SERVER SUITE TECHNICAL BRIEF

Configuring PuTTY for Kerberos-Based Authentication to Linux & UNIX

How to implement Active Directory-based silent authentication for PuTTY to AIX, HP-UX, Red Hat, Solaris, SUSE Ubuntu, VMware and other non-Windows systems using the Centrify Suite

PuTTY is a popular open source Windows utility that lets you log in to remote Linux and UNIX computers. (Read more information about PuTTY.) The baseline PuTTY utility does not support Kerberos GSS key-exchange, and is frequently deployed in environments where users log in using root, shared service or local accounts. To enhance security and enable single sign-on with your Active Directory account, Centrify delivers a packaged and tested version of PuTTY that works seamlessly with UNIX and Linux systems that have been joined to Active Directory using the Centrify Server Suite or Centrify Express. Centrify also enables you to centrally configure security settings for PuTTY using Windows Group Policy.

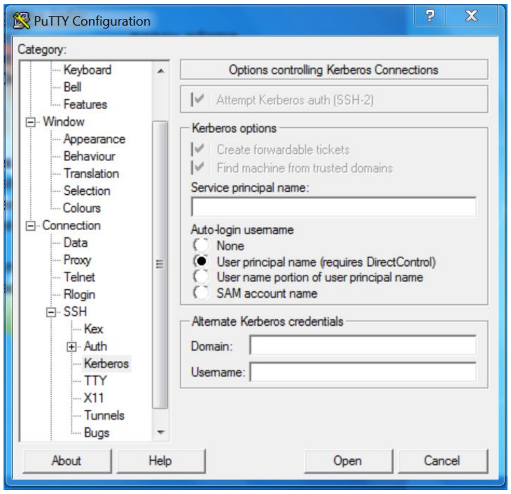
You can download the Centrify-enabled version of PuTTY along with Centrify Express, our free Active Directory-based solution for authentication and single sign-on to cross-platform systems.

How the Centrify-Enabled PuTTY Works

When the Centrify Server Suite Agent is installed on a UNIX or Linux computer, it sets up a Kerberos environment in order to communicate securely with Active Directory. Centrify has recompiled the open source Windows PuTTY client with the Server Suite Kerberos libraries, enabling PuTTY to connect securely via SSH (Secure Shell) to Server Suite-managed systems. If a user has previously authenticated to Active Directory, they enjoy transparent single sign-on and are not challenged to log in again because the Server Suite-managed system will honor their Kerberos ticket. If a user has not previously authenticated to Active Directory, they

will be challenged to log in. They can log in with their Active Directory credentials, or they can log in with any UNIX account that is managed within Active Directory using Server Suite. In either case, access to that computer is controlled through the user's Active Directory account, ensuring that access controls and Group Policies for that user are respected.

Centrify has customized the SSH Kerberos property page (see the screenshot). When the Attempt Kerberos Auth (SSH-2) option is checked, the Centrify-Enabled version of PuTTY will try to connect to remote systems using Kerberos first. Additional options let you specify how PuTTY searches for computers to connect to, and how user names, Kerberos credentials, and passwords are handled. You can control these settings globally through Group Policy. Centrify provides a user manual that documents these settings (along with installation steps and other instructions).



Options controlling Kerberos Connections

☑ Attempt Kerberos auth (SSH-2)

Kerberos options

☑ Create forwardable tickets

☑ Find machine from trusted domains

Service principal name:

Auto-login username

○ None

● User principal name (requires DirectControl)

○ User name portion of user principal name

○ SAM account name

Alternate Kerberos credentials

Domain:

Username:

Centrify has added only Kerberized SSH functionality. Other connections such as rlogin and telnet are not affected, and all other features remain the same as in the official PuTTY open source release. You can use the Centrify-Enabled version of PuTTY with systems that have not been secured through Active Directory using Server Suite, but of course you do not receive the security and compliance benefits of using the two together.

Centrally Configuring PuTTY Using Windows Group Policy

With the Centrify Server Suite you have the ability to use Windows Group Policy to globally apply security and configuration settings across mixed UNIX, Linux and Mac systems. The Centrify installer for the Centrify-Enabled PuTTY includes a Group Policy Object administrative template that you can use to globally control the configurable PuTTY settings, including the Kerberos options for SSH connections that Centrify has added. For example, you can control:

- Whether Kerberos credentials can be passed to another SSH server.
- How PuTTY locates a target computer within trusted domains.
- How the UNIX account name is provided to the SSH server on the target computer.
- Whether users can specify alternative Kerberos credentials.
- How many times a password attempt is allowed.

Benefits of Using the Centrify-Enabled PuTTY

The baseline PuTTY utility does not support Kerberos GSS key-exchange, and it is frequently deployed in environments where users log in using root, shared service or local accounts, which prevents security managers from assigning access rights and privileges based on an individual user's role, and prevents IT compliance auditors from linking actions taken on audited systems with specific individuals.

By deploying the Centrify-Enabled PuTTY utility for remote access to Server Suite-managed UNIX and Linux systems, you gain the following benefits:

- IT Security. Kerberos provides a secure, encrypted connection to the remote computer to protect session data as it moves across the network. The Centrify-Enabled PuTTY leverages the Active Directory Kerberos trust model for verifying host identity, thus eliminating the need to distribute RSA key fingerprint files and registry entries to every host in the enterprise. You can also centrally configure PuTTY through Group Policy so you can enforce a consistent security policy for the way users connect to sensitive systems.
- IT Compliance. Enforcing the use of the Centrify-Enabled PuTTY for Active Directory-based authentication can ensure that users are logging in using their individual Active Directory credentials instead of with superuser or other shared accounts. The access controls (defined using Centrify's unique, granular Zone-based access controls) and role-based privileges (defined using Centrify Server Suite) set for that user will thus be enforced on the UNIX and Linux systems.
- Quick, Consistent Deployment. Centrify provides a packaged and tested version of PuTTY that includes a standard Windows installer and full documentation. This helps you get PuTTY deployed quickly and consistently throughout your organization..

Contact Centrify

Centrify provides unified identity management across data center, cloud and mobile environments that result in single sign-on (SSO) for users and a simplified identity infrastructure for IT. Centrify's unified identity management software and cloud-based Identity-as-a-Service (IDaaS) solutions leverage an organization's existing identity infrastructure to enable single sign-on, multi-factor authentication, privileged identity management, auditing for compliance and enterprise mobility management.

Santa Clara, California:	+1 (669) 444-5200	Email	sales@centrify.com
EMEA:	+44 (0) 1344 317950	Web	http://www.centrify.com
Asia Pacific:	+61 1300 795 789		
Brazil:	+55 11 3958 4876		
Latin America:	+1 305 900 5354		