How To - Implement Single Sign On Authentication with Active Directory

Applicable to – English version of Windows

This article describes how to implement single sign on authentication with Active Directory integration.

Cyberoam – ADS integration feature allows Cyberoam to map the users and groups from Active Directory for the purpose of authentication.

Prerequisites:

- NetBIOS Domain name
- FQDN Domain name
- Search DN
- Active Directory Server IP address
- Administrator Username and Password (Active Directory Domain)
- IP address of Cyberoam Interface connected to Active Directory server
- Import AD groups

Configuring ADS authentication

Logon to Cyberoam Web Admin Console and follow the below given steps:

Step 1: Create ADS user groups.
Please check Cyberoam version before you continue as this is version specific step.

All Versions below 9.5.3 build 14
Go to Group> Add Group and create all the ADS user groups

For mapping the ADS user groups with the Cyberoam user groups, create all the ADS user groups into Cyberoam before ADS users log on to Cyberoam for the first time. If the ADS groups are not created in Cyberoam, all the users will be assigned to the Default group of Cyberoam.

If all the ADS user groups are created in Cyberoam before users log on to Cyberoam then user will be automatically created in the respective group when they log on to Cyberoam.

Version 9.5.3.14 or above
Instead of creating groups again in Cyberoam, you can import AD groups into Cyberoam using Import Wizard.

One can import groups only after integrating and defining AD parameters into Cybeoam.

If you intend to import group, skip this step.

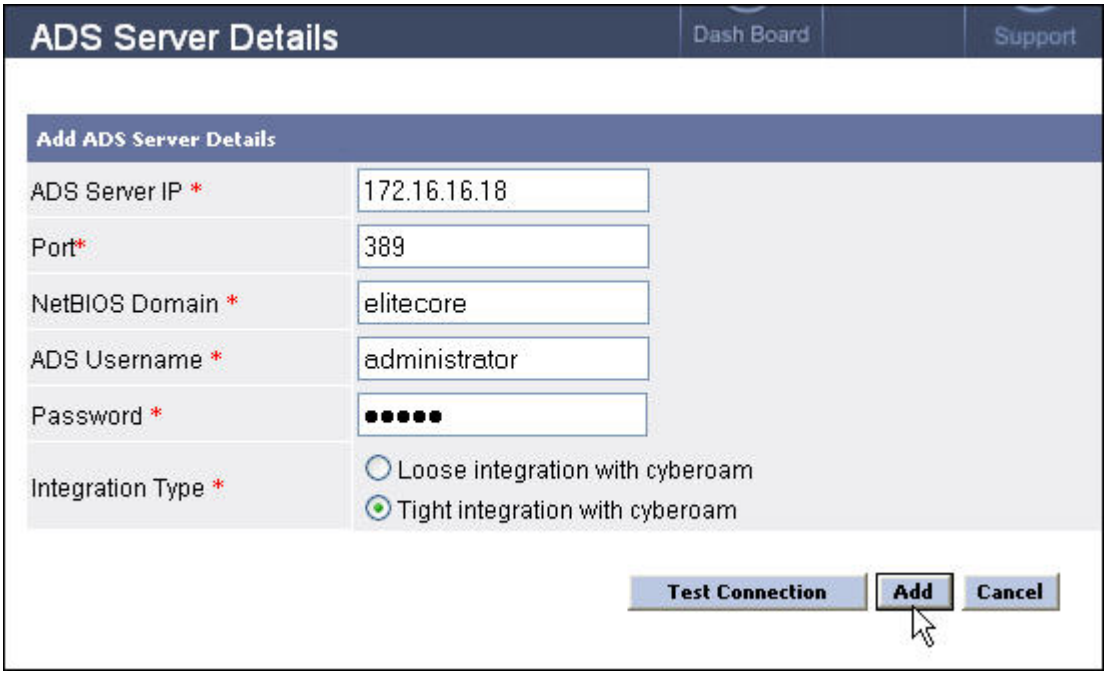
Step 2: Define Authentication parameters
Go to User>Authentication Settings
Select ‘Active Directory’ under Configure Authentication & Integration parameters
Select Default Group.

Cyberoam will create user(s) in the respective groups if groups are already created in Cyberoam otherwise user will be created in the group selected as Default group.

