



Server Suite

Upgrade Guide

Version: 2023.x

Publication Date: 6/3/2024

Server Suite Upgrade Guide

Version: 2023.x, Publication Date: 6/3/2024

© Delinea, 2024

Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

Table of Contents

Upgrade Guide	i
Upgrade and Compatibility Guide	1
Preparing For An Upgrade	1
Upgrading the Operating System	1
Upgrading Computers Accessed by Multiple Users	1
Compatibility Between Versions of Delinea Software	2
Finding Upgrade Packages	2
Disabling Command-line Auditing	3
Upgrading Delinea Management Services on Windows Computers	3
What Should You Upgrade First?	3
Updating Administrative Components	3
Access Control and Privilege Management Compatibility	4
Auditing Infrastructure Compatibility	4
Access Control and Privilege Management Compatibility	4
Auditing Infrastructure Compatibility	4
Upgrading Components Interactively	5
Upgrading Auditing Components Silently on Windows	5
Upgrading Auditing Infrastructure	5
Why Are There Formal Steps for Upgrading an Audit Installation	6
Upgrading Auditing Components in a Specific Order	6
Unsupported Configurations	6
Updating Auditing-Related Databases	6
Restarting Computer After Agent Upgrade	7
Updating Agents Out of Sequence	7
Best Practices for Upgrading Large Audit Installations	7
Upgrading Managed Computers	8
Using the install.sh Shell Script to Update Packages	8
Configuring install.sh to Run Without User Interaction	9
Using a Native Package Manager on Linux Computers	10
Upgrading Packages on a Linux Computer	10
Using a Native Package Manager on UNIX Computers	12
Upgrading Packages Individually on a UNIX Computer	12
Upgrading Agents on Solaris Systems	16
Upgrading and Migrating Solaris svr4 Packages to IPS on Solaris 11	16
Upgrading Managed Mac OS X Computers	18
Compatibility for Additional Packages	18
Should You Be Concerned About Compatibility?	18
Removing the CentrifyDC-samba Package	19
Compatibility for CentrifyDC-nis Package	19
Compatibility for CentrifyDC-krb5 Package	20
Compatibility for CentrifyDC-ldapproxy Package	20
Compatibility for CentrifyDC-openssh Package	20

Table of Contents

Compatibility for CentrifyDC-Apache and CentrifyDC-Web Packages	20
Upgrading Version-Dependent Packages	20
Working with Classic Zones After an Upgrade	20
What To Do If There Are Problems During an Upgrade	21
Remove and Re-install Authentication and Privilege	21
Remove and Re-install Delinea Audit and Monitoring Service	21
Remove and Re-install Agent Features	22
Known Issues	22
Installation and Uninstallation Issues	22
Configuration Issues	23
Environment Issues	24
RunAsRole Issues	25
Desktop with Elevated Privileges Issues	25
Roles and Rights Issues	26
Compatibility with Third Party Products Issues	27
Application Manager Issues	27

Upgrade and Compatibility Guide

The guide provides the following information:

- [Preparing for an Upgrade](#)
- [Upgrading Delinea Management Services on Windows Computers](#)
- [Upgrading the Auditing Infrastructure](#)
- [Upgrading Managed Computers](#)
- [Compatibility for Additional Packages](#)
- [What To Do For Problems During Upgrade](#)
- [Known Issues](#)

Preparing For An Upgrade

This chapter provides an overview of the upgrade process and a summary of the compatibility requirements between the core components of Server Suite software. You should review the information in this chapter before upgrading any components on the computers where Delinea software is installed.

Upgrading the Operating System

Upgrading the operating system (OS) on a managed computer can make major changes to the configuration files and utilities installed on it. In many cases, operating system upgrades and operating system patches can changes affect the behavior of Delinea software. If the behavior of Delinea software is modified because of an operating system upgrade, it is possible for users to be locked out and unable to access to computer resources. To prevent this from happening, Delinea recommends that you first remove any Delinea packages you have installed before upgrading the operating system, then reinstall the packages after the operating system upgrade has been completed and the computer has been verified to be operating normally.

You should note that removing Delinea software prior to applying operating system patches or upgrading the operating system is not required in most cases. However, because operating system changes can affect authentication and authorization services, it is considered a best practice to ensure the upgrade does not interrupt services for any users.

Upgrading Computers Accessed by Multiple Users

In most cases, you can upgrade Delinea software on computers that are accessed by multiple users without entering single-user mode. However, upgrading authentication, authorization, and auditing services on a computer can potentially prevent users from logging on or using computer resources. If possible, you should perform upgrades when other users who might access the computer are logged off, then reboot the computer after completing the upgrade.

You should note that having all users logged off and rebooting the computer after an upgrade are not required steps, but are best practices to ensure the upgrade does not interrupt services for any users. In most cases, users who are already logged on are not affected by the upgrade. However, users who attempt to log on while files are being replaced during the upgrade process might be temporarily locked out of the managed computer you are upgrading.

Compatibility Between Versions of Delinea Software

In most cases, newer versions of Delinea software releases are backward-compatible with previous versions, enabling you to mix and match components from different versions and upgrade components over time when it is convenient to do so. However, there are some limitations to take into account when mixing and matching versions, and these limitations might influence which components you upgrade and how quickly you upgrade from one version to another.

In most organizations, the agents you install on managed computers are upgraded on a staggered schedule while administrative tools are upgraded at a set time to take advantage of new features.

To ensure flexibility of the upgrade process:

- Agents are always backward-compatible with older versions of the administrative console.

However, using an older version of the administrative console with a newer agent limits the features and functionality available. If you are using an administrative console from version 2.x to manage zones, agents from version 4.x and 5.x must use the `--compat` option to join 2.x-compatible zones.

- Agents are always forward-compatible with the administrative console for one version.

You can upgrade the administrative console without upgrading agents at the same time. However, there are limitations to features and functionality when using older agents with an upgraded console. For example, agents from version 4.x cannot be included in hierarchical zones. In addition, some features require an upgrade. For example, if you want to use the Delinea Agent for Windows for access control and privilege management, you must either upgrade or remove the Delinea auditing service for Windows.

- Group policies are not guaranteed to be compatible with different agent and administrative console versions.

New group policies cannot be enforced on computers with an agent from a previous version of Delinea software. If a group policy is applied to a computer that has an older version of the agent, the policy is ignored. You should only apply group policies that are supported in both the agent and administrative console versions you are using.

Finding Upgrade Packages

You can find Server Suite and agent packages for all supported operating systems on the [Delinea Customer Download Center](#). From the Customer Download Center, you can choose to download individual agent packages one at a time or download an archive that includes agents for all operating systems at once.

