Centrify Server Suite 2016

Deployment Manager User's Guide

April 2016

Centrify Corporation

Legal notice

Contents

About this guide

The *Deployment Manager User's Guide* provides complete information for installing and using DirectManage Deployment Manager. DirectManage Deployment Manager is available as part of the Centrify Server Suite and as a standalone executable in the Centrify Express line of products. Centrify Express products can be downloaded for free from the Centrify website. Deployment Manager enables you to discover and analyze remote computers on your network, download and deploy Centrify software, and managing accounts and operations for remote computers from a central console.

Intended audience

This guide is intended for administrators who want to use Deployment Manager on a Windows computer to evaluate security risks, and to install, update, and manage Centrify software on remote computers.

The guide assumes that you have a working knowledge of how to perform administrative tasks on the Linux, UNIX, and Mac OS/X computers that you manage and that you are familiar with how to navigate and perform common activities in a Windows operating environment. If you are unfamiliar with any of the platforms you intend to support, you may need to consult additional, operating system-specific documentation to perform certain tasks or understand certain concepts.

Using this guide

Depending on your role and responsibilities, you might want to read portions of this guide selectively. The guide provides the following information:

- Chapter 1, "Introduction to Deployment Manager," introduces the basic features of DirectManage Deployment Manager and describes how Deployment Manager collects information from remote computers.
- Chapter 2, "Installing Deployment Manager," provides step-by-step instructions for installing DirectManage Deployment Manager as a standalone executable.
- Chapter 3, "Getting started with Deployment Manager," describes how to navigate the Deployment Manager console and introduces the basic steps involved in performing a security assessment and deploying Centrify software.
- Chapter 4, "Performing an identity risk assessment," provides step-by-step instructions for performing a security assessment, generating summary and detailed reports, and evaluating the results.

- Chapter 5, "Deploying Centrify software packages," provides step-by-step instructions for downloading and deploying Centrify software.
- Chapter 6, "Performing administrative tasks using Deployment Manager," describes how to manage computers, local accounts, the software inventory, and other information from Deployment Manager.
- Chapter 7, "Setting Deployment Manager options," describes configuration options you can set in Deployment Manager to customize operations to suit your needs.

In addition to these chapters, an index is provided for your reference.

Conventions used in this guide

The following conventions are used in this guide:

- `Fixed-width` font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *`italicized`*, the fixed-width font is used to indicate variables. In addition, in command line reference information, square brackets (`[ ]`) indicate optional arguments.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles and to emphasize specific words or terms.
- Standalone software packages include version and architecture information in the file name. For example, the standalone software package `CentrifyDM-`*`version`*`-win64.exe` in documentation refers to a 64-bit release of Centrify DirectManage Deployment Manager with a file name that includes specific version information, such as `CentrifyDM-5.1.2-win64.exe`.

Finding information about Centrify products

Centrify provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrify and Centrify products and features, start by visiting the Centrify website. From the Centrify website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrify products, and get the latest news about upcoming events and webinars.

Contacting Centrify

You can contact Centrify by visiting our website, www.centrify.com. On the website, you can find information about Centrify office locations worldwide, email and phone numbers for contacting Centrify sales, and links for following Centrify on social media. If you have questions or comments, we look forward to hearing from you.

Getting customer support

If you have a Centrify account, click Support on the Centrify website to log on and access the Centrify Customer Support Portal. From the support portal, you can to search knowledge base articles, open and view support cases, connect with other Centrify users on customer forums, and access additional resources—such as online training, how-to videos, and diagnostic tools.

Introduction to Deployment Manager

This chapter introduces the core features of Centrify DirectManage Deployment Manager. Deployment Manager provides a centralized console for discovering, analyzing, and managing remote computers.

The following topics are covered:

- Discovering remote computers
- Managing the software inventory
- Evaluating security risks and vulnerabilities
- Deploying Centrify software on remote computers
- Managing remote computers and account information
- Collecting and storing information from remote computers

Discovering remote computers

With Deployment Manager, you select a method for finding computers of interest. For example, you can discover remote computers on your internal network by specifying a subnet and mask or a range of IP addresses. Based on the selection criteria and other information you provide, Deployment Manager locates remote computers that match your criteria.

If the connection to a remote computer is successful, Deployment Manager collects detailed information about that computer, including the platform vendor, operating system version, and the computer host name. All of the information collected from successfully discovered computers is stored in a compact database on the computer where Deployment Manager is installed.

The primary goal of discovering remote computers is to identify computers that are candidates for deploying Centrify software packages. You can also discover computers to prepare for a security assessment that will help you locate potential risks and vulnerabilities.

After you successfully discover computers of interest, you can use Deployment Manager to perform additional administrative tasks remotely.

Managing the software inventory

You can use Deployment Manager to download and store Centrify software packages, including assessment tools, analysis tools, and agents for all supported operating systems

and platforms. You can download software directly from the Centrify Download Center, or from a network location that's accessible from the computer where Deployment Manager is installed.

With Deployment Manager, you can check whether discovered computers have up-to-date software installed and keep track of your software inventory. You can also configure Deployment Manager to periodically check the Centrify Download Center for product catalog updates and to automatically get updates when they become available. Information about the software you have downloaded is stored in the Deployment Manager database, so you have a historical record of activity and the packages available.

Evaluating security risks and vulnerabilities

You can use the Deployment Manager Assessment feature to check discovered computers for a wide range of potential issues and generate a report of findings. The assessment report can help you determine the overall risk level across computers in your organization and specific areas where you have the most exposure. The report also highlights steps you can take to reduce risk and improve security, compliance, and operational efficiency.

The results of each assessment you run are stored in the Deployment Manager database, so you have a historical record of activity and an archive of past assessment results.

Deploying Centrify software on remote computers

The primary purpose of Deployment Manager is to assist you in deploying Centrify software on remote computers from a central location. As part of the deployment process, you can download and run analysis tools that check the current state of each discovered computer. The analysis includes checks for all basic system requirements, such a supported operating environment, required patches and libraries, and available disk space. The analysis also checks the configuration of DNS and for the availability of an Active Directory domain and domain controller. At the conclusion of the analysis, any errors or warnings are listed in Deployment Manager under an Open Issues node.

Depending on the error or warning reported, you might then be able to resolve the issue directly from Deployment Manager or by opening a remote terminal session on the computer where the problem was found.

After you resolve issues and are ready to install, you can use Deployment Manager to deploy a Centrify agent and join an Active Directory domain from a central location. Information about the software you have deployed is stored in the Deployment Manager database, so you have a historical record of activity and can keep track of which version of the agent is installed where.

Managing remote computers and account information

Deployment Manager enables you to execute administrative commands, edit files, and modify account information on remote computers from a central location. For example, you can use Deployment Manager to analyze and manage remotely-defined users and groups. You can add, modify, or delete users and groups on remote computers or map those users and groups to Active Directory users and groups.

With Deployment Manager, you can enable or disable auditing on remote computers. You can also open remote terminal sessions to run virtually any command or script from a central location.

Collecting and storing information from remote computers

The first step in a security assessment or a deployment is to identify the computers that you want to evaluate or on which you want to deploy software. Deployment Manager then connects to each of those remote computers to collect information such as the host name, the operating system vendor and version, and the platform architecture.

To complete this part of the discovery process, you must provide account credentials with sufficient permissions for Deployment Manager to log on and execute privileged commands. Deployment Manager uses the account credentials to run scripts that execute specific commands on each remote computer. The specific commands executed and the permissions required vary depending on the operating system. For example, Deployment Manager might execute the `uname` command, use `cat` or `grep` to collect information from system files, and call platform-specific commands such as `isainfo`, `vmware`, `rpm`, and `sw_vers`.

In general, Deployment Manager requires root-level permissions assigned to a non-root account to ensure it can obtain system information from protected files.

Collecting and changing user and group information

During discovery, Deployment Manager also collects information about the local users and groups defined on each remote computer. For most platforms, Deployment Manager calls `getent` to get the effective local users and groups from the local `/etc/passwd` and `/etc/group` files. On some platforms, however, different commands are used. For example:

- On Mac OS X, it calls `dscl` to get both effective and local accounts.
- On IBM AIX, it calls `lsuser` and `lsgroup` for effective accounts.
- On HP-UX it calls `pwget` and `grget` for effective accounts.

Deployment Manager also allows you to add, change, and delete local accounts on remote computers. To do so, it calls `useradd`, `usermod`, and `userdel` on most platforms, and `dscl` on Mac OS X.

Modifying the configuration of security software

If you are running any type of network security software, for example, an anti-virus program, IP scanner, or intrusion detection software, you may need to modify its configuration to allow Deployment Manager to operate. Otherwise, the scanner or security software may identify Deployment Manager activity as a threat and lock it out of your network.

Storing information securely

When you enter account information in Deployment Manager, the user name and password can be stored temporarily in memory or stored securely in the Deployment Manager database. If you choose to store the credential information in the Deployment Manager database, credentials are encrypted using the access token of the currently logged on Windows user.

The credentials are secure because only the user who added the credential information to the database can use that information to connect to remote computers. Even if other users have access to Deployment Manager and the Deployment Manager database, they cannot decrypt the stored credentials without the access token for the Windows user account that was used to encrypt the information. To retrieve and decrypt the stored credentials, you must log on and access the Deployment Manager database using the same Windows account and from the same computer you used when the password was first encrypted.

If you don't want to store any credentials locally in the Deployment Manager database, you can choose to cache them temporarily each time you start a new Deployment Manager session. For more information about the options for handling credentials, see "Selecting a method for credential handling" on page 70.

Installing Deployment Manager

This chapter describes the minimum system requirements and how to install DirectManage Deployment Manager as a standalone executable from its own setup program on a Windows computer. If you are installing DirectManage Deployment Manager as part of the Centrify Server Suite, you can skip this chapter. For more information about installing Deployment Manager as part of Centrify Server Suite, see the *Centrify Server Suite Planning and Deployment Guide*.

The following topics are covered:

Preparing to install

You can install Deployment Manager on any supported Windows operating system, and use it to discover, evaluate, and deploy software on any supported non-Windows computer. For information about the versions of Windows and non-Windows computers that Centrify currently supports, see the supported platforms section on the Centrify website.

http://www.centrify.com/resources

Note Not all Deployment Manager features are supported on all platforms where you can install Centrify software. For example, you can deploy the Centrify agent on Mac OS X computers, but you cannot use Centrify Identity Risk Assessor to evaluate risks or the Manage Audit feature to enable auditing on Mac OS X computers.

You should also verify that the computer has .NET Framework, version 4.5 or later installed. You can download the .NET Framework from the Microsoft Download Center, if needed:

.NET Framework version 4.5.2

Centrify also recommends the following minimum hardware configuration:

- 2 GB RAM
- 1 GB free disc space
- 2 GHz processor

You must also have network connectivity from the computer where you install Deployment Manager to each of the UNIX, Linux, and Mac OS X computers you want to manage.

Running the standalone setup program

You can install Deployment Manager as a standalone executable using its own individual setup program. If you downloaded the Centrify Express DirectManage Deployment Manager software package from the Centrify website, the package includes a standalone setup program for installing Deployment Manager outside of the suite. You can also install Deployment Manager using the standalone setup program packaged with the other DirectManage components if you want to install it without any other suite components.

If you are installing Deployment Manager as a component of Centrify Server Suite, see the *Centrify Server Suite Planning and Deployment Guide*.

To install Deployment Manager with its standalone setup program:

1. Double-click the `CentrifyDM-`*`version`*`-win32.exe` or `CentrifyDM-`*`version`*`-win64.exe` Deployment Manager setup program.
2. If a User Account Control message is displayed, click **Yes**.
3. At the Welcome page, click **Next**.
4. Click **I accept the terms of the License Agreement**, then click **Next**.
5. Accept the default location for Deployment Manager files or click **Change** to select a different location, then click **Next**.

   If a previous version of the Deployment Manager database is found on the local computer, you are prompted to convert the database to the current version. As part of this data migration step, you can create a backup copy of the current database in a specified location and choose whether to overwrite any previously saved backup copy. To upgrade the database and continue with the installation, click **Next**.
6. Click **Install** to start the installation.
7. Leave the Launch DirectManage Deployment Manager console option selected if you want to open Deployment Manager automatically, then click **Finish** to close the setup program.

Where files for Deployment Manager are installed

By default, Deployment Manager files are installed in the following location:
`C:\Program Files\Centrify\Deployment Manager`

The setup program also creates directories for Deployment Manager under the *User* directory of the person who installs Deployment Manager. Depending on the version of Windows you are using, the path to these additional directories will vary.

On older versions of Windows, the path to the additional Deployment Manager directories is this:
`C:\Documents and Settings\User\Application Data\Centrify\DeploymentManager`

On new versions of Windows, the path to the additional Deployment Manager directories is this:
`C:\Users\User\AppData\Roaming\Centrify\DeploymentManager`

The `DeploymentManager` directory contains:

- The database file (`datastore.sdf`) that stores all of the information Deployment Manager collects. Deployment Manager handles all database management tasks for this file automatically.
- A `Log` directory to contain log files if logging is enabled.
- A `Packages` directory to contain the software packages that you download and plan to deploy on remote computers.

Note You can change the location of the `Log` directory or the `Packages` directory. For example, you can move those directories to a shared network folder to make them accessible to multiple users. You should not, however, move the database file or attempt to share it with multiple users. If you choose to encrypt and store account credentials in the Deployment Manager database, only the user account used to encrypt them can decrypt them.

Removing Deployment Manager from a computer

You can remove Deployment Manager from a computer using the standard Control Panel for managing Windows programs. For example, you can open the Programs and Features Control Panel, select Deployment Manager in the list of installed programs, then click **Uninstall**. If you are prompted to confirm the removal, click **Yes**.

Uninstalling Deployment Manager does not remove the Microsoft SQL Server Compact Edition database that contains the information gathered by Deployment Manager, however. If you install a new version of Deployment Manager, all of the information from the previous version is still available.

If you want to completely remove Deployment Manager and all existing information from your computer, you can manually delete the `datastore.sdf` database file. Deleting the `datastore.sdf` file removes the Deployment Manager database and all of the information previously collected. To completely remove Deployment Manager, you should also delete the contents of the `Packages` directory, which contains any software packages you downloaded.

Getting started with Deployment Manager

This chapter describes how to work with the Deployment Manager console, including the basic steps for performing a security assessment and deploying Centrify software.

