

Xerox

DocuShare[®]

DocuShare
LDAP/Active Directory-
Handbuch



Datum der Veröffentlichung: März 2011

Dieses Dokument bezieht sich auf DocuShare Version 6.6.1

Erstellt von:

Xerox Corporation
DocuShare Business Unit
3400 Hillview Avenue
Palo Alto, California 94304
USA

© 2011 Xerox Corporation. Alle Rechte vorbehalten. Xerox®, DocuShare® und Fuji Xerox® sind Marken der Xerox Corporation in den USA und/oder anderen Ländern. Alle anderen Marken sind Eigentum der jeweiligen Hersteller und werden als solche anerkannt.

Inhaltsverzeichnis

Kapitel 1 Die LDAP-Struktur

LDAP-Überblick	1-1
LDAP-Struktur	1-2
Verzeichnisse	1-2
Attribute	1-2
Relative Distinguished Name	1-3
Distinguished Name	1-3
Directory Information Tree	1-4
DIT-Organisation anhand von geographischen Domänen	1-4
DIT-Organisation anhand von DNS	1-5

Kapitel 2 LDAP/DocuShare-Konfiguration

DocuShare-Konfiguration	2-1
A: LDAP-Konfiguration	2-1
B: Erweiterte Konfiguration	2-2
C: LDAP-Provider aktivieren	2-2
D: Benutzer binden	2-3
E: Gruppe binden	2-3
F: Domäne einrichten	2-3
G: Hinzufügen	2-4
H: Anmeldung anzeigen	2-5
LDAP und SSL	2-6
Zertifikate	2-6
Zertifikate in DocuShare importieren	2-6
Zertifikate exportieren und als CER-Datei speichern	2-7
Zertifikate in DStTrustStore platzieren	2-8
Active Directory-Verwaltung	2-10
Active Directory-Verwaltung verwenden	2-11
A: Verbinden	2-11
B: Anbinden	2-11
C: Stamm-DN suchen	2-11
D: Directory Information Tree anzeigen	2-12
E: Agentenkonto suchen	2-12
F: Nächster Schritt	2-13
LDIFDE-Befehl für Active Directory	2-14
Syntax und Verwendung des LDIFDE-Befehls	2-15
Beispiel zum LDIFDE-Befehl	2-16
Ausführen des LDIFDE-Befehls	2-16
Die erzeugte adexport.txt-Datei	2-17
Analyse des Inhalts der adexport.txt-Datei	2-19

A: DIT-Stammverzeichnis (Directory Information Tree)	2–19
B: Benutzer-RDN-Schlüssel	2–19
C: Relative Authentifizierungs- und Verzeichnisdienstlocatoren	2–20
D: Attribute von „Benutzer binden“	2–20
E: Attribute von „Gruppe binden“	2–20

LDAP-Überblick

Die hier zur Verfügung gestellten Hintergrundinformationen dienen lediglich zur Erläuterung grundlegender Konzepte. Sie bieten jedoch keine Anleitungen zur Implementierung von LDAP oder Windows Active Directory. Bei den Informationen in diesem Handbuch wird davon ausgegangen, dass der Active Directory-Server bereits installiert ist und entweder durch einen Active Directory-Administrator oder einen LDAP-Administrator verwaltet wird. Die Beispiele in diesem Anhang beziehen sich auf Microsoft Windows 2000 Server mit Microsoft Internet Explorer (IE) Version 6.X.

LDAP (Lightweight Directory Access Protocol) ist eine verschlankte Alternative zum X.500 Directory Access Protocol (DAP). LDAP verwendet statt des beim X.500 erforderlichen OSI-Protokollpakets das TCP/IP-Protokollpaket. Als verschlankte Version vereinfacht LDAP einige Arbeitsschritte, bietet jedoch keine Unterstützung für einige X.500 DAP-Funktionen.

LDAP ist das zwischen einem Verzeichnis-Client und einem Server verwendete Protokoll. LDAP legt die zwischen einem LDAP-Client und einem LDAP-Server übertragenen Mitteilungsinhalte fest. Der LDAP-Client, in diesem Fall der DocuShare-Server, kommuniziert mit dem LDAP-Server. Der LDAP-Server fungiert als Gateway und greift auf das LDAP-Verzeichnis zu. Das LDAP-Verzeichnis kann entweder unabhängig auf dem LDAP-Server oder als Verzeichnis auf einem X.500-Server installiert werden.

DocuShare übermittelt Abfragen zu Verzeichnisinhalten an den LDAP-Server. Der LDAP-Server greift auf das Verzeichnis, entweder LDAP oder X.500, zu und übermittelt die Ergebnisse an DocuShare. Mithilfe des LDAP-Protokolls können Client-Funktionen für die Verzeichnisdaten gelesen und aktualisiert werden.

Hinweis: DocuShare aktualisiert die LDAP-Verzeichnisdaten nicht. DocuShare liest nur die Ergebnisse der an den LDAP-Server gesendeten Abfragen.

LDAP-Struktur

Die Einträge in einem LDAP-Verzeichnis sind in einer bestimmten hierarchischen Struktur angeordnet.

Verzeichnisse

Ein Verzeichnis ist eine bestimmte Art von Datenbank. Verzeichnisse sind für die Unterstützung einer großen Anzahl von **Lese**-Abfragen sowie des **Schreib**-Zugriffs optimiert, der normalerweise Systemadministratoren vorbehalten ist. Ähnlich wie die Seiten eines Telefonbuchs wird das LDAP-Verzeichnis öfter gelesen als aktualisiert.

Genau wie ein Telefonbuch Privatpersonen, Unternehmen und Organisationen aufführt, listet ein LDAP-Verzeichnis Objekte wie Benutzer, Server, Drucker usw. auf. So wie ein Telefonbuch Informationen zu den einzelnen Einträgen aufführt, wie beispielsweise Namen, Telefonnummern und Adressen, enthalten die Einträge in einem LDAP-Verzeichnis sachdienliche Informationen zu jedem Objekt. Diese Objektinformationen werden als **Attribute** bezeichnet.

Attribute

Jeder Objekteintrag in einem LDAP-Verzeichnis enthält ein oder mehrere Attribute. Jedes Attribut setzt sich aus einem **Typ** und einem **Wert** zusammen. Telefonbucheinträge verfügen über Attribute wie beispielsweise Name und Telefonnummer einer Person. LDAP-Attribute haben das Format **commonName=Jana Schmidt telephoneNumber=555-555-5555**. [Tabelle 1-1](#) enthält eine Auflistung einiger gängiger LDAP-Attribute zusammen mit dem jeweils zugeordneten Alias.

Tabelle 1-1:

LDAP-Attribut	Attribut-Alias	Beschreibung des Attributs	Beispiel
commonName	cn	Hauptname eines Eintrags	Jutta Dall
Surname	sn	Nachname der Person	Dall
userID	uid	Benutzer-ID oder Anmeldename	jdall
telephoneNumber	-	Telefonnummer	555-123-4567
organizationalUnitName	ou	Name der Organisationsabteilung	meine Abteilung
organization	o	Name der Organisation	meine Firma
domainComponent	dc	DNS-Komponente	xyz.com

Relative Distinguished Name

Der **RDN** (Relative Distinguished Name) wird durch ein **Attributdatenpaar** (Typ und Wert) dargestellt, wie beispielsweise:

cn=Jutta Dall

uid=Schmidt

ou=Marketing

dc=Xerox

Distinguished Name

Die Einträge im Verzeichnis werden durch einen definierten Namen (Distinguished Name; DN) organisiert. Der definierte Name entspricht in etwa dem absoluten Dateipfad unter Windows. Der DN eines Objekts setzt sich aus dem Namen und dem Pfad des Eintrags im Verzeichnis zusammen.

