Centrify Zero Trust Privilege Services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service

Centrify-enabled PuTTY User's Guide

December 2020 (release 2020.1)

Centrify Corporation

Legal Notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify for Mobile, Centrify for SaaS, DirectManage, Centrify Express, DirectManage Express, Centrify Suite, Centrify User Suite, Centrify Identity Service, Centrify Privilege Service and Centrify Server Suite are registered trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

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

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

About this guide

The *Centrify-enabled PuTTY User's Guide* describes how to install and configure the Centrify-enabled PuTTY program on Windows computers. PuTTY is open-source client software that enables you to open telnet, secure shell, rlogin and raw TCP sessions on remote computers. The PuTTY client available in Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service has been modified to support Kerberos-based authentication on remote computers that are managed by Centrify software.

Intended audience

This guide is intended for users who want to use the Centrify-enabled PuTTY client to open sessions on remote computers and have their identity authenticated using their Kerberos credentials. This guide assumes that you are familiar with Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service components and that you have sufficient privileges to perform administrative tasks on your managed computers.

Documentation conventions

The following conventions are used in Centrify documentation:

- `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*, this font indicates variables. Square brackets (`[ ]`) indicate optional command-line arguments.
- **Bold** text is used to emphasize commands or key command results; buttons or user interface text; and new terms.
- *Italics* are used for book titles and to emphasize specific words or terms. In fixed-width font, italics indicate variable values.

- Standalone software packages include version and architecture information in the file name. Full file names are not documented in this guide. For complete file names for the software packages you want to install, see the distribution media.
- For simplicity, UNIX is used to refer to all supported versions of the UNIX and Linux operating systems. Some parameters can also be used on Mac OS X computers.

Finding more 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.

For access to documentation for all Centrify products and services, visit the Centrify documentation portal at docs.centrify.com. From the Centrify documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

For details about supported platforms, please consult the release notes.

For the most up to date list of known issues, please login to the Customer Support Portal at http://www.centrify.com/support and refer to Knowledge Base articles for any known issues with the release.

Product names

Over the years we've made some changes to some of our product offerings and features and some of these previous product names still exist in some areas. Our current product offerings include the following services:

Current Overall Product Name	Current Services Available
Centrify Identity-Centric PAM	Privileged Access Service
	Gateway Session Audit and Monitoring
	Authentication Service
	Privilege Elevation Service
	Audit and Monitoring Service
	Privilege Threat Analytics Service

Whether you're a long-time or new customer, here are some quick summaries of which features belong to which current product offerings:

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	Centrify Privileged Service (CPS)		Privileged Access Service
DirectControl (DC)			Authentication Service
DirectAuthorize (DZ or DZwin)			Privilege Elevation Service
DirectAudit (DA)			Audit and Monitoring Service
	Infrastructure Services		Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service, and Privilege Threat Analytics Service
DirectManage (DM)	Management Services	Consoles that are used by all 3 services: Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	
DirectSecure (DS)	Isolation and Encryption Service		Still supported but no longer being developed or updated

Previous Product Offering	Previous Product Offering	Description	Current Product Offering
	User Analytics Service		Privilege Threat Analytics Service
Deployment Manager		Deployment Manager provided a centralized console for discovering, analyzing, and managing remote computers. This feature is no longer included starting with Infrastructure Services release 19.6.	

Depending on when you purchased a Centrify product offering, you may have purchased one of the following product bundles:

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
		Centrify Identity-Centric PAM Core Edition	Privileged Access Service and Gateway Session Audit and Monitoring	
Centrify Server Suite Standard Edition			Authentication Service and Privilege Elevation Service	
	Centrify Infrastructure Services Standard Edition	Centrify Identity-Centric PAM Standard Edition	Privileged Access Service, Authentication Service, and Privilege Elevation Service	
Centrify Server Suite Enterprise Edition			Authentication Service, Privilege Elevation Service, and Audit and Monitoring Service	

Previous Product Bundle	Previous Product Bundle	Current Product Bundle	Services Included	Description
	Centrify Infrastructure Services Enterprise Edition	Centrify Identity-Centric PAM Enterprise Edition	Privileged Access Service, Authentication Service, Privilege Elevation Service, Audit and Monitoring Service (includes Gateway Session Audit and Monitoring)	
Centrify Server Suite Platinum Edition				Discontinued bundle that included DirectControl, DirectAuthorize, DirectManage, DirectAudit, and DirectSecure

