Delinea

Server Suite

Delinea-Enabled PuTTY User's Guide

Version: 2023.x

Publication Date: 5/16/2024

Server Suite Delinea-Enabled PuTTY User's Guide

Version: 2023.x, Publication Date: 5/16/2024

Table of Contents

Delinea-Enabled PuTTY User's Guide

The *Delinea-enabled PuTTY User's Guide* describes how to install and configure the Delinea-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 Server Suite has been modified to support Kerberos-based authentication on remote computers that are managed by Server Suite software.

Intended Audience

This guide is intended for users who want to use the Delinea-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 Server Suite components and that you have sufficient privileges to perform administrative tasks on your managed computers.

Using the Delinea 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 Server Suite has been modified to enable users to be authenticated using their Kerberos credentials before establishing a remote connection.

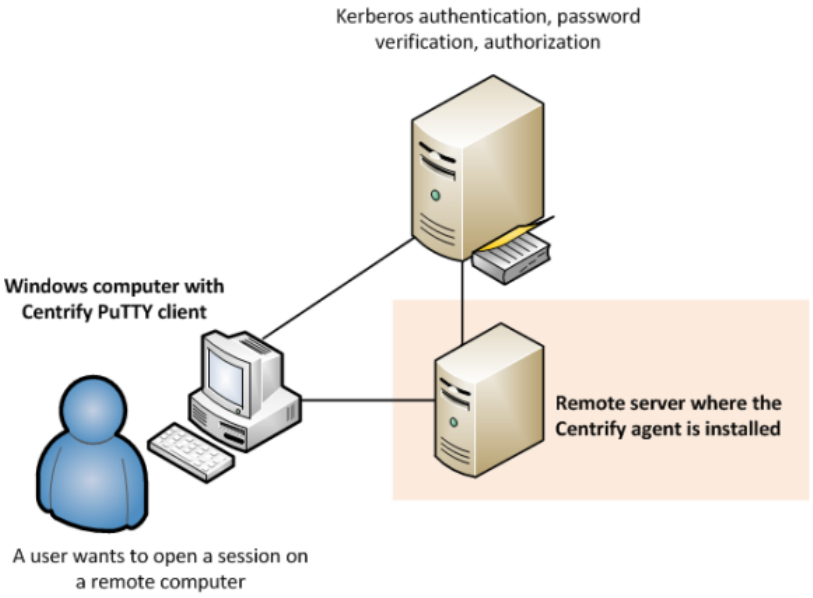
Accessing Remote Server Suite-Managed Computers

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 Server Suite Agent. However, the most common reason for using the Delinea PuTTY client is to open secure shell (ssh) sessions on remote Server Suite-managed computers. If you have the Server Suite 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 Delinea PuTTY client to access Server Suite-managed computers through SSH, the Server Suite 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 Server Suite Agent is also responsible for setting up and managing the Kerberos environment on Server Suite-managed computers. You are not required to configure any DNSto-realm mapping because the agent already knows the relationship between the host computers and their service principal names (SPNs).

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



If you use the Delinea PuTTY client with other protocols or to access remote computers that are not managed by the Server Suite 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.

> The Delinea PuTTY client is based on PuTTY version 0.64. This version of the Delinea PuTTY client is compatible with the Server Suite Agent, version 4.x and later, and with Centrify OpenSSH, version 4.x, and later.

Installing Delinea PuTTY

The Delinea 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 Delinea PuTTY client by selecting it when you install other Server Suite components or as a standalone executable using its own setup program. If you downloaded the Delinea 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 Server Suite.

To install the Delinea 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.

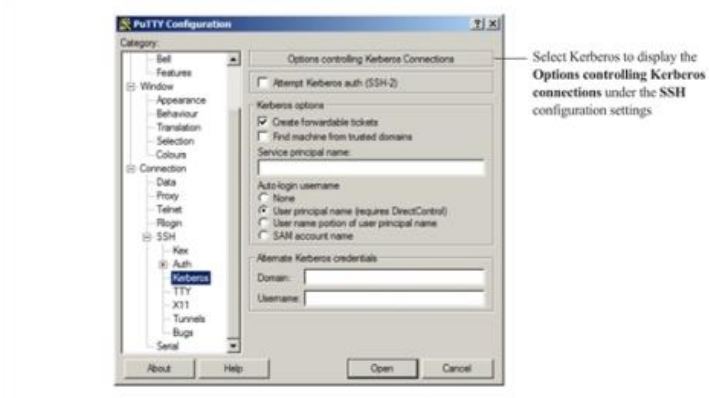
For more information about using these programs, see the official PuTTY documentation. For references to the official PuTTY documentation, see Getting More Information.

