

What's New in Centrify Server Suite™ 2015.1

Centrify Server Suite Standard Edition

Desktop rights for Windows 8 and Windows Server 2012

The DirectAuthorize desktop right can now be enabled via Active Directory group policy on:

- Windows 8
- Windows 8.1
- Windows Server 2012
- Windows Server 2012 R2

This feature helps customers to quickly reduce identity related risks on Windows with minimal setup and configuration on the part of the customer's Centrify administrator. Desktop rights allow IT admins to safely use a non-privileged desktop for e-mail and Web browsing, and quickly change to a desktop with elevated privileges for IT system administration, all while retaining their unique Active Directory user identity for auditing and attribution.

Hadoop support

As part of Centrify's on-going commitment to enable customers to quickly secure authentication throughout their Hadoop deployments, the Centrify agent now provides infinite renewal of the user's Kerberos's Ticket Granted Ticket (TGT) for a user who has logged out while his Hadoop job is still running, enabling the completion of Hadoop jobs that extend beyond the period of the Kerberos TGT.

Smart card and certificate management

This release supports Microsoft Authentication Mechanism Assurance for smart cards. This enables single sign-on systems to validate that the user's initial logon to a server or workstation was performed with a smart card and PIN.

The Centrify agent now supports the SHA-2 (Secure Hash Algorithm) cryptographic hash function for signing the Certificate Signing Request (CSR) in certificate auto-enrollment using the version 3 template. This update is consistent with guidance from NIST regarding the deprecation of SHA-1 and the implementation of SHA-2.

Case is now ignored by default for user names of smart card users to improve compatibility with some operating systems where the use of upper case characters will cause login to fail (e.g. RHEL 7.0).

OpenSSL has been upgraded to version 0.9.8zf in this release.

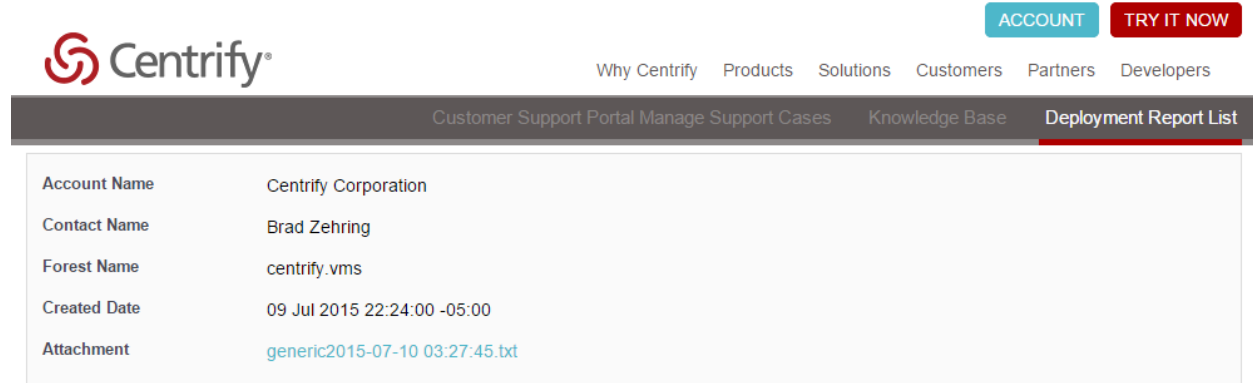
Enhancements to DirectManage Access Manager

When zone-enabling a user, the validation logic now checks if the user's login name or `unixname` matches the `samaccountname` of another user in the same domain in order to help avoid confusing user naming practices.

Centrify PuTTY has been upgraded to version 0.64.

