

Clientix v 5.6

Interfaz LDAP – Active Directory



Contenido

REVISIONES DE ESTE DOCUMENTO	2
GENERALES.....	3
DIRECTORIO LDAP.....	3
CLIENTIX-LDAP : ESQUEMA DE INTEGRACIÓN.....	3
INSTALACIÓN	5
PRERREQUISITOS.....	5
CONFIGURACIÓN INICIAL.....	5
CREAR GRUPO DE USUARIOS	8
CREACIÓN DE USUARIOS	9
INCLUSIÓN EN ÁRBOL DE ACCESO	12
NOTAS FINALES	13
MENSAJES DE ERROR	13

Revisiones de este Documento

Fecha	Autor	Descripción del cambio
2018-08-30	C. Ramirez	Se arregla comentario sobre el valor por defecto del parámetro LDAP_SEARCH_FIELDNAME
2016-09-16	C. Ramirez	Se agrega pantalla que aparece al hacer clic en la lupa de creación de usuarios + instrucciones de cómo usarla. Se agrega documentación del parámetro LDAP_SEARCH_FIELDNAME y la opción 3 del parámetro LDAP_DIRECTORY_TYPE Se agrega instrucciones para incluir el usuario en el Árbol de Acceso
2014-10-22	M. Belfort	Desarrollo inicial

Generales

Directorio LDAP

LDAP son las siglas de “Lightweight Directory Access Protocol” (en español “Protocolo Ligero de Acceso a Directorios”) que hacen referencia a un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

LDAP es una base de datos que permite mantener información de personas o instituciones. En este sentido el directorio activo proporciona a Clientix un mecanismo único para la administración de usuarios que están autorizados a utilizar el sistema, los cuales se colocaran en este directorio según las reglas definidas por el administrador de seguridad.

La interfaz de LDAP permite a Clientix el reutilizar la información contenida dentro de este directorio con el objetivo de unificar la validación de acceso en un punto único. De esta forma si el usuario es inactivado en el LDAP este se encontrará automáticamente inactivado en la plataforma Clientix.