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 additional support

If you have a Centrify account, click Support on the Centrify website to log on and access the Centrify Technical Support Portal. From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrify users, ask questions, or share information, visit the Centrify Community website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

Using the Centrify PuTTY client

PuTTY is free open-source software that enables you to connect to remote computers using network protocols such as `telnet`, `ssh`, `rlogin` or raw TCP. The version of PuTTY that is widely available, however, does not support Kerberos authentication. The version of PuTTY that is available in Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service has been modified to enable users to be authenticated using their Kerberos credentials before establishing a remote connection.

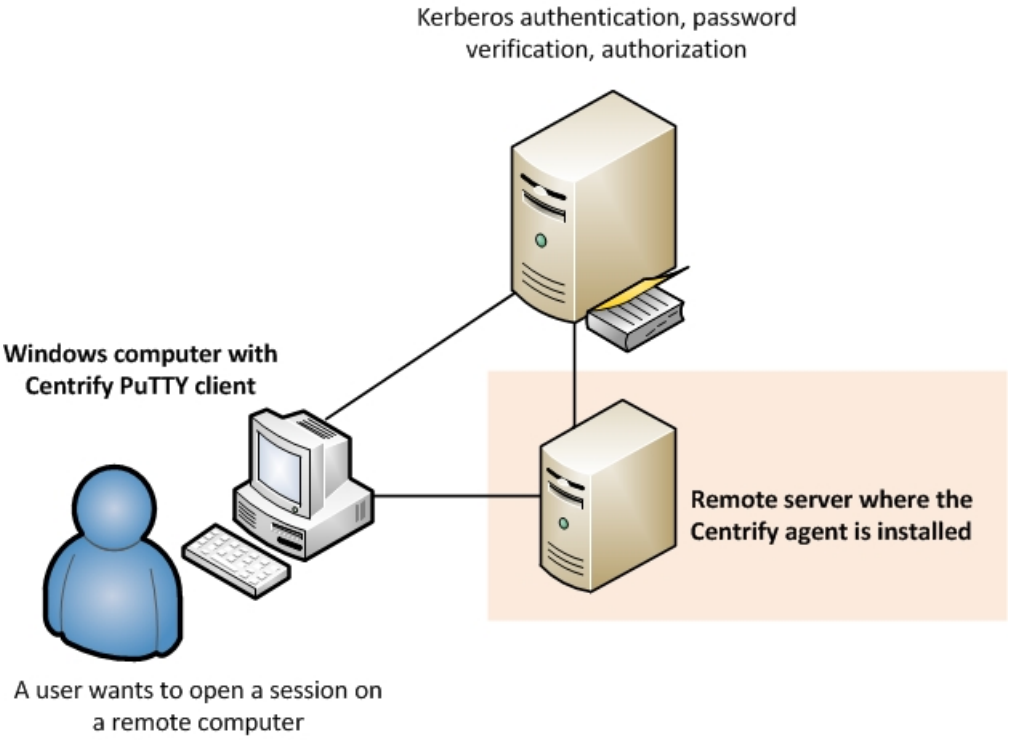
Accessing remote Centrify-managed computers

You can use the Centrify version of the PuTTY client with any supported protocol and to remotely access any Linux, UNIX, or Windows computer on your network, including computers that are not managed by the Centrify agent. However, the most common reason for using the Centrify PuTTY client is to open secure shell (`ssh`) sessions on remote Centrify-managed computers. If you have the Centrify agent and Centrify OpenSSH installed on a remote computer, you can securely access that computer using your Active Directory credentials and take full advantage of centralized Kerberos authentication and consistent password policies across platforms.

If you use the Centrify PuTTY client to access Centrify-managed computers through SSH, the Centrify agent can determine the UNIX login name to use from the user principal name (UPN) in Active Directory, making it possible for you to connect to any managed computers with a single Active Directory identity.

The Centrify agent is also responsible for setting up and managing the Kerberos environment on Centrify-managed computers. You are not required to configure any DNS-to-realm mapping because the agent already knows the relationship between the host computers and their service principal names (SPNs).