Enhancements to Deployment Report

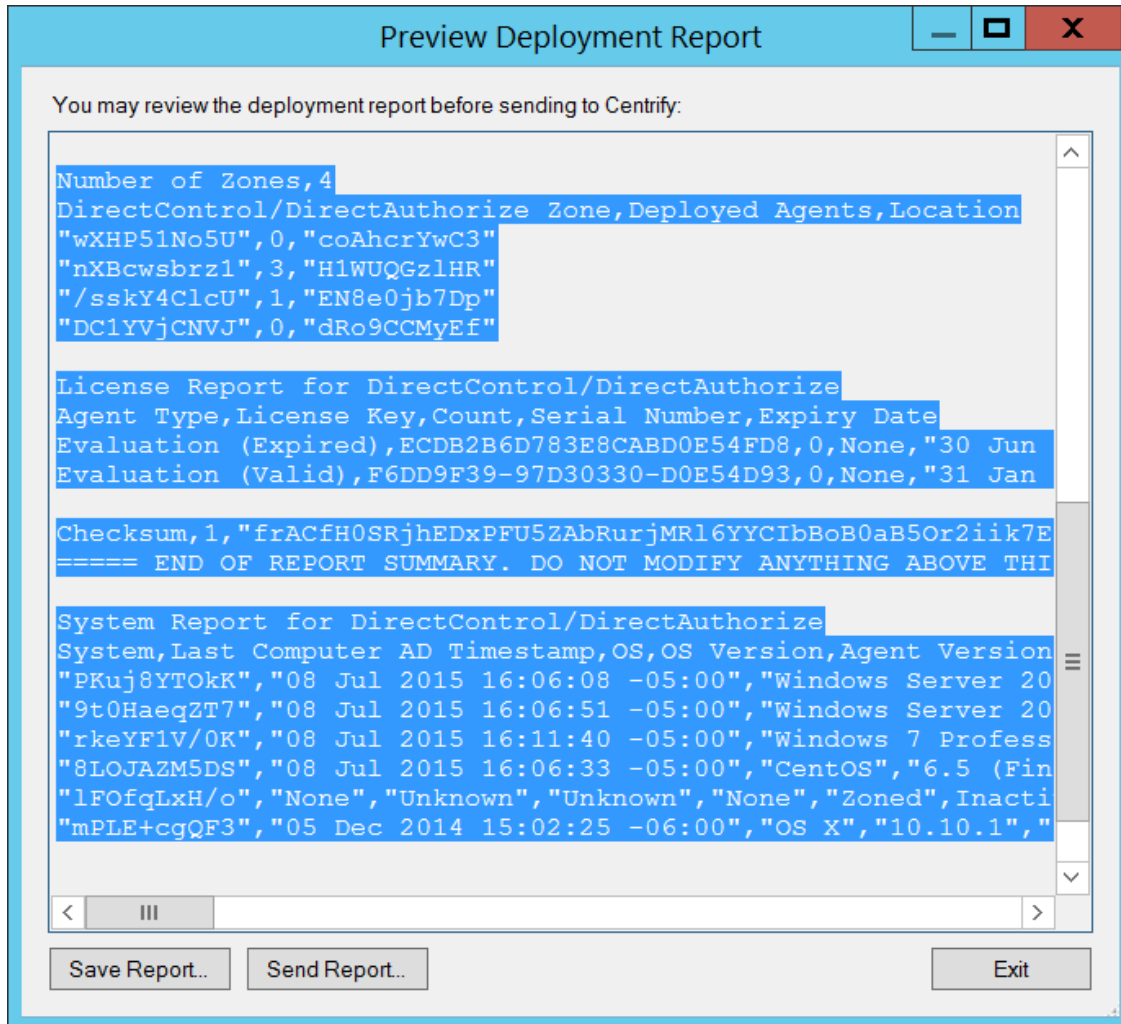
You can now send a deployment report directly to the Centrify Support Portal, where the report will automatically be validated and processed for you.



The screenshot shows the Centrify Customer Support Portal interface. At the top right, there are buttons for 'ACCOUNT' and 'TRY IT NOW'. The navigation menu includes 'Why Centrify', 'Products', 'Solutions', 'Customers', 'Partners', and 'Developers'. The main content area is titled 'Deployment Report List' and displays a table with the following information:

Account Name	Centrify Corporation
Contact Name	Brad Zehring
Forest Name	centrify.vms
Created Date	09 Jul 2015 22:24:00 -05:00
Attachment	generic2015-07-10 03:27:45.txt

You can preview the report prior to sending. By default, computer names are obfuscated.



The screenshot shows a 'Preview Deployment Report' dialog box. The title bar reads 'Preview Deployment Report'. The main content area contains the following text:

```
You may review the deployment report before sending to Centrify:

Number of Zones,4
DirectControl/DirectAuthorize Zone,Deployed Agents,Location
"wXHP51No5U",0,"coAhrYwC3"
"nXBcwsbrz1",3,"H1WUQGz1HR"
"/sskY4ClcU",1,"EN8e0jb7Dp"
"DC1YVjCNVJ",0,"dRo9CCMyEf"

License Report for DirectControl/DirectAuthorize
Agent Type,License Key,Count,Serial Number,Expiry Date
Evaluation (Expired),ECDB2B6D783E8CABD0E54FD8,0,None,"30 Jun
Evaluation (Valid),F6DD9F39-97D30330-D0E54D93,0,None,"31 Jan

Checksum,1,"frACfH0SRjhEDxPFU5ZAbRurjMR16YYCibBoB0ab5Or2iik7E
===== END OF REPORT SUMMARY. DO NOT MODIFY ANYTHING ABOVE THI

System Report for DirectControl/DirectAuthorize
System,Last Computer AD Timestamp,OS,OS Version,Agent Version
"PKuj8YTOkK","08 Jul 2015 16:06:08 -05:00","Windows Server 20
"9t0HaeqzT7","08 Jul 2015 16:06:51 -05:00","Windows Server 20
"rkeYF1V/0K","08 Jul 2015 16:11:40 -05:00","Windows 7 Profess
"8LOJAZM5DS","08 Jul 2015 16:06:33 -05:00","CentOS","6.5 (Fin
"lFOfqLxH/o","None","Unknown","Unknown","None","Zoned",Inacti
"mPLE+cgQF3","05 Dec 2014 15:02:25 -06:00","OS X","10.10.1","
```

At the bottom of the dialog box, there are three buttons: 'Save Report...', 'Send Report...', and 'Exit'.

