

Centrify Infrastructure Services 18.11 Agent for Windows 3.5.2 Release Notes

© 2007–2018 Centrify Corporation.

This software is protected by international copyright laws.

All Rights Reserved.

Contents

| | | |
|------|--|----|
| 1. | About Centrify Agent for Windows..... | 2 |
| 2. | Supported Platforms and System Requirements..... | 3 |
| 3. | Feature Changes..... | 3 |
| 3.1 | Feature Changes in Agent for Windows 3.5.2 (Release 18.11) | 3 |
| 3.2 | Feature Changes in Agent for Windows 3.5.1 (Release 18.8) | 4 |
| 4. | Bugs Fixed..... | 5 |
| 4.1 | Bugs Fixed in Agent for Windows 3.5.2 (Release 18.11) | 5 |
| 4.2 | Bugs Fixed in Agent for Windows 3.5.1 (Release 18.8) | 5 |
| 5. | Known Issues..... | 6 |
| 5.1 | Installation and Uninstall | 6 |
| 5.2 | Configuration | 7 |
| 5.3 | Environment | 8 |
| 5.4 | RunAsRole | 9 |
| 5.5 | Desktop with Elevated Privileges | 10 |
| 5.6 | Roles and Rights | 12 |
| 5.7 | Compatibility with 3 rd Party Products | 13 |
| 5.8 | Application Manager | 14 |
| 5.9 | Network Manager | 14 |
| 5.10 | Endpoint Enrollment | 14 |
| 5.11 | Centrify Agent for Windows | 14 |

| | | |
|----|---|----|
| 6. | Additional information and support..... | 15 |
|----|---|----|

1. About Centrify Agent for Windows

The Centrify Agent for Windows package contains software to support auditing, access control, and privilege management on Windows computers. Audit and Access features must be installed together but their services can be enabled separately on the Windows computers you want to manage.

For auditing, the Centrify Agent for Windows requires the Centrify Auditing & Monitoring Service feature set, which is available in Centrify Infrastructure Services. Centrify Auditing & Monitoring Service enables detailed auditing of user activity on a wide range of UNIX, Linux and Windows computers. With Centrify Auditing & Monitoring Service, you can perform immediate, in-depth troubleshooting by replaying user activity that may have contributed to system failures, spot suspicious activity by monitoring current user sessions, and improve regulatory compliance and accountability by capturing and storing detailed information about the applications used and the commands executed. If you enable auditing, the Centrify Agent for Windows records user activity on the Windows computer when it is installed.

For access control and privilege management, the Centrify Agent for Windows requires the Centrify Authentication Service and Centrify Privilege Elevation Service feature sets, which are available in Centrify Infrastructure Services. With Centrify Authentication Service and Centrify Privilege Elevation Service, you can configure and manage role-based access controls for Windows servers. The Centrify Agent for Windows extends the access control and privilege management features available for Linux and UNIX computers, so that you can use a single console to manage multiple platforms. You can deploy the Centrify Agent for Windows in a Windows-only environment or as part of a mixed environment that includes Windows, Linux, and UNIX computers.

Centrify Agent for Windows provides both privilege elevation and auditing functionalities, and for more information about the auditing feature, refer to the Centrify Auditing & Monitoring Service Release Notes for more detailed information.

You can obtain information about previous releases from the Centrify Support Portal, in the Documentation & Application Notes page.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

2. Supported Platforms and System Requirements

For the list of the supported platforms by this release, refer to the "Supported Platforms" section in the Centrify Infrastructure Services release notes.

For the platforms to be removed support in coming releases, refer to the "Notice of Termination Support" section in the Centrify Infrastructure Services release notes.

For a complete list of supported platforms in the latest releases, refer to the 'Centrify Infrastructure Services' section in the document available from www.centrify.com/platforms.

