



Army Knowledge Online (AKO)

AKO Directory Services

Interface Control Document

Version 4.2

22 January 2003

Contents

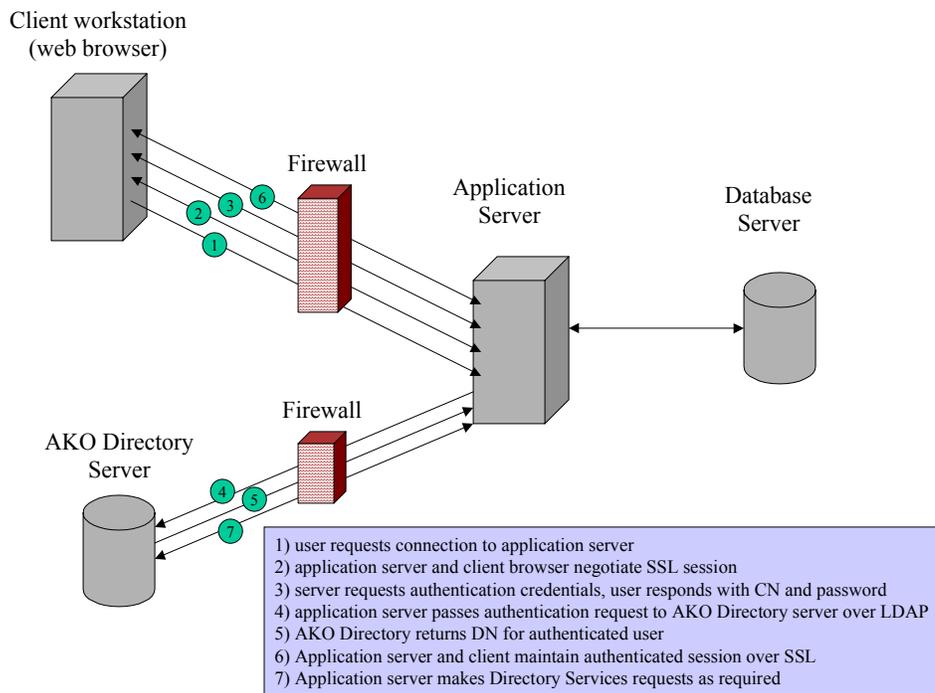
1	INTRODUCTION.....	1
2	DIRECTORY STRUCTURE AND CONTENT	2
2.1	DIRECTORY LOCATION.....	2
2.2	DIRECTORY TREE.....	2
2.3	ARMYPERSON SCHEMA	2
3	SECURITY.....	3
3.1	SECURE LDAP.....	3
3.2	AUTHENTICATED ACCESS TO THE AKO DIRECTORY SERVER	3
3.3	SSL.....	3
3.4	FIREWALL CONFIGURATIONS	3
4	CONNECTION TO THE AKO DIRECTORY SERVER.....	4
4.1	CONNECT USING IPLANET WEB SERVER 4.1	4
4.2	CONNECT USING IPLANET WEB SERVER 6.X	10
4.3	CONNECT USING MICROSOFT INTERNET INFORMATION SERVER (IIS).....	20
4.4	CONNECT USING LOTUS DOMINO	33
4.5	CONNECT USING SILVERSTREAM 4.7.....	38
4.6	CONNECT USING APACHE 1.3.14	44
4.7	CONNECT USING BEA WEBLOGIC	45
4.8	CONNECT USING ATG DYNAMO	48
4.9	CONNECT USING COGNOS.....	49
4.10	CONNECT USING COLDFUSION	49
4.11	CONNECT USING XEROX DOCUSHARE 2.X	50
4.12	CONNECT USING XEROX DOCUSHARE 3.X	58
4.13	CONNECT USING NETEGRITY SITEMINDER FOR SINGLE SIGN-ON	65
4.14	INSTALLING AND CONFIGURING THE SSO WEB AGENT ON WINDOWS AND IIS. 67	
4.15	INSTALLING AND CONFIGURING THE SSO WEB AGENT ON UNIX.....	107
4.16	INSTALLING AND CONFIGURING THE SSO WEB AGENT ON DOMINO	109
5	ARMYPERSON SCHEMA	112
5.1	ATTRIBUTE NAMES AND DEFINITION.....	112
5.2	ACCOUNT TYPES.....	117
5.3	BRANCH CODES	119
5.4	CINC.....	121
5.5	HQDA FUNCTIONAL AREA	122
5.6	LOCATION.....	123
5.7	MACOM.....	124
5.8	MOS / CAREER FIELDS	125
5.9	RANK.....	135

1 INTRODUCTION

Directory services functionality includes user authentication and user attribute lookup for attributes such as e-mail address, first and last name, and SSN. The Army is migrating to a centralized Enterprise Directory to support single point of entry for all users and all applications. By leveraging this existing AKO Army Enterprise Directory, applications will not duplicate the effort of registering, validating, and maintaining user ids and passwords, and the end users will benefit from having a single user id and password that works at all applications across the Army enterprise.

The AKO Directory provides Enterprise Directory Services for Army web applications. Directory services include user authentication, currently via userid and password, and user attribute lookup for unrestricted attributes such as e-mail address, first name (GIVENNAME) and last name (SN). The AKO Directory also provides secured access for lookup of restricted user attributes such as SSN.

Authentication is negotiated between the client and the application server, with referrals to the Directory Services server to validate the user's credentials. The session is maintained by the application server and the client – the Directory server is not "in the loop". The Web server maintains session information (either using an explicit sessions key, or using the SSL session key) for the duration of the session. Additional Directory Services requests can be made by the application server to obtain user attributes from the Directory Server.



To request credentials for your server to interface to the AKO Directory Server, complete the request form located at:

https://www.us.army.mil/portal/jhtml/reference/request_index.jhtml

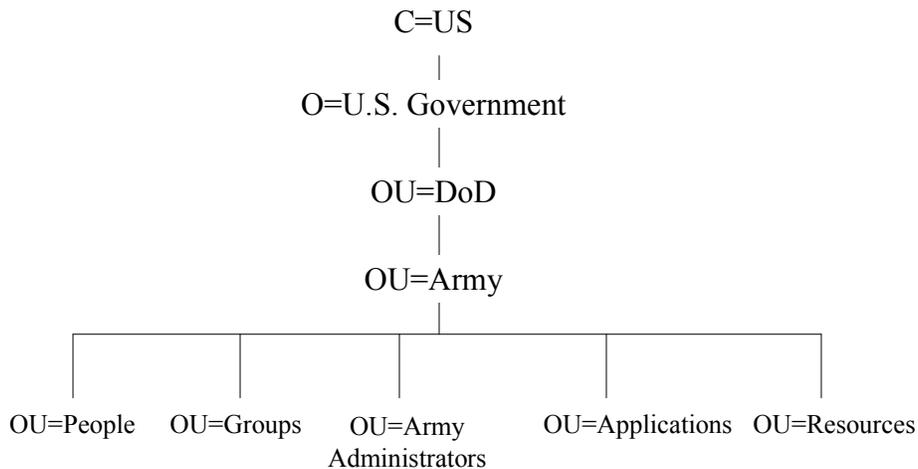
2 DIRECTORY STRUCTURE AND CONTENT

2.1 Directory location

The Production AKO Directory Server run the iPlanet 5.x Directory Server. It can be found at the DNS location of:

directory.us.army.mil

2.2 Directory Tree



The form of the fully qualified distinguished name of a person entry is:

CN=first.last,OU=People,OU=Army,OU=DoD,O=U.S. Government,C=US

The form of the fully distinguished name of a group is:

name=group_name,OU=Groups,OU=Army,OU=DoD,O=U.S. Government,C=US

2.3 ArmyPerson Schema

The ArmyPerson schema is included in the appendix. Access to the data elements (attributes) is restricted to authenticated applications only. "Default" access (i.e., those attributes that any authenticated application may access) allows the application to "read" many of the person entry attributes, including Common Name, Rank, e-mail address, and to "compare" hashed passwords for user authentication. For those applications that require access to sensitive attributes, a Memorandum of Agreement must be completed justifying the need. Example attributes and needs include access to the armySSN attribute for Personnel Applications, where SSN is used as the database key in the Personnel System.

3 SECURITY

3.1 Secure LDAP

Connection to the AKO Directory Server is available via secure LDAPS (Port 636). Access using unencrypted LDAP (Port 389) is not available. The signed certificates required to establish an encrypted session are posted in the AKO Portal, Army Knowledge Collaboration Center, in the folder:

Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) /
AKO Interface Control Document/Certificates

3.2 Authenticated access to the AKO Directory Server

Anonymous access to the AKO Directory Server is not allowed. All Application Servers must authenticate at the server-to-server level with the AKO Directory Server in order to process any LDAP transaction. The "default" access for authenticated Application Servers will allow reading of unrestricted fields. Applications can request and be granted access to read restricted fields as required.

The form of the fully qualified distinguished name of the server is:

CN=serverid,OU=Army Administrators,OU=Army,OU=DoD,O=U.S. Government,C=US

To request a ServerID for an Application Server, complete the request form:

https://www.us.army.mil/portal/jhtml/reference/request_index.jhtml

3.3 SSL

The web Application Server shall initiate an SSL session upon initial connection with the Client. The Client / Application Server authentication transaction shall take place AFTER the SSL session has been negotiated.

3.4 Firewall configurations

Firewalls should be configured to pass only those ports needed for all users. For specific exceptions, ports should be opened on an IP – to – IP address basis. Contact your DOIM or IMO about your facility's firewalls. To enable an LDAP connection to AKO, firewalls must be opened for *requests* FROM the Web / Application Server TO the AKO Directory Server, and for *responses* FROM the AKO Directory Server TO the Web / Application Server for **Port 636** (secure LDAP).

For Single Sign-On implementation, firewalls must be opened for *requests* FROM the Web Server TO the AKO Policy Servers, and for *responses* FROM the AKO Policy Servers TO the Web Server.

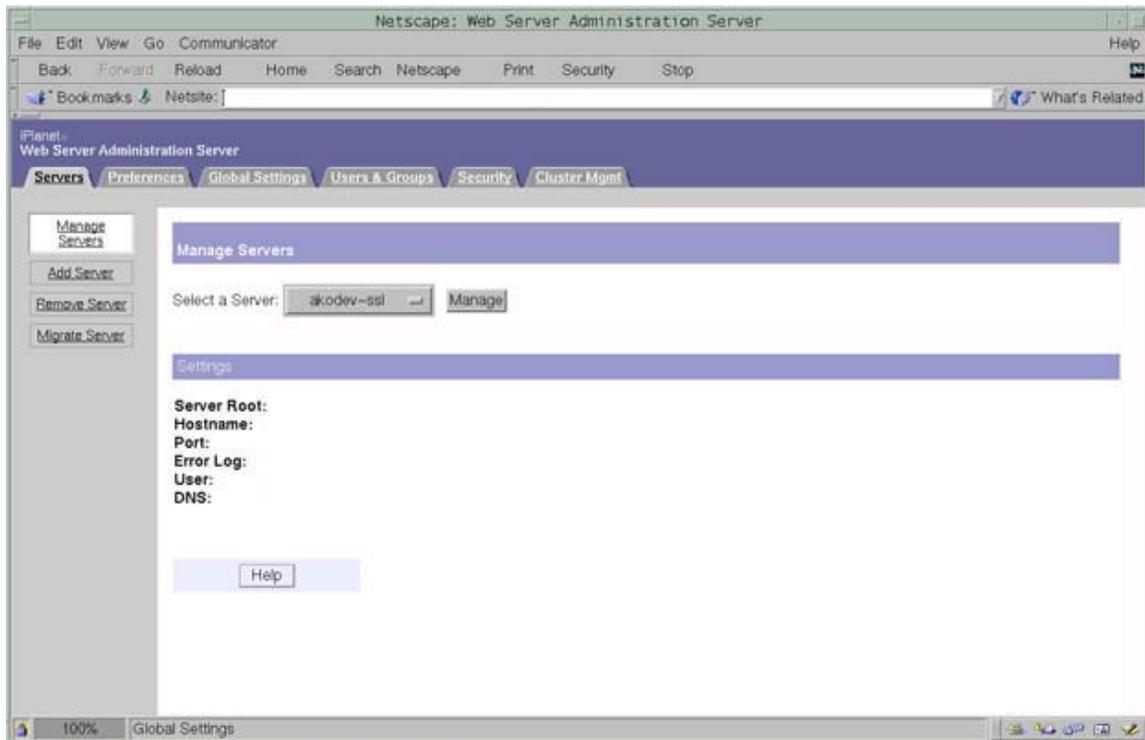
- The IP addresses are: 140.183.234.247, 140.183.234.107, 140.183.234.158
- The TCP Ports are: **44441,44442, 44443**.

Note that some operating systems (especially LINUX) install their own firewall – these will also need to be configured as above or disabled.

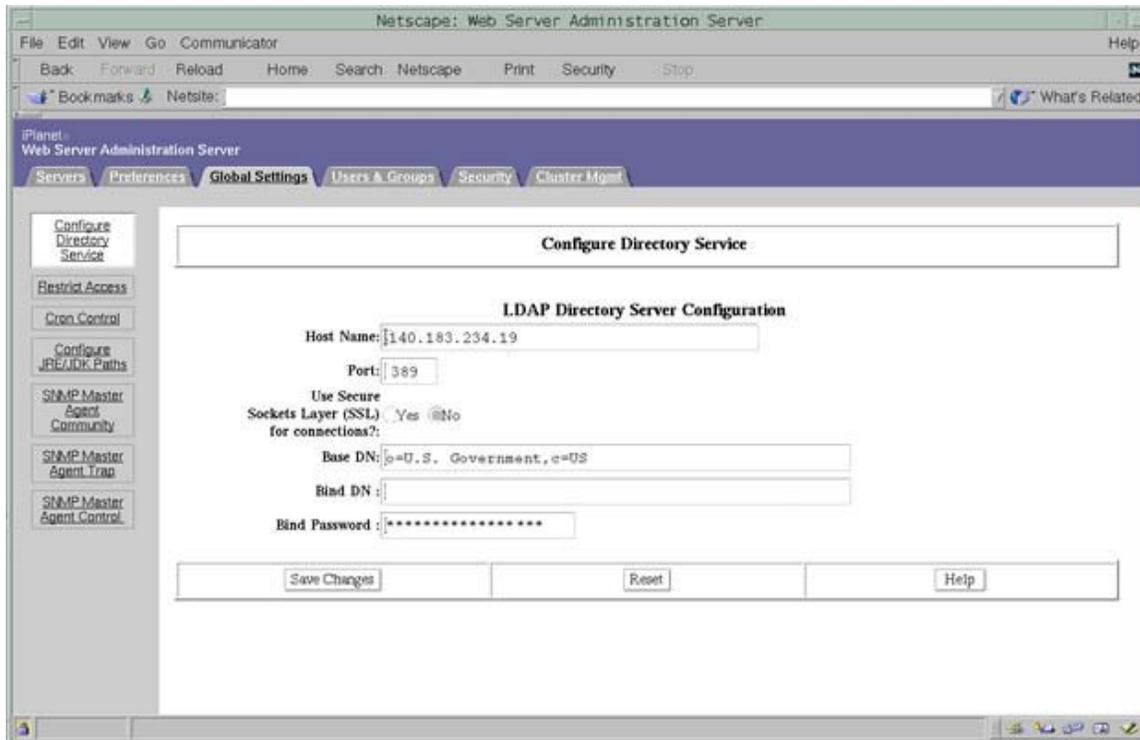
4 CONNECTION TO THE AKO DIRECTORY SERVER

4.1 Connect Using iPlanet Web Server 4.1

The following two steps illustrate the configuration of the Netscape 4.1 web server to the AKO Directory Server.



Open the Web Server Administration page in the Netscape Browser. Click on "Global Settings" to configure the Directory Server.



On the Configure Directory Server page, type the DNS entry for the AKO Directory Server, `directory.us.army.mil`, in the Host Name box.

In the Port box, type 636. Select 'Yes' for Use Secure Layer (SSL).

Base DN must be set to `o=U.S. Government,c=US`

Bind DN should be the DN given to you by the AKO

Bind Password will also be given to you by the AKO

Click "Save Changes"

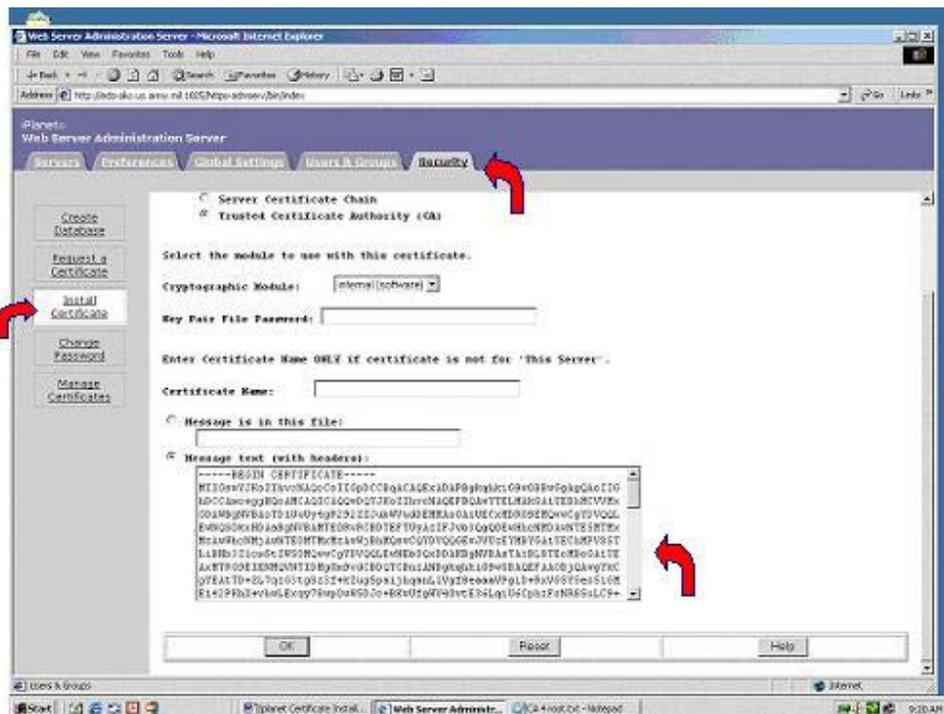
If you are using SDK version lower than 1.4, you will need to install the JSSE package, which enables the cryptographic mechanism for SSL, into your SDK's lib directory. The "java.security" file will need to be modified to include the Provider.

Installing the Directory Server and Trusted Root certificates

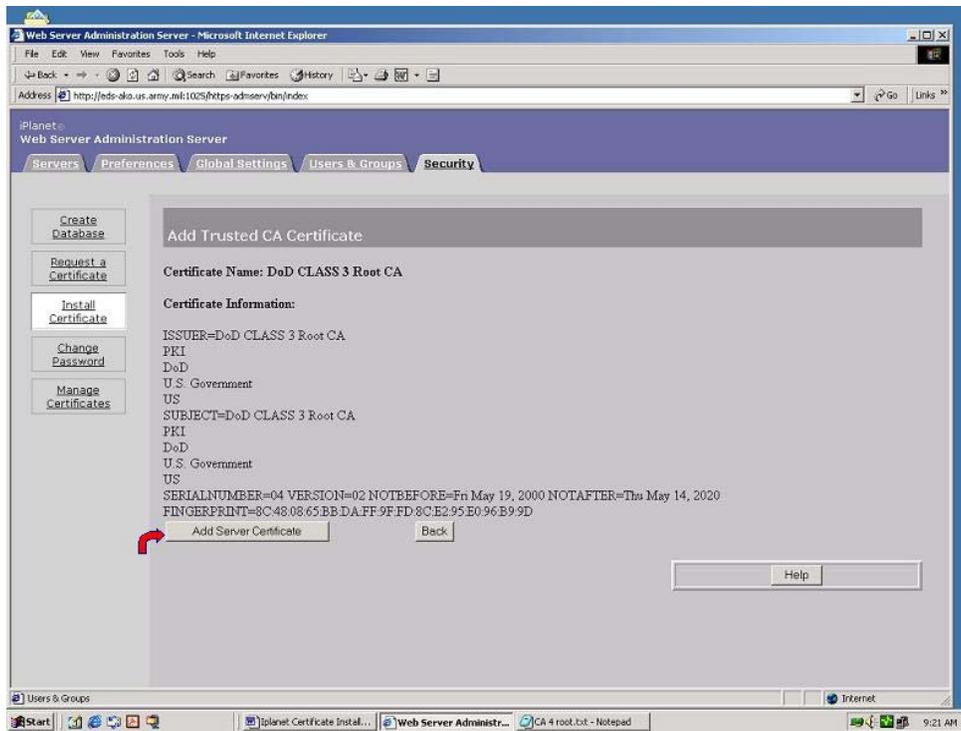
Download the DISA CA-4 root certificates, in the ".txt" format. This certificate will be installed in your server, which will then "trust" all servers whose certificates were signed by this Certificate Authority.

To install a certificate, perform the following steps:

1. Access either the Administration Server or the Server Manager and choose the Security tab
2. Click the Install Certificate link
3. Check the type of certificate you are installing – "Trusted Certificate Authority (CA)"
4. Enter the Key-Pair File Password
5. Select Message text (with headers) and paste the DoD Root Certificate text, including the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE--- lines
6. click OK



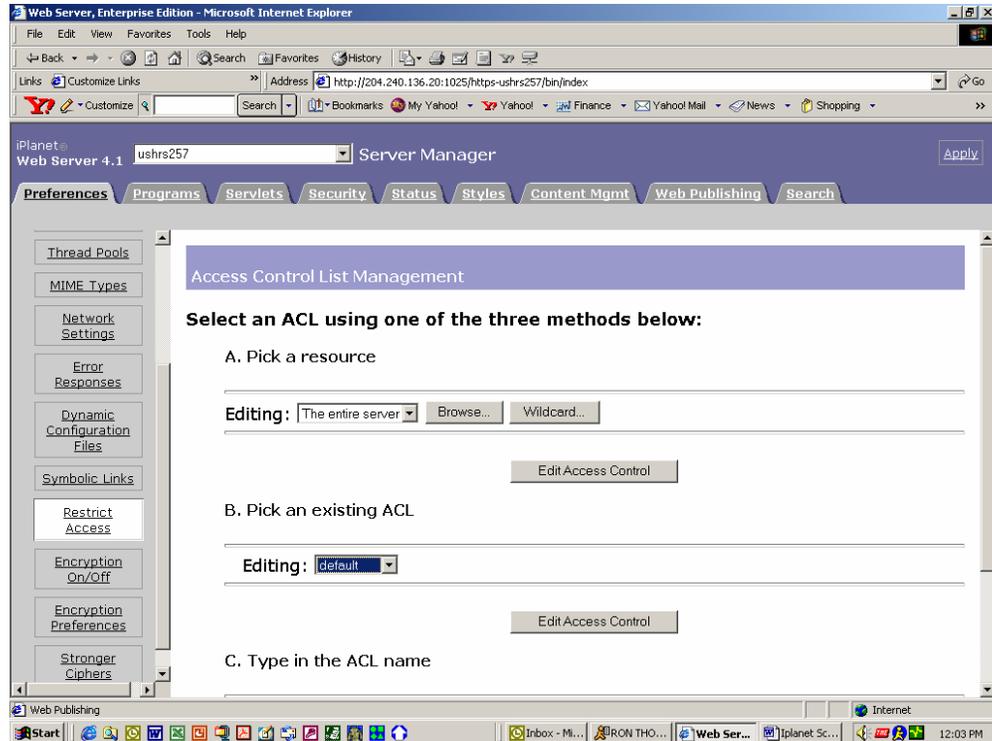
7. Select add Certificate if you are installing a new certificate



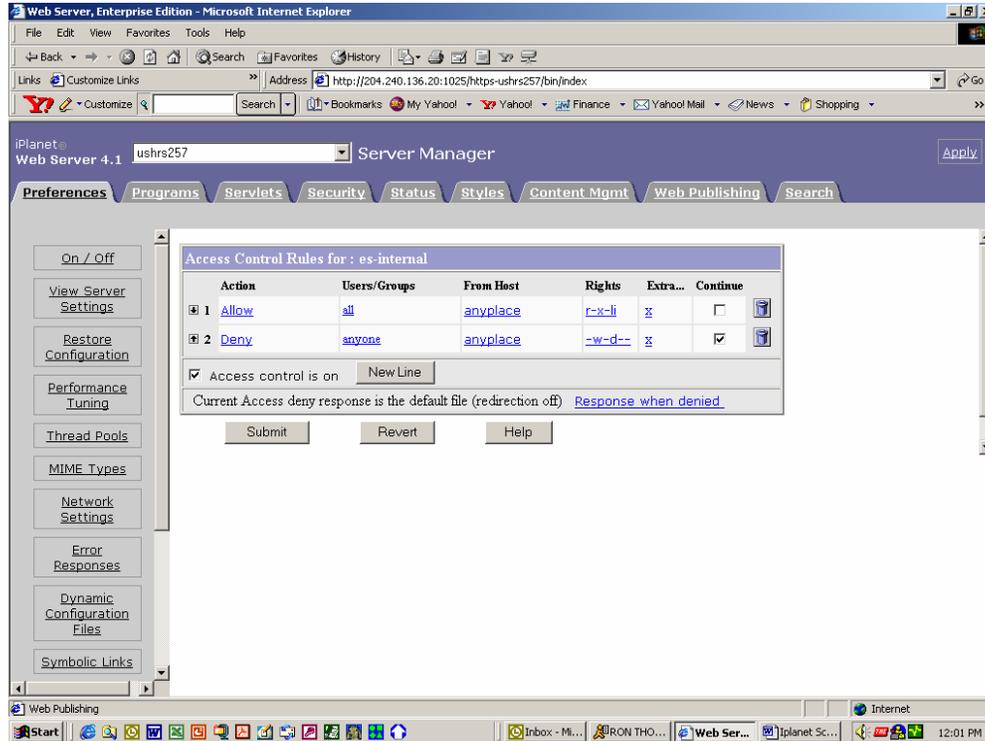
8. For the Server Manager, click Apply, and then Restart for changes to take effect. The certificate is stored in the server's certificate database

Configuring Access Control

On the "Preferences" tab, select "Restrict Access". Choose a resource, eg, "the entire server". Edit the Access Control. Set "all" users (as authenticated via the default LDAP Directory) to ALLOW access.



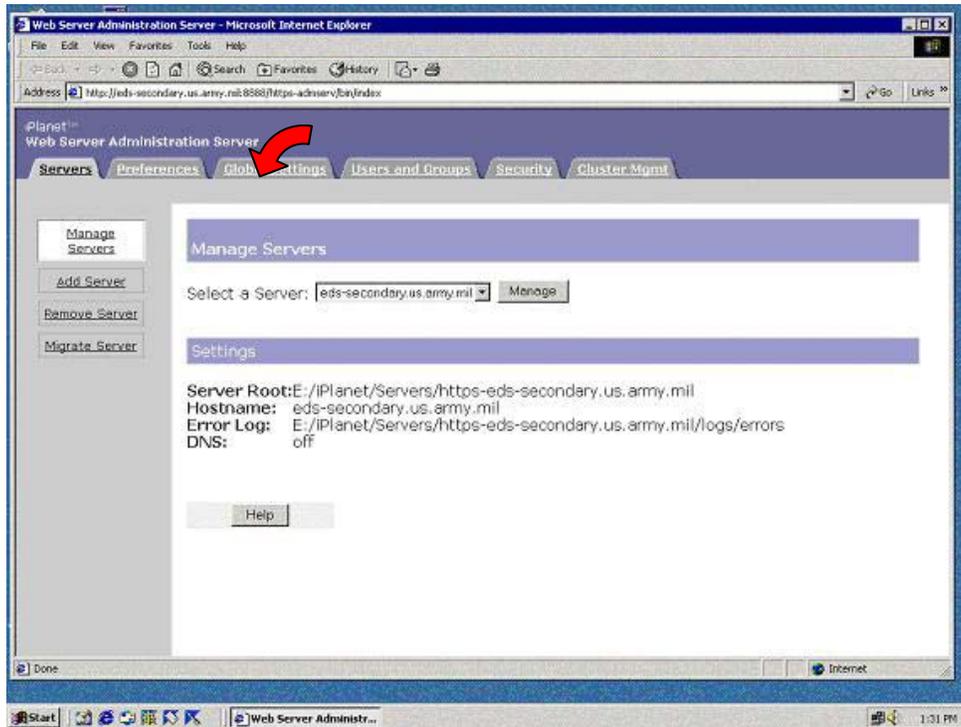
Set "all" users (unauthenticated) to DENY access. The "continue" checkbox after the "allow all" setting should be UNCHECKED. The authentication source should be set to the "default LDAP Directory". Additional access control - by user, or by file structure - can be configured either on these screens or within the underlying application or database.

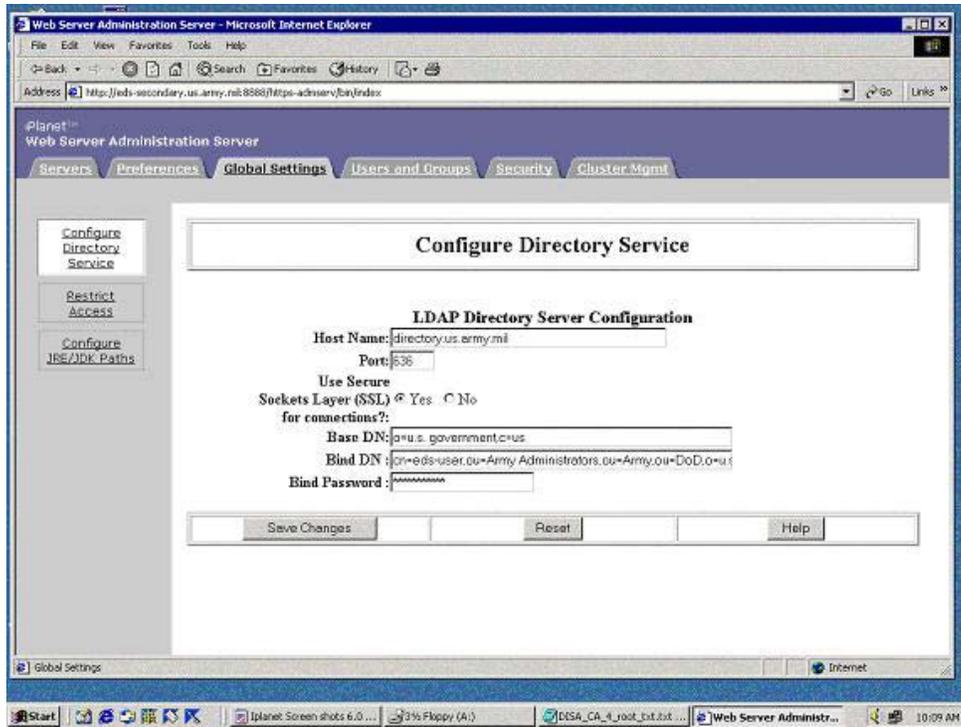


4.2 Connect Using iPlanet Web Server 6.x

The following steps illustrate the configuration of the Netscape 6.x web server for connection to the AKO Directory Server.

- Open the Web Server Administration page in the Netscape Browser. Click on “Global Settings” to configure the Directory Server.

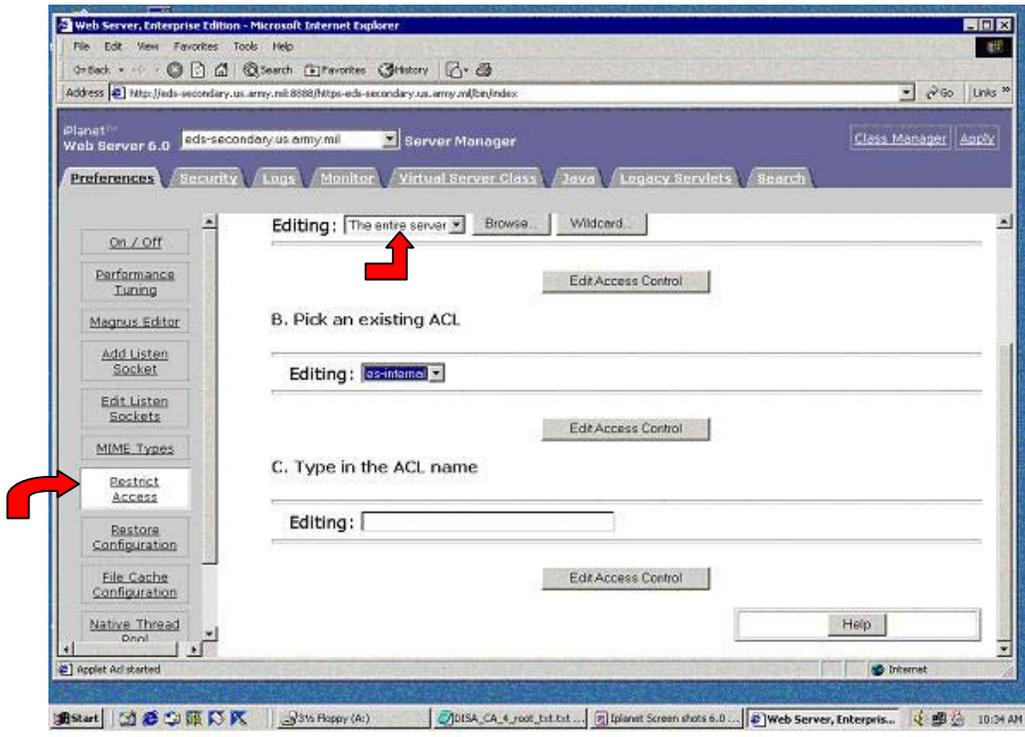




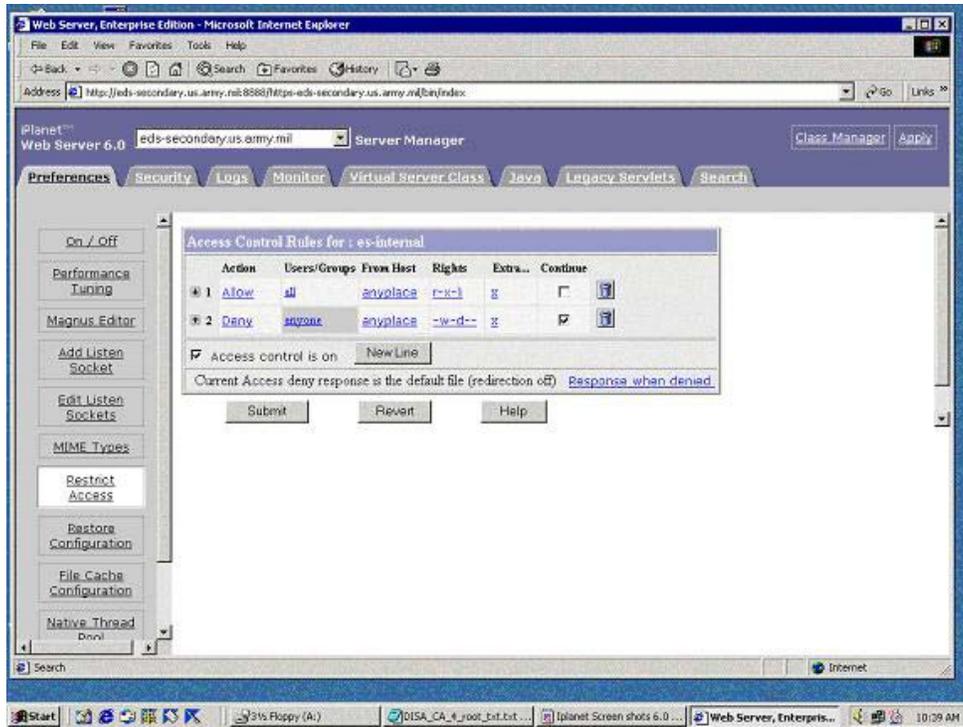
- On the Configure Directory Server page, type the DNS entry for the AKO Directory Server in the Host Name box:
directory.us.army.mil
- In the Port box, type 636. Select 'Yes' for Use Secure Layer (SSL).
- Base DN must be set to o=U.S. Government,c=US
- Bind DN must be the DN given to you by the AKO
- Bind Password will also be given to you by the AKO
- Click "Save Changes"

Configuring Access Control

On the “Preferences” tab, select “Restrict Access”. Choose a resource, eg, “the entire server”. Edit the Access Control. Set “all” users (as authenticated via the default LDAP Directory) to ALLOW access.