Click Update to save the settings

Step 3: Configure Cyberoam to use Active Directory

Click Add to configure Active Directory parameters
Specify IP address of Active Directory



Specify TCP/IP port number in Port field. It is the port on which ADS server listens for the authentication requests. On Cyberoam appliance, the default port for ADS traffic is 389. If your AD server is using another port, specify port number in Port field.

Specify NetBIOS Domain name. If you do not know NetBIOS name, refer to section 'Determine NetBIOS Name, FQDN and Search DN'.

Specify Active Directory Administrator Username and password

Cyberoam allows implementing AD integration in two ways:

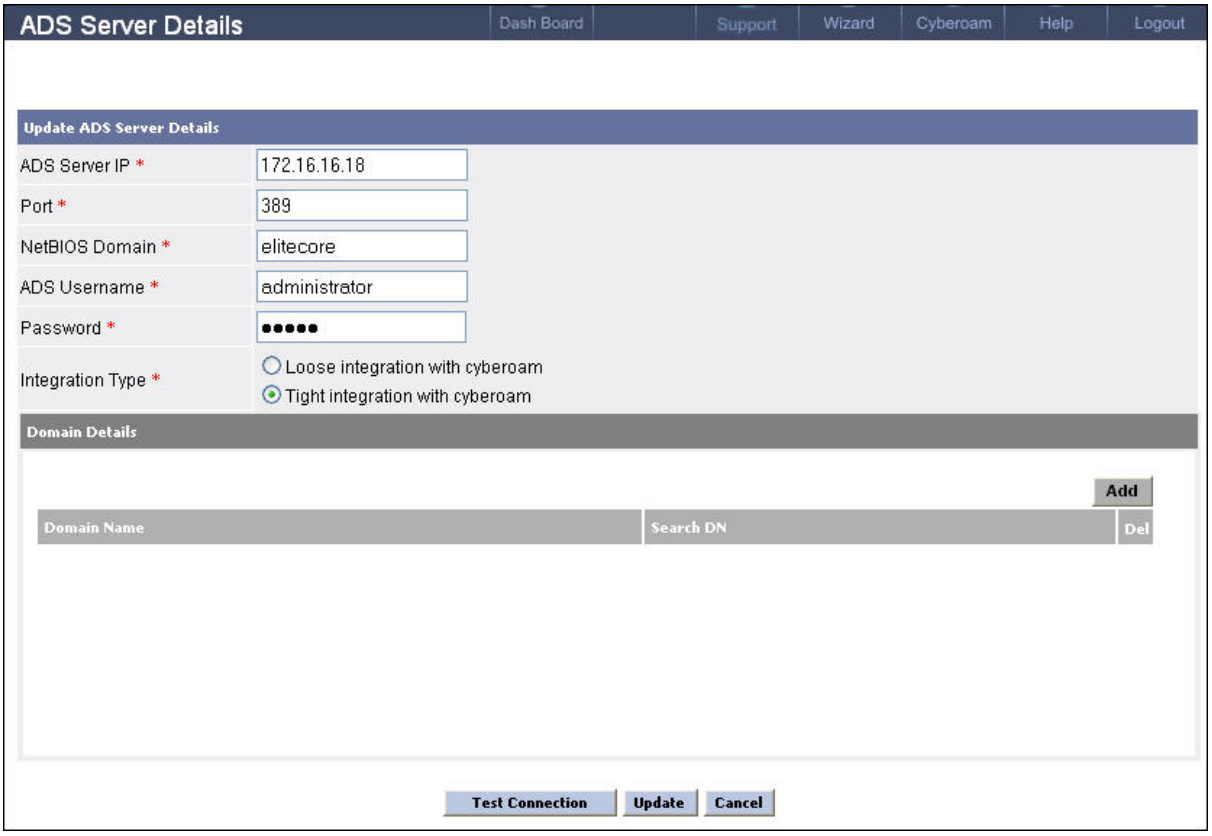
- Tight Integration – With tight integration, Cyberoam synchronizes groups with AD every time the user tries to logon. Hence, even if the group of a user is changed in Cyberoam, on subsequent log in attempt, user logs on as the member of the same group as configured in Active Directory. In this case group membership of each user is as defined in the Active Directory.