3. Feature Changes

3.1 Feature Changes in Agent for Windows 3.5.2 (Release 18.11)

- The Windows Agent will use subnet mask information from a connector together with the Active Directory Site information to prioritize the connection to the Centrify Connectors. (Ref: CS-46425)
- Added ability to specify an alternative user for Run with Privilege. Alternative user must be configured in Centrify and must provide valid credentials at the time the user invokes Run with Privilege. (Ref: CS-45742)
- Centrify added a group policy entitled "Configure Windows authentication user privilege elevation grace period". This group policy supports a kerberos authentication grace period for user privilege elevation, including runasrole, run with privilege, new desktop, and switch desktop. This group policy can be helpful to avoid re-authentication for alternate users. For example, if a role is configured to require re-authentication, an alternate user will be asked to authenticate twice: once to obtain the list of roles, and again when the user selects the role that has the re-authentication requirement. You can avoid the second authentication by configuring a user privilege elevation grace period. (Ref: CS-46619)
- Added an option to perform a local leave of the zone for cases when a user is experiencing problems removing the "Centrify Privilege Elevation Service" from the Agent Configuration. (Ref: CS-45186)
- The DZdiag command line utility and UI Diagnostics tool now includes information about whether an Offline MFA profile is configured. (Ref: CS-46763)
- You can access the troubleshooting tool directly from the Centrify Tray Icon context menu. (Ref: CS-46487)

- Added ability to specify and validate an ITSM ticket number for privilege elevation. (Ref: CS-46481, CS-45961)
- Added integration with McAfee Endpoint Drive Encryption software that enables features such as Auto Pre-boot and Password Synchronization. (Ref: CS-45515)
- Added support to configure a yubikey and use it as second factor for logging in to the offline system. (Ref: CS-46771)

3.2 Feature Changes in Agent for Windows 3.5.1 (Release 18.8)

- Added a warning prompt to install the Microsoft Hotfix described in this link, <https://support.microsoft.com/en-us/kb/3022752>, when a user is adding Centrify Privilege Elevation Service and the hotfix is not already installed. This resolves an issue where Users that had elevated Privileges did not have sufficient permission to access the "Security Settings" node in the local group policy editor on Windows 8.1 and Windows 2012 R2 (Ref: CS-9927, CS-45687)
- Command line tools DzJoin and DzLeave now support joining and leaving zones using custom credentials. Note that the specified user still needs to be in the local administrators group for these tools to be executed successfully. (Ref: CS-45993)
- For windows 10, the Windows Agent is no longer using Mobile Device Management (MDM) protocol to enroll as a Windows device. MDM features for Windows devices such as wipe device, device location, ping device are not available in the Centrify Identity Platform. (Ref: CS-45856)
- Improved the "Forgot password" interface in the Logon Screen to retry in the event of a password reset failure due to password complexity requirements. Note: This requires enabling the corresponding feature in the Centrify Portal. (Ref: CS-45642)
- Added a new group policy "Continue with MFA Challenges after failed windows authentication in Logon Screen" to control the behavior of MFA during logon whether to follow PCI DSS or NIST 800-53 guidelines or not. When this policy is set to Enabled, authentication on the Windows logon screen continues with MFA challenges even with the wrong password or use of expired/locked-out/disabled accounts. (Ref: CS-43817)
- Added a new group policy "Custom message for Locked User Accounts" to allow administrators to customize the message displayed to a user when the user's account has been locked out. (Ref: CS-45070)
- Endpoint enrollment for personal device is now available for Windows 7 and Windows 8.1 platforms. (Ref: CS-44997)
- Added a new System Right, "PowerShell remote access is allowed", enabling users assigned to the role with this right to have PowerShell remote access to the machine. (Ref: CS-45170)
- Removed the requirement that a user must be a local administrator in order to enroll their personal device to Centrify Identity Platform. (Ref: CS-44513)
 - Enrolling as a personal device requires the machine has been enrolled as corporate device
 - If the Group Policy "Disable endpoint enrollment automatically" is enabled, the user will not be able to enroll their device to Centrify Identity Platform

- o After enrolling a device into Centrify Identity Platform, it will be displayed as "Corporate" instead of "Personal" in the "Owner" column under "Endpoint Category"