The following topics are covered:

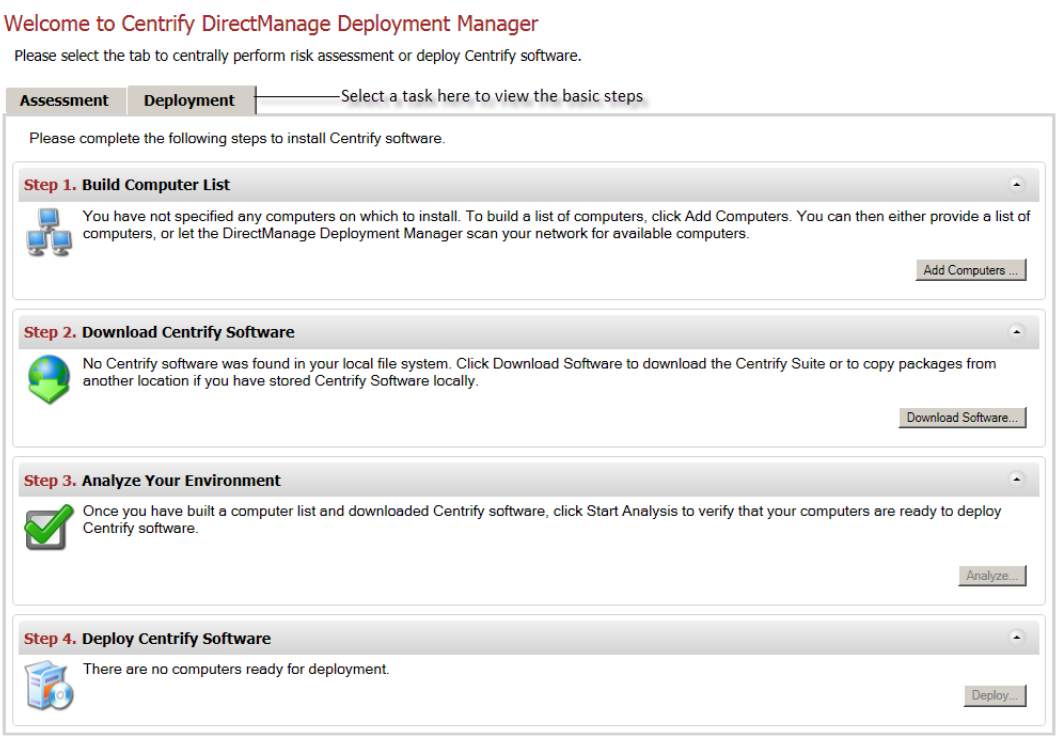
- Starting Deployment Manager for the first time
- Basic steps for performing a risk assessment
- Basic steps for deploying Centrify software

Starting Deployment Manager for the first time

By default, Deployment Manager launches automatically when you finish running the setup program. If you deselect the Launch DirectManage Deployment Manager console option, you can start Deployment Manager at any time from the Start menu or by clicking the DirectManage Deployment Manager desktop icon.

Deployment Manager is a standard Microsoft Management Console with navigational nodes in the left pane, and results in the right pane. Initially, the Deployment Manager left pane only displays the Centrify DirectManage Deployment Manager node and a Welcome page with tabs for Assessment and Deployment tasks in the right pane. By default, the steps for

Deployment are displayed because deployment is the more common task. In most cases, however, you would perform a security assessment on remote computers before deploying.



As you complete steps in the security assessment or deployment process, Deployment Manager adds information to the Assessment tab or Deployment tab on the Welcome page and navigational nodes to the left pane. For example, after you add computers, the left pane in Deployment Manager will include the Computers and History nodes and the Welcome page will display your computer inventory. Similarly, after you download software, Deployment Manager displays a Software node. You can then use these navigational nodes to access and manage the information stored in the Deployment Manager database.

Basic steps for performing a risk assessment

Performing a security assessment can help you evaluate remote computers for potential security risks, compliance issues, and operational inefficiencies that might be costly for your organization. With Deployment Manager, there are four simple steps to complete the security assessment:

1 Identify the computers to evaluate.

You can specify how to find the remote computers you want to evaluate, for example, by specifying a local subnet or range of IP addresses of interest.

2 Download the assessment tools software.

The assessment tools software package contains the platform-specific `surveyor` program for the computers you want to evaluate.

3 Start the assessment on remote computers.
The `surveyor` program runs on the computers you have selected for evaluation and checks for a wide range of potential issues that you might want to address to improve security in your organization.

4 Generate the identity risk assessment report.
After the `surveyor` program has collected information from the computers selected for evaluation, you can generate an executive summary of the results or a summary and a detailed report that includes information about the specific tests performed on individual computers.

The security assessment is an optional preliminary step that helps you identify and evaluate risks before deploying Centrify software. In most cases, you should complete a security assessment once on each target set of computers where you plan to deploy the Centrify agent. You can also run the security assessment after deploying agents if you want to compare before and after results.

Basic steps for deploying Centrify software

With Deployment Manager, there are four simple steps to complete the deployment of Centrify software:

1 Add computers to Deployment Manager.
You can specify how to find the remote computers you want to add to the Deployment Manager inventory, for example, by specifying a local subnet or range of IP addresses. Deployment Manager attempts to connect to the computers matching the criteria you specify and collects information—such as the host name and operating system—about the computers it finds. If you have already added the computers of interest as part of a security assessment, you can skip this step.

2 Download the analysis tools and agent software.
You can download Centrify analysis tools and agents from the Centrify Download Center or by connecting to a network drive.

3 Analyze remote computers.
You can select any computers that were successfully discovered, and have Deployment Manager analyze them to determine whether they are ready for deployment or have potential issues.

4 Deploy Centrify software.
You can select the computers that are ready to have software installed or upgraded and deploy the Centrify agent to those computers. Optionally, you can join an Active Directory domain during this step or later after the files are installed.

After you complete each step, Deployment Manager displays the results on the Deployment tab and updates the navigational nodes in the left pane.

In most cases, you complete the deployment process for one target set of computers at a time. After deployment, you can use Deployment Manager to perform other administrative tasks, for example, to manage accounts or enable auditing on a remote computer. You can also repeat steps at any time. For example, if you add computers to the network or want to update Centrify software, you would repeat the steps for adding computers or downloading software.

Performing an identity risk assessment

This chapter explains how to perform a security assessment with Deployment Manager. The security assessment is an optional step that helps you evaluate the current state of remote computers in your organization and identify potential vulnerabilities in the security of your network. In most cases, you perform the security assessment before deploying Centrify software. If you are not performing a security assessment, you can skip this chapter and continue to "Deploying Centrify software packages" on page 29.

The following topics are covered:

How the risk assessment works

As described in "Basic steps for performing a risk assessment" on page 17, you start a risk assessment by identifying the remote computers you want to evaluate and downloading the assessment tool software package. The assessment tool software package contains the platform-specific `surveyor` program. When you begin the assessment, the `surveyor` program runs on the remote computers and checks for a wide range of common issues. For example, the `surveyor` program checks the authentication methods you currently use and identifies weak encryption algorithms that might leave computers vulnerable to attack. The `surveyor` program also examines the password policies and login history for local user accounts, the use of the `root` user account, and security settings in configuration files to identify potential areas of concern that might affect the security, compliance, or operational efficiency of your organization.

The `surveyor` program returns the results from tests on individual computers and across all computers evaluated to Deployment Manager. Based on the number and severity of issues reported by the `surveyor` program, you can then use Deployment Manager to generate a report that summarizes your overall risk level in the following main categories:

- User credentials and privilege management policies.
- Computer access policies.

- Security configuration settings.

The assessment report identifies, at a high-level, where you have the most risk, the types of issues detected, and recommendations for ways to reduce the risk your organization faces. You can also generate a detailed report that captures the specific issues found on each computer with additional information about the tests performed, the result or each test, and why the issue reported might be a cause for concern.

Identifying the computers to evaluate

The first step in the security assessment is to identify the remote computers you want to evaluate. You can identify the computers to include by specifying search criteria, such as a subnet and mask or a range of IP addresses, in the Add Computers wizard. The Add Computers wizard checks for computers matching the criteria you specify and returns the discovered computers in a list. You can then choose which computers to keep. The computers you select are added to the Deployment Manager database and available for you to manage from the Deployment Manager console.

Preparing to discover computers

To gather information, Deployment Manager must be able to connect to each computer that matches the criteria you specify. To ensure a successful discovery, you should do the following before you start the Add Computers wizard:

- Verify that your have network connectivity to the remote computers you want to include in the assessment.
- Verify that all of the computers you want to evaluate allow secure shell (`ssh`) connections.
- Verify that you have a user name and password for an account with sufficient privileges to run administrative commands on each computer.

  If you have the `ALL` permission granted in a `sudoers` file for your own account or a master `root` account and password for all computers, you can provide this information once and store it in the Deployment Manager database.

- Decide which method to use for discovering computers and collect the necessary information.

  For example, if you want to use a specific subnet or IP-address range, you should know the subnet address or range to search. If you import a list of computers from a text file, you should prepare the text file in the proper format before starting the Add Computers wizard.

  For information about creating a list of computers to discover, see "Adding computers from an import text file" on page 22.

Identifying an account to use for the risk assessment

If you have a user name and password for an account that is allowed to use the `root` password or been granted `ALL` permission in the `sudoers` file on the computers you want to discover, no additional configuration is necessary. With the `root` password or `ALL` permission granted, Deployment Manager can execute all of the commands required for the risk assessment. If the account you want to use is configured in a `sudoers` file that only grants permissions for specific commands, the `surveyor` might not be able complete all tests. The detailed portion of the assessment report will indicate if any tests were skipped.

Adding computers from an import text file

When you run the Add Computers wizard, you have the option to import a list of IP addresses or host names from a text file. This option is especially useful if you have a spreadsheet, database report, or Wiki site where you have already recorded information about the computers you want to evaluate.

To create a text file for discovering computers, you must list each computer name or IP address on a separate line. You can also provide optional login information for each computer. The basic format for entries in the file is:
ip|*host*,[*user*],[*password*],[*privilege_command_type*],[*privilege_passwd*]

If you want to add comments at the beginning of a line or after a host name, use the pound (#) symbol. Everything after the # sign is ignored. For example:

```
# My list of computers to discover
192.168.133.1                          # no login credentials
jules-rh5                              # no login credentials
shea-sol10,root,aJuba8!,none           # with account information
kayla-hpux,kayla,Gr8tful,sudo,aJuba8!  # with account information
```

You can save the file in any well-known location. When you run the Add Computers wizard, you type the path or browse to the file.

If you include privileged account information and any passwords in the text file, be sure to delete the file after the listed computers are discovered. If you do not include the account information in the text file, you can set a user name and password for each computer in Deployment Manager after running the Add Computers wizard.

The Add Computers wizard displays a sample import file with comments that describe the format. For additional details about the format of the import file, see the sample displayed in the Add Computers wizard.

Starting the Add Computers wizard

After you have decided on a method for discovering computers in your network, you can use the Add Computers wizard to provide the information required for Deployment Manager to connect to the computers you want to include in the assessment.

To add computers to be evaluated:

1 Start Deployment Manager.

By default, you should see Centrify DirectManage Deployment Manager selected in the left pane and the Deployment tab on the Welcome page displayed in the right pane.

2 Click the Assessment tab on the Welcome page.

3 Click **Add Computers** in Step 1.

4 Select the method for discovering the computers to add, then click **Next**.

- Discover computers from the network
- Import a computer list from a text file
- Add a single computer

If adding a single computer, type the computer name or IP address, click **Next**, then skip to Step 8.

5 Specify the criteria for discovering computers of interest, then click **Next**.

- If discovering computers on the network, select the local subnet, a subnet address and mask, or a range of IP addresses.
- If importing computers from a file, browse to the location of the text file to import.

6 Review the list of computers Deployment Manager found to see if any should be removed, then click **Next**.

If Deployment Manager can connect to computers matching the criteria you specified, those successfully discovered computers are selected to be added to the computer inventory by default. You can deselect any successfully discovered computer that you want to exclude from the inventory.

7 Review the list of computers matching the criteria you specified that Deployment Manager could not access to select any that should be added, then click **Next**.

If Deployment Manager cannot establish a connection, it displays the unreachable computers in a separate list. You can add computers that are inaccessible. However, you must resolve the connection issue before you can proceed with the risk assessment for unreachable computers.

8 Type account information that will enable you to log on and run privileged commands on each computer, then click **Next**.

- Type a **User name** with permission to log on to one or more of the computers you are adding. In most cases, you should use your own user account or another user account that can log on to multiple computers. Although you can use the `root` super-user account, Centrify recommends that you use a standard user account with the ability to run privileged commands on the computers you are adding.
- Select the **Specify privileged command in tasks that require root privilege** option if using your own user account or another user account to execute privileged commands. If you are using the `root` user account to log on, leave this option unchecked.

- For Execute using, select **sudo** to use `sudo` and settings in the `sudoers` file or **su** to use the switch user (su) command to execute privileged commands.
- Type the password for the `root` user or for your own account.

  If you are executing privileged commands using `sudo`, the policies defined in the `sudoers` file determine whether you should type the `root` password or the password for your own account. To ensure the account can execute all required privileged commands, Centrify recommends that you grant the `ALL` permission to that user name in the `sudoers` file.

  If you are executing privileged commands using `su`, you must provide the `root` password.

You can only use DirectAuthorize to control the execution of privileged commands if you have defined rights, roles, and role assignments using DirectManage Access Manager. For information about defining rights, roles, and role assignments, see the *Centrify Server Suite Planning and Deployment Guide*.

The information you provide is stored in the Deployment Manager database as described in "Storing information securely" on page 12. You can then use this same information on additional computers or specify different account information for any of the computers you are adding.

9 Select the authentication method and provide the password or private key information for the user account you specified in Step 8, then click **Next**.

- Select **Authenticate using password** to authenticate by typing the password for the user name you specified in Step 8.
- Select **Authenticate using private key** if you want to use a private key instead of a password to authenticate your identity on to the computers you are adding. For example, use this option if you have a private key for `ssh`. You can then browse to and select the private key file and type the pass phrase for the private key.
- Select the **Enable remote terminal connection using private key** option to establish a remote connection and authenticate using a private key.
- Select the **Apply the same account to other computers** option to use the same user name, privileged command, and authentication method for multiple computers.

  You should select this option if the user account you specified in Step 8 has access to all or most of the computers you are adding or if you using a `root` account with the same password on the computers you are adding. If you don't select this option, you are prompted to enter separate credentials for each computer you are adding.

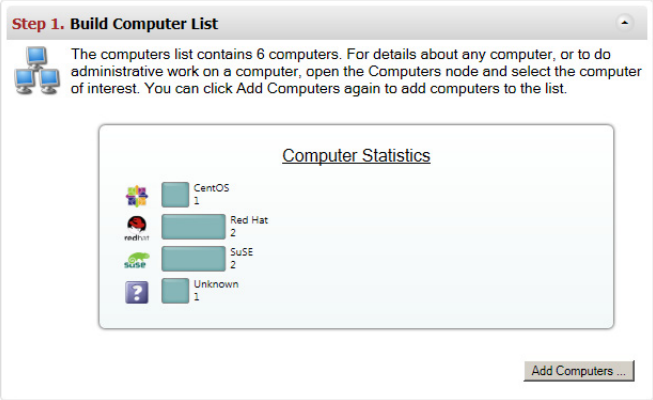
10 Select whether you want to use the existing account information for the next computer in the list or specify new account information, then click **Next**.

- If you are using the same user name and password for multiple computers, you are prompted to select the computers where the account information applies.

- If you are specifying different account information for some of the computers you are adding, repeat Step 8 to Step 10 for the each computer that requires different credentials.

