



BeyondTrust

AD Bridge
Config Tool Reference Guide
Powered by PowerBroker

Table of Contents

Introduction	3
Overview	3
Access the Config Tool	3
Options	3
Commands	3
Event Log	4
Lsass	5
Lsass PAM	6
Lsass Active Directory	7
Lsass Local Provider	10
User Monitor	11
System Initialization	12
Netlogon	13
SNMP	14
AutoEnroll	15
lwpkcs11	16

Introduction

AD Bridge joins Unix, Linux, and Mac OS X computers to Active Directory so that you can centrally manage all your computers from one source, authenticate users with the highly secure Kerberos protocol, control access to resources, and apply group policies to non-Windows computers.

This guide describes how to manage Unix, Linux, and Mac OS X computers using the AD Bridge config tool.

Overview

The AD Bridge config tool provides policies similar to the GPO policies that can be applied to local Linux and Unix systems. The config tool policies can be set before the system is joined to a domain. If a GPO policy and config tool policy are applied to a target, the GPO policy overrides the config tool policy.

Access the Config Tool

The config tool is located at `/opt/pbis/bin/config`.

Usage: `config [OPTIONS] [COMMAND]`

Access Help

```
/opt/pbis/bin/config --help
```

Options

Option	Description
<code>--verbose</code>	Display additional information.

Commands

SETTING [VALUE]: Change **SETTING** to the given **VALUE(s)** or the default value if no value is specified.

Commands	Description
<code>--list</code>	Display names of all settings.
<code>--show SETTING</code>	Display current value(s) of SETTING.
<code>--detail SETTING</code>	Display current value(s) and details of SETTING.
<code>--file FILE</code>	Read FILE with each line beginning with a setting name followed by value(s). Use '!' for reading from stdin.
<code>--dump</code>	Dump all settings in a format suitable for use with <code>--file</code> .

Event Log

Command Name	Description
AllowDeleteTo	List of users that can delete entries from log.
AllowReadTo	List of users that can read entries from log.
AllowWriteTo	List of users that can write entries from log.
MaxDiskUsage	Max size in bytes of eventlog database. Default Value: 104857600
MaxEventLifespan	Maximum number of days that events are saved in eventlog. Default Value: 90
MaxNumEvents	Maximum number of events to hold in eventlog database. Default Value: 100000

Lsass

Command Name	Description
DomainSeparator	Character used to designate the domain name separator. Default Value: \
SpaceReplacement	Character used to designate space characters in names of objects. Default Value: ^
EnableEventlog	Configure Lsass to log events to the event log. Default Value: false
LogInvalidPasswords	Configure Lsass to log events for failed authentication attempts due to invalid passwords.
SaslMaxBufSize	Size of the buffer to allocate for decoding incoming LDAP responses (bytes). Default Value: 16777215
Providers	Configure which Lsass providers to load. Default Value: ActiveDirectory

Lsass PAM

Command Name	Description
DisplayMotd	Display message of the day. Default Value: false
PAMLogLevel	Configure PAM Lsass logging detail level. Default Value: error
UserNotAllowedError	Message displayed at console logon failed attempt. Default Value: Access denied
NssApplyAccessControl	Filter users returned by NSS based on RequireMembershipOf. Default Value: false

Lsass Active Directory

Command Name	Description
AssumeDefaultDomain	Apply domain name prefix to account name at logon. Default Value: false
CreateHomeDir	Whether home directories should be automatically created upon user logon. Default Value: true
CreateK5Login	Whether .k5login file is to be created on user logon. Default Value: true
SyncSystemTime	Whether system time should be synchronized with AD domain controller. Default Value: true
TrimUserMembership	Whether to remove a cached group membership entry derived from PAC with information from LDAP showing the user disappearing from a group. Default Value: true
LdapSignAndSeal	Whether all LDAP traffic should be sent both signed and sealed. Default Value: false
LogADNetworkConnectionEvents	Configure Lsass to log events for offline query failures and transitions. Default Value: true
NssEnumerationEnabled	Whether to enumerate users or groups for NSS. Default Value: true
NssGroupMembersQueryCacheOnly	Whether to return only cached info for NSS group members. Default Value: true
NssUserMembershipQueryCacheOnly	Whether to return only cached info for NSS user's groups. Default Value: false
RefreshUserCredentials	Whether to refresh user credentials against AD domain controller. Default Value: true
CacheEntryExpiry	Duration for when Lsass object cache entries are marked stale. Default Value: 14400
DomainManagerCheckDomainOnlineInterval	How often the domain manager should check whether a domain is back online. Default Value: 300

