Centrify
THE BREACH STOPS HERE

SOLUTION BRIEF

Identity Services Automation for ServiceNow®

Identity meets Enterprise Service Management

End-users are seeking modern ways to interact with IT and other shared services groups across their organization. They look for self help — where they can get secure access to apps, manage their own passwords, search for known apps or servers, request access to services that they need. IT-users need to automate tasks like account provisioning and password resets, and manage privileged access to on-premises and cloud-based infrastructure. Centrify's identity management integrations with ServiceNow help automate processes, improve visibility, and provide a better experience for ServiceNow end-users and privileged IT-users.

Centrify has partnered with ServiceNow to offer solutions that make life simpler and more secure for end-users and IT-users. These integrations include self-service password reset, single sign-on (SSO) with built-in multi-factor authentication (MFA), and automated provisioning and de-provisioning of users based upon role membership within Active Directory, LDAP directories or Centrify Cloud Directory.

Centrify leverages ServiceNow's advanced workflows to offer self-service application access request for end-users, and self-service privileged access request for resources (servers, network devices) for IT-users.

Leveraging our certified integrations with ServiceNow, organizations can now use their existing identity infrastructure to manage identity-related IT activities — such as user authentication, access control, user account and application provisioning, policy enforcement, and compliance.

The following Centrify Identity Platform integrations are available in the ServiceNow Store. Each of these integrations requires subscription to Centrify Application Service or Centrify Infrastructure Service and ServiceNow.

Centrify Single Sign-on & Provisioning

Centrify
Single Sign-on & Provisioning

Accessing cloud and on-premises applications becomes difficult when there are multiple usernames and passwords to remember. But storing passwords in a file, or re-using passwords across different cloud apps is a security risk.

Centrify Single Sign-On & Provisioning enables secure single sign-on and automated account provisioning to ServiceNow and thousands of other applications.

Single Sign-On

An administrator configures user roles within the Centrify Cloud Manager. Roles control which users can access which SaaS and mobile apps. IT then selects which apps to deploy from Centrify's catalog of thousands of apps. End-Users login to the Centrify User Portal with their network credentials. They then click on ServiceNow or any other pre-provisioned app tile to get instant access.

Benefits for IT

- Save time, improve IT efficiency and security
- One-click access to all apps, without the integration hassles
- Improve security by eliminating the use of easy-to-remember, reused and/or improperly stored passwords
- Improve app security with multi-factor authentication

Benefits for end-users

- Reduce frustration — only one password to remember
- Instant access to ServiceNow and all other apps
- Easy to use multi-factor authentication

Provisioning

Setting up and removing user accounts is one of the most onerous and labor-intensive tasks IT faces, especially in periods of rapid expansion or contraction of the business.

With Centrify, ServiceNow administrators can automate provisioning and de-provisioning of end-users and IT-users based on their role membership within Centrify.

How it works

An administrator configures user roles within the Centrify Cloud Manager for provisioning. Roles control which users will be provisioned automatically into ServiceNow and other SaaS applications from any of the directory services supported by Centrify.

When an employee is terminated, IT initiates a de-provisioning workflow that removes/disables a user from Active Directory or another directory service. Centrify will deactivate their access to ServiceNow and every other cloud or on-premises application.

Benefits for IT

- Save time by automatically creating or updating user accounts across apps within ServiceNow
- Improve efficiency by deploying the right apps the first time, with single sign-on
- Improve security with automatic role-based permissions within ServiceNow
- See who has access to which apps, how they received access, and when changes occurred
- Prevent unauthorized access by automatically revoking access to all ServiceNow apps at once

Benefits for end-users

- Immediate access to all assigned apps, from day one
- No additional user credentials to remember

Centrify Password Reset

Centrify Password Reset

End-users typically use the ServiceNow interface for all IT-related service tasks, including password resets. Centrify Password Reset supports self-service and help desk-assisted password resets.

How it works

End-Users access a custom password reset URL hosted on your ServiceNow tenant to initiate the password reset. The password reset propagates all the way into the directory to which the end user belongs — Active Directory, Centrify Cloud Directory, or LDAP.

Benefits for IT

- Reduce helpdesk volume due to forgotten passwords
- Deliver a modern service experience with immediate response
- Provide a consistent user experience for all end-user IT requests
- Significantly reduce IT service requests by leveraging ServiceNow
- Ensure policy compliance and security

Benefits for end-users

- Control over own user account
- No wait times, emails, phone calls, between users and the support staff

Centrify App Access

Centrify App Access

ServiceNow's advanced workflows help organizations automate services with consistency and at large scale. In the past, some of these automated workflows required manual intervention — at the critical junctures of approval, provisioning, and user self-service.

When end-users request access to an application through ServiceNow service catalog, ServiceNow's advanced workflows will properly route the approval to the right fulfillers or approvers.

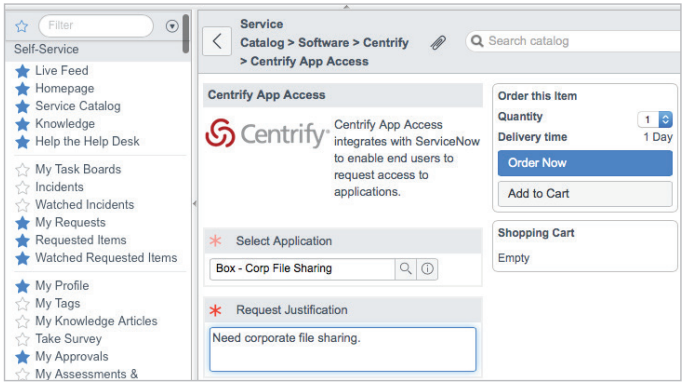
However, once the app access is approved, the final provisioning of the app requires manual IT intervention when IT provisions access for each user within each application. Days can elapse between when a user opens a ticket, when the approvals come in, and when IT fulfills the order.