11 Click **Finish** to exit the wizard and retrieve information for the specified computers.

After you complete the Add Computers step, the Deployment Manager console displays the navigational nodes for Computers, History, and Open Issues and the Welcome page displays the added computers in a graphic format, organized by platform. For example:



You can click on any category to expand the list of computers grouped by operating system and see details for individual computers. For example, click `Unknown` to see computers that were unreachable. You can then look at the Open Issues node for each of those computers to see why the computer was unreachable. For example, the Open Issues might indicate that the `ping` command failed or that the user credentials were invalid.

Downloading the assessment tool software

Before you can run the risk assessment on the computers you have discovered, you must first download the platform-specific Centrify Identity Risk Assessor and add it to the Deployment Manager database.

In most cases, you should download software packages from the Centrify Download Center. Connecting to the Centrify Download Center directly guarantees that you are getting the latest packages for the computer platforms you want to evaluate. However, if you are working within an isolated network, you can copy the packages to a network location beforehand, then download them to Deployment Manager from that location.

Note If you are copying software from a network or local folder or upgrading from a previous release of Deployment Manager, you might be required to import the offline Centrify product catalog to guarantee that you have the latest package information. Deployment Manager can import the product catalog automatically if it is located in the same network or local directory you select for the software download step. For more information about importing the product catalog, see "Importing the product catalog" on page 62.

To download the Centrify Identity Risk Assessor:

1 Start Deployment Manager.

By default, you should see Centrify DirectManage Deployment Manager selected in the left pane and the Deployment tab on the Welcome page displayed in the right pane.

2 Click the Assessment tab on the Welcome page.

3 Click **Download Software** in Step 2.

4 Select a location that is accessible to Deployment Manager from which you can download software, then click **Next**.

- Select **Download from the Centrify Download Center** if you have an Internet connection and a `centrify.com` account. You can then type the email address and password for the `centrify.com` account.

  If you have not registered for a `centrify.com` account, click the website link to set up a free account.

  You can also select **Remember my email and password** to save the account information and enable Deployment Manager to periodically check for and download software updates from the Centrify Download Center.

- Select **Copy from network or local drive** if you do not have an Internet connection and have copied the software to a network location. You can then type the path or click **Browse** to locate the folder that contains Centrify Identity Risk Assessor packages. After you have selected the location that has the software and clicked Next, skip to Step 6. Deployment Manager will automatically import the latest product catalog if it is located in the directory you specify.

5 Select the Centrify Identity Risk Assessor software package, then click **Next**.

6 Confirm the list of packages, then click **Finish**.

After you complete the Download Software step, the Deployment Manager console displays the navigational node for Software, and the Welcome page displays the packages you have downloaded.

Beginning the risk assessment

After you have added computers and downloaded Centrify Identity Risk Assessor packages, the computers that are ready to be evaluated are listed as Ready to Assess in the Perform risk assessment step.

To begin the risk assessment:

1 Start Deployment Manager.

By default, you should see Centrify DirectManage Deployment Manager selected in the left pane and the Deployment tab on the Welcome page displayed in the right pane.

2 Click the Assessment tab on the Welcome page.

3 Click **Begin Assessment** in Step 3.

If you want to analyze a subset of computers listed, expand the Ready to Assess category, then select individual computers.

As described in "How the risk assessment works" on page 20, Deployment Manager starts a `surveyor` program that performs a series of tests on each computer you are evaluating. The `surveyor` program returns the results from tests on individual computers and across all computers evaluated to Deployment Manager. The time it takes to complete the analysis depends are the number of computers being analyzed and your network configuration.

When all of the tests are complete, the results are listed in the Archived Assessment Results list. You can then generate a report to display the results.

Generating the identity risk report

After the `surveyor` program returns the assessment results, they are listed as Archived Assessment Results. You can select any of the archived assessment results to generate a report that highlights potential risks and areas of concern. You can also delete any previously archived assessment result if it is no longer needed. Keep in mind, however, that you won't be able to generate reports for the assessment results you delete.

To generate the identity risk assessment report:

1 Start Deployment Manager.

By default, you should see Centrify DirectManage Deployment Manager selected in the left pane and the Deployment tab on the Welcome page displayed in the right pane.

2 Click the Assessment tab on the Welcome page.

3 Select the name of the archived assessment results

4 Click **Generate Report** in Step 4.

5 Accept the default location or click **Browse** to select a new location for the report output.

You should note that the report output that you generate from your assessment results is not stored in the Deployment Manager database. You can save, manage, and delete the report output through the file system in the location you select. However, because the assessment results are archived in the Deployment Manager database, you can regenerate the report output from a previous assessment, if needed.

6 Select the content to include in the report, then click **OK**.

By default, the report includes an executive summary and detailed information about the test results for each computer. You can select or deselect any of the detailed sections for the report.

- **Detailed test results per computer** provides detailed information about the tests performed and the results of each test on individual computers grouped by computer name.
- **Detailed test results per test case** provides about the tests performed and the results of each test grouped by test name and category.
- **Test results and scoring methodology** provides detailed information about how risk scores are determined and calculated.

Deployment Manager generates the executive summary and the detailed sections you select and displays the output in your default browser. Note that your browser configuration might require you to allow blocked content to view the report.

Reviewing the content of the risk report

The executive summary provides an overview of potential issues and your risk level in key areas of concern. This information is captured in pie charts and risk scores to help you quickly visualize where you might have vulnerabilities and where your current policies have reduced your organization's risks. The report also provides a simplified summary of findings and links to additional resources and information about issues found and best practices that could help you improve the security of you organization and reduce identity risks. To see more detailed information about individual tests, test results, or how risk scores are calculated, select the appropriate detail report options and regenerate the report.

Rerunning the risk assessment

You can rerun the risk assessment at any time to generate new assessment results and a corresponding assessment report. For example, if you make changes to the configuration of computers you have previously evaluated, you might want to rerun the Centrify Identity Risk Assessor on those computers. You can then compare the results of the new assessment with the previous assessment result to see the effect of your changes on your risk level.

If you run the Centrify Identity Risk Assessor before deploying other Centrify software, you might want to run the Centrify Identity Risk Assessor again after you deploy the software to see if there are additional steps you can take to improve security.

Deploying Centrify software packages

This chapter explains how to deploy Centrify software packages using Deployment Manager. If you performed the optional security assessment, the steps for deployment are similar.

The following topics are covered:

Identifying the computers you want to manage

The first step in the deployment process is to identify the computers on which to deploy Centrify software. If you performed a risk assessment and have already added the computers on which you want to deploy, you can skip this section and continue on to "Downloading Centrify software packages" on page 34.

If you are not performing a risk assessment, you can identify the computers on which to deploy by specifying search criteria—such as a subnet and mask or a range of IP addresses—in the Add Computers wizard. The computers you select are added to the Deployment Manager database and available for you to manage from the Deployment Manager console.

Preparing to discover computers

To gather information, Deployment Manager must be able to connect to each computer that matches the criteria you specify. To ensure a successful discovery, you should do the following before you start the Add Computers wizard:

- Verify that your have network connectivity to the remote computers you want to manage.

  If Deployment Manager is unable to reach a computer, you can continue to add it to the Deployment Manager inventory. However, you will need to resolve the network connectivity issue before you can continue with the deployment for that computer.

- Verify that all of the computers on which you want to deploy allow secure shell (`ssh`) connections.

You can configure Deployment Manager to attempt a `telnet` connection if you have legacy computers that don't support secure shell (`ssh`) connections. For more information about allowing `telnet` connections, see "Allowing telnet connections to remote computers" on page 76. On Mac OS X computers, you should verify that you have `ssh`—or `telnet` if allowing `telnet` connections—installed and enabled. These programs are not enabled by default on Mac OS X computers.

- Verify that you have a user name and password for an account with sufficient privileges to run administrative commands on each computer.

  If you have the `ALL` permission granted in a `sudoers` file for your own account or a master `root` account and password for all computers, you can provide this information once and store it in the Deployment Manager database. For more information about selecting an account to use, see "Identifying an account to use for deployment" on page 30.

- Decide which method to use for discovering computers and collect the necessary information.

  If you want to use a specific subnet or IP-address range, you should know the subnet address or range to search. If you import a list of computers from a text file, you should prepare a text file in the proper format before starting the Add Computers wizard. For information about creating a list of computers to discover, see "Adding computers from an import text file" on page 31.

Identifying an account to use for deployment

If you have a user name and password for an account that is allowed to use the `root` password or been granted `ALL` permission in the `sudoers` file on the computers you want to discover, no additional configuration is necessary. With the `root` password or `ALL` permission granted, Deployment Manager can execute all of the commands required for deployment. If you want to explicitly configure a `sudoers` file that only grants permissions for specific commands required for deployment, you should note that some of the commands are operating system specific and the path for locating the commands can be different on different operating systems. If you configure the `sudoers` file to only include the required commands, be sure you use the commands and paths as appropriate for the operating system of the computer you are managing.

The following table summarizes the commands that the account you use for Deployment Manager must be able to run.

Basic commands	User and group commands	Centrify commands
`cat`	`useradd`	`/usr/bin/adcheck`
`cd`	`userdel`	`/usr/sbin/adinfo`
`chmod`	`usermod`	`/usr/sbin/adjoin`
`cp`	`passwd`	`/usr/sbin/adleave`
`chown`	`chgroup, groupmod`	`/usr/sbin/adreload`

Basic commands	User and group commands	Centrify commands
date	rmgroup, groupdel	/usr/sbin/dacontrol
domainname	mkgroup, groupadd	
dscl		
echo		
grep		
gunzip		
hostname		
ls		
lsldap		
mkdir		
mv		
rm		
sed		
sh		
stty		
touch		
vmware		
ypwhich		

The following is a sample `sudoers` section for Deployment Manager commands:

```
## Sudo policy for Centrify DirectManage Deployment Manager

User_Alias DMOPERATORS = vstest

Cmnd_Alias DMCOMMANDS = /bin/sh, /bin/ls, /bin/touch, /bin/grep, /bin/echo, /
bin/cat, /bin/mv, /bin/rm, /bin/sed, /bin/date, /bin/mkdir, /usr/bin/gunzip,
/bin/cp, /bin/chmod, /usr/sbin/adreload, /usr/sbin/dacontrol, /usr/sbin/
adjoin, /bin/hostname, /usr/bin/ypwhich, /bin/domainname, /usr/sbin/usermod,
/usr/sbin/groupmod, /usr/bin/passwd, /usr/sbin/userdel, /usr/sbin/groupdel, /
usr/sbin/adinfo, /usr/sbin/adleave, /usr/sbin/useradd, /usr/sbin/groupadd, /
usr/sbin/adcheck, /bin/stty, /bin/chown

DMOPERATORS ALL = DMCOMMANDS
```

Adding computers from an import text file

When you run the Add Computers wizard, you have the option to import a list of IP addresses or host names from a text file. This option is especially useful if you have a spreadsheet, database report, or Wiki site where you have already recorded information about the computers you want to discover.

To create a text file for discovering computers, you must list each computer name or IP address on a separate line. You can also provide optional login information for each computer. The basic format for entries in the file is:

ip|*host*,[*user*],[*password*],[*privilege_command_type*],[*privilege_passwd*]

If you want to add comments at the beginning of a line or after a host name, use the pound (#) symbol. Everything after the # sign is ignored. For example:

```
# My list of computers to discover
192.168.133.1                          # no login credentials
jules-rh5                              # no login credentials
shea-sol10,root,aJuba8!,none           # with account information
kayla-hpux,kayla,Gr8tful,sudo,aJuba8!  # with account information
```

You can save the file in any well-known location. When you run the Add Computers wizard, you type the path or browse to the file.

If you include privileged account information and any passwords in the text file, be sure to delete the file after the listed computers are discovered. If you do not include the account information in the text file, you can set a user name and password for each computer in Deployment Manager after running the Add Computers wizard.

Starting the Add Computers wizard

After you have decided on a method for discovering computers in your network, you can you can click Add Computers to provide the information required for Deployment Manager to connect to the computers you want to discover.

To add computers to Deployment Manager:

1. Start Deployment Manager.
2. Click **Add Computers** in Step 1.
3. Select the method for discovering the computers to add, then click **Next**.
   - Discover computers from the network
   - Import a computer list from a text file
   - Add a single computer

   If adding a single computer, type the computer name or IP address, click **Next**, then continue to Step 7.
4. Specify the criteria for discovering computers of interest, then click **Next**.
   - If discovering computers on the network, select the local subnet, a subnet address and mask, or a range of IP addresses.
   - If importing computers from a file, browse to the location of the text file to import.
5. Review the list of computers Deployment Manager found to see if any should be removed, then click **Next**.

   If Deployment Manager can connect to computers matching the criteria you specified, those successfully discovered computers are selected to be added to the computer

inventory by default. You can deselect any successfully discovered computer that you want to exclude from the inventory.

6 Review the list of computers matching the criteria you specified that Deployment Manager could not access to select any that should be added, then click **Next**.

If Deployment Manager cannot establish a connection to one or more remote computers, it displays the unreachable computers in a separate list. You can add computers from this list. However, you must resolve the connectivity issue before you can proceed with the deployment.

7 Type a user name with permission to log on to one or more of the computers you are adding.

In most cases, you should use your own user account or another user account that can log on to multiple computers. Although you can use the `root` super-user account, Centrify recommends that you use a standard user account with the ability to run privileged commands on the computers you are adding.

If you are adding multiple computers, the computer to which this information applies is the first computer in the list. You can then use this same information on additional computers or specify different account information for any of the computers you are adding.

8 Select the **Specify privileged command in tasks that require root privilege** option if you are using your own user account or another user account to execute privileged commands.

If you are using the `root` user account, you can leave this option unchecked.

9 Select **sudo** to use `sudo` and settings in the `sudoers` file or **su** to use the switch user (`su`) command to execute privileged commands.

You can only use DirectAuthorize to control the execution of privileged commands if you have defined rights, roles, and role assignments using DirectManage Access Manager. For information about defining rights, roles, and role assignments, see the *Centrify Server Suite Planning and Deployment Guide*.

10 Type the password for the `root` user or for your own account, then click **Next**.

- If you are executing privileged commands using `sudo`, the policies defined in the `sudoers` file determine whether you should type the `root` password or the password for your own account. To ensure the account you specified in Step 7 can execute all required privileged commands, Centrify recommends that you grant the `ALL` permission to that user name in the `sudoers` file.
- If you are executing privileged commands using `su`, you must provide the `root` password.

11 Select the authentication method and provide the password or private key information for the user account you specified in Step 7, then click **Next**.

- If you select **Authenticate using password**, type the password for the user name you specified in Step 7.
- If you select **Authenticate using private key** to use a private key instead of a password, click **Browse** to locate the private key file and type the pass phrase.

  This option is most commonly used when you have created a private key for using `SSH`. If you want to establish a remote connection to a computer using PuTTY and a private key, you can select the **Enable remote terminal connection using private key** option, then click **Browse** to locate the PuTTY private key file.

You can also select the **Apply the same account to other computers** option to use the same user name, privileged command, and authentication method for multiple computers. You should select this option if the user account you specified in Step 7 has access to all or most of the computers you are adding or if you using a `root` account with the same password on the computers you are adding. If you don't select this option, you are prompted to enter separate credentials for each computer you are adding.

12 Select whether you want to use the existing account information for the next computer in the list or specify new account information, then click **Next**.