Configuring the Delinea 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 Delinea PuTTY client adds its own SSH Kerberos configuration page to the standard Windows PuTTY client. All other functionality in the Delinea PuTTY client is the same as in the official PuTTY client, version 0.64.

Starting the Delinea PuTTY Client

After installation, you can start the Delinea 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 Delinea PuTTY client as they are in the open-source PuTTY client. For example:

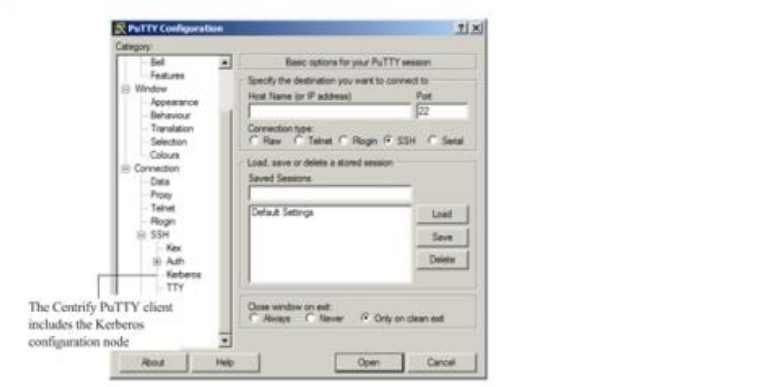


Configuring Kerberos Authentication for Secure Shell Connections

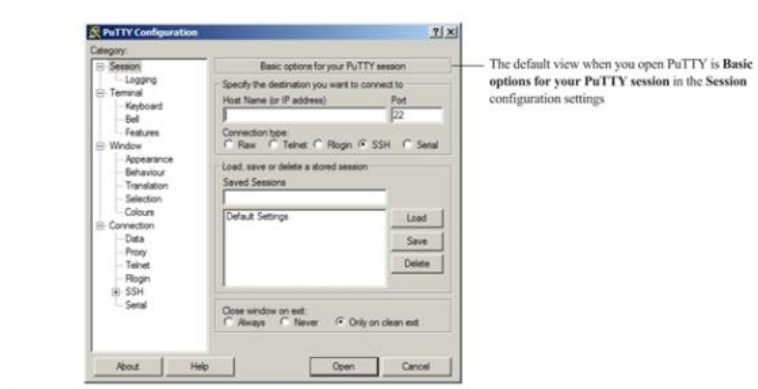
The Kerberos configuration options that have been added to the Centrify version of the PuTTY client are available under the Connection and SSH configuration settings.

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 Delinea 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 Delinea PuTTY, see Configuring Group Policies for Delinea 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 Delinea 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 Delinea 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 Delinea PuTTY group policies. For more information about the group policies for configuring Delinea PuTTY, see Configuring Group Policies for Delinea PuTTY.

  - Type a specific **Service principal name** if a target computer is in a different forest or if the Delinea 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 Delinea 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 Delinea 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 Delinea PuTTY client does not automatically generate the UNIX user account name.

   - Select **User principal name (requires DirectControl)** if you want the Delinea 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 Delinea 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 Delinea PuTTY client would use jdoe as the UNIX user name for authentication.

   - Select **SAM account name** if you want the Delinea 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 Delinea PuTTY client will initiate an LDAP connection to the currently logged-in domain controller. If the connection or lookup request fails, the Delinea 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 Delinea 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 Delinea 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 Delinea PuTTY, see Configuring Group Policies for Delinea 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 Delinea 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 Delinea 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 Delinea PuTTY, see Configuring Group Policies for Delinea PuTTY.

Configuring Group Policies for Delinea 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 Delinea 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 Delinea PuTTY settings, an administrator must copy either the admx file or the xml file to the appropriate domain controller. If your organization centrally manages Delinea 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 Delinea PuTTY client. For more information about the opensource 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, Delinea 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 Delinea 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 Delinea 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 Delinea 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 Delinea PuTTY client user interface, save them in a session, then load the session using the -load option.

The following example illustrates how to use Delinea 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 Server Suite 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