Set “anyone” users (unauthenticated) to DENY access. The “continue” checkbox after the “allow all” setting should be UNCHECKED. The authentication source should be set to the “default LDAP Directory”. Additional access control - by user, or by file structure - can be configured either on these screens or within the underlying application or database.



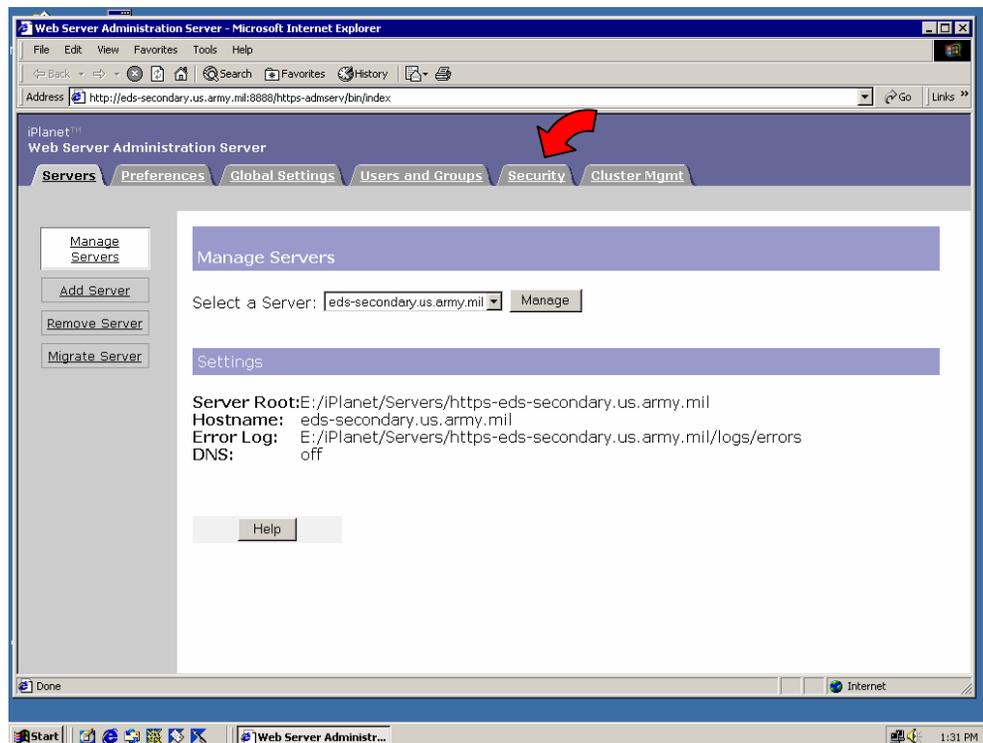
Installing Server Certificates on iPlanet

For the application server to "trust" the AKO Directory Server and establish an encrypted LDAPS session, you must install the Trusted Root Certificate for the Certificate Authority that signed the AKO Directory Server's certificate. This is the DISA CA_4_Root Certificate. This root certificate is posted in the AKO Portal, Army Knowledge Collaboration Center, in the folder:

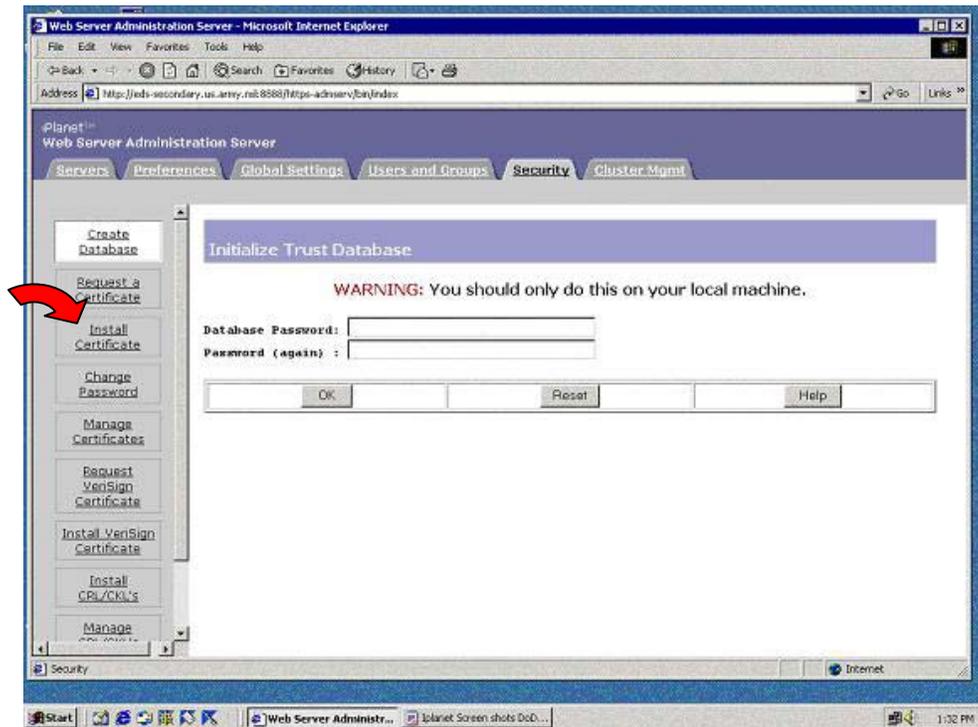
Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) /
AKO Interface Control Document/Certificates

To install a certificate, perform the following steps:

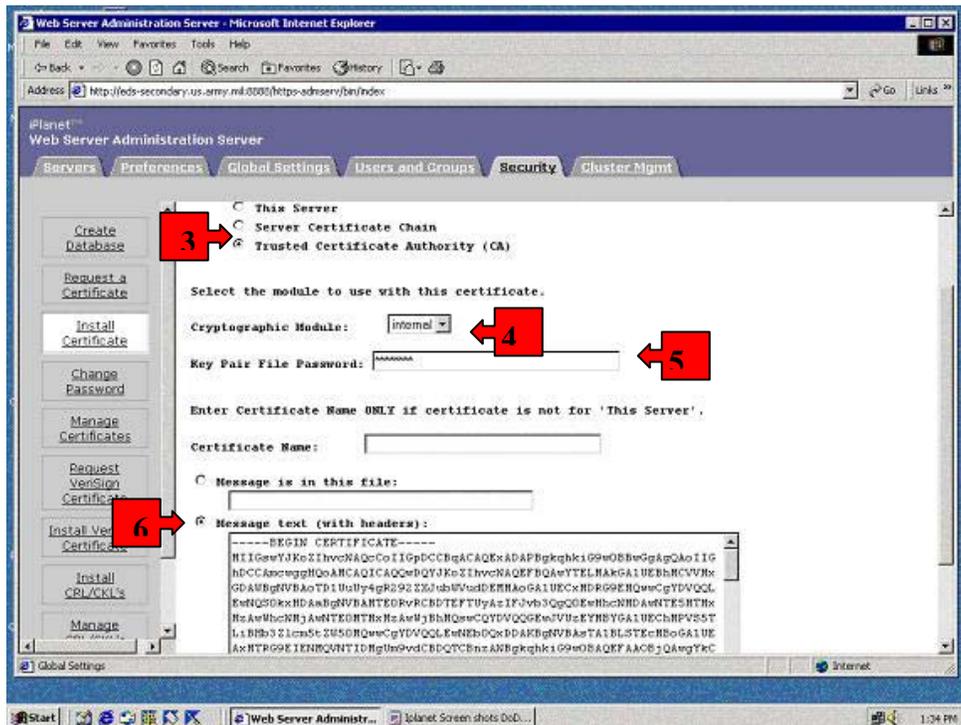
- Access the Web Server Administration Server, choose the Security tab



- Click the Install Certificate link.



- Check the type of certificate you are installing – "trusted certificate authority":

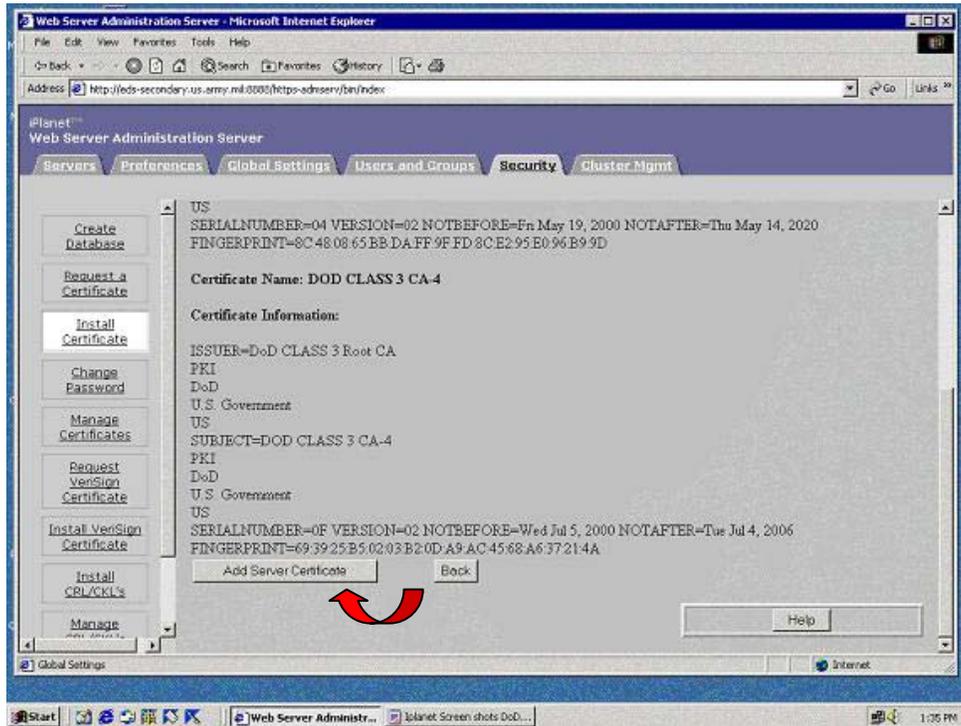


Note: Leave the name for the certificate field blank if it will be the only one used for this server instance

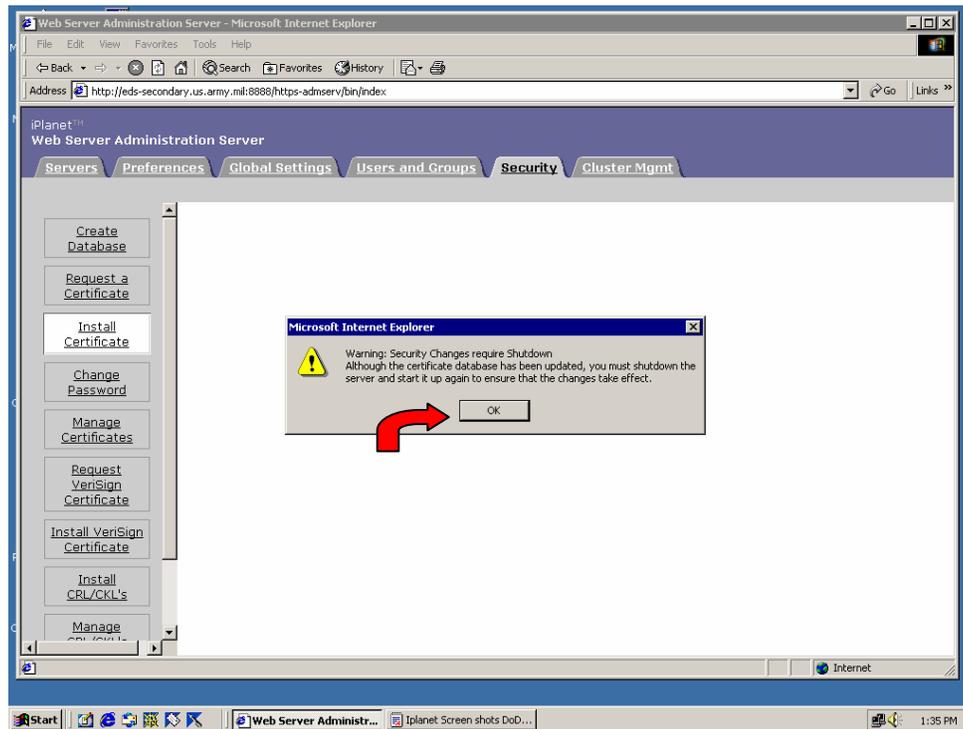
- Select Trusted Certificate Authority (CA)
- Select Cryptographic Module (internal)
- Enter the Key-Pair File Password.
- Select text (with headers) and paste the DISA CA-4 Root Certificate text.

Note: If you copy and paste the text, be sure to include the headers “Begin Certificate” and “End Certificate” — including the beginning and ending hyphens

- Click OK

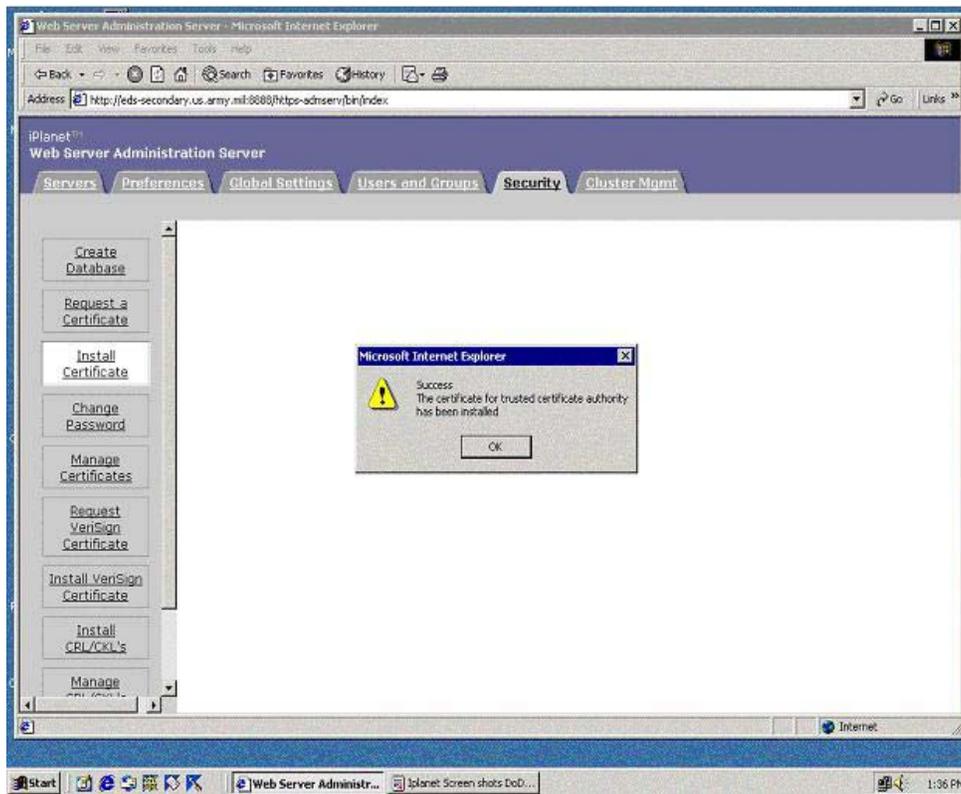


- Select add Certificate



- Click OK

Note: The certificate is stored in the server's certificate database. The filename will be <alias>-cert7.db. For example: https- serverid-hostname-cert7.db



Note: The Certificate has been successful added

- Click OK

4.3 Connect Using Microsoft Internet Information Server (IIS)

LDAP Extension Patches – Microsoft extensions to support LDAP connections require that Windows 2000 Service Pack 3 (SP3) be installed for all functionality to work correctly. For legacy Windows NT applications, LDAP connections to authenticate users require the ADSI extensions. To read LDAP schema extensions (see Section 5.1), a patch is required – contact AKO to obtain this patch.

Security Patches - IIS has some known security holes in the default installation that must be patched. The latest patches released by Microsoft can be found at:



<http://www.microsoft.com/technet> under the security icon:

In particular, there is an LDAP over SSL vulnerability that has been identified. A patch is available to fix this vulnerability. Please read the Security Bulletin

<http://www.microsoft.com/technet/security/bulletin/ms01-036.asp>

for information on obtaining this patch.

Configuration - IIS cannot be configured to authenticate against the AKO Directory Server in its native installed form. Instead, either the **Single Sign-On** module must be deployed, or a **forms-based authentication** must be written. Both options are discussed below.

Single Sign-On using the Netegrity web agent is discussed in the Netegrity section of this document. If user attributes look-ups are required, the LDAP connection is still required. For the user's identity, Netegrity populates the user header with an "SM_USER" variable. Unfortunately, active server pages cannot read header variables that include an "under_score". Therefore AKO has added 2 additional header variables that can be read by active server pages:

```
dim userID, userDN
userID = Request.ServerVariables("HTTP_USERCN")
userDN = Request.ServerVariables("HTTP_USERDN")
```

These variables can be used within an Active Server Page for further LDAP queries or for use in access control lists.

Allowing access within IIS – NT 4.0

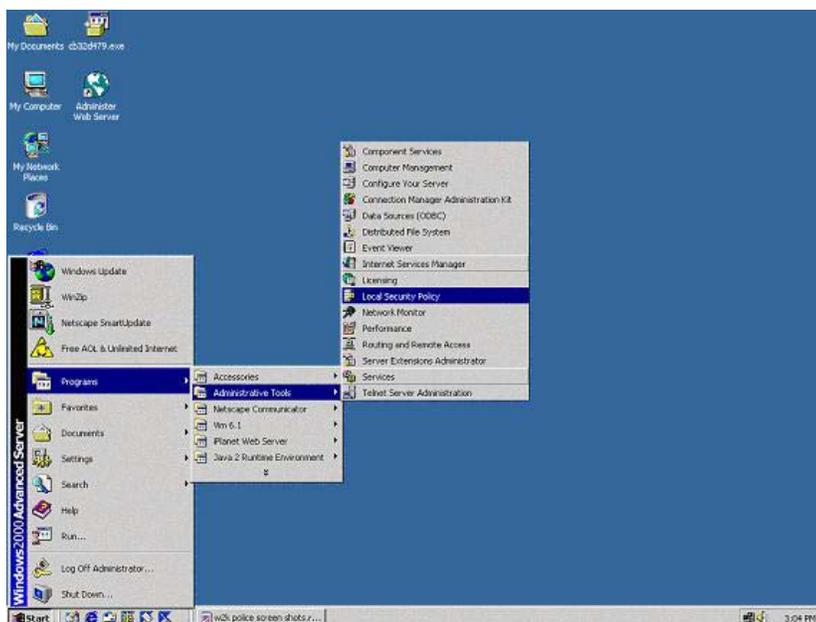
Access control will be managed at the application level, not by the NT Operating System. Therefore, within IIS you must grant the Everyone group the User Right Access to access this IIS server from the network:

1. From the **Start** button, select Programs, and then select Administrative Tools (Common).
2. Click **User Manager** or **User Manager for Domains**.
3. Click **Select Domain** from the **User** menu.
4. Enter the domain name if this is a domain controller or enter the local computer name if this is a member server or stand-alone server.
5. Click **OK**.
6. From the **Policies** menu click **User Rights**.
7. Add the special group Everyone and click **OK**.
8. Re-run Site Server setup.

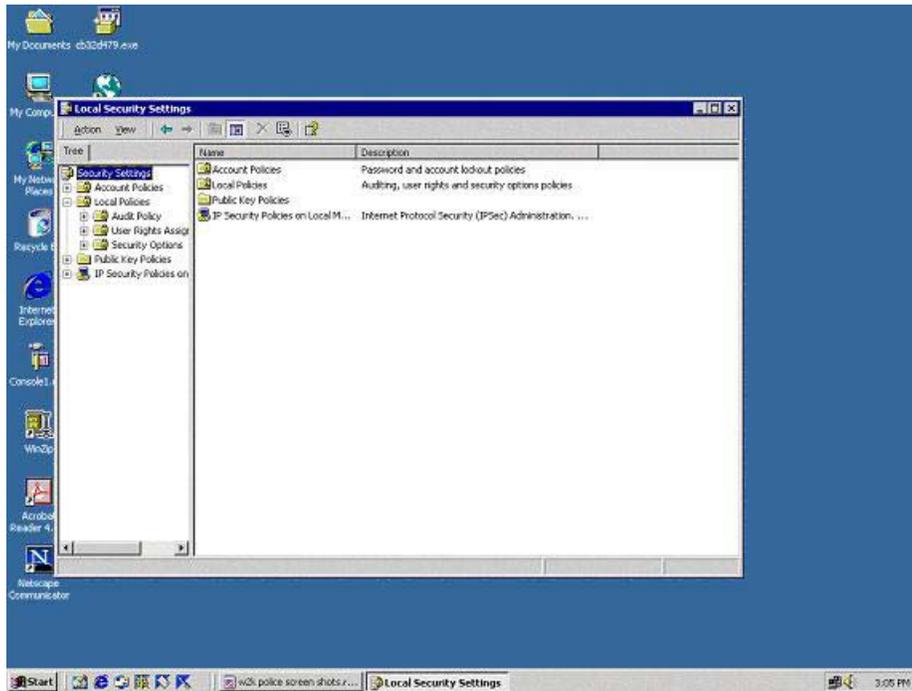
Allowing access within IIS - Windows 2000

Access control will be managed at the application level, not by the Win2K Operating System. Therefore, within IIS you must grant the Everyone group the User Right Access to access this IIS server from the network:

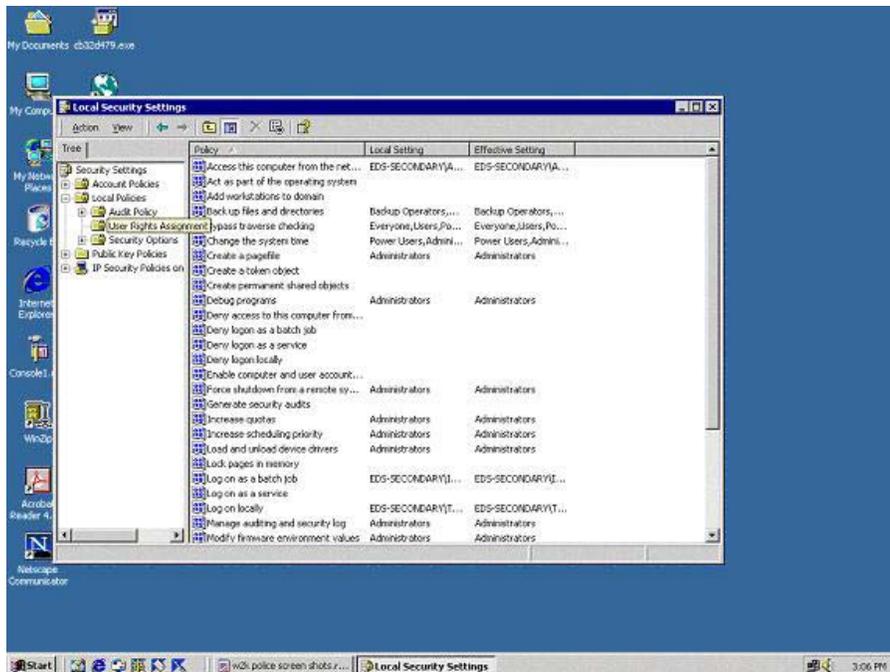
- From the **Start** button, select Programs, and then select Administrative Tools and then select Local Security Policy (Common).



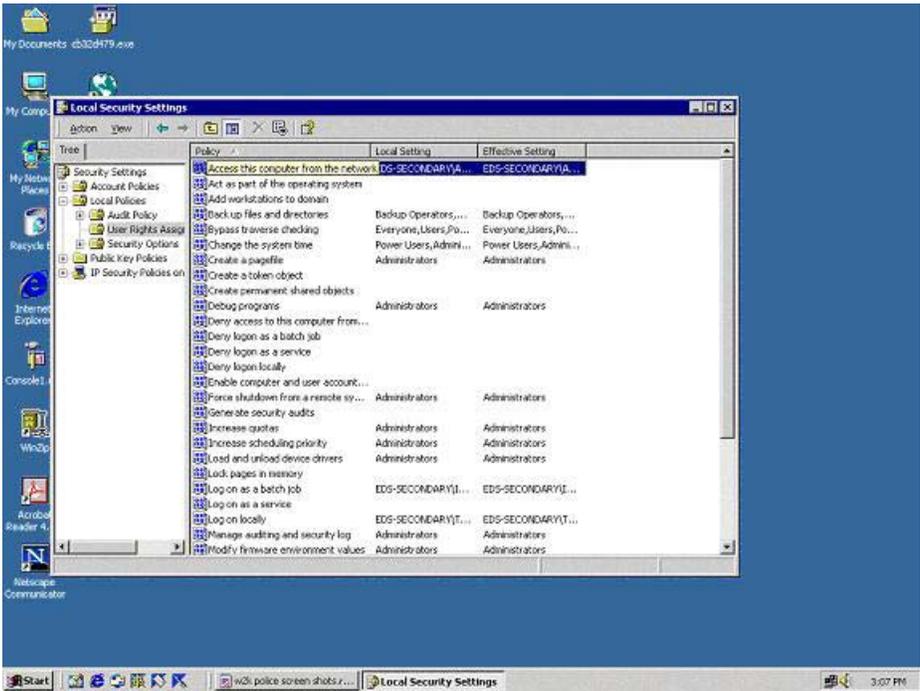
Select Local Policies



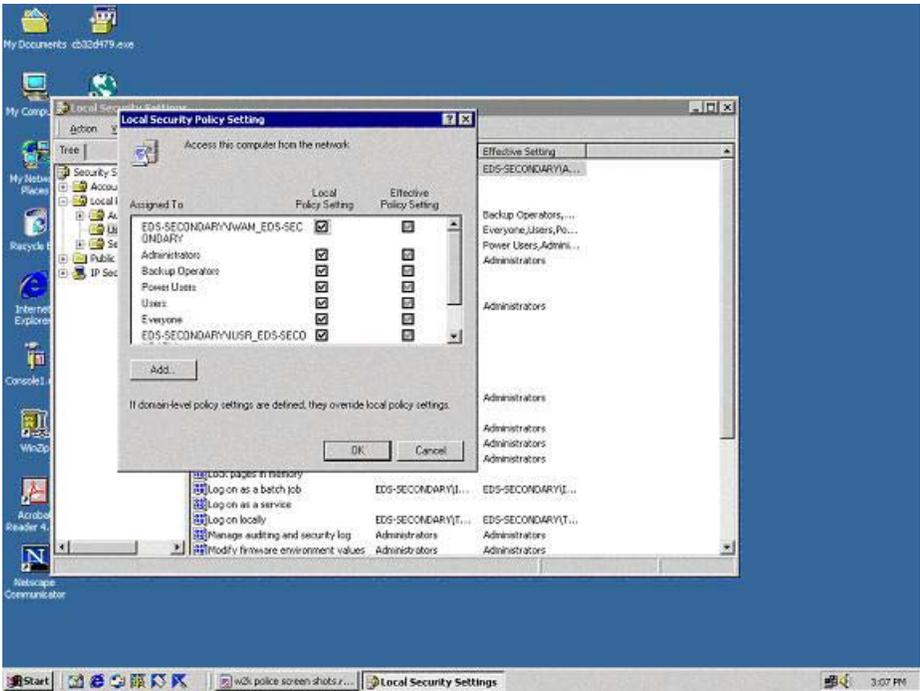
- Select User Rights Assignment



- Select **Access this computer from the network**



- Add the special group **Everyone** and click **OK**.



- Restart your Server.

Forms Based Authentication

- Create an HTML Login page that accepts a username / password
- Write a server-side script to authenticate the user against the AKO Directory Server

The following Visual Basic code segment will perform the connection to the AKO Directory Server and authenticate the user. This code can be placed into an .asp script or a Visual Basic IIS Application. It uses ADSI class libraries that are included in the ADSI extensions. These are included with Window2000 and later releases. They extensions for Windows NT 4.0 can be downloaded from Microsoft:

<http://www.microsoft.com/NTWorkstation/downloads/Other/ADSI25.asp>

```
'=====
<%@ Language=VBScript %>

<%
Option Explicit
On Error Resume Next
Response.Buffer = True
Response.Expires = 0

'CAPTURE VARIABLES FROM QUERYSTRING
dim sUserName, sPassWord
sUserName = lcase(request("username"))
sPassWord = request("password")

'SETUP RETURN TO FORMSLOGIN.ASP WHEN AN ERROR IS DETECTED
dim sErr
sErr = "formslogin.asp?username=" & sUserName & "&error="

'VALIDATE FOR LENGTH OF USERNAME AND PASSWORD
If Len(sUserName) = 0 Or Len(sPassWord) = 0 Then
    response.write "AKO AUTHENTICATION FAILURE<br>"
    response.write "Authentication failed. Please try logging in again.<br>"
```

```

    response.write "You must be a registered AKO user to access this site.<br>"
    response.write "Use the back button on your browser to try again."
    Response.end
End If

'SETUP CONNECTION TO AKO DIRECTORY
dim akoServer, dnUserName, oLDAP
'use port 636 for LDAP-S
akoServer = "LDAP://directory.us.army.mil:636/"
dnUserName = "cn=" & sUserName & ",ou=People,ou=Army,ou=DoD,o=U.S.
Government,c=US"
Set oLDAP = GetObject("LDAP:")

'VALIDATE USERNAME AND PASSWORD
dim oContainer
'tell IIS to use encryption (flag = 2) for LDAP-S
Set oContainer = oLDAP.OpenDSObject(akoServer & dnUserName, dnUserName,
sPassWord, 2)
If Err.Number <> 0 Then
'EXIT WITH ERROR - INCORRECT USERNAME & PASSWORD - RETURN TO
FORMSLOGIN.ASP
    response.write "AKO AUTHENTICATION FAILURE1<br>"
    response.write ("Error Number: " & Err.Number & "<br>")
    response.write "Authentication failed. Please try logging in again.<br>"
    response.write "You must be a registered AKO user to access this site.<br>"
    response.write "Use the back button on your browser to try again."
    Response.end
    Set oContainer = Nothing
    Set oLDAP = Nothing
    'exit function
End If

```

'READ USER ATTRIBUTES USING ADMIN ACCOUNT

dim SUPERBROKER, SUPERBROKERPWD

'VALUE OF ADMINISTRATOR USERNAME OBTAINED FROM AKO

SUPERBROKER = ""

'VALUE OF ADMINISTRATOR PASSWORD OBTAINED FROM AKO

SUPERBROKERPWD = ""

dim dnAdmin, akoRank, akoEmail

dnAdmin = "cn=" & SUPERBROKER & ",ou=army
administrators,ou=Army,ou=DoD,o=U.S. Government,c=US"

'tell IIS to use encryption (flag = 2) for LDAP-S

Set oContainer = oLDAP.OpenDSObject(akoServer & dnUserName, dnAdmin,
SUPERBROKERPWD, 2)

If Err.Number <> 0 Then

'EXIT WITH ERROR CODE - INCORRECT ADMIN USERNAME & PASSWORD -
RETURN TO FORMSLOGIN.ASP

 response.write "AKO AUTHENTICATION FAILURE2
"

 response.write ("Error Number: " & Err.Number & "
")

 response.write "Authentication failed. Please try logging in again.
"

 response.write "You must be a registered AKO user to access this site.
"

 response.write "Use the back button on your browser to try again."

 Response.end

 Set oContainer = Nothing

 Set oLDAP = Nothing

 'Exit Function

End If

'GET USER ATTRIBUTES FROM AKO DIRECTORY

akoRank = oContainer.Get("armyRank")

sUserArmyAccountType = oContainer.Get("armyAccountType")

```
akoEmail = oContainer.Get("mail")
```

```
'DEBUG STATEMENTS TO DEMONSTRATE RETURNED VALUES FROM LDAP
```

```
'NEED TO TAKE OUT ON ACTUAL OPERATIONAL ENVIRONMENT
```

```
response.write("Rank: " & akoRank & "<br>")
```

```
response.write("armyAccountType: " & sUserArmyAccountType & "<br>")
```

```
response.write("email: " & akoEmail)
```

```
%>
```

Adding a Internet Certificate into the Certificate Manager in IIS 4

Microsoft has documented adding a foreign certificate to an IIS 4 server. This can be found at:

<http://support.microsoft.com/support/kb/articles/q218/4/45.asp>

Adding a Internet Certificate into the Certificate Manager in IIS 5

To install a Certificate in IIS (Web Server) you must first install the Certificate Manager in your MMC.

To add Certificate Manager to the MMC

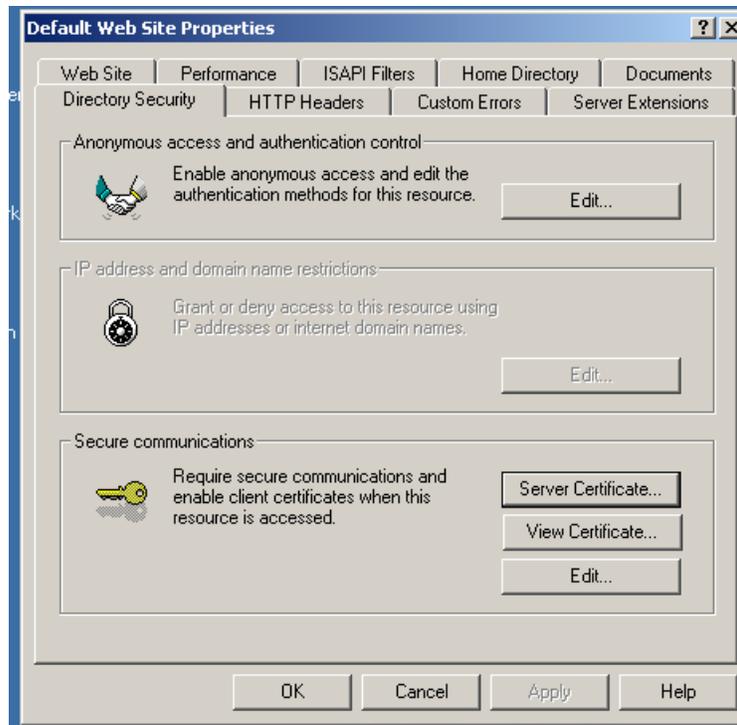
Note If you already have Certificate Manager installed in the MMC, it will point to the correct Local Computer certificate store.

1. Open an MMC console and select **Add/Remove Snap-in** from the Console menu.
2. Click **Add**
3. Select **Certificate Manager**.
4. Click **Add**
5. Select the **Computer account** option.
6. Select the **Local Computer** option.
7. Click **Finish**.

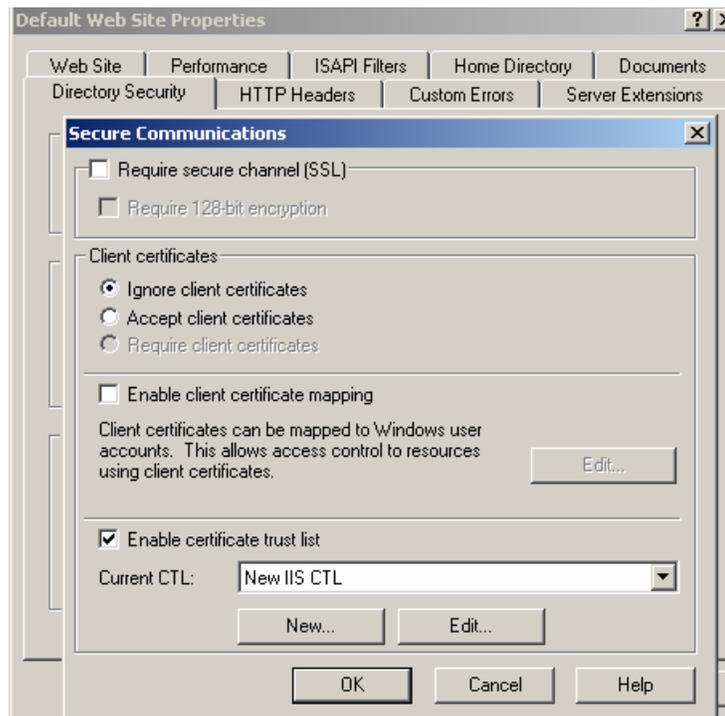
Before installing a foreign Trusted Root Certificate, you **MUST** request and install an SSL Certificate for the IIS Web Server, using Certificate Wizard. The Certificate Wizard will guide you through the steps to create a new certificate or and to import the signed certificate. You must enable certificate trust lists (CTLs) to use the New and Edit buttons.