Because the Centrify agent automatically manages the Kerberos authentication and policy enforcement on Centrify-managed computers, you can use the Centrify PuTTY client to connect to those computers using a secure and well-established authentication, authorization, and policy enforcement infrastructure.



If you use the Centrify PuTTY client with other protocols or to access remote computers that are not managed by the Centrify agent, the program operates in the same way as the standard PuTTY client. You can configure connections for other protocols and set other configuration options as you would for the open-source PuTTY client.

Note: The Centrify PuTTY client is based on PuTTY version 0.64. This version of the Centrify PuTTY client is compatible with the Centrify agent, version 4.x and later, and with Centrify OpenSSH, version 4.x, and later.

Installing Centrify PuTTY

The Centrify PuTTY client software is only supported on Windows computers. Before installing, you should verify that you have a supported version of one of the Windows operating system product families. For example, you can use Windows 7 or Windows 8. Alternatively, you can install on computers in the

Windows Server product family—such as Windows Server 2008 R2 or Windows Server 2012—if you want your computer to be configured with additional server roles.

For more detailed and most up-to-date information about supported operating system versions, see the Centrify website.

You can install the Centrify PuTTY client by selecting it when you install other Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service components or as a standalone executable using its own setup program. If you downloaded the Centrify PuTTY client as a separate software package from the Centrify website, the package includes the standalone setup program for installing the PuTTY client outside of Centrify Authentication Service, Privilege Elevation Service, and Audit & Monitoring Service.

To install the Centrify PuTTY client from its standalone setup program:

1. Double click on the `putty-`*`version`*`.msi` file to start the PuTTY client setup program.

   If another version of the software is installed on the local computer, you are prompted to remove it before you can proceed.
2. On the Welcome page, click **Next**.
3. Select a folder where the software should be installed by accepting the default location or clicking **Browse** to select a different location and specify who can use the PuTTY client on this computer. then click **Next**.
4. On the Confirm installation page, click **Next** to start the installation.
5. If you see a User Account Control warning, click Yes to continue.
6. Click **Finish** upon successful completion of the installation.

In addition to the PuTTY client (`putty.exe`), the following PuTTY-related programs are installed:

- `pageant.exe` is a secure shell (`ssh`) authentication agent for the PuTTY, PSCP, and Plink programs.
- `plink.exe` is a command-line interface to the PuTTY backend.
- `pscp.exe` is a command-line secure file copy (SCP) client.
- `psftp.exe` is a secure file transfer (SFTP) client.

- `puttygen.exe` is an RSA and DSA key generation utility.
- `puttytel.exe` is a Telnet-only client.

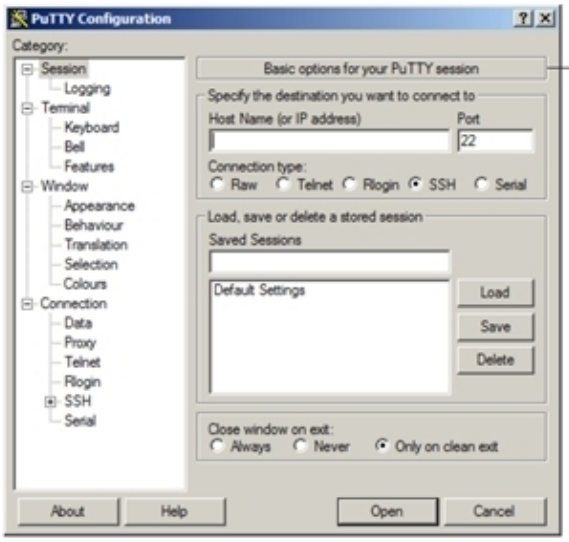
For more information about using these programs, see the official PuTTY documentation. For references to the official PuTTY documentation, see Getting more information.

Configuring the Centrify PuTTY client

The Centrify-enabled version of the open-source PuTTY client adds Kerberos authentication for accessing remote computers using secure shell (`ssh`) network connections. To enable you to configure Kerberos authentication for secure shell sessions, the Centrify PuTTY client adds its own SSH Kerberos configuration page to the standard Windows PuTTY client. All other functionality in the Centrify PuTTY client is the same as in the official PuTTY client, version 0.64.