4. Bugs Fixed

4.1 Bugs Fixed in Agent for Windows 3.5.2 (Release 18.11)

- Fixed an issue where the event log entry was not created when a local user failed to elevate with a role that requires MFA re-authentication. (Ref: CS-47271)
- Fixed an issue where after the Centrify Agent is installed a Windows 10 Notification Area setting "Select which icons appear on the taskbar" would stop showing the list of applications to select from. Please note that the Taskbar Settings is a UWP and is not supported in privileged desktop. (Ref: CS-46977)
- We have fixed the memory allocation issues related to Microsoft KB: KB5014697 (Win 11) / KB5014692 (Win10) / KB5014699 (Win2019) / KB5014702 (Win2016) KB updates.

4.2 Bugs Fixed in Agent for Windows 3.5.1 (Release 18.8)

- Fixed an issue where MFA would always be bypassed if the Centrify System Tray was not running and the screensaver was active. Now the Grace Period is always disabled and MFA will be enforced if the Centrify System Tray is not running. (Ref: CS-45932)
- To reduce confusion, the term "MDM Enrollment" has been replaced with "Endpoint Enrollment" in the Endpoint Enrollment Group Policy settings. (Ref: CS-45678)
- Fixed an issue where, in Agent Configuration, when changing tenant via Settings under "Centrify Identity Services Platform", the device would not unenroll the previous tenant which could lead to a discrepancy between the device and cloud portal. (Ref: CS-45428)
- Fixed an issue where Installing an IWA certificate into the current user's window certificate store instead of local machine's would fail to add "Centrify Identity Services Platform" services. (Ref: CS-45292)
- Fixed an issue where the user would be incorrectly prompted to restart the machine when changing zones using the dzjoin CLI even though a restart was unnecessary. (Ref: CS-45185)
- Fixed an issue where an audit notification message would incorrectly be displayed to users who were configured as 'audit not requested' (Ref: CS-44943)

5. Known Issues

5.1 Installation and Uninstall

- Upgrading from the beta build to this version may result in offline MFA mode if there are multiple authentication servers registered in your AD forest. To resolve this, uninstall the beta build first and then install this new version. (Ref: CS-41915)
- Upgrading Windows while the Agent is installed will result in a failure of the Windows upgrade. The workaround is to uninstall the agent before performing the upgrade or perform a fresh Windows install without keeping existing applications and settings. (Ref: CS-42200)
- Currently the MFA login feature is not supported on Windows Server 2016 "Server Core" systems. This feature component will not be installed on Windows Server 2016 "Server Core" systems. (Ref: CS-42192, CS-42527)
- The Centrify Common Component should be the last Centrify Server Suite component uninstalled. If the component is uninstalled before other component, it must be reinstalled by the uninstall process to complete its task. (Ref: 36226a)
- If you intend to install the software on the desktop with elevated privilege, you should not check the "Run with UAC restrictions" option when creating the desktop. (Ref: 39725b)
- When you double-click on the Centrify Agent for Windows msi and select the "repair" option, the existing files are replaced irrespective of their version number, even when they are identical. As a result, a prompt to restart the system is displayed as files that were in use were replaced. However, if you use the Easy Installer to do the repair and a file on the disk has the same version as the file that is part of the installer package, the installed file will not be replaced. Therefore, there will not be any prompt to restart the system. (Ref: 26561a)
- When the Centrify Agent for Windows is either installed or uninstalled and the prompt for a machine restart is deferred using the "restart later" option or ignored, other components of DirectManage may display errors due to an incomplete installation. A restart is mandatory if requested after install or uninstall operation. (Ref: 36307a)
- Users may notice a few "Side by side" configuration errors in the Event Viewer after installing the Centrify Agent for Windows, if Microsoft KB945140 related components have been installed on the local machine previously. These errors will go away after you restart the computer and have no functional effect. (Ref: 35302a)
- If you uninstall the Centrify Agent for Windows while the DirectAudit Agent Control Panel is open, files needed by the uninstall process may be blocked. You should close the DirectAudit Agent Control Panel for a successful conclusion to the uninstall process. (Ref: 25753a)
- If you have installed the Access feature of Centrify Agent for Windows from Centrify Server Suite 2013 and are trying to upgrade the component to the latest version, you may see the following error during the

installation process, "Service 'DirectAuthorize Agent' could not be installed. Verify that you have sufficient privileges to install system services." If you see this error message, it typically indicates that the existing service is taking longer time to stop and hence the new service is not getting installed. When you see this error, wait for some time (typically 30 seconds) and click on Retry button on the error message box. (Ref: 47270a)