After installing the certificate and enabling CTLs, you can choose to "trust" various Certificate Authorities by installing their Trusted Root.

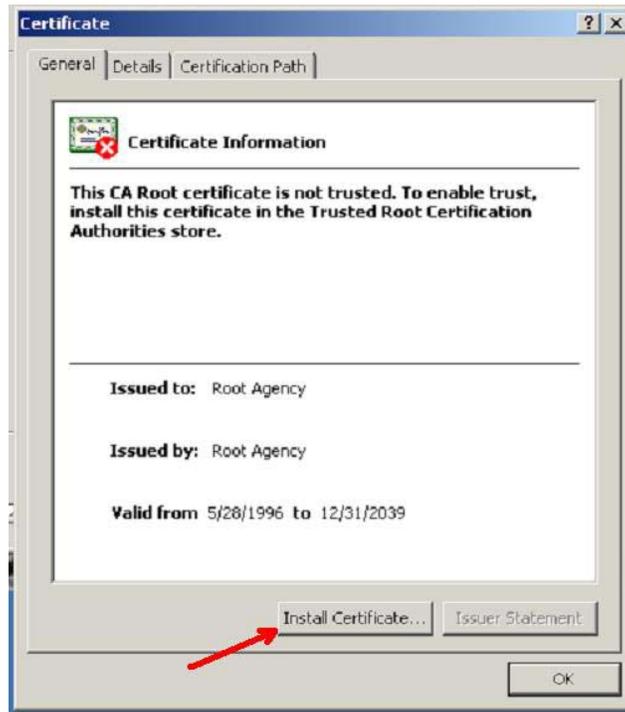
1. On the **Directory Security** property sheet, under **Secure Communications** click **Server Certificate** to access the Web Server Certificate Wizard and change settings regarding your certificates.



2. On the **Directory Security** or **File Security** property sheet, under **Secure Communications** click **Edit** to install foreign Trusted Root certificates. Under **Enable certificate trust list** click either **New** to add a Certificate trust that you have saved in a file or **Edit** to access the CTL Wizard and change settings regarding your certificate trust lists.



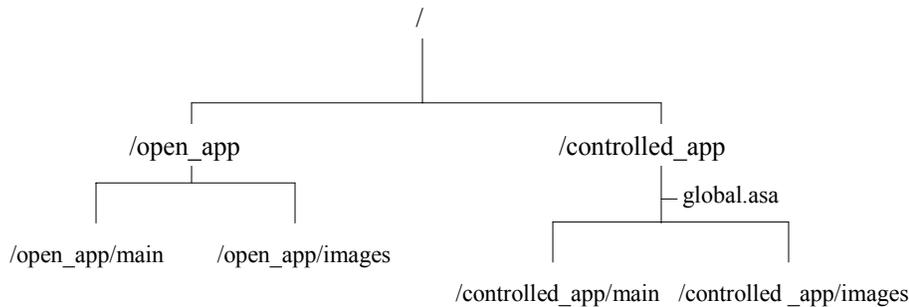
3. On the **Directory Security** or **File Security** property sheet, under **Secure Communications**, click **Edit**. Under **Enable certificate trust list** select the Trusted Root Certificate you just installed and select the **view** button. Note the label <**This CA Root certificate is not trusted**>. In order for this certificate to be trusted, you must "install" this certificate in a trusted Root Certification Authorities store by clicking the install button to store the certificate.



Access Control in IIS - .asp pages

IIS supports several methods for implementing page, file, and field level access control. Note that the "out of the box" method using NT or Active Directory "groups" within the IIS Management Console will not work when using the a "foreign" LDAP Directory such as the AKO Directory, as the "foreign" users cannot be added to the NT or Active Directory "groups". Thus, access control must be implemented using .asp code and/or SQLServer database controls.

The first step to access control is to create the file global.asa at the root of all protected pages:



In the validate.asp script, after successful authentication, the session variables can be populated:

```
Sub ValidationSuccessful
...
Session("dnUserName") = Request.Form("dnUserName")
Session("sUserArmyAccountType") = Request.Form("sUserArmyAccountType")
....
End Sub
```

On each .asp page that is to be protected, the dnUserName session variable should be checked to ensure that the user has already successfully authenticated, and then can be used to compare against any role-specific permissions:

```
<%
....
If IsEmpty(Session("dnUserName")) Then
    Response.Redirect("//login.asp")
End If
...
%>
```

For Netegrity implementations, the user's identity can be obtained using:

```
dim userID, userDN
userID = Request.ServerVariables("HTTP_USERCN ")
userDN = Request.ServerVariables("HTTP_USERDN ")
```

Access Control in IIS - files

To protect objects that are not .asp files, eg Word, PowerPoint, or Acrobat files, one can implement the following:

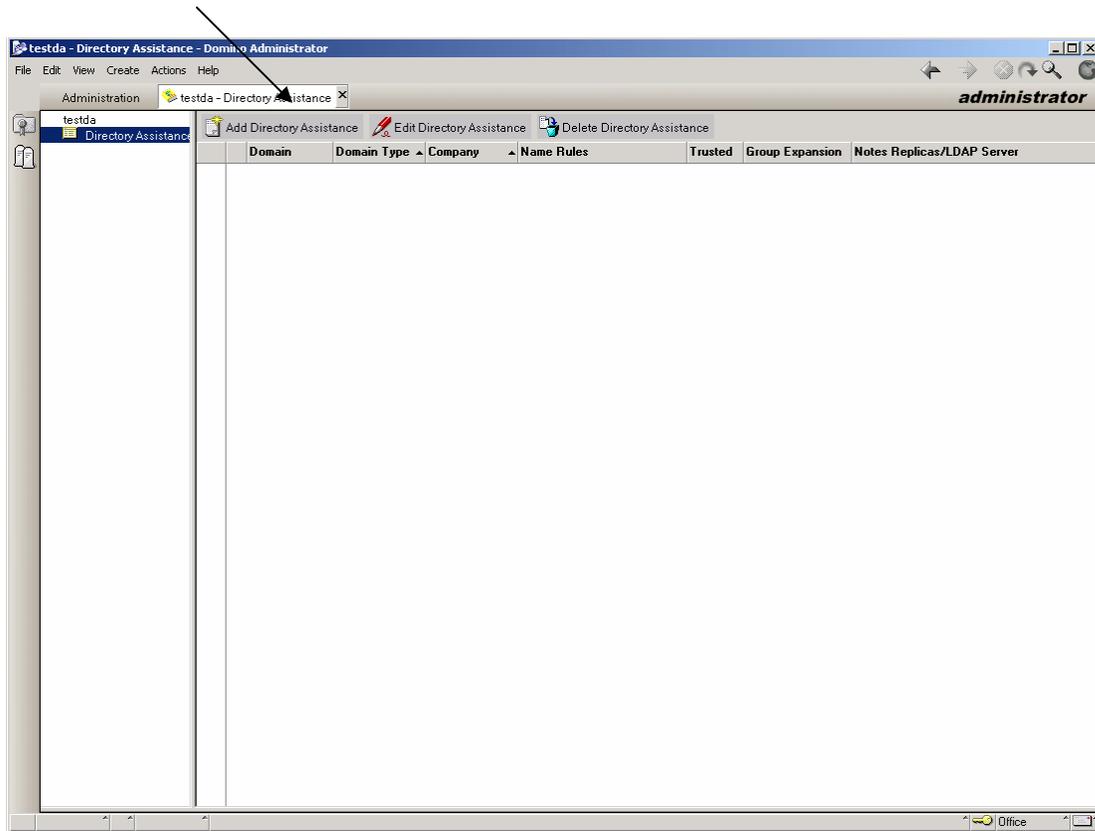
- Use IIS directory security to lock up all content directories so that only the localhost (127.0.0.1) can access them. These files can be located on other physical servers and are shared out to the web server, which maps them as virtual directories in IIS.
- Provide a dynamic file that "serves" the requested file after checking for their authentication session variable. An example download file, startDownload.asp, can be downloaded from the AKO Army Knowledge Collaboration center, in the folder

Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) / AKO
Interface Control Document.

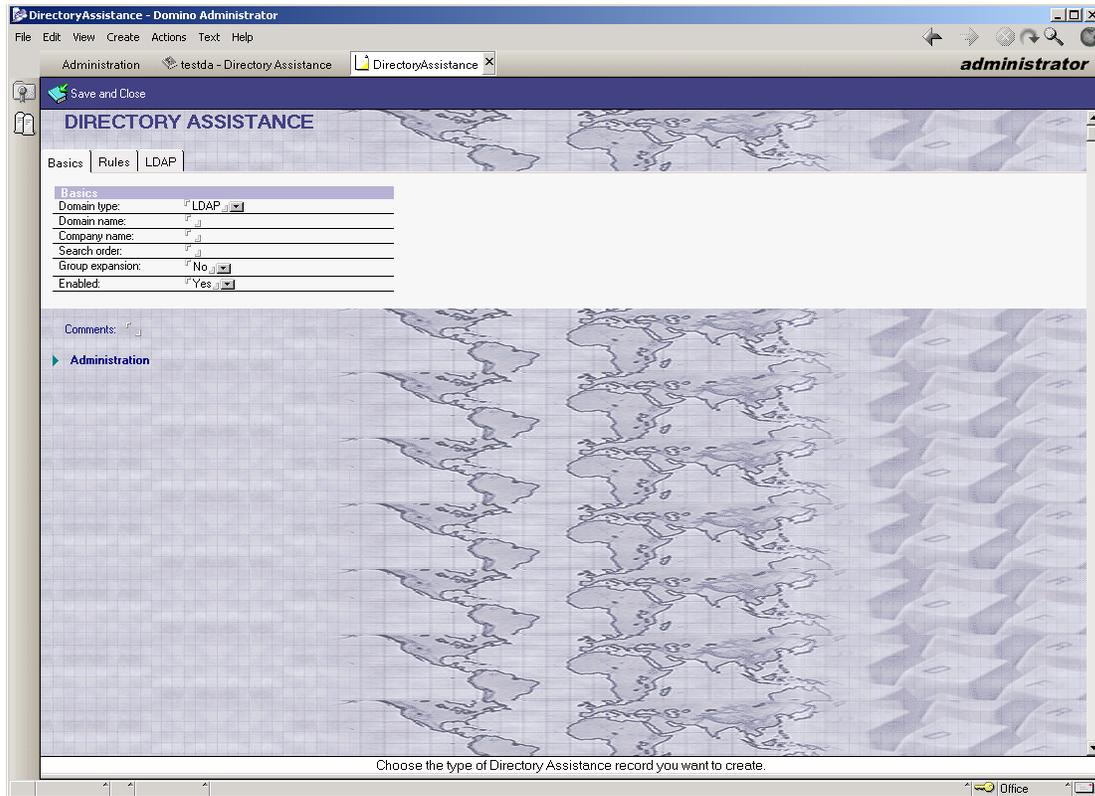
4.4 Connect Using Lotus Domino

The following are steps to guide you on connecting/authenticating to the AKO Directory Server located at directory.us.army.mil:

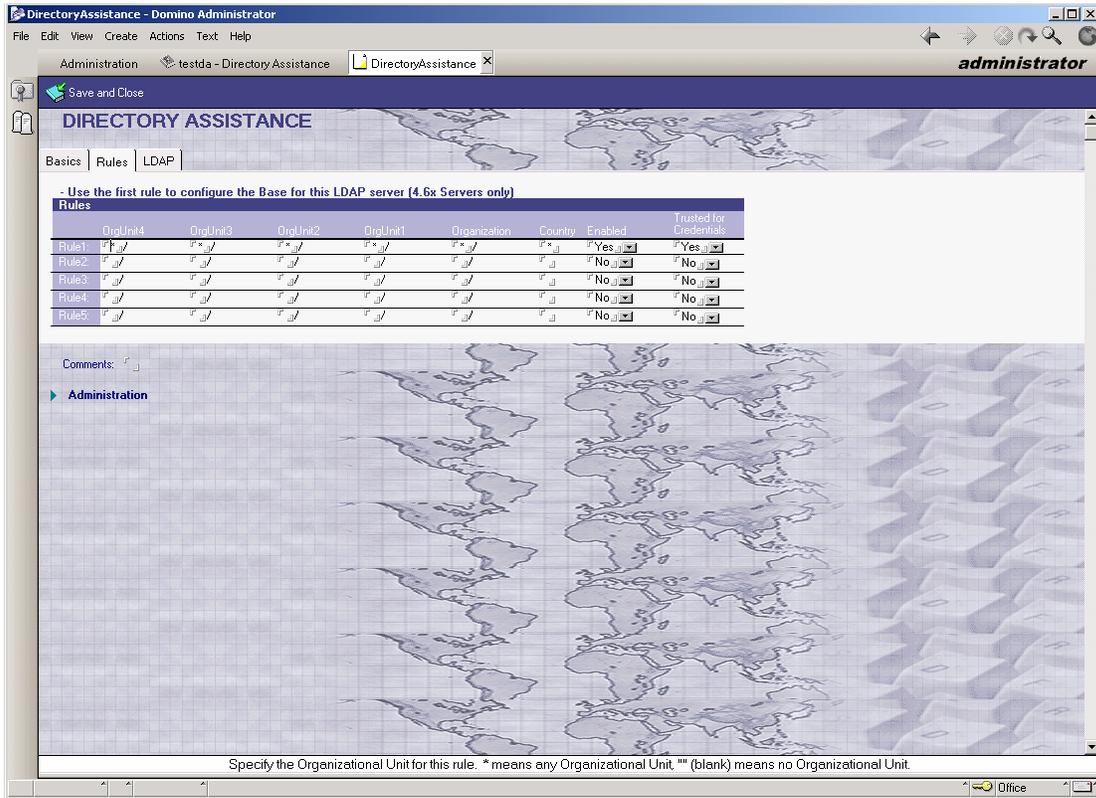
- Test LDAP connectivity using LDAPsearch to the AKO directory.
- Create a database using the Directory Assistance database template.
- Choose Add Directory Template



- On the Basics tab, the Domain Type should have 'LDAP' selected.
- Enter the Domain Name and Company Name. The Search Order can be left blank. If you have more than one directory, you can choose the order that the directories are searched using this field.



- On the Rules tab, choose 'Yes' for Trusted for Credentials



For the LDAP tab:

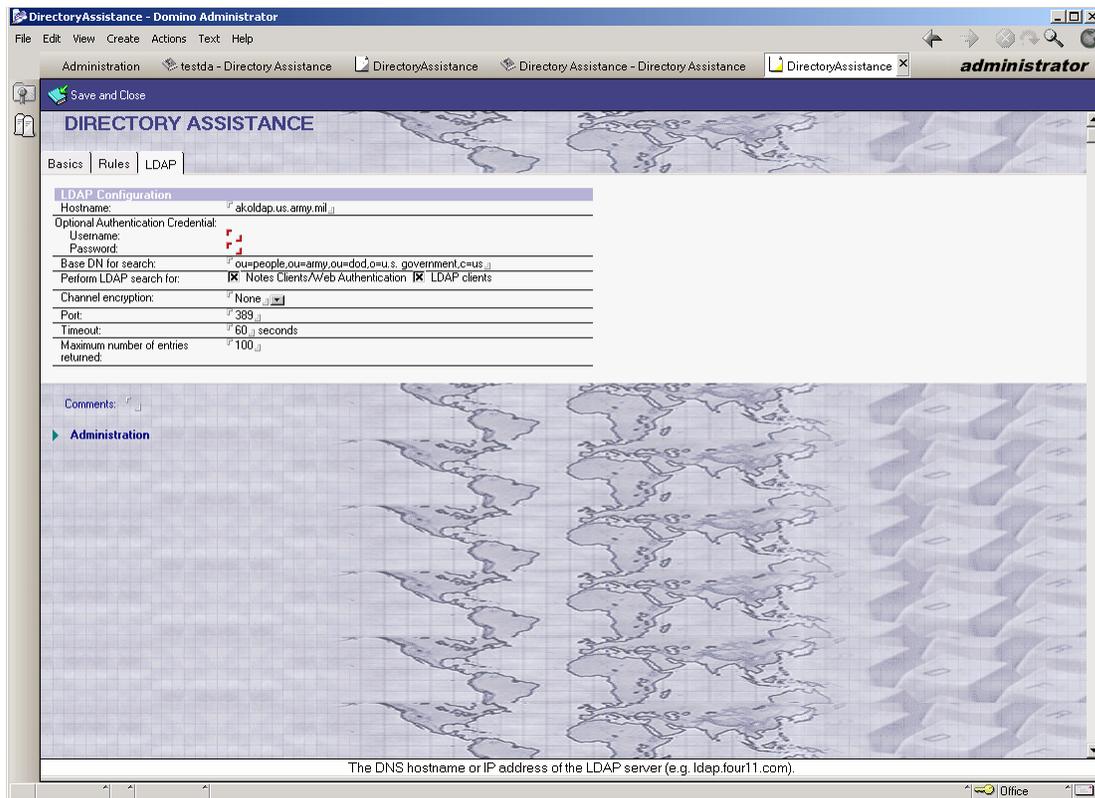
- In the Optional Authentication Credentials fields, enter the serverid and password for connection to the AKO DIRECTORY server. Use the fully qualified DN for the serverid, of the form:

cn=serverid,ou=Army Administrators,ou=army,ou=dod,o=u.s. government,c=us

- enter the host server name that holds the LDAP directory - directory.us.army.mil
- Enter the ServerID and password that were issued for your application server.
- For the Base DN Search, enter:

ou=people,ou=army,ou=dod,o=u.s. government,c=us

- Perform LDAP search for notes clients/web authentication and LDAP clients
- Choose SSL for Channel Encryption
- Port should be 636
- Keep the defaults for the rest.



- Save and close database.
- Next, open the Sever document and go to the Basics tab. Enter the Directory Assistance database name that was just created.

- On the Security tab, ensure that the Web Server Authentication is set to "Fewer name variations with higher security".
- Save the document.
- Edit the notes.ini file to launch the LDAP task when the server starts.
- Restart the server so that the changes will take effect.

Cross certify the AKO Directory Server in the Domino Administrator client

- Select File / Tools / Add Internet Cross Certificate (Note that this affects the Domino Directory on which the user is sitting, so you must perform this step from the console, not remotely.)
- In the "Server Name" text box, type the name of the target server - directory.us.army.mil
- In the "protocol" list box, select LDAP
- Click the "Connect" button
- Verify the data, and click the "Cross Certify" button

4.5 Connect Using SilverStream 4.7

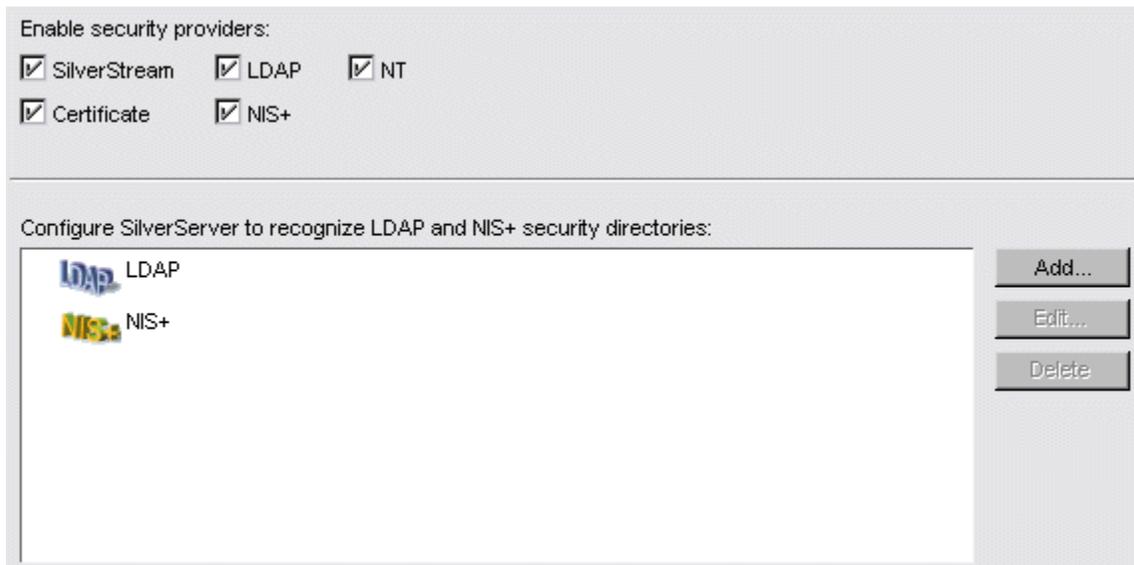
The following are steps to guide you on connecting/authenticating to the AKO Directory Server located at directory.us.army.mil:

Note: These steps assume general knowledge and understanding of SilverStream server administration.

The first step to add directory authentication through AKO is to add and configure the security provider access.

▶▶ To set up LDAP security:

1. Invoke the SMC.
2. Select **Security** options.
3. Select the **Security Providers** panel.



4. The provider list is shown. Click **Add**.

A wizard appears.

5. Select **LDAP** and click **Next**.

The following dialog displays. Use this dialog to specify the server and the login attribute and user name/password.

Item	Description
Server	The name of the LDAP server - directory.us.army.mil
User Login Attribute	If you specify an attribute as the value of this property, it defines the LDAP attribute that can be used to uniquely identify a user. Enter cn
User Name and Password	Enter your ServerID and password to allow the SilverStream server access to LDAP information. The SilverStream server will use these system login credentials anytime the SilverStream server needs to access generic LDAP server information. These account values are required since the AKO Directory does not allow anonymous access. Please contact the AKO Helpdesk for assistance in obtaining this information if you don't have a username/password.

6. Click **Next**.

The following dialog displays.

Use this dialog to specify groups on the LDAP server.

Item	Description
Group Location	(Required) A distinguished name that identifies the level in the hierarchy where you want to start specifying group entries. Enter <code>ou=groups,ou=Army,ou=DoD,o=u.s. government</code>
Group Filter	(Required) The LDAP search filter is used to determine what constitutes a group for this LDAP server. Enter <code>(objectclass=organizationalunit)</code>
Group Description Attribute	(Optional) An attribute used to identify a group description in SilverStream. The name you enter is the LDAP attribute to which you want to map the description. For example: <code>ako</code>

Group Additional Attributes	<p>Select All if you want all of the specified LDAP group attributes to be listed in SilverStream. Select None if you want no additional attributes to appear.</p> <p>The specified attributes will be displayed in a tab when you select a group in the Users & Groups panel and open the Property Inspector.</p>
Group/Users Attribute	<p>(Required) An attribute used to display all members (users) of a group in SilverStream. The name you enter is the LDAP group attribute that lists users. Enter cn</p>

7. Click **Next** when you have finished specifying groups.

The next panel asks you to specify users on the LDAP server.

Add security provider server [X]

User Location:

User Filter:

User Description Attribute:

User Additional Attributes:
 All None

Full Name:

Enter the properties for the LDAP users.

< Back **Finish** Cancel

8. Specify users as follows:

Item	Description
User Location	(Required) A distinguished name that identifies the point in the hierarchy where you want to start specifying users. Enter <code>ou=people,ou=Army,ou=DoD,o=u.s. government</code>
User Filter	(Required) The LDAP search filter is used to determine what constitutes a user for this LDAP server. Enter <code>(objectclass=people)</code>
User Description Attribute	(Optional) An attribute used to identify a user description in SilverStream. The name you enter is the LDAP attribute to which you want to map the description. For example: <code>title</code>
Additional Attributes	Select All if you want all of the specified LDAP user attributes to be listed in SilverStream. Select None if you want no additional attributes to appear. The specified attributes will be displayed in a tab when you select a user in the Users & Groups panel and open the Property Inspector.
Full Name	(Required) Specifies the full name attribute, if available. Enter <code>cn</code>

9. Click **Finish**.

The SMC displays the settings under the LDAP directory. You can access the new settings anytime by selecting **Users& Groups** in the Security options in the SMC.

The following steps will set up an "alias" for the users' distinguish name (DN). The users will only have to enter their common name as their login name instead of their full DN.

▶▶**To override the defaults for login name components:**

1. Invoke the SMC.
2. Select **Security** options.
3. Select the **Server Security** panel.
4. Specify the default realm and the default authority.

Field	Description
Default Security Realm	Defines the security realm for any login name that does not explicitly define a realm. Choose LDAP from the drop down list.
Default Security Authority	Choose the <i>server name</i> that was created earlier. (eg. directory.us.army.mil)

5. A full login name can always be specified, in which case the defaults are ignored.

4.6 Connect Using Apache 1.3.14

The following components and libraries are required to implement LDAP based authentication in Apache:

- *OpenLDAP* version 1.2.11 libraries from <http://www.openldap.org/>, or *Netscape Directory C SDK* libraries from <http://www.mozilla.org/directory>
- Apache LDAP authentication module, *mod_auth_ldap* version 1.5, authored by Muhammad A. Muquit, and referenced on <http://modules.apache.org/>

Apache's core set of modules does not include an LDAP based authentication capability, therefore it is necessary to acquire a third party module and compile/link it with Apache. There are more than 5 modules available on the Apache Modules server (<http://modules.apache.org/>), however the particular module that is recommended above, was based upon its relative currency and the positive feedback from members within the Apache developer's community.

There are two options to choose from when installing the *mod_auth_ldap* module within Apache: static compilation, or linked as a dynamically static object (DSO). Specific directions applying to each option are present within the module's installation files.

Acquire the archive files containing the *mod_auth_ldap* module and the *OpenLDAP* libraries from their respective web sites (note: *Netscape Directory C SDK* libraries can be substituted in place of the *OpenLDAP* libraries). Follow the directions contained within each archive file and install/compile them within the operating system. After this process is completed; static or dynamic libraries will be created that will allow the installation of *mod_auth_ldap* into the Apache environment.

NOTE: The AKO Directory Server is accessible using LDAP over SSL exclusively. The *LDAP_Port* must be set to 636 and the SSL version of the *Netscape Directory C SDK* libraries must be used in compiling *mod_auth_ldap*.

Apache installation directions for the *mod_auth_ldap* module are dependent upon a static or dynamic library; follow the specific directions for the type of environment Apache was compiled to.

After Apache successfully recognizes *mod_auth_ldap*, configure your *httpd.conf* or *.htaccess* files according to the directive template below:

```
<Directory />
AuthType Basic
LDAP_Server directory.us.army.mil
LDAP_Port 636
BASE_DN "ou=people,ou=army,ou=dod,o=u.s. government,c=us"
UID_Attr cn
</Directory>
```

4.7 Connect Using BEA WebLogic

To connect BEA WebLogic to the AKO Directory, configure the web server (eg, iPlanet) to connect to the AKO Directory as discussed in the sections above. The web server will provide user authentication, identification, and session management. The BEA WebLogic web "listener" will pick up the REMOTE_USER CGI environment variable, which will hold the user's Distinguished Name:

```
String remote_user_DN = request.getRemoteUser();
```

The DN can then be used within a BEA WebLogic application for additional LDAP queries, and for comparison with access control lists.

To connect to the AKO Directory from the application server, you will need to install the JSSE package, which enables the cryptographic mechanism for SSL, into your SDK's lib directory if you are using SDK version lower than 1.4 . The "java.security" file will need to be modified to include the Provider.

Single Sign-On

Install and configure the Netegrity module. Netegrity populates the user header with an "SM_USER" variable. BEA's web "listener" will pick up the SM_USER header variable, which will hold the user's Common Name, or the SM_USERDN header variable, which will hold the user's Distinguished Name. If user attributes look-ups are required, legacy code will need to be modified to use these variables instead of the REMOTE_USER variable that is used when LDAP authentication is implemented with the iPlanet web server.

Code example:

```
String username = request.getHeader(SM_USER);  
String userDN = request.getHeader(SM_USERDN);
```

Retrieving AKO Attributes Using Java Within Weblogic 6.1

Accessing AKO Directory attributes, using Java, from within Weblogic 6.1 (servlet or EJB) requires three changes to the Weblogic environment. These changes are necessary to allow Java to connect to the AKO Directory using secure ldap.

The first step is to add the appropriate DoD root certificate authorities to the Java 1.3 trusted certificate file. The second step is to change the default security provider for Weblogic's version of Java. The third step is to modify Weblogic's startup scripts to include the libraries for the correct Java security provider.

Assumptions:

- Weblogic is running on Windows. Unix path names and extensions will differ.
- These directions assume C:\bea as the Weblogic 6.1 installation directory.

- These directions assume that the standard Sun Java ldap libraries will be used to accesses AKO. These directions may not work for the Netscape ldap libraries.

Updating the Java Trusted Certificate Store:

1. The certificates are posted in the Army Knowledge Collaboration Center, in the folder

Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) / AKO Interface Control Document/Certificates

Download the following files:

- a. [dod_class3_root_cer](#)
- b. [DISA_CA4_root_cer](#)

2. Execute the following commands:

- a. `keytool -import -alias "DoD Class 3 Root CA" -file dodclass3root.cer -keystore C:\bea\jdk131\jre\lib\security\cacerts`
- b. `keytool -import -alias "DOD CLASS 3 CA4" -file dodca4.cer -keystore C:\bea\jdk131\jre\lib\security\cacerts`

Note: The password is “changeit”

Changing the Java Default Security Provider:

1. Edit the java security properties file C:\bea\jdk131\jre\lib\security\java.security

- a. Find the following section:

security.provider.1=sun.security.provider.Sun
security.provider.2=com.sun.rsa.jca.Provider

- b. Modify the section as follows:

security.provider.1=com.sun.net.ssl.internal.ssl.Provider
security.provider.2=sun.security.provider.Sun
security.provider.3=com.sun.rsa.jca.Provider

Modify the Weblogic Startup Script:

1. Download the following packages from Sun (<http://www.javasoft.com>):

- a. JSSE 1.0.3_01

This package contains three required library files; jcert.jar, jnet.jar and jsse.jar

- b. JCE 1.2

This package contains a required library file called jce1_2-do.jar

c. JAAS 1.0

This package contains a required library file called jaas.jar

Note: If later versions of these packages are used, the library names may be different.

2. Edit the Weblogic startup script. This file is usually called startWebLogic.cmd.
 - a. Find the line starting with:
set CLASSPATH=
 - b. Modify the line by adding the following libraries at the beginning of the classpath:
jaas.jar, jce1_2-do.jar, jcert.jar, jnet.jar, and jsse.jar

4.8 Connect Using ATG Dynamo

To connect ATG Dynamo to the AKO Directory, configure the web server (eg, iPlanet) to connect to the AKO Directory as discussed in the sections above. The web server will provide user authentication, identification, and session management. If user authentication against the AKO directory is all that is required, no further action is needed.

For additional LDAP functionality and for using the user identity in access control, the ATG Dynamo Personalization Server is needed. Rather than performing the authentication test that is included in the ProfileFormHandler, the ProfileFormHandler must be modified to pick up the remote_user CGI environment variable, which will hold the user's Distinguished Name:

```
String remote_user_DN = request.getRemoteUser();
```

If using Netegrity Single Sign-On, instead of the iPlanet Remote_User variable, one instead uses SM_USERDN, which holds the user's Distinguished Name, or SM_USER, which holds the user's Common Name:

```
String username = request.getHeader(SM_USER);
```

```
String userDN = request.getHeader(SM_USERDN);
```

This DN can then be used within the ATG Dynamo user Profile and from applications for additional LDAP queries, and for comparison with access control lists. The AKO Directory specific Properties for configuring the Profile Repository Object to connect to the AKO Directory for additional LDAP queries are provided:

InitialContextEnvironment.properties should include:

```
providerURL=ldap://directory.us.army.mil:636
```

```
securityCredentials=<your server's password>
```

```
securityPrincipal=cn\=<your ServerID>
```

ldapArmyProfile.xml should include:

```
<search-root dn="ou=DoD,o=u.s. government,c=us"/>
```

To connect to the AKO Directory from the application server, you will need to install the JSSE package, which enables the cryptographic mechanism for SSL, into your SDK's lib directory if you are using SDK version lower than 1.4 . The "java.security" file will need to be modified to include the Provider.

4.9 Connect Using Cognos

To connect Cognos to the AKO Directory, configure the web server (eg, iPlanet) to connect to the AKO Directory as discussed in the sections above. The web server will provide user authentication, identification, and session management. The Cognos web "listener" will pick up the Remote_User CGI environment variable, which will hold the user's Distinguished Name. The DN can then be used within Cognos for comparison with access control lists.

Details on the necessary modifications to Cognos to implement this are in development.

4.10 Connect Using ColdFusion

ColdFusion is a popular development and application server product set. It connects to an Enterprise LDAP Directory Server using CFLDAP tags that implement LDAP commands. Sample code for a Custom Tag for versions 4.5 and above have been posted in the AKCC in the folder:

Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) / AKO Interface Control Document

ColdFusion 4.x requires that the SSL certificate target server (the AKO Directory) be loaded into a cert7.db file. This file is the certificate keyfile for the Netscape web browser. To import the certificate, point the Netscape browser at:

<https://directory.us.army.mil:636>

Use the certificate wizard to "Accept this certificate forever (until it expires)".

ColdFusion MX no longer uses the Netscape Cert7 format certificate store file (cert7.db) to make a secure LDAP (SSL v2) connection. cfdap SSL support in ColdFusion MX now uses Java Secure Socket Extension (JSSE), and JSSE does not accept cert7.db as a keystore.

Therefore, one can omit the second token of the string for the *secure* attribute of the *cfdap* tag that was formally used to specify the location of the cert7.db file. Instead, use SECURE="CFSSL_BASIC" to indicate an encrypted LDAP connection

The simplest way to import to the client's keystore is to use the keytool command to import the server's cert into the cacerts store in /jre/lib/security. For example, enter the following:

```
keytool -import -keystore cacerts -alias ldap -file ldap.crt
```

(The keytool utility is in the jre/bin directory and the initial password is "change it"). The certificate must be in X.509 format.

At this point, restart the ColdFusion MX server.

Single Sign-On with ColdFusion

There is no web agent that interfaces with the native ColdFusion web server. However, ColdFusion can be configured to run under the Microsoft IIS web server. The web agent for IIS will protect the server from unauthenticated users, and will populate the header variables `SM_USER` and `SM_USERDN`. These header variables, which contain the user's unique AKO identity, can be read by ColdFusion applications and used programmatically for access control.