At a minimum, you should download the Delinea Agent Installer and the ADCheck Diagnostic Tool. You can then use the `install.sh` shell script interactively or with the `centrify-suite.cfg` configuration file to install and enable features on the computers you want to upgrade. Delinea recommends that you use the `install.sh` shell script to install or upgrade all Delinea packages on managed computers, especially if you have multiple Delinea packages installed that you wish to upgrade. The `install.sh` installation script performs a thorough set of pre-installation and post-installation steps to ensure a successful installation or upgrade with minimal disruption to your environment.

Alternatively, you can use the native package manager for your operating system to upgrade the components you have installed. If you want to use a native package manager, see [Using a native package manager on Linux computers](#) for Linux computers or [Using a native package manager on UNIX computers](#) for UNIX computers.

Disabling Command-line Auditing

If you have auditing enabled on a computer you are upgrading, you should check whether auditing is configured for individual commands or all user activity. If you have enabled auditing for specific commands, you should temporarily disable auditing on the managed computer before upgrading, then restart the auditing of individual commands after completing the upgrade. If you are auditing all user activity on a managed computer, you do not need to stop the auditing service. There will be a brief interruption while files are replaced, then auditing will continue without requiring you to manually restart it.

Upgrading Delinea Management Services on Windows Computers

This section describes how to upgrade Authentication & Privilege and Audit & Monitoring administrative components on Windows computers. It includes a more detailed discussion about compatibility between components.



In releases before 2017.2, you installed the DirectManage Access and DirectManage Audit sets of components. Those component areas have been renamed and are now called Authentication & Privilege and Audit & Monitoring, respectively.

What Should You Upgrade First?

You are not required to upgrade Delinea software components in any particular order. Depending on where you have components installed and how they are distributed, you might update components used for auditing before updating components for access control and privilege management. Alternatively, you might update one set of agents immediately, followed by one administrative console, then update other components at a later time.

Although there's no technical requirement to upgrade components in a specific order, most organizations upgrade one or more administrative consoles and components that might require changes to a database first—for example, Access Manager if upgrading access control and privilege management—then deploy upgraded agent software after upgrading all of other components.

Similarly, if you upgrading the auditing infrastructure, you might upgrade Audit Manager, the management database, and the audit store before upgrading collectors and agents.

Updating Administrative Components

As noted in General compatibility between versions of Delinea software, most organization upgrade the administrative consoles at a set time, often as part of planned maintenance, then upgrade agents opportunistically over a period of time. It is common, therefore, to have a mix of components from different versions of Delinea software within certain limits.

To help you plan for the upgrade, you should identify which versions of different components you currently have installed and which components will require an upgrade.

Depending on whether you are upgrading Authentication & Privilege, Audit & Monitoring, or both feature sets, you might have different compatibility requirements.

Access Control and Privilege Management Compatibility

You can upgrade to Server Suite—with Access Manager, version 5.1.x or later—to manage zones and agents (adclient) from version 3.x, 4.x, or 5.x. If you have agents from version 2.x, you must manage them using a console from version 4.x or earlier. If you use an older version of the console, you cannot take advantage of any features or enhancements introduced in newer versions of the console. If you upgrade to the latest release, you can continue to manage all of your currently deployed agents but must upgrade those agents to take full advantage of any new features.

You must upgrade UNIX, Linux, or Mac agents to 5.0 or later to use hierarchical zones. If you have zones from a previous release of Delinea software, you can use admigrate to convert those zones to hierarchical zones.

To manage Windows computers with Access Manager, the Delinea Agent for Windows must be version 3.0 or later.

Auditing Infrastructure Compatibility

You can upgrade to Server Suite—with Audit Manager, Audit Analyzer, and Collector service version 3.1.x or later—to manage auditing on UNIX, Linux, and Windows computers from version 2.x or 3.x. If you have agents from version 1.x, you must manage them using a console from version 1.x.

You must update the collector service to version 3.x to receive audit data from Windows computers with 3.x Windows agents.

Because the auditing infrastructure is a multi-tiered architecture that collects information to be preserved, reviewed, and archived, Delinea recommends a more formal upgrade process than for other components. This is especially true for larger organizations that collect a great deal of audit data. If you are upgrading the auditing infrastructure, therefore, see [Upgrading the auditing infrastructure](#) for more detailed information about the process to follow.

Access Control and Privilege Management Compatibility

You can upgrade to Server Suite—with Access Manager, version 5.1.x or later—to manage zones and agents (adclient) from version 3.x, 4.x, or 5.x. If you have agents from version 2.x, you must manage them using a console from version 4.x or earlier. If you use an older version of the console, you cannot take advantage of any features or enhancements introduced in newer versions of the console. If you upgrade to the latest release, you can continue to manage all of your currently deployed agents but must upgrade those agents to take full advantage of any new features.

You must upgrade UNIX, Linux, or Mac agents to 5.0 or later to use hierarchical zones. If you have zones from a previous release of Delinea software, you can use admigrate to convert those zones to hierarchical zones.

To manage Windows computers with Access Manager, the Delinea Agent for Windows must be version 3.0 or later.

Auditing Infrastructure Compatibility

You can upgrade to Server Suite—with Audit Manager, Audit Analyzer, and Collector service version 3.1.x or later—to manage auditing on UNIX, Linux, and Windows computers from version 2.x or 3.x. If you have agents from version 1.x, you must manage them using a console from version 1.x.

You must update the collector service to version 3.x to receive audit data from Windows computers with 3.x Windows agents.

Because the auditing infrastructure is a multi-tiered architecture that collects information to be preserved, reviewed, and archived, Delinea recommends a more formal upgrade process than for other components. This is especially

true for larger organizations that collect a great deal of audit data. If you are upgrading the auditing infrastructure, therefore, see [Upgrading the auditing infrastructure](#) for more detailed information about the process to follow.

Upgrading Components Interactively

You can upgrade components on any Windows computer interactively by clicking the links on the Server Suite Getting Started page. If the setup program detects components are installed, you have the option to update, modify, or remove those components. You can then follow the prompts displayed to review the components to be updated and complete the upgrade.

If the setup program detects components are installed, you are prompted to confirm that you want to continue with the upgrade. You can then follow the prompts displayed to review the components to be updated and complete the upgrade.

Upgrading Auditing Components Silently on Windows

If you want to perform a “silent” or unattended installation of the Delinea auditing components, you can do so by specifying the appropriate command line options and Microsoft Windows Installer (MSI) file to deploy. You can also use an unattended installation to automate the installation or upgrade on remote computers if you use a software distribution product, such as Microsoft System Center Configuration Manager (SCCM), to deploy software packages.

If you have the physical CD or ISO image for Delinea software, you can find the Microsoft Windows Installer (MSI) files for auditing components in subdirectories under the DirectAudit folder.