- Centrify Agent for Windows and its installer are built on .NET. Therefore, .NET is always installed as a pre-requisite before the agent is installed. If .NET is removed from the system later, Centrify Agent for Windows will not run properly. User will also experience problem when trying to remove Centrify Agent for Windows from the system. To properly uninstall Centrify Agent for Windows, please make sure Centrify Agent for Windows is uninstalled before .NET. (Ref: 39051a)
- The list of rescue users is stored in different places in Suite 2013.3 (or previous releases) and Suite 2014 and this list is not automatically migrated to its new location when upgrading from Suite 2013.3 or a previous release to Suite 2014. Because of this, it's highly recommended that Centrify Agent for Windows should not be upgraded in disconnected mode (i.e. when the system cannot connect to the Active Directory). If a system is upgraded in disconnected mode, the list of rescue users will be lost and only local administrators will be able to login to the system after reboot. (Ref: 57622a)
- If you install Access feature of Centrify Agent for Windows without installing the Audit feature, the registry key value for HKEY_LOCAL_MACHINE\SOFTWARE\Centrify\AuditTrail\AuditTrailTargets is set to zero as expected, which means the audit trail is not sent to DirectAudit Audit Store database. However, if you try to change the installed features list of Centrify Agent for Windows and add the Audit feature later, the change process does not automatically set the AuditTrailTargets value to the expected new value of 1, which means to send audit trail data to DirectAudit Audit Store database. This is a known issue and workaround is to set this value manually to 1 after the installer finishes the process of adding new feature. (Ref: 59353b)
- If you have installed the Access feature of Centrify Agent for Windows from earlier version and then upgraded the component to the latest version while the Agent for Windows is not currently connected to any Active Directory domain controller, only users who have been assigned a role with rescue rights will be able to log on to the computer until the connection to Active Directory is restored. (Ref: 58858b)

5.2 Configuration

- In a cross-forest environment, forest A user cannot enroll a device joined to forest B when forest A does not have a connector. (Ref: CS-44805)
- When a machine that has MFA for Windows login enabled is reconfigured to connect to a different forest, the previous setting for the authentication server may no longer be valid. However, if there are Group Policy login

settings applied to the machine in the new forest, the new settings will be enabled when the Group Policy Editor refreshes. (Ref: CS-41928)

- In Windows 2016 and Win10, during the login process, selecting SMS or using other mechanisms like Security Question/Phone call/Password/Email/Mobile for MFA and clicking the "Commit" button will be intermittently unresponsive. (Ref: CS-41699)
- It can take a long time for users in offline mode to be re-prompted for their passcode.

In the event that the Agent cannot connect to the Centrify Authentication Server, and a user is required to enter an offline passcode, it can take up to several minutes for the agent to re-prompt for the passcode if the user enters it incorrectly. If the user tries to cancel login by pressing "back" or by switching the user, the login screen may become unresponsive. This time lag between an incorrect passcode and the re-prompt can also occur when a user incorrectly enters their offline passcode for privilege elevation. (Ref: CS-41302)

