SERVER SUITE TECHNICAL BRIEF

Secure, Active Directory-Based Single Sign-On with AbsoluteTelnet/SSH and Centrify

This single sign-on solution via AbsoluteTelnet/SSH requires that the target UNIX systems be joined to Active Directory using Centrify Server Suite. To see for yourself how Server Suite enables you to centrally control access to UNIX, Linux and Mac systems from Active Directory:

AbsoluteTelnet 5.0 from Celestial Software integrates with Active Directory to provide single sign-on to UNIX hosts running both Server Suite and OpenSSH servers by leveraging a user's existing credentials. Windows users running AbsoluteTelnet accessing UNIX systems running Server Suite and OpenSSH can be controlled centrally through Active Directory.

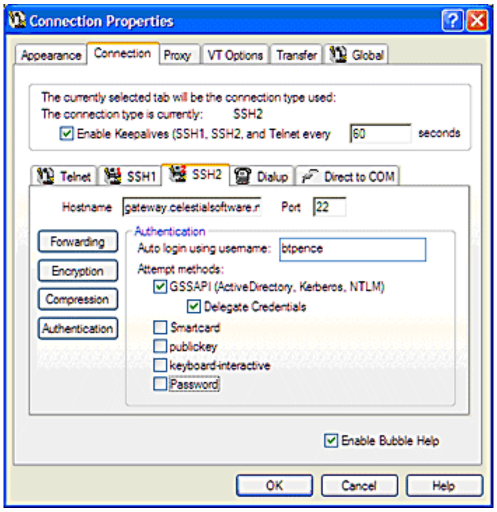
AbsoluteTelnet/SSH 5.0 Configuration

AbsoluteTelnet/SSH 5.0 running on a Windows computer that has been joined to Active Directory will support single sign-on to other computers that are properly configured for Kerberos-authenticated SSH connections. AbsoluteTelnet/SSH provides built-in support for Microsoft Kerberos-based authentication over SSH connections, so no additional configuration is required beyond simply selecting GSSAPI as the method of authentication when you are connecting to a remote system. UNIX systems running DirectControl and later versions of OpenSSH will provide the required Kerberos support to enable single sign-on for AbsoluteTelnet clients.

Using AbsoluteTelnet to Connect to a Remote DirectControl-Enabled System

The following instructions will show the options to select for a Kerberized SSH connection to a UNIX host.

1. Launch AbsoluteTelnet/SSH 5.
2. From the Options menu, choose Properties, and then click the Connection tab.
3. Fill in the hostname of the server you want to connect to. Use the fully qualified domain name (FQDN) so the host can be found in Active Directory.
4. The username field is filled in with the current Windows user. If the UNIX username is the same, leave this field alone. Otherwise, fill in the username of the UNIX account you are connecting to.
5. Enable GSSAPI authentication and (optionally) the credential delegation.
6. Click OK.
7. On the File menu, choose Connect, or click the Connect button on the toolbar.



The currently selected tab will be the connection type used:
The connection type is currently: SSH2
☑ Enable Keepalives (SSH1, SSH2, and Telnet every 60 seconds

Hostname gateway.celestialsoftware.r Port 22

Authentication
Auto login using username: btpence
Attempt methods:
☑ GSSAPI (ActiveDirectory, Kerberos, NTLM)
☑ Delegate Credentials
□ Smartcard
□ publickey
□ keyboard-interactive
□ Password

☑ Enable Bubble Help

Summary

Centrify Server Suite integrates UNIX systems with Active Directory to provide a fully configured and automatically maintained MIT Kerberos client environment that enables applications such as OpenSSH and AbsoluteTelnet/SSH to securely and seamlessly authenticate users based on their initial login, leveraging the mutual trust relationship that both the user and the computers share through the Active Directory domain controller infrastructure.

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		