You can now determine license usage of Centrify Server Suite Standard Edition using the currently logged in user credential.

Deployment Report now shows whether a computer is using a workstation or server license.

The Active Directory forest name is no longer obfuscated in the deployment report.

You can now launch the Deployment Report utility in silent mode. Please see the utility's command-line help page for command usage.

Group policy for Centrify PuTTY

The default for `Auto-login username` is now `User principal name` (require `DirectControl`).

Centrify OpenSSH upgrade

Centrify OpenSSH is now based on open source version 6.7p1 of OpenSSH.

Centrify LDAP Proxy

This release adds support for:

- Packet data signing
- The auto-private group
- Configuration for `autofs` to get maps via LDAP.

Enhancements to scripts and command line utilities

- `Addns` has new options for using the target interface name and ignoring certain error conditions when updating a record.
- `Adflush` has a new option to clarify whether a cache will be completely removed.
- `Adinfo` has a new option to show the suite version.
- `Adjoin` has a new option to specify a pre-existing computer role.
- `Adlicense` has a new option to change the customer-defined license type.
- `Adlicense` has a new option to display the license mode and type.
- `Adedit` now supports provisioning attributes from the Zone Provisioning Agent (ZPA).
- `Admigrate` now copies and migrates the ZPA provisioning attributes in the zone container.

Enhancements to configuration parameters

New parameters enable new options for how Server Suite will act in certain deployment use cases.

- Whether `adclient` will perform a "Logon Hours" restriction check in addition to Active Directory.
- Whether domain controller and global catalog lookup are restricted to a specific site list, to improve performance where network latency is an issue.
- Whether Kerberos Ticket Granting Tickets will be automatically renewed for certain users and groups (even after they have logged off) in order to assure completion of Hadoop jobs.
- Whether a script will define how the user's home directory will be created.

Centrify PAM plug-in

Two new options have been added in regard to checking for password expiration. The plug-in can now check for expiration even before attempting user authentication, which is useful for Web applications where it is not possible to prompt the user to change passwords; and, it can now skip checking for password expiration entirely.

Access Module for PowerShell

Cmdlets have been enhanced to show effective rights from a computer role and support generation of a UID or GID using Apple's scheme in Centrify classic zones.

Centrify Server Suite Enterprise Edition

Improved performance and scalability for auditing

Significant performance and scalability improvements were made across the audit infrastructure, including *nix agents, collectors, and audit store databases.

Better support for troubleshooting on Windows endpoints

You can now control the ability to start and stop the Windows DirectAudit Agent by Active Directory group policy. IT admins who are enabled by group policy can use the Agent Control Panel to turn audit services on or off, making it easier to troubleshoot endpoints.

Enhancements to Audit Analyzer and Session Player

- Report generation progress is now shown in the status bar of the Audit Analyzer.
- Column filtering has been added to the Audit Analyzer query result pane.
- New and changed columns in session auditing now distinguish between the actual user and the shared account used to log into a resource by Centrify Privilege Service™.
- In the display of audit store databases, a new column "Effective Size" has been added to show the size of data in the database.
- Audit Analyzer now gives better feedback in the user interface when exporting a large number of sessions.
- You can now search for audited sessions using a user's display name as search.

Enhancements to Audit Manager

- New options enable support for segregation of duties by prohibiting a person in an auditor role from viewing or deleting sessions of their own activity.
- Column filtering has been added to the Audit Manager query results.
- You can now see when the last agent/collector update was recorded in the audit store database.
- You can now define an audit role using Active Directory security groups as one of the search criteria, enabling you to search for audited sessions of users that belong to a particular Active Directory security group. Note: This feature was added in the previous release of Server Suite 2015.
- You can now assign "View" permission to one or more users, which limits these users to read-only access to the Audit Manager console.

Centrify *nix Agent for DirectAudit

- Two new Active Directory group policies have been added for setting client idle timeout and agent status timeout values.
- A new resource monitor has been added to monitor CPU, file descriptor and memory usage during runtime, and restart services if possible.
- Detection of free disk space has been improved.
- Informational display from the DirectAudit daemon has been improved, and the daemon is now under more accurate control and reporting of its state.
- New options have been added to control user login in specific shells.
- New options have been added to restrict processing of account information in certain conditions.
- Improvements have been made to make it easier to determine the suite version number from the command line.
- NSS query performance for the local user has been improved.
- General modification of any DirectAudit for UNIX group policy value is now possible through configuration.
- New parameters were introduced in `centrifyda.conf` to support new options and features. For details, please refer to the Release Notes and the [Configuration and Tuning Reference Guide](#).