- Administrator should always leave the zone before joining the computer to a different domain. Otherwise, DirectAuthorize may not function correctly after the computer is joined to a different domain. (Ref: 54278b)
- In some large environment with multiple domain controllers, it may take up to one minute for the new zone setting in Centrify Agent Configuration to take effect. (Ref: 58128b)
- If one of the Global Catalog servers is unavailable, user may not be able to configure the zone for Centrify Agent for Windows. (Ref: 58621b)
- Microsoft normally automatically distributes and installs root certificates to the Windows system from trusted Certificate Authorities (CA) and users are seamlessly able to use a secure connection by trusting a certificate chain issued from the trusted CA. However, this mechanism may fail if the system is in a disconnected environment where access to Windows Update is blocked or this feature of automatic root certificate installation is disabled. Without updates on the certificate trust list (CTL), the default CTLs on the system may not be adequate for secure connections of Centrify multi-factor authentication especially for older versions of Windows such as Windows 7 and Windows Server 2008 R2. To ensure the success of Centrify multi-factor authentication, user may need manually distribute and install the latest CTLs and the required root certificate to systems in a disconnected environment. See Centrify KB-6724 for further information. (Ref: CS-39703)

5.3 Environment

- On Windows 10 and Win2K16 machines with Centrify Privilege Elevation Service, following will occur (Ref: CS-43883):
 - Pop up an error dialog several seconds after clicking "Open file location" in the context menu of a shortcut on the start menu. Explorer windows will display correctly.
 - No responses to the following actions

- Clicking "Open file location" in the context menu of a shortcut on desktop
 - Clicking "Open file location" in the context menu of a shortcut on the Centrify Start menu in the Privileged Desktop
 - Slow response to "OK", "Cancel" in the shortcut property page after "Open file location" in the general tab is clicked. The dialog will close after several seconds.
- On some Windows 10 machines, the smart card login option may not be displayed if another credential method has been recently used. To display the smart card login option, remove and insert a smart card into the reader. This will cause the login screen to reload and will display the smart card login option. (Ref: CS-41282)
- Centrify Agent for Windows requires you to patch to at least build 10.0.14393 on Windows 10 and Windows Server 2016 to use MFA features. (Ref: CS-41387)
- Selective two-way external trusts are not supported. Both Windows machines and Centrify zones are required to be in the same forest or different forests with a two-way forest trust established. (Ref: 40713b, 44644b, 44647b, 44657b, 40643b, 40650b, 45341b, 45372b)
- Environment with no Global Catalog is not supported. (Ref: 46577a)
- DirectAuthorize for Windows requires machine time to be synchronized with domain controller. VMware virtual machine has a known issue that its time may not be synchronized with domain controller. This problem occurs more often on an overloaded virtual machine host. If the system clocks on the local Windows computer and the domain controller are not synchronized, DirectAuthorize for Windows does not allow any domain users to login. You can try the following KB from VMware to fix the time synchronization issue.
http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1189 (Ref: 47795b)

5.4 RunAsRole

- If you use the "RunAsRole.exe /wait" command to run a Python script, the input/output cannot be redirected for versions of Python below 3.0.0. (Ref: 45061a)
- Run As Role menu is not available on the start screen in Windows 8 or Windows 2012 or later because Microsoft doesn't support any custom context menu on the start screen. User has to go to the Windows desktop in order to launch an application using Run As Role context menu. (Ref: 35487a)
- On Windows 8, Windows 8.1, Windows Server 2012 and Windows Server 2012 R2, use "Run as role" with Local Administrators group privilege on Control Panel does not have sufficient permission to add printers if the printer drivers are not pre-installed on the computer. The workaround is to define a role run as a user with Local Administrator privilege or with a group as a member of Local Administrators group. (Ref: 68826a)

- The "Run as role" for Windows Media Player is not recommended. Please use privilege desktop instead. (Ref: 55615a)
- When running "RunAsRole.exe /wait sc.exe" with no argument provided to sc.exe, sc.exe will prompt

Would you like to see help for the QUERY and QUERYEX commands? [y | n]:

Typing 'y' or 'n' doesn't do anything because the input cannot be successfully redirected to sc.exe. (Ref: 47016b)

- It is not recommended to change zone via Run As Role since the role that is in use may no longer be available once after leaving from the previous zone during the change zone process. (Ref: 58043a)
- On Windows Server 2008 R2 and Windows 7, if the Agent machine has no internet connection and the .NET CLR settings (checkCertificateRevocationList) is set to True, the MFA authentication will be failed because the CLR is unable to verify the certificate through internet. The workaround is to enable the internet connection or turn off the CLR settings (set checkCertificateRevocationList to False which is also the default value). (Ref: CS-40147)

