

# Centrify DirectAuthorize centrally manages and enforces role-based entitlements for fine-grained control of user access and privileges on UNIX and Linux systems

According to Gartner<sup>1</sup>, UNIX and Linux systems inherently lack a scalable and simple model for administrative delegation, and organizations that give too many users root permission run unnecessary security risks and will invariably fail audits. By controlling how users access systems and what they can do, DirectAuthorize enables organizations to lock down sensitive systems and eliminate uncontrolled use of root accounts and passwords. Key features include:

## ROLE-BASED PRIVILEGE MANAGEMENT

### Grant users rights to execute commands with elevated privileges, eliminating the need for access to privileged accounts and passwords

IT security administrators can define rights to execute specific privileged commands, storing the required account information securely in Active Directory. Once that right is assigned to a role, users or groups in that role can execute the privileged command without having to switch accounts or know the passwords of privileged accounts. For example, a backup operator role can be granted the right to execute backup commands with enough privilege to ensure all files are backed up – without needing the root password.

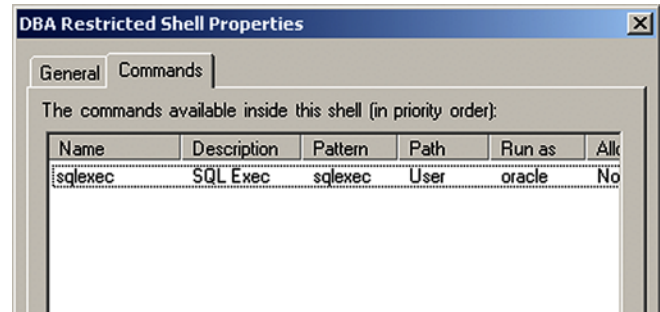
### Assign users a Restricted Environment with access only to a specific “whitelist” of commands

To completely lock down sensitive systems, DirectAuthorize’s unique Restricted Environment further enables IT security administrators to limit users or groups within a role just to specific commands. For example, a database administrator role can be assigned a Restricted Environment that permits only database-related commands.

### Simplify the execution of privileged commands

Users in a Restricted Environment no longer need to switch to root or other privileged accounts in order to run commands that require privilege. Instead, users can simply log in with their Active Directory account and seamlessly execute, with privilege, the commands available to them within their role without changing their behavior or learning to use a new command like sudo.

<sup>1</sup> Gartner Research ID # G00130427



## ROLE-BASED ACCESS CONTROLS

### Lock down sensitive systems with fine-grained controls that set who can access a system and how

DirectAuthorize is a seamlessly integrated component of the Centrify Suite. It adds finer-grained access controls by enabling IT security managers to define user roles within a specific Zone. The role specifies which PAM-enabled interfaces or applications a user in that role can use to access systems in the Zone (for example, a backup operator may have access only through SSH).

### Set time windows when a role can access a system, and set time periods when a role assignment is active

DirectAuthorize roles can, for example, specify that a backup operator can log in to systems within a Zone only on Wednesdays and Fridays between 5-9 p.m. A contract system administrator’s account could be set to a start date of August 4th and an expiration date of August 29th. Modeled on the same Active Directory settings available for Windows accounts, DirectAuthorize’s date- and time-based access settings enable consistent, role-based policy enforcement across your heterogeneous enterprise.

### Tie users’ UNIX and Linux entitlements to centrally managed Active Directory identities for a global view of entitlements across the enterprise

DirectAuthorize entitlements are assigned to users and groups that are centrally administered from Active Directory. Thus authentication, access controls and authorizations are tied to a single Active Directory identity, providing the accountability that is the heart of IT security and compliance best practices.

## Centrify DirectAuthorize's Unique Benefits at a Glance

DirectAuthorize is a component of the Centrify Suite, which provides a single, unified architecture for access control, authentication, authorization and auditing. In working with customers to understand their IT security and compliance challenges, we focused on delivering the following benefits:

### Centralized, role-based management designed for compliance

- Consolidates UNIX and Linux entitlement management in Microsoft Active Directory, streamlining administration and closing security gaps caused through lax deprovisioning and change management practices
- Links entitlements to Active Directory accounts and groups, enhancing accountability and compliance reporting through a global view of users' entitlements across the enterprise
- Role-based entitlement model meets regulatory requirements for defining "least access" controls and administrative privileges delegated according to job duty
- Restricted Environment feature permits users to execute only specific "whitelisted" commands, resulting in unambiguous compliance reporting compared to systems that require you to pile on "deny" specifications
- Built-in reports for users and computers give auditors a complete view of authorizations

### Simplified privilege management that goes beyond existing products

- Graphical user interface makes creating and managing roles and rights far easier compared to complex sudo policy config files or other solutions' proprietary scripting languages that can only approximate the rich modeling available via Active Directory
- Unique ability to control users' access to secured systems via PAM-enabled apps and interfaces (SSH, FTP, etc.)
- Unique Restricted Environment feature provides the option to restrict users to a "whitelist" of specific commands, compared to older, cumbersome and error-prone solutions that permit all actions except those that are put on a "deny" list
- Simplifies users' workflow, enabling them to execute commands with privilege without having to change accounts or remember additional passwords or learn new commands

### Single, cost-effective architecture for cross-platform authentication, access control and authorization

- Comprehensive privilege management provided as part of an integrated authentication, access control and authorization solution that is priced below what you would expect to pay for a single, older point product that addresses just one of these areas

- Part of a comprehensive suite designed from the ground up to seamlessly integrate with a wide array of UNIX and Linux systems with existing Active Directory infrastructure, tools and processes

### Rapid, non-intrusive deployment and management

- Leverages existing Active Directory domain controller infrastructure; no additional servers or network infrastructure needed

### DirectAuthorize's unique Restricted Environment feature

lets you specify the commands — and only the commands — available to a user. Here a DBA role is restricted to running the `sqlxexec` command using an Oracle account.

- No Active Directory schema changes required
- Does not require proprietary changes to UNIX kernel
- Streamlines IT management by leveraging existing Active Directory tools and processes
- Management data is stored in Active Directory, a modern LDAP database that has a rich ecosystem of available administration, provisioning and reporting tools

### Highly available and fault-tolerant

- Leveraging Active Directory domain controller infrastructure ensures high availability and fault-tolerant network connection
- Local caching ensures entitlements are enforced even in cases when the computer is disconnected

### About Centrify

Centrify is the leading provider of security and compliance solutions that centrally control, secure and audit cross-platform systems and applications using Active Directory.

To contact us at:

PHONE: +1 (408) 542-7500  
EMEA: +44 (0) 1344 317950  
EMAIL: [info@centrify.com](mailto:info@centrify.com)  
WEB: [www.centrify.com](http://www.centrify.com)

To get started, try our free version:

[www.centrify.com/express](http://www.centrify.com/express)

Copyright © 2005-2011 Centrify Corporation. All rights reserved. Centrify and DirectAuthorize are trademarks of Centrify Corporation.  
DS-014-2011-02-15