Before running the Microsoft Windows Installer (MSI) for any component, you should verify the computers where you plan to install meet the prerequisites described in the *Auditing Administrator’s Guide*.

To install the auditing components silently:

1. Open a Command prompt window or prepare a software distribution package for deployment on remote computers.

For information about preparing to deploy software on remote computers, see the documentation for the specific software distribution product you are using. For example, if you are using Microsoft System Center Configuration Manager (SCCM), see the Configuration Manager documentation.

2. Select the appropriate package for the auditing component you want to upgrade.

For example, locate the following file to install the audit management server on 64-bit operating systems:

Centrify DirectAudit Audit Management Server64.msi

3. Run the installer with no user interface and specify the package for the auditing component you want to upgrade.

For example, to upgrade an agent on 64-bit operating systems, run the following command:

```
msiexec /qn /i "Delinea Agent for Windows64.msi"
```

Upgrading Auditing Infrastructure

This chapter describes the recommended steps for upgrading auditing-related components to ensure you can continue auditing activity throughout the upgrade process. Keep in mind that upgrading the auditing infrastructure

might require updates to the existing database, but, in most cases, should not require any computers to be shutdown or restarted to complete the upgrade.

Why Are There Formal Steps for Upgrading an Audit Installation

In most organizations that deploy auditing, the auditing infrastructure—the installation—consists of components on multiple computers that must be able to communicate with each other to collect, transfer, and store information about user and computer activity. This multi-tiered architecture might be widely distributed and might include hundreds or thousands of computers that must be monitored. Upgrading all of those computers without interrupting ongoing auditing service requires a formal upgrade process that allows computers from different versions to continue communicating for a period of time.

Upgrading Auditing Components in a Specific Order

Because the upgrade process is expected to take a period of time—the length of time depends on the size and complexity of your installation—there are specific rules about the configurations supported and the order in which you should upgrade auditing components. To ensure auditing continues uninterrupted during the upgrade period, you should upgrade audit installation components in the following order:

1. Audit store databases
2. Management server databases
3. Consoles and collectors and the management server service
4. Agents

By following this upgrade order, you can ensure components can continue to communicate while you upgrade the rest of the audit installation. For example, an upgraded audit store can continue to receive audit data from collectors and respond to requests from the management server and consoles that have not be updated.

Be sure to upgrade all of your audit store databases before upgrading other components. You can upgrade the database without upgrading other components from a Command window by running the following command:

```
setup.exe /database
```

Unsupported Configurations

If you upgrade auditing components in a different sequence than the one described in Upgrading auditing components in a specific order, you might end up with an unsupported configuration that requires you to upgrade the remaining components immediately or suspend auditing of user activity until you can complete the upgrade.

You might encounter this situation if you upgrade the Audit Manager and Audit Analyzer consoles or a collector before upgrading the management and audit store databases.

Updating Auditing-Related Databases

If an upgrade requires an update to the database, you are prompted to run the database maintenance wizard and to select the databases to upgrade. If the wizard can connect to the databases selected and the database upgrade is successful, no further action is required.

You can upgrade audit store databases and the management database interactively using the Database Maintenance Wizard or by running the following command:

```
setup.exe /database
```

Upgrade and Compatibility Guide

Upgrading the auditing databases, however, requires specific Windows and database permissions. Before attempting to upgrade the database, verify that you have a user account that meets the following requirements:

- The Windows account you use to update the database with the Database Maintenance Wizard must be an Active Directory domain user and a local administrator on computer where you are running the setup.exe program.
- Your Windows or SQL login account must be either a member of sysadmin fixed server role or a member of db_owner database role on each of the database instances being upgraded. If the account is a member of db_owner database role, you must also have the EXTERNAL ACCESS ASSEMBLY permission on each of the database servers hosting the management database and audit store databases.

You can use the following SQL statement to grant the EXTERNAL ACCESS ASSEMBLY permission to a specific user:

```
GRANT EXTERNAL ACCESS ASSEMBLY TO [DOMAIN\user]
```

For example, to grant this permission to the account john@acme.com, you might execute the following SQL statement:

```
GRANT EXTERNAL ACCESS ASSEMBLY TO [ACME\john]
```

Restarting Computer After Agent Upgrade

If a computer has both Delinea Privilege Elevation Service and Delinea Audit & Monitoring Service enabled, you must restart the computer after upgrading the agent. If a computer only has Delinea Audit & Monitoring Service, there's no requirement to restart.

Updating Agents Out of Sequence

The recommended upgrade steps suggest that you to update deployed agents last. However, upgrading the agent is much simpler than upgrading the audit store or management database. which might require a database administrator to be involved. In most cases, it is safe to update the agent at any point in the upgrade process. If there are restrictions that would prevent a new agent from using an older collector, those restrictions are documented in the release notes.

Best Practices for Upgrading Large Audit Installations

When upgrading the Delinea Audit & Monitoring Service environment to a newer version, always follow this order for minimal service disruption:

1. Upgrade the audit databases.
2. Upgrade the audit collectors.
3. Upgrade the agents.
4. Upgrade remaining components (such as the consoles, PowerShell cmdlets, SDK, Audit Management server and so forth).
5. Delinea recommends using the Database Maintenance Wizard to "Generate the SQL scripts" for upgrading the databases rather than letting the Database Maintenance wizard perform an in-process upgrade.

Upgrade and Compatibility Guide

6. When performing a database upgrade by manually running the scripts, follow this order for minimal service disruption:
 - Upgrade the “Active” audit store database(s).
 - Upgrade the remaining audit store databases.
 - Upgrade the audit management database.
7. To upgrade the audit databases, typically the sysadmin rights on the database server are needed. This is because some of the operations performed during the database upgrade (such as marking an assembly with EXTERNAL ACCESS) requires permissions that are typically only assigned to the users with sysadmin rights. If the database environment is hardened and the user cannot run the upgrade scripts as a sysadmin, here’s a minimum set of permissions that the user must have in order to upgrade the databases:
 - User must have db_owner rights
 - User must have the EXTERNAL ACCESS ASSEMBLY rights
8. If the user is unsure whether the user has necessary rights to run the database upgrade or not, we recommend that the user generate the SQL scripts for database upgrade and hand them over to the database administrator for execution.
 - The audit database upgrade scripts are idempotent, which means accidentally running them multiple times will not cause any harm.
9. The database upgrade scripts sometimes log warning messages (for example, for exceeding key length). These warnings can be safely ignored. However, if any errors are received while running the database upgrade scripts, please notify Centrify support.

This information is also available in KB-32276.

Upgrading Managed Computers

This chapter describes how to update Delinea software on managed Linux and UNIX computers. You can also upgrade Delinea software on Mac OS X computers using the install.sh shell script in a Terminal application or by downloading, unpacking, and running the latest Mac OS X installer. For more information about upgrading Delinea software on Mac OS X computers, see the **Administrator’s Guide for Mac**.