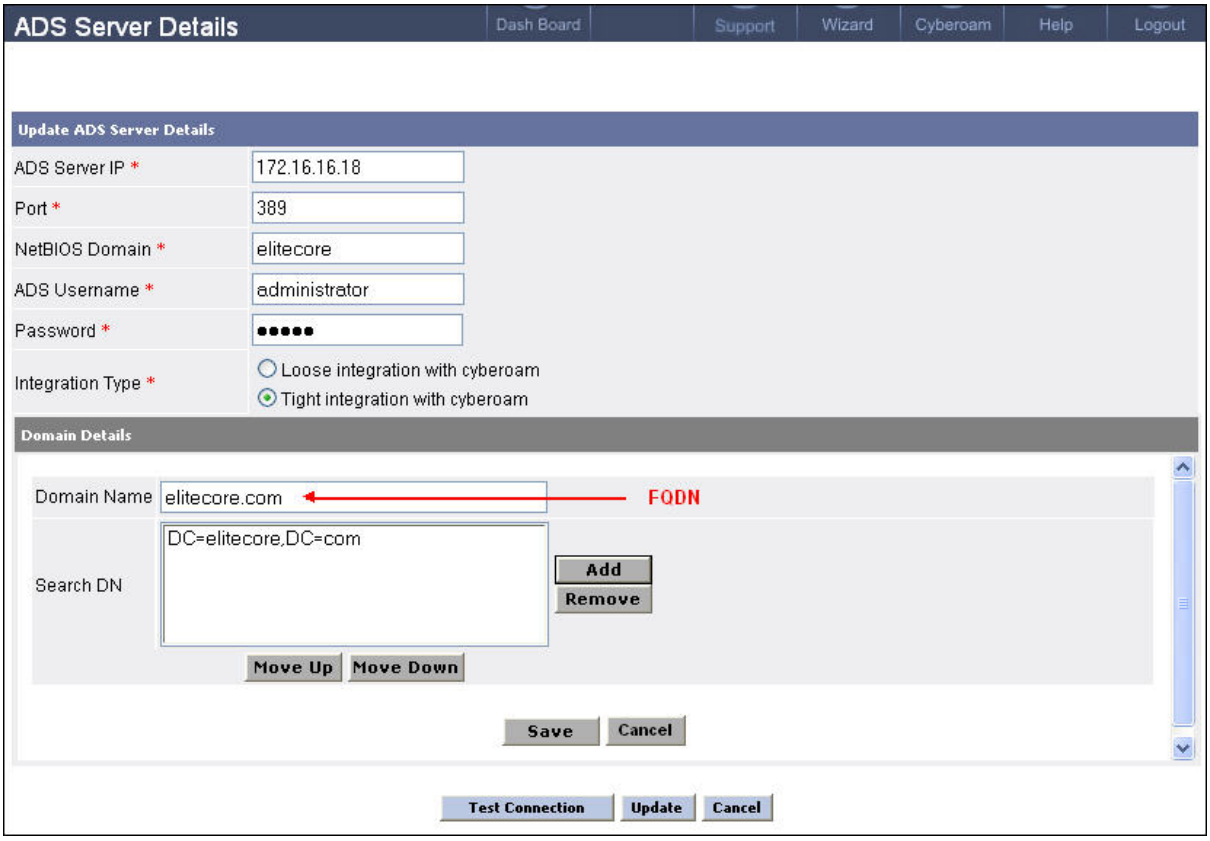
- Loose Integration – With loose integration, Cyberoam does the Group management and does not synchronize groups with AD when user tries to logon. By default, users will be the member of Cyberoam default group irrespective of Active Directory group, administrator can change the group membership. Cyberoam will use authentication attribute for authenticating users with Active Directory.

Click “Test Connection” to check whether Cyberoam is able to connect to the Active Directory or not. If Cyberoam is able to connect to the Active Directory, click Add to save the configuration.

