input type="checkbox"/>	SecretB	Text		FolderD/FolderX/	05/27/2018 03:27 PM
<input type="checkbox"/>	SecretC	File	File-C.pdf	FolderD/.../FolderZ/	05/27/2018 09:55 AM

SailPoint IdentityIQ connector integration enhancements

For customers who enable self-service for their users within SailPoint IdentityIQ, the Centrify Connector Integration offers unique value for self-service access request to systems and accounts managed by PAS.

The connector integration is enhanced to enable access request to Centrify Zone roles, in addition to resources and accounts managed by PAS.

Access request from within SailPoint IIQ to:

- Centrify Zone roles
 - Writes new Zone information to Active Directory
 - User access updates based on agent settings



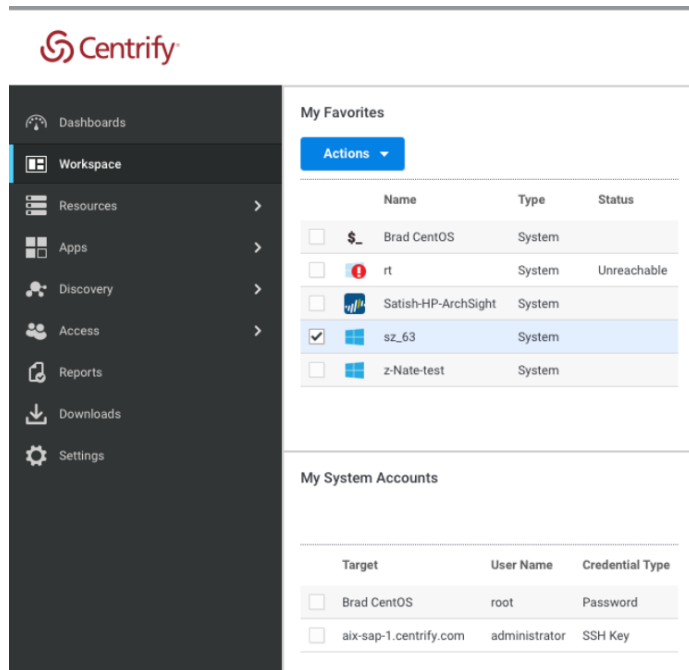
New UI for system and account tiles in old User Portal

The new Centrify PAS user interface puts a laser focus on managing your IT infrastructure. IT system and account logins for low privileged users (such as Help Desk) now appear in a user Workspace.

User Portal tiles for PAS systems and accounts are migrated into a new Workspace user interface.

- New “My System Accounts” table in the user Workspace
- Automatically migrates existing tiles
- Portal Login permission is changed to Workspace Login

- Accounts with this permission will appear in the user Workspace
- Enables users without PAS administrative rights to access systems and accounts
 - Minimizes user interface for these users



Improved DB performance

Performance at enterprise scale is a feature. Improved PAS architecture and queries for PostgreSQL enable fast page loads and queries for enterprise scale resource and account loads.

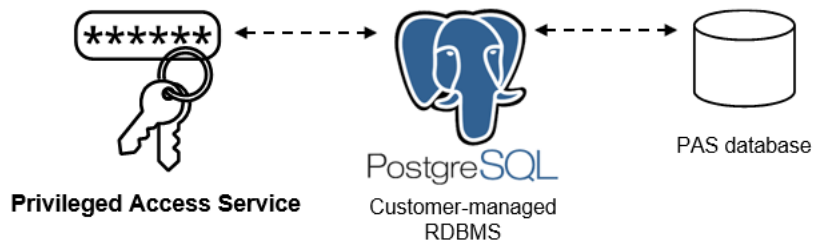
- Orders of magnitude improvements for page loads and database queries
- Scales to large enterprise deployment scale
- Requires upgrade to version 19.2 database

If you are a customer using Centrify cloud service, no action needed. These enhancements will be part of the 19.2 deployment.

For customers who are using on-premises deployment, please follow

<https://centrify.force.com/support/Article/KB-11818-How-To-Enable-FastDB-on-Customer-Managed-Privilege-Access-Service-PostgreSQL-Database> to enable the feature.

The Improved DB performance for customer-managed PostgreSQL database will be available in Release 19.3, details will be included in release notes.



The following apps have been updated:

- Lynda (User / Password)
- SEMRush (User / Password)

The following apps have been renamed:

- 1 and 1 → 1&1 IONOS

Changes

The following list records issues resolved in this release and behavior changes.

- Inbound provisioning has been enhanced to support user specified / custom attributes (CC-65342).
- The IWA service now starts automatically after a connector auto-upgrade (CC-66213).
- Android OS 9 devices no longer show as “unknown” in the Endpoints dashboard Total Devices by OS Version list (CC-64887).”
- On Samsung devices with KNOX version 3 and above, it is now possible to configure a POP email account that uses SSL / TLS (CC-64974).