When you upgrade agents installed on Linux computers, the upgrade process does not automatically enable desktop auditing on those systems. For information about enabling desktop auditing on supported Linux systems, see the **Auditing Administrator’s Guide**.

Using the install.sh Shell Script to Update Packages

The Delinea Agent installation script, install.sh, is a shell script that you can run interactively or configure to run silently on any supported UNIX, Linux, or Mac OS X computer.

You can use the install.sh shell script to upgrade any installed Delinea software except Delinea sudo. If you have the Delinea sudo package, you can upgrade the package before or after you upgrade the Delinea Agent and other packages.

To use the install.sh script interactively:

Upgrade and Compatibility Guide

1. Unzip and extract the contents of the file you downloaded from the Delinea Customer Download Center. For example:

```
gunzip centify-infrastructure-services-<release>-platform-arch.tgz
tar -xvf centify-infrastructure-services-<release>-platform-arch.tar
```

2. Run the `install.sh` script to start the update on the local computer's operating environment. For example:

```
./install.sh
```

The installer checks that it is possible to update Delinea software on the local computer. For example, it will check that the computer is a supported platform and that any required patches are installed. For more information about the ADCheck diagnostic tool, see the *Planning and Deployment Guide*.

3. Specify the type of upgrade you want to perform.

- (E) option: This option upgrades Server Suite access control, privilege management, secure shell, and auditing features. Any other Delinea packages you have installed are unchanged as long as they are compatible with the version being upgraded.
- (S) option: This option upgrades Server Suite access control, privilege management, and secure shell (Centrify-enabled OpenSSH) features. Any other Delinea packages you have installed are unchanged as long as they are compatible with the version being upgraded.
- Custom (C) option: This option allows you to select the Delinea packages located in the current directory and choose whether to erase (E), update (U), reinstall (R), keep unchanged (K) each package. If there is a package available for which there is no corresponding version already installed, you can choose to install the package.
- (X) option: This option installs or upgrades the access control and privilege management components as unlicensed Delinea Express components.

If you want to install or upgrade additional packages such as the Delinea Network Information Service (adnisd) or the Delinea LDAP proxy service, you should use the custom install option and select the packages to install.

Configuring `install.sh` to Run Without User Interaction

You can use the `install.sh` shell script to upgrade computers silently without user interaction. When you run `install.sh` without user interaction, you have the same upgrade options that you have when using `install.sh` interactively. When using `install.sh` without user interaction, however, you specify the type of upgrade on the command line and in a configuration file.

`--std-suite` upgrades authentication and privilege elevation features. Any other Delinea packages you have installed are unchanged as long as they are compatible with the version being upgraded.

`--ent-suite` upgrades authentication, privilege elevation, Delinea-enabled OpenSSH, and auditing features. Any other Delinea packages you have installed are unchanged as long as they are compatible with the version being upgraded.

In both cases, you can customize the upgrade by modifying the default `centrify-suite.cfg` configuration file. With the default `centrify-suite.cfg` configuration file, the `install.sh` script upgrades the Delinea Agent access control and privilege management features or the Delinea access control, privilege management, and auditing features.

Upgrade and Compatibility Guide

If you have already installed OpenSSH before you upgrade, either upgrade option also upgrades the OpenSSH packages.

All other packages available are left unchanged. For more detailed information about configuring a silent upgrade using the configuration file, see “Setting the parameters in a custom configuration file for the installation script” and the details for the INSTALL parameter in the Planning and Deployment Guide.

Using a Native Package Manager on Linux Computers

When you upgrade using the install.sh shell script, the script manages all dependencies and compatibility issues for you. If you want to upgrade Delinea software packages using the native package manager, you should first determine whether there are any compatibility issues or dependencies between the packages you have installed. For details about specific version compatibility requirements and upgrade scenarios, see [Compatibility for Additional Packages](#).

As of version 5.4.0, the core Delinea Agent bundle consists of four packages that must always be upgraded to the same version simultaneously: CentrifDC, CentrifDC-openssl, CentrifDC-openldap, and CentrifDC-curl. When fixes and patches are released, you can update individual packages of the core bundle, as long as the version is the same version as the other core packages.

After you have determined whether you have any version dependencies, you can use the native package manager to upgrade packages simultaneously. You can also use the native package manager to remove old packages individually or remove all packages simultaneously.

If you want to install or upgrade software packages using common native package installers, such as the Red Hat or Debian package manager, you should note that the software packages are signed with a GNU Privacy Guard (GPG) key. You need to import the key to verify the package authenticity before installing or upgrading the package. To import the key, download the RPM-GPG-KEY-centrify file from the Delinea Download Center then run the appropriate command for the package manager. For example:

```
rpm --import RPM-GPG-KEY-centrify
```

If you are not using a native package manager, you can use any other installation program you have available for the local operating environment. For example, if you use another program, such as SMIT, YAST, APT, or YUM to install and manage software packages, you can use that program to install Server Suite software packages.

Upgrading Packages on a Linux Computer

You do not need to stop any running Delinea process to perform the upgrade. While you do not usually need to restart Delinea processes or reboot your computer after upgrade, you may need to restart other processes that depend on PAM or NSS modules. Rebooting the computer after upgrade is recommended as a best practice.

It is best to install all Delinea packages simultaneously, if you are upgrading individual packages, however, you might see warnings from the package manager about package dependencies or version conflicts. If you see that a dependency is generated because of a package you have yet to upgrade, it is safe to ignore the warning.

Fresh Installation Using RPM

If you are performing a fresh installation on a Linux computer that supports the Red Hat Package Manager (rpm), you can install the packages individually. For example, to install the Delinea Audit & Monitoring Service package you would enter commands similar to the following:

```
rpm -i CentrifDA-5.4.0*-platform.arch.*rpm
```

Upgrade and Compatibility Guide

The platform and architecture you specify in the file name on the command line should identify the specific operating system you are using, for example `Centrify-5.4.0-rhel4.x86_64.rpm` or `centrify-5.4.0-suse10.ia64.rpm`. After the package manager updates the packages installed, you can optionally restart Delinea processes or reboot the computer.

You can verify the Delinea packages that were installed using the following command:

```
rpm -qa CentrifyDC-\*
```

Upgrading Existing Packages Using RPM

If you are upgrading an existing installation of an agent package on a Linux computer that supports the Red Hat Package Manager (`rpm`), you should add all of the packages you want to upgrade to a directory of your choice, and issue a single command similar to this:

```
rpm -Uhv my_dir/\*.rpm
```

Where `my_dir` is a directory that you specify.