Ein DN setzt sich aus durch Kommata getrennten RDN-Attributdatenpaaren zusammen, wie beispielsweise:

cn=Jochen Schmidt,ou=Marketing,dc=Xerox,dc=com

cn=Jochen Schmidt,ou=Technik,dc=Xerox,dc=com

Bei der DN-Pfadangabe wird zuerst die unterste Ebene angegeben. Beim Dateisystem unter Windows wird zuerst die oberste Ebene angegeben. Im Dateisystem unter Windows können mehrere Dateien denselben Namen tragen, sofern sie in unterschiedlichen Verzeichnissen gespeichert sind, und genauso können mehrere Benutzer denselben RDN besitzen, sofern der DN eindeutig ist. Wie das oben angeführte DN-Beispiel zeigt, kann sowohl für die Marketing-Abteilung als auch für die Technikabteilung ein Jochen Schmidt aufgelistet sein.

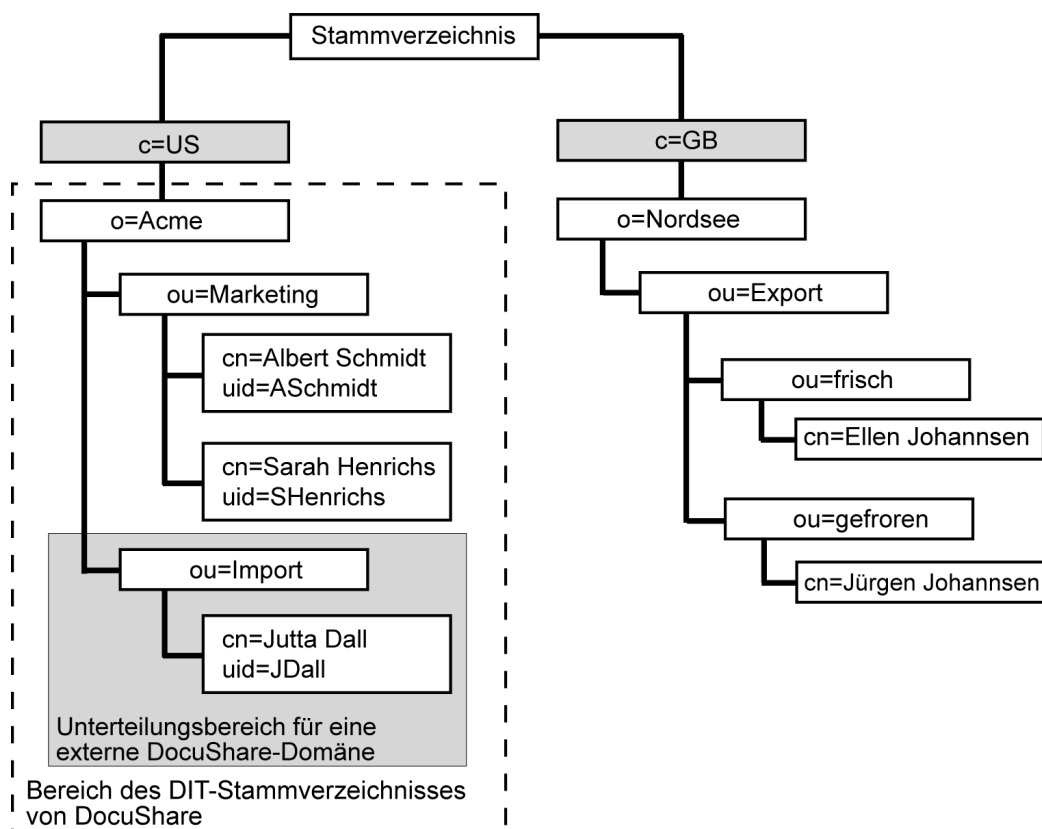
Directory Information Tree

Im Verzeichnis werden Einträge in einer hierarchischen baumähnlichen Struktur angeordnet, die als **Directory Information Tree** bzw. **DIT** bezeichnet wird. Ein DIT basiert auf dem definierten Namen der Einträge, wobei der DN in Zweige unterteilt wird, die üblicherweise geographische oder organisatorische Strukturen darstellen. Microsoft Active Directory wird oftmals anhand von geographischen Domänen oder DNS organisiert.

DIT-Organisation anhand von geographischen Domänen

In der nachfolgenden Abbildung wird dargestellt, wie der Administrator einer Importfirma für Fisch und Meeresfrüchte die LDAP-Verzeichnishierarchie anhand geographischer Gesichtspunkte organisieren könnte. Um einen DocuShare-Server für die US-amerikanische Firma Acme als Host einzurichten, definiert der Administrator das **DIT-Stammverzeichnis** als **o=Acme, c=US**.

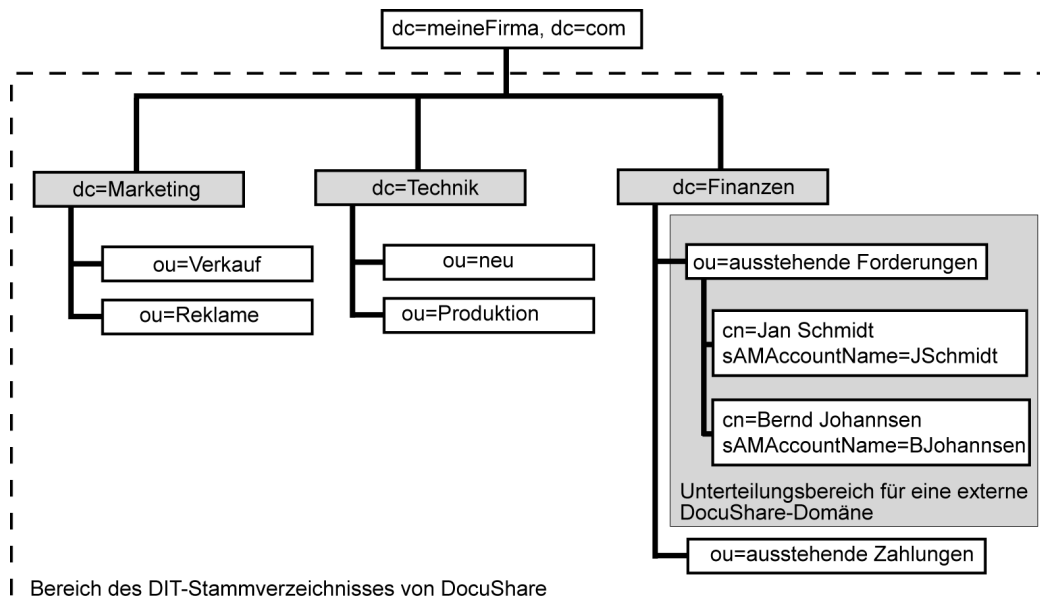
Um eine **externe Domäne** für die Importabteilung von Acme festzulegen, definiert der Administrator den relativen Authentifizierungslocator und den relativen Verzeichnisdienstlocator als **ou=Import**.



DIT-Organisation anhand von DNS

Die nachfolgende Abbildung stellt dar, wie der Administrator des Unternehmens die LDAP-Verzeichnishierarchie anhand von DNS organisieren könnte. Das Unternehmen verwendet in den Abteilungen Marketing, Technik und Finanzen Windows-Domänenserver. Indem das DIT-Stammverzeichnis als **dc=meineFirma, dc=com** definiert wird, kann der Administrator für jede Abteilung innerhalb eines Ressorts eine externe Domäne einrichten.

Um eine **externe Domäne** für die Abteilung des Ressorts Finanzen einzurichten, die sich um ausstehende Zahlungen kümmert, definiert der Administrator den relativen Authentifizierungslocator und den relativen Verzeichnisdienstlocator als **ou=ausstehende Forderungen, dc=Finanzen**.