Step 4: Add Domain Query

If Cyberoam is able to connect to the Active Directory, click Add to enter Domain name

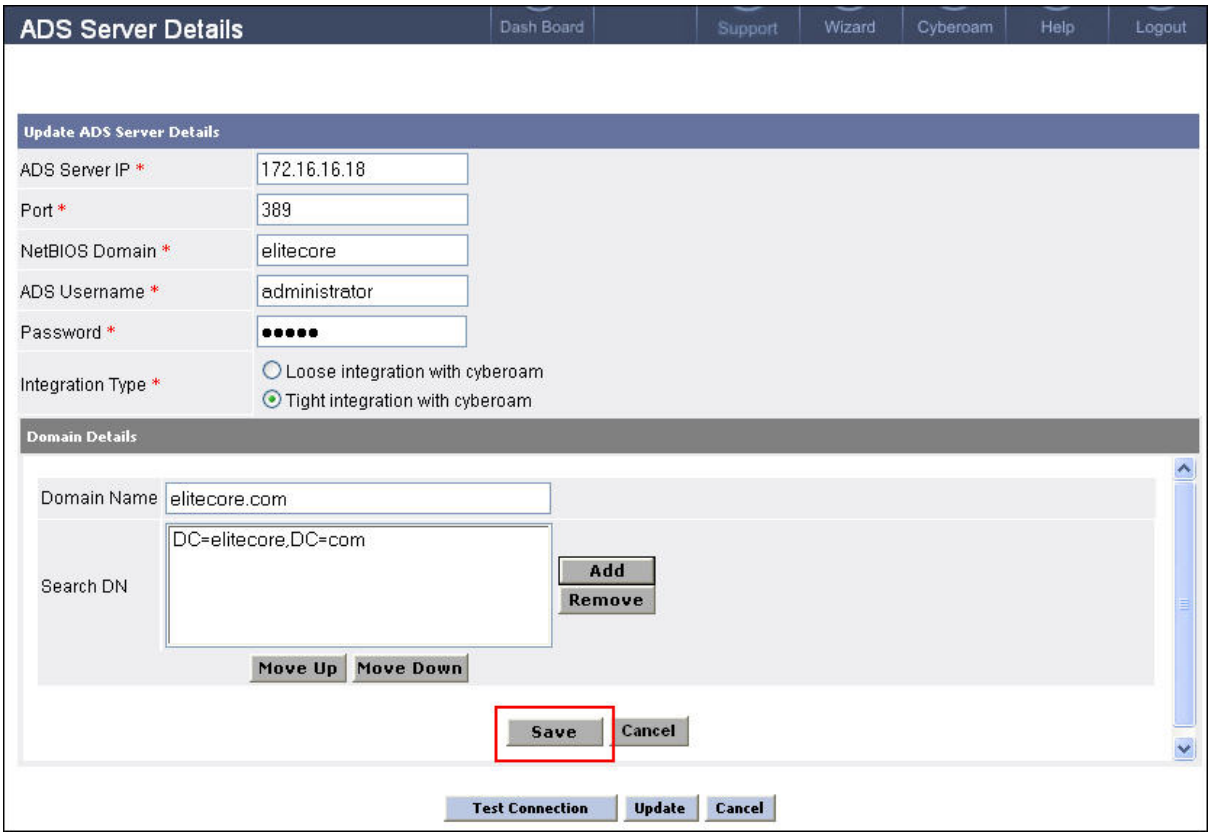




Enter Domain name (FQDN Domain Name)

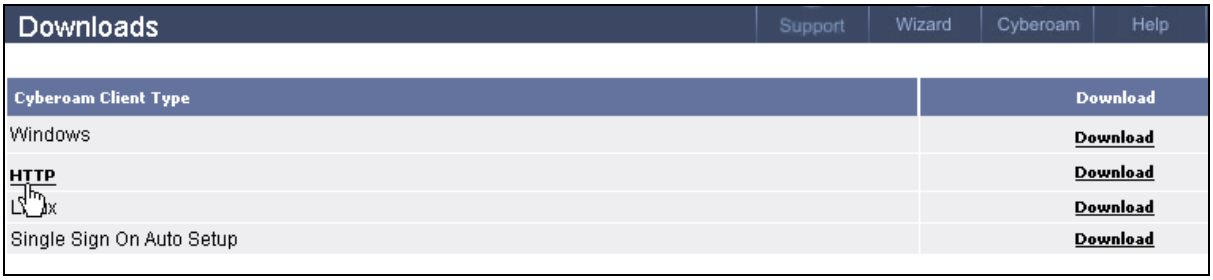
Click Add and enter Search DN. Check the steps provided in section 'Determine NETBIOS Name, FQDN and Search DN' to find the Search DN.