Fresh Installation Using the Debian Package Manager

On a Debian, Ubuntu, or Linux MINT computer, the order that you install the core package depends on whether you are performing a fresh installation or upgrading an existing installation. Any Delinea packages other than the core packages can be listed after the core bundle in any order.

For example, to perform a fresh installation of the core authentication service package, you would enter commands similar to the following:

```
dpkg -i ./centrifydc-openssl-5.4.0-platform-arch.deb
./centrifydc-openldap-5.4.0-platform-arch.deb
./centrifydc-curl-5.4.0-platform-arch.deb
./centrifydc-5.4.0-platform-arch.deb
```

Upgrading Packages Using the Debian Package Manager

If you are upgrading an existing installation, the order of the core packages is different than that in a fresh installation. Delinea packages other than the core packages can be listed after the core bundle in any order.

For example, if you were updating all of the Delinea Agents, you would enter commands similar to the following, noting that the packages in **bold** are the core agent packages, and must be entered in the order below:

```
dpkg -i --force-confnew --force-confmiss
\--ignore-depends=centrifydc-nis
\--ignore-depends=centrifydc-ldaproxy
\--ignore-depends=centrifyda./centrifydc
__./centrifydc-5.4.0-***platform-arch***.deb__
**./centrifydc-openssl-5.4.0-***platform-arch***.deb**
**./centrifydc-openldap-5.4.0-***platform-arch***.deb**
**./centrifydc-curl-5.4.0-***platform-arch***.deb**
./centrifydc-ldaproxy-5.4.0-***platform-arch***.deb
./centrifydc-nis-5.4.0-***platform-arch***.deb
./centrifyda-3.4.0-***platform-arch***.deb
```



If you are upgrading the core agent package from version 5.4.0 or later, to any later version, you must include Delinea in the list of packages to ignore. If you do not have `centrifydc-nis`, `centrify-ldapproxy`, or `centrifyda` installed, the `--ignore-depends` command for those packages is not necessary.

The platform and architecture you specify on the file name in the command line should identify the specific operating system you are using, for example `centrifydc-5.4.0-deb7-i386.deb`. After the package manager updates the packages installed, you can optionally restart Delinea processes or reboot the computer.

You can verify the Delinea packages that were upgraded using the following command:

```
dpkg -s CentrifyDC-\*
```

Using a Native Package Manager on UNIX Computers

When you upgrade using the Delinea `install.sh` shell script, the script manages all dependencies and compatibility issues for you. If you want to upgrade Delinea software packages using the native package manager, you should first determine whether there are any compatibility issues or dependencies between the packages you have installed. You can then upgrade packages individually or simultaneously. For details about specific version compatibility requirements and upgrade scenarios, see [Compatibility](#) for additional packages.

After you have determined whether you have any version dependencies, you can use the native package manager to upgrade all packages simultaneously. You can also use the native package manager to remove old packages individually or remove all packages simultaneously.

Upgrading Packages Individually on a UNIX Computer

With the exception of Solaris computers, you do not need to stop any running Delinea process to perform an upgrade on UNIX machines. On Solaris computers, you should stop all Delinea processes before upgrading. You should note that while rebooting the computer or restarting agent services after an upgrade is not required for Delinea processes in most cases, you may need to reboot the computer or restart any processes that rely on PAM or NSS modules after you complete the upgrade to ensure that the upgraded binaries and libraries are being run. Rebooting the computer after upgrade is recommended as a best practice.

To upgrade Delinea software using the native package manager, follow these basic steps:

- Stop all Delinea processes running on Solaris computers.

For example:

```
/usr/share/centrifydc/bin/centrifydc stop  
/etc/init.d/centrify-sshd stop  
/etc/init.d/adsagent stop
```

- Upgrade the core agent packages using the native package manager. The four core packages must be upgraded together.
- Upgrade other Delinea packages using the native package manager.
- Restart Delinea processes or reboot the computer.

Depending on the order in which you are upgrading individual packages, you might see warnings from the package manager about file dependencies. If you see that a dependency is generated because of a package you have yet to upgrade, it is safe to ignore the warning.

Upgrade and Compatibility Guide

The next sections illustrate the commands to use on different platforms. The actual file name that you specify on the command line—including a specific build number, platform, and architecture—will identify the specific operating system you are updating, for example `centrifydc-5.4.2-sol8-sparc-local.tgz` or `centrifydc5.4.2aix53ppc-bff.gz`.

Performing Upgrades on UNIX Computers

The process for simultaneous upgrades on UNIX computers is similar to that for Linux computers. However, the native package managers on different platforms vary in their ability to perform simultaneous upgrades.

This section includes the following topics:

Upgrading Packages on Solaris Computers

On Solaris computers, it is necessary to spool all packages that are to be installed simultaneously. The package manager can then take the spooled packages and install them all at once using one command. Before upgrading on Solaris computers, however, you should stop all Delinea processes that are running.



On Solaris 10 computers that use Solaris zones, you should upgrade the core agent packages as a separate step. You can then upgrade other Delinea packages using a simultaneous upgrade.

To perform upgrades on Solaris computers:

1. Stop existing Delinea processes.

For example, if you are upgrading the core agent, Delinea-enabled OpenSSH, and Delinea NIS packages, you would enter commands similar to the following:

```
/usr/share/centrifydc/bin/centrifydcstop  
etc/init.d/centrify-sshd stop  
/etc/init.d/adnisd stop (on Solaris 9)  
svcadm disable centrifydc_server (on Solaris 10 or later)
```

2. Create a new admin file.

If you are upgrading an existing installation, make a copy of the system default admin file (`/var/sadm/install/admin/default`) and modify it to ignore dependencies. In the examples below, this file is called `my_admin`. It should look like this:

```
mail=  
instance=overwrite  
partial=nocheck  
runlevel=nocheckdepend=nocheck rdepend=quit  
space=quit  
setuid=nocheckconflict=nocheckaction=nocheck basedir=default
```

If you are performing a fresh installation, you can use the original system admin file and keep the default settings.

3. Unzip and extract each package into a temporary directory, for example, `my_tmp_dir`.

To unzip and extract the agent core packages, you would enter commands similar to the following:

Upgrade and Compatibility Guide

```
gunzip centrififydc-5.4.0-*platform-arch*-local.tgz
tar xvf centrififydc-5.4.0-platform-arch-local.tar
gunzip centrififydc-openssl-5.4.0-*platform-arch*-local.tgz
tar xvf centrififydc-openssl-5.4.0-*platform-arch*-local.tar
gunzip centrififydc-openldap-5.4.0-*platform-arch*-local.tgz
tar xvf centrififydc-openldap-5.4.0-*platform-arch*-local.tar
gunzip centrififydc-curl-5.4.0-*platform-arch*-local.tgz
tar xvf centrififydc-curl-5.4.0-*platform-arch*-local.tar
```

4. Spool the packages.

Spool the packages to a specified directory, for example, `my_spool_dir`.