DocuShare-Konfiguration

Melden Sie sich als Administrator bei Ihrer DocuShare-Site an, wenn Sie diese so konfigurieren möchten, dass LDAP/Active Directory verwendet wird, und führen Sie dann die Schritte A bis F aus. Konfigurieren Sie DocuShare korrekt über die **Active Directory-Verwaltung** oder den **LDIFDE**-Befehl für Active Directory, um die erforderlichen Informationen zu sammeln. Beide Verfahren zur Informationssammlung werden in diesem Kapitel beschrieben.

A: LDAP-Konfiguration

Verwenden Sie die DocuShare-Verwaltungsseite **LDAP-Konfiguration**, um eine Verbindung zwischen Ihrem DocuShare- und dem LDAP-Server herzustellen und den DIT festzulegen, der zum Einrichten externer DocuShare-Domänen verwendet werden soll.

1. Öffnen Sie die Seite **LDAP-Konfiguration** über die Befehle der Verwaltung.
2. Geben Sie in das Feld **Host(s)** entweder den Host-Namen, die IP-Adresse oder den DNS-Namen des LDAP/Active Directory-Servers ein (vorzugsweise FQDN oder IP-Adresse, sofern kein FQDN vorhanden ist). Fügen Sie bei mehreren LDAP-Serveradressen jeweils ein Leerzeichen zwischen den Einträgen ein.
3. Geben Sie in das Feld **Anschluss** die von Ihrem LDAP-Server verwendete Anschlussnummer ein, sofern diese vom Standardwert 389 abweicht.
4. **Optional:** Geben Sie in das Feld **SSL** die für Secure Socket Layer verwendete Anschlussnummer ein.
5. Geben Sie in das Feld **DIT-Stammverzeichnis** die Informationen ein, die Sie durch die Active Directory-Suche in Bezug auf „namingContext“ gefunden haben. Diese Informationen können folgendes Format haben:
dc=adoc,dc=Xerox,dc=com.
6. Geben Sie in das Feld **Benutzer-RDN-Schlüssel** das Attribut **cn** ein. Dies ist der Alias für das Attribut **commonName**. Das Attribut hängt vom verwendeten LDAP-Servertyp (iPlanet usw.) ab.
7. Wählen Sie im Feld **Systemagent** die Angabe **Agent** aus.
Die meisten Active Directory-Server erfordern eine Anmeldung entweder über ein Agenten- oder ein Dienstkonto.
8. Geben Sie in das Feld **DN** den definierten Namen des Agentenkontos ein.
Beispielsweise: **cn=Jochen,cn=Benutzer,dc=adoc,dc=xerox.**
9. Geben Sie in das Feld **Kennwort** das Kennwort für das Agentenkonto ein.

10. Wechseln Sie zum Abschnitt **LDAP-Verbindung testen** im unteren Bereich der Seite „LDAP-Konfiguration“.
Verwenden Sie **LDAP-Verbindung testen**, um zu prüfen, ob die Verbindung gültig und die Anmeldung beim LDAP-Server erfolgreich ist.
11. Wählen Sie im Feld **Verbindungs-DN** die Angabe **Agent** aus.
12. Geben Sie in das Feld **Name** den definierten Namen ein, den Sie in Schritt 8 in das Feld **DN** eingegeben haben.
13. Geben Sie in das Feld **Kennwort** das Kennwort ein, das Sie in Schritt 9 in das Feld **Kennwort** eingegeben haben.
14. Klicken Sie auf **Übernehmen und testen**.
Wenn Sie die Verbindung zum LDAP-Server korrekt eingerichtet haben, wird eine Erfolgsmeldung angezeigt.
15. Wiederholen Sie die Schritte 11 bis 14, wählen Sie jedoch im Feld **Verbindungs-DN** die Option **Benutzer** aus.

Hinweis: Bei diesem Test wird nicht die Gültigkeit des DIT-Stammverzeichnisses oder des relativen Authentifizierungslocators externer Domänen überprüft. Bei diesem Test wird lediglich überprüft, ob DocuShare eine positive Antwort vom LDAP-Server erhält.

B: Erweiterte Konfiguration

Legen Sie auf der Seite **Erweiterte LDAP-Konfiguration** fest, wie bestimmte Objektklassen auf Ihrem LDAP-Server definiert werden.

1. Klicken Sie unten auf der Seite „LDAP-Konfiguration“ auf die Option **Erweitert**.
Die Seite „Erweiterte LDAP-Konfiguration“ wird angezeigt.
2. Suchen Sie unten auf der Seite „Erweiterte LDAP-Konfiguration“ nach dem Abschnittstitel **Objektklassen**.
3. Ersetzen Sie im Feld **Benutzer** den Standardeintrag **person** durch das Wort **user** (in Kleinbuchstaben).
4. Ersetzen Sie im Feld **Statische Gruppe** den Standardeintrag **groupOfUniqueNames** durch das Wort **group** (in Kleinbuchstaben).
5. Klicken Sie auf **Übernehmen**.

C: LDAP-Provider aktivieren

Verwenden Sie die DocuShare-Verwaltungsseiten **Sicherheitsdienste** und **Verzeichnisdienste**, um sowohl die Sicherheits- als auch die Verzeichnis-Quelldienste für LDAP zu aktivieren. Dadurch können die Benutzer die externen LDAP-Domänen bei der Anmeldung aus der Dropdown-Liste für die Domänen auswählen.

1. Öffnen Sie die Seite **Sicherheitsdienste** über die Befehle der Verwaltung.
2. Aktivieren Sie auf der Seite „Sicherheitsdienste“ das Kontrollkästchen **LDAP**, um LDAP als Authentifizierungsquelle für alle externen Domänen zu aktivieren, und klicken Sie dann auf **Übernehmen**.
3. Öffnen Sie die Seite **Verzeichnisdienste** über die Befehle der Verwaltung.
4. Aktivieren Sie auf der Seite „Verzeichnisdienste“ das Kontrollkästchen **LDAP**, um LDAP als Authentifizierungsquelle für alle externen Domänen zu aktivieren, und klicken Sie dann auf **Übernehmen**.

D: Benutzer binden

Verwenden Sie die DocuShare-Verwaltungsseite **Benutzer binden**, um eine Zuordnung zwischen den DocuShare-Kontoeigenschaften und den LDAP-Kontoattributen herzustellen.

1. Öffnen Sie die Seite **Benutzer binden** über die Befehle der Verwaltung.
2. Geben Sie in das Feld **Vorname** das Attribut ein, das LDAP als Vornamen des Benutzers verwendet. Dies ist normalerweise **givenName**.
3. Geben Sie in das Feld **Nachname** das Attribut ein, das LDAP als Nachnamen des Benutzers verwendet. Dies ist normalerweise **surname** oder **sn**. Diese Angabe ist erforderlich.
4. Geben Sie in das Feld **Benutzername** das Attribut ein, das LDAP als Anmeldenamen des Benutzers verwendet. Dies ist normalerweise **sAMAccountName**. Diese Angabe ist erforderlich.
5. Wenn das LDAP-Verzeichnis zusätzliche Attribute enthält, wie beispielsweise E-Mail-Adressen, Postanschriften, Telefonnummern oder Homepage-Adressen, geben Sie diese Attribute in die jeweiligen Felder auf der Seite „Benutzer binden“ ein.
6. Klicken Sie auf **Übernehmen**, um diese Informationen zu speichern.

E: Gruppe binden

Verwenden Sie die DocuShare-Verwaltungsseite **Gruppe binden**, um eine Zuordnung zwischen den DocuShare-Kontoeigenschaften und den LDAP-Kontoattributen herzustellen.

1. Verwenden Sie die Informationen, die Sie mithilfe des LDIFDE-Befehls erhalten haben, und geben Sie diese Attribute in die entsprechenden Felder auf der Seite „Gruppe binden“ ein.