5.5 Desktop with Elevated Privileges

- In desktop with elevated privilege a mouse left click does not work for SysTray Icons that involve opening the WinRT(or new Window) UI. The Systray icons affect are Time, Volume Control, or any third party icons on Windows 10/2016. (Ref: CS-39454)
- Server Manager cannot be started on multiple desktops at the same time. The bug exists on Windows 2012R2, 2016. (Ref: CS-42060)
- On a desktop with elevated privileges on Windows 8, 10 & 2016, the search for files or folders will be intermittently disabled from the Start menu ("Start" menu > "Search" > "For Files or Folders..."). (Ref: CS-42066)
- On a desktop with elevated privileges, if you open the Task Manager and select "File > New Task" to run an application without selecting the "Create this task with administrative privileges" option, the application will be launched on the default desktop. This issue occurs when User Account Control (UAC) is enabled. (Ref: 32169a)
- If the sAMAccountName attribute of an Active Directory account is changed while the old account name is still cached on the computer, you may see the following error message when creating a new desktop or using "Run as role" with a right configured to run as the modified user account:

"Failed to open new desktop. Right xxx references bad user account."

The workaround is to restart the computer. (Ref: 35124a)

- On a desktop with elevated privileges, if you use "Control Panel > Programs > Programs and Features" to uninstall a program, you may see the following warning message and cannot uninstall the software.

"The system administrator has set policies to prevent this installation."

This issue happens when User Account Control (UAC) is enabled and when "Run with UAC restrictions" is selected when creating the new desktop.
(Ref: 33384a)

- When you open the Start menu "Help and Support" item on a desktop with elevated privileges, the Windows Help and Support is launched on the default desktop. Switch to the default desktop to view the information.
(Ref: 32147a)
- If you shut down, restart, or log off from a desktop with elevated privileges, all running applications are terminated forcibly without being prompted to save any open documents. (Ref: 40749a)
- You cannot launch Windows Security Options using "Start menu -> Windows Security" on a privilege desktop with elevated privileges when using a remote desktop connection. You must switch back to the default desktop to continue. (Ref: 45995b)
- Installation of IE9 on desktops with elevated privileges may cause the privileged desktop to become unusable. Use "RunAsRole" for installation of IE9 instead. (Ref: 44930a)
- You cannot use the Start menu option "Switch User" while you are using a role-based, privileged desktop. To use the "Switch User" shortcut, change from the privileged desktop to your default Windows desktop. From the default desktop, you can then select Start > Switch User to log on as a different user. (Ref: 39011b)
- On a DirectAuthorize desktop using a role with local administrator privilege, the Stand By option in the shutdown menu does not work. This is a known issue and will be addressed in future release. (Ref: 58280a)
- VMWare registers to run VMWareUser.exe on the guest operating system to enable user to copy and paste text between the guest and managed host operating systems. Creating multiple desktops with different user accounts causes multiple VMWareUser.exe are run in different user accounts in the same logon session. VMWareUser.exe cannot support this scenario and therefore an error message is displayed on the default desktop which blocks all the UI operation on the new desktop. To workaround this problem, user can disable the VMWare user program on the guest machine by deleting the registry value name "VMware User Process" from HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run. (Ref: 49268a)
- On a privileged desktop on Windows 8, Windows 8.1, Windows 2012 and Windows 2012 R2, you may not be able to access the VMware shared folder.
(Ref: 40686c)
- Windows logo key keyboard shortcuts are not supported on privileged desktop. Depends on the key and operation system, the shortcut could either have no effect or its effect is applied to the default desktop instead. (Ref: 47588b)
- A Start menu on privileged desktop on Windows 8, Windows 8.1, Windows 2012 and Windows 2012 R2, to make up for a limitation of Windows 8, Windows 8.1, Windows 2012 and Windows 2012 R2. In addition, navigating to a Modern