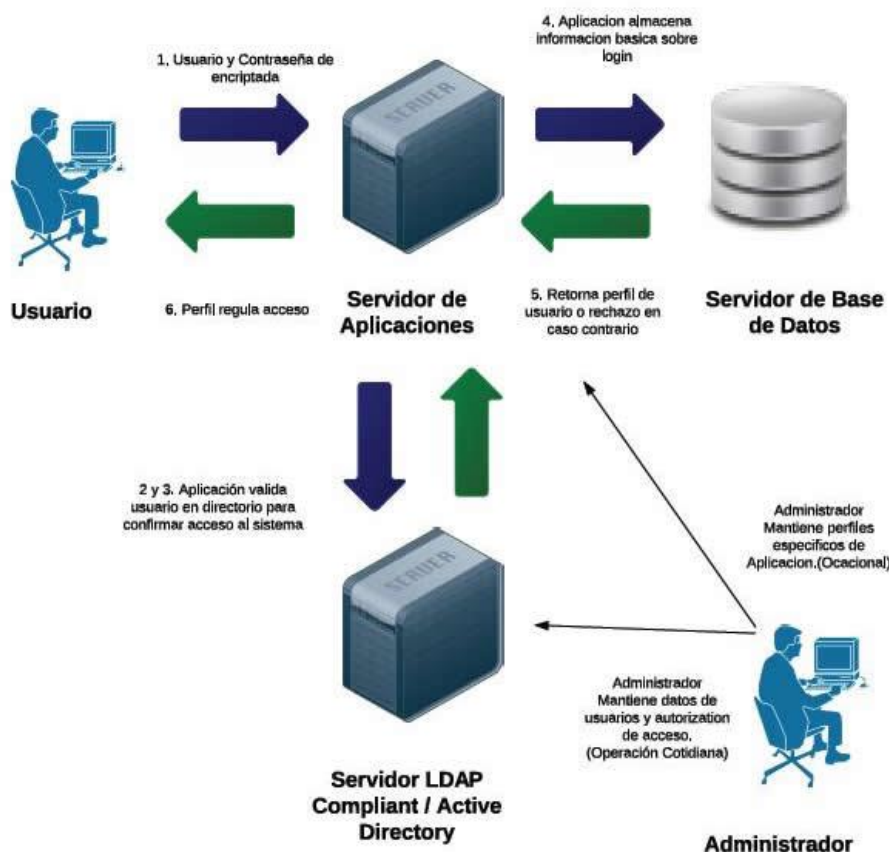
Clientix-LDAP : Esquema de integración

La base de datos LDAP es organizada en una estructura tipo árbol la cual puede ser definida bajo diferentes jerarquías tales como país, región, departamento, etc. Esta estructura es definida por el administrador del LDAP y Clientix no tiene requerimientos específicos bajo este tema.

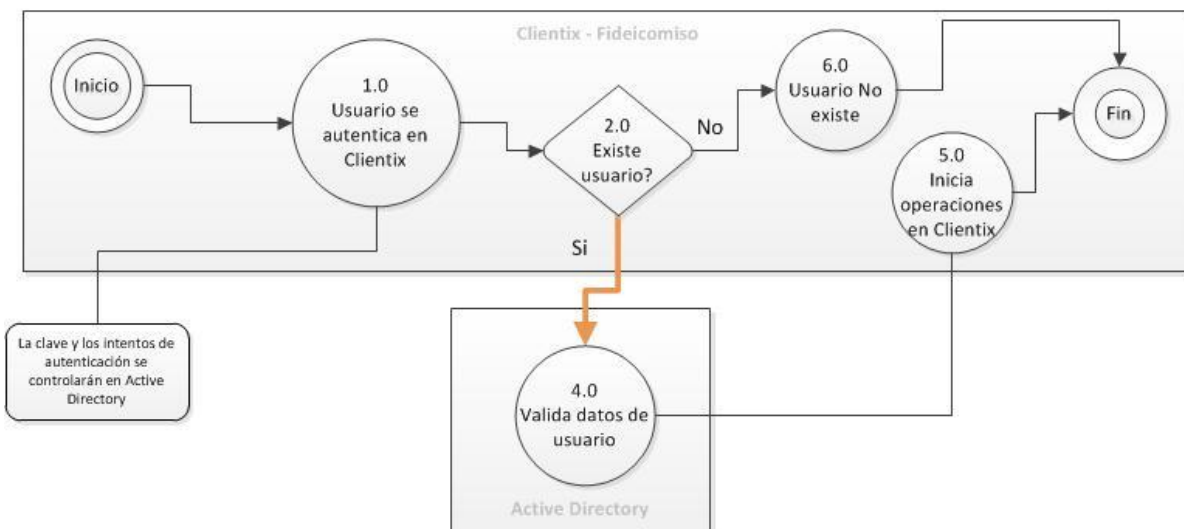
Clientix mantiene una base de datos de usuarios y grupos requerida para mantener su seguridad interna del módulo de Clientix. Estos usuarios deben existir tanto en LDAP como en Clientix para poder acceder el sistema. Adicionalmente los grupos de usuarios son independientes a estos creados en el sistema Clientix.

La seguridad específica del módulo Clientix debe ser realizada dentro de Clientix propiamente, mediante los Grupos de Usuarios, Acceso a Menú y Árboles de Acceso.

La infraestructura y detalle de la operación de la interfaz de LDAP y Clientix se presentan en los gráficos mostrados a continuación.



