

Centrify DirectControl centrally secures privileged user access to cross-platform systems and applications by leveraging Active Directory

Centrify DirectControl centralizes authentication and privileged user access across disparate systems and applications by extending Active Directory-based authentication, enabling single sign-on and use of Windows Group Policy. With DirectControl, enterprises can easily migrate and consolidate complex UNIX-based environments into Active Directory, allowing organizations to easily establish global UNIX identities, centrally manage exceptions on legacy systems and delegate administration. DirectControl's non-intrusive and organized approach to identity and access management results in stronger security, improved compliance and reduced operational costs.

Centrify DirectControl is part of Centrify Suite 2012. From the data center and into the cloud, more organizations rely on Centrify Suite to secure authentication, enable single sign-on, consolidate identities, manage privileged users and audit user sessions.

BEFORE CENTRIFY

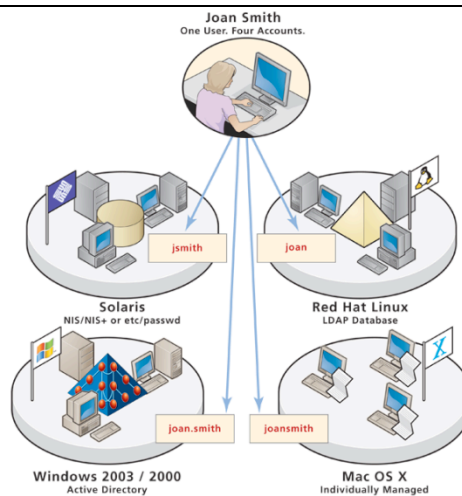
One User. Multiple Accounts. Separate Identity Silos.

The Challenge

Security. Legacy identity silos, such as /etc/passwd, are not secure. Fractured identity silos make de-provisioning complex, creating a major security risk of unauthorized access from shared or orphan accounts.

Compliance. No central place for access and policy enforcement and no way to support compliance reporting across systems.

Operational Costs. Administrators have too many systems to manage, no consistent way to manage systems and a burdensome helpdesk load.



AFTER CENTRIFY

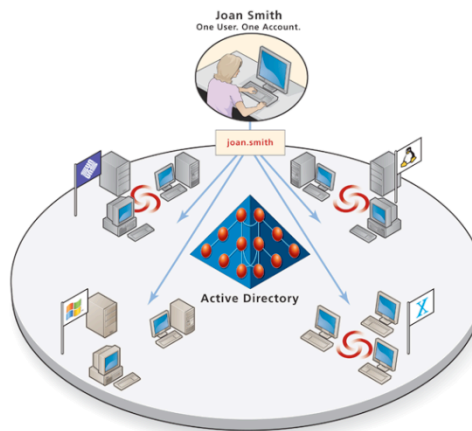
One User. One Account. One Directory Infrastructure.

The Solution

Cross-Platform Security. Eliminate unsecure identity stores, such as NIS, and provision access across UNIX, Linux and Mac through one Active Directory account.

Built for Compliance. Patented Zone feature enables granular access control to limit access to only what is required for the job function. Centralized reporting gives an up-to-date picture of who has access to what systems.

Reduced Operational Costs. One directory infrastructure streamlines IT operations with a single set of administrative tools and processes. Single sign-on enhances user productivity and reduces helpdesk burdens.



DirectControl Benefits

Strengthen Security.

Centrify's patented Zones feature enables easy setup of privileged user access, providing a least-access model to systems and applications by organizational role and permitting delegated administration according to security best practices.

Reduce Operational Costs.

DirectControl reduces the cost of operating non-Windows systems by leveraging the authentication and Group Policy of your existing Active Directory infrastructure and eliminating costly legacy infrastructure such as NIS.

Improve Compliance.

DirectControl improves compliance by limiting the access rights of privileged users, consistently applying security policy across platforms and providing the detailed and specific reports on access controls that auditors demand.

Non-intrusive and broadest platform set.

DirectControl does not require intrusive changes to your systems, applications and Active Directory environment while supporting over 350 platform releases.

Why Customers Choose DirectControl

Here's why more than 3,500 customers say that DirectControl is the only solution that meets their requirements.

Requirement	Compelling Reason
Strengthen Security	<ul style="list-style-type: none"> Simplifies de-provisioning of user access across non-Windows systems Least-access model ensures privileged users can access only the systems and applications required to do their job Local system enforcement through Adclient deployed on-premise and in cloud computing environments
Reduce Operational Costs	<ul style="list-style-type: none"> Migrate and eliminate NIS Delegate administration of users, systems and applications across non-Windows systems Kerberos-based single sign-on reduces helpdesk costs and enhances user productivity
Improve Compliance	<ul style="list-style-type: none"> Centralized reporting of system access and policy provides proof of compliance for PCI, SOX, FISMA, HIPAA and more Consistent and easy to manage security policies across UNIX, Linux and Mac OS X
Non-intrusive and broad platform support	<ul style="list-style-type: none"> No Active Directory schema changes required to store UNIX profiles or support advanced features Nothing to install on domain controllers Low overhead agent is easy to install and manage across systems 350 + UNIX and Linux releases supported – more than any other vendor

DirectControl Features

- Use DirectControl Zones to easily migrate and centralize complex and siloed UNIX identity stores
- A Global Zone enables the enterprise to define a consistent UNIX identity namespace for new users and systems
- Centrally manage system overrides to easily migrate and manage legacy systems without modifying existing UNIX profiles
- Child Zones inherit identities and role assignments within the Centrify Zones hierarchy
- UNIX Profile Variables enable the granular assignment of UNIX profile attributes

Supported Platforms

Over 350 Linux, UNIX & Mac Systems, including:

Apple Mac OS X
 CentOS Linux
 Citrix XenServer
 Debian Linux
 Hewlett Packard HP-UX
 IBM AIX
 Linux on IBM System z
 Mandriva Linux One
 Novell SUSE Linux
 OpenSUSE Linux
 Oracle Enterprise Linux
 Oracle OpenSolaris
 Oracle Solaris
 Red Hat Enterprise Linux
 Red Hat Fedora
 Red Hat Linux
 Scientific Linux
 Silicon Graphics IRIX
 Ubuntu Linux
 VMware ESX Server

SAP, Web Apps & Databases

Apache HTTP Server
 Apache Tomcat
 IBM DB2
 IBM Informix
 IBM WebSphere
 JBoss AS
 Oracle Database 10g
 Oracle WebLogic
 SAP

64-bit support is available on all major platforms.

For a detailed list of supported releases go to:

www.centrify.com/platforms

DS-001-2011-10-10

How Centrify DirectControl Works