Database changes and improvements

DirectAudit database stored procedures can now be run under a user-specified service account, making it easier to comply with organizational security policies.

Database performance when storing audit session data has been improved significantly. This allows a higher number of DirectAudit agents to be supported in an audit store database instance.

Performance when updating session review status in Audit Analyzer has been improved.

Performance when querying audit data in Audit Analyzer has been improved.

Version detection has been added to validate that the Centrify SDK aligns with the version of the DirectAudit database prior to database rotation.

A new scheduled task has been added to the Audit Management Server component to calculate the approximate amount of disk space taken by an audited session on the database server.

The default SQL Connection timeout has been changed to 30 seconds to improve system reliability.

FindSessions Tool

The FindSessions utility's search result pane will now allow a user to copy the session URI and display the session's indexed commands/events list.

Windows DirectAudit Agent

Active Directory users and groups now have the ability to stop the DirectAudit Windows Agent when permitted by group policy.

The DirectAudit Windows agent heartbeat rate default interval has been lengthened to decrease network traffic over limited-bandwidth connections.

Centrify Audit Module for PowerShell

Enhancements include:

- A new cmdlet to physically remove database files from the server.
- A new sample script to illustrate how to perform database rotation.
- The ability to search sessions by the user's display name.

Deployment Manager

Deployment Manager now supports the SHA-2 Secure Hash Algorithm for key exchange. In previous versions of Deployment Manager only the SHA-1 algorithm was supported.

Note: Because of this change, Centrify strongly suggests you upgrade to this new version of Deployment Manager (version 5.2.3) in order to successfully use Deployment Manager with the *nix client installation packages for Server Suite 2015.1.

In addition:

- The workstation or server license type for the computer can now be configured using `adjoin`.
- PuTTY in Deployment Manager has been upgraded from version 0.63 to version 0.64.
- Users can now group computers into custom groups and operations can be performed on these groups.
- `Connect Prompt` and `Connect Expects` can now be configured in both the option page and the computer property page.

Supported Platforms

Support has been added for the following operating systems:

- CentOS 7.1 (x86_64)
- Citrix XenServer 6.5 (x86_64)
- Debian Linux 8.x (x86, x86_64)
- Fedora 22 (x86, x86_64)
- Oracle Enterprise Linux 7.1 (x86_64)
- Red Hat Enterprise Linux Desktop 7.1 (x86_64)
- Red Hat Enterprise Linux Server 7.1 (x86_64)
- Red Hat Enterprise Linux Server 7.1 (ppc64)
- Scientific Linux 7.1 (x86_64)
- Ubuntu Desktop 15.04 (x86, x86_64)
- Ubuntu Server 15.04 (x86, x86_64)

Deprecated Platforms for Windows

- Windows Server 2003 and 2003 R2 are no longer supported by the Centrify Windows Agent 3.2.3 in Suite 2015.1.
- All 32-bit versions of Windows and Windows Server will not be supported after Centrify Windows Agent 3.2.3 in Suite 2015.1.
- All versions of Windows Server 2008 will not be supported after Centrify Windows Agent 3.2.3 in Suite 2015.1.

Note: Windows Server 2008 R2 64-bit version will continue to be supported.

Deprecated Features

ADM format files for Active Directory Group Policy

This is the last release in which Centrify Active Directory group policies will be defined in ADM (Administrative Template File) file format. Beginning with the next release of Server Suite, only ADMX (Administrative Template File XML based) format files will be included.

Desktop rights and the run-as account

Desktop rights on Windows using an Active Directory user account as the “run as” account will not be supported in the next release of Server Suite.

Note: Desktop rights using an Active Directory security group account as the “run as” account will continue to be supported.

Customized desktop backgrounds

Customized backgrounds for privileged desktops created by desktop rights on Windows will not be supported in the next release of Server Suite.

Contact Centrify

Centrify strengthens enterprise security by managing and securing user identities from cyber threats. As organizations expand IT resources and teams beyond their premises, identity is becoming the new security perimeter. With our platform of integrated software and cloud-based services, Centrify uniquely [secures and unifies identity](#) for both privileged and end users across today’s hybrid IT world of cloud, mobile and data center. The result is stronger security and compliance, improved business agility and enhanced user productivity through [single sign-on](#). Over 5000 customers, including half of the Fortune 50 and over 80 federal agencies, leverage Centrify to secure their identity management. Learn more at www.centrify.com.

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		