Interfaz Clientix - Autenticación en Active Directory



Instalación

Prerrequisitos

Previo a la implementación de la interfaz del LDAP en Clientix es necesario considerar los siguientes elementos:

- Servidor LDAP debe estar instalado y activo.
- El servidor LDAP debe tener definidos los usuarios a utilizar por Clientix.
- El servidor de LDAP debe estar visible desde el servidor de Clientix a través de la red.
- Acceso a la plataforma Clientix con opción a crear usuarios.
- Contar con los parámetros de LDAP:
 - Base de búsqueda (LDAP Search Base):
Ejemplo: o=University of Virginia,c=US
 - Host, ejemplo: ldap.virginia.edu
 - LDAP Port: 389 (por defecto)

Configuración Inicial

Para poder realizar la configuración inicial es necesario entrar al sistema Clientix con un usuario que tenga acceso a la funcionalidad de administración. Una vez dentro del sistema se procede a realizar los siguientes pasos:

1. Definir parámetros de LDAP:

Entrar en la opción de menú “ClientTools > Sistema > Parámetros”,
Hacer clic en el botón FILTRO,
En el campo “Código de Herramienta” especificar: **ACUS**
Hacer clic en el botón ESTABLECER FILTRO.

Los parámetros que se debe especificar son:

- a. **LDAP_BASE_DN**, define la base de búsqueda de LDAP. Es una cadena de caracteres. Ejemplos:

o=University of Virginia,c=US
dc=example,dc=com

- b. **LDAP_DIRECTORY_TYPE**, campo tipo entero que define el tipo de servidor LDAP al cual se está realizando la conexión. Las opciones posibles son:

Valor	Opción	Notas
0	Open LDAP	
1	Active Directory	Directorio Activo de Microsoft
3	Open LDAP Extendido	LDAP 3.0 Se agrega el LDAP_BASE_DN al nombre de usuario en la autenticación

- c. **LDAP_EXCL_GRP**, Define el nombre del Grupo de Exclusión usado para permitir el acceso de usuarios sin que se requiera que estén definidos en el directorio LDAP. Estos usuarios son generalmente administradores que requieran acceso a la aplicación en caso de no existir conexión al servidor LDAP. El parámetro espera una cadena de caracteres con el código del grupo separados por comas. En caso de ser **0** este parámetro no tendrá efecto y solo súper-administradores tendrán acceso sin la autenticación de LDAP.
- d. **LDAP_HOST**, define la ruta donde se encuentra ubicado el servidor LDAP. Por ejemplo: ldap.virginia.edu.
El prefijo de la ruta "LDAP::/" no es requerido.
- e. **LDAP_PORT**, es un número entero que define el Puerto en el cual se encuentra definido el LDAP. El puerto por defecto de LDAP es el **389**. Solo cambiar en caso de ser diferente a 389.
- f. **LOGIN_MODE**, este parámetro permite definir la modalidad a utilizar el módulo de Clientix en cuanto a su autenticación. Por defecto el sistema usa el modo **CLX** el cual autentifica contra la base de datos local. En caso de LDAP en este parámetro debe asignarse el valor: **LDAP**.
- g. **LDAP_SEARCH_FIELDNAME**, es opcional y permite especificar el campo DN para realizar las búsquedas en el directorio LDAP. El valor por defecto es "cn" en el caso de LDAP y "sAMAccountName" en el caso Active Directory.

2. Crear el o los Grupos de Usuarios requeridos (ver sección **Crear Grupo de Usuarios** para más información)
3. Crear un usuario de administración de Clientix con nombre de usuario que se encuentre en el directorio LDAP. Este usuario será el que esté capacitado para crear otros usuarios dentro de Clientix.

EL detalle con este usuario es que será utilizado al hacer clic en la lupa de Creación de Usuarios que permite desplegar los usuarios activos en el directorio LDAP y luego seleccionarlos sin tener que escribir el nombre de usuario manualmente.

4. Asignar usuario de administración de Clientix recién creado al Grupo que permita crear usuarios.
5. Salir del sistema e intentar entrar con el usuario de administración de Clientix recién creado, el cual se debe encontrar habilitado en el directorio LDAP.
6. Configurar otros usuarios del sistema.
7. Asignar los otros usuarios creados al Árbol de Acceso.