Weitere Informationen finden Sie weiter hinten in diesem Kapitel unter *LDIFDE-Befehl für Active Directory / Analyse des Inhalts der adexport.txt-Datei / E: Eigenschaften von „Gruppe binden“*.
2. Klicken Sie auf **Übernehmen**, um diese Informationen zu speichern.

F: Domäne einrichten

Verwenden Sie die DocuShare-Verwaltungsseite **Domänen**, um externe Domänen auf Ihrer lokalen DocuShare-Site einzurichten. Jede externe DocuShare-Domäne stellt einen Zweig im LDAP-Verzeichnisbaum dar. Jeder Zweig enthält eine Reihe von DocuShare-Benutzerkonten und -Gruppenkonten.

1. Öffnen Sie die Seite **Domänen** über die Befehle der Verwaltung.
2. Geben Sie in das Feld **Hinzufügen** den Namen der externen Domäne ein, die Sie zu Ihrer lokalen Site hinzufügen möchten.

Dies kann ganz einfach ein beschreibender Name sein, wie beispielsweise Technik.
3. Wählen Sie auf den Verwaltungsseiten unter „Dienstanbieter | Sicherheitsdienste“ und unter „Dienstanbieter | Verzeichnisdienste“ jeweils **LDAP** aus.

4. Geben Sie in das Feld **Relativer Authentifizierungs-Locator** ein bzw. mehrere Attributpaare ein, um den Pfad zu dem Verzeichnis zu definieren, das die Benutzer- und Gruppenkonten enthält.

Verwenden Sie die Attributkomponenten des DN, die sich links vom DIT-Stammverzeichnis und rechts vom Benutzer-RDN befinden.

Beispielsweise lautet der DN für ein Benutzerkonto in einer Domäne folgendermaßen:

cn=Benutzername,ou=Technik,ou=docushare,dc=adoc,dc=xerox,dc=com.

Die Technik-Domäne befindet sich unter dem Zweig **ou=Technik, ou=docushare**. Das DIT-Stammverzeichnis lautet **dc=adoc, dc=xerox, dc=com**.

5. Geben Sie in das Feld **Relativer Verzeichnisdienst-Locator** ein oder mehrere Attributpaare ein.

Geben Sie dieselben Attributpaare ein wie in das Feld **Relativer Authentifizierungs-Locator**.

DocuShare 6.5 unterstützt nur LDAP für Authentifizierungs- und Verzeichnisdienste; daher sind die Werte für „Relativer Authentifizierungs-Locator“ und „Relativer Verzeichnisdienst-Locator“ identisch.

6. Klicken Sie auf **Hinzufügen**, um diese externe Domäne zu Ihrem lokalen Anmeldemenü hinzuzufügen.

G: Hinzufügen

Nachdem Sie die Angaben auf den Seiten für die LDAP-Konfiguration, die Dienstanbieter, das Anbinden von Benutzern und die Domänen abgeschlossen haben, können Sie jetzt Benutzer- und Gruppenkonten zur externen Domäne Ihrer DocuShare-Site hinzufügen. Wenn Sie an dieser Stelle in der neuen externen Domäne die Funktion **Benutzer auflisten** bzw. **Gruppen auflisten** verwenden, ist die Domäne leer. Sie müssen jetzt die Domäne auf dem LDAP-Server öffnen und die Benutzer- bzw. Gruppenkonten auswählen, die Mitglieder der externen Domäne sein sollen.

1. Öffnen Sie die Seite **Hinzufügen** über die Befehle der Verwaltung.
Diese Seite entspricht nicht der Seite **Benutzer hinzufügen**.
2. Wählen Sie einen **Kontotyp** und eine externe **Domäne** aus.
3. Wählen Sie aus, wie die Liste der externen Domänenkonten gefiltert werden soll, und fügen Sie einen einfachen Filter z. B. auf Basis eines Namens, Namensteils oder einer bestimmten Objekteigenschaft hinzu.
4. Klicken Sie auf **Los**, um eine Liste der Kontotypen anzuzeigen, die Sie ausgewählt haben.
5. Wählen Sie die Konten aus, die an Ihrer Site lokal angezeigt werden sollen, und klicken Sie auf den Pfeil **Hinzufügen**, um diese in das Feld **Ausgewählt** zu übernehmen. Wenn Sie ein Konto nicht in das Feld „Ausgewählt“ übernehmen, wird der betreffende Benutzer oder die Gruppe vom Zugang zu Ihrer Site ausgeschlossen.
6. Zum Abschluss klicken Sie auf **Konten hinzufügen**. DocuShare übernimmt die Benutzer- oder Gruppenkonten der externen Domäne in die lokale Liste.
7. Auf der Seite **Benutzer auflisten/suchen/hinzufügen** können Sie die Benutzer anzeigen, die der neuen externen Domäne zugewiesen wurden.

H: Anmeldung anzeigen

1. Kehren Sie zur DocuShare-Homepage zurück.
2. Im Anmeldebereich der Startseite sollte die neue externe Domäne im Menü für die Anmeldedomäne angezeigt werden.
3. Die Benutzer externer Domänen müssen die jeweils richtige Domäne zur Anmeldung auswählen, andernfalls zeigt DocuShare eine Fehlermeldung sowie eine erneute Eingabeaufforderung an.

LDAP und SSL

SSL (*Secure Socket Layer*) ist ein von Netscape entwickeltes Protokoll zur Übertragung privater Dokumente über das Internet. SSL verwendet einen öffentlichen Schlüssel, um über SSL-Verbindungen übertragene Daten zu verschlüsseln. Sowohl Netscape Navigator als auch Internet Explorer unterstützen SSL. Viele Websites verwenden SSL für sensible Benutzerinformationen wie beispielsweise Kreditkartennummern oder Kontenkennwörter. SSL-Sitzungen werden durch URLs gestartet, die statt mit **http** mit **https** beginnen.

Zertifikate

Bei SSL verwenden Server und Clients Zertifikate als Identifikationsbeleg, bevor eine sichere Verbindung hergestellt wird. Zertifikate enthalten darüber hinaus öffentliche und private Schlüssel, die zum Erstellen einer Sitzung verwendet werden. Server und Clients verschlüsseln und entschlüsseln Daten mithilfe von Sitzungsschlüsseln.

Zertifikate können selbst-signiert sein oder von einer Zertifizierungsinstanz (*Certificate Authority*, CA) wie beispielsweise Entrust, Equifax, Valicert oder Verisign ausgegeben werden. Von CAs ausgegebene Zertifikate werden als Zertifikate **vertrauenswürdiger dritter Parteien** betrachtet. Im Grunde bürgen Zertifikate dritter Parteien für die Identität des Benutzers. Die meisten Client-Browser sind so konfiguriert, dass sie von CAs ausgegebene Zertifikate erkennen und diesen vertrauen.

Bei selbst-signierten Zertifikaten fungiert der Benutzer als Zertifizierungsinstanz. Selbst-signierte Zertifikate müssen im Autorisierungsspeicher des Browsers gespeichert werden. Diese Zertifikate werden nicht als von vertrauenswürdigen dritten Parteien ausgegeben betrachtet.

Zertifikate werden entweder als Client- oder als Serverzertifikate ausgegeben. DocuShare unterstützt keine client-seitigen Zertifikate. DocuShare verwendet eine Kopie des Zertifikats des LDAP-Servers, um eine SSL-Sitzung mit dem LDAP-Server herzustellen.

Zertifikate in DocuShare importieren

Je nachdem, welche CA das Zertifikat ausgegeben hat, muss der Administrator das Zertifikat unter Umständen vom LDAP-Server in den Zertifikatsspeicher des Webbrowsers des DocuShare-Servers importieren. Bei selbst-signierten Zertifikaten ist der Import des Zertifikats in den Zertifikatsspeicher des Webbrowsers des DocuShare-Servers **unbedingt erforderlich**.