Starting the Centrify PuTTY client

After installation, you can start the Centrify PuTTY client from the Start menu or by opening the `putty.exe` executable in the file location you specified during installation. By default, the **Basic options for your PuTTY session** are displayed. These options are the same in the Centrify PuTTY client as they are in the open-source PuTTY client. For example:



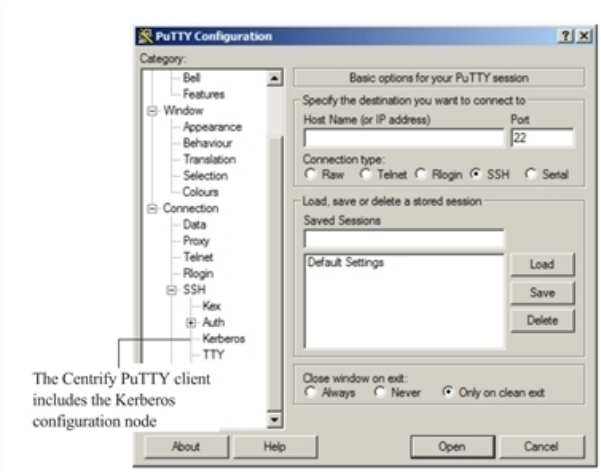
The default view when you open PuTTY is **Basic options for your PuTTY session** in the **Session** configuration settings

Configuring Kerberos authentication for secure shell connections

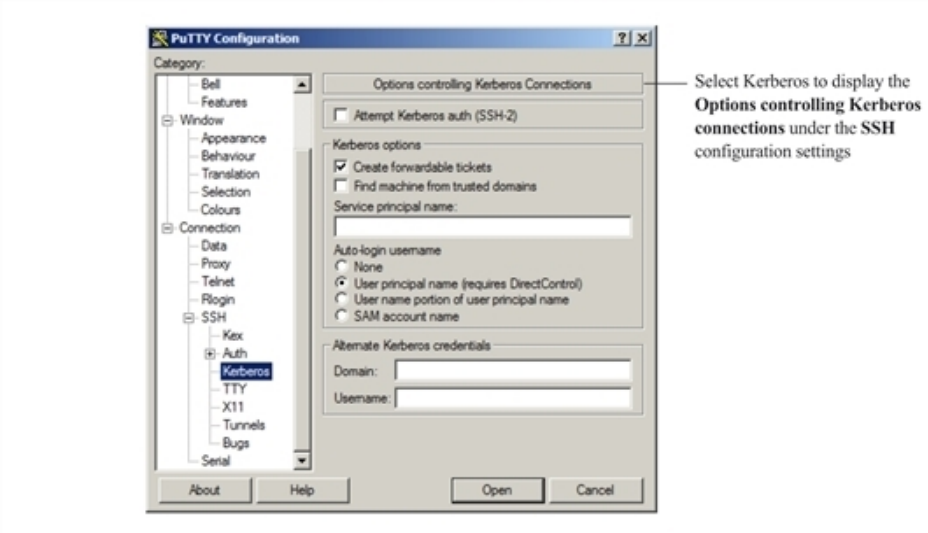
The Kerberos configuration options that have been added to the Centrify version of the PuTTY client are available under the Connection and SSH configuration settings.

To configure Kerberos settings:

1. Expand SSH under the Connection configuration settings. For example:



2. Select **Kerberos** to display the Options for controlling Kerberos connections. For example:



3. Set the appropriate options to configure Kerberos authentication for secure shell remote connections.

- Select **Attempt Kerberos Auth (SSH-2)** if you want the Centrify PuTTY client to attempt to use Kerberos authentication before any other authentication method when opening a new secure shell session.

  If you do not select this option or select this option and Kerberos authentication fails, the authentication options you have defined in Connection > SSH > Auth are used. The number of times you can type the wrong password before Kerberos authentication fails and other authentication options are used can be configured by group policy settings. For more information about the group policies for configuring Centrify PuTTY, see Configuring group policies for Centrify PuTTY.

- Select **Create forwardable tickets** if you want to allow the same Kerberos credentials used for authentication when connecting to other Kerberos-authenticated services.

  The option is selected by default to enable single sign-on, allowing you to be authenticated silently on other servers without providing a password. If you deselect this option, you are prompted to provide a password any time you connect to another Kerberos-authenticated service.