- If you are using the same user name and password for multiple computers, you are prompted to select the computers where the account information applies.
- If you are specifying different account information for some of the computers you are adding, repeat Step 7 to Step 12 for the each computer that requires different credentials.

13 Click **Finish** to exit the wizard and retrieve information for the specified computers.

After you complete the Add Computers step, the Deployment Manager console displays the navigational nodes for Computers, History, and Open Issues and the Welcome page displays the added computers in a graphic format, organized by platform.

You can click a category to expand the list of computers grouped by operating system and see details for individual computers. For example, click `Unknown` to see computers that were unreachable. You can then look at the Open Issues node for each of those computers to see why the computer was unreachable. For example, the Open Issues might indicate that the `ping` command failed or the user credentials were invalid.

Downloading Centrify software packages

Before you can deploy, you must first download the platform-specific Analysis Tools and Centrify agents and make the software accessible to Deployment Manager.

In most cases, you should download packages from the Centrify Download Center. Connecting to the Centrify Download Center guarantees that you are getting the latest

packages for the computer platforms you manage. However, if you are working within an isolated network, you can copy the packages to a network location beforehand, then download them to Deployment Manager from that location.

Note If you are copying software from a network or local folder or upgrading from a previous release of Deployment Manager, you might be required to import the offline Centrify product catalog to guarantee that you have the latest package information. Deployment Manager can import the product catalog automatically if it is located in the same network or local directory you select for the software download step. For more information about importing the product catalog, see "Importing the product catalog" on page 62.

To download Centrify software packages for deployment:

1. Start Deployment Manager.
2. Click **Download Software** in Step 2.
3. Select a location that is accessible to Deployment Manager from which you can download software, then click **Next**.
   - Select **Download from the Centrify Download Center** if you have an Internet connection and a `centrify.com` account. You can then type the email address and password for the `centrify.com` account.

     If you have not registered for a `centrify.com` account, click the website link to set up a free account.

     Select Remember my user name and password to save the account information and enable Deployment Manager to periodically check for and download software updates from the Centrify Download Center.
   - Select **Copy from network or local drive** if you do not have an Internet connection and have copied the software to a local or network location. You can then type the path or click **Browse** to locate the folder that contains Centrify software packages. After you have selected the location that has the software and clicked Next, skip to Step 5. Deployment Manager will automatically import the latest product catalog if it is located in the directory you specify.
4. Select the Analysis Tools and Centrify agent software packages, then click **Next**.

   By default, packages are filtered to show only the latest software and to show only the packages that are applicable for the computer platforms that you have discovered. You can turn these filters off to select or deselect specific packages or packages for specific platforms.
   - If you deselect the **Show only the latest software** option, you can see and select older versions of the software packages available.
   - If you deselect the **Show only software for managed computers** option, you can see and select software packages for any supported platform.

For example, if you have used Add Computers to discover Red Hat and Debian Linux computers, by default, only the software packages that are applicable for those two platforms are available for you to download. The packages available for all other platforms are not visible. However, if you intend to add computers with different platforms at a later date, you might want to download packages for them now. In that case, deselect the **Show only software for managed computers** option, then select the individual packages you need.

5 Confirm the list of packages, then click **Finish**.

After you complete the Download Software step, the Deployment Manager console displays the navigational node for Software, and the Welcome page displays the packages you have downloaded.

Analyzing computers for potential issues

Before deploying software to computers on your network, you should first use the Analysis Tools to check whether the selected computers meet all the prerequisites. For example, the analysis tool, `adcheck`, verifies that selected computers have a supported operating system and required patches installed. The program also checks for potential problems that might prevent a successful deployment. For example, the analysis will report warnings or errors if DNS is not configured properly or does not respond to lookup requests, or if there are problems connecting to an Active Directory domain controller or locating the global catalog.

Note You should download the Analysis Tools for all platforms you intend to support and run the analysis on all of the computers you plan to manage.

To analyze your environment for a successful deployment:

1 Start Deployment Manager.

2 Select the Identified but Not Analyzed category, then click **Analyze**.

After the initial discovery, computers that are reachable with a recognized operating system are listed as **Identified but Not Analyzed** under Computers Not Analyzed. If you have computers listed as **Not Identified**, you should check the Open Issues for those computers. It may be that the IP address was found but not reachable or that the computer has an unsupported operating system.

If you want to analyze a subset of computers, expand the Identified but Not Analyzed category, then select individual computers.

3 Type the Active Directory domain name and select an option for the domain controllers to analyze, then click **OK**.

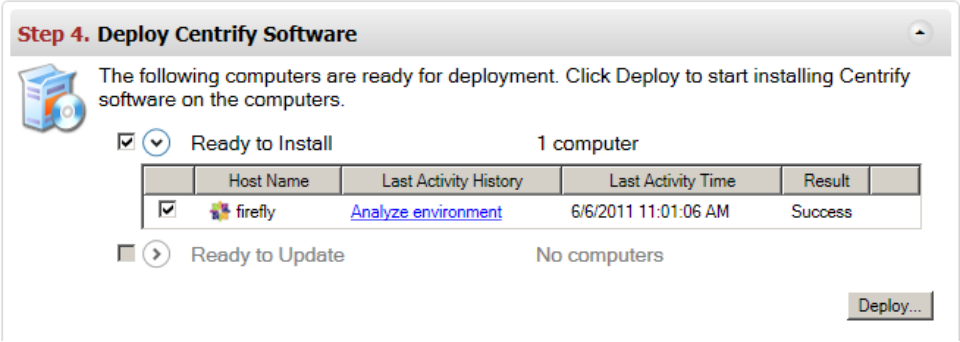
You should specify the domain you intend to join for the selected computers. Optionally, you can connect to a maximum number of domain controllers, a specific domain controller, or all domain controllers in a site for the analysis.

4 Click **OK** to begin analysis.

Deployment Manager analyzes each computer in the selected set of computers to determine its status, compatibility for installing Centrify software, and the ability to join an Active Directory domain. The time it takes to complete the analysis depends are the number of computers being analyzed and your network configuration.

Deployment Manager then displays the results of the analysis by listing computers in different categories. For example, computers that do not have an agent installed are listed under the Computers with No Centrify Software category as Ready to Install, Ready to Install with Warnings, or Not Ready to Install.

If no issues are detected during the analysis, Deployment Manager moves the computer into the Read to Install category under Step 4. For example:



5 Expand the categories to explore the computers that have issues or warnings that might prevent software from being installed or updated.

6 Restart computers that are reported as Not Ready to Install or Not Ready to Update to ensure that the operating system boots properly before making any changes to those computers.

7 Review and resolve open issues for each computer.

8 Re-run the Analyze command for one or more computers in your environment to verify your fixes.

Review and resolve open issues

There are many common problems that the Analysis Tools can report that will require you to make changes before installing Centrify software. For example, if the analysis finds there's not enough disk space available on a particular computer, it reports this information as an open issue for that computer. You can then view the details about that open issue to see more detailed information how much more disk space is required.

Viewing details about Open Issues

You can view the open issues for all computers in the repository or for individual computers by selecting Open Issues under the Centrify Deployment Manager node or an individual computer node or by viewing a computer's details in the analysis results.

To see the details about an open issue, select the issue, right-click, then select **Properties**. Properties for an open issue typically provide suggestions for how to resolve the issue or whether the issue can be ignored.

Resolving open issues

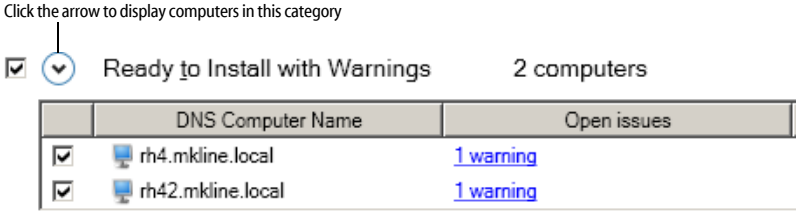
The options available for resolving open issues from Deployment Manager depend on the type of issue reported. For most issues, you can right-click and select one of the following responses:

Select	If the issue is
Ignore	A warning or informational issue that is not fatal and you can deploy software without making changes to the computer with the issue. Selecting Ignore removes the issue from the list of Open Issues.
Re-analyze	A warning or informational issue that you have fixed since the last time you analyzed the computer. For example, if the computer was offline, and is now online, the new analysis should resolve connection issues.
SSH	A warning or an error that you can fix by logging on to the remote computer using a secure shell (`ssh`) connection. Centrify recommends you use secure shell (`ssh`) connections to perform administrative tasks whenever possible.
Telnet	A warning or an error that you can fix by logging on to the remote computer using a `telnet` connection if you configure Deployment Manager to allow `telnet` connections.

Some issues also provide specific solutions for you to select on the right-click menu. For example, if the user name or password provided for a computer is not valid or has not been specified, you can right-click that open issue, and select the **Set user name and password** option to update the user name and password. If a computer displays the **Check clock synchronization** issue, the right-click menu allows you to select **Synchronize Clock** to correct the issue.

To resolve the errors and warnings that were found:

1 Expand one of the categories with errors or warnings. For example, click the expansion arrow for computers listed as **Ready to install with Warnings**.



2 Click on the warning or error message link to display details about the issue found for the selected computer.

3 Take an appropriate action to resolve the issue reported.

For more information about responding to warnings and fixing errors, see "Resolving open issues" on page 57.

Re-analyzing target computers after resolving open issues

You should always re-run the analysis of your environment after resolving issues to verify your changes fixed the problem and that no new issues have been introduced. You can re-run the Analyze command for all or selected computers in selected categories at any time. You can also select individual computers, right-click, then select Analyze Environment to re-run the analysis on a specific computer.

Deploying agents on remote computers

After you have analyzed computers and resolved any open issues, such as installing patches or rebooting computers that were unreachable, you should see computers listed under Step 4. Deploy Centrify Software as Ready to Install.

Deployment Manager determines the correct version of the Centrify agent to install on each computer and records details about the installation and other activities under the History node.

To deploy an agent on the computers that are ready:

1 Start Deployment Manager and select the **Centrify Deployment Manager** node.

2 Under Step 4. Deploy Software, select the computers that are in the Ready to Install category, then click **Deploy**.

You can click the check box for a category to select all computers in that category, or expand a category to select computers individually.

3 Select the edition to install, then click **Next**.

The edition you select controls the features that are available in the agent you are installing. For example:

- **Centrify Express** is a free version of the agent that provides the ability to join a domain and authenticate users.
- **Centrify Server Suite Standard Edition** is a fully-featured version of Centrify software for access control and privilege management that includes extensions for managing NIS maps and applying group policies.
- **Centrify Server Suite Enterprise Edition** is an enterprise version of Centrify software that includes all of the components of the Standard Edition, plus additional

components that enable a managed computer to act as a NIS server, and components that enable session-level auditing.

Depending on the operating system of the computers where you are installing the agent and the suite edition you select, the remaining steps in the Manage Software wizard vary. Follow the prompts displayed. For more information about any step, press F1 to display context-sensitive help.

4 Select the version of the suite edition you selected to install, then click **Next**.

5 Select the specific components of the suite that you want to install, then click **Next**.

6 Select the operation to perform after installation, if prompted, then click **Next**.

For example, select one of the following options:

- **Add computers to Active Directory and join Auto Zone** if you want to have user and group profiles generated automatically after installing the software. If you select this option, follow the prompts displayed to specify how profiles are generated.
- **Add computers to Active Directory and join a specific zone** if you want to join a specific zone after installing the software. If you have existing users and groups, you should prepare for migration before adding computers to an Active Directory domain and a zone to prevent the migration from disrupting user activity. If you select this option, follow the prompts displayed to specify domain and zone information.
- **Do not add computers or join after install** if you want to complete the software installation but join a domain and zone at a later time. If you select this option, you can use the Manage Zone wizard to join after you have analyzed your user population and prepared for migration.

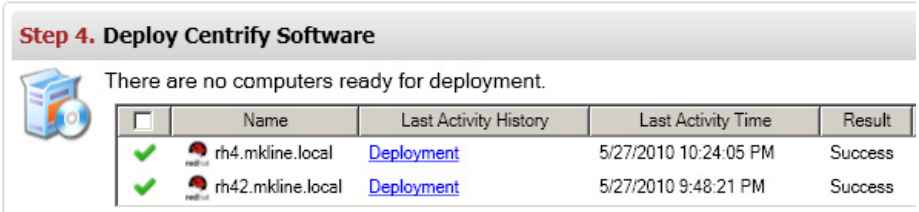
For more information about joining a domain and zone, see "Joining the domain from Deployment Manager" on page 41. For more information about any step, press F1 to display context-sensitive help.

7 Check the default list of service types and service principal names, then click **Next**.

You can add or remove services and service principal names, if needed. The default services listed are the most commonly used services. For each service, there are two service principal names: the computer name and the computer name and domain.

8 Review your selections, then click **Finish** to install software on the selected computers.

When the deployment of software packages is complete, the Welcome page displays a check mark for each computer on which software was successfully deployed.



Joining the domain from Deployment Manager

You have the option to join the domain directly from the Manage Software wizard or at a later time from within Deployment Manager or by running the `adjoin` command. In most cases, you should join the domain as a separate step from deploying the software. The delay between installing the software and joining the domain enables the user community to verify that the software installation does not affect their day-to-day activities and allows administrators time to prepare for migration and import existing users and groups into Active Directory.

To join computers to the Active Directory domain using Deployment Manager:

1. Log on to the computer where Deployment Manager is installed using an account with permissions to both create computer objects and join computers to zones.

   In most cases, you can use a member of the Join Operators or Zone Administrators group.

2. Start Deployment Manager.
3. Select the **Computers** node.
4. Select one or more computer objects in the right pane, right-click, then select **Manage Zone**.

   If the Manage Zone option is not available, select **Refresh Computer Information** to make sure a connection to the selected computer is available on the network.

5. Select **Join computers to zone**, then click **Next**.
6. Select whether you want to add the computers to Auto Zone or to a specific zone, then click **Next**.
   - You should select Auto Zone if you want to simplify the management of user and group profiles but do not want to create and manage zones, delegate zone administration, or configure rights, roles, and role assignments.
   - You must add computers to a specific zone if you want to create role-based access controls and assign roles to users.
7. Specify the Active Directory user credentials to use to join the domain, then click **Next**.

   You must provide an account that can connect to Active Directory. The account must also have permission to create new computer objects under the default Computers container for the specified domain, unless you have previously prepared a computer account to use.

   If you have previously created a computer account in Active Directory, you can select **Use current login user** and **Use precreated computer object** to join using the previously prepared computer object.

8 Type a zone name or click **Browse** to search for and select the zone to join.

For example, after clicking **Browse**, type all or part of the zone name, click **Find Now**, then select the zone in the results and click **OK**.

Keep in mind that a computer can only be joined to one zone at a time. Your initial analysis of the user population and zone design should identify a child zone for the computer to join.