Alternatively, ColdFusion can access the IIS server variable `REMOTE_USER`. One must modify the Registry to cause the Web Agent to set this variable:

Add a new `DWORD` value called `SetRemoteUser`. Create this value in the registry in the location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder
WebAgent\Microsoft IIS
```

To enable, set the value to 1. To disable `SetRemoteUser`, set the value to 0.

In the Directory Security tab of the Microsoft Management Console, configure the Anonymous Access and Authentication Control settings as follows:

- Select Basic Authentication and Allow Anonymous Access
- Deselect Windows NT Challenge/Response. This authentication method prohibits the IIS Web Agent from setting the `REMOTE_USER` variable. Even if the IIS Web Agent does not set `REMOTE_USER`, it may still be set by the Web server, based on values that the browser supplies.

4.11 Connect Using Xerox DocuShare 2.x

Xerox DocuShare is a document scanning, management, and .electronic records system that enables web access to files.

Using the LDAP extension, a DocuShare user account is created automatically when a user first logs in to the server using his or her LDAP user name and password.

DocuShare validates the user name and password by accessing the LDAP directory service and, if the credentials are valid, DocuShare allows the user to log in under that LDAP user name. If the user name and password are invalid, the login fails.

Note: Two accounts, **Guest** and **admin**, are created automatically when DocuShare is installed and do not use the LDAP directory service. To restrict access so that no unauthenticated users can access any content, restrict access so that **Guest** cannot access any content.

Subsequent logins use the automatically created DocuShare user account, which is stored locally, and synchronize the local data with that on the LDAP directory server. However, the LDAP password is not stored locally. Therefore, if LDAP is later disabled, all local user accounts based on LDAP accounts will not be accessible until the local password is changed to a new value.

DocuShare user accounts have a number of properties that are stored in the user account database: first name, last name, mailstop, phone, email, email format, Upload Helper setting, homepage, username and password. Likewise, a user account in the LDAP directory service has several properties that are stored in the LDAP user account database. When a DocuShare user account is created automatically, some of the properties are obtained from the LDAP user account and are set in the new local user account. The properties that are configurable and are given default values include: First Name, Last Name, Phone, Email and username. The username must remain the same as the LDAP username and therefore cannot be changed. The password is set to a special private password and also cannot be changed when LDAP is enabled. Any remaining properties are set to the DocuShare default values. Users cannot edit the properties that are obtained from their LDAP user accounts.

DocuShare groups are created automatically and the group members are the same as those on the LDAP directory server. When groups are enabled and a user logs in, DocuShare creates a local group, if it does not already exist, and adds the user as a member of the group. If the user is later removed from the LDAP group, he or she is automatically removed from the DocuShare group.

AKO has implemented LDAP over SSL is to be enabled. A Netscape browser, version 4.x (not 6.x) must be installed on the same server as DocuShare. To obtain the LDAP server site certificate.

1. Launch the Netscape browser that must be installed on the DocuShare server.
2. Enter the URL to the LDAP server `https://directory.us.army.mil:636/` into the the browser. (You **MUST** include the `https`, or your browser will not attempt to negotiate an encrypted session.)
3. If a certificate for the LDAP server (or it's Trusted Root) has not already been accepted on the DocuShare server, then a user interface will be presented to accept the new site certificate.
4. Click **Next** after you have read the information.
5. The user interface displays a description of the certification. Feel free to view the **More Info...** Click **Next** when you have read the information.
6. Click the button next to **Accept this certificate forever (until it expires)** and click **Next**.
7. Leave the **Warn me before I send information to this site** check box blank and then click **Next**.
8. Click **Finish**.

For Solaris systems, permissions for **nobody** must be granted to the certificate database to allow DocuShare to access the certificate when communicating with the LDAP server. This can be accomplished in one of three ways:

- Change the ownership of the certificate database (typically `/.netscape/cert7.db`) and its parent directory to **nobody**. For example, execute the following:

```
chown nobody /.netscape; chown nobody /.netscape/cert7.db
```

- Give read / write permission to the organization for the certificate database and its parent directory. For example, execute the following:

```
chmod o+rw /.netscape; chmod o+rw /.netscape/cert7.db
```

- Relocate the cert7.db file to the DocuShare bin directory and change the ownership of the copy of the file to **nobody**. Further additions of certificates will not be added to the copy of cert7.db. Nor will that copy of the certificate be refreshed when the certificate expires and a new certificate needs to be accepted.

Enabling LDAP

LDAP is initially disabled. To enable LDAP:

1. Log in to DocuShare as admin. Go to the Administration area.
2. In the **Server Configuration** section, go to the **LDAP Parameters** page. This page consists of three areas: Enable LDAP, Configure LDAP Connection, and Test LDAP Connection.
3. Select **Yes** next to **Enable LDAP**. Click **Update Properties**. LDAP is now enabled.

Although enabled, LDAP must be configured before DocuShare will become operational.

Configuring LDAP

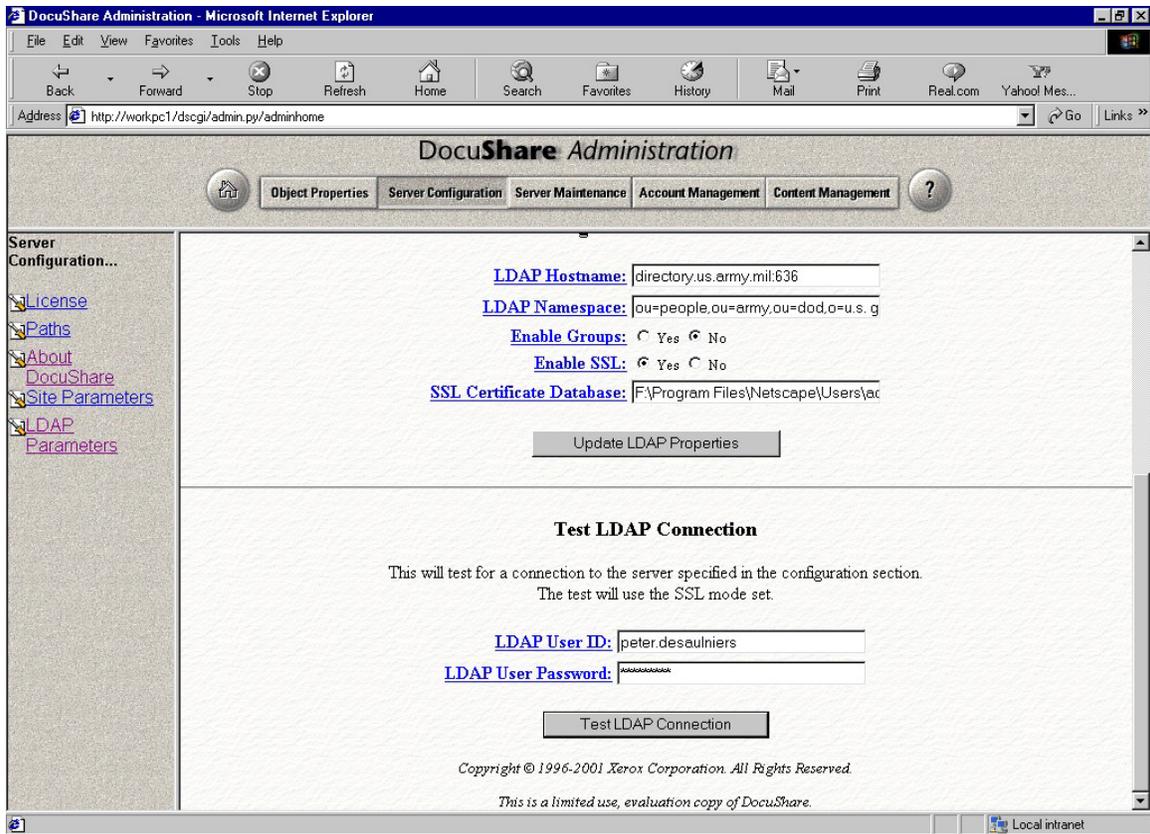
To configure LDAP:

1. In the **LDAP Hostname** field: enter the fully qualified host name for the LDAP server:
`directory.us.army.mil`
2. In the **LDAP Namespace** field: enter the attributes that describe the LDAP namespace containing the users and groups that are to be used by DocuShare.
`ou=people,ou=army,ou=dod,o=u.s. government,c=us`
3. To enable DocuShare to automatically manage groups, select **Yes** next to **Enable Groups**.

To enable and configure SSL-enabled LDAP:

1. Select **Yes** next to **Enable SSL**.
2. In the **SSL Certificate Database** field: enter the file system path to the local certificate database, cert7.db. Do not put quotes around this entry even if the entry contains spaces.
`Example(NT): c:\program files\netscape\users\default\cert7.db`
`Example(Unix): /.netscape/cert7.db`
3. Click **Update LDAP Properties**. This configuration information is now stored in the DocuShare configuration database.

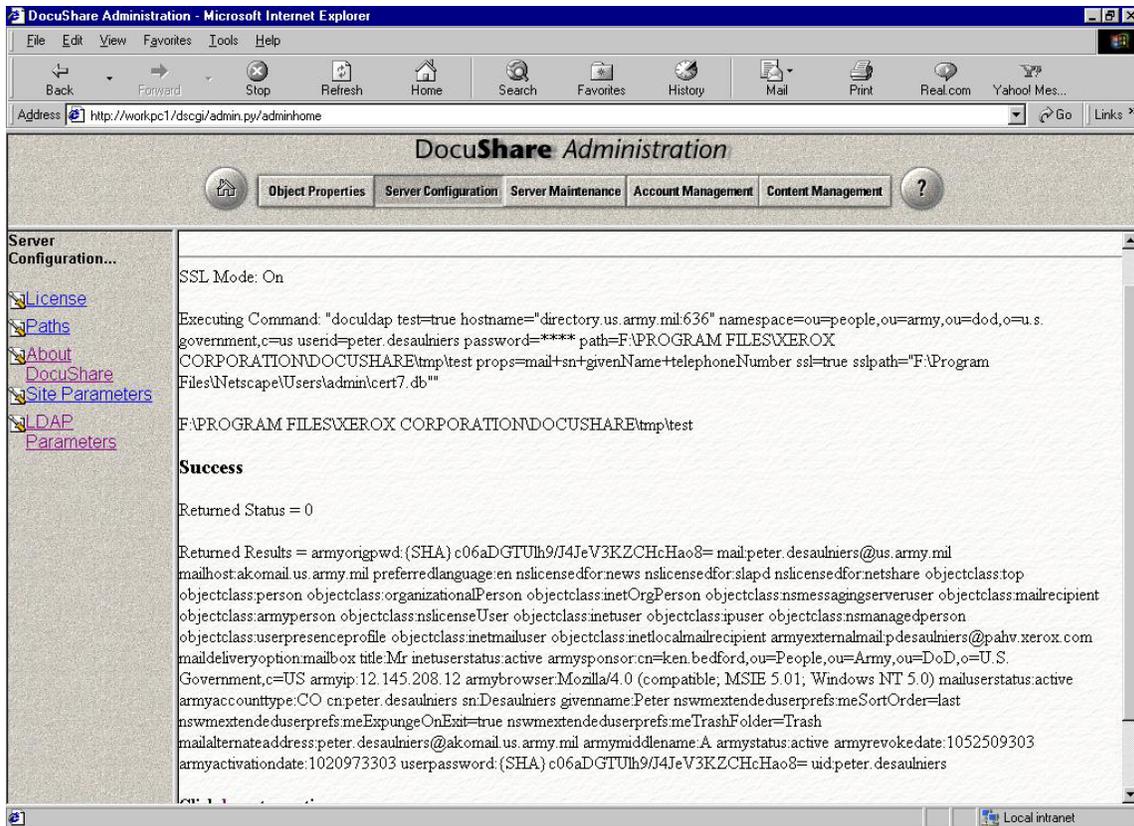
The LDAP-enabled DocuShare should now be operational. To verify that it is, use the **Test LDAP Connection** feature.



Testing Connection

To test the LDAP connection:

1. In the **LDAP User ID** field: enter a valid AKO user name.
2. In the **LDAP User Password** field: enter the password for this user.
3. Click **Test LDAP Connection**. An **LDAP Test Results** page displays. This page contains the following information:
 - **SSL mode**: indicates whether SSL was enabled or not.
 - **Executing command**: shows the detailed parameters given to the doculdap command that was executed to perform the test.
 - **Path to the file containing the LDAP data returned from the command**. The file will be named **test** as opposed to the user name for normal operation.
 - **Result of the test**: either **Success** or **Failed**.
 - **Returned Status**: the numeric value of the status returned from the doculdap command. Zero is success, all others are failure.
 - **Returned Results**: a list of attributes returned as the result of a test search in the LDAP data file.
4. Click to continue to the LDAP Parameters page



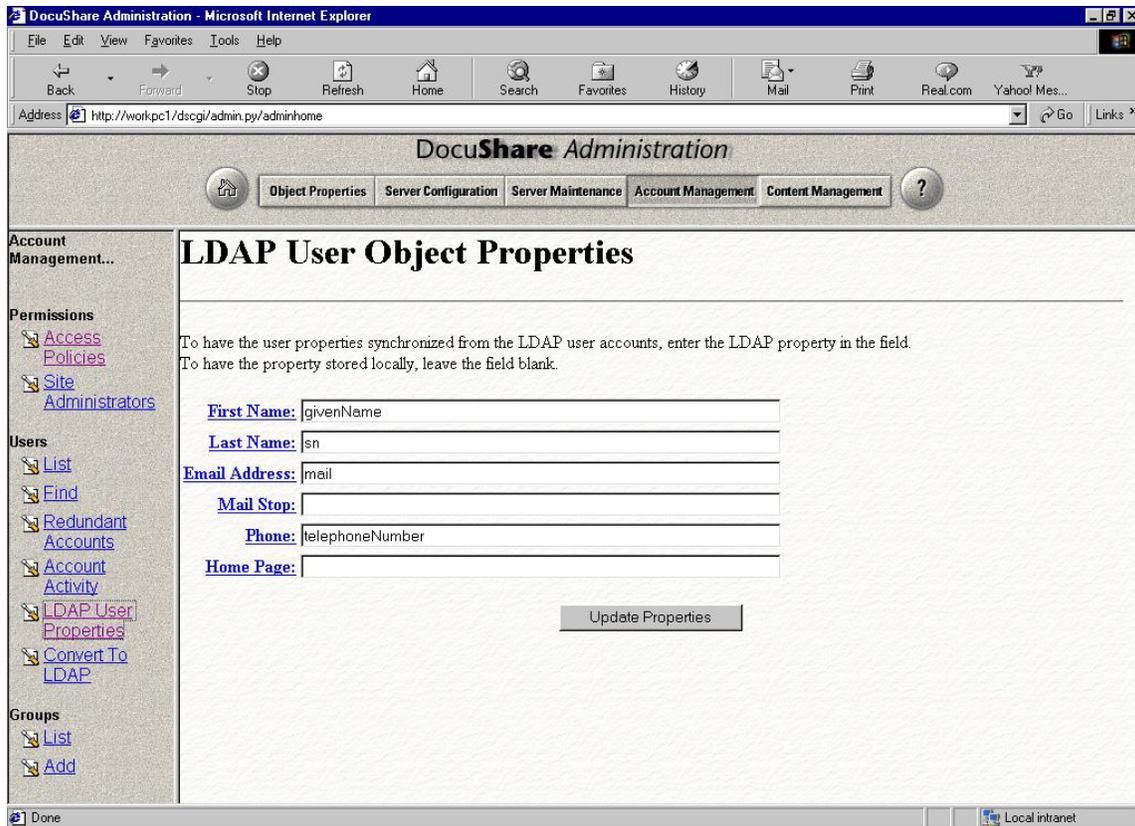
Configuring DocuShare User Properties

The LDAP-driven user properties are synchronized with the current values on the LDAP directory service each time the user logs in to his or her account on DocuShare. The transfer of data is one way, from LDAP to DocuShare only. The LDAP extension does not support the writing back of data to LDAP.

For this version, only properties that have values that are of type *string* are supported. All properties in the AKO Directory, except "telephonenumber" are of type *string*.

To configure the DocuShare User Properties:

1. In the **Account Management** section of the DocuShare Administration area, click the **LDAP User Properties** link. The **LDAP User Object Properties** page displays.
2. For each DocuShare user object properties that will have its data synchronized with a corresponding LDAP property, enter the distinguished name of the LDAP property. For example, enter **givenName** for the user's first name properties or **sn** for the user's last name property. The AKO person object attributes is included in this ICD as Section 5.1.
3. For each DocuShare user object property that will have its data stored locally, either leave the field blank or remove any entry that presently exists.
4. Click **Update Properties**.



Pre-loading multiple LDAP user accounts into DocuShare

Since user accounts are normally created only when a user first logs in, this may not satisfy the need to initially populate the DocuShare server with LDAP-based user accounts. An alternative to the normal method would be to use DocuShare's account creation capabilities to initially create all the LDAP-driven user accounts that will be used on the DocuShare server. Once created, then the user's access permissions and object ownership may be established, even prior to the first login by the user.

To pre-load user accounts into DocuShare:

1. Log in to DocuShare as **admin**.
2. In the **Server Configuration** section of the Administration area, disable LDAP.
3. In the **Account Management** section of the Administration area, use the **Add** link under **Users** to add each new DocuShare user account. The user's last name, user name and password are required entries when creating DocuShare user accounts.
4. The DocuShare user name must be set to the exact spelling of the user name (e.g. CN) for the corresponding LDAP account. The user name must be entered entirely in lower case regardless of how it exists in the corresponding LDAP user account.

5. Any value for the user's password may be entered since it will be reset to an internal password when the account is converted to LDAP later.
6. Enter any useful value for the last name since it will be synchronized to the actual corresponding LDAP value the first time the user logs in to DocuShare with LDAP enabled.
7. When all of the new DocuShare accounts have been added, re-enable LDAP
8. To complete the process, use the **Convert to LDAP** feature to convert each newly added DocuShare account to an LDAP-driven DocuShare user account.

4.12 Connect Using Xerox DocuShare 3.x

Xerox DocuShare is a document scanning, management, and electronic records system that enables web access to files.

The LDAP Configuration page is used to establish the connection to the LDAP server and define the root for the branches that will be identified as DocuShare External Domains.

Login to DocuShare with Site Administrator access and navigate to the Admin Home site. Expand the menu for Account Management and then LDAP Accounts. Select Configuration under the LDAP Accounts menu to display the LDAP Configuration page.

Administration Main Menu Page - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print Mail

Address http://192.129.67.37/docushare/jsp/admin/Main.jsp Go Links

Administration Menu

- Object Properties
- Account Management
 - Access Policies
 - Users
 - Groups
 - Domains
 - LDAP Accounts
 - Configuration**
 - Add
 - Convert
 - Rename
 - Synchronize
 - Bind User
 - Bind Group
 - Providers
- Services
- Content Management
- Site Management
- Admin UI Configuration

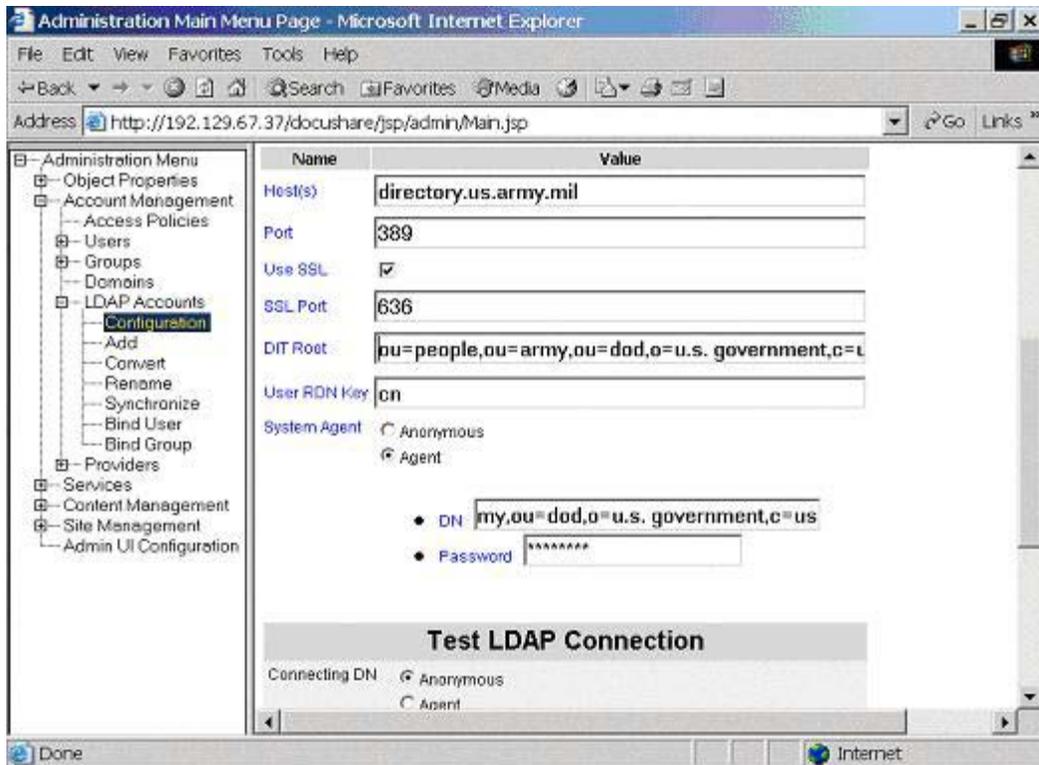
Test Status = Success.

LDAP Configuration

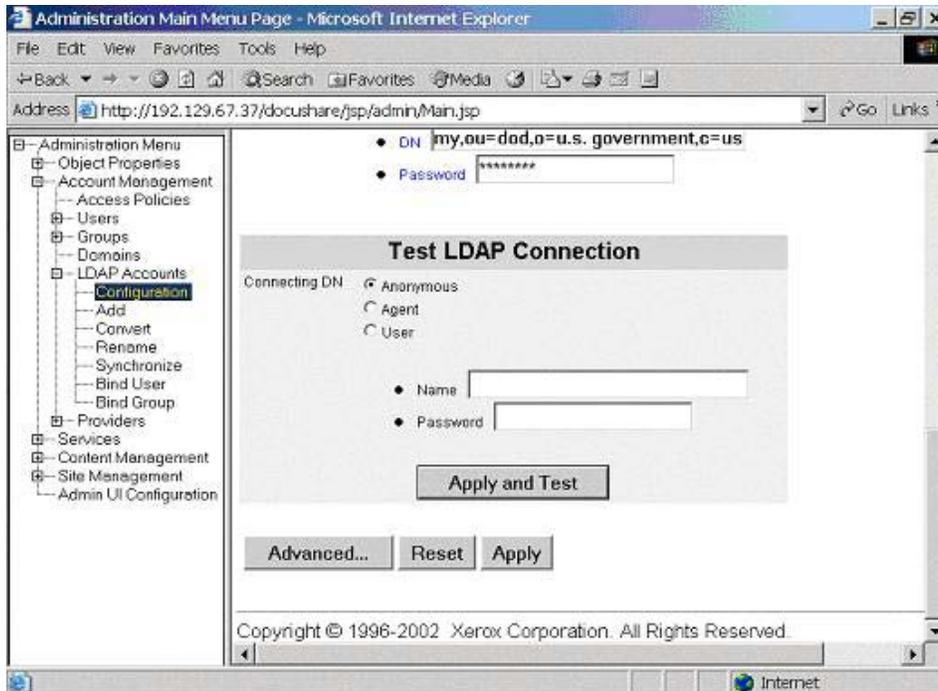
- Use this page to configure this site so it can communicate with an external server.
- When you have completed configuration, click **Apply**.
- Although not required for normal operation, you may include additional information in your LDAP configuration by clicking **Advanced** and filling in the Advanced information fields.
- Test the communication link between this site and the LDAP server by filling fields under Test LDAP Connection and clicking **Test**.

Name	Value
Host(s)	directory.us.army.mil
Port	389
Use SSL	<input checked="" type="checkbox"/>
SSL Port	636

Done Internet

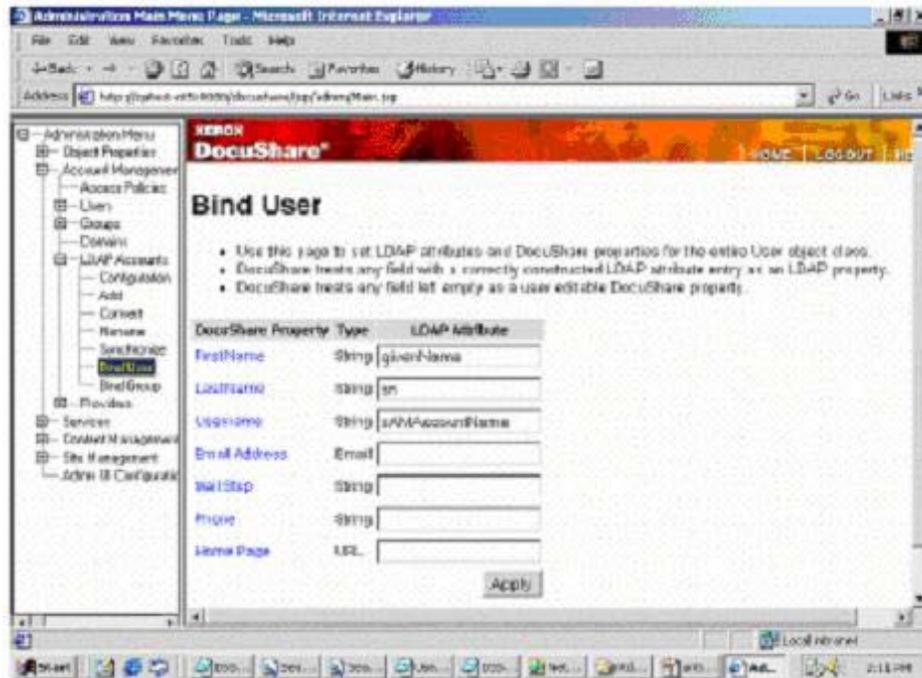


- Host(s) – The AKO Directory Server Host Name or IP Address is:
directory.us.army.mil
- Separate multiple LDAP servers with a space character.
- Port – The port used by the LDAP server – leave as the default of 389.
- Use SSL – this must be checked
- SSL Port – The port used for SSL – leave as the default of 636.
- DIT Root – This is in the form of a Distinguished Name (DN). Enter:
ou=army,ou=dod,ou=u.s.government,c=us
- User RDN Key – enter CN (for Common Name).



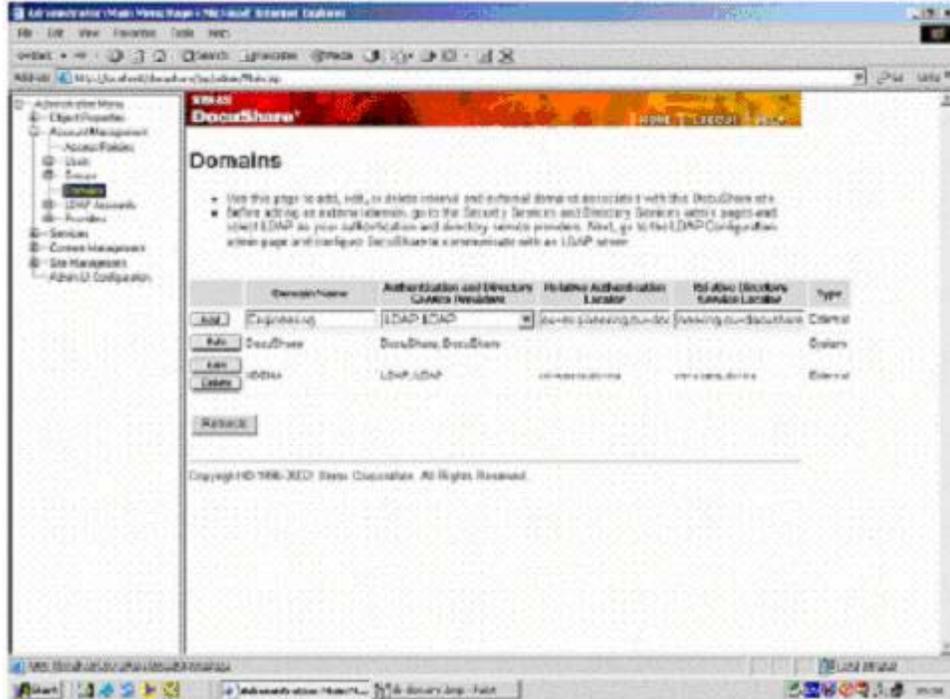
- System Agent – "agent" must be selected
- DN - An LDAP account name, in the form of a DN, that has been assigned by AKO to your application server (the "ServerID").
- System Agent Password – Login password for your application's ServerID account.

The **Bind User** page establishes the LDAP attributes that contains the values associated with a DocuShare user properties.



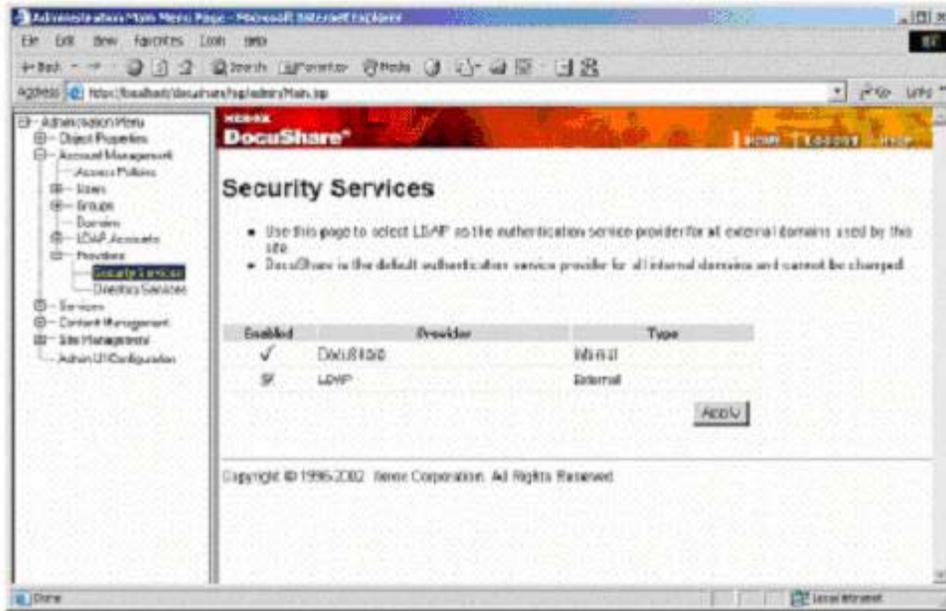
- Name – Use the attribute for a person’s first name. This is givenName.
- Last Name – Use the attribute for a person’s last name. This is sn or surname.
- Username – Use the attribute for the person’s login name. This is cn or common name.
- The remaining attributes are optional.

The **Domains** page is used to define one or more external Domains. Each DocuShare External Domain represents a branch in the LDAP directory tree that contains a collection of users and groups who will have DocuShare accounts. DocuShare 3.0 supports only LDAP for Authentication and Directory services. The values for Relative Authentication Locator and Relative Directory Service Locator will be the same.



- Domain Name – Administrator defined name to identify the DocuShare External Domain
- Relative Authentication Locator – One or more attribute data pairs used to define the path to the directory location containing the user and group entries for the DocuShare External Domain. Use the components of the DN that are right of the users RDN and left of the DIT Root. Enter:
"ou=people"
- Relative Directory Service Locator – One or more attribute data pairs. In DocuShare 3.0 this is the same text string used for the Relative Authentication Locator. Enter:
"ou=people"

The **Security Services** page is used to enable LDAP Providers. This will allow users to select the LDAP External Domains from the Domains drop down list at the Login prompts.



DocuShare's LDAP and SSL

With SSL, servers and/or clients use certificates to provide proof of identity prior to establishing a secure connection. The certificate also contains public and private keys that are used to establish the session. Session keys are used to encrypt the data before sending and to decrypt data received.

The certificates for the AKO Directory Server are posted in the AKO Knowledge Collaboration Center in the folder:

Army Communities / Army CIO/G-6 / AKM / Goal 4 (AKO) /

AKO Interface Control Document/Certificates

or you can search the AKCC for <ako icd> and select the folder.

Copy the .cer formatted certificate for the Directory Server (directory_server_cert.cer) to the directory containing the DSTrustStore file

```
<ds3_install-dir>\jdk1.3.1\jre\lib\security
```

Open a command prompt window and navigate to the directory containing the DSTrustStore.

The keytool utility is used to place the SSL certificate into the DSTrustStore. It needs to be executed from the directory containing both the certificate file (.cer) and the dstruststore file.

DocuShare 3.0 does not set the PATH environment variable to include the directory containing the keytool utility. You will need to set the PATH variable so the system will find keytool. At the command prompt use the "set PATH" command to set the variable.

```
set PATH=%PATH%;<ds3_install-dir>\jdk1.3.1\bin
```

You may now import the certificate file into the DSTrustStore using the keytool command. At the prompt run the keytool utility using the `-import` argument.