DomainManagerUnknownDomainCacheTimeout	How long an unknown domain is cached as unknown in the domain manage. Default Value: 3600
MachinePasswordLifespan	Machine password expiration lifespan in seconds. Default Value: 2592000
ServicePrincipalName	Update the local krb5 keytab file and computer account service principal name attribute in AD with the provided list of instances. Changes take affect on domain join. Default adds host service class. Default Value: host
MemoryCacheSizeCap	The maximum bytes to use for the in-memory cache. Old data will be purged if the total cache size exceeds this limit. A value of 0 indicates no limit. Default Value: 0
HomeDirForceLowercase	Forces the home directory (/.../domainname/username) to be lowercase. Lowercase home directory is created on user login. If configured, /etc/pbis/user-override file takes precedence. Default Value: false
HomeDirPrefix	Prefix path for user's home directory. This value is used in place of the %H in the HomeDirTemplate setting. Value must be an absolute path. Default Value: /home
HomeDirTemplate	Format string for user's home directory path. This value can contain substitution string markers for HomeDirPrefix (%H) , Domain (%D) , and User (%U) . Default Value: %H/local/%D/%U
RemoteHomeDirTemplate	Format string for the mount path of the remote Windows Folder. This value can contain substitution string markers for HomeDirPrefix (%H) , Domain (%D) , and User (%U) .
HomeDirUmask	Umask for home directories. Default Value: 022
LoginShellTemplate	Default login shell template. Default Value: /bin/sh
SkeletonDirs	Skeleton home directory template directories. Default Value: /etc/skel
UserDomainPrefix	Domain short name prefix to be used when AssumeDefaultDomain setting is enabled.
DomainManagerIgnoreAllTrusts	When true, ignore all trusts during domain enumeration.

DomainManagerIncludeTrustsList	When DomainManagerIgnoreAllTrusts is true, these trusts are included.
DomainManagerExcludeTrustsList	When DomainManagerIgnoreAllTrusts is false, these trusts are excluded.
RequireMembershipOf	Restrict logon access to computer to specific users or group members, or SIDs
IgnoreGroupAlias	When enabled, Group Alias will not be used when displaying group names.
SmartcardEnabled	Smart Card services will not be used when disabled. Default Value: false
SmartcardRedirector	Smart Card redirector services will not be used when disabled. Default Value: false
SmartcardRequiredForLogin	Smart Card will be required for login. Default Value: false

Lsass Local Provider

Command Name	Description
Local_AcceptNTLMv1	Allows local provider to accept NTLMv1. Default Value: true
Local_HomeDirTemplate	Format string for Lsass local provider account user's home directory path. This value can contain substitution string markers for HomeDirPrefix (%H) , Domain (%D) , and User (%U) . Default Value: %H/local/%D/%U
Local_HomeDirUmask	Umask for Lsass local provider account home directories. Default Value: 022
Local_LoginShellTemplate	Default login shell template for Lsass local provider accounts. Default Value: /bin/sh
Local_SkeletonDirs	Skeleton home directory template directories for Lsass local provider accounts. Default Value: /etc/skel

User Monitor

Command Name	Description
UserMonitorCheckInterval	Frequency in seconds that the user monitor service queries the system to see who can log in. Default Value: 1800

System Initialization

Command Name	Description
LsassAutostart	Start lsass when lwsmd starts. Default Value: true
EventlogAutostart	Start eventlog when lwsmd starts. Default Value: true
GpagentAutostart	Start gpagent when lwsmd starts. Default Value: false

Netlogon

Command Name	Description
BlacklistDC	List of blacklisted domain controller IP addresses.

SNMP

Command Name	Description
SNMPEnabled	True to send SNMP traps. Default Value: false
SNMPTarget	The IP address or machine name to send SNMP traps to. Default Value: localhost
SNMPPort	The port to send SNMP traps to. Default Value: 162
SNMPCommunity	SNMP Community. Default Value: public
SNMPLogonAuthenticationGroup	Enable all traps in the Logon/Authentication group. Default Value: false
SNMPAccountGroup	Enable all traps in the Account group. Default Value: false
SNMPSystemServicesGroup	Enable all traps in the System/Services group. Default Value: false
SNMPDomainGroup	Enable all traps in the Domain group. Default Value: false
SNMPSudoGroup	Enable all traps in the Sudo group. Default Value: false

AutoEnroll

Command Name	Description
Authentication	Name of certificate or passphrase. Default Value: none
AutoEnrollPollingInterval	Frequency in seconds autoenrollment queries CA Authority Service. Default Value: 28800
CertificateTemplateNames	List of certificate template names to auto enroll.
DeleteCertificatesWhenRemoved	Delete enrolled certificates when the certificate is removed from the CertificateTemplateNames list. Default Value: false
EnableAutoEnroll	Enable Auto Enroll functionality. Default Value: false
EnableWireless	Configure and enable the wireless interface. Default Value: false
EncryptPrivateKey	Certificate enrollment generates a private key file which by default is encrypted. Default Value: true
ManagedCertificateLifecycle	Renew, update and remove certificates. Default Value: false
SecurityType	(0) None (1) WPA2 - Enterprise or (2) WPA2 - Personal Default Value: 0
SSID	SSID of wireless router. Default Value: none

lwpkcs11

Command Name	Description
ModuleSearchList	Determines which pkcs11 module lwpkcs11 daemon uses to access Smart Card functionality. Default: <code>/usr/lib64/opensc-pkcs11.so</code> <code>/usr/local/lib/libpkcs11.so</code> <code>/usr/lib/libpkcs11.so</code>