- Select **Find machine from trusted domains** if you want the Centrify PuTTY client to look for computers in external trusted domains if it cannot locate a target computer in the local Active Directory forest or a trusted forest.

  If you select this option and the Centrify PuTTY client cannot locate a target computer, the program will attempt an LDAP connection to the domain controller in the trusted domains using your login credentials. The LDAP connection can only succeed if the domain controller is accessible and you have Read access in Active Directory. You can control the LDAP connection setting by using Centrify PuTTY group policies. For more information about the group policies for configuring Centrify PuTTY, see Configuring group policies for Centrify PuTTY.

  - Type a specific **Service principal name** if a target computer is in a different forest or if the Centrify PuTTY client cannot access the Kerberos Distribution Center (KDC) for the computer.
  - You might have to specify the service principal name if a computer is located in an external trusted domain that is not

accessible. For example, if firewall settings prevent the Centrify PuTTY client from making an LDAP connection to the domain controller in the trusted domains, you can explicitly identify the computer by its service principal name.

4. Select an **Auto-login username** option to specify how the Centrify PuTTY client determines the UNIX user account name to use for authentication when opening a secure shell connection.
   - Select **None** if you want to be prompted to specify the user name for Kerberos authentication or if you want to set a default auto-login user name as a Connection > Data configuration option.

     If you select this option, the Centrify PuTTY client does not automatically generate the UNIX user account name.
   - Select **User principal name (requires DirectControl)** if you want the Centrify PuTTY client to use your user principal name (UPN) as the UNIX account name.

     This option requires the Centrify agent to be installed. With this option, the agent automatically maps the UPN in the Kerberos ticket to the UNIX profile for the Active Directory user name presented in the ticket.
   - Select **User name portion of user principal name** if you want the Centrify PuTTY client to use the user name portion of the UPN as the UNIX user name.

     If you select this option and the UPN is `jdoe@xyz.com`, the Centrify PuTTY client would use `jdoe` as the UNIX user name for authentication.
   - Select **SAM account name** if you want the Centrify PuTTY client to look up the sAMAccountName attribute in Active Directory and use it as the UNIX user name.

     If you select this option, the Centrify PuTTY client will initiate an LDAP connection to the currently logged-in domain controller. If the connection or lookup request fails, the Centrify PuTTY client will prompt you to enter the UNIX user name.
5. Type a **Domain** and **Username** if you do not want to use the Kerberos credentials for the account you used to log on to the Windows computer where you are running the Centrify PuTTY client.

   By default, your current Kerberos credentials for your Windows account are used for authentication on the remote computer. If you want to use a different user name and password, specify the domain and user name for

the alternate Kerberos credentials you want to use. When the Centrify PuTTY client opens the secure shell session on the remote computer, it will prompt you to provide the password for your alternate credentials.

The ability to use alternate Kerberos credentials can be configured by group policy settings. For more information about the group policies for configuring Centrify PuTTY, see Configuring group policies for Centrify PuTTY.

Saving and managing passwords for remote sessions

By default, the Kerberos credentials for the Active Directory account you used to log on to the Windows computer are used for authentication on remote computers. If the remote computer is found and authentication is successful, you are not prompted to provide a password.

If you open a secure shell session using alternate Kerberos credentials or the Centrify PuTTY client cannot locate the target computer using the Kerberos credentials you provided, it will prompt you to provide the new credentials.

If you are prompted for a password, you can select **Remember my password** to have your password stored in the Windows credential cache the password so that you are not prompted for again the next time you access the same remote computer. By saving your password or your user name and password in the Windows credential cache, you can have single sign-on (SSO) access to remote UNIX and Linux computers using your Active Directory user credentials.

If the Centrify PuTTY client cannot find the computer you specify using your own or the alternate Kerberos credentials you have specified, you can try other credentials or other configuration options, such as **Find machine from trusted domains**. If the new credentials or configuration options are successful, you can then select Remember my password to access that computer the next time you open a connection to it. After saving your information, you can use single sign-on to access computers in external or untrusted forests or in disjointed domains.

You can manage cached passwords by using the Credential Manager Control Panel or by opening a Command Prompt window and typing `control keymgr.dll`.

The number of times you can type the wrong password before Kerberos authentication fails and other authentication options are used can be configured by group policy settings. For more information about the group policies for configuring Centrify PuTTY, see Configuring group policies for Centrify PuTTY.