So importieren Sie Zertifikate von bestimmten LDAP-Servern:

1. Öffnen Sie auf dem DocuShare-Server einen Webbrowser.
2. Stellen Sie über die Adresse `https://<ihr.Ldap.server>:636` eine Verbindung zum LDAP-Server her.
Anschluss 636 ist der Standardanschluss für SSL.
3. Wenn das Zertifikat nicht im Browser des DocuShare-Servers installiert wurde, wird eine Sicherheitsmeldung angezeigt, die Sie auffordert, das Zertifikat zu installieren.
4. Klicken Sie zum Installieren des Zertifikats auf **Zertifikat anzeigen** im unteren Bereich der Sicherheitsmeldung.
Es wird ein Zertifikatsfenster angezeigt.
5. Klicken Sie auf die Registerkarte **Details** und dann auf **In Datei kopieren**.

Zertifikate exportieren und als CER-Datei speichern

Nachdem Sie das Zertifikat vom LDAP-Server importiert haben, müssen Sie das Zertifikat in das DocuShare-Verzeichnis exportieren und als Zertifikatsdatei speichern.

So exportieren Sie das Zertifikat und speichern es als Zertifikatsdatei:

1. Klicken Sie im unteren Bereich des Assistentenfensters auf **Weiter**.
Wenn das Zertifikat einen privaten Schlüssel enthält, wird das Fenster **Privaten Schlüssel exportieren** angezeigt.
2. Wählen Sie im Fenster **Privaten Schlüssel exportieren** die Option **Nein, privaten Schlüssel nicht exportieren**.
DocuShare benötigt keinen privaten Schlüssel, um eine SSL-Sitzung mit dem LDAP-Server herzustellen.
3. Klicken Sie auf **Weiter**.
Das Fenster „Exportdateiformat“ wird angezeigt.
4. Wählen Sie im Fenster „Exportdateiformat“ die Option **Base-64-codiert X.509 (.CER)** aus.
5. Klicken Sie auf **Weiter**.
Das Fenster „Exportdatei“ wird angezeigt.
6. Geben Sie in das Feld **Dateiname** den Pfad zu dem Verzeichnis ein, in das Sie das Zertifikat exportieren möchten. Beispielsweise **D:**.
7. Geben Sie in das Feld **Dateiname** nach dem Verzeichnispfad einen Dateinamen für das Zertifikat mit der Dateierweiterung **.CER** ein. Beispielsweise: **D:\SSL_Cert4LDAP.CER**.
8. Klicken Sie auf **Weiter**, um den Export des Zertifikats abzuschließen.
Das Fenster „Fertigstellen des Assistenten“ wird angezeigt.
9. Klicken Sie auf **Fertig stellen**, um den Assistenten zu schließen.
Das LDAP-Zertifikat wird als .CER-Datei auf Ihrer DocuShare-Site gespeichert.
10. Befolgen Sie die Anweisungen auf der nächsten Seite unter **Zertifikate in DStTrustStore platzieren**.

Zertifikate in DStTrustStore platzieren

Nach dem Speichern des Zertifikats als Zertifikatsdatei müssen Sie diese in der Datei **DStTrustStore** platzieren.

So platzieren Sie die .CER-Zertifikatsdatei in die Datei **DStTrustStore**:

1. Suchen Sie mithilfe des Assistenten für den Zertifikatexport die exportierte .CER-Datei.
2. Kopieren Sie die .CER-Datei in das DocuShare-Verzeichnis, in dem die DStTrustStore-Datei **jdk1.5.0\jre\lib\security** enthalten ist.
3. Öffnen Sie ein Eingabeaufforderungsfenster, und navigieren Sie zu dem Verzeichnis, das **dstruststore** enthält.

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.
C:\>cd\xerox\docushare\jdk1.5.0\jre\lib\security
C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security\dir
Volume in drive C is Local Disk
Volume in Serial Number is 508B-0D2F
Verzeichnis C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security
18-11-02  15:55      <DIR>      -
18-11-02  15:55      <DIR>      --
02-10-02  12:25          7.365 cacerts
02-10-02  12:26          589 dstruststore
02-10-02  12:26          2.271 java.policy
02-10-02  12:26          4.115 java.security
10-11-02  15:43          844 SLL_Cert4LDAP.cer
          5 Files(s)      15,184 bytes
          2 Dir(s)  1,486,024,704 bytes free

C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security
```

4. Geben Sie bei Aufforderung den Befehl **set PATH** ein, um die Umgebungsvariable PATH festzulegen. Verwenden Sie **set PATH=%PATH%;<Ihr DocuShare-Verzeichnis>\jdk1.5.0\jre\bin**.

```
C:\Xerox\Docushare\jdk1.5.0\jre\lib\security>set
PATH=%PATH%;C:\XEROX\DocuShare\jdk1.5.0\jre\bin
```

5. Nachdem Sie die Variable PATH eingegeben haben, geben Sie **keytool** ohne Argumente in die Befehlszeile ein.
Das Keytool-Dienstprogramm wird angezeigt. Das Keytool-Dienstprogramm platziert das SSL-Zertifikat in **DSTrustStore**.
6. Geben Sie folgenden Keytool-Dienstprogrammbefehl in die Befehlszeile ein:
keytool -import -alias <alias_name> -file <cert_file> -keystore dstruststore
Ersetzen Sie **<alias_name>** durch einen eindeutigen Namen für die Zertifikatsdatei.
Ersetzen Sie **<cert_file>** durch den Namen der exportierten Zertifikatsdatei (.CER), die Sie in das Verzeichnis mit der Datei **dstruststore** kopiert haben.
7. Drücken Sie die Eingabetaste, um den Befehl auszuführen.
Sie werden nach einem Kennwort gefragt.
8. Geben Sie **password** ein, und drücken Sie die Eingabetaste.

```
C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security>keytool -import -alias Test LDAPss1 -file
SDL_Cert4LDAP.cer -keystore dstruststore
```

```
Enter keystore password: password
```

```
Owner: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
```

```
Issuer: OU=EFS File Encryption Certificate, L=EFS, CN=Administrator
```

```
Serial number: 5ee8abd44c2cd2b14ffbee159f03d354
```

```
Valid from: Tue Feb 19 10:57:21 PST 2002 until: Thu Jan 26 10:57:21 PST 2102
```