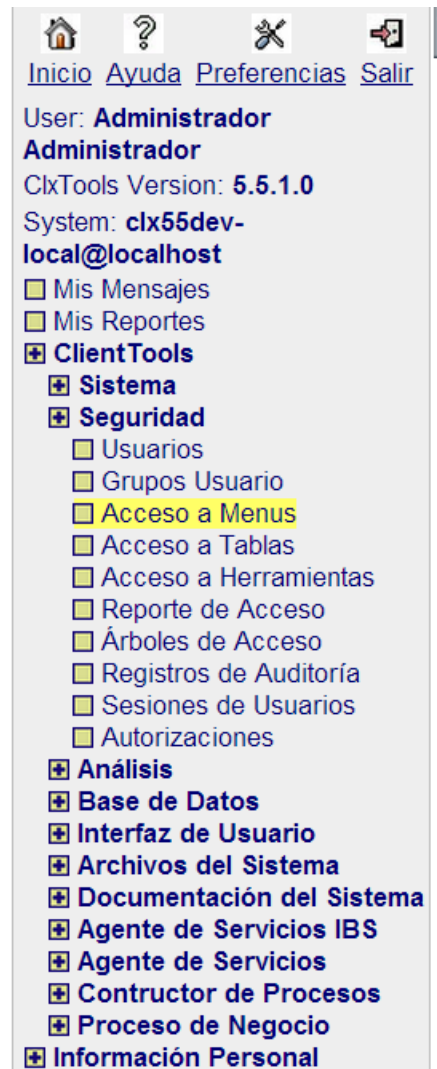
Crear Grupo de Usuarios

Los perfiles de los usuarios están representados por: Grupos de Usuarios + Accesos a Menú + Árboles de Acceso.

Para crear los Grupos de Usuarios es necesario entrar en la opción “ClientTools > Seguridad > Grupos de Usuarios”. Dentro de esta opción se encuentra los botones requeridos para crear nuevos grupos o modificar los ya existentes.

Una vez creado el Grupo, las garantías de acceso a las distintas opciones de menú y las acciones que se pueden realizar dentro de dichas opciones se define en la opción “ClientTools > Seguridad > Acceso a Menús > ASISTENTE DE ACCESO”.

Es posible dar las garantías de acceso a nivel de Grupo o a nivel de Usuario, sin embargo, se recomienda asignar siempre la seguridad a nivel de Grupos de Usuarios ya que facilita su administración.