To spool the core packages, you would run commands similar to the following:

```
pkgadd -s /my_spool_dir -d /my_tmp_dir/CentrifyDC CentrififyDC
pkgadd -s /my_spool_dir -d /my_tmp_dir/CentrifyDC-openssl CentrififyDC-openssl
pkgadd -s /my_spool_dir -d /my_tmp_dir/CentrifyDC-openldap
CentrififyDC-openldap
pkgadd -s /my_spool_dir -d /my_tmp_dir/CentrifyDC-curl CentrififyDC-curl
```

5. Upgrade the packages.

To upgrade the core packages, you would enter commands similar to the following:

```
/usr/sbin/pkgadd -a my_admin -n -d /my_spool_dir CentrififyDC-openssl
/usr/sbin/pkgadd -a my_admin -n -d /my_spool_dir CentrififyDC-openldap
CentrififyDC-curl
/usr/sbin/pkgadd -a my_admin -n -d /my_spool_dir CentrififyDC
```

6. Restart Centrifify processes after the upgrade is complete.

7. Verify the upgrade.

To verify that the upgrade was successful, run the following command:

```
/usr/bin/pkginfo | grep -i Centrifify
```

Upgrading Packages on HP-UX Computers

On HP-UX computers, it is necessary to spool all packages that are to be installed. The package manager can then take the spooled packages and install them all at once using one command.

To perform upgrades on HP-UX computers

1. Copy and unzip all depot.gz packages into a temporary directory, for example, `my_dir`.

To unzip and extract the agent core packages, enter commands similar to the following:

Upgrade and Compatibility Guide

```
gunzip centrifdc-5.4.0-*platform-arch*.depot.gz
```

```
gunzip centrifdc-openssl-5.4.0-*platform-arch*.depot.gz
```

```
gunzip centrifdc-openldap-5.4.0-*platform-arch*.depot.gz
```

```
gunzip centrifdc-curl-5.4.0-*platform-arch*.depot.gz
```

2. Spool each package.

On HP-UX computers, you can use the default spool directory, but you must create a working directory, for example `my_dir`.

To spool the agent core packages to `my_dir`, enter commands similar to the following:

```
swcopy -s /full_path/my_dir/centrifdc-openssl-5.4.0-*platform-arch*.depot
```

```
CentrifDC-openssl
```

```
swcopy -s /full_path/my_dir/centrifdc-openldap-5.4.0-*platform-arch*.depot
```

```
CentrifDC-openldap
```

```
swcopy -s /full_path/my_dir/centrifdc-curl-5.4.0-*platform-arch*.depot
```

```
CentrifDC-curl
```

```
swcopy -s /full_path/my_dir/centrifdc-5.4.0-*platform-arch*.depot
```

```
CentrifDC
```

3. Upgrade the packages.

Use a single command to upgrade all packages. For example, to update the core agent packages, enter a command similar to the following:

```
swinstall -s CentrifDC-openssl CentrifDC-openldap CentrifDC-curl
```

```
CentrifDC
```

4. Verify the upgrade.

Verify that the upgrade was successful by running the following commands:

```
swlist \| grep -i Centrif
```

```
swverify CentrifDC
```

Upgrading Packages on AIX Computers

On AIX computers, it is necessary to unzip all packages that are to be installed. The package manager can then take the unzipped packages and install them all at once, using one command.

To perform upgrades on AIX computers do the following:

1. Copy and Unzip the packages to a directory, for example, `my_dir`.

If you are upgrading the core agent packages, you would run commands similar to the following:

Upgrade and Compatibility Guide

```
gunzip centrifidc-5.4.0-*platform-arch*-bff.gz
```

```
gunzip centrifidc-openssl-5.4.0-*platform-arch*-bff.gz
```

```
gunzip centrifidc-openldap-5.4.0-*platform-arch*-bff.gz
```

```
gunzip centrifidc-curl-5.4.0-*platform-arch*-bff.gz
```

2. Upgrade the packages.

You can now upgrade the packages using commands similar to the following:

```
inutoc .
```

```
installp -aY -d my_dir all
```

Upgrading Agents on Solaris Systems

Before upgrading agents on Solaris systems you'll need the installation packages appropriate for your Solaris system, as listed in the table below.

Solaris Agent Installation Packages

Solaris version	Package type	x86 or Sparc	Agent package filename
Solaris 10	svr4	x86	centrifid-server-suite-2021.1-sol10-x86.tgz
Solaris 10	svr4	Sparc	centrifid-server-suite-2021.1-sol10-sparc.tgz
Solaris 11	svr4	x86	centrifid-server-suite-2021.1-sol10-x86.tgz
Solaris 11	svr4	Sparc	centrifid-server-suite-2021.1-sol10-sparc.tgz
Solaris 11	IPS	x86	centrifid-server-suite-2021.1-sol11-i386.tgz
Solaris 11	IPS	Sparc	centrifid-server-suite-2021.1-sol11-sparc.tgz

To upgrade the Solaris svr4 packages:

- Follow the instructions here: [Using the install.sh shell script to update packages](#) or [Performing upgrades on UNIX computers](#)

Upgrading and Migrating Solaris svr4 Packages to IPS on Solaris 11

If you have a Solaris 11 system on which you've installed a previous release of the Delinea Agent for *NIX and you want to upgrade and use Solaris IPS, you do the upgrade in 3 steps:

1. Run the install-last-svr4.sh script.

This upgrades your previous agent to a temporary, in-between version 9.9.9.

2. Run the install-last-svr4.sh script again and uninstall the version 9.9.9 packages.

This prepares the system so that you can install the IPS packages.

3. Run the IPS-specific install script, install-ips.sh to install the Solaris IPS packages.

Upgrade and Compatibility Guide

These steps assume that there aren't any child zones configured on this Solaris system.

You'll need the IPS specific `tgz` file and also the `svr4` `tgz` for your system in order to perform these steps.

Before you upgrade:

- Make sure that the agents components that are installed before you upgrade are the same ones that you want to have installed after the upgrade. It's easier to do the upgrade in place this way.

For example, if you have the audit agent currently installed but you don't want it installed in the new version, remove it before upgrading. Or, if you don't have the ldap proxy component installed but you do want it installed in the new version, install it first (the same version as the other agent components that are already installed).

To upgrade and migrate the Solaris `svr4` packages to IPS on Solaris 11:

1. Log on or switch to the root user.
2. Change to the appropriate directory that contains the Delinea Agent package you want to install.

For example, change to the `Agent_Unix` directory.