```
Certificate fingerprints:
```

```
MD5: 78:C7:A3:04:32:69:EB:97:76:FE:F4:8A:11:A2:65:26
```

```
SHA1: 02:DD:9A:BE:BE:DE:3C:AA:22:AE:14:9A:F2:F2:5B:11:61:6D:5A:5F
```

```
Trust this certificate? [no]: yes
```

```
Certificate was added to keystore
```

```
C:\Xerox\DocuShare\jdk1.5.0\jre\lib\security>
```

9. Überprüfen Sie die Angaben auf dem Bildschirm, um sicherzustellen, dass Keytool das Zertifikat erfolgreich zum Schlüsselspeicher hinzugefügt hat. Wenn Keytool diesen Vorgang erfolgreich ausgeführt hat, kann Ihr DocuShare-Server das Zertifikat jetzt verwenden, um eine SSL-Sitzung mit dem LDAP-Server herzustellen.
10. Führen Sie nach abgeschlossenem Import des Zertifikats einen Neustart des DocuShare-Servers durch.

Active Directory-Verwaltung

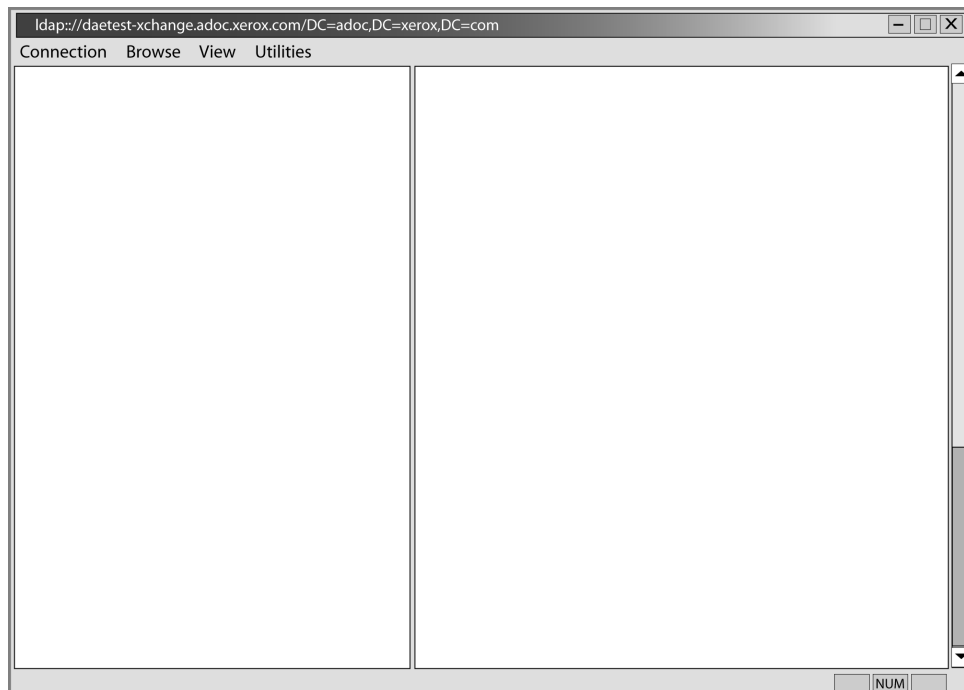
Sie können mit der Active Directory-Verwaltung (ldp.exe) verschiedene Arbeitsschritte an Active Directory durchführen und Abfragen an den LDAP-Verzeichnisserver senden.

Bei Verwendung von ldp.exe zur Herstellung der Verbindung mit einem LDAP-Server mit aktiviertem SSL müssen Sie zunächst das SSL-Zertifikat auf Ihrem DocuShare-Server aktivieren. Zum Importieren und Laden eines SSL-Zertifikats befolgen Sie die Anweisungen unter **LDAP und SSL** in *Kapitel 2* des vorliegenden Handbuchs.

So installieren und verwenden Sie die Active Directory-Verwaltung zur Konfiguration Ihrer DocuShare-Site:

1. Legen Sie den Datenträger mit der Server-Software für Windows 2000 ein, suchen Sie die Datei **sreadme.doc** und lesen Sie diese aufmerksam durch.
2. Suchen Sie die Datei **setup.exe** im Verzeichnis „Support\Tools“.
3. Klicken Sie auf die Datei **setup.exe**, um die Installation der Datei „ldp.exe“ zu starten.
4. Befolgen Sie die auf dem Bildschirm angezeigten Anweisungen, um **ldp.exe** zu installieren.
5. Klicken Sie nach Abschluss der Installation im Windows-Startmenü auf **Active Directory-Verwaltung**.

Hierdurch wird „ldp.exe“ gestartet und die Active Directory-Verwaltung wird angezeigt. Die Verwaltung verfügt über eine Navigationsleiste mit Befehlen sowie einen linken und rechten Fensterbereich, in dem Informationen angezeigt werden.



Active Directory-Verwaltung verwenden

Sie können die Active Directory-Verwaltung zum Sammeln von Informationen zu Ihrem LDAP-Server verwenden. Diese Informationen benötigen Sie, um Ihre DocuShare-Site so zu konfigurieren, dass sie den Server für externe Domänen verwendet. Befolgen Sie die Anweisungen in den Schritten A bis F.

Hinweis: Dieses Verfahren basiert auf der Verwendung der Verwaltung zum Sammeln von Informationen aus einer LDAP-Server-Standardinstallation. Je nach Konfiguration des Servers können Abweichungen auftreten.

A: Verbinden

1. Wählen Sie in der Navigationsleiste der Active Directory-Verwaltung **Verbindung** aus, und wählen Sie dann im Menü „Verbindung“ die Option **Verbinden** aus.

Das Dialogfeld „Verbinden“ wird angezeigt.

2. Geben Sie in das Feld **Server** entweder die IP-Adresse oder den DNS-Namen des LDAP Active Directory-Servers ein.
3. Geben Sie in das Feld **Anschluss** die verwendete Anschlussnummer ein, sofern diese vom angezeigten Standard abweicht.
4. Klicken Sie auf **OK**.

Sie haben jetzt die LDAP-Serveradresse und die Anschlussnummer eingestellt.

B: Anbinden

Nachdem Sie die Verbindung zum LDAP-Server eingerichtet haben, müssen Sie den Server jetzt an ein Administratorkonto binden, das zum Suchen im Verzeichnis berechtigt ist.

1. Wählen Sie in der Navigationsleiste der Active Directory-Verwaltung **Verbindung** aus, und wählen Sie im Menü „Verbindung“ die Option **Binden** aus.

Das Dialogfeld „Binden“ wird angezeigt.

2. Geben Sie in das Feld **Benutzer** den Namen des Benutzerkontos, in das Feld **Kennwort** das entsprechende Kennwort und in das Feld **Domäne** die Domäne ein.
3. Klicken Sie auf **OK**.

Wenn Sie erfolgreich eine Verbindung und eine Anbindung für den LDAP-Server erstellt haben, zeigt der Server **Antworttext im rechten Fensterbereich** der Active Directory-Verwaltung an.

C: Stamm-DN suchen

Der Stamm-DN ist der Ausgangspunkt für Ihre Suche im Verzeichnisbaum.

1. Durchsuchen Sie den Antworttext im rechten Fensterbereich der Active Directory-Verwaltung nach einem Verweis auf **namingContext**.

Das Format von **namingContext** richtet sich nach dem verwendeten LDAP-Server.

2. Der markierte Text ist der Stamm-DN für den DIT.

Beispielsweise könnte der markierte Stamm-DN Folgendes sein:

dc=adoc,dc=Xerox,dc=com. Ihr tatsächlicher Stamm-DN hängt von der individuellen Struktur Ihres LDAP-Verzeichnisbaums ab. Notieren Sie sich diese Informationen zur späteren Referenz.

D: Directory Information Tree anzeigen

1. Wählen Sie in der Navigationsleiste der Active Directory-Verwaltung **Anzeigen** und anschließend im Menü „Anzeigen“ die Option **Struktur** aus.

Das Dialogfeld „Strukturansicht“ wird angezeigt.

2. Geben Sie in das Feld **Basis-DN** den mithilfe der oben erwähnten namingContext-Suche gefundenen Stamm-DN ein.
3. Klicken Sie auf **OK**.

Der DIT für Ihren LDAP-Server wird im linken Fensterbereich der Active Directory-Verwaltung angezeigt.

4. Sehen Sie sich die Baumstruktur genau an, um festzustellen, wo sich das DIT-Stammverzeichnis für neu einzurichtende externe DocuShare-Domänen befindet.

Das Stammverzeichnis sollte sich an einer der oberen Positionen in der Hierarchie befinden, sodass es alle der Zweige (beispielsweise „organizationUnit“ und „domainComponents“) einschließt, die auf den DocuShare-Server zugreifen können.

Für unser Beispiel verwenden wir **dc=adoc, dc=xerox,dc=com** als DIT-Stammverzeichnis, da wir nur die Benutzer in der ADOC-Domäne einschließen möchten und nicht alle Benutzer von Xerox.com.

E: Agentenkonto suchen

In den meisten Fällen akzeptiert Active Directory keine anonymen Abfragen an das Verzeichnis. Für Abfragen vom Server ist entweder ein Agenten- oder Dienstkonto erforderlich. Verwenden Sie den Suchbefehl, um nach dem DN des Agentenkontos zu suchen.

1. Wählen Sie in der Navigationsleiste der Active Directory-Verwaltung **Durchsuchen** und anschließend im angezeigten Menü die Option **Suchen** aus.

Das Dialogfeld „Suchen“ wird angezeigt.

2. Geben Sie in das Feld **Basis-DN** einen Stamm-DN ein.

Je nachdem, welcher Wert als Stamm-DN verwendet wird und an welcher Position sich das Agentenkonto in der Hierarchie befindet, müssen Sie unter Umständen die Option **Unterstruktur** auswählen, um den Suchbereich zu erweitern.

3. Geben Sie einen Filter in das Feld **Filter** ein.

Hier wurde das Attribut „sAMAccountName“ als Filter verwendet, da uns der AnmeldeName für das Agentenkonto bekannt war. Dieses Attribut ist in Active Directory eindeutig und wurde von Windows NT übernommen. Wäre uns der „commonName“ („cn“) des Kontos bekannt gewesen, hätten wir beispielsweise „commonName=Peter Pan“ verwenden können. iPlanet-Server verwenden entweder das Attribut „uid“ oder „commonName“ („cn“).

4. Bestimmen Sie den **Suchbereich**.

Legen Sie unter **Unterstruktur** fest, dass **Eine Ebene** nicht weitreichend genug ist.

5. Klicken Sie auf **Ausführen**.

Die Suchergebnisse werden als Text im rechten Fensterbereich der Active Directory-Verwaltung angezeigt. Ein Suchergebnis kann beispielsweise zeigen, dass der **distinguishedName** für das Agentenkonto „cn=TestUser1,cn=users,dc=adoc,dc=xerox,dc=com“ lautet.

F: Nächster Schritt

Nachdem Sie die Schritte A bis E ausgeführt haben, sollten Sie die Active Directory-Verwaltung zum Sammeln von Informationen verwenden können. Diese Informationen benötigen Sie, um Ihre DocuShare-Site so zu konfigurieren, dass für die Benutzerkonto-Authentifizierung LDAP verwendet wird.

- die IP-Adresse bzw. den DNS-Namen des LDAP-Servers
- das DIT-Stammverzeichnis
- das Agentenkonto für DocuShare

LDIFDE-Befehl für Active Directory

Wenn Ihr LDAP-Server unter Windows 2000 oder Windows 2003 ausgeführt wird, können Sie den Befehl **LDIFDE** verwenden, um den Inhalt des gesamten LDAP-Verzeichnisses oder eine bestimmte Domäne innerhalb des LDAP-Verzeichnisses in eine Textdatei zu schreiben. Diese Textdatei enthält fast alle Informationen, die für die Konfiguration von DocuShare zur Verwendung mit LDAP erforderlich sind.

Bei der vom LDIFDE-Befehl erstellten Datei handelt es sich um die primäre Datei, die vom DocuShare-Support zur Fehlerbehebung bei LDAP-Konfigurationsproblemen verwendet wird.



Ressourcen: Weitere Informationen zur Verwendung des LDIFDE-Befehls finden Sie auf der Website unter <http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q237/6/77.ASP&NoWebContent=1>

Syntax und Verwendung des LDIFDE-Befehls

Um den LDIFDE-Befehl zu verwenden, öffnen Sie ein Eingabeaufforderungsfenster auf Ihrem LDAP-Server und geben Sie **C:\Windows\system32>ldifde -?** ein. Drücken Sie anschließend die Eingabetaste. Der LDIFDE-Befehl gibt die folgenden Parameter wieder:

LDIF Directory Exchange

General Parameters

=====