Start screen to use Modern-style apps from a privileged desktop is not possible from either the charm bar or using a Windows. Note: you must switch back to the default desktop in order to go to Modern Start screen. (Ref: 41245c)

- The Challenge Pass-Through Duration setting is currently not supported for Centrify Windows multi-factor authentication. The Challenge Pass-Through Duration setting does not require a user, who has successfully met a multi-factor authentication challenge, to re-authenticate through mfa to use an mfa-required right or role if that user chooses the same challenge mechanism when prompted within the duration specified in the setting. (Ref: CS-39432)

5.6 Roles and Rights

- No 'Require multi-factor authentication' system right for the predefined 'Windows Login' role. To define this system right for MFA, use the predefined Require MFA for logon role, or create a new custom role. (Ref: CS-40888)
- Windows Network Access rights do not take effect on a Linux or UNIX machines. If you select a role to start a program or create a desktop that contains a Network Access right, you can only use that role to access Windows computers. The Windows computers you access over the network must be joined to a zone that honors the selected role. The selected role cannot be used to access any Linux or UNIX server computers on the network. (Ref: 32980a)
- Network Access rights are not supported on the Windows 2008 R2 Terminal Server if "RDC Client Single Sign-On for Remote Desktop Services" is enabled on the client side. (Ref: 34368b)
- To elevate privileges to the "Run as" account specified in a Windows right, the "run as" account must have local logon rights. If you have explicitly disallowed this right, you may receive an error such as "the user has not been granted the requested logon type at this computer" when attempting to use the right. (Ref: 34266a)
- If your computer network is spread out geographically, there may be failures in NETBIOS name translation. If a NETBIOS name is used, Active Directory attempts to resolve the NETBIOS name based on the domain controller that the user belongs to, which in a multi-segment network might fail. Therefore, Network Access rights might not work as expected if the remote server is located using NETBIOS name. You may need to consult your network administrator to work around this issue. (Ref: 39087a)
- File hash matching criteria in the Application right is not supported for a file larger than 500MB. This is to make sure DirectAuthorize does not spend too much CPU and memory resources to calculate the file hash. User trying to import a file with the size larger than 500MB will see an empty value for the file hash field. (Ref: 56778a)
- For a small set of application, enabled matching criterion - "Product Name", "Product version", "Company", "File Version" or "File Description" of a Windows Application Right may fail to match after upgrading agent

under the following conditions: - Any value for the enabled matching criteria is defined by either import from a process or file - The matching criteria is defined by 5.1.3 or 5.2.0 DirectManage Access Manager since the number of affected application is expected to be relatively low, proactively updating the defined matching criteria of Windows Application Right is not necessary. (Ref: 60053a)

- Smart card users can continue to use their own smart card to logon, but there will be no Centrify MFA features applied to smart card users. (Ref: CS-41539)

5.7 Compatibility with 3rd Party Products

- MFA may be skipped when connecting through XenDesktop because the Citrix Credential Provider may be used instead of the Centrify Credential Provider. The workaround is to disable the Citrix Credential Provider through the Group Policy "Centrify Settings\Windows Settings\MFA Settings\Specify the credential providers to exclude from the logon screen." (Ref: CS-46744)
- Even when Windows Chrome Update is run from a privileged desktop it will unexpectedly launch the Chrome browser in default desktop at the end of the installation. (Ref: CS-45503)
- VirtualDesktop is not compatible with Centrify Agent for Windows. Users should use the Centrify system tray applet to create virtual desktop instead. (Ref: 44641b)
- Attempting to launch SCOM Operation Console on privileged desktops will fail if there is an existing instance on other desktops and a new SCOM Operation Console will be started on the desktop with the existing instance. The workaround is to close all existing instances before starting a new SCOM Operation Console. (Ref: CS-43790)
- The startup path for "SharePoint 2010 Management Shell" and "Exchange Management Shell" may set to C:\Windows instead of user home directory if it is launched via RunAsRole.exe or from a desktop with elevated privilege. (Ref: 38814b, 46943b)
- On a desktop with elevated privileges, if you install McAfee Security Scan products and click "View Readme", the Readme.html is shown on the default desktop. Similar issues may happen with other third party programs. The alternate way to view the Readme.html on the desktop of a managed computer is to open the Readme.html file directly. (Ref: 34642a)
- Attempting to enable Kerberos authentication for Oracle databases will fail. This issue is being brought to the attention of Oracle Support for a resolution in upcoming releases. (Ref: 33835b)
- The Microsoft Snipping Tool utility has a bug that prevents it from running on a desktop with elevated privileges. (Ref: 31931a)
- Some applications do not use the process token to check the group membership. They check the user's group membership on its own. Therefore, any Windows rights configured to use a privileged group will not take effect in these applications. The workaround is to use a privileged user account instead of a privileged group. Here is the list of known application with this issue:

1. vCenter Server 5.1
2. SQL Server
3. Exchange 2010 or above

4. SCOM 2007

(Ref: 45318a, 45218a, 43779a, 38016a)

- Privilege elevation using Windows Rights for Internet Explorer (IE) 7 is not supported. (Ref: 33425a)
- Privilege elevation using Windows rights for "Remote Desktop" is not supported. (Ref: 45222b)
- Privilege elevation using Windows rights for taskmgr.exe, explorer.exe, and cmd.exe are not recommended. A user granted privileges with Windows rights is implicitly granted to run any executable under the same privilege. (Ref: 45861a, 40525a)
- Users may notice an error and cannot install ActivClient after installing Centrify Agent for Windows. During the installation of ActivClient, it attempts to change the local security setting. However, there is a known issue for Centrify Agent for Windows of blocking the local security setting (Ref: 63609b). Therefore, users may not be able to install ActivClient successfully after installing Centrify Agent for Windows. We suggest installing ActivClient before installing Centrify Agent for Windows. If Centrify Agent for Windows has been installed, please uninstall it and follow the installation sequence suggested. This issue happens on Windows 8.1 and Windows 2012 R2 only. (Ref: 76016b)
- McAfee Virus scan enterprise blocks our kerberos/authentication binaries(Dzkerberos.dll & DzMsv1_0.dll) from loading into lsass.exe on Windows server 2008 R2 Sp1. (Ref: CS-42755)

5.8 Application Manager

- Application Manager does not support Server Core edition of Windows. (Ref: CS-40656)
- Application Manager may not be able to generate Audit Trail event for the uninstall, change or repair operations which require reboot. (Ref: CS-45641)

5.9 Network Manager

- Network Manager does not support Server Core edition of Windows. (Ref: CS-42675)

5.10 Endpoint Enrollment

- When a Windows machine is enrolled by a user as a personal device and subsequently that user is disabled, after upgrading the product, there is no way to let another user to enroll a personal device for that machine. The workaround is to remove the service "Centrify Identity Services Platform" in Agent Configuration and add that service again. (Ref: CS-44514)

5.11 Centrify Agent for Windows

- Auditing status is incorrectly displayed on Authorization Center and the desktop notification message when the following Group Policies are enabled:

- Audited user list
- Non-audited user list
(Ref: CS-46321)
- Centrify Agent for Windows installation may prematurely end on systems that have Citrix Virtual Delivery Agent version 7.9 or higher installed. Please refer to the Centrify Knowledge Base for possible workarounds to deploy Centrify Agent for Windows on systems affected by this issue. (Ref: CS-46288)

6. Additional information and support

In addition to the documentation provided with this package, see the Centrify Knowledge Base for answers to common questions and other information (including any general or platform-specific known limitations), tips, or suggestions. You can also contact Centrify Support directly with your questions through the Centrify Web site, by email, or by telephone.

The Centrify Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Centrify products. For more information, see the Centrify Resources web site:

www.centrify.com/resources

To contact Centrify Support or to get help with installing or using this version of Centrify Agent for Windows software, send email to Support or call **1-669-444-5200**, option 2.

For information about purchasing or evaluating Centrify products, send email to info.