Configuring group policies for Centrify PuTTY

Centrify provides group policy administrative templates that allow you to centrally manage the configurable PuTTY settings for Kerberos authentication using secure shell connections. The group policy administrative templates are available in both `admx` and `xml` file formats.

- The `admx` template, `centrify_putty_settings.admx`, is installed by default in the `C:\Windows\PolicyDefinitions` directory.
- The `xml` file, `centrify_putty_settings.xml`, is installed by default in the same directory as the Centrify PuTTY program. For example, if you used the default location in the setup program, the file is located in `C:\Program Files (x86)\Centrify\Centrify PuTTY`.

To use group policies to configure Centrify PuTTY settings, an administrator must copy either the `admx` file or the `xml` file to the appropriate domain controller. If your organization centrally manages Centrify PuTTY settings through these group policies, you do not have to configure them manually for individual secure shell sessions.

By default, all group policies are set to **Not Configured**. Individual policies must be set to **Enabled** to activate a setting. Policies can also be set to **Disabled** to explicitly disable a setting. For details about how policies with Enabled or Disabled settings are inherited or overridden based on where they are applied, see the *Group Policy Guide* and Microsoft documentation for group policies.

Most group policy settings are equivalent to the configuration settings described in Configuring the Centrify PuTTY client. For more information about the open-source PuTTY client configuration settings, see the standard PuTTY documentation. For information about specific group policies, select the group policy, right-click to select **Properties**, then click the **Explain** tab.

Using other Centrify-enabled PuTTY programs

In addition to the main PuTTy client (`putty.exe`), Centrify has modified the standard versions of the `pscp.exe`, `psftp.exe`, and `plink.exe` programs to support Kerberos authentication.

The modified `pscp.exe` program supports the following command formats:

```
pscp [options] [user@]host:source target
pscp [options] source [source...] [user@]host:target
pscp [options] -ls [user@]host:filespec
```

The modified `psftp.exe` program supports the following command formats:

```
psftp [options] [user@]host
```

The modified `plink.exe` program supports the following command formats:

```
plink [options] [user@]host [command]
```

Many of the PuTTY settings can be provided as options to the command line tools. You can also save command line settings into sessions and load them when executing commands using the `–load` option. If the settings in a saved session conflict with those specified when invoking the command, the specified options take precedence.

In addition to the standard PuTTY command line options, Centrify PuTTY provides the following options:

Option	Description
-k	Use Kerberos authentication and provide a UNIX user account name during login. This option is equivalent to selecting **Attempt Kerberos auth (SSH-2)** and **None** for the Auto-login username in the Centrify PuTTY Kerberos configuration page.
-K	Use Kerberos authentication and do auto login. This option is equivalent to selecting both **Attempt Kerberos auth (SSH-2**) and the **User principal name (requires DirectControl)** for the Auto-login username in the Centrify PuTTY Kerberos configuration page.
-spn	Specify the service principal name (SPN) of the target computer. This option takes effect only when the –k or –K option is used. This option is equivalent to specifying the computer's service principal name for the **Service principal name** in the Centrify PuTTY Kerberos configuration page.

The other Kerberos settings—such as Create forwardable tickets and Find machine from trusted domains—are not exposed as options to the `pscp.exe`, `psftp.exe` and `plink.exe` programs. You can configure these settings using

the Centrify PuTTY client user interface, save them in a session, then load the session using the `-load` option.

The following example illustrates how to use Centrify PuTTY command line options to facilitate administrative tasks. In this example, the `pscp.exe` program is used to retrieve the file `/etc/group` from a remote Linux computer named `RedHatLinux` with the current user's login name and Kerberos credentials for authentication on the remote computer:

```
pscp -K RedHatLinux:/etc/group c:\temp
```

Because this command uses the `-K` option, you don't need to specify a user name in the command line or be prompted for password during runtime. Therefore, the command can be embedded in a batch file for administrative use. However, this command would require the remote `RedHatLinux` computer to have the Centrify agent installed and be joined to an Active Directory domain.

Getting more information

For more information about the open-source version of PuTTY and standard PuTTY documentation, see the following resources:

- PuTTY website: http://www.chiark.greenend.org.uk/~sgtatham/putty/
- PuTTY documentation: http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html