```
-i          Turn on Import Mode (The default is Export)
-f filename Input or Output filename
-s servername The server to bind to (Default to DC of logged in Domain)
-c FromDN ToDN Replace occurrences of FromDN to ToDN
-v          Turn on Verbose Mode
-j          Log File Location
-t          Port Number (default = 389)
-u          Use Unicode format
-?          Help
```

Export Specific

=====

```
-d RootDN      The root of the LDAP search (Default to Naming Context)
-r Filter      LDAP search filter (Default to "(objectClass=*)")
-p SearchScope Search Scope (Base/OneLevel/Subtree)
-l list        List of attributes (comma separated) to look for in an LDAP search
-o list        List of attributes (comma separated) to omit from input.
-g            Disable Paged Search.
-m            Enable the SAM logic on export.
-n            Do not export binary values
```

Import

=====

```
-k          The import will go on ignoring 'Constraint Violation' and 'Object
Already Exists' errors
-y          The import will use lazy commit for better performance
```

Credentials Establishment

=====

Note that if no credentials is specified, LDIFDE will bind as the currently logged on user, using SSPI.

```
-a UserDN [Password | *]      Simple authentication
-b UserName Domain [Password | *] SSPI bind method
Example: Simple import of current domain
ldifde -i -f INPUT.LDF
```

```
Example: Simple export of current domain
ldifde -f OUTPUT.LDF
```

Example: Export of specific domain with credentials

```
ldifde -m -f OUTPUT.LDF
-b USERNAME DOMAINNAME *
-s SERVERNAME
-d "cn=users,DC=DOMAINNAME,DC=Microsoft,DC=Com"
-r "(objectClass=user)"
```

Beispiel zum LDIFDE-Befehl

Im folgenden Abschnitt wird ein Beispiel für einen LDIFDE-Befehl dargestellt, mit dem der Inhalt von Active Directory auf dem Server „Corvette“ in die Datei **adexport.txt** geschrieben wird.

Ausführen des LDIFDE-Befehls

Geben Sie den Befehl **C:\Windows\system32\LDIFDE.exe -f adexport.txt -s corvette** ein, und drücken Sie die Eingabetaste.

Der Befehl wird ausgeführt. Im Folgenden wird sein Verlauf dargestellt:

```
Connecting to "corvette"
Logging in as current user using SSPI
Exporting directory to file adexport.txt
Searching for entries...
Writing out entries.....
.....
132 entries exported

The command has completed successfully

C:\Documents and Settings\Administrator>LDIFDE -f adexport.txt -s corvette
Connecting to "corvette"
Logging in as current user using SSPI
Exporting directory to file adexport.txt
Searching for entries...
Writing out entries.....
.....
132 entries exported

The command has completed successfully
```

Die erzeugte adexport.txt-Datei

Im Folgenden wird der Inhalt der adexport.txt-Datei gezeigt, die in unserem Beispiel vom LDIFDE-Befehl erzeugt wurde. In diesem Beispiel wird allerdings nur ein bestimmter Teil des Gesamtinhalts dargestellt. Beachten Sie besonders die **fett** formatierten Elemente; diese Elemente müssen Sie für DocuShare konfigurieren, damit der betreffende LDAP-Server verwendet wird.