The integration of Centrify App Access with ServiceNow offers complete IT services automation — all through preconfigured policy, federated identity, and automated user account provisioning. End-Users request access to applications from within ServiceNow service catalog. Once the app access is approved, the end-user receives the app provisioned automatically with no manual intervention by IT.

How it works

An end user requests access to an application from the ServiceNow service catalog using Centrify App Access. ServiceNow initiates a workflow and processes approvals according to the assigned workflow. If access has been approved, the ServiceNow platform will call upon the Centrify platform to grant access and provision the user into the application.

- Single Sign-On apps: Centrify App Access provisions the app into the user's account, and the user can open the app without entering additional authentication
- Shared username/password apps: If the requested application is for a shared account (such as corporate social media), Centrify provisions the end user with a vaulted set of credentials. The requestor gets 1-click access to the shared app but never knows the shared account password
- If the requested application is for a non-shared account, the end-user must enter their username and password when launching the app for the first time; then the credentials are secured in the Centrify password vault for subsequent use



Benefits for IT

- Save time with automation: The user requesting access gets their request routed to the owner of the resource immediately
- Close the gap between automated workflow and account provisioning, for a seamless experience from start to finish
- Save time, improve efficiency and security: Centrify reduces IT service requests, helps deliver a consistent application delivery process ensuring policy IT compliance and security

- Enforce role-based policy: Assign correct access permissions/ licensing within apps, ensuring policy compliance and security
- Prevent unauthorized application access: IT can terminate access to all apps from a single directory
- Report on app access: Raise visibility to who has access to which apps — how they received that access, who approved that access or when it changed

Centrify Privileged Access Request

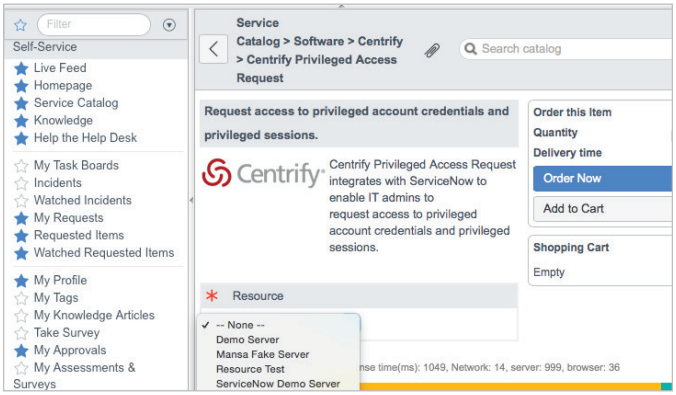
Centrify Privileged Access Request

One of the most common causes of data breaches today is stolen credentials to critical resources within an organization by external attackers and internal personnel. To reduce risk and minimize the attack surface, your business should control access to the "keys to the kingdom" — privileged account credentials or remote management sessions, by granting access to appropriate users only when they need it, and for a specific amount of time.

Centrify Privileged Access Request enables IT users to request temporary or permanent access to privileged accounts or a privileged session to perform a designated task from the ServiceNow asset management database.

How it works

- The IT-user selects Centrify Privileged Access Request from the ServiceNow catalog, selecting the resource, whether they need login or checkout privilege and written justification.
- Approvals are processed within ServiceNow in accordance to the asset-assigned workflow and ITIL processes. Once an approval is processed, ServiceNow will call upon Centrify to enable access to the server or device.
- If Centrify knows the IT-user, it will notify ServiceNow when the one-time access is approved or denied. ServiceNow notifies the IT-user on approval with links to enable secure access or password checkout through Centrify.



Benefits for IT management

- Control privileged access to critical assets
- Leverage ServiceNow's strong workflow capabilities
- Ensure policy compliance and security
- Deliver a modern service experience for controlling privileged access
- Significantly reduce IT service requests by leveraging ServiceNow

Benefits for IT-users

- Simple request process for gaining privileged access to critical assets
- No need to store or remember shared account credentials

Benefits of Centrify for ServiceNow

- End-Users get a single sign-on access experience for ServiceNow and all business applications (such as Office 365, Salesforce) hosted in the cloud or the data center
- Centrify ensures users only gain access to applications as defined by enterprise security policy
- Centrify adds strong authentication to ServiceNow and other applications, using its built-in and easy-to-use multi-factor authentication
- IT Management controls IT-user privileged access to critical resources, minimizing the attack surface and reducing risk using a streamlined request and approval system, leveraging identity policies in existing Active Directory, LDAP, or the Centrify Cloud Directory

Centrify
THE BREACH STOPS HERE

As the only industry recognized leader in both Privileged Identity Management and Identity-as-a-Service, Centrify provides a single platform to secure every user's access to apps and infrastructure in today's boundaryless hybrid enterprise through the power of identity services. This is the Next Dimension of Security in the Age of Access.

Founded in 2004, Centrify is enabling over 5,000 customers, including over half the Fortune 100, to defend their organizations. Centrify is a privately held company based in Santa Clara, California. To learn more visit www.centrify.com. The Breach Stops Here.

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

BRF003739EN-01102018