If you downloaded individual agent packages from the Delinea Download Center, unzip and extract the contents. For example, you'll need the following two `.tgz` files:

```
centrify-infrastructure-services-2021.1-sol11-i386.tgz
```

```
centrify-infrastructure-services-2021.1-SolarisVersion-platform-arch.tgz
```

For each package, extract them; here's an example:

```
gunzip -d centrify-infrastructure-services-<release>-platform-arch.tgz
```

```
tar -xf centrify-infrastructure-services-<release>-platform-arch.tar
```

3. Change to the `/lastsvr4` sub-directory and run the `install-last-svr4.sh` script to prepare the previous installation for upgrade:
 - a. The script prompts you, "Do you want to continue and upgrade to v.9.9.9?"
Enter Y for yes.
 - b. The script prompts you to confirm your selection:
Enter Y to continue (or enter N to change the settings).
The script unpackages the files and installs the new packages.
4. Run the `install-last-svr4.sh` script a 2nd time and uninstall the 9.9.9 version components:
 - a. The script prompts you, asking if you want to erase, reinstall, or keep the current package.
Enter E to erase.
 - b. The script prompts you to confirm your selection to uninstall the package.
Enter Y to continue.
The script uninstalls and removes the version 9.9.9 files.
 - c. You can run the following command to verify the Solaris agent package `svr4` installation status:

Upgrade and Compatibility Guide

```
pkginfo | grep -i Centrifly
```

Note that there is no space between "pkg" and "info"; if you search for "pkg info" you'll be searching for IPS packages.

5. Change to the directory (up one level) that contains the installation packages and run the install-ips.sh script.

- a. The script will list that it found previously installed svr4 packages and prompts you, asking if you want to continue.

Enter Y for yes.

- b. The script will list out the package versions to install and prompts you to confirm.

Enter Y to confirm and continue.

The script installs the IPS packages.

6. You can run the following command to verify the Solaris agent package IPS installation status:

```
pkg info | grep -i Centrifly
```



The space between "pkg" and "info"; if you search for "pkginfo" you'll be searching for svr4 packages.

Upgrading Managed Mac OS X Computers

In most cases, you can update agents on Mac OS X computers by simply installing the new agent either directly or remotely on top of an existing agent. As a best practice, you should perform in-place upgrades using a local Mac administrative (admin) account or any other user account that has local administrative rights and reboot the computer after completing the upgrade. In most cases, you should not perform the upgrade while you are logged on as an Active Directory user in a currently active session.

In rare cases, you might be advised to run adflush to clear the Active Directory cache before performing an in-place upgrade. For example, if you are updating agents from version 4.x, or earlier, to 5.1.x, run adflush first to ensure a smooth upgrade. It is highly unusual for an upgrade to require you to leave and rejoin a managed Mac computer to the domain.

Compatibility for Additional Packages

In general, Delinea software packages are not version-dependent on each other. However, there are compatibility limitations in some situations. This chapter describes specific compatibility requirements for packages that are not part of the core agent packages or have been added to or removed from the core agent packages. If you are only upgrading the core agent packages and have no other packages installed, you can skip this chapter.

Should You Be Concerned About Compatibility?

Compatibility issues are managed automatically when you use the install.sh shell script to upgrade packages. If you plan to update packages using a native package manager, however, you should be aware of potential compatibility issues and be able to manually manage dependencies between packages. Depending on the version of Delinea software you currently have installed, the version you are upgrading to, and which packages you have installed, you might have many or no compatibility concerns. The first step is to identify which software packages and versions you have deployed.

Upgrade and Compatibility Guide

The core agent package for access control and privilege management for versions before version 5.4.0 is CentrifyDC. For all releases after and including 5.4.0, the core agent package is split into four distinct packages:

CentrifyDC

CentrifyDC-openssl

CentrifyDC-openldap

CentrifyDC-curl

The core agent package for auditing is CentrifyDA. Other packages you might have installed include:

CentrifyDC-nis

CentrifyDC-krb5

CentrifyDC-ldapproxy

CentrifyDC-openssh

CentrifyDC-web

CentrifyDC-apache

CentrifyDC-adbindproxy



When you upgrade to version 5.4.0 of the Delinea Agent, you must also upgrade all of the other Delinea packages you have installed to version 5.4.0 as well. If you fail to upgrade a package other than the core packages, and attempt to upgrade the core agent packages to 5.4.0, the upgrade will fail. For agent versions after 5.4.0, you may not be required to simultaneously upgrade each of the packages other than the core agent packages.

Removing the CentrifyDC-samba Package

If you are upgrading the core agent package for access control and privilege management and have Delinea Samba installed, you should remove the Delinea Samba CentrifyDC-samba) package, install open-source Samba, and install the Delinea adbindproxy package (CentrifyDC-adbindproxy). See the **Samba Integration Guide** for details about that procedure.

Compatibility for CentrifyDC-nis Package

If you are upgrading the core agent packages and have the CentrifyDC-nis package installed, you should also upgrade the CentrifyDC-nis package. The CentrifyDC-nis package must have the same major version number as the core agent packages. The version number for the CentrifyDC-nis package should never be higher than the version number of the core agent packages.



Some platforms, the adnisd package might prevent the ypbind service from starting properly because of the order in which services are started. For example, if ypbind is configured to start before the adnisd service, the bind will fail. This issue does not occur if you are installing new packages. However, to prevent unintended changes to the existing startup sequence during an upgrade, upgrading the adnisd package will not modify your existing startup configuration. You can manually correct the startup sequence after an upgrade by manually running the chkconfig script. For example, run the following command after the adnisd upgrade:

```
chkconfig adnisd on
```

Compatibility for CentrifyDC-krb5 Package

The Delinea Kerberos client tools are no longer packaged with the Server Suite agent or available from the Delinea Download Center. The client tools were formerly provided as a separate software package or as part of the core agent package to support Kerberos-based authentication on older operating systems. The package is no longer relevant on currently-supported operating systems.

Compatibility for CentrifyDC-ldapproxy Package

If you are upgrading the core agent packages and have the CentrifyDCldapproxy package installed, you should also upgrade the CentrifyDCldapproxy package. The CentrifyDCldapproxy package must have the same major version number as the core agent package. The version number for the CentrifyDCldapproxy package should never be higher than the version number of the core agent package. If you upgrade the core agent packages to a version number that is higher than the CentrifyDCldapproxy package version, the installation script removes the CentrifyDCldapproxy package. To retain the CentrifyDCldapproxy package when you upgrade the core agent packages, you must make sure that both packages are upgraded to the same version number.

Compatibility for CentrifyDC-openssh Package

In most cases, the core agent packages and the CentrifyDCopenssh packages are installed and upgraded together. Therefore, in most cases, they will have the same major version number. If you have the CentrifyDCopenssh package installed and are upgrading the core agent to version 5.1.2 or later, you must also upgrade the CentrifyDCopenssh package. If you use the installation script to upgrade, it enforces this compatibility requirement.