```
keytool -import -alias <alias_name> -file <cert_file> -keystore  
dstruststore
```

Replace `<alias_name>` with a unique alias name for the certificate file.

Replace `<cert_file>` with the name of the certificate file (.cer) you exported and copied to the directory containing the dstruststore file.

Immediately after starting the keytool you will be prompted for a password. Type “password” for the password. When keytool completes, examine the message output to ensure the certificate was successfully added to the keystore.

4.13 Connect Using Netegrity SiteMinder for Single Sign-On

Single Sign-On is available to authenticate and identify users for most web and application server COTS products. Note that user attribute look-ups still require an LDAP connection from the application server to the AKO Directory server to enable those transactions.

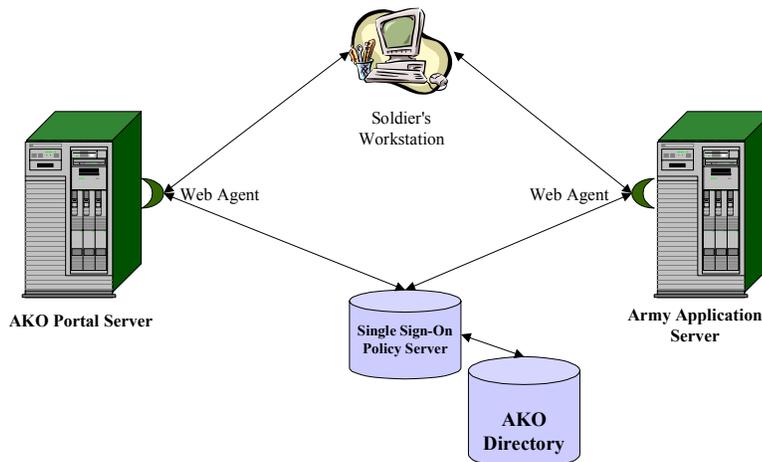
To request access to the web agents required to interface to AKO's single sign-on, complete the request form located at:

https://www.us.army.mil/portal/jhtml/reference/request_index.jhtml

After approval, you will be granted access to a folder in the AKO Knowledge Collaboration Center that contains documentation on Netegrity SiteMinder and the Web Agents for deployment onto the application servers.

How Single Sign-On works

AKO has stood up a Policy Server to manage user sessions across geographically distributed Army web application servers. Each web application server has a "web agent" deployed onto that server and configured to communicate with the AKO Policy Server. When a user first logs on to an Army web application server, the user is challenged for their userid and password. The web agent sets a session cookie in the user's browser, and also sets a corresponding record in the Policy Server. While the user session remains active, the web agent on any Army web application server to which the user navigates will intercept the user's requests, verify the session cookie and the user's permissions against the Policy Server, and allow (or deny) the user access to that web application server.



For Single Sign-On implementation:

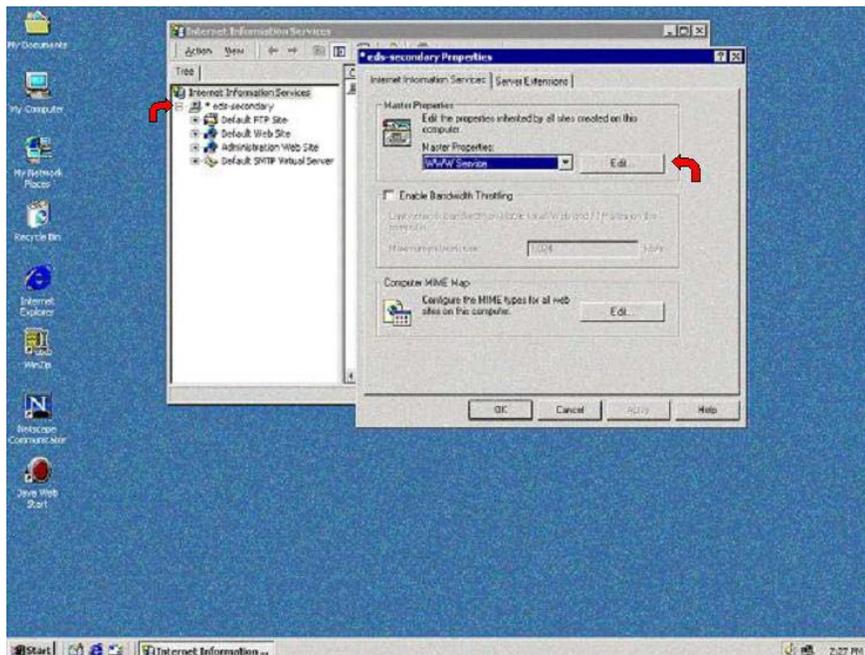
- all Web Servers must have a DNS entry. The configuration is transparent for *.army.mil DNS entries, but can be made to work with other extensions.
- Include all of the AKO Policy Servers in a "round robin" in the configuration of the Web Agent. The IP addresses are:
 - 140.183.234.247
 - 140.183.234.107
 - 140.183.234.158
- firewalls must be opened for *requests* FROM the Web Server TO the AKO Policy Servers, and for *responses* FROM the AKO Policy Servers TO the Web Server for **Ports 44441,44442, 44443**.
 - The Netegrity Web Agent is tied to the Web Server, not to the operating system. Therefore, use the IP addresses of the Web Servers. If you are protecting one web site, then you need just its IP. If you are protecting multiple web sites on a single physical server, then you need all the IPs for all the web sites plus the IP of physical server.
 - For load balanced web sites, you need the IP addresses of all of the (eg, 3) Web Servers - not the IP address of the switch. Note that this means that each web server needs it's own "real" IP (if they have a 10.10.10.x IP, then those need to be translated by the switch to a "real" IP).

4.14 Installing and Configuring the SSO Web Agent on Windows and IIS

Important Note: One MUST configure the IIS web server to run the SSL filter first. If you are running several virtual web servers in a single instance of IIS, then you must check the properties of each individual virtual web server, and also of the top-level IIS web server. If you do not implement SSL for all virtual web servers, then the SSL filter is NOT placed first by "default", and userid/password requests may be transmitted "in the clear" from the user to your web server.

To ensure that your SSL filter runs first on you IIS Sever, these are the steps you must take to configure the filters so that the SSL filter runs first.

- Go to the Internet Services Manager
- Right click on the web server, select Properties
- Select WWW Service in the Master Properties and the select the edit button.



- Select the ISAPI Filters Tab
- Make sure the **sspifilt** filter is first in the list

To move the **sspifilt** to the top, use the up and down arrow tabs on the left side of the screen.

- Then click the apply button
- Click OK

Configuring the Web Agent for IIS

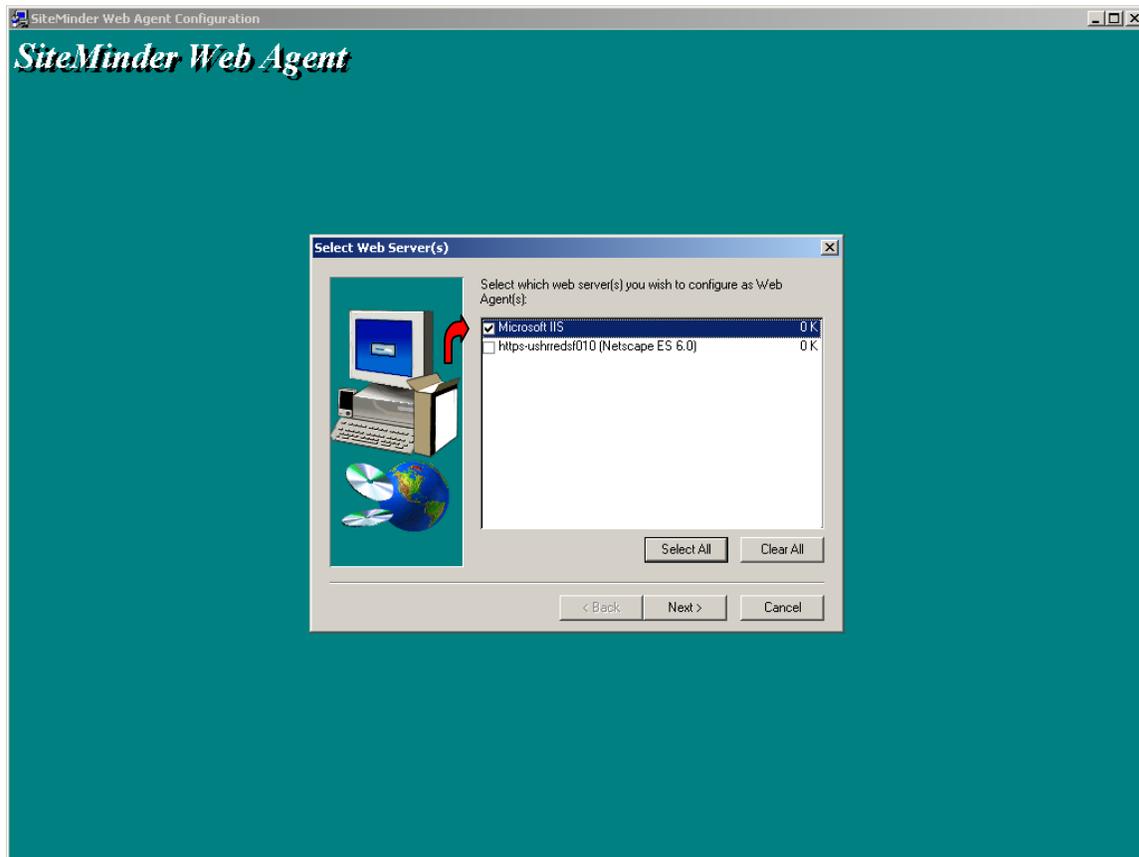
After you have a Web Agent installed, you must configure the Web Agent. SiteMinder Web Agents installed on IIS Web servers are automatically configured as forms credential collectors and SSL credential collectors. Additionally, IIS Web Agents can be configured as cookie providers.

1. If necessary, open the Web Agent Configuration Wizard by selecting:

Programs | SiteMinder | Web Agent Configuration Wizard from the Windows **Start** menu.

If you indicated that you wanted to configure the Web Agent after the installation, SiteMinder automatically opens the Web Agent Configuration Wizard for you.

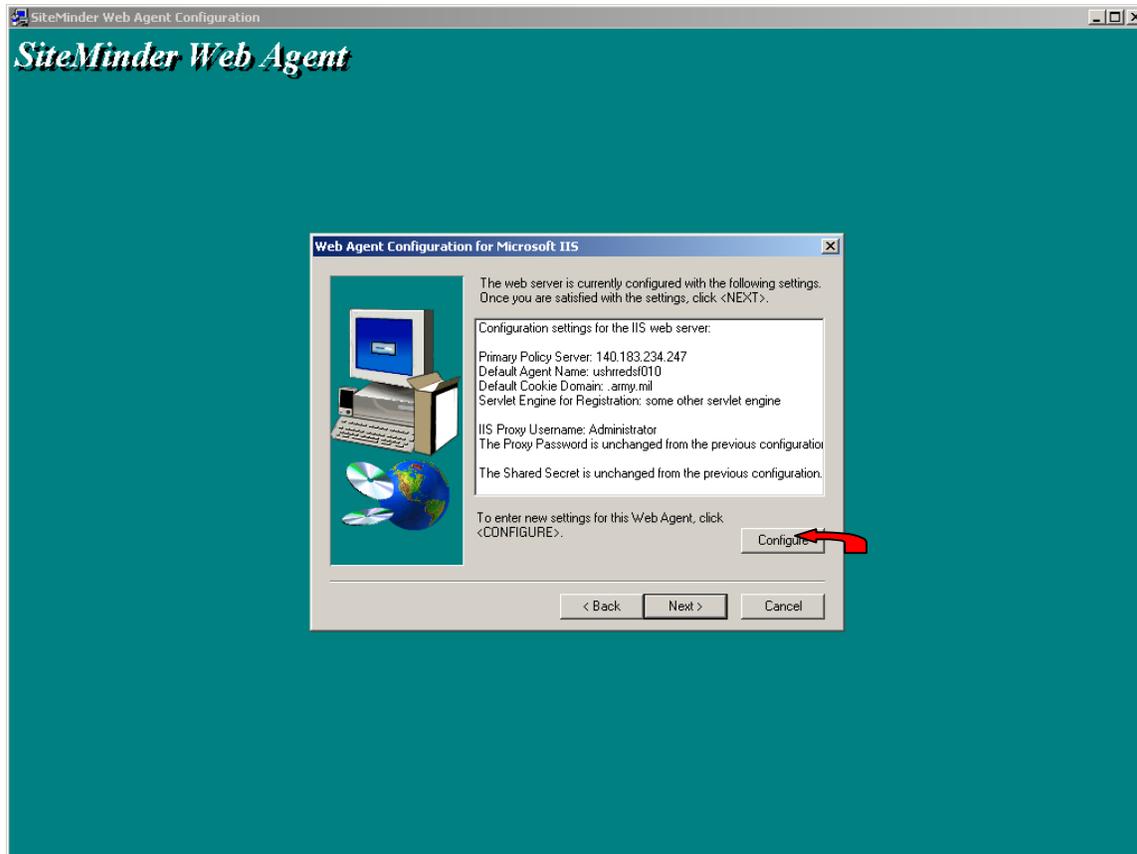
2. In the Select Web Server dialog box, select the Web server(s) that you want to configure as Web Agents, then click **Next**.



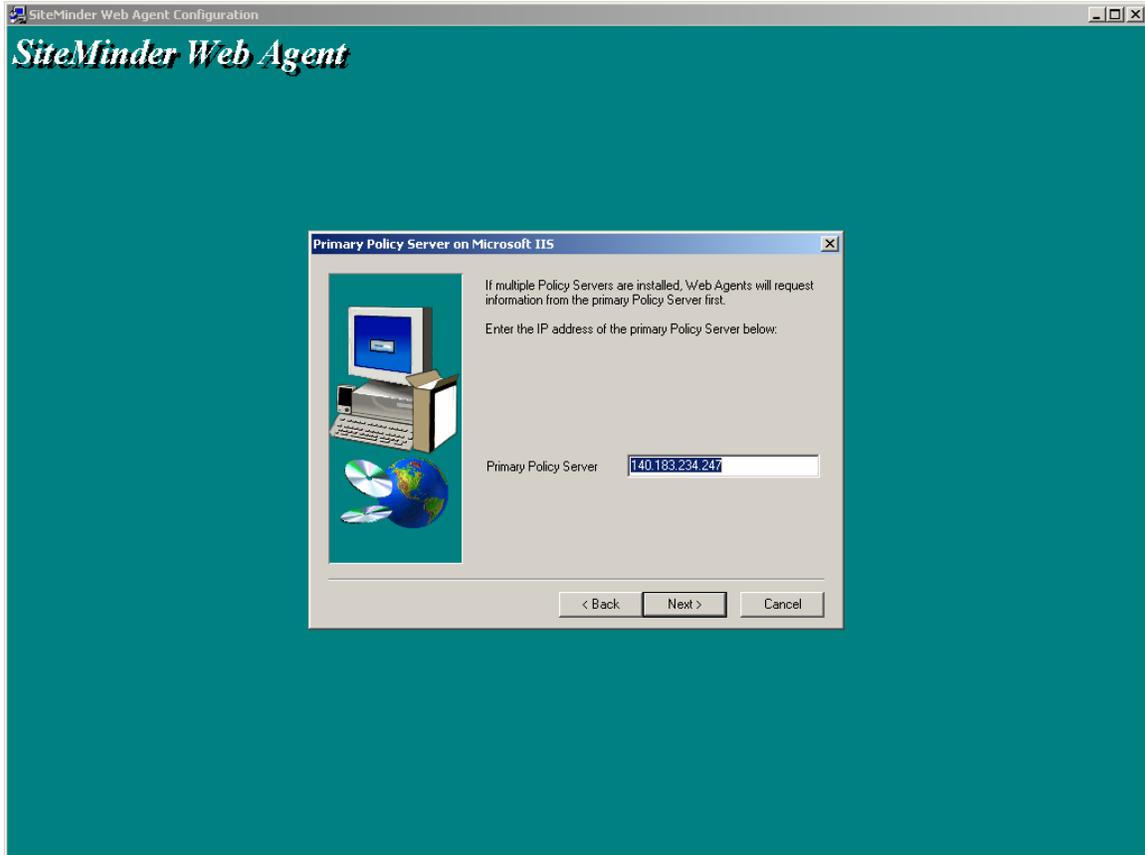
If you select multiple Web servers, the configuration wizard will configure the first Web server, then display the current settings for the next selected Web server. If you want to modify these settings, click **Configure** and repeat steps 4-10 of this procedure.

3. In the **Web Agent Configuration for <your server>** dialog box, SiteMinder displays the configuration information for the Web server you selected.

- To configure a new Web Agent, click **Configure**
- To change the configuration settings, click **Configure**
- To accept the configuration settings, click **Next** then skip to step 10 of this procedure.



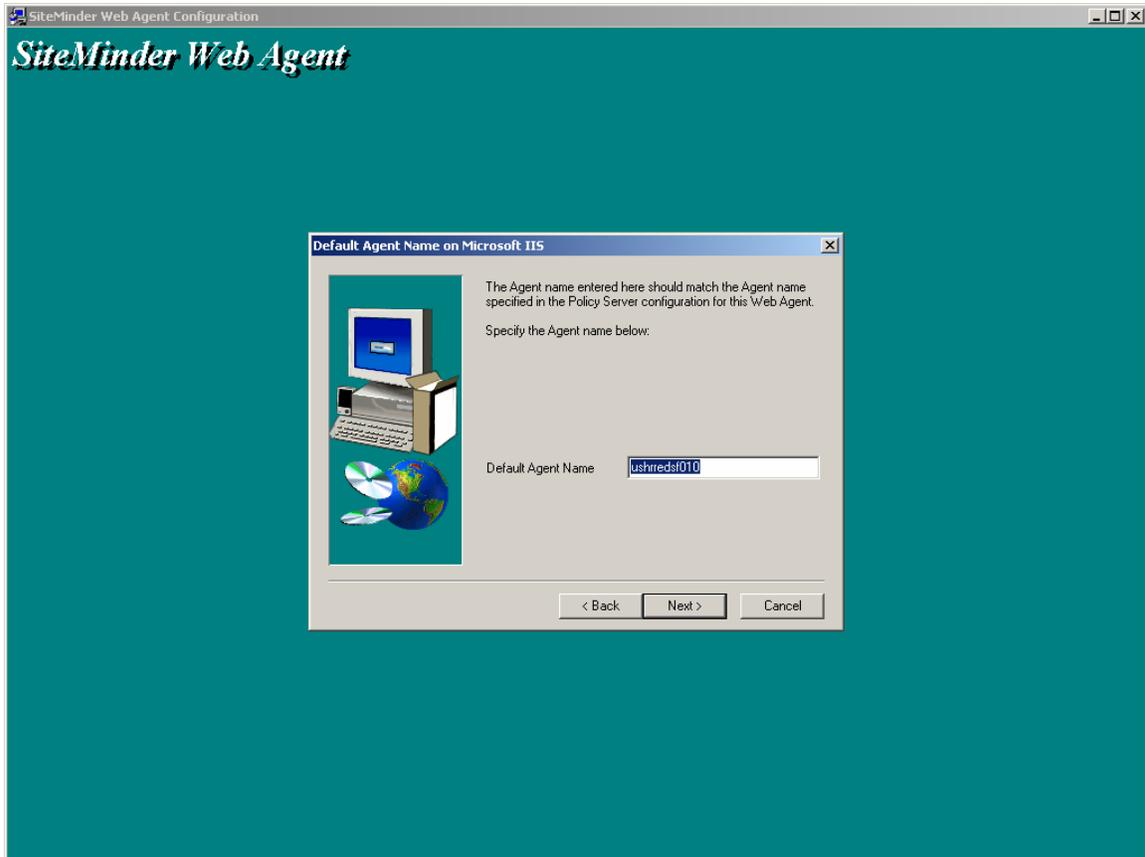
4. In the **Primary Policy Server on <your server>** dialog box, complete the following:
- Enter the IP addresses of the Policy Server to which you want the Web Agent to connect and communicate with first. (**AKO Primary Policy Server Address – 140.183.234.247**) The default IP address is the address of your local machine.



- Click **Next**

5. In the Default Agent Name on < *your server* > dialog box, complete the following:

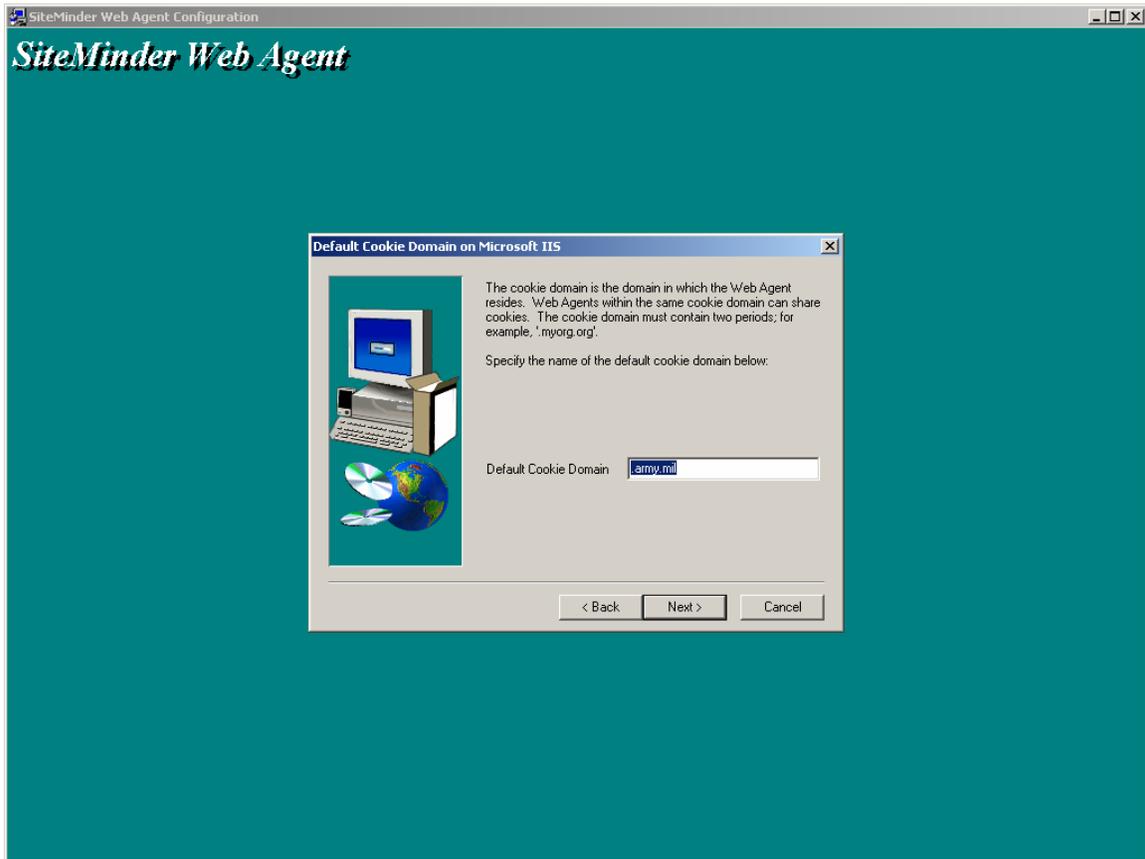
- a. Enter the Agent Name. The Agent Name is assigned by AKO and *must* match the agent name on the Policy Server



- b. Click **Next**

6. In the Default Cookie Domain <*your server*> dialog box, complete the following:

- a. Enter the domain of the Web server, using two periods. [.army.mil]



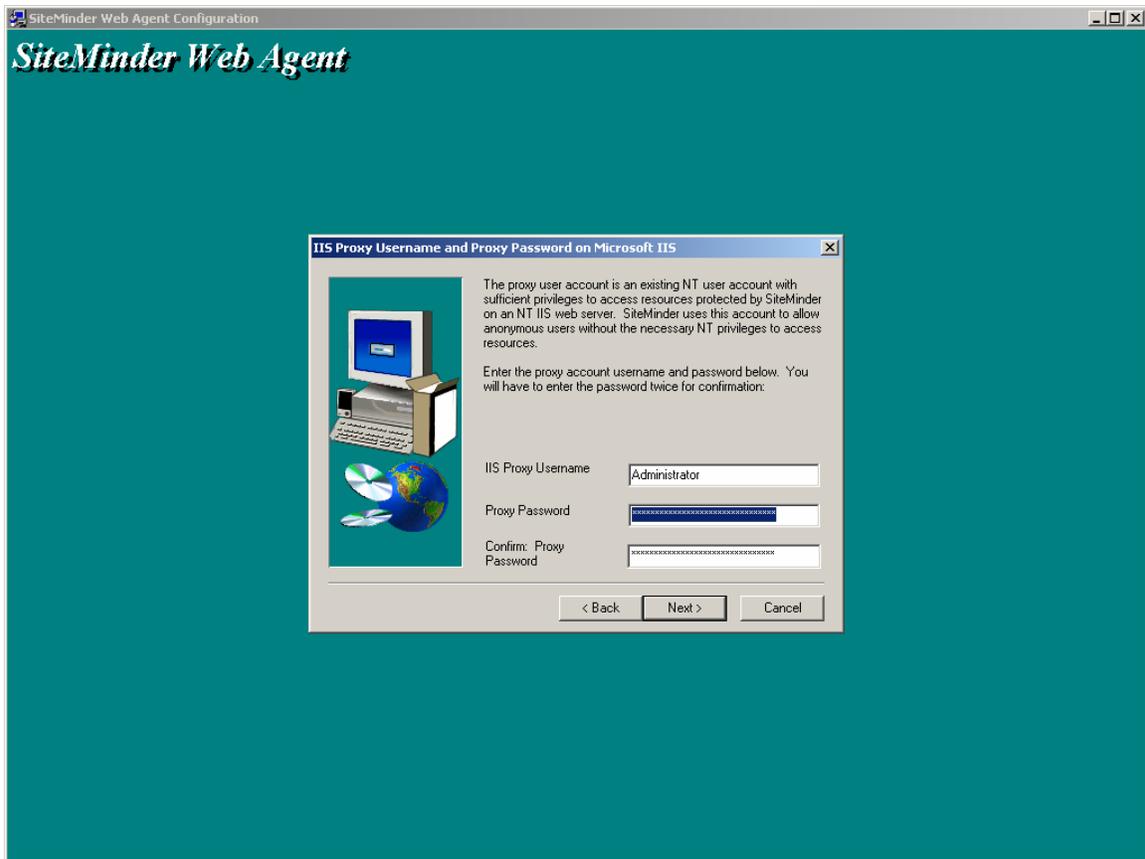
- b. Click **Next**.

7. In the IIS Proxy Username and Proxy Password on *<your server>* dialog box, complete the following:

a. Specify the Proxy Username and Password.

The proxy account must have read or execute privileges to access the files protected by the Web Agent. The account's password must be at least 6 characters long.

b. Confirm the NT password by entering it again in the **Confirm NT Password** field.



c. Click **Next**

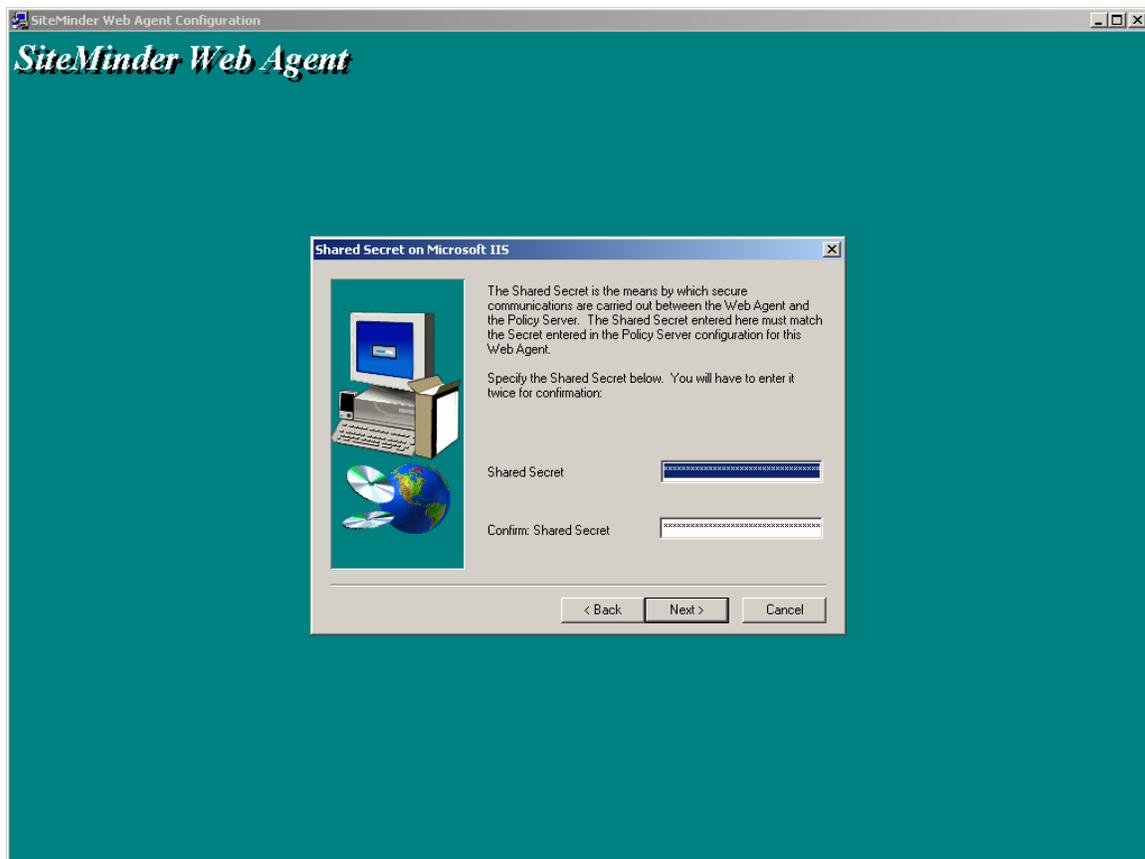
8. In the Shared Secret on *<your server>* dialog box, complete the following:

a. Enter an alphanumeric Secret that will be shared with the Policy Servers with which the Web Agent communicates. The Shared Secret is assigned by AKO, and must match the Shared Secret on the Policy Server.

b. Will the web agent be providing advanced authentication over SSL? **YES**

(SSL should already be configured for the IIS Web Server, and no additional action it is required as Netegrity does not directly interact with it.)

c. Confirm the Shared Secret by entering it again in the *Confirm Shared Secret* field.

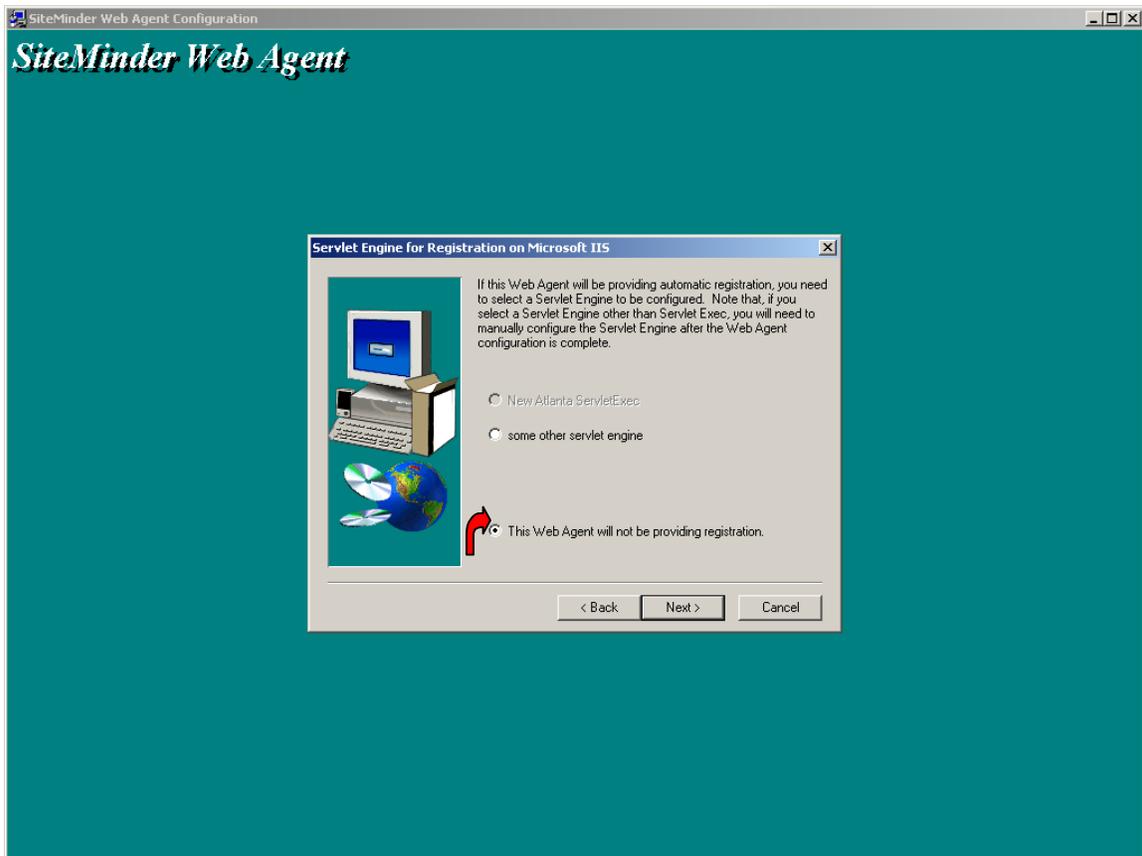


d. Click **Next**

9. Complete one of the following:

- If you have a servlet engine installed on the selected Web server, specify one of the following options for Registration in the Select Servlet Engine for Registration on *<your server>* dialog box, then click **Next**
- If you do not have a servlet engine installed, proceed to step 10.
- If you do not want to configure this Web Agent for Registration Services, select **This Web Agent will not be providing registration.**

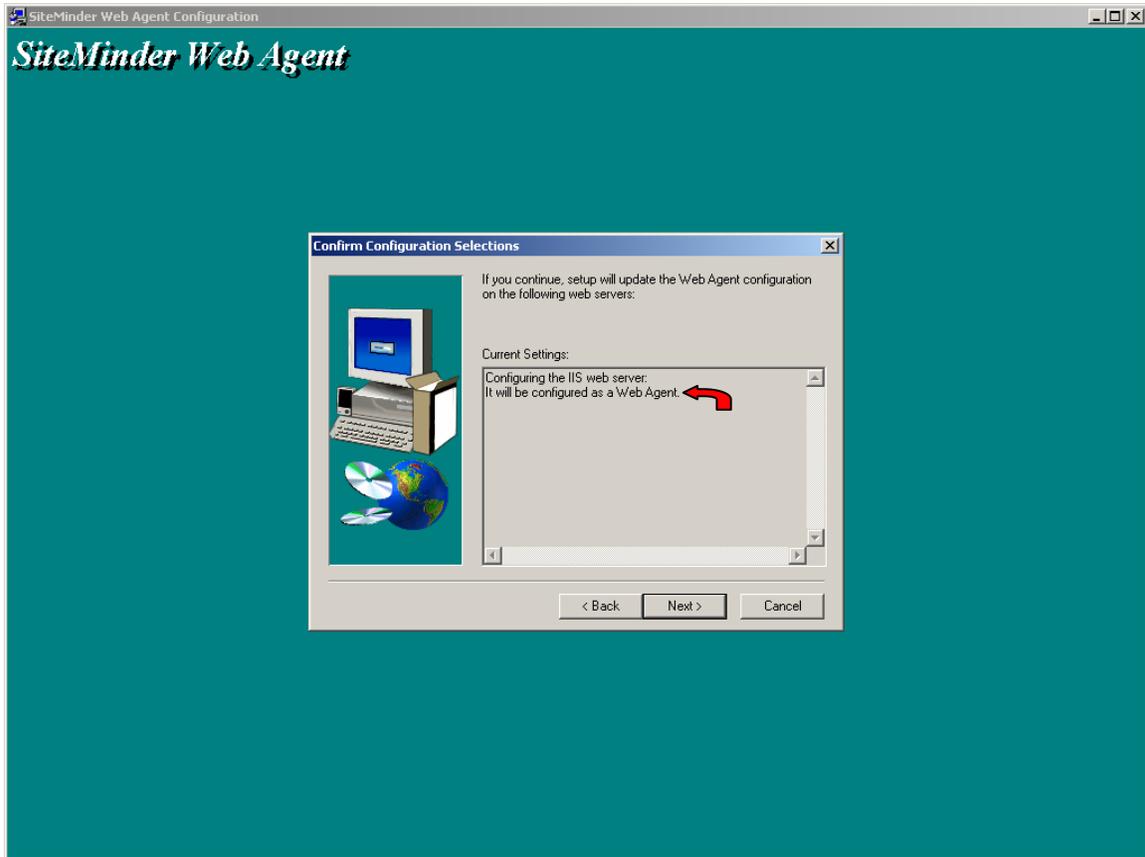
Note: Registration services from the Web Agent to Primary Policy Server is disabled for AKO.



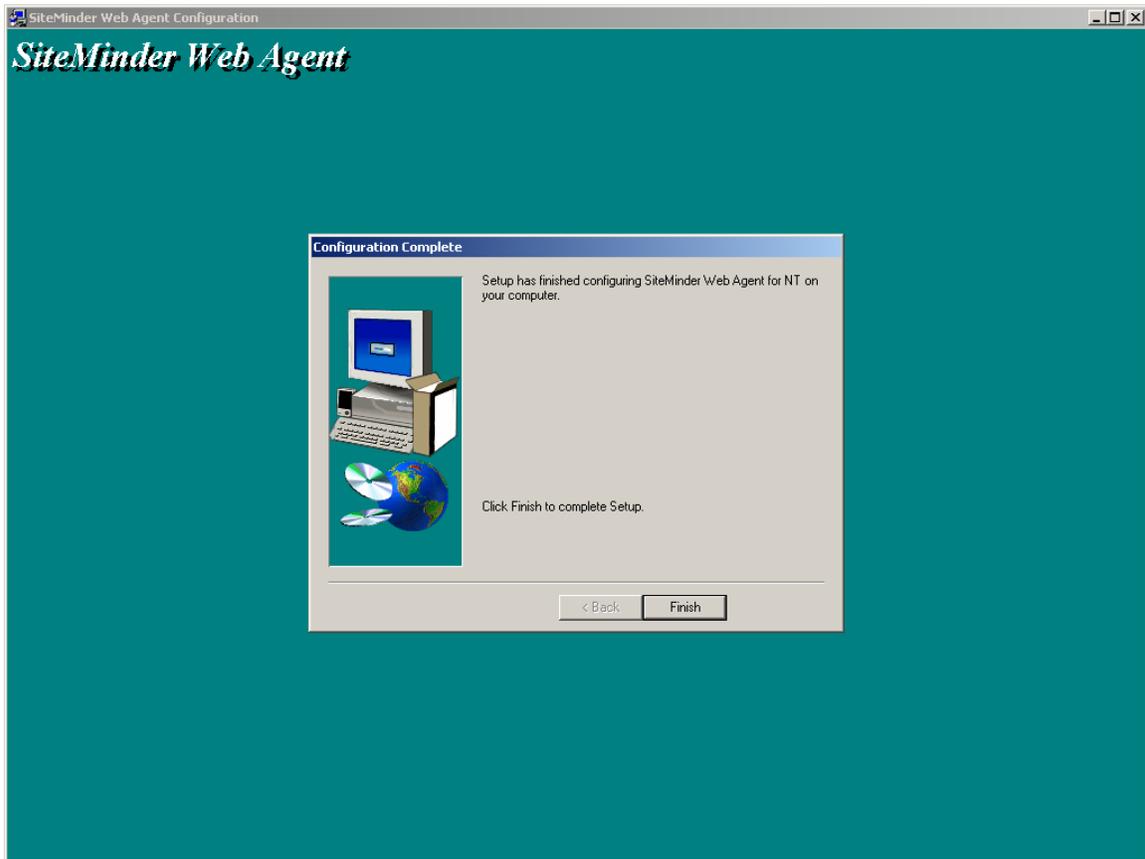
If the Web Agent Configuration Wizard does not detect a servlet engine, the Select **Servlet Engine for Registration on <your server>** dialog box is not displayed.

10. Confirm that the configuration settings are correct by clicking **Next**.

11. Confirm that SiteMinder is configuring the correct Web servers as a Web Agent, then click **Next**.



12. Click **Finish** to complete the configuration.

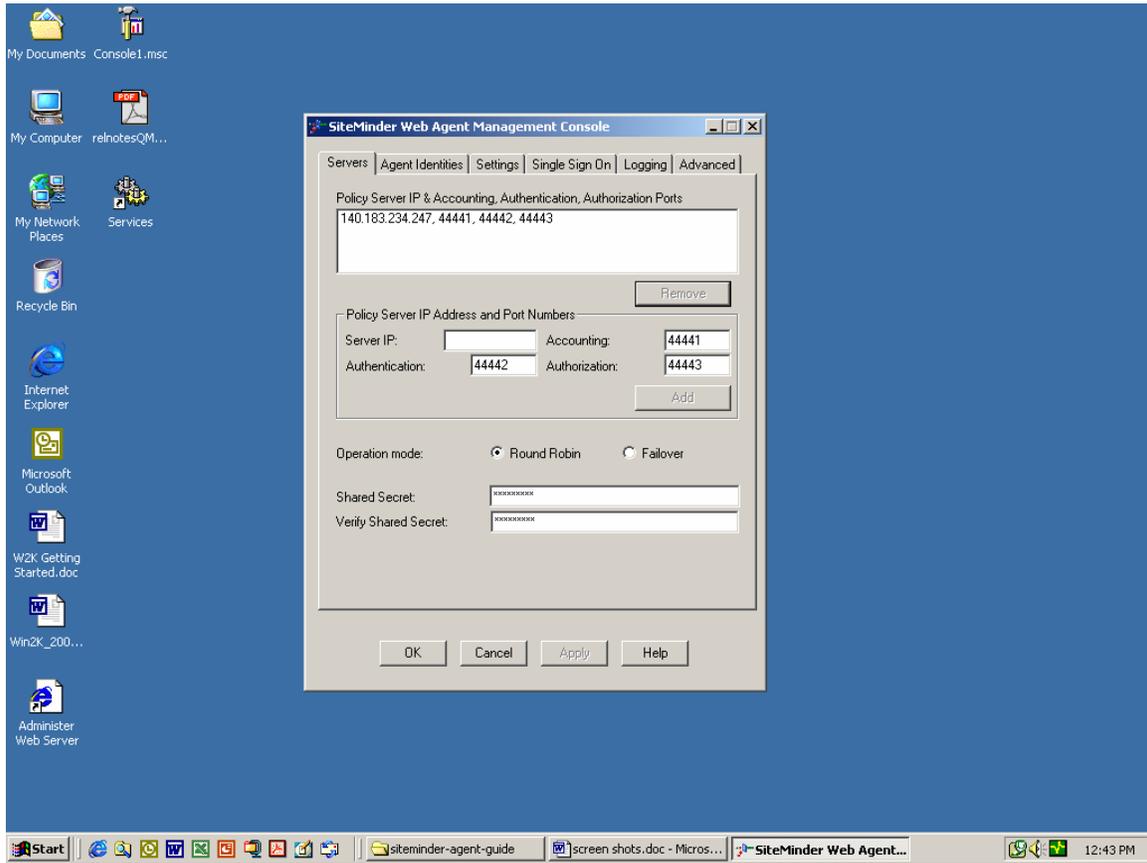


Starting the Web Agent IIS Management Console

To start the IIS Management Console, begin at the Start menu and select:

Programs | SiteMinder | IIS Web Agent Management Console.

The Console opens.



The components for the IIS Web Agent are displayed under six tabs:

- **Servers** — for configuring information about the Policy Server(s) with which the IIS Web Agent interacts.
- **Agent Identities** — for adding, removing, and modifying logical Agent identities for virtual servers.
- **Settings** — for configuring Web Agent settings.
- **Single Sign On** — for configuring the Web Agent in a single sign-on environment.
- **Logging** — for determining how the Web Agent logs error messages.
- **Advanced** — for configuring TCP/IP connections, custom error pages, full logoff support, and other advanced features.

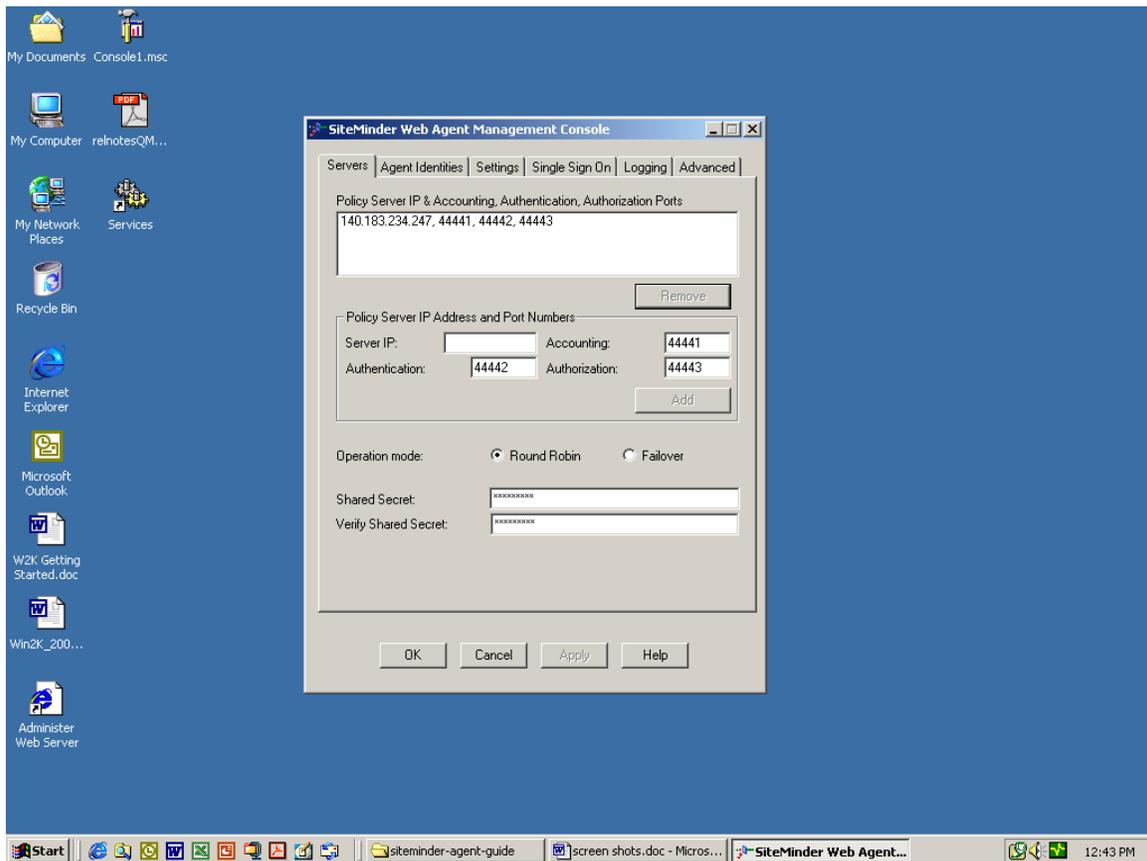