9 Specify additional join options, as needed, then click **Next**:

- Select the **Computer name** and **Computer alias** options if you have disjointed DNS. For example, if the Active Directory DNS uses `ocean.local` but the remote computer is registered in DNS with `ocean.net`, you should specify the computer name as *`computer`*`.ocean.local` and the computer alias as *`computer`*`.ocean.net`.
- Click **Container**, then click **Change** to navigate to and select an organizational unit for the computer account, then click **OK** to continue selecting join options.
- Click **Domain controller**, then type the fully-qualified domain name for a specific domain controller to ensure that the remote computer connects to the appropriate domain controller even if Deployment Manager connects to a different domain controller.
- Select **Trusted for delegation** if you want users to be able to forward their Kerberos ticket-granting ticket to other remote computers as they move around the network. This is useful option if users typically use SSH to a gateway computer, then use SSH to remotely access other computers from that computer.

10 Select either Server license or Workstation license as the type of license to be used, then click **Next**.

11 Review and modify, if necessary, the list of service principal names for the services provided by the computer, then click **Next**.

You can click **Add** to add more service principal names or select one or more of the service principal names listed if you want to modify or remove a service principal name.

12 Specify whether to use the current credentials or another administrative account after joining the domain, then click **Next**.

If group policies lock down the use of the `root` account, you should specify an alternate account with appropriate permissions to perform administrative functions after the computer has joined Active Directory.

If you are not keeping the current credentials, type the user name and password for an Active Directory account. You can also select which privileged command to use for tasks requiring `root` permissions: DirectAuthorize (`dzdo`), the `su` command, or `sudo` and the `sudoers` file. If you select the `su` command, you must type the password for the local `root` user on the computer joining the domain.

Note You should only select DirectAuthorize after you have defined a role with permission to execute privileged commands.

13 If you selected Centrify Server Suite Enterprise Edition, you must specify an auditing installation to which agents send audit data.

If you want to specify the installation later or the location of the installation is published by using the Installation group policy, click **Next**. You can use the Manage Audit wizard to specify the installation name from Deployment Manager at a later time if you are not using group policy. If the installation is configured manually, you can specify the installation name, then click **Next**.

14 If you selected Centrify Server Suite Enterprise Edition, you can specify whether to enable or disable auditing, then click **Next**.

15 Review information about the join, then click **Finish** to join selected computers to the specified domain and zone.

After you click Finish, Deployment Manager opens an secure shell connection to the remote computer and changes to the `root` account (or `sudo`) to run the `adjoin` command.

Performing administrative tasks using Deployment Manager

This chapter describes the information stored in the Deployment Manager database and how to perform administrative tasks using Deployment Manager.

The following topics are covered:

Working with computers

After you have discovered computers, you can view and manage those computers from Deployment Manager by expanding the **Computers** node. The computers are organized into categories to help you quickly find computers of interest based on specific criteria. For example, you can navigate to computers grouped by operating system or by zone or locate the computers that have Centrify software installed. From these different computer-related categories, you can select individual computers to complete administrative tasks.

Viewing and modifying computer information

As you select computer categories, Deployment Manager displays the list of computers in that category with detailed information about each computer, including the host name, IP address, operating system, platform, and architecture. After you deploy Centrify software on discovered computers, you can see additional details about the versions of the software you have installed.

In addition to the details displayed for computers in the computer list, you can view and modify information—such as the port used for remote secure shell (ssh) connections and the credentials used to access—for individual computers. To change the information for an

individual computer, select the computer name, right-click, then click **Properties**. From the computer properties, you can click:

- **Deployment** to view and change deployment information, such as computer name, location, IP address, operating system, agent version, joined domain and zone, and whether the computer is configured as a NIS or LDAP server. For example, you might click **Credentials** to view or edit the credentials used for remote connections to the selected computer.
- **Notes** to record any information about the computer. For example, you might use this tab to record the department and user group responsible for managing the computer.
- **Network** to view and change network information such as the port used for secure shell connections, the prompt to expect on the target computer, and the console responses to expect on the target computer. For example, you might use this tab to specify the custom prompt configured for the computer.

If you make any changes to the computer properties, click **Apply** to save your changes and continue working or click **OK** to save your changes and close the properties dialog.

What to do if a computer is listed as unknown

If Deployment Manager was not able to access a computer during discovery, it shows the host name as `<Unknown>`. You must be able to connect to those computers before you can view details or manage operations for them using Deployment Manager.

If a computer is listed as `<Unknown>` in any category, check for the following most common causes:

- Access to the computer is blocked by a firewall.
- The DNS server might not be configured properly to locate the computer.
- The secure shell (`ssh`) client package might not be installed on the computer or the `ssh` process might not be running.
- The IP address is another type of resource, such as a printer.
- The user name, password, or privileged command information might not be valid for the computer.

Viewing details for individual computers

You can view information that is specific to a individual computer. For example, you might want to review and resolve open issues that are specific to one computer without viewing issues for any other computer. You might also want to see locally defined users for a computer isolated from the users defined on other computers.

To view information that is specific to a computer, select and expand the computer name, then select one of the following:

- **Groups** to list the groups that are defined locally on the selected computer.

- **Users** to list the users that are defined locally on the selected computer.
- **Open Issues** to list the issues that you need to resolve before installing Centrify software on the selected computer.
- **History** to list all the actions performed on the selected computer, and whether the action was successful.

Managing activity on discovered computers

If you select an individual computer, you can right-click or use the Action menu to perform administrative tasks on that computer. You can manage computers from Deployment Manager by selecting any of the following administrative activities from the right-click or Action menu:

- Analyze Environment
- Refresh Computer Information
- Manage Software
- Manage Audit
- Manage Zone
- Download Sudoers File
- Remote Session
- Export Users and Groups
- Run Script
- Delete
- Properties

Analyze Environment

Select this action to check whether a selected computer meets the system requirements for Centrify software. If you select this action and there are potential problems, they are listed as errors or warnings under the Open Issues for the selected computer. This action is the same as analyzing the environment during deployment, but is most often used to re-run the analysis on a computer after making changes.

Refresh Computer Information

Select this action to update information for a selected computer. Deployment Manager connects to the computer and refreshes information, such as the domain, zone, computer name, and installed Centrify software.

Because administrators can perform operations on computers without using Deployment Manager, it is possible for the information recorded in the Deployment Manager database to become out-of-date. For example, if an administrator logs on to a computer and

manually deletes Centrify files, Deployment Manager has no record of the activity and might indicate that Centrify software is still installed. Similarly, if an administrator connects to a computer using `putty` and adds or deletes local users or groups, Deployment Manager will not show an accurate list of users and groups.

You should periodically refresh the computer information to ensure Deployment Manager presents an accurate view of your environment.

To refresh computer information:

1 Navigate to and select one or more computers.

2 Right-click and select **Refresh Computer Information**.

While Deployment Manager is connecting to one or more computers to update information, it displays the busy icon for the selected computers and for all the nodes that contain them.

Manage Software

Select this action to install, modify, or remove Centrify software on a selected computer.

Manage Audit

Select this action to specify an installation name, enable auditing, or disable auditing on a selected computer. This option is only available if the auditing service is installed on the selected computer. You can also enable or disable auditing by running the `dacontrol` command directly on a managed computer.

To enable or disable auditing from Deployment Manager:

1 Navigate to the computer in the left pane, right-click, then click **Manage Audit**.

2 Specify whether to use the current installation name or change the installation name, then click **Next**.

3 Specify whether to enable or disable auditing, then click **Next**.

4 Click **Finish** to complete the changes you made.

Manage Zone

Select this action to join a selected computer to a new Active Directory domain and zone or leave the domain. If you select **Join computers to a zone**, this action is the same as "Joining the domain from Deployment Manager" on page 41. If you select **Remove computers from the zone**, you can use this action to leave an Active Directory domain and zone.

You can join any computer on which you have installed the agent to an Active Directory domain. For computers that are already joined to a zone, you can move them to a different zone. You can join a specific zone or join to Auto Zone. This option is not available if the agent is not installed.

To join a computer to an Active Directory domain:

1 Navigate to the computer in the left pane.

2 Select the computer, right-click, then click **Manage Zone**.

3 Select the action to perform for a selected computer, then click **Next**.

4 Verify the computer information and select **Use the current login user** or select **Use another user** and type the Active Directory user name and password for an account with permission to create a computer object in the specified domain, then click **Next**.

5 Select whether to join Auto Zone or join a specific zone, then click **Next**.

Auto Zone allows computers to join Active Directory without defining any zones ahead of time. If you select Auto Zone, every Active Directory user and group in the forest and in forests with a two-way trust relationship are valid users or groups on the computers in the Auto Zone. If you use Centrify Express, you must join Auto Zone. For all other editions of Centrify software, you can choose to join Auto Zone or a specific zone.

Depending on whether you choose to join Auto Zone or a specific zone, the wizard will prompt you with different options. Because joining a specific zone is the most common scenario, the remaining steps describe the options for joining a specific zone.

6 Click **Browse** to search for and select the zone you want to join, use the join options to specify details about the join operation, then click **Next**.

Some join options might be required settings to address the characteristics of your environment. For example, if you have a disjointed DNS namespace, you should select the **Computer name** and **Computer alias** options to specify the computer name used in Active Directory and the computer alias registered in DNS for a computer when these names differ. For more information about the join options to use, press F1.

7 Select either Server license or Workstation license as the type of license to be used, then click **Next**.

8 Review and modify, if necessary, the list of service principal names for the services provided by the computer, then click **Next**.

9 Keep the current credentials or specify credentials for an Active Directory account that can be used after joining the Active Directory domain, then click **Next**.

10 Verify the information, then click **Finish** to join the zone.

Download Sudoers File

Select this action to download the `sudoers` file for the selected computer to a location on your Windows computer. In the Access Manager console, you can then import the `sudoers` file and convert the `sudoers` data to roles, rights, and role assignments in DirectManage Access Manager.

To download the sudoers file:

1. Navigate to the computer in the left pane.
2. Select the computer, right-click, then click **Download Sudoers File.**
3. Click **Browse** and navigate to a directory in which to save the `sudoers` file.
4. Type a name for the file and click **Save**.

   Use a name that identifies the source computer if you plan to import `sudoers` files from multiple computers.
5. Click **Next**.
6. Review the contents of the file and click **Finish**.

You can now import the `sudoers` file using DirectManage Access Manager to convert the `sudoers` declarations into access rights and role definitions. For more information about rights and roles, see the *Centrify Server Suite Administrator's Guide for Linux and UNIX*.

Remote Session

Select this action to connect to a selected computer using a remote terminal application, such as secure shell (`ssh`).

To connect remotely to a computer:

1. Navigate to the computer in the left pane.
2. Select the computer, right-click, then click **Remote Session** > ***appName*** where *appName* is the remote terminal application, such as `SSH`, `WinSCP`, or another application.

   Depending on the application you select, you might have to make further selections. For example, if you select SSH, you must also select an option for logging on using a private key, stored account information, or by specifying new credentials.

   Once connected to the remote computer, you can run commands in a terminal window, including Centrify commands such as `adinfo` to get information about the Active Directory configuration.

You can modify the remote terminal applications available in the Remote Access menu by configuring the Terminal option. For more information, see "Configuring terminal applications" on page 71.

Export Users and Groups

Select this action to create a file with a list of local users and a file with a list of local groups. The user file mimics the `/etc/passwd` file with an entry for each user and profile attributes separate by colons (:). The group file mimics the `/etc/group` file with an entry for each group and profile attributes separate by colons (:). You can specify the folder location for storing these files. The files are automatically named using the following naming convention:
computerName`_Users`
computerName`_Groups`

Run Script

Select this action to run custom scripts on a selected computer. This option is only available if you have created one or more scripts to run. The list of scripts available depends on the files you have placed in the script directory and keywords you have defined in the scripts themselves. For information about writing scripts and using keywords, see "Creating and using scripts" on page 63. For more information about specifying the directory for custom scripts, see "Specifying a directory for custom scripts" on page 69.

Delete

Select this action to delete a selected computer. The computer is removed from every category in which it appears.

Properties

Select this action to display information about a selected computer. The information displayed depends on whether the selected computer is joined to an Active Directory domain.

If the selected computer is not connected to Active Directory, selecting Properties displays the Deployment tab with details about the discovered computer, such as the computer name, location, IP address, operating system, and Centrify software version information. You can click the Notes tab to record additional details about the selected computer.

If the computer is connected to Active Directory, selecting Properties displays the Active Directory computer properties with additional tabs for Centrify - Deployment and Centrify Notes. You can click the Centrify - Deployment tab to view information about the discovered computer and the joined domain and zone. You can click the Centrify Notes tab to record additional details about the selected computer.

Displaying Active Directory Users and Computers (ADUC) Properties requires:

- Deployment Manager running on a computer that is joined to an Active Directory domain.
- Windows Server Administration Tools Pack (`adminpak`) or Remote Server Administration Tools are installed.

- The current user, or the Active Directory user account specified when the computer joined the domain has permission to retrieve the computer object.

Working with local accounts

By default, local user and group accounts are still valid on the remote computers that join the Active Directory domain. Deployment Manager retrieves and displays information about these users and groups. You can then select one or more groups or one or more users to complete additional tasks. For example, from the Local Accounts node or on individual computers, you can view, add, modify, or delete the groups and users that are defined on the computers that Deployment Manager has discovered.

Managing local groups

When a computer is discovered, and each time it is refreshed, Deployment Manager retrieves information about its local groups and displays this information in a **Groups** node under the **Local Accounts** node. If you select the Groups node under Local Accounts, you can see detailed information for all groups on all discovered computers, including the group name, the computer where the group was discovered, the numeric group identifier (GID), and the users who are members of the group.

If you select an individual group, you can right-click or use the **Action** menu to view, modify, or delete a group. For example, you can select a group name, right-click, then click **Properties** to change the GID, group name, or group membership for the selected group.

Each individual computer also has a Groups node with a list of groups that are specific to that computer. You can use Deployment Manager to take the following actions:

- Add new groups
- Delete groups
- Modify group properties

You should note, however, that modifying group properties or deleting a group can cause problems with file and directory permissions or disrupt user activity. Therefore, Deployment Manager displays a warning if you make changes to individual groups. You can disable this warning if you are confident making changes to local groups.

Add new groups

You can create new local groups on any of the computers that Deployment Manager has successfully discovered. Deployment Manager automatically generates a unique GID for the group. You can change this attribute to a different unique value. You can add users at the same time you create the group or create the group and add users later.

To add a new local group:

1 Expand **Computers > All Computers >** *computerName*, right-click **Groups**, then click **Add Group**.

Note You must use the Groups node of a specific computer to create a new group.

2 Create a profile for the new group by providing the required information, then click **OK**.

- **GID** is a required field that must be unique on the selected computer.

  If you change this field to a GID that conflicts with an existing GID, Deployment Manager records an error in the History node for the computer.

- **UNIX name** is a required field and must be unique for the computer.

3 (Optional) Click **Add** to select local users from the list of available user accounts, then click **OK** to add the selected local user to the group.

Repeat Step 3 for each user you want to add.

4 Click **OK** to save the information and create the group.

5 Click **Yes** if Deployment Manager displays a warning about modifying local group accounts.

Deployment Manager automatically refreshes the computer information after creating the group. If you don't see the new group displayed, check the History node for an error message that explains why the group was not created.

Delete groups

You can delete local groups from any of the computers that Deployment Manager has successfully discovered. Keep in mind that deleting groups can affect file ownership and permissions, and disrupt user activity. Before deleting a group, be certain that you know how the group is used, who the members are, and what to expect as the result of the deletion.