```
dn: DC=infodev,DC=dsbu,DC=xerox,DC=com
changetype: add
masteredBy: CN=NTDS Settings, CN=CORVETTE, CN=Servers, CN=infodev-dsbu-site,
CN= Sites, CN=Configuration, DC=infodev, DC=dsbu, DC=xerox, DC=com
auditingPolicy:: AAE=
creationTime: 127199619543431088
dc: infodev
forceLogoff: -9223372036854775808
fSMORoleOwner: CN=NTDS Settings, CN=CORVETTE, CN=Servers, CN=infodev-dsbu-
site, CN= Sites, CN=Configuration, DC=infodev, DC=dsbu, DC=xerox, DC=com
•
•
•
•
[Sample Directory Record for a single User]
dn: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox,
DC=com
changetype: add
accountExpires: 9223372036854775807
badPasswordTime: 0
badPwdCount: 0
codePage: 0
cn: Duncan Donkey
countryCode: 0
displayName: Duncan Donkey
mail: ddonkey@infodev.xerox.com
givenName: Duncan
instanceType: 4
lastLogoff: 0
lastLogon: 0
logonCount: 0
distinguishedName: CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev,
DC=dsbu, DC=xerox, DC=com
objectCategory: CN=Person, CN=Schema, CN=Configuration, DC=infodev, DC=dsbu,
DC=xerox, DC=com
objectClass: user
objectGUID:: xmi02W78IEmpYca7AtiupQ==
objectSid:: AQUAAAAAAAAUVAaAqDfWZRUIr0f4n7R0bgQAAA==
primaryGroupID: 513
pwdLastSet: 127293917905389760
name: Duncan Donkey
sAMAccountName: duncan
sAMAccountType: 805306368
sn: Donkey
userAccountControl: 512
userPrincipalName: duncan@infodev.dsbu.xerox.com
uSNChanged: 7353
uSNCreated: 7349
whenChanged: 20040518220950.0Z
whenCreated: 20040518220933.0Z
•
•
•
```

Fortsetzung der Textdatei...

[Sample Directory Record for a Group]

dn: CN=labusers,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
changetype: add
member: CN=Greg Wong,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Janet Gilmore,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Jennings\, Ferris,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
member: CN=Cua\, Kiam T,CN=Users,DC=infodev,DC=dsbu,DC=xerox,DC=com
info: Authorized Login User to the InforDev Lab
cn: labusers
description: InfoDev Lab Users
groupType: -2147483644
instanceType: 4
distinguishedName:CN=labusers, CN=Users, DC=infodev, DC=dsbu, DC=xerox,
DC=com
objectCategory: CN=Group, CN=Schema, CN=Configuration, DC=infodev, DC=dsbu,
DC=xerox, DC=com
objectClass: group
objectGUID:: Cm9phZkOn0ig4iEWMRPWsg==
objectSid:: AQUAAAAAAAAUVAAAAqDfWZRUIr0f4n7R0VgQAAA==
name: labusers
sAMAccountName: labusers
sAMAccountType: 536870912
uSNChanged: 3975
uSNCreated: 2540
whenChanged: 20040302161513.0Z
whenCreated: 20040130190128.0Z

Analyse des Inhalts der adexport.txt-Datei

Bei unserer adexport.txt-Beispieldatei wird der Distinguished Name (DN) für Duncan Donkey verwendet, bei dem es sich um ein Mitglied des Digital Actors-Teams in der InfoDev-Abteilung von DSBU bei der Xerox Corporation handelt.

In unserem Beispiel ist der DN für Duncan Donkey folgendermaßen definiert:

CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com

Wenn Sie den Distinguished Name eines Benutzers genauer untersuchen, erhalten Sie die für die Identifizierung folgender Angaben erforderlichen Informationen:

- a. DIT-Stammverzeichnis (Directory Information Tree)
- b. Benutzer-RDN-Schlüssel
- c. Relative Authentifizierungs- und Verzeichnisdienstlocatoren
- d. Attribute von „Benutzer binden“
- e. Attribute von „Gruppe binden“

A: DIT-Stammverzeichnis (Directory Information Tree)

Legen Sie das DIT-Stammverzeichnis auf der Ebene der Verzeichnisstruktur fest, die alle Zweige des Verzeichnisses mit den Benutzern enthält, für die der Zugriff auf den DocuShare-Server erforderlich ist. In unserem Beispiel haben nur Mitglieder der DSBU-Organisation bei Xerox auf unseren exemplarischen DocuShare-Server Zugriff.

Die DSBU-Organisation umfasst mehrere Abteilungen und Teams innerhalb der einzelnen Abteilungen. Diese Abteilungen und Teams sind im LDAP-Verzeichnis nach DCs (Domain Components; Domänenkomponenten) und OUs (Organizational Units; Organisationseinheiten) organisiert. In unserem Beispiel richten wir eine externe Domäne in DocuShare ein, um Benutzer zu authentifizieren, die Mitglied des Digital Actors-Teams in der InfoDev-Abteilung von DSBU bei der Xerox Corporation sind.

In unserem Beispiel wird das DIT-Stammverzeichnis des DN für Duncan Donkey hier in Fettschrift dargestellt: **CN=Duncan Donkey, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com**

Wenn Sie das DIT-Stammverzeichnis auf dieser Hierarchieebene definieren, können externe Domänen für die einzelnen Abteilungen bzw. Teams innerhalb von DSBU erstellt werden.

B: Benutzer-RDN-Schlüssel

Der Benutzer-RDN-Schlüssel ist der für die Identifizierung des Benutzers verwendete Attribut-Alias.

In unserem Beispiel wird der Benutzer-RDN-Schlüssel des DN für Duncan Donkey hier fett formatiert angezeigt: **CN=Duncan Donkey**, OU=Digital, OU=Actors, DC=infodev, DC=dsbu, DC=xerox, DC=com

C: Relative Authentifizierungs- und Verzeichnisdienstlocatoren

Die relativen Authentifizierungs- und Verzeichnisdienstlocatoren zeigen zum Verzeichniszweig der externen Domäne, in der bestimmte Benutzer oder Gruppen enthalten sind.

In unserem Beispiel wird der relative Authentifizierungs- und Verzeichnisdienstlocator hier fett formatiert angezeigt: CN=Duncan Donkey, **OU=Digital, OU=Actors, DC=infodev**, DC=dsbu, DC=xerox, DC=com.

D: Attribute von „Benutzer binden“

Die vom FDIFDE-Befehl erzeugte Textdatei enthält die Attribut-Aliasangaben, mit denen der Nachname, Benutzername und die E-Mail-Adresse der aufgeführten Benutzer identifiziert werden. Verwenden Sie diese Attribut-Aliasangaben, um die DocuShare-LDAP-Eigenschaften von **Benutzer binden** zu konfigurieren. In der vom FDIFDE-Befehl erzeugten Textdatei werden Benutzer innerhalb des LDAP-Verzeichnisses mit dem Eintrag **objectClass: user** identifiziert.

In unserem Beispiel finden Sie die **LDAP-Attribut-Aliasangaben** für die folgenden Eigenschaften:

Nachname = **sn**

Benutzername = **sAMAccountName**

E-Mail-Adresse = **mail**

In unserem Beispiel gelten die folgenden Werte für die betreffenden LDAP-Attribut-Aliasangaben:

sn: Donkey

sAMAccountName: duncan

mail: ddonkey@infodev.xerox.com

E: Attribute von „Gruppe binden“

Die vom FDIFDE-Befehl erzeugte Textdatei enthält die Attribut-Aliasangaben, mit denen Titel, Beschreibung und Zusammenfassung der einzelnen Gruppen aufgelistet werden. Verwenden Sie diese Attribut-Aliasangaben, um die DocuShare-LDAP-Eigenschaften von **Gruppe binden** zu konfigurieren.

In der vom FDIFDE-Befehl erzeugten Textdatei werden Gruppen innerhalb des LDAP-Verzeichnisses mit dem Eintrag **objectClass: group** identifiziert.

In unserem Beispiel finden Sie die **LDAP-Attribut-Aliasangaben** für die folgenden Eigenschaften:

Titel = **cn**

Beschreibung = **description**

Zusammenfassung = **info**

In unserem Beispiel gelten die folgenden Werte für die betreffenden LDAP-Attribut-Aliasangaben:

cn: labusers

description: InfoDev Lab Users

info: Authorized Login User to the InfoDev Lab