Note: When modifying any Web Agent settings, the Web server must be restarted for the changes to be effective.

Defining Policy Servers

From the Servers tab, configure the Policy Servers that communicate with the Web Agent. By default, this tab lists the IP address of the Policy Server that was specified during the IIS Web Agent installation.

From the Servers tab, one can do the following:

- Add policy servers
- Specify an operation mode
- Define the shared secret that is exchanged between the Web Agent and the Policy Server



Adding Policy Servers

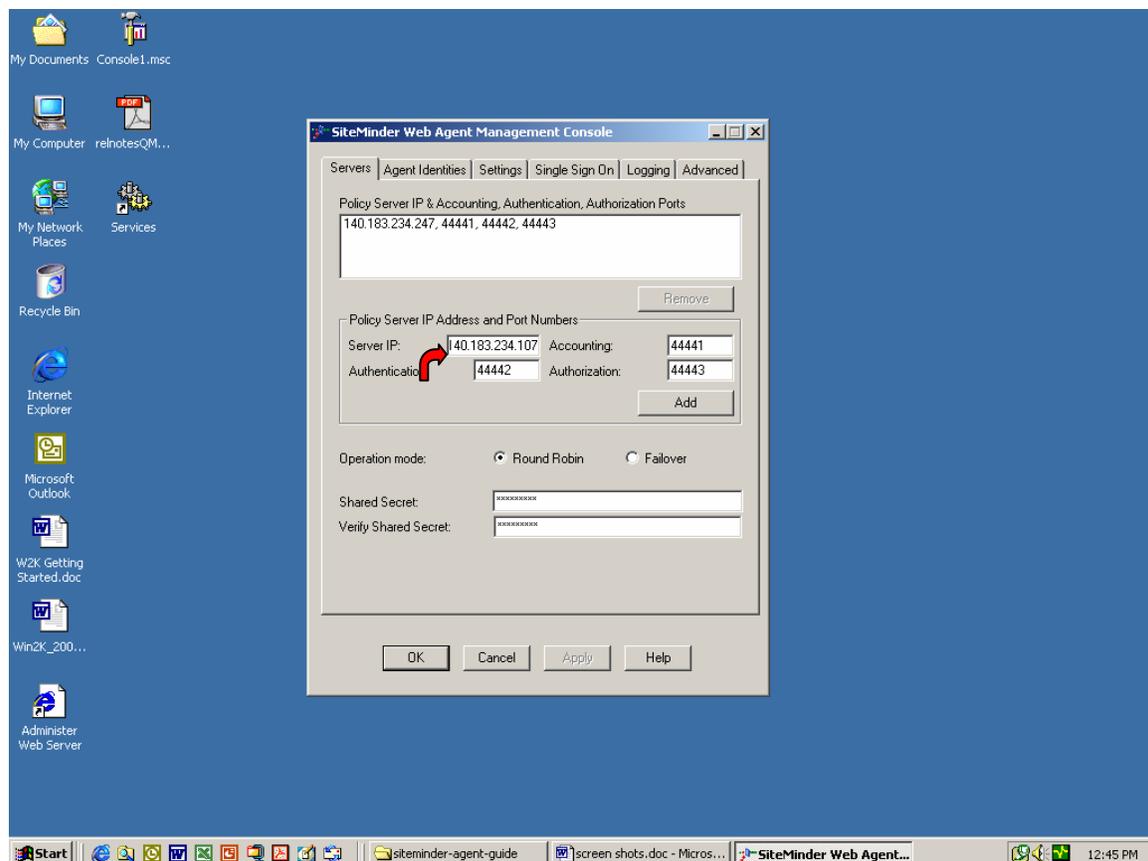
On the Servers tab, the primary Policy Server specified during the Web Agent installation is displayed by default. AKO has implemented "round robin" Policy Server, and the additional servers must be added.

Note that it is recommended to debug the connectivity and verify all the policies on the Primary Policy Server before proceeding to add additional Policy Servers.

To add a Policy Server:

1. In the Console, select the Servers tab to move it to the front.
2. In the **Server IP** field, enter the IP address of the additional Policy Servers, one at a time:

140.183.234.107, 140.183.234.158



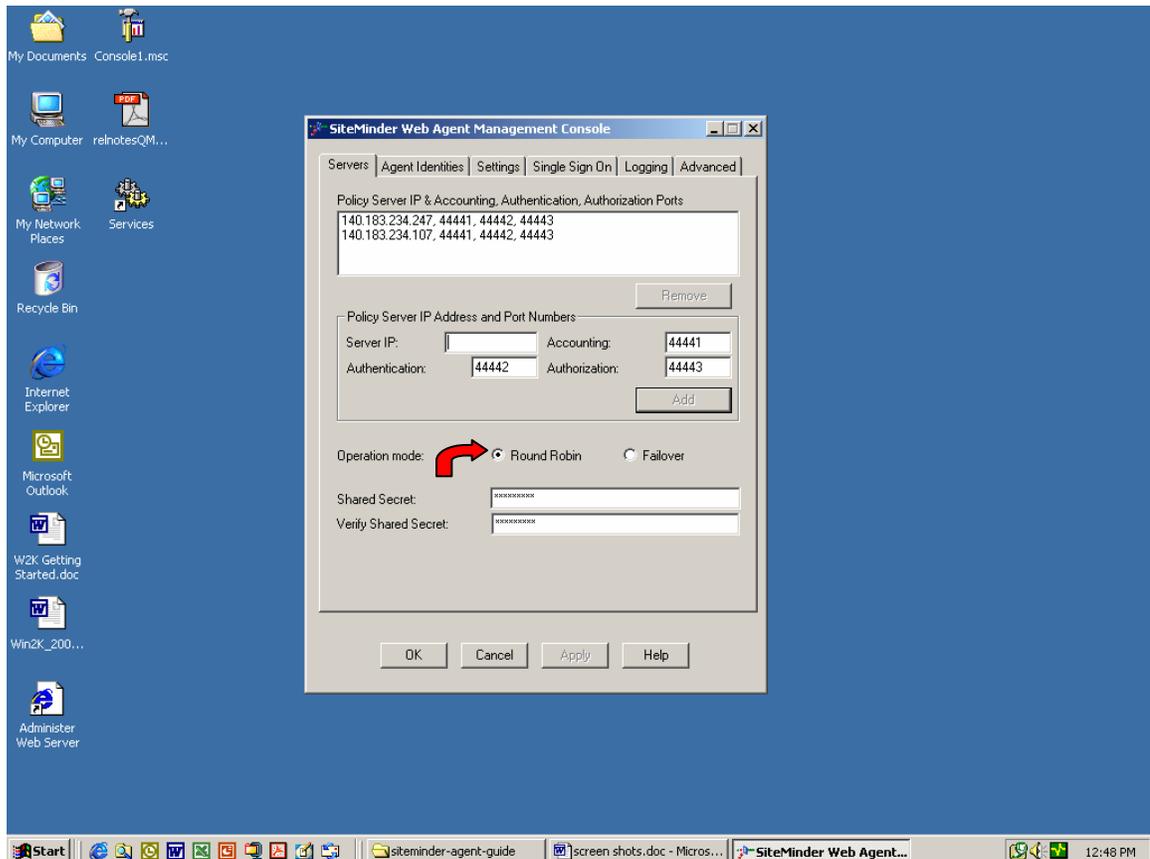
3. In the **Authentication** field, enter the port number for the authentication service.
 - The authentication service processes the Web Agent user authorization requests. The default is 44442.
4. In the **Accounting** field, enter the port number for the accounting service.
 - The accounting service processes the Web Agent requests to log user activity. The default is 44441.

5. In the **Authorization** field, enter the port number for the authorization service.
 - The authorization service processes the Web Agent user authorization requests. The default is 44443.
6. Click **Add**, The Policy Server is added to the list of Policy Servers.
7. Click **OK** to save your changes and exit the Console.
8. From the Services control panel, stop and restart the Web server.

Note: To add multiple Policy Servers, Repeat the above procedures. Each Policy Server is added to the list of Policy Servers in the Servers tab.

Selecting an Operation Mode

The operation mode determines how the Web Agent works with multiple Policy Servers. Specifically, it determines whether the Web Agent operates in round robin load balancing mode or in failover mode.

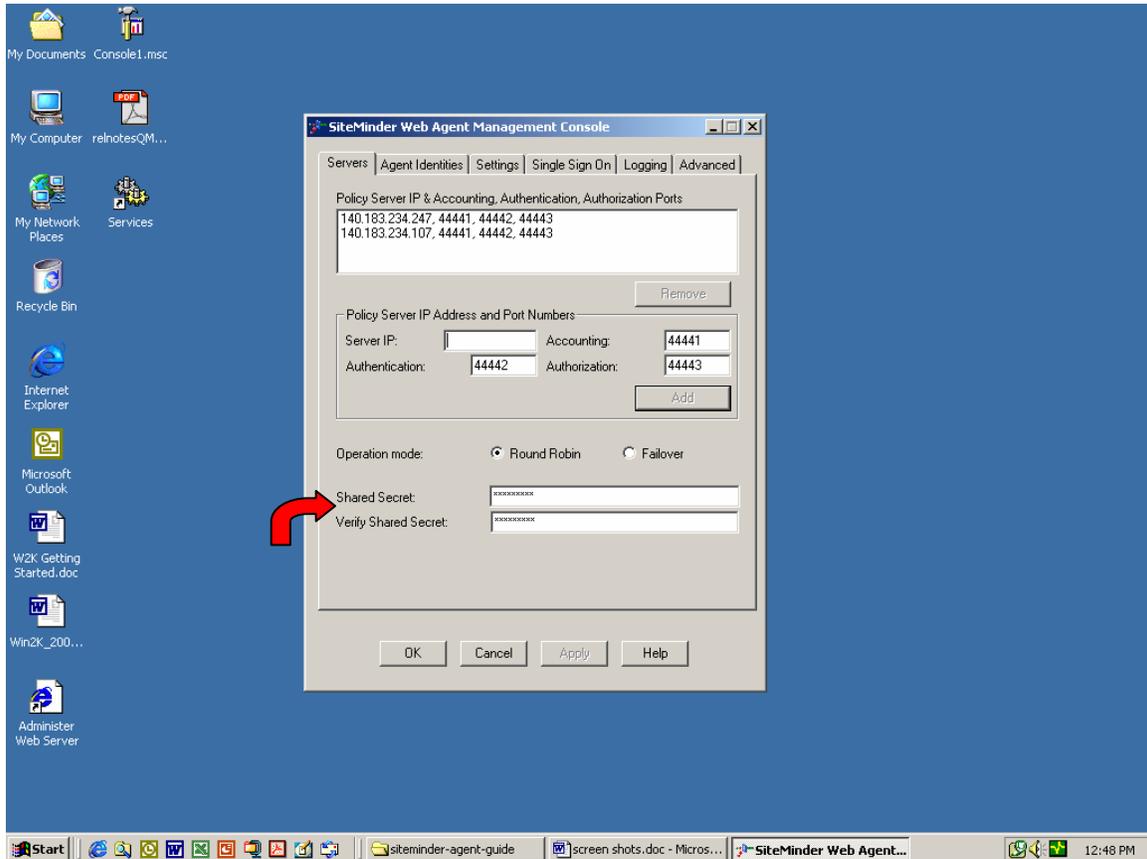


Choose an operation mode:

1. Select the radio button for "round robin", as AKO has implemented "round robin" Policy Servers.

Modifying the Shared Secret

Enter an alphanumeric Secret that will be shared with the Policy Servers with which the Web Agent communicates. The Shared Secret is assigned by AKO, and must match the Shared Secret on the Policy Server.



To modify the shared secret:

1. In **Shared Secret** field, enter a new secret. This setting applies to all Policy Servers listed on the Servers tab.

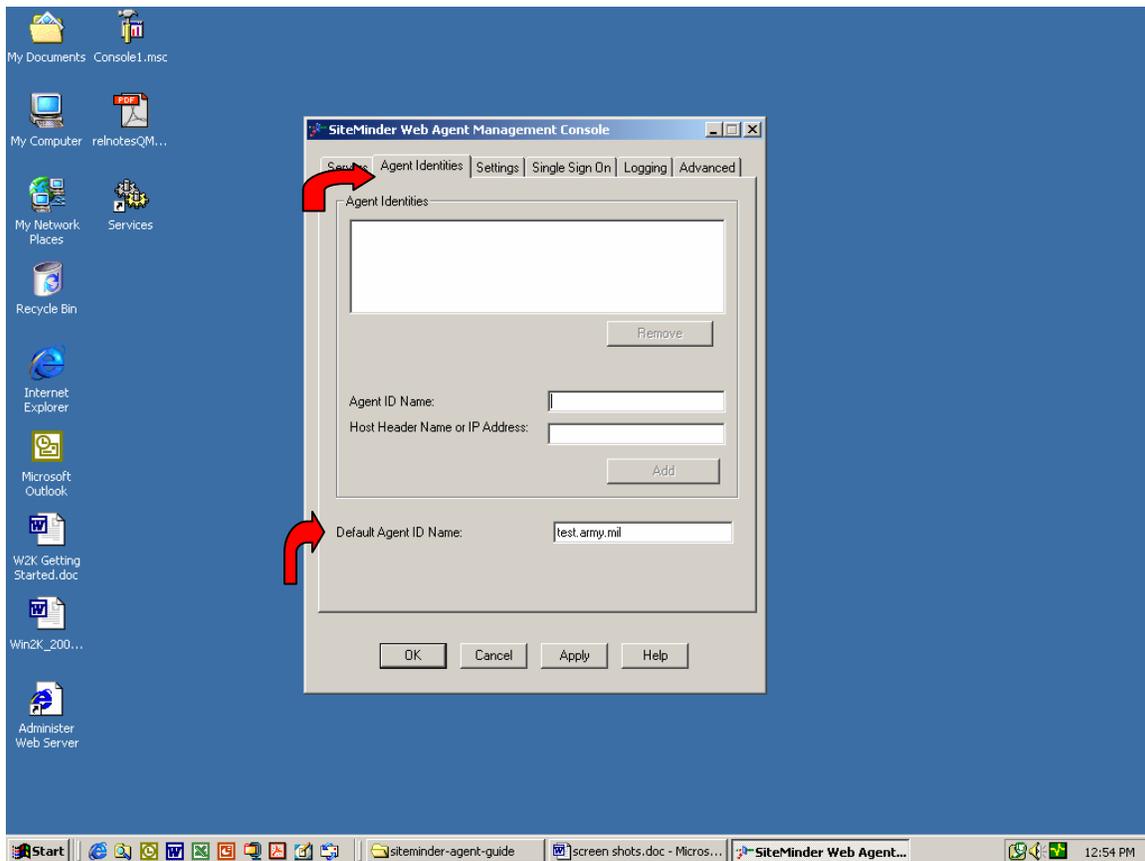
Note: The shared secret is case-sensitive. *(A Shared Secret specific to your application servers will be provided to you by AKO).*

2. Click **OK** to save your changes and exit the Console.

Modifying Default Agent Name

The default Agent name identifies the Agent identity that the Web Agent uses when it detects an IP address on its Web server that does not have an Agent identity assigned to it. By default, the default Agent name is the name of the installed IIS Web Agent. If you use the default Agent name, ensure that it is defined in the Policy Server User Interface exactly as it is defined for the Agent.

SiteMinder does not use the default Agent name unless there are no other Agent identities defined for a virtual server.



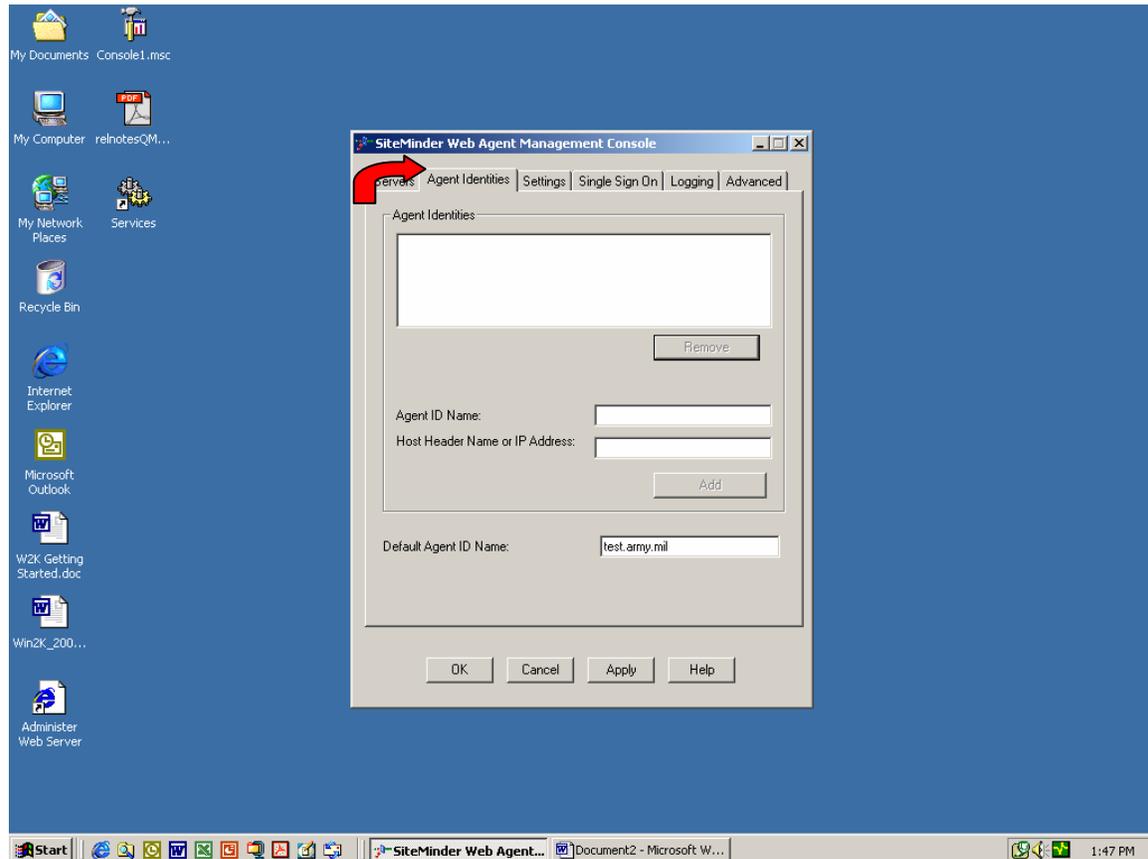
To change the default Agent name:

1. In the **Default Agent ID Name** field, enter a new name.
2. Click **OK** to save your changes and exit the Console.
3. From the Services control panel, stop and restart the Web server.
4. When you modify the default Agent, you must also submit changes to AKO in order for them to enter the changes in the Policy Server User Interface.

Defining Agents Identities for Virtual Servers

Use the Agent Identities tab to add and remove Agent identities for virtual servers. By default, when you install a Web Agent, the Web Agent is placed in the Agent list.

The following dialog box shows the Agent Identities tab.

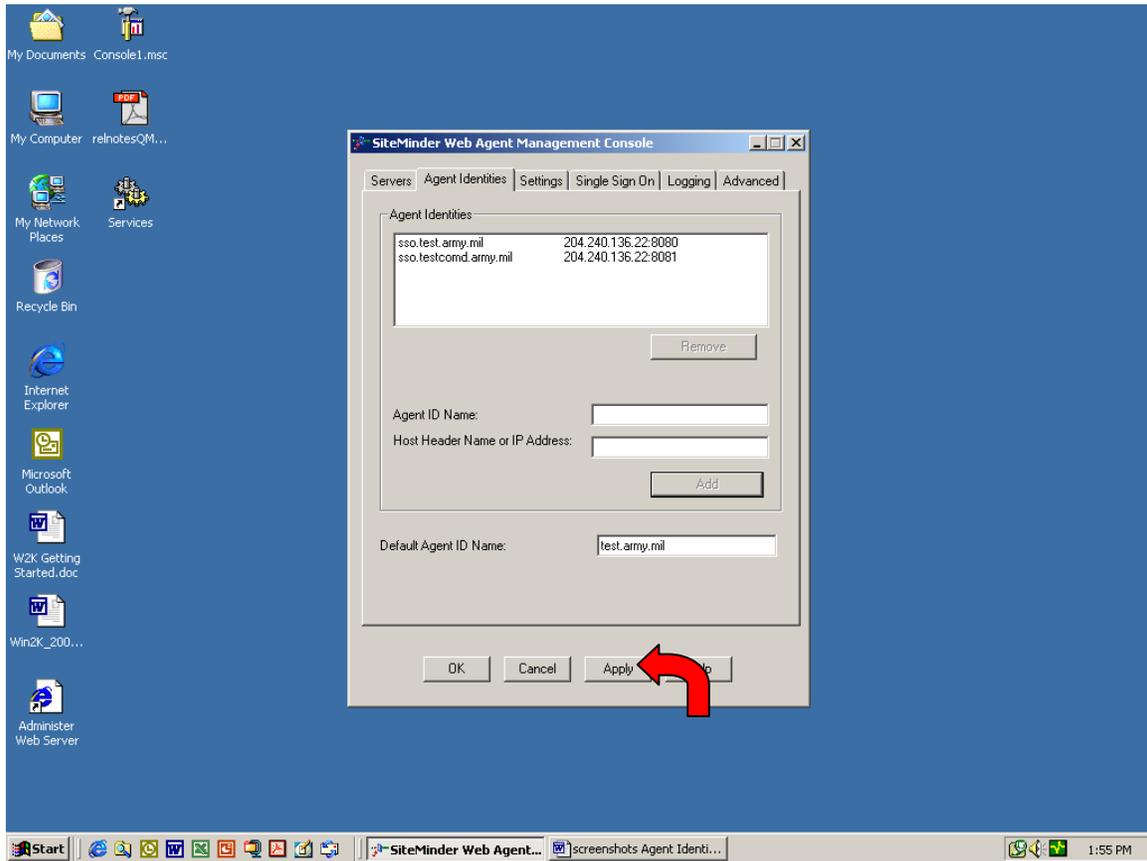


Note: If you add an Agent Identity, it must also be defined in the Policy Server with the same Agent name.

To configure a Web Agent identity for a virtual server:

1. Select the Agent Identities tab to move it to the front.
2. In **Agent ID Name** field, enter the name of the Web Agent identity to be added.
3. In the Host Header Name or IP Address field, enter the virtual server's unique or shared host header or IP address.
4. Click **Add**. SiteMinder adds the Agent identity to the list.

5. Click **Apply**.



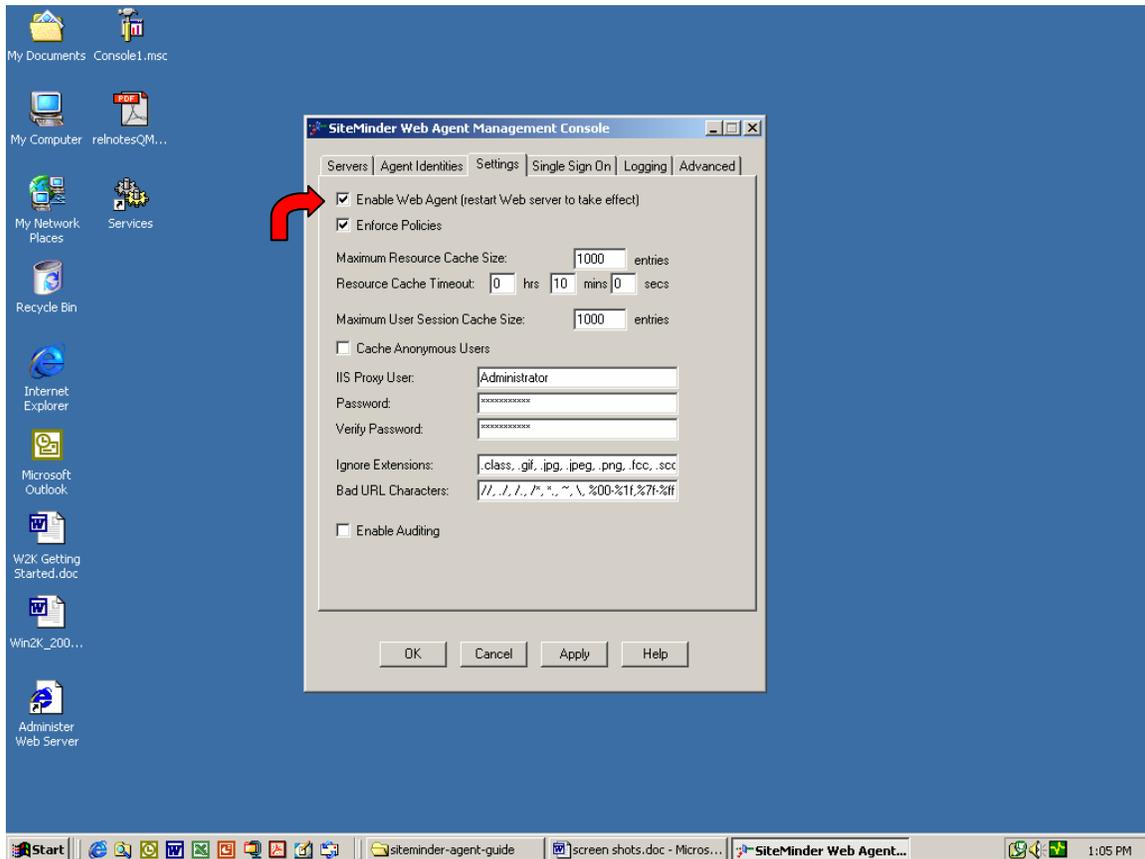
6. Repeat steps 2 through 5 to add other Agent identities.
7. Click **OK** to save your changes and exit the Console.
8. From the Services control panel, stop and restart the Web server.

Note: Ensure that the Agent name that has been added is exactly as defined in Policy Server.

Enabling and Disabling an IIS Web Agent

You must enable a Web Agent for it to communicate with the Policy Server to gather management information, such as key updates. Enabling the Web Agent does *not* enable it to protect resources based on policies. The **Enforce Policies** check box enables full operation of the Web Agent.

Note: To enable the Web Agent to implement access control, see the next section, **Enforcing Policies to Enable Access Control**.



To enable a Web Agent:

1. Select the **Enable Web Agent** check box.
2. Click **OK** to save your changes and exit the Console.
3. From the Services control panel, stop and restart the Web server.

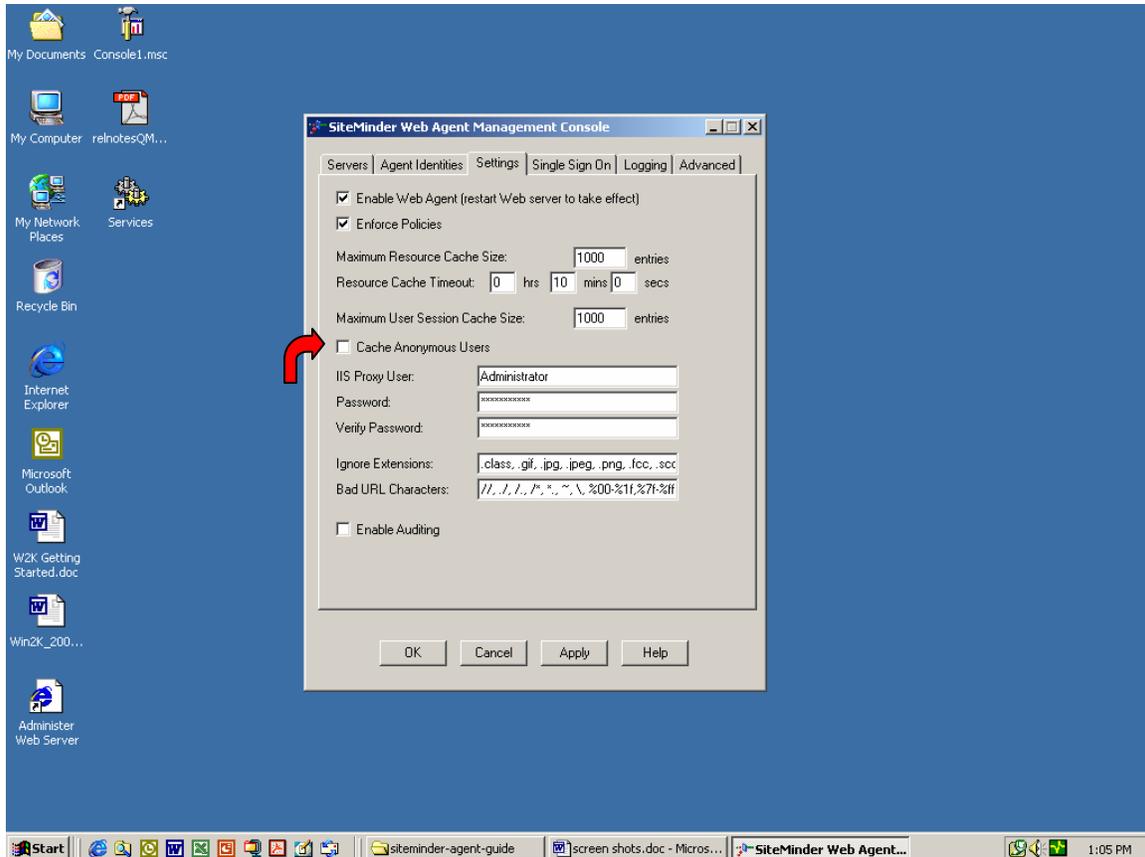
To disable the Web Agents:

1. Deselect the **Enable Web Agent** check box.
2. Click **OK** to save your changes and exit the Console.
3. From the Services control panel, stop and restart the Web server.

Caching Anonymous Users

The **Cache Anonymous Users** setting tells the Web Agent whether to store anonymous user information in cache.

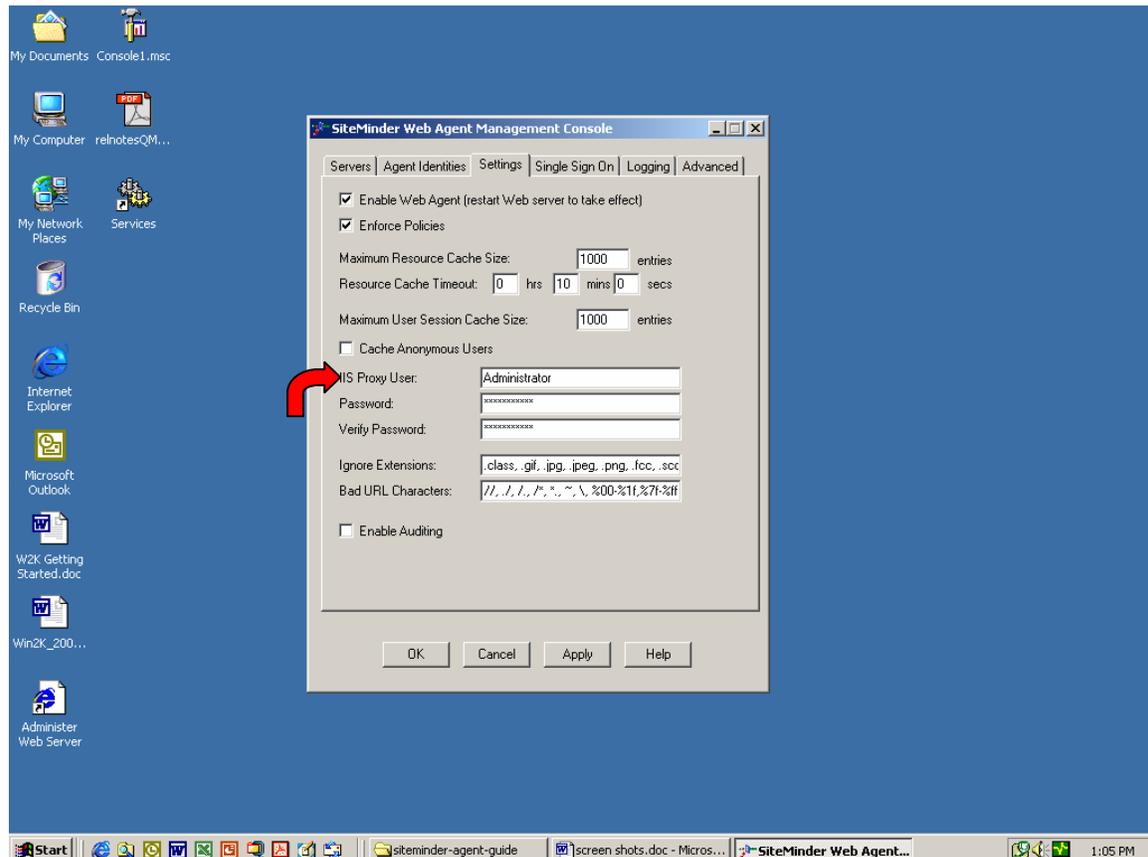
For access controlled Army applications, no anonymous users are allowed, and therefore no information need to be cached about them.



1. Ensure that the **Cache Anonymous Users** check box is *unchecked*.
2. Click **OK** to save your changes and exit the Console.
3. From the Services control panel, stop and restart the Web server.

Configuring an IIS Proxy User

When users want to access resources on an IIS Web server protected by SiteMinder, they will not have the necessary server access privileges. Therefore, the Web Agent uses an existing NT user account that does have sufficient privileges. This NT user account, assigned by an NT administrator, acts as a *proxy user account* for users granted access by SiteMinder.



To modify the IIS proxy user account:

1. In the **IIS Proxy User** field, enter the user name for the existing NT user account.

Note: *This account should have sufficient privileges to access NT file system resources protected by SiteMinder.*

2. In the **Password** field, enter the user password for the NT account.
3. In the **Verify Password** field, re-enter the password.
4. Click **OK** to save your changes and exit the Console.
5. From the Services control panel, stop and restart the Web server.

Note: *Users authenticated and authorized by SiteMinder will now have access to resources on the IIS Web server.*

Configuring How the Web Agent Interprets URLs

The Web Agent monitors URLs in resource requests and enforces the security policies for these resources. SiteMinder Web Agents interpret and parse URLs differently from the Web servers where the resources reside. These differences can result in performance and security issues, and can potentially allow unauthorized users to gain access to resources. You need to consider these issues in the design of your Web site and the configuration of the SiteMinder Web Agent.

The next sections describe the settings that you can modify to determine how the Web Agent handles characters in URLs.

Specifying File Extensions to Ignore

The **Ignore Extensions** field lists the most common file extensions (.gif, .jpg, .jpeg, .png, and .class) that the Web Agent can ignore. This means that the Agent passes requests for files with these extensions directly to the Web server; there is no authorization process. By default, these extensions are included in the **Ignore Extensions** field because they typically specify types of files that do not require as much security as other resources.

Note: *Use the ignore extensions feature with caution. There are some security issues that you may want to consider. It is strongly recommended that you remove all entries and leave the **Ignore Extensions** field blank.*

To protect URLs that do not have periods, there are three options:

- Configure the **overrideignoreextfilter** parameter. Specify a list of strings for resources that do not have a period in the path, like servlets.
- Include a period and extension somewhere in the path of every resource that you want to protect. If a bogus extension is appended to the end of a URL, this triggers the two-period rule, which prompts the Web Agent to challenge the user.
- Ensure that protected resources do not have extensions in the **Ignore Extension** field.

Configuring the overrideignoreextfilter parameter