To delete a local group:

1 Select one or more individual groups, right-click, then click **Delete**.

2 Click **Yes** to confirm you want to delete the selected group or groups.

3 Click **Yes** if Deployment Manager displays a warning about modifying local group accounts.

Deployment Manager automatically refreshes the computer information. After the refresh completes, the selected groups are not displayed in the list of groups. You can also check the History node to see a success or failure message for the deletion.

Modify group properties

You can edit the profile attributes for any local group from any of the computers that Deployment Manager has successfully discovered. This includes adding or removing users as members of the group.

To modify group properties:

1 Select any individual group, right-click, then click **Properties**.

2 Change any of the fields displayed for the group, then click **OK**.

3 Click **Yes** if Deployment Manager displays a warning about modifying local group accounts.

Deployment Manager automatically refreshes the computer information. After the refresh completes, the profile changes are displayed in the details pane for the selected group.

Managing local users

When a computer is discovered, and each time it is refreshed, Deployment Manager retrieves information about its local users and displays this information in a **Users** node under the **Local Accounts** node. If you select the Users node under Local Accounts, you can see detailed information for all users on all discovered computers, including the user name, the computer where the user was discovered, the user's numeric identifier (UID) and primary group identifier (GID), GECOS field definition, home directory, and default shell.

If you select an individual user name, you can right-click or use the **Action** menu to view, modify, or delete the users. For example, you can select a local user name, right-click, then click **Properties** to change the UID, login name, or group membership for the selected user.

Each individual computer also has a Users node with a list of users that are specific to that computer. You can use Deployment Manager to take the following actions:

- Add new local users
- Map local accounts to Active Directory
- Reset a local user's password
- Delete users
- Modify user properties

You should note, however, that modifying user properties or deleting a user can cause problems with file and directory permissions or disrupt user activity. Therefore, Deployment Manager displays a warning if you make changes to individual user profiles. You can disable this warning if you are confident making changes to local users.

Add new local users

In most cases, the goal of deploying Centrify software is to reduce the number of local user accounts because local accounts are less secure and more difficult to manage than Active Directory user accounts. However, Deployment Manager does allow you to create new local users on any of the computers that it has successfully discovered. Deployment Manager automatically generates a unique UID for the new user, and assigns a primary group ID to the account. You can change these generated attributes, if needed.

To add a new local user:

1 Right-click the *computerName* > **Users** node and select **Add User**. For example, expand **Computers** > **All Computers** > *computerName*, right-click **Users**, then click **Add User**.

Note You must use the Users node of a specific computer to create a new user.

2 Create a profile for the new user account by providing the required information, then click **OK**.

- **UID** is a required field that must be unique on the selected computer.

  If you change this field to a UID that conflicts with an existing UID, Deployment Manager records an error in the History node for the computer.
- **UNIX name** is a required field that must be unique on the selected computer.
- **Shell** is a required field.
- **Home Directory** is a required field.
- **GECOS** is an optional field.

  This field can contain any information your organization wants to record about a user or be left blank.
- **Primary Group** is a required field and must be the GID for a valid group.

  Deployment Manager assigns the GID of the group that is most used on the selected computer as the default value.

3 Click **OK** to save the information.

4 Click **Yes** if Deployment Manager displays a warning about modifying local user accounts.

5 Type the default password and re-type the default password for the new user, then click **OK**.

Deployment Manager automatically refreshes the computer information after creating a user. If you don't see the new user displayed, check the History node for an error message that explains why the user was not created.

Map local accounts to Active Directory

In most cases, you use Centrify group policies or configuration parameter settings to control any special handling for local accounts. However, Deployment Manager provides a shortcut for mapping local accounts to Active Directory accounts by writing the appropriate configuration parameter to the Centrify configuration file for you. You can use this shortcut to map any local user account to an Active Directory user account on any of the computers that Deployment Manager has successfully discovered.

Mapping a local account to Active Directory is especially useful for accounts that have special privileges, such as local system accounts or service accounts for applications. By mapping a local account to an Active Directory account, you improve the security of the account because users must know the Active Directory password to gain access and Active Directory password policies can ensure that passwords are complex and changed frequently.

To map a local user to an Active Directory user in Deployment Manager:

1. Select any individual user, right-click, then click **Map to AD User**.

   You can navigate to users through the Computers node or Local Accounts node.

2. Connect to Active Directory using the current logon credentials or specify another Active Directory account to use for locating users, then click **OK**.

3. Type all or part of the name of the Active Directory account you want to find. For example, type *o* to find the `Oracle Admin` account, then click **Find Now**.

4. Select the Active Directory user, for example, `Oracle Admin`, then click **OK**.

Deployment Manager completes the mapping and automatically refreshes the computer information. The Active Directory account is displayed in the **Mapped AD User** field for the user.

Reset a local user's password

You can reset a local user's password on any of the computers that Deployment Manager has successfully discovered.

To reset a local user's password:

1. Select any individual user, right-click, then click **Local User Password Reset**.

   You can navigate to users through the Computers or Local Accounts node.

2. Type a new password and re-type the password to confirm it, then click **OK**.

Delete users

You can delete local users from any of the computers that Deployment Manager has successfully discovered. Keep in mind that deleting users can affect file ownership and permissions, and disrupt user activity. Before deleting a user, be certain that you know how

the account is used, the groups that will be affected by the change, and what to expect as the result of the deletion.

To delete a local user:

1. Select one of more individual users, right-click, then click **Delete**.
2. Click **Yes** to confirm you want to delete the selected user or users.
3. Click **Yes** if Deployment Manager displays a warning about modifying local user accounts.

Deployment Manager automatically refreshes the computer information. After the refresh completes, the selected user or users are not displayed in the list of users. You can also check the History node to see a success or failure message for the deletion.

Modify user properties

You can edit the profile attributes for any local user account from any of the computers that Deployment Manager has successfully discovered.

To modify information about a user:

1. Select any individual user, right-click, then click **Properties**.
2. Change any of the fields displayed for the user, then click **OK**.
3. Click **Yes** if Deployment Manager displays a warning about modifying local user accounts.

Deployment Manager automatically refreshes the computer information. After the refresh completes, the profile changes are displayed in the details pane for the selected user.

Working with software packages

After you have downloaded Centrify software, you can use the Software node to view details about the packages that have been added to the Deployment Manager database. To see a list of individual packages, select Analysis Tools, Centrify Identity Risk Assessor, or Centrify platform-specific agents. Deployment Manager displays the list of packages in each category with detailed information about each package, including the file name, publication date, and supported platforms.

You can then select individual packages to view more specific information, such as the versions of an operating system that a specific package supports. For example, select a package from the list, right-click, then click **Properties** to see the platforms that the package supports. On the Packages tab, expand a platform, such as Red Hat, to see the specific versions of the Red Hat Linux operating system that the package supports.

If there is a Warnings tab, it typically indicates the availability of an updated package or a warning that your product catalog may be out-of-date. For information about importing a new product catalog, see "Importing the product catalog" on page 62.

Resolving open issues

The Open Issues node lists the issues that Deployment Manager has found for all discovered or analyzed computers. You can then select individual issues to view additional details, including possible solutions.

Each individual computer also has an Open Issues node with a list of issues that are specific to that computer. You can use Deployment Manager to view, troubleshoot, and resolve issues that have been detected during discovery or by the Analysis Tools on each discovered computer.

To resolve an open issue:

1. Navigate to the issue.
2. Right-click the issue, then click **Properties** to get more information about the issue, including tips on how to fix it.
3. Right-click the issue, then select an appropriate resolution, if one is available.

Selecting an appropriate resolution

For most issues, you can select one of the following responses:

- Select **Ignore** if the issue is a warning that does not prevent you from deploying. Selecting Ignore removes the issue from the list of Open Issues.
- Select **Re-analyze** if the issue is one you have fixed since the last time you analyzed the computer. For example, if the computer was offline, and is now online, the new analysis should resolve the connection issue.
- Select **SSH** if the issue is one you can fix by logging on to the remote computer using a secure shell (`ssh`) connection. For example, you can use this option to remove files on a remote computer if you need to free up disk space. You might also use this options to install missing libraries or to edit configuration files on a remote computer. Centrify recommends that you use secure shell (`ssh`) connections to perform administrative tasks whenever possible.
- Select **Telnet** if the issue is one you can fix by logging on to the remote computer and a secure shell connection is not possible. You should only select this option if `telnet` is your only alternative for connecting to a remote computer and you have configured Deployment Manager to allow `telnet` connections. For more information about

configuring the option to allow `telnet` connections, see "Allowing telnet connections to remote computers" on page 76.

Some issues also provide specific solutions for you to select on the right-click menu. For example:

- If the user name or password provided for a computer is not valid or has not been specified, right-click, then select the **Set user name and password** option to update the user name and password.
- If a computer displays the **Check clock synchronization** issue, right-click, then click **Synchronize Clock** to correct the issue.

Potential issues you might see

The following table lists the warnings and errors that Deployment Manager might return during the discovery and analysis of computers and suggests possible solutions.

Type	Issue	What it means and how to respond
Error	`Operating system patch required`	A required operating system patch was not found. Review the properties for this issue to identify the specific operating system patches that are required and not applied, then log in remotely to the computer and update the operating system to include missing patches.
Error	`Library path is not set correctly`	On Solaris computers, this error is returned if certain required libraries—such as `/lib` or `/usr/lib`—are missing from the system library path. Review the properties for this issue to identify the libraries that are missing from the system library path, then log in remotely to update the system library path.
Error	`Perl not installed or version not supported`	Perl must be available on computers where you plan to deploy the Centrify agent. Review the properties for this issue to identify the version of Perl required, then log in remotely to the computer and update Perl to a version supported by Centrify software.
Error	`Insufficient disk space`	There is not enough disk space available for deploying the Centrify agent. Review the properties for this issue to see the disk space required, then log in remotely to the computer and free up enough disk space for Centrify software.
Error	`No DNS to resolve hosts`	The DNS entry was not found in the hosts database. Review the properties for this issue for more information, then log in remotely to the computer. Open the `/etc/nsswitch.conf` file and add `dns` to the `hosts` entry. For example: `hosts: centrifydc files dns`

Type	Issue	What it means and how to respond
Warning	`DNS connectivity problem`	The analysis tools send UDP and TCP requests to each DNS server specified in the `/etc/resolv.conf` file and record the results, including elapsed time, which is used to set the status of each DNS server. If the analysis tools fail to connect to a DNS server, this warning is returned. Review the properties for this issue for more information, then log in remotely to the computer. • Open the `/etc/resolv.conf` file and verify that you have listed the correct DNS servers with the correct IP addresses. • Verify that the specified DNS servers are running and reachable.
Warning	`One or more DNS servers are dead or marginal`	Based on the elapsed time of the UDP and TCP requests, each DNS server found is rated **good**, **marginal**, or **dead**. This warning message is returned for each marginal or dead server. Review the properties for this issue for more information, then log in remotely to the computer. • Open the `/etc/resolv.conf` file and verify that you have listed the correct DNS servers with the correct IP addresses. • Verify that the specified DNS servers are running and reachable.
Error	`No DNS server available`	Based on the elapsed time of the UDP and TCP requests, each DNS server is rated **good**, **marginal**, or **dead**. If no good servers are found, this error is returned. Review the properties for this issue for more information, then log in remotely to the computer. • Open the `/etc/resolv.conf` file and verify that you have listed the correct DNS servers with the correct IP addresses. • Verify that the specified DNS servers are running and reachable.
Error	`Invalid domain name`	An attempt to connect to a specified domain failed. Review the properties for this issue for more information and verify that you entered the domain name correctly after clicking **Analyze** or **Analyze Environment**.
Error	`No domain controller available`	No domain controllers are responding to a connection request. Review the properties for this issue for more information and verify that a domain controller is operational for the domain and that it is reachable from the computer running Deployment Manager.
Error	`No DNS record found for domain controller`	Name resolution failed for the domain controller. Review the properties for this issue for more information, then log in remotely to the computer. Open the `/etc/hosts` file and add an entry for the domain controller. For example: `192.168.1.111 dc1 dc1.acme.com`

Type	Issue	What it means and how to respond

Error	`Specified domain controller does not belong to the requested domain`	An attempt to connect to a specified domain using a specified domain controller failed.
		Verify that the specified domain controller is operational, serves the specified domain, and is reachable from the computer running Deployment Manager.
		Review the properties for this issue for more information, then log in remotely to the computer and verify the `/etc/hosts` file and `/etc/resolv.conf` file have entries for the specified domain controller.
		For example, if the domain controller is 192.167.1.111:
		`#/etc/hosts: 192.168.1.111 dc1 dc1.acme.com`
		`#/etc/resolv.conf nameserver: 192.168.1.111`

Error	`Domain controller 1 does not provide global catalog service`	If the Global Catalog for a given domain is on a different domain controller, you can specify the location of the Global Catalog by adding the `dns.gc.domain_name` parameter to the configuration file. For example: `dns.gc.mylab.test: dc3.mylab.test`

Error	`Domain controller is down`	An attempt to connect to a domain using a specified domain controller failed.
		If the specified domain controller is not available from the computer running Deployment Manager, try using another domain controller that serves the specified domain.
		Review the properties for more information, then log in remotely to the computer and verify the `/etc/hosts` file and `/etc/resolv.conf` file have entries for the specified domain controller.
		For example, if the domain controller is 192.167.1.111:
		`#/etc/hosts: 192.168.1.111 dc1 dc1.acme.com`
		`#/etc/resolv.conf nameserver: 192.168.1.111`

Error	`No domain controller available in the site`	No domain controllers in the site are responding. Review the properties for more information, then make sure that at least one domain controller is operational for the site and that it is reachable from the computer running Deployment Manager.
Error	`Not all DNS servers are duplicates of each other`	The running DNS servers do not respond to SRV and domain controller lookups requests with the same results. Review the properties for more information, then make sure that all running DNS servers respond to requests with the same information.
Warning	`Unknown site for domain controller`	The Active Directory site was not found for a specified domain controller. Review the properties for more information, then verify that the specified domain controller belongs to a site.

Type	Issue	What it means and how to respond
Error	`Site for domain controller does not match`	The Active Directory site found does not match the site associated with the domain controller. Review the properties for more information, then verify the Active Directory site for the domain controller.
Note	`Clock is not synchronized`	The system clock on the domain controller and the system clock on the selected computer are not synchronized. Select the issue, right-click, then select **Synchronize Clock**.
Error	`Clock is not synchronized under NTP`	The clock skew between on the domain controller and the selected computer is over one minute. Select the issue in the **Open Issues** node, right-click, then select **Synchronize Clock** from the pop-up menu.
Warning	`Clock skew over 5 seconds among Domain Controllers`	Synchronize clocks among your domain controllers.
Error	`Clock skew over 60 seconds among Domain Controllers`	Synchronize clocks among your domain controllers.
Error	`User name or password is empty`	Select the issue, then right-click and select **Set Username and Password**.
Error	`User name or password is too long`	Select the issue, then right-click and select **Set Username and Password**.
Error	`Cannot ping the computer`	Be certain the computer is not shut down or behind a firewall that prevents `ping`. Select the issue, then right-click and select **Refresh Computer Information**.