Creación de Usuarios

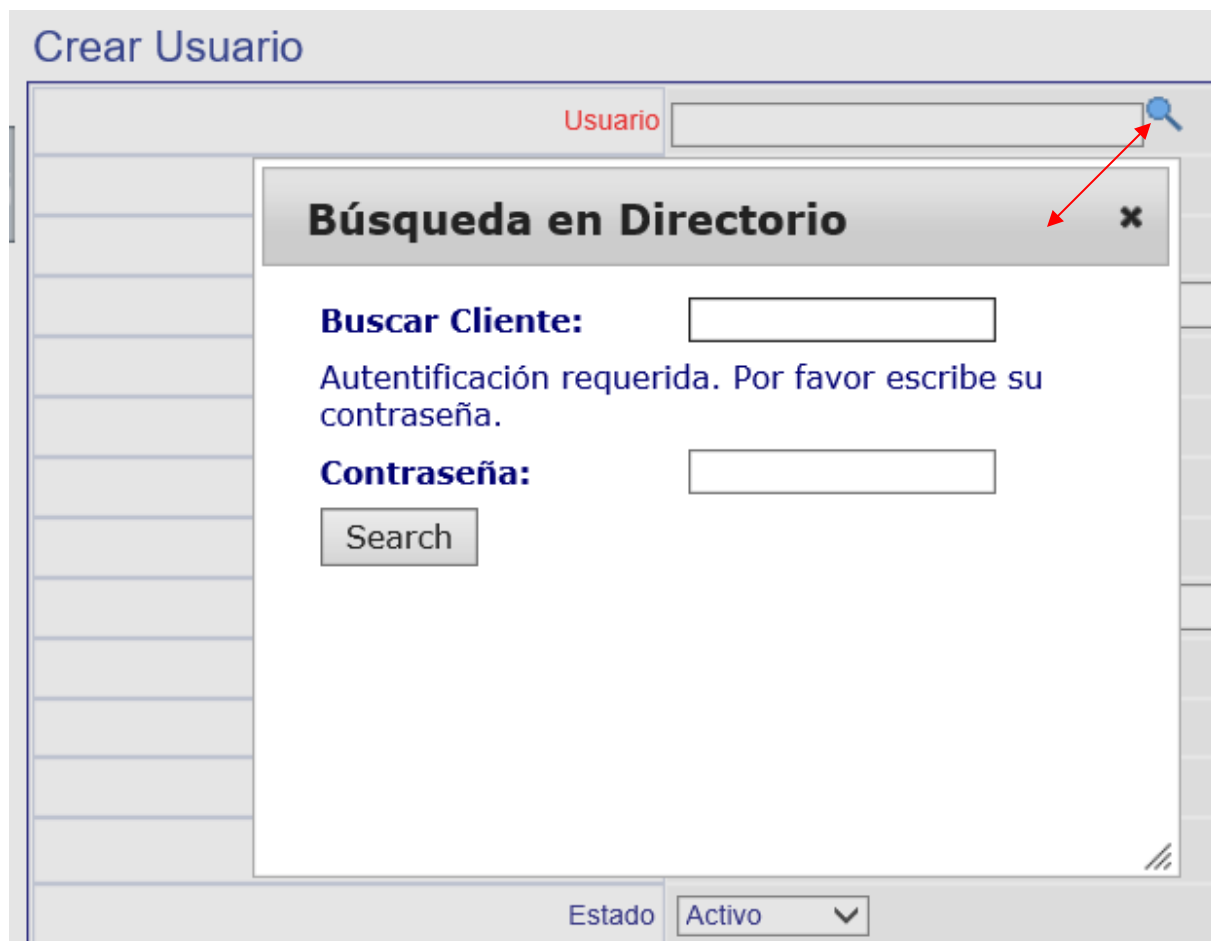
Para crear usuarios dentro del módulo de Clientix es necesario realizar los siguientes pasos:

1. Entrar al menú “ClientTools > Seguridad > Usuarios”
2. Hacer clic en botón **CREAR**
3. Se mostrará la pantalla de creación de usuarios presentada a continuación.

Crear Usuario

Usuario	<input type="text"/>
Contraseña	<input type="password"/>
Confirmar	<input type="password"/>
Nombre Usuario LDAP (CN)	<input type="text"/>
Nombre	<input type="text"/>
Apellido	<input type="text"/>
Compañía	<input type="text"/>
Posición	<input type="text"/>
Correo Electrónico	<input type="text"/>
Número de Teléfono	<input type="text"/>
Número de Fax	<input type="text"/>
No de Ref.. Externo	<input type="text"/>
Auditar este Usuario	No ▼
Estado	Activo ▼
Administrador de Sistema	No ▼
Por defecto la contraseña expira en 30 días o según lo definido en parámetros.	
Contraseña expira	No ▼
Cambio de contraseña será requerido en el próximo inicio de sesión.	
Solicitar cambio de contraseña	No ▼
Intentos de login	0
Contador de Login	0

4. La lupa anexa al campo “Usuario” permite realizar consultas al directorio LDAP para facilitar la búsqueda de los nuevos usuarios. La opción de búsqueda de usuario solo se encuentra activa cuando el parámetro modo de Login (LOGIN_MODE) se encuentra asignado a tipo LDAP



El campo “Buscar Cliente” permite especificar total o parcialmente el nombre de usuario y filtrar la lista que aparecerá al hacer clic en el botón SEARCH.

Este campo no se puede dejar en blanco.

Si se especifica * se muestra la lista completa del directorio LDAP.

También se puede usar * a modo de comodín al principio, al final, o en ambas partes, en caso de no recordar el nombre completo del usuario.

Se debe especificar en el campo “Contraseña” la contraseña del usuario con el que se hizo Login en Clientix. Esto es necesario para poder autenticar y consultar el directorio LDAP.