Compatibility for CentrifyDC-Apache and CentrifyDC-Web Packages

If you are upgrading the core agent packages to 5.x and have Delinea for Apache or Java applications installed, the CentrifyDC-apache or CentrifyDC-web package should be version 4.x or later. For example, CentrifyDC_apache-4.2.0-*nnn* is compatible with CentrifyDC version 5.x.

Upgrading Version-Dependent Packages

If you are upgrading a computer that has one or more Delinea software packages that are version-dependent on one another, you should either:

- Remove the Delinea packages that are version-dependent before upgrading the core agent packages, upgrade the core agent packages, then re-install the new versions of the version dependent packages.
- Simultaneously upgrade the core agent packages and all of the additional packages that are version-dependent.

If you are upgrading a computer where there are no version dependencies, Delinea recommends you upgrade all packages simultaneously, if possible.

Working with Classic Zones After an Upgrade

Server Suite supports both classic and hierarchical zones. After you upgrade the agents, you can choose to either migrate your classic zones into a hierarchical zone structure or maintain them as classic zones. If you want to convert your classic zones into hierarchical zones, you can use the admigrate program. For details about using the

Upgrade and Compatibility Guide

admigrate program to migrate a classic zone to a new parent or child hierarchical zone, see the man page for admigrate.



You can only migrate classic zones to hierarchical zones if you have upgraded the Delinea Agent to version 5.x or later.

You are not required to migrate any existing classic zones. If you choose to maintain your existing zones as classic zones, however, you should be aware that the authorization model in classic zones differs from the authorization model used in hierarchical zones. For example:

- In classic zones, any user with a profile in a zone is automatically granted login access to all computers joined to the zone.
- In hierarchical zones, a user with a profile in a zone must be assigned to a role with login rights and PAM access rights before being able to login to a computer joined to a zone.

In addition, there are configuration parameters, commands, APIs, and features that are only applicable in classic zones and other parameters, commands, APIs, and features that are only applicable in hierarchical zones. For example, authorization is an optional feature that can be enabled or disabled in classic zones, so there is a configuration parameter and a zone property option to support the feature in classic zones. For hierarchical zones, authorization is required for access to any managed computer, so the configuration parameter and zone property option are not visible in hierarchical zones.

What To Do If There Are Problems During an Upgrade

In most cases, upgrading Delinea software is a seamless process that does not interrupt services. If you are not able to complete an upgrade successfully, however, there are a few steps you can take to restore your working environment. This chapter covers the steps to take if you have problems during the upgrade process.

Remove and Re-install Authentication and Privilege

If you have problems upgrading any Authentication & Privilege components, such as Access Manager, you should use the Control Panel application to uninstall the software, then rerun the setup program to install the components cleanly.

If you want to restore an older version of the software rather than attempt a fresh installation of the latest version—run the setup program for that version of the software.

Remove and Re-install Delinea Audit and Monitoring Service

If you have problems upgrading any Delinea Audit and Monitoring Service components, such as Audit Manager or Audit Analyzer, you should do the following:

- Use the Control Panel application to remove the auditing infrastructure components from the local computer.
- Use ADSI Edit to remove the service connection point for the installation. If you publish this information in more than one location, remove all of the service connection points from the forest.
- Rerun the setup program to install the components cleanly.

If you want to restore an older version of the software rather than attempt a fresh installation of the latest version—run the setup program for that version of the software.

Remove and Re-install Agent Features

If you have problems upgrading any agent features, such as access control and privilege management or auditing services, you should do the following:

1. Log on as root and disable auditing on UNIX computers where auditing is enabled:
`dacontrol -d`
2. Use the `adleave` command to remove the UNIX computer from its current zone and Active Directory domain.
3. Use the Delinea Privilege Elevation Service settings to remove the local Windows computer from its current zone, then use the Windows Control Panel application to remove the agent services from the local computer.
4. Rerun the `install.sh` script or the agent setup program to install the agent cleanly.
2. You can join the domain from the installation script on UNIX computers or join a zone from the agent configuration wizard on Windows computers.
5. Log on as root and enable auditing on UNIX computers where you want auditing enable
`dacontrol -e`

Known Issues

The following are known issues organized by category.

Installation and Uninstallation Issues

- 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)
- The Delinea Common Component should be the last 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 Delinea 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

Upgrade and Compatibility Guide

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)

- If you uninstall the Delinea 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)
- 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, Delinea Agent for Windows will not run properly. User will also experience problem when trying to remove Delinea Agent for Windows from the system. To properly uninstall Delinea Agent for Windows, please make sure Delinea Agent for Windows is uninstalled before .NET. (Ref: 39051a)

Configuration Issues

- 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)
- In Windows 2016 and Windows 10, 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)
- In some large environment with multiple domain controllers, it may take up to one minute for the new zone setting in Delinea 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 Delinea 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

Upgrade and Compatibility Guide

CTLs on the system may not be adequate for secure connections of multi-factor authentication especially for older versions of Windows such as Windows 7 and Windows Server 2008 R2. To ensure the success of 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 Delinea KB-6724 for further information. (Ref: CS-39703)

Environment Issues

- On Windows 10 and Windows 2016 machines with Delinea Privilege Elevation Service, the 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 Delinea 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 computers, 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)
- An environment with no Global Catalog is not supported. (Ref: 46577a)
- Delinea Privilege Elevation Service 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, Delinea Privilege Elevation Service 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)

RunAsRole Issues

- 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)
- The 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)
- 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)

Desktop with Elevated Privileges Issues

- 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)
- 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)

Roles and Rights Issues

- There is no 'Require multi-factor authentication' system right for the predefined 'Windows Login' role. To define this system right for MFA, use the pre-defined 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

Upgrade and Compatibility Guide

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)

Compatibility with Third Party Products Issues

- VirtualDesktop is not compatible with Delinea Agent for Windows. Users should use the Delinea system tray applet to create virtual desktop instead. (Ref: 44641b)
- 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)
- 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)
- 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:
 - vCenter Server 5.1
 - SQL Server
 - xchange 2010 or above
 - SCOM 2007(Ref: 45318a, 45218a, 43779a, 38016a)
- Users may notice an error and cannot install ActivClient after installing Delinea Agent for Windows. During the installation of ActivClient, it attempts to change the local security setting. However, there is a known issue for Delinea Agent for Windows of blocking the local security setting (Ref: 63609b). Therefore, users may not be able to install ActivClient successfully after installing Delinea Agent for Windows. We suggest installing ActivClient before installing Delinea Agent for Windows. If Delinea 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)

Application Manager Issues

Application Manager does not support the Server Core edition of Windows. (Ref: CS-40656).