Error	`Cannot open socket connection of computer`	Select the issue, then right-click and select **Refresh Computer Information**.
		If refresh does not work, log in locally to the computer and verify that the SSH process is running.
		For example, type the following `ps -e` command, and you should see output similar to the following if `ssh` is running:
		`ps -e |grep -i ssh`
		`5789 sshd`
		`7342 ssh-agent`

Error	`Authentication failure`	Select the issue, then right-click and select **Set Username and Password**.

Reviewing historical activity

The **History** node records information about the actions you have taken with Deployment Manager. You can then select actions to view additional details about each event.

Each individual computer also has a History node with a list of event that are specific to that computer. You can use Deployment Manager to view and track the complete record of all of the actions that have been taken for each discovered computer.

When you perform any action on a computer, a summary of the event is recorded under the History node with the date and time of the action and an indication of whether the action was successful. For example, the History node is updated when you analyze the environment, fix issues, refresh computer information, deploy software, or join a domain.

If any risk assessment or deployment operation failed, the Details column displays additional information about the error that caused the failure. To see more detailed information about any successful or failure event, select the event, right-click, then click **Properties**. You can then click the **Trace** tab to see all of the commands executed and the corresponding result code.

To filter the list of historical events displayed, you can right-click the History node then select **Show the latest history for each computer**. After you select this option, only the last operation for each computer is displayed. You can also delete the record of previous actions performed from the History node. To delete one or more records, select the event, right-click, then click **Delete**.

Importing the product catalog

When you download software from the Centrify Download Center, Deployment Manager reads a manifest, or product catalog file, to determine which packages are available and are appropriate to download for the computers you have discovered. The manifest is stored locally in the Deployment Manager repository and the most current copy is stored on the Centrify Support site. To be certain that it is reading the latest manifest, Deployment Manager compares the time stamp of its local copy with that on the Support site, and downloads the newer one when necessary, at the following intervals:

- Whenever you start Deployment Manager.
- Once per day if Deployment Manager is left running.
- Whenever you download Centrify software.

If you are using Deployment Manager in an isolated network and have downloaded Centrify software to a local or network location for installation, the manifest that installs with the program may or may not be up-to-date. To update to the latest manifest, you can download a copy of the manifest from a computer with Internet access, copy it to a location Deployment Manager can access, then import it.

Note A copy of the product catalog is included with the software and you can import it into Deployment Manager without connecting to the Internet or accessing the Centrify Download Center. Over time, the version included in the software package will be outdated. In general, you should periodically get the latest version of the product catalog directly from the Centrify Download Center. If Deployment Manager is installed on a

computer with Internet access, you can automatically check the Centrify web site for new versions of the Centrify product catalog. For more information about setting this option, see "Enabling automatic updates for the Centrify product catalog" on page 70.

To import a copy of the Centrify Product Catalog:

1. On a computer with Internet access, go to the Centrify Support Portal and download the product catalog.
2. When the dialog appears, click **Save** to save the file.
3. Specify a location that is accessible by the computer running Deployment Manager, or save the file locally, then copy it to a location that Deployment Manager can access.
4. Start Deployment Manager.
5. Select the Centrify DirectManage Deployment Manager node, right-click, then click **Import Centrify Product Catalog**.
6. Navigate to the location that contains the product catalog file, select the file, `centrify-product-catalog-offline.xml`, and click **Open**.
7. Click **OK** when you see the confirmation message.

Creating and using scripts

With Deployment Manager, you can create and store scripts that you want to execute on the remote computers you are managing. If you place one or more script files in the Scripts directory, Deployment Manager adds an entry for each one to the **Run Script** menu. You can then select any script on the **Run Script** menu to have Deployment Manager upload and execute the script through a terminal connection on the target computer.

By default, scripts are stored in one of the following locations:

```
C:\Users\User\AppData\Roaming\Centrify\DeploymentManager\Scripts
C:\Documents and Settings\User\Application Data\Centrify\DeploymentManager\Scripts
```

You can specify a different location. For information about selecting a different location for the scripts directory, see "Specifying a directory for custom scripts" on page 69.

The scripts you create should run against one or more target objects. You use keywords within the script to specify the target objects to which the script applies. For example, you can specify that a script applies to users, groups, computers, or any combination of the three. You also use keywords to provide a name and description of the script. After you specify a target object for the script, such as users, the script is available on the Run Script menu for all users.

The following table lists the keywords you can use:

Use this keyword	To specify
`require-user`	The script is available if a user is selected.
`require-group`	The script is available if a group is selected.
`require-computer`	The script is available if a computer is selected.
`display-name=`*`name`*	The name displayed in the Run Script menu as the name of the script to execute. If you do not specify a `display-name` keyword, the name of the script file appears instead.
`description=`*`desc`*	A description for the script that appears in the status bar when the cursor hovers over the menu item.
`run-with-privilege`	The script requires elevated privileges to run. If you use this keyword, the script must be run by `root` or a user with `root`-level permissions.

To use a keyword, you must precede it by a comment character (`#`) and place it at the top of the script before the content. The following shows the keywords for a sample script:

```
#require-user
#require-computer
#display-name=Sample Script
#description=This sample script applies to users and computers
```

Note that there must be no spaces between the comment character and the keyword, otherwise, the line is considered a comment.

If you specify `require-`*`object`* keywords for more than one target object, the script is available for all specified target objects. For example, if you specify both `require-user` and `require-computer` at the beginning of a script, the script is available for both users and computers. If you do not use any of the `require-`*`object`* keywords, the script is available for all computers, groups, and users.

You can also use environment variables to refer to the attributes of a selected user or group. The following table lists the environment variables you can use in scripts:

Use this variable	To specify
`$cdm_user_name`	Login name of the selected user.
`$cdm_user_uid`	UID of the selected user.
`$cdm_user_shell`	Shell of the selected user.
`$cdm_user_home`	Home directory of the selected user.
`$cdm_user_gecos`	GECOS of the selected user.
`$cdm_user_gid`	Primary group GID of the selected user.
`$cdm_user_map`	SAM account name of the Active Directory user mapped to the selected user.
`$cdm_group_name`	Name of the selected group.

Use this variable	To specify
`$cdm_group_gid`	GID of the selected group.
`$cdm_group_members`	Members of the selected group.

The following is an example of a simple script that echoes the selected user's name:

```
#display-name=Display User Name
#require-user

echo ====================
echo "Selected user: $cdm_user_name "
echo ====================
```

The `#require-user` keyword specifies that the script appears in the Run Script menu for individual users and the `#display-name` keyword specifies that the script is displayed on the menu as **Display User Name**.

To execute this script, highlight a user, right-click, then select **Run Script > Display User Name**. The script echoes the selected user's name on the remote computer. You can verify that the script ran successfully by looking at the History node for the computer to which the selected user belongs.

Note You can select multiple target objects when executing a script, and the script is executed against all of them.

Converting the database to the current version

Deployment Manager includes a Microsoft SQL Server Compact Edition database that serves as a repository for all of the information that the Deployment Manager gathers. If you upgrade to a new version, Deployment Manager continues to use the same database to maintain the information that it has already gathered. In some cases, however, updates to Deployment Manager require changes to the database schema such that the newer edition of Deployment Manager cannot use the old database schema.

When you install, the Deployment Manager setup program automatically checks whether you already have a database installed and whether a previously installed database schema is compatible with the new database schema. If the database schema has changed, the Deployment Manager setup program automatically converts the existing database to the new schema and, by default, creates a backup of the original file.

In certain rare cases, however, you may need to convert the database schema manually after you have run the Deployment Manager setup program. For example, if you move an existing database to a different location, upgrade Deployment Manager, then copy the old database back to the data store location, you could end up with an incompatible database schema.

If you have a database schema that is incompatible with the current version of Deployment Manager, starting Deployment Manager displays a warning message that indicates the

database schema is invalid. To update the database schema manually after running the setup program, you can use the `ConvertDatabase.exe` program. The `ConvertDatabase.exe` program is a separate standalone utility included with Deployment Manager that converts an existing database schema to the latest schema.

To convert the database schema manually:

1. Open a Command prompt.
2. Change to the Deployment Manager installation directory.

   For example, if you use the default location:
   ```
   C:\Program Files\Centrify\Deployment Manager
   ```
3. Execute the `ConvertDatabase` program.

   For example:
   ```
   ConvertDatabase /F C:\Users\User\AppData\Roaming\Centrify
   \DeploymentManager\datastore.sdf
   ```

   Where

   - `/F` specifies the path to the database file to convert. The location in this example is the default location for the database file on Windows Vista, Windows 7, or later.
   - *`User`* is the name of the user account that installed Deployment Manager.

   By default, `ConvertDatabase` creates a backup copy of the database file in the same location as the original file. You can use the `/B` option to specify a different location or `/N` to convert the database without creating a backup file.

Changing your account password

If you are storing UNIX credentials in the Deployment Manager database, the information is encrypted using your Windows account access token. However, it is a common security policy for organizations to require users to change their account password at a set interval, such as every 90 or 120 days. In certain situations, changing the account password might prevent stored UNIX credentials from being properly decrypted. If this happens, any task you attempt to perform will return an "Authentication failure" as an open issue.

To ensure that changing your password does not prevent stored credentials from being decrypted, you should always use the `Ctrl-Alt-Del` key combination to select **Change a password** so that you are prompted to provide both the old password and the new password. Note that the account you used when you installed Deployment Manager controls the access token used to encrypt and decrypt UNIX credentials. This account might be a local Windows user account or an Active Directory domain user account. In either case, using `Ctrl-Alt-Del` to set a new password will allow credentials to be properly decrypted after the change.

Creating and using custom groups

By default, you can organize computers based on the operating system, zone, or a manually-defined location. In some cases, however, you might want to group computers based on other criteria. For example, you might want one set of computers in a Development group and another set in a Production group or have separate groups for the computers that host web applications and another for computers that host internal databases. By creating custom groups, you can select a group then execute administrative operations on all of the computers in that group at once. For example, after creating a group and adding computers to it, you might want to change credentials used, run an identity risk assessment, or upgrade the Centrify agent.

To create one or more custom groups

1. Open the Registry Editor and expand HKEY_CURRENT_USER > Software > Centrify.
2. Select Deployment Manager, right-click, then select New > **DWORD (32 bit) Value**.
3. Type Custom Groups as the registry key name.
4. Select Custom Groups, right-click to select **Modify** and type 1 as the registry value, then click **OK**.
5. Close the Registry Editor and open Deployment Manager.
6. Expand Computers and select the new Custom Groups node in the navigation pane.
7. Select Custom Groups, right-click to select **Add Group** and type a new group name, then click **OK**.
8. Select your custom group, right-click to select **Add Computers to Custom Group**.
9. Select the computers you want to add to the group, then click **Add**.
10. Repeat Step 7 to Step 9 for each custom group of computers.

Setting Deployment Manager options

This chapter explains how to configure Deployment Manager options.

The following topics are covered:

Specifying a default account for downloading software

You can register for a free Centrify account by visiting the Centrify website. For convenience, you can specify a default account for downloading software packages from the Centrify Download Center.

If you specify a default user name and password for the Centrify Download Center, you are not be required to provide the account information each time you download Centrify software.

To specify a default Centrify account for downloading packages:

1. Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.
2. Click the **General** tab.
3. Type a valid `centrify.com` user account name and password.

The user account name is the email address you used to register for an account.

4 Click **OK** to save the information if you are done setting options.

The user name and password you specify can be stored securely in the Deployment Manager database and only available to you. If you save credential information in the database, it is encrypted with the access token for the Windows account you used to log on. In addition, the encryption and decryption must take place on the same computer. Therefore, even if other users have access to the Deployment Manager database, they cannot decrypt the stored password because they do not have the Windows access token used to encrypt the password.

Specifying a default package directory

By default, Deployment Manager places downloaded software packages in the `C:\Documents and Settings\`*`User`*`\Application Data\Centrify\DeploymentManager\Packages` or `C:\Users\`*`User`*`\AppData\Roaming\Centrify\DeploymentManager\Packages` directory. You can specify a different default location for the packages you download, if you like. For example, you might want use a shared network folder to make the software packages available to multiple users.

To specify a default location for downloaded packages:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **General** tab.

3 In Package destination, type a local or network path or click **Browse** to navigate to a location to store downloaded packages.

4 Click **OK** to save the information if you are done setting options.

Specifying a directory for custom scripts

You can create custom scripts to execute on remote computers. Deployment Manager looks for custom scripts in the directory that you specify in the General tab. If Deployment Manager finds any files in that location, it adds them to the Run Script menu for the computer, user, or group that the script targets. For information about creating scripts and using keywords to define script targets, see "Creating and using scripts" on page 63.

To specify a script directory:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **General** tab.

3 In the Script directory field, type a local or network path, or click **Browse** to navigate to a location in which you want Deployment Manager to look for custom scripts.

4 Click **OK** to save the information if you are done setting options.

Enabling automatic updates for the Centrify product catalog

If Deployment Manager is installed on a computer with Internet access, you can automatically check the Centrify website for new versions of the Centrify product catalog.

If you check this option and have Internet access, Deployment Manager periodically connects to the Centrify website and automatically downloads updates to the Centrify product catalog when new versions are available.

To automatically update the Centrify product catalog:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **General** tab.

3 Check the **Enable Centrify Product Catalog Auto Update** option.

4 Click **OK** to save the information if you are done setting options.

Selecting a method for credential handling

Deployment Manager provides options to allow you to specify how to handle the user credentials that enable you to log on to remote computers. depending on your organization's security policies and who has access to the computer where Deployment Manager is installed, you can either encrypt and stores credentials in a local database or cache credentials temporarily.

If you choose to encrypt and stores credentials in a local database, Deployment Manager uses the currently logged on Windows user account to encrypt the credentials for connecting to remote computers. The credentials are secure because only the Windows account that was used to encrypt the credentials can decrypt and retrieve them from the database. Because the encrypted credentials are stored locally, you can use them to connect to discovered computers without re-entering a user name and password.

If you choose to cache UNIX credentials temporarily in memory, the credentials you use to connect to remote computers are not stored or saved from one Deployment Manager session to the next. When you close Deployment Manager, the credential cache is removed from memory and cannot be accessed again. You must then re-enter UNIX credentials each time you start a new Deployment Manager session to manage remote UNIX computers.

To select a method for handling credentials securely:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Credential** tab.

3 Select either the **Encrypt and store UNIX credentials locally** option or the **Cache UNIX credentials in memory** option.

   In most cases, you should select **Encrypt and store UNIX credentials locally** for ongoing management of remote computers from Deployment Manager.

   If you are running an identity risk assessment, select **Cache UNIX credentials in memory** to store the required credentials only for the duration of the assessment and the generation of the assessment report. You can change from one option to the other at any time. However, selecting **Cache UNIX credentials in memory** removes any previous stored credentials and will require you to reenter this information the next time you use Deployment Manager before you can perform any other tasks on discovered computers.

4 Click **OK** to save the information if you are done setting options.

If you store credentials in the Deployment Manager database and are periodically required to change your account password in accordance with your organization's security policies, always use `Ctrl-Alt-Del` to set your new password. For more information about the implications of changing your password, see "Changing your account password" on page 66.