Al hacer clic en el botón SEARCH, aparece la lista de usuarios en el directorio LDAP. Hacer clic en uno de ellos se asignarán los distintos campos en la forma de entrada de datos de “Crear Usuario”

Si no se encuentran coincidencias, aparecerá el mensaje “0 Encontrado(s)”

5. Completar la información en la forma de entrada de datos de “Crear Usuario”.
6. Hacer clic en el botón **GUARDAR** para completar el registro.
7. Una vez creado se debe asignar el usuario a un Grupo previamente definido.

Para realizar esta tarea, de la lista de usuarios en la opción “ClientTools > Seguridad > Usuarios”, marcar el usuario al cual se desea agregar a un Grupo y hacer clic en el botón DESPLEGAR.

Dentro se encontrará la sección “Grupo de Conjunto de Miembros” donde se puede asignar el o los Grupos a los que pertenecerá.

Grupo de Conjunto de Miembros

SEL	Código	Nombre	Notas o Descripción	Estado
<input type="checkbox"/>	EXCLUSION	GRUPO DE EXCLUSION		Active
<input type="checkbox"/>	OFICIAL_OPE	Oficial de Operaciones	Oficial de Operaciones	Active
<input type="button" value="DESPLEGAR"/> <input type="button" value="MODIFICAR"/> <input type="button" value="EXCLUIR"/> <input type="button" value="CREAR AGRUPAR"/> <input type="button" value="INCLUIR ESTE USUARIO EN UN GRUPO"/>				
Mostrando: 1 - 2 de 2				

Para incluir el usuario en un Grupo, hacer clic en el botón INCLUIR ESTE USUARIO EN UN GRUPO

Para excluir el usuario de un Grupo, hacer clic en el botón EXCLUIR

Inclusión en Árbol de Acceso

Los Árboles de Acceso permite definir la seguridad a nivel de registro.

Para incluir usuarios dentro del Árbol de Acceso general, es necesario realizar los siguientes pasos:

1. Entrar al menú “Configuración General > Árbol de Acceso”
2. Marcar el registro “AAA” y hacer clic en el botón DESPLEGAR
3. En la sección “Usuarios Asignados” Hacer clic en el botón INCLUIR USUARIO
4. Especificar el nombre del usuario o seleccionar uno mediante la lupa.

Añadir Usuario

Usuario	<input type="text"/>
Estado	Activo ▼
Predeterminada	Si ▼
<input type="button" value="GUARDAR"/> <input type="button" value="CANCELAR"/>	

5. Hacer clic en el botón GUARDAR

Notas Finales

Mensajes de error

El sistema Clientix mantiene una lista de códigos de errores del LDAP.

La lista de código comunes de LDAP (<http://support.microsoft.com/kb/218185>) es la siguiente:

Code	Value	Description
LDAP_SUCCESS	0x00	Successful request.
LDAP_OPERATIONS_ERROR	0x01	Intialization of LDAP library failed.
LDAP_PROTOCOL_ERROR	0x02	Protocol error occurred.
LDAP_TIMELIMIT_EXCEEDED	0x03	Time limit has exceeded.
LDAP_SIZELIMIT_EXCEEDED	0x04	Size limit has exceeded.
LDAP_COMPARE_FALSE	0x05	Compare yielded FALSE.
LDAP_COMPARE_TRUE	0x06	Compare yielded TRUE.
LDAP_AUTH_METHOD_NOT_SUPPORTED	0x07	The authentication method is not supported.
LDAP_STRONG_AUTH_REQUIRED	0x08	Strong authentication is required.
LDAP_REFERRAL_V2	0x09	LDAP version 2 referral.
LDAP_PARTIAL_RESULTS	0x09	Partial results and referrals received.
LDAP_REFERRAL	0x0a	Referral occurred.
LDAP_ADMIN_LIMIT_EXCEEDED	0x0b	Administration limit on the server has exceeded.
LDAP_UNAVAILABLE_CRIT_EXTENSION	0x0c	Critical extension is unavailable.
LDAP_CONFIDENTIALITY_REQUIRED	0x0d	Confidentiality is required.
LDAP_NO_SUCH_ATTRIBUTE	0x10	Requested attribute does not exist.
LDAP_UNDEFINED_TYPE	0x11	The type is not defined.
LDAP_INAPPROPRIATE_MATCHING	0x12	An inappropriate matching occurred.
LDAP_CONSTRAINT_VIOLATION	0x13	A constraint violation occurred.
LDAP_ATTRIBUTE_OR_VALUE_EXISTS	0x14	The attribute exists or the value has been assigned.
LDAP_INVALID_SYNTAX	0x15	The syntax is invalid.
LDAP_NO_SUCH_OBJECT	0x20	Object does not exist.
LDAP_ALIAS_PROBLEM	0x21	The alias is invalid.
LDAP_INVALID_DN_SYNTAX	0x22	The distinguished name has an invalid syntax.
LDAP_IS_LEAF	0x23	The object is a leaf.
LDAP_ALIAS_DEREF_PROBLEM	0x24	Cannot de-reference the alias.
LDAP_INAPPROPRIATE_AUTH	0x30	Authentication is inappropriate.
LDAP_INVALID_CREDENTIALS	0x31	The supplied credential is invalid.
LDAP_INSUFFICIENT_RIGHTS	0x32	The user has insufficient access rights.
LDAP_BUSY	0x33	The server is busy.

LDAP_UNAVAILABLE	0x34	The server is unavailable.
LDAP_UNWILLING_TO_PERFORM	0x35	The server does not handle directory requests.
LDAP_LOOP_DETECT	0x36	The chain of referrals has looped back to a referring server.
LDAP_NAMING_VIOLATION	0x40	There was a naming violation.
LDAP_OBJECT_CLASS_VIOLATION	0x41	There was an object class violation.
LDAP_NOT_ALLOWED_ON_NONLEAF	0x42	Operation is not allowed on a non-leaf object.
LDAP_NOT_ALLOWED_ON_RDN	0x43	Operation is not allowed on RDN.
LDAP_ALREADY_EXISTS	0x44	The object already exists.
LDAP_NO_OBJECT_CLASS_MODS	0x45	Cannot modify object class.
LDAP_RESULTS_TOO_LARGE	0x46	Results returned are too large.
LDAP_AFFECTS_MULTIPLE_DSAS	0x47	Multiple directory service agents are affected.
LDAP_OTHER	0x50	Unknown error occurred.
LDAP_SERVER_DOWN	0x51	Cannot contact the LDAP server.
LDAP_LOCAL_ERROR	0x52	Local error occurred.
LDAP_ENCODING_ERROR	0x53	Encoding error occurred.
LDAP_DECODING_ERROR	0x54	Decoding error occurred.
LDAP_TIMEOUT	0x55	The search was timed out.
LDAP_AUTH_UNKNOWN	0x56	Unknown authentication error occurred.
LDAP_FILTER_ERROR	0x57	The search filter is incorrect.
LDAP_USER_CANCELLED	0x58	The user has canceled the operation.
LDAP_PARAM_ERROR	0x59	An incorrect parameter was passed to a routine.
LDAP_NO_MEMORY	0x5a	The system is out of memory.
LDAP_CONNECT_ERROR	0x5b	Cannot establish a connection to the server.
LDAP_NOT_SUPPORTED	0x5c	The feature is not supported.
LDAP_CONTROL_NOT_FOUND	0x5d	The ldap function did not find the specified control.
LDAP_NO_RESULTS_RETURNED	0x5e	The feature is not supported.
LDAP_MORE_RESULTS_TO_RETURN	0x5f	Additional results are to be returned.
LDAP_CLIENT_LOOP	0x60	Client loop was detected.
LDAP_REFERRAL_LIMIT_EXCEEDED	0x61	The referral limit was exceeded.
LDAP_SASL_BIND_IN_PROGRESS	0x0E	Intermediary bind result for multi-stage binds