For the his parameter, specify a list of strings that the Web Agent matches against all URLs. If the Web Agent finds a match, it treats the resource as protected resource, regardless of the **Ignore Extensions** setting. From the list of strings in the **overrideignoreextfilter** setting, only one must match a value in the requested URL. Also, the specified string can be a partial string of the requested URL. For example, the string */servlet/* would protect the following:

/dira/app1/servlet/app

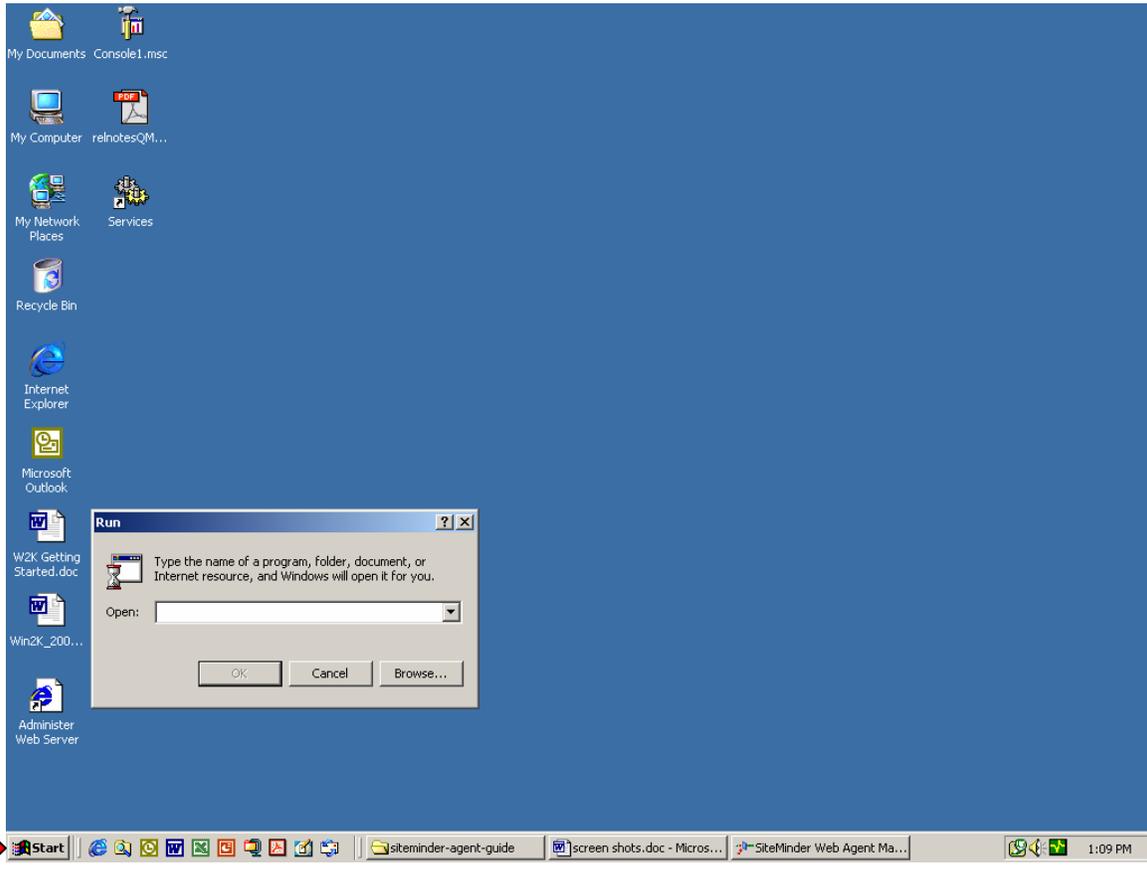
/dirb/servlet/app1

/dirc/mydir/servlet/app2

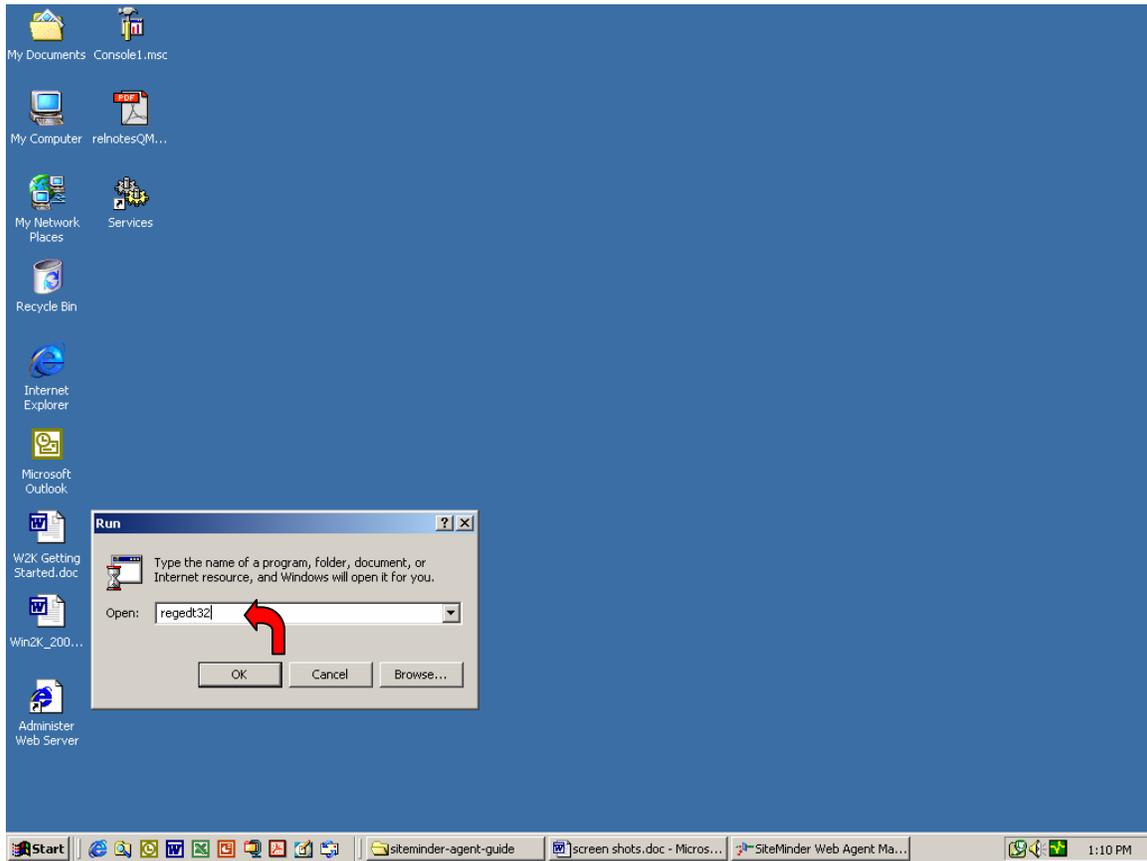
Note: *It is better to specify more general strings than exact paths.*

To configure the `overrideignoreextfilter` setting, add a string value to the Windows registry, as follows:

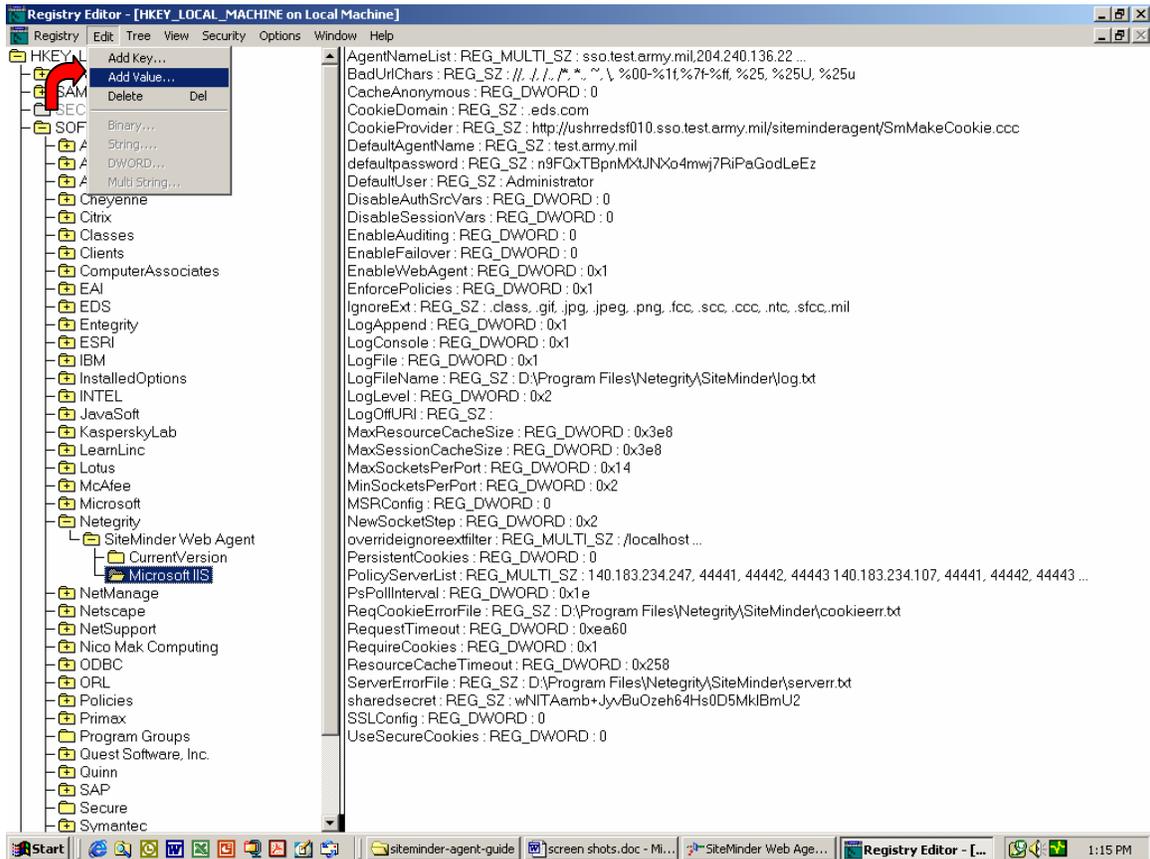
1. Select **Start | Run** .



2. In the **Open** field, enter **regedt32** and click **OK** .



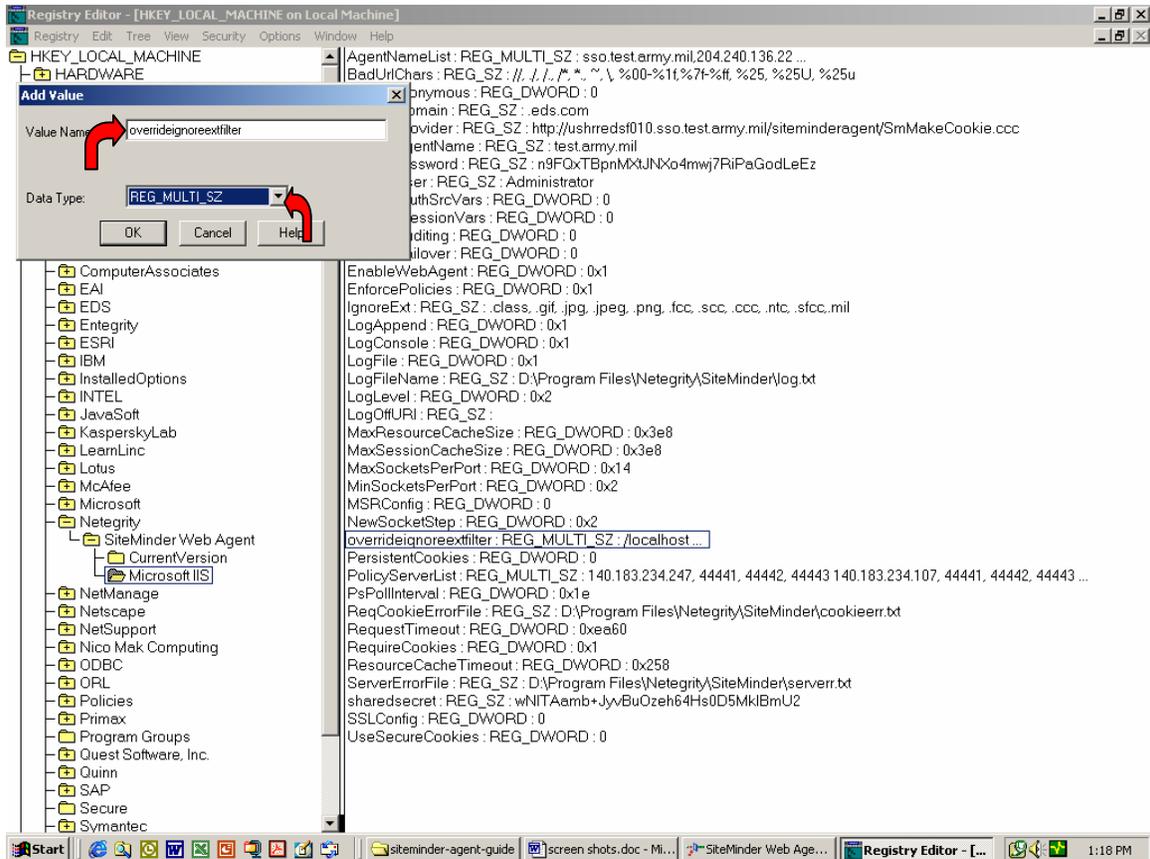
4. Select Edit | Add Value



5. In the **Add Value** dialog box, configure the fields as follows then click **OK** :

a. **Value Name** : overrideignoreextfilter

b. **Data Type** : REG_MULTI_SZ

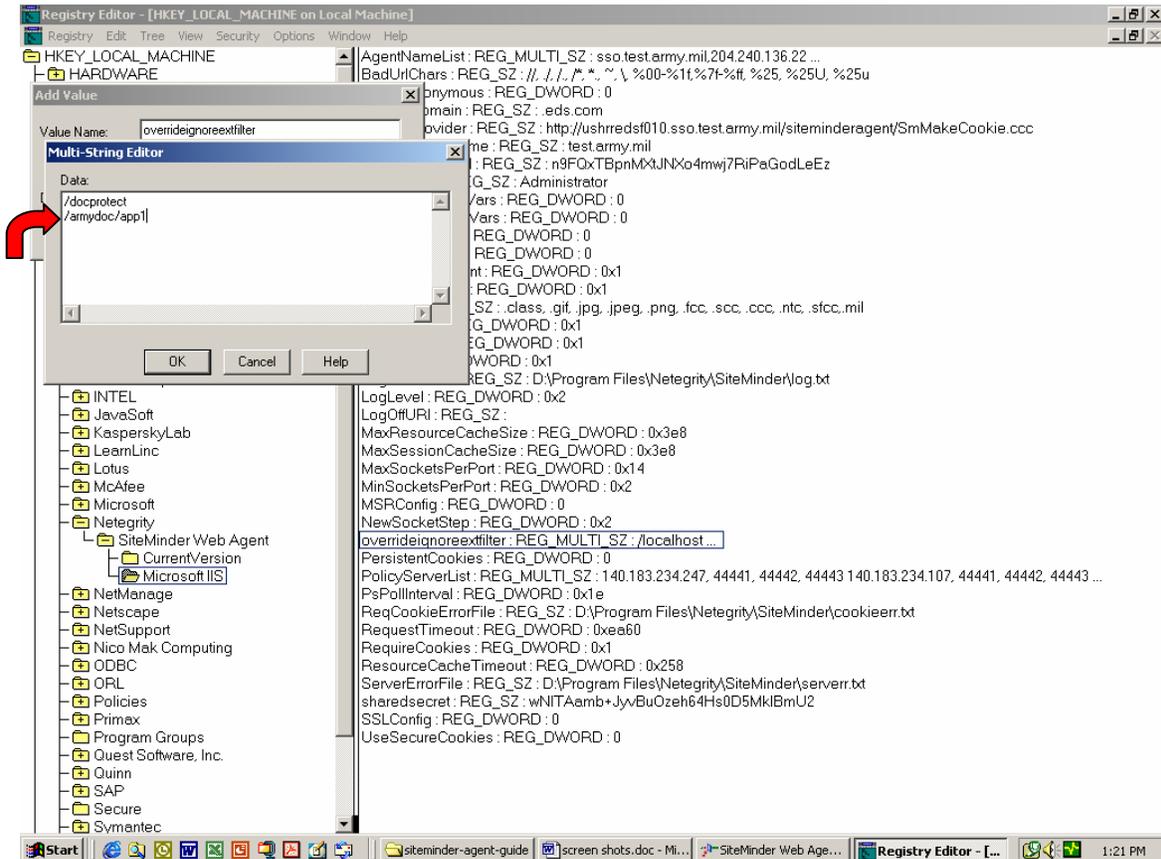


The **Multi-String Editor** dialog box opens.

6. In the **Multi-String Editor** dialog box, add strings for resources without periods. Enter as many strings as you want, placing each string on its own line, for example:

/docprotect

/armydoc/

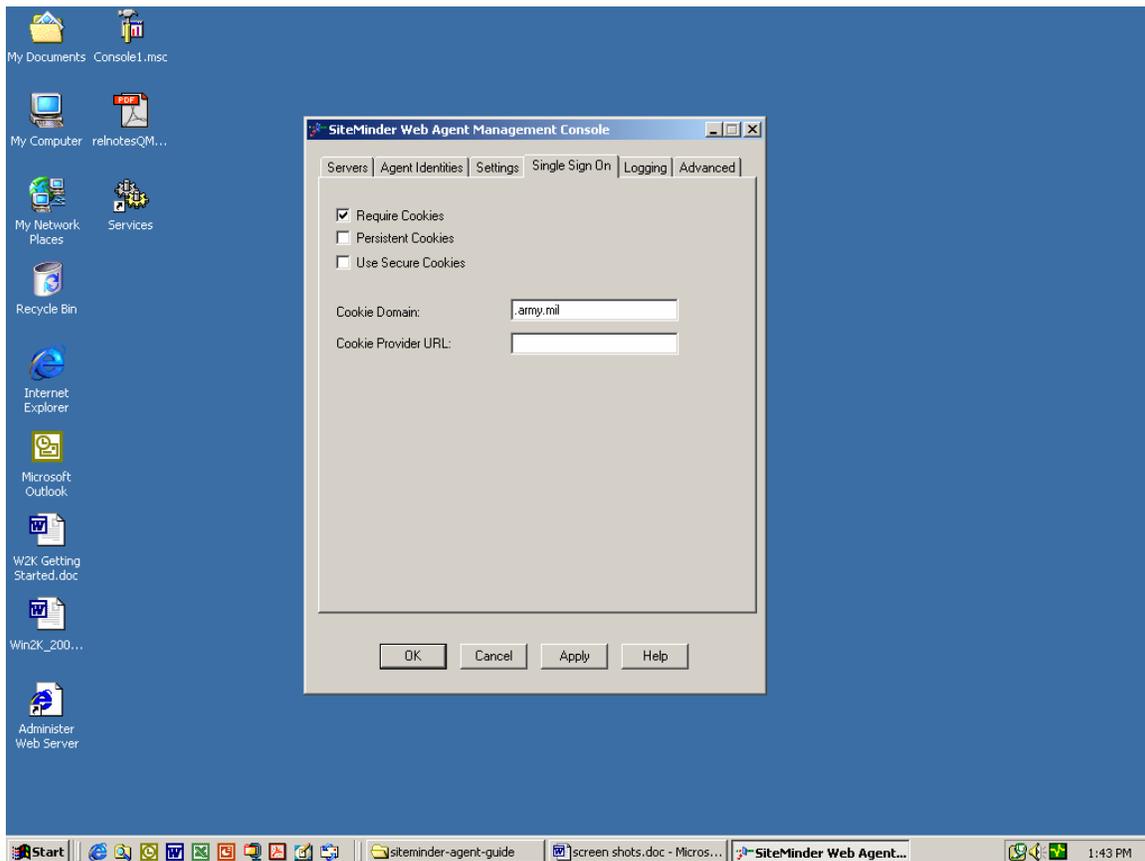


Configuring Single Sign-On

SiteMinder's single sign-on feature enables authenticated and authorized users to navigate seamlessly within a single cookie domain or across multiple cookie domains without being re-authenticated. Single sign-on simplifies the use of applications across different Web servers and platforms.

These settings are modified on the Single Sign On tab of the IIS Web Agent Management Console or in the WebAgent.conf file. The settings are common for all Web Agents on all platforms; however, the configuration procedures are different.

The Single Sign On tab, shown in the following dialog box, allows the set up a single sign-on environment.



To configure single sign-on, configure the following settings:

Require Cookies - Cookies are used to provide secure single sign-on in a SiteMinder environment and to track session and idle timeouts. The "require cookies: box should be **checked**.

If the Web Agent is configured to require cookies, a user's Web browser must accept HTTP cookies. If the browser does not, the user receives an error message from the Agent denying them access to all protected resources.

If the Web Agent does not require cookies, but the user's Web browser is

accepting cookies, the Web Agent functions normally; however, the user may get challenged for their credentials unexpectedly and the Web Agent may not strictly enforce timeouts.

Persistent Cookies - For implementation of Single Sign-On on any U. S. Government system, **DO NOT** select "persistent cookies".

Use Secure Cookies - To ensure that cookies are sent to Web servers only across secure HTTP connections (HTTPS) enable this option. This feature further secures connections between browsers and Web servers. In a single sign-on environment, if a user moves from an SSL Web server to a non-SSL server, single sign-on is no longer valid because secure cookies cannot be passed over traditional HTTP connections. In this case, the user will have to re-authenticate. The "use secure cookies" box should be **NOT be checked**.

Cookie Domain - The cookie domain setting defines the cookie domain of the Web Agent, which you specified during the Web Agent installation. This must be a fully qualified domain name with at least two periods (.). For implementation with AKO Single Sign-On, this should be set to `<.army.mil>`.

Cookie Provider URL - Leave the cookie provider URL blank.

4.15 Installing and Configuring the SSO Web Agent on UNIX

Login as person with admin rights to the web server directory - but NOT Root

1. Create a Netegrity folder
2. Download the appropriate Web Agent .tar file (eg, *smwa-4.63-so.tar*) into this folder.
Note that each flavor of UNIX has its own Web Agent.
3. untar the web agent, eg: *tar -xvf smwa-4.61-so.tar*
4. change to the newly created Web Agent install folder, eg: *cd smwa-4.63-so-install*
5. launch the install process: *smwa-install*
6. Go through the installation script
 - Point it to the location of the web server. For example:
/netscape/suitespot4/https-portaldev
 - Point it to the location for the Netegrity install. For example:
/netegrity/siteminder

Configure the Web Agent on Unix

1. Go to the install directory (*/netegrity/siteminder*) execute *smwa-config*
2. Provide the necessary information:
 - web server - choose the instance of the web server
 - AKO primary policy server address - 140.183.234.247
 - web Agent Name – The Web Agent name is assigned by AKO and must match the Web Agent name on the Policy Server
 - cookie domain - *.army.mil*
 - Shared Secret - the Shared Secret is assigned by AKO and must match the Shared Secret on the Policy Server
 - Will the web agent be providing advanced authentication over SSL ? YES (your ssl is already configured, and you do not need Netegrity to interact with it)
 - Will this web Agent be providing self-registration services? NO
 - confirm your information

Installing The Patch To The Webserver

1. Untar the quarterly maintenance release (eg, *smwa-4QMR1-so.tar*) file
2. change to the newly created Web Agent install folder, eg: *cd smwa-4QMR1-so-install*
3. *smwa-install*
4. Go through the installation script (same as above)
 - Point it to the location of the web server. For example:
/netscape/suitespot4/https-portaldev
 - Point it to the location for the Netegrity install. For example:
/netegrity/siteminder
5. This overwrites the current WebAgent.conf file on the Web Server

Configure The Patch

1. change to the Web Agent install folder, eg: *cd smwa-4QMR1-so-install*
2. *smwebagent-config*
3. Provide the necessary information:

- web server root - **/netscape/suitespot4**
- web server - **choose the instance of the web server**
- Select an option – **p** (you want to preserve the settings you have already created, and simply update the configuration)
- confirm your information

Turning The Web Agent On

1. Go to the web server config directory (**/netscape/suitespot4/https-*****/config**)
2. Via the WebAgent.conf file
3. Change **enablewebagent=YES**
4. Change **enablefailover=NO**
5. In order to support round robin policy server configuration,
Add lines under : `policyserver="140.183.234.247, 44441, 44442, 44443"`
policyserver="140.183.234.107, 44441, 44442, 44443"
policyserver="140.183.234.158, 44441, 44442, 44443"
6. Go to the iPlanet Admin Interface and remove the currently existing acl's
7. Restart the Web server for the web agent to be turned on

4.16 Installing and Configuring the SSO Web Agent on Domino

1. Install the Web Agent as per the appropriate Windows (section 4.12) or UNIX (section 4.13) instructions.
2. Navigate to the directory where the Web Agent is installed to run the configuration.

Note: You can also run the configuration from the same directory you ran the installation.

3. Enter `./smwebagent-config` to run the configuration script.
4. At the prompt to configure a Domino Web server, enter **Y**.
5. At the prompt, specify the location of the notes.ini file, which is the instance of the Domino server that you just installed.

Note: The installation automatically writes the path to the WebAgent.conf in the notes.ini file.

6. Enter the SiteMinder Policy Server IP address. The AKO Primary Policy Server is at: **140.183.234.247** The secondary Policy Servers are at:
 - 140.183.234.107
 - 140.183.234.158
7. Enter the Web Agent Name. The Web Agent name is assigned by AKO and must match the Web Agent name on the Policy Server.
8. Enter the cookie domain in which the Web Agent will be located. The domain must contain two periods: [**army.mil**].
9. Enter the Shared Secret that will be shared with the Policy Servers with which the Web Agent communicates. The Shared Secret is assigned by AKO, and must match the Shared Secret on the Policy Server.
10. Confirm the shared secret by entering it again at the next prompt.

After you enter the shared secret, the installation displays the following message:

This Web Agent by default will enforce policies on the webserver, provide forms-based authentication, and provide single-signon across multiple domains.

At this point, the Domino-specific configuration begins.

11. At the prompt, enter **Y** if you want all users successfully logged into SiteMinder to be logged into Domino as the Domino SuperUser.
12. Enter **Y** to allow users access to files in a Notes database (an .nsf file) that is also specified in the **IgnoreExt** parameter of the WebAgent.conf file. For these resources, SiteMinder identifies all users as the Super User, so Domino permits complete access.

- If you want to authenticate each user before allowing access to these files, enter **N**.
13. Enter the name of the Domino Super User. This name must also be in the Domino Directory.
- The Domino Super User is used to authenticate the user at the Domino server if the **SkipDominoAuth** parameter in the WebAgent.conf file is set to **Yes**, or when you want to avoid Domino's authentication process to display resources in an .nsf file.
14. Enter the name of the Domino Default User
- The Default User is used to authenticate with Domino if the current user is not found in the Domino directory. It is also used when a resource is not protected. This user should have a general-purpose level of access. After you specify the Default User, the installation script displays your configuration selections.
15. Enter **Y** if the configuration selections displayed are correct.
16. Edit the WebAgent.conf file:
- Change **enablewebagent=YES**
 - Change **enablefailover=NO**
 - add the secondary (round robin) Policy Server by adding a line under:


```

      policyserver="140.183.234.247, 44441, 44442, 44443"
      policyserver="140.183.234.107, 44441, 44442, 44443"
      policyserver="140.183.234.158, 44441, 44442, 44443"
      (if it was not added above)
      
```
17. Restart the Domino server.

Adding the Domino Web Agent DLL

For the Domino Web Agent to operate properly, you must add the DominoWebAgent.dll file, *dominowebagent.so*, to the filter DLLs. The Web Agent DLL must be the first DLL in the list.

1. Open Lotus Notes.
2. Select File | Database | Open.
3. In the Server field, select the Domino Server where you installed the Web Agent
4. In the Database scroll box, select the server's address book. In the Filename field you will see the file name names.nsf.
5. Open the Server folder and select Servers.

6. Choose your server and click **Edit Server**.
7. Select the Internet Protocols tab.
8. In the DSAPI section of the dialog box, add the full path to the DSAPI filter file names, for example:

c:\Program Files\Netegrity\SiteMinderWebAgent\Bin\dominowebagent.so

Reconfiguring Web Agents on Domino

Reconfigure a Web Agent for the following reasons:

- You have upgraded the Web Agent and now you need to update the Configuration
- You need to change the configuration settings previously defined for a Web Agent
- You need to remove the configuration settings from the Web Agent without uninstalling the entire Web Agent (you would need to configure the Web Agent again at a later time)

To reconfigure a Web Agent on Domino

1. Navigate to the netegrity/siteminder/ directory.
2. Enter **smwebagent-config** to run the configuration script.
3. At the prompt to configure a Domino Web server, enter **Y**.

The configuration script detects and lists the installed Web servers. It then provides you with the following options:

- (o)verwrite the configuration with new settings you specify
- (p)reserve settings but update the configuration
- (r)emove the configuration, or
- (l)eave the web server configured as it is and cancel the configuration

4. Complete one of the following:
 - To change the existing configuration settings, enter **o** and complete steps 5-15.
 - To update the configuration of a Web Agent that you upgraded and retain the configuration settings that were initially defined for it, enter **p** and at the prompt, confirm the settings. The configuration is now upgraded.
 - To remove the configuration settings from the Web Agent, enter **r** and at the prompt, confirm the removal. Before you use the Web Agent again, you must configure it.
 - To exit the configuration script without changing the configuration settings, enter **l**.

5 ARMYPERSON SCHEMA

5.1 Attribute Names and Definition

Attribute Name	Field Contents	Data Source	Access restrictions
<i>Standard LDAP attributes</i>			
cn	Populated with the same value as UID	Registration process	Available to any authenticated AKO user
sn	Surname	Registration process	Available to any authenticated AKO user
description	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
facsimiletelephonenumber	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
generationQualifier	<i>Not used</i>		<i>Restricted</i>
givenname	First Name	Registration process	Available to any authenticated AKO user
homephone	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
jpegphoto	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
mail	AKO e-mail address, form is "cn@us.army.mil"	Registration process	Available to any authenticated AKO user
photo	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
postaladdress	Organization Address inputed by user during registration	Registration process	<i>Restricted</i>
postalcode	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
state/province	Populated with the same value as armystateorprovincename		<i>Restricted</i>
street	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
telephonenumber	<i>Not used</i>	<i>Not Populated</i>	<i>Restricted</i>
title	Rank for military, title for others	TAPDB (for military) User modifiable for non-military	Available to any authenticated AKO user
uid	Populated with the same value as CN	Registration process	Available to any authenticated AKO user
usercertificate			
userpassword	hashed	User modifiable	<i>Restricted</i> (allowed for compare, not for read)

x500uniqueidentifier	<i>Not used</i>	<i>Not Populated</i>	Restricted
country			Restricted
mailForwardingAddress	User's e-mail Forwarding Address	User modifiable	Restricted
Army specific LDAP extensions			
armyAccountType	Types of accounts representing AKO user base	TAPDB (for military, DA civilians)	Available to any authenticated AKO user
armyActivationDate	Date of activation of guest account	Registration process	Restricted
ArmyAOC1	Primary AOC for Officers	TAPDB	Available to any authenticated AKO user
ArmyAOC2	Secondary AOC for Officers	TAPDB	Available to any authenticated AKO user
armyBABR	See Basic Branch Table, Column 1	TAPDB (for military)	Available to any authenticated AKO user
armyBABRDesc	See Basic Branch Table, Column 2	TAPDB (for military)	Available to any authenticated AKO user
armyBrowser	Type of browser the used during registration	Registration process	Restricted
armyCategory	F – Full Account G – Guest Account	<i>Not Populated</i>	Restricted
armyCFD	<i>Not used</i>	<i>Not Populated</i>	Restricted
armyChangePWDDate	Date of last password change	<i>Not Populated</i>	Restricted
armyCINC	See CINC Table, Column 1	<i>Not Populated</i>	Restricted
armyCINCDesc	See CINC Table, Column 2	<i>Not Populated</i>	Restricted
armyCity	City of current station	<i>Not Populated</i>	Restricted
armyCOBO	Country of Birth Officer	<i>Not Populated</i>	Restricted
armyComment	Reserved space for freeform text	<i>Not Populated</i>	Restricted
armyCompany	<i>Not used</i>	<i>Not Populated</i>	Restricted
armyCountry	USA	<i>Not Populated</i>	Restricted
armyCRMGOFF	Current Management Office (for Officers)	<i>Not Populated</i>	Restricted
armyCHRSVC	Status of Discharge	TAPDB (for military)	Restricted

<i>armyDepartment</i>	Department currently attached to	<i>Not Populated</i>	Restricted
<i>armyDOB</i>	Date of Birth	<i>Not Populated</i>	Restricted
<i>armyEDIPI</i>	DOD-wide unique identifier for electronic systems, generated by DEERS.	DEERS	Restricted
<i>armyExternalMail</i>	Email address outside of AKO for sending notices	Registration process, updatable by User	Available to any authenticated AKO user
<i>armyHQDA</i>	See HQDA Table, Column 1	<i>Not Populated</i>	Restricted
<i>armyHQDADesc</i>	See HQDA Table, Column 2	<i>Not Populated</i>	Restricted
<i>armyIP</i>	IP of the computer the user is using	Registration process	Restricted
<i>armyKey</i>	Lost Password Key	Registration process	Restricted
<i>armyLapsedAccounts</i>	Guest accounts that have lapsed due to Sponsor inactivity.		Restricted
<i>armyLocation</i>	Continental Location	<i>Not Populated</i>	Restricted
<i>armyMACOM</i>	MACOM Code	TAPDB – decoded from the UIC	Restricted
<i>armyMiddleName</i>	Middle names for those who wish to have one in the directory	Registration process	Available to any authenticated AKO user
<i>armyMOS</i>	Primary Military Occupational Specialty - See MOS Column 1	TAPDB (for military)	Available to any authenticated AKO user
<i>armyMOSDesc</i>	Description of the Primary Military Occupational Specialty - See MOS Column 2	TAPDB (for military)	Available to any authenticated AKO user
<i>armyMOS2</i>	Current Military Occupational Specialty - See MOS Table, Column 1	TAPDB (for military)	Available to any authenticated AKO user
<i>armyMOS2Desc</i>	Description of the Current Military Occupational Specialty - See MOS Table, Column 2	TAPDB (for military)	Available to any authenticated AKO user
<i>armyNickName</i>	Name the user wishes to be called	Registration process	Restricted

<i>armyOrganizationalUnit</i>	Description of the Current Organization of the user	Registration process	Restricted
<i>armyOriginalACType</i>	Account type at time of registration	Registration process	Restricted
<i>armyOrigPWD</i>	Password at time of registration (hashed)	Registration process	Restricted
<i>armyPending</i>	Guest accounts pending approval	Registration process	Restricted
<i>armyPhoneNumber</i>	Current Duty Phone Number	Registration process, updatable by User	Restricted
<i>armypromin</i>	Identifies COL(P)	TAPDB	Restricted
<i>ArmyRank</i> <i>Note: planned replacement of armyRank by the 2 fields armyGrade and armyPGRAD</i>	Grade designated from TAPDB	TAPDB (for military and DA civilians)	Available to any authenticated AKO user
<i>armyGrade</i>	Grade designated from TAPDB, in the form: O-1, 2, 3, 4.... E-1, 2, 3, 4, 5,	TAPDB (for military and DA civilians)	Available to any authenticated AKO user
<i>armyPGRAD</i>	Grade code from TAPDB, in the form: L5, K5, J5, I5, ... Z5, Y5, X5, W6, W5, V5,	TAPDB (for military and DA civilians)	Available to any authenticated AKO user
<i>armyRevokeDate</i>	Date of revocation of guest account	Not Populated	Restricted
<i>armySOB</i>	State of Birth	Not Populated	Restricted
<i>armySponsor</i>	Account sponsoring the guest account	Registration process	Restricted
<i>armySponsored</i>	Guest accounts sponsored by full account	Registration process	Restricted
<i>armySSI</i>	-		Restricted
<i>armySSN</i>	Social Security Number	Registration process	Restricted
<i>armyStateorProvinceName</i>	State of current Station	Not Populated	Restricted
<i>armyStatus</i>	Status of the Account	TAPDB, guest expiration process	Restricted

<i>armySuffix</i>	Suffix of user names	Registration process	<i>Restricted</i>
<i>armyTimeZone</i>	Time Zone of User	<i>Not Populated</i>	<i>Restricted</i>
<i>armyUIC</i>	UIC code of user	TAPDB	<i>Restricted</i>
<i>armyUserRank</i>	User Entered Rank	<i>Not Populated</i>	<i>Restricted</i>
<i>armyYearsOfService</i>	Years Served		<i>Restricted</i>
<i>armyZipCode</i>	Zip code of current Station		<i>Restricted</i>

5.2 Account Types

The value of "armyAccountType" is populated at account creation for all account types, and periodically refreshed from TAPDB, for Army personnel. When a "full" account holder changes their Army status, the armyAccountType is updated. For example, when a soldier leaves active duty and becomes a reservist, the armyAccountType is changes from AA to RE. If a soldier retires and becomes a DA Civilian, the armyAccountType changes from AR to DA. The order of precedence in determining armyAccountType is: Active Army, DA civilian, retired, reserve, guard, and NAF.

Non-appropriated Funds civilians are included in the Army personnel system, and are granted a "full" account of type "NF".

United States Military Academy cadets are granted a "full" account of type "WC".

Contracted ROTC cadets (typically juniors and seniors are granted a "full" account of type "RC".

Non-contracted ROTC cadets (typically freshmen and sophomores are granted a "guest" account of type "CA". Upon accession to contacted ROTC status, these are auotmatically upgraded to a "full" account of type "RC".

Local Nationals are coded "LN", as "guest" accounts, in the AKO Directory.

Account Abbreviation	Account Description
Full Account Types	
AA	Active Army
AR	Army Retired
MR	Medical Retired
NG	National Guard
RE	Army Reserves
DA	Department of the Army (DA) Civilian
NF	Non-appropriated Funds DA civilian
WC	USMA cadet
RC	ROTC Cadet - Contracted
AC	Administrative Contractor (AKO SysAdmins)
Guest Account Types	
MD	Medical Discharged
IE	Initial Entry Recruit
LN	Local National Employee
DC	DoD Civilian
AV	Army Volunteer
CO	Contractor
DR	DA Civilian, Retired
FM	Family Member
FO	Foreign Officer
CA	ROTC Cadet – not contracted

AF	US Air Force
CG	US Coast Guard
MC	US Marine Corps
NA	US Navy
HS	Homeland Security
FC	Federal Civilian Agencies

5.3 Branch Codes

TAPDB_CODE	5.3.1.1.1.1 DESCRIPTION
AD	AIR DEFENSE ARTILLERY
AG	ADJUTANT GENERAL
AN	ARMY NURSE CORPS
AR	ARMOR
AV	AVIATION
CA	CIVIL AFFAIRS (RESERVE AND GUARD ONLY)
CH	CHAPLAINS
CM	CHEMICAL
DE	DENTAL CORPS
DL	BRANCH UNASSIGNED (RESERVES ONLY)
EN	ENGINEER
FA	FIELD ARTILLERY
FI	FINANCE
GO	GENERAL OFFICERS (NOT USED BY ACTIVE COMPONENT)
IN	INFANTRY
JA	JUDGE ADVOCATE GENERAL CORPS
MC	MEDICAL CORPS
MI	MILITARY INTELLIGENCE
MP	MILITARY POLICE
MS	MEDICAL SERVICE CORPS
NC	NON-COMMISSIONED OFFICER
OD	ORDNANCE
QM	QUARTERMASTER
SC	SIGNAL

SF	SPECIAL FORCES
SP	ARMY MEDICAL SPECIALIST CORPS
SS	STAFF SPECIALIST
TC	TRANSPORTATION
VC	VETERINARY CORPS
WC	WOMENS ARMY CORPS (HISTORY ONLY)

5.4 CINC

CINC Abbreviation	CINC Description
NONE	None
USCENTCOM	United States Central Command
USEUCOM	United States European Command
USJFCOM	United States Joint Forces Command
USPACOM	United States Pacific Command
USSOUTHCOM	United States Southern Command
USSPACECOM	United States Space Command
USSOCOM	United States Special Operations Command
USSTRATCOM	United States Strategic Command
USTRANSCOM	United States Transportation Command

5.5 HQDA Functional Area

HQDA Abbreviation	HQDA Description
NONE	None
ODCSINT	Office of the Deputy Chief of Staff for Intelligence (Army)
ODCSLOG	Office of the Deputy Chief Of Staff, Logistics
ODCSOPS	Office of the Deputy Chief of Staff, Operations & Plans
ODCSPERS	Office of the Deputy Chief of Staff, Personnel
ODISC4	Office of the Director of Information Systems for Command, Control, Communications & Computers (Army)
ACSIM	Assistant Chief of Staff for Installation Management
ASA (FM)	Assistant Secretary of the Army (Financial Management)
PA&ED	Program Analysis & Evaluation Directorate
OCE	Office of the Chief of Engineers
OASG	Office of the Army Surgeon General
ARNG	Army National Guard
OTJAG	Office of the Judge Advocate General
OCCH	Office of the Chief of Chaplains
USACFSC	United States Army Community and Family Support Center
CSA GRP	Chief of Staff Initiative Group

5.6 Location

Location
CONUS
OCONUS-Korea
OCONUS- Europe
OCONUS-Other

5.7 MACOM

MACOM Abbreviation	MACOM Description
NONE	None
MTMC	Military Traffic Management Command
USACE	U.S. Army Corps of Engineers
USACIDC	U.S. Army Criminal Investigation Command
FORSCOM	Forces Command
HSC	U.S. Army Health Services Command
USAISC	U.S. Army Information Systems Command
INSCOM	U.S. Army Intelligence and Security Command
USAMC	U.S. Army Materiel Command
MDW	U.S. Army Military District of Washington
USASOC	U.S. Army Special Operations Command
TRADOC	U.S. Army Training and Doctrine Command
USAREUR	U. S. Army Europe
USARPAC	U. S. Army Pacific Command
EUSA	Eighth U. S. Army
MEDCOM	Medical Command
ATEC	Army Test and Evaluation Command
USMA	United States Military Academy
SMDC	Space and Missile Defense Command
USARSO	U.S. Army South

5.8 MOS / Career Fields

Officer Branch and Functional Area codes

TAPDB_CODE	DESCRIPTION
11	INFANTRY
12	ARMOR
13	FIELD ARTILLERY
14	AIR DEFENSE ARTILLERY
15	AVIATION
18	SPECIAL FORCES
21	CORPS OF ENGINEERS
24	INFORMATION SYSTEMS ENGINEERING
25	SIGNAL CORPS
30	INFORMATION OPERATIONS
31	MILITARY POLICE CORPS
34	STRATEGIC INTELLIGENCE
35	MILITARY INTELLIGENCE
38	CIVIL AFFAIRS (RC ONLY)
39	PSYCHOLOGICAL OPERATIONS AND CIVIL AFFAIRS DESIGNATED
40	SPACE OPERATIONS
41	PERSONNEL PROGRAMS MANAGEMENT
42	ADJUTANT GENERAL'S CORPS
43	HUMAN RESOURCES MANAGEMENT
44	FINANCE CORPS
45	COMPTROLLER
46	PUBLIC AFFAIRS
47	ACADEMY PROFESSOR, UNITED STATES MILITARY ACADEMY
48	FOREIGN AREA OFFICER
49	OPERATIONS RESEARCH/SYSTEMS ANALYSIS
50	FORCE MANAGEMENT
51	ARMY ACQUISITION CORPS
52	NUCLEAR RESEARCH AND OPERATIONS
53	INFORMATION SYSTEMS MANAGEMENT
54	OPERATIONS, PLANS, AND TRAINING
55	JUDGE ADVOCATE GENERAL'S CORPS
56	CHAPLAIN CORPS
57	SIMULATIONS OPERATIONS
59	STRATEGIC PLANS AND POLICY
60	MEDICAL CORPS
61	MEDICAL CORPS
62	MEDICAL CORPS

63	DENTAL CORPS
64	VETERINARY CORPS
65	ARMY MEDICAL SPECIALIST CORPS
66	ARMY NURSE CORPS
67	MEDICAL SERVICE CORPS
68	MEDICAL SERVICE CORPS
70	FIELD MEDICAL ASSISTANT
74	CHEMICAL CORPS
88	TRANSPORTATION CORPS
90	MULTIFUNCTIONAL LOGISTICIAN
91	ORDNANCE CORPS
92	QUARTERMASTER CORPS

Warrant Officer MOS Codes

001A	UNQUALIFIED IN AUTHORIZED WARRANT OFFICER MOS
002A	PATIENT
003A	STUDENT
004A	DUTIES UNASSIGNED OR IN TRANSIT
011A	BRANCH/MOS IMMATERIAL
131A	FIELD ARTILLERY TARGETING
140A	COMMAND AND CONTROL SYSTEM TECHNICIAN
140B	FAAD SYSTEM TECHNICIAN
140D	HAWK SYSTEM TECH
140E	PATRIOT SYSTEM TECH
150A	AIR TRAFFIC CONTROL TECHNICIAN
151A	AVIATION MAINTENANCE TECHNICIAN
152B	OH-58A/C SCOUT PILOT
152C	OH-6 SCOUT PILOT
152D	OH-58D SCOUT PILOT
152F	AH-64 PILOT
152G	AH-1 PILOT
152H	AH-64D ATTACK PILOT
153A	ROTARY WING AVIATOR (AIRCRAFT NONSPECIFIC)
153B	UH-1 PILOT
153D	UH-60 PILOT
153E	MH-60 PILOT
154C	CH-47D PILOT
154E	MH-47 PILOT
155A	FIXED WING AVIATOR (AIRCRAFT NONSPECIFIC)
155D	U-21 PILOT

155E	C-12 PILOT
155F	JET AIRCRAFT PILOT
155G	O-5A/EO-5B/RC-7 PILOT
180A	SPECIAL FORCES TECHNICIAN
210A	UTILITIES OPERATION AND MAINTENANCE TECHNICIAN
215D	TERRAIN ANALYSIS TECHNICIAN
250A	COMMUNICATIONS SECURITY TECHNICIAN
250B	TACTICAL AUTOMATED NETWORK TECHNICIAN
250N	NETWORK MANAGEMENT TECHNICIAN
251A	DATA PROCESSING TECHNICIAN
311A	CID SPECIAL AGENT
350B	ALL SOURCE INTELLIGENCE TECHNICIAN
350D	IMAGERY INTELLIGENCE TECHNICIAN
350L	ATTACHE TECHNICIAN
351B	COUNTERINTELLIGENCE SPECIAL AGENT
351C	AREA INTELLIGENCE TECHNICIAN
351E	INTERROGATION TECHNICIAN
352C	TRAFFIC ANALYSIS TECHNICIAN
352D	EMITTER LOCATION/IDENTIFICATION TECHNICIAN
352G	VOICE INTERCEPT TECHNICIAN
352H	MORSE INTERCEPT TECHNICIAN
352J	EMANATIONS ANALYSIS TECHNICIAN
352K	NON-MORSE INTERCEPT TECHNICIAN
353A	IEW EQUIPMENT TECHNICIAN
420A	MILITARY PERSONNEL TECHNICIAN
420C	BANDMASTER
550A	LEGAL ADMINISTRATOR
600A	PHYSICIAN ASSISTANT
640A	VETERINARY SERVICES TECHNICIAN
670A	PELL SERVICES MAINTENANCE TECHNICIAN
880A	MARINE DECK OFFICER
881A	MARINE ENGINEERING OFFICER
882A	MARINE MOBILITY OFFICER
910A	AMMUNITION TECHNICIAN
912A	LAND COMBAT MISSILE SYSTEMS TECHNICIAN
913A	ARMAMENT REPAIR TECHNICIAN
914A	ALLIED TRADES TECHNICIAN
915A	UNIT MAINT TECH (LIGHT)
915D	UNIT MAINT TECH (HEAVY)
915E	SUPPORT MAINTENANCE TECHNICIAN
916A	HIGH TO MEDIUM ALTITUDE AIR DEFENSE (HIMAD) SYSTEM TECH

917A	MANEUVER FORCES AIR DEFENSE (MFADS) SYSTEM TECH
918A	TEST MEASUREMENT AND DIAGNOSTIC EQUIPMENT MAINT SPT TECH
918B	ELECT SYSTEM MAINTENANCE TECHNICIAN
919A	ENG EQUIP REP TECH
920A	PROPERTY BOOK TECHNICIAN
920B	SUPPLY SYSTEMS TECHNICIAN
921A	AIRDROP SYSTEMS TECHNICIAN
922A	FOOD SERVICE TECHNICIAN

Enlisted MOS Codes

00B	DIVER
00D	SPECIAL DUTY ASSIGNMENT
00U	EQUAL OPPORTUNITY
00Z	CMD SGT MAJOR
02B	CORNET OR TRUMPET PLAYER
02C	BARITONE OR EUPHONIUM PLAYER
02D	FRENCH HORN PLAYER
02E	TROMBONE PLAYER
02F	TUBA PLAYER
02G	FLUTE OR PICCOLO PLAYER
02H	OBOE PLAYER
02J	CLARINET PLAYER
02K	BASSOON PLAYER
02L	SAXOPHONE PLAYER
02M	PERCUSSION PLAYER
02N	PIANO PLAYER
02S	SPECIAL BAND MEMBER
02T	GUITAR PLAYER
02U	ELECTRIC BASS PLAYER
02Z	BANDS SENIOR SERGEANT
09B	TRAINEE, UNASSIGNED
09C	TRAINEE, LANGUAGE
09D	COLLEGE TRAINEE
09R	SIMULTANEOUS MEMBERSHIP PROGRAM
09S	COMMISSIONED OFFICER CANDIDATE
09T	COLLEGE STUDENT ARMY NATIONAL GUARD OFFICER PROGRAM (CSOP)
09W	WARRANT OFFICER CANDIDATE
11B	INFANTRYMAN
11C	INDIRECT FIRE INFANTRYMAN
11H	HEAVY ANTIARMOR WEAPONS INFANTRYMAN

11M	FIGHTING VEHICLE INFANTRYMAN
11X	INFANTRY RECRUIT
11Z	INFANTRY SENIOR SERGEANT
12B	COMBAT ENGINEER
12C	BRIDGE CREWMEMBER
12Z	COMBAT ENGINEERING SENIOR SERGEANT
13B	CANNON CREWMEMBER
13C	TACFIRE OPERATIONS SPECIALIST
13D	FIELD ARTILLERY TACTICAL DATA SYSTEM SPECIALIST
13E	CANNON FIELD SPECIALIST
13F	FIRE SUPPORT SPECIALIST
13M	MULTIPLE LAUNCH ROCKET SYSTEM (MLRS) CREWMEMBER
13P	MULT LAUNCH ROCKET SYS/LANCE OPERATIONS/FIRE DIRECTION SPEC
13R	FIELD ARTILLERY FIREFINDER RADAR OPERATOR
13Z	FIELD ARTILLERY SENIOR SERGEANT
14D	HAWK MISSILE SYSTEM CREWMEMBER
14E	PATRIOT FC ENH OP/MNT
14J	AD C4I TACTICAL OPERATIONS CEN ENH OPERATOR/MAINT
14L	AN/TSQ-73 CCS OP/MNT (RC)
14M	MANPADSRMBR (RC)
14R	LINE OF SIGHT-FORWARD-HEAVY CREWMEMBER
14S	AVENGER CREWMASTER
14T	PATRIOT LS ENH OP/MNT
14Z	ADA SENIOR SERGEANT
16X	AIR DEFENSE RECRUIT
18B	SPECIAL FORCES WEAPONS SERGEANT
18C	SPECIAL FORCES ENGINEER SERGEANT
18D	SPECIAL FORCES MEDICAL SERGEANT
18E	SPECIAL FORCES COMMUNICATIONS SERGEANT
18F	SF ASST OP&INTEL SGT
18X	SF RECRUIT
18Z	SPECIAL FORCES SENIOR SERGEANT
19D	CAVALRY SCOUT
19K	M1 ARMOR CREWMAN
19Z	ARMOR SENIOR SERGEANT
23R	HAWK MISSILE SYSTEM MECHANIC
25M	MEDIA ILLUSTRATOR
25R	VISUAL INFORMATION/AUDIO EQUIPMENT REPAIRER
25V	COMBAT DOCUMENTATION/PRODUCTION SPEC
25Z	VISUAL INFORMATION CHIEF
27E	TOW/Dragon REPAIRER

27G	CHAPARRAL/REDEYE REPAIRER
27M	MULTIPLE LAUNCH ROCKET SYSTEM REPAIRER
27T	PEDESTAL MOUNTED STINGER, LINE OF SIGHT
27X	PATRIOT SYSTEM REPAIRER
27Z	LAND COMBAT/AIR DEFENSE SYSTEMS MAINTENANCE CHIEF
31C	SINGLE CHANNEL RADIO OPERATOR
31F	MOBILE SUBSCRIBER EQUIPMENT NETWORK SWITCHING SYSTEM OPRTR
31L	WIRE SYSTEMS INSTALLER
31P	MICROWAVE SYSTEMS OPERATOR-MAINTAINER
31R	MCHAN XMSN SYS OP MNT
31S	SATELLITE COMMUNICATIONS SYSTEMS OPERATOR-MAINTAINER
31T	SATELLITE/MICROWAVE SYSTEMS CHIEF
31U	SIGNAL SUPPORT SYSTEMS SPECIALIST
31W	MOBILE SUBSCRIBER EQUIPMENT COMMUNICATIONS CHIEF
31Z	COMMUNICATIONS-OPERATIONS CHIEF
33W	EW/I SYSTEMS REP
35B	LCSS TEST SPECIALIST
35C	SURVEY RDE REPRESENTATIVE
35D	ATC EQUIP REP
35E	RADIO COM SEC REPRESENTATIVE
35F	SP ELECT DEVICES REPRESENTATIVE
35H	TEST MEASUREMENT & DIAGNOSTIC EQUIP MAINTENANCE SUPPORT SPEC
35J	COMPUTER/AUTOMATION SYSTEM REPAIRER
35L	AVIONIC COMM EQ REP
35M	RADAR REPRESENTATIVE
35N	WIRE SYSTEM EQUIP REP
35R	AVIONIC SPECIAL EQUIPMENT REPAIRER
35W	ELECT MAINTENANCE CHIEF
35Y	INTEGRATED FAMILY OF TEST EQUIP OPER/MAINT
35Z	SR ELECT MAINTENANCE CHIEF
37F	PSYCHOLOGICAL OPERATIONS SPECIALIST
38A	CIVIL AFFAIRS SPECIALIST
39B	AUTOMATIC TEST EQUIPMENT OPERATOR/MAINTAINER
42E	OPTICAL LABORATORY SPECIALIST
43M	FABRIC REPAIR SPECIALIST
44B	METAL WORKER
44E	MACHINIST
45B	SMALL ARMS REPAIRER
45D	SELF PROPELLED FIELD ARTILLERY TURRET MECHANIC
45E	M1 ABRAMS TANK TURRET MECHANIC
45G	FIRE CONTROL SYSTEMS REPAIRER

45K	TANK TURRET REPAIRER
45N	M60A1/A3 TANK TURRET MECHANIC
45T	BRADLEY FIGHTING VEHICLE SYSTEM TURRET MECHANIC
46Q	JOURNALIST
46R	BROADCAST JOURNALIST
46Z	PUBLIC AFFAIRS CHIEF .
51B	CARPENTRY AND MASONRY SPECIALIST
51H	CONSTRUCTION ENGINEERING SUPERVISOR
51K	PLUMBER
51M	FIREFIGHTER
51R	INTERIOR ELECTRICIAN
51T	TECHNICAL ENGINEERING SUPERVISOR
51Z	GENERAL ENGINEERING SUPERVISOR
52C	UTILITIES EQUIPMENT REPAIRER
52D	POWER GENERATION EQUIPMENT REPAIRER
52E	PRIME POWER PRODUCTION SPECIALIST
52G	TRANSMISSION AND DISTRIBUTION SPECIALIST
52X	SPECIAL PURPOSE EQUIPMENT REPAIRER
54B	CHEMICAL OPERATIONS SPECIALIST
55B	AMMUNITION SPECIALIST
55D	EXPLOSIVE ORDNANCE DISPOSAL SPECIALIST
57E	LAUNDRY AND BATH SPECIALIST
62B	CONSTRUCTION EQUIPMENT REPAIRER
62E	HEAVY CONSTRUCTION EQUIPMENT REPAIRER
62F	CRANE OPERATOR
62G	QUARRYING SPECIALIST
62H	CONCRETE AND ASPHALT EQUIPMENT OPERATOR
62J	GENERAL CONSTRUCTION EQUIPMENT OPERATOR
62N	CONSTRUCTION EQUIPMENT OPERATOR
63A	ABRAMS TANK SYSTEM MAINTAINER
63B	LIGHT WHEEL VEHICLE MECHANIC
63D	SELF-PROPELLED FIELD ARTILLERY SYSTEM MECHANIC
63E	M1 ABRAMS TANK SYSTEM MECHANIC
63G	FUEL AND ELECTRICAL SYSTEMS REPAIRER
63H	TRACK VEHICLE REPAIRER
63J	QUARTERMASTER AND CHEMICAL EQUIPMENT REPAIRER
63M	BRADLEY FIGHTING VEHICLE SYSTEM (BFVS MAINTAINER)
63N	M60A1/AE TANK SYSTEM MECHANIC
63S	HEAVY-WHEEL VEHICLE MECHANIC
63T	BRADLEY FIGHTING VEHICLE SYSTEM MECHANIC
63W	WHEEL VEHICLE REPAIRER

63Y	TRACK VEHICLE MECHANIC
63Z	MECHANICAL MAINTENANCE SUPERVISOR
67G	UTILITY AIRPLANE REPAIRER (RC)
67N	UTILITY HELICOPTER REPAIRER
67R	AH-64 ATTACK HELICOPTER REPAIRER
67S	SCOUT HELICOPTER REPAIRER
67T	TACTICAL TRANSPORT HELICOPTER REPAIRER
67U	MEDIUM HELICOPTER REPAIRER
67V	OBSERVATION/SCOUT HELICOPTER REPAIRER
67Y	AH-1 ATTACK HELICOPTER REPAIRER
67Z	AIRCRAFT MAINTENANCE SENIOR SERGEANT
68B	AIRCRAFT POWERPLANT REPAIRER
68D	AIRCRAFT POWERTRAIN REPAIRER
68F	AIRCRAFT ELECTRICIAN
68G	AIRCRAFT STRUCTURAL REPAIRER
68H	AIRCRAFT PNEUDRAULICS REPAIRER
68J	AIRCRAFT ARMAMENT/MISSILE SYSTEM REPAIRER
68K	AIRCRAFT COMPONENTS REPAIR SUPERVISOR
68N	AVIONIC MECHANIC
68P	AVIONIC MAINTENANCE SUPERVISOR
68X	ARM/ELECT SYS REP
68Y	AH-64D ARM/ELL/AV SYS
71D	LEGAL SPECIALIST
71G	PATIENT ADMINISTRATION SPECIALIST
71L	ADMINISTRATIVE SPECIALIST
71M	CHAPLAIN ASSISTANT
73C	FINANCE SPECIALIST
73D	ACCOUNTING SPECIALIST
73Z	FINANCE SENIOR SERGEANT
74B	INFORMATION SYSTEM OPR-ANALYST
74C	RECORD TELECOMMUNICATIONS CENTER OPERATOR
74G	TELECOM CMPT OPR-MNT
74Z	DATA PROCESSING NCO
75B	PERSONNEL ADMINISTRATION SPECIALIST
75F	PERSONNEL INFORMATION SYSTEM MANGEMENT SPECIALIST
75H	PERS SVC SPC
76J	MEDICAL SUPPLY SPECIALIST
77F	PETROLEUM SUPPLY SPECIALIST
77L	PETROLEUM LABORATORY SPECIALIST
77W	WATER TREATMENT SPECIALIST
79R	RECRUITER

79S	CAREER COUNSELOR
79T	RCTR & RETN NCO
81L	LITHOGRAPHER
81T	TOPOGRAPHIC ANALYST
81Z	TOPOGRAPHIC ENGINEERING SUPERVISOR
82C	FIELD ARTILLERY SURVEYOR
82D	TOPOGRAPHIC SURVEYOR
88H	CARGO SPECIALIST
88K	WATERCRAFT OPERATOR
88L	WATERCRAFT ENGINEER
88M	MOTOR TRANSPORTATION OPERATOR
88N	TRAFFIC MANAGEMENT COORDINATOR
88P	LOCOMOTIVE REPAIRER (RC)
88T	RAILWAY SECTION REPAIRER (RC)
88U	LOCOMOTIVE OPERATOR (RC)
88X	RAILWAY SENIOR SERGEANT (RC)
88Z	TRANSPORTATION SENIOR SERGEANT
91A	MEDICAL EQUIPMENT REP
91B	MEDICAL NCO
91C	PRACTICAL NURSE
91D	OPERATING ROOM SPECIALIST
91E	DENTAL SPECIALIST
91K	MEDICAL LAB SPECIALIST
91M	HOSP FOOD SVC SP
91P	X-RAY SPECIALIST
91Q	PHARMACY SPECIALIST
91R	VETERINARY FOOD INSPECTION SPECIALIST
91S	PREVENTIVE MEDICINE SPECIALIST
91T	ANIMAL CARE SPECIALIST
91V	RESPIRATORY SPECIALIST
91X	MENTAL HEALTH SPECIALIST
92A	AUTOMATED LOGISTICAL SPECIALIST
92G	FOOD SERVICE OPS
92M	MORTUARY AFFAIRS SPECIALIST
92R	PARACHUTE RIGGER
92Y	UNIT SUPPLY SPECIALIST
92Z	SENIOR NONCOMMISSIONED LOGISTICIAN
93C	AIR TRAFFIC CONTROL (ATC) OPERATOR
93F	FIELD ARTILLERY METEOROLOGICAL CREWMEMBER
93P	AVIATION OPERATIONS SPECIALIST
95B	MILITARY POLICE

95C	CORRECTIONS NCO
95D	CID SPECIAL AGENT
96B	INTELLIGENCE ANALYST
96D	IMAGERY ANALYST
96H	AERIAL INTELLIGENCE SPECIALIST
96R	GROUND SURVEILLANCE SYSTEMS OPERATOR
96U	UAV OPERATOR
96Z	INTELLIGENCE SENIOR SERGEANT
97B	COUNTERINTELLIGENCE AGENT
97E	INTERROGATOR
97L	TRANSLATOR/INTERPRETER
97Z	COUNTERINTELLIGENCE/HUMAN INTELLIGENCE SENIOR SERGEANT
98C	SIGNALS INTELLIGENCE ANALYST
98D	EMITTER LOCATOR/IDENTIFIER
98G	VOICE INTERCEPTOR
98H	MORSE INTERCEPTOR
98J	NONCOMMUNICATIONS INTERCEPTOR/ANALYST
98K	NON-MORSE INTERCEPTOR/ANALYST
98X	EW/SIGINT RECRUIT
98Z	SIGNALS INTELLIGENCE/ELECTRONIC WARFARE CHIEF

5.9 Rank

TapDB Code	Rank Code	Rank Definition	Rank Abbreviation
B5	O11	GENERAL OF THE ARMY	GA
C5	O10	GENERAL	GEN
D5	O9	LIEUTENANT GENERAL	LTG
E5	O8	MAJOR GENERAL	MG
F5	O7	BRIGADIER GENERAL	BG
G5	O6	COLONEL	COL
H5	O5	LIEUTENANT COLONEL	LTC
I5	O4	MAJOR	MAJ
J5	O3	CAPTAIN	CPT
K5	O2	FIRST LIEUTENANT	1LT
L5	O1	SECOND LIEUTENANT	2LT
M1	W5	CHIEF WARRANT OFFICER FIVE	CW5
M5	W4	CHIEF WARRANT OFFICER, FOUR	CW4
N5	W3	CHIEF WARRANT OFFICER, THREE	CW3
O5	W2	CHIEF WARRANT OFFICER, TWO	CW2
P5	W1	WARRANT OFFICER, ONE	WO1
Q5	Q5	CADET U.S. MILITARY ACADEMY	CMA
Q6	Q6	CADET SENIOR ADVANCED ROTC	CSR
R1	E9	SERGEANT MAJOR OF THE ARMY	SMA
R3	E9	COMMAND SERGEANT MAJOR	CSM
R4	E9	STAFF SERGEANT MAJOR	SSM
R5	E9	SERGEANT MAJOR	SGM
S5	E8	FIRST SERGEANT	1SG
S6	E8	MASTER SERGEANT	MSG
T4	E7	MASTER SERGEANT, SEVEN	MS7
T6	E7	PLATOON SERGEANT	PSG
T7	E7	SERGEANT FIRST CLASS	SFC
U4	E6	SERGEANT FIRST CLASS, SIX	SF6
U5	E6	STAFF SERGEANT	SSG
V5	E5	SERGEANT	SGT

W5	E4	CORPORAL	CPL
W6	E4	SPECIALIST	SPC
X5	E3	PRIVATE FIRST CLASS	PFC
Y5	E2	PRIVATE, TWO	PV2
Z5	E1	PRIVATE, ONE	PV1

ⁱ Rank Abbreviation is placed in Title.