If you store credentials temporarily in memory, you can re-enter the information by editing the Properties for one or more computers each time you start a Deployment Manager session before performing any other operation.

Configuring terminal applications

Deployment Manager enables you to remotely access computers that it has discovered using the terminal applications of your choice. You can edit the existing list of terminal applications, add new terminal applications, or modify the arguments for any of the terminal applications you want to support.

Modifying the default list of terminal applications

By default, Deployment Manager supports several common terminal applications, such as SSH, WinSCP, and VNC. You can change how these application are displayed on the Remote Session menu, remove any application, change the name, location, or arguments for an application, or specify whether an Active Directory user name and password are required to run any application.

To modify the terminal applications displayed on the Remote Sessions menu:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Terminal** tab.

3 Select an existing application in the list and do one of the following:

- Click **Move Up** or **Move Down** to change an application's location in the menu.
- Click **Remove** to remove an application.
- Click **Edit** to change the name, location, or arguments for an application or to specify whether an Active Directory user name and password are required.

4 Click **OK** to save the information if you are done setting options.

Adding new terminal applications

If you have access to a terminal application that is not listed on the default Remote Sessions menu, you can add the application so that it is available for opening sessions on remote computers.

To add new terminal applications to the Remote Sessions menu:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Terminal** tab.

3 Click **Add** to add a new terminal application.

4 Type the name of the application as you want it to appear on the Remote Session menu.

You can use the vertical bar (|) to create a submenu. For example, type `SSH|Kerberos Login` to display `Kerberos Login` as a submenu item (**Remote Session > SSH > Kerberos Login**).

5 Type the location or click **Browse** to browse to the location for the terminal application executable file.

By default, terminal applications are stored in the `External` directory below the Deployment Manager installation directory. For example, the default installation directory is `C:\Program Files\Centrify\DirectManage Deployment Manager`. If you type the path to the application and want to use the default location, you can use the variable `${InstallDir}` to specify the base path. For example:
`${InstallDir}\External\putty.exe`

6 Type the command-line arguments for the terminal application.

For example, for Kerberos Login for PuTTy, you might specify the following:
`-ssh -k ${ip}`

7 Select the **Only available upon joining to Active Directory** option if you want to require an Active Directory account and password before executing the command.

8 Click **OK** to save the information if you are done setting options.

Configuring log settings

By default, logging is disabled in Deployment Manager for performance reasons. If you are troubleshooting an issue, you might want to temporarily enable logging to capture detailed information about operation. In most cases, however, Centrify recommends that you enable logging only if instructed to do so by Centrify Support. If you choose to enable logging, you can also specify the location of the log file.

To configure logging for Deployment Manager:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Log Settings** tab.

3 Select **Enable Deployment Manager console log** to start recording details about console operations in a log file.

4 (Optional), Type a path name or click **Browse** to specify a location for the log file.

5 Click **OK** to save the information if you are done setting options.

After you have collected enough information for Centrify Support or your own troubleshooting purposes, be sure to return to the Log Settings tab and deselect the **Enable Deployment Manager console log** option to stop recording operations in the log file.

Setting time out values for remote tasks

Deployment Manager enables you to complete tasks on remote computers. You can use the Time Out tab to control the maximum time allowed to complete each type of task to prevent any operation from hanging indefinitely.

The number of seconds you specify apply to the task on each computer. If you start a task that affects multiple computers, the time out applies to how long it takes for the operation to complete on each computer, not the overall time it takes to complete the task on all computers. If you make changes, you can click **Restore Defaults** at any time to restore the default values for all tasks.

The default time out setting for each task are as follows:

This task	Times out after
Discover computer task	30 seconds
Analyze computer task	90 seconds
Refresh computer task	30 seconds
Fix issue task	30 seconds
Install software task	600 seconds
Uninstall software task	600 seconds
Join computer task	600 seconds
Leave zone task	600 seconds
Manage local account	30 seconds
Manage audit task	30 seconds
Assessment task	300 seconds

In changing the time out values for remote tasks, you should keep in mind the constraints of your network and the effect that the network topology might have on the time it takes to complete a task. For example, if you have a widely distributed network or slow network connections on some subnets, you might want to increase the time allowed to complete some tasks.

To change time out values for remote tasks:

1. Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.
2. Click the **Time Out** tab.
3. Use the arrow keys or type a new value for one or more tasks.
4. Click **OK** to save the information if you are done setting options.

Selecting the port for secure shell connections

By default, Deployment Manager operations that access remote computers using a secure shell (`ssh`) connection use port number 22, which is the port most commonly used for secure shell sessions. If you have configured the `sshd` process to run on a non-standard port, however, you can configure Deployment Manager to use a different default port for these connections by setting a network option. For example, you might have configured firewall rules to ensure all secure shell connections use a port other than the standard port to improve security. You can configure Deployment Manager to use that port for common remote operations, such as the discovery of new computers, analyzing remote computers, and deploying packages.

To set a new default port for secure shell connections:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Network** tab.

3 Type or select a new SSH port number.

4 Click **OK** to save the information if you are done setting options.

Overriding the default port for secure shell sessions

You can also change the port used on individual computers by modifying the properties for a specific computer. For example, if you change the default port number to the non-standard port, such as 6504, that your organization uses for the `sshd` process, you might discover that specific computers require the standard port or a different non-standard port. To allow remote connections to those specific computers, you can override the default port on a computer-by-computer basis.

To configure the secure shell port to use for specific computers:

1 Add the computer to Deployment Manager as described in "Starting the Add Computers wizard" on page 32.

2 Expand Computers and All Computers to select the discovered computer.

3 Right-click, then click **Properties**.

4 Select the **SSH Port** option, then type or select the port number to use.

5 Click **OK** to save the information for the selected computer.

6 Right-click, then click **Refresh Computer Information**.

Configuring the network connection test

Many Deployment Manager operations require a connection to a remote computer. By default, Deployment Manager uses a two-step process for these operations to optimize performance. In the first step, Deployment Manager sends a `ping` request to each specified IP address to verify that the computer is reachable. If a computer responds within a configurable number of seconds, Deployment Manager then connects to the computer using a secure shell (`SSH`) connection to gather information. Computers that don't respond to the `ping` request are skipped. Sending a `ping` request to each computer is a relatively lightweight operation and it eliminates the overhead associated with attempting to connect to computers that are not reachable.

In certain cases, however, computers that do not respond to a `ping` command might still be reachable through a secure shell connection. For example, computers isolated behind a

corporate firewall may fail to respond to the `ping` request, but allow a connection from a remote shell. For these situations, Deployment Manager provides a network option that enables you to control the preliminary `ping` request. If you disable the `ping` request, some operations, such as the discovery of computers on the network take longer to complete, but Deployment Manager will not skip any computers that are available for `SSH` connections.

To control the ping request for testing network connections:

1. Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.
2. Click the **Network** tab.
3. Select **Send ping requests to determine accessibility** and set the **Reply must be received within [ ] seconds** `ping` timeout value if you want to keep the default behavior but change the time allowed for a response to the `ping` request.

   Using the `ping` request to test accessibility improves the performance of operations that require a connection to remote computers, but might miss computers that are reachable through a secure shell connection.

   To skip the `ping` request, deselect **Send ping requests to determine accessibility**. With this setting, Deployment Manager attempts to connect to every computer matching the criteria you specify, such as an IP subnet or IP address range. This setting allows Deployment Manager to find computers it wouldn't find using a `ping` request, but operations take longer to complete.
4. Click **OK** to save the information if you are done setting options.

Allowing telnet connections to remote computers

By default, you can only connect to remote computers using secure shell (`ssh`) sessions to ensure the security of sensitive information, such as administrative passwords. In some cases, however, you might require the use of `telnet` to connect to a remote computer. For example, if you have legacy computers that don't allow secure shell sessions or have `ssh` disabled, you might want to allow a `telnet` connection to be used.

If you select the **Allow remote connections using telnet** network option, Deployment Manager will still attempt a secure shell (`ssh`) connection to remote computers first, but will allow a `telnet` connection if the secure shell connection fails. In essence, this setting provides a fallback alternative for connecting to computers where `ssh` is not available or not supported.

If you choose to allow `telnet` connections to remote computers, however, you should be aware that passwords are not secure because they are transferred over the network as plain text. If you configure Deployment Manager to allow `telnet` connections and an attempt to use a secure shell connection fails, Deployment Manager will attempt to open a session on the remote client using port number 23.

To allow telnet connections:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Network** tab.

3 Select **Allow remote connections using telnet**.

4 Click **OK** to save the information if you are done setting options.

Configuring text strings for remote connections

By default, Deployment Manager expects the most common prompt strings that end with one of the following characters on target computers: `#`, `$`, `>`, or `%`. Although Deployment Manager can identify the most common prompt strings by using the default prompt matching syntax, users often customize the prompt string to something that is not recognizable. You can modify the regular expression Deployment Manager uses to identify prompt strings globally on the Network tab or on individual computers.

In addition to the prompt string, you can add and edit any other strings expected on target computers and appropriate responses. For example, if a new connection is going to prompt for a password or an interactive response to a question, you can add the appropriate expected and response strings globally on the Network tab or on individual computers.

To allow telnet connections:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Network** tab.

3 Modify the **Expect shell prompt on target** regular expression to customize the prompt to expect on target computers.

For example, to match a prompt ending with a square bracket such as:
`[wsadmin1:/home/wsadmin1]`

You could modify the regular expression to include the bracket character as follows:
`[\#\$\>\]]\s*$`

To match the `bash` shell prompt when the prompt is displayed in the red, the prompt ends with the character `m`:
`[m\#\$\>]\s*$`

4 Click **Add** to add any additional expected text strings and appropriate responses.

For example, if target computers display a password prompt, you might add the following console interaction as the Expect text and Response:

```
[Pp]assword:
${pwd}
```

5 Click **OK** to save the information if you are done setting options.

Configuring a "jump box" server

If your organization uses a jump box server, you must manually configure the connection to it in the **Jump Box** tab. A jump box functions like a proxy server and provides a way to isolate access to a private network. It is usually a computer that is connected to two networks and has two network cards. One network card is configured with an external IP address that is accessible from the Internet. The second network card provides an internal IP address that is only accessible to computers on the internal network. The jump box is then configured to correctly route traffic between the two networks.

If you use a jump box, Deployment Manager cannot discover the computers connected to the jump box. Instead, Deployment Manager returns a list of all the computers that match the discovery criteria you specify. Because Deployment Manager cannot connect directly to any of the computers discovered, it cannot verify connectivity or collect any information about the computers connected to the jump box.

To configure the connection to a jump box:

1 Select the **Centrify DirectManage Deployment Manager** node, right-click, then click **Options**.

2 Click the **Jump Box** tab.

3 Select **Enable connection through jump box server** to configure the connection to a jump box server.

4 Type the host name or IP address of the jump box server.

5 Type a user name that has access to the jump box server.

In most cases, the jump box user is `root` or a similarly privileged user. If you want to specify an account without `root` privileges, create a cache directory—such as `/var/centrifydm`—on the jump box server with the account you want to use as the jump box owner and set the permission on the directory to `755`.

```
mkdir /var/centrifydm
chown swan /var/centrifydm
chmod 755 /var/centrifydm
```

If you change the jump box user, reset the directory owner and permission on the `/var/centrifydm` directory to reflect the new jump box user.

6 Type the password for the user account with access to the jump box server.

If you store credentials temporarily in memory, you must re-enter the information for the server each time you start a Deployment Manager session before performing any other operation.

7 Type the command and command-line arguments to open a connection from the jump box server to other computers.

The default command for opening a connection is `ssh`. For example:

```
ssh -o NumberOfPasswordPrompts=1 ${usr}@${ip} -p ${sshport}
```

If you want to specify additional details about the connection command, click **Advanced**. For more information about configuring advanced connection settings, see "Advanced connection commands" on page 79.

8 Type the command and command-line arguments to transfer files between the jump box and other computers.

The default file transfer command is `scp`. For example:

```
scp ${source} ${usr}@${ip}:${target}
```

If you want to specify additional details about the file transfer command, click **Advanced**. For more information about configuring advanced file transfer settings, see "Advanced file transfer commands" on page 80.

9 Click **OK** to save the information if you are done setting options.

Advanced connection commands

You can specify additional commands to execute or change the expected interactions with the target computer when Deployment Manager makes a remote connection.

To set advanced Connection command options:

1 Under **Connection commands**, click **Advanced**.

2 Type the commands to execute on target computers.

Deployment Manager interprets each line as a new command, and executes them in order. Therefore, the command that opens the connection must be the first line. You can then type additional commands, each on a separate line. A command definition must not be spread across multiple lines or it will be interpreted as multiple commands.

3 Add or change the set of possible shell prompts on target computers.

The default setting lists the most common shell prompts. For example:

```
[\$\#\>\: ]\s*$
```

4 Type the expected console output to be received from target computers.

This field enables you to add to or change the expected prompts and specify the responses for the target computers. For example, there are two default console interactions. The first line illustrates an expected prompt for a password and the response provides one using an environment variable:

```
Expect Text                    Response
[Pp]assword                     ${pwd}
```

The second line illustrates a prompt to continue and the response required:

```
Are you sure you want to continue  yes
```

5 Select an entry to change or remove, then click **Edit** or **Remove**, or click **Add** to add an entry, type the Expect Text of the prompt, the appropriate Response, then click **OK**.

Prompts are expected in the order they are listed. You can use Move Up and Move Down to move entries up or down in the list.

6 Click **OK** to save the advanced connection commands.

Advanced file transfer commands

You can specify additional commands to execute or change the expected interactions with the target computer when Deployment Manager makes a remote file transfer connection.

To set advanced File transfer command options:

1 Under **File transfer commands**, click **Advanced**.

2 Type a different location for the cache directory.

When using a jump box, Deployment Manager first copies packages to this temporary location on the jump box server before copying them to the target computers. The default location is:

```
/tmp/Centrify/DM
```

3 Type the commands to execute on target computers.

Deployment Manager interprets each line as a new command, and executes them in order. Therefore, the command that starts the file transfer, for example the `scp` command, must be the first line. You can then type additional commands, each on a separate line.

A command definition must not be spread across multiple lines or it will be interpreted as multiple commands.

4 Add or change the set of possible shell prompts on target computers.

The default setting lists the most common shell prompts. For example:

```
[\$\#\>\: ]\s*$
```

5 Type the expected console output to be received from target computers.

This field enables you to add to or change the expected prompts and specify the responses for the target computers. For example, there are two default console interactions. The first line illustrates an expected prompt for a password and the response provides one using an environment variable:

```
Expect Text                    Response
[Pp]assword                     ${pwd}
```

The second line illustrates a prompt to continue and the response required:

```
Are you sure you want to continue  yes
```

6 Select an entry to change or remove, then click **Edit** or **Remove**, or click **Add** to add an entry, type the Expect Text of the prompt, the appropriate Response, then click **OK**.

Prompts are expected in the order they are listed. You can use Move Up and Move Down to move entries up or down in the list.

7 Click **OK** to save the advanced file transfer commands.

Index

D

E

G

H

I

J

L

M

N

P

R

S

T

U

W

Z