Click OK to save the query.

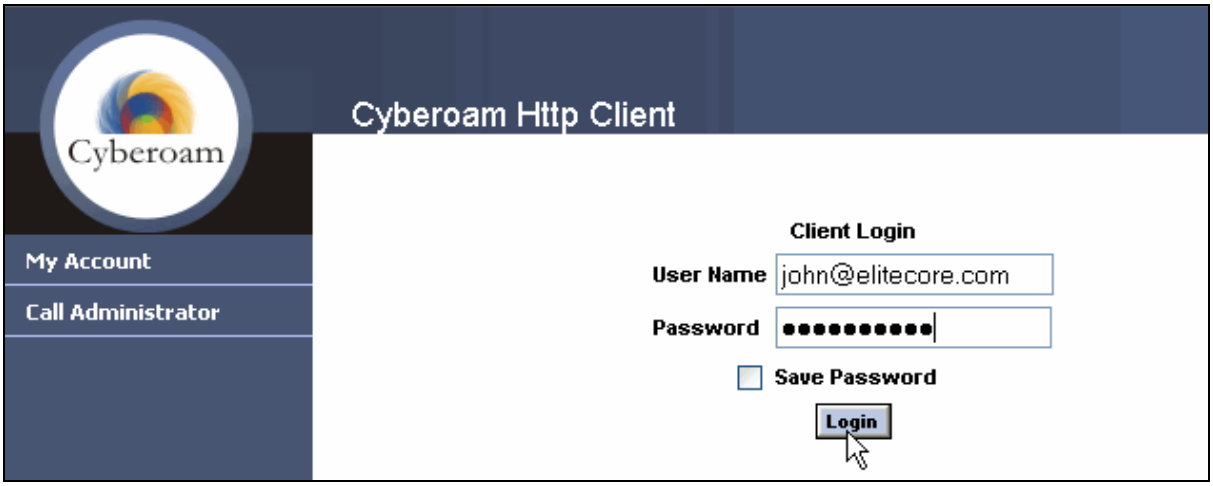


Click Save to save the Domain details

Step 5: Test Active Directory integration
Go to Help>Downloads and click HTTP to open the HTTP client login page.



Specify username and password



Username will be displayed on User>Manage Live Users page if user is able to log on to Cyberoam successfully.

This completes the AD configuration.

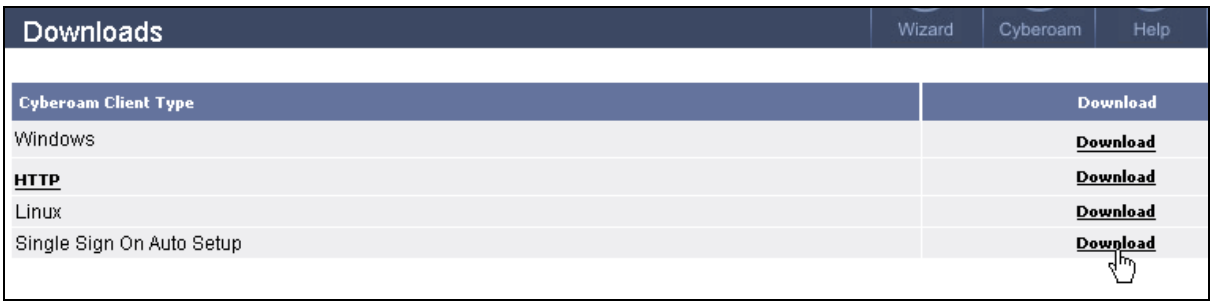
Import AD Groups

If you have deployed v 9.5.3 build 14 or above, import AD groups into Cyberoam using Import Wizard before configuring for single sign on.

Single Sign on Implementation

Step 6: Use the following procedure for implementing Single Sign On (SSO) for ADS if the SSO Client is to be installed on Windows 2000, Windows XP or Windows 2003:

Step 6.1: Download SSCyberoamAutoSetup.zip from Help>Download page from Cyberoam Web Admin Console on Domain Controller or on any of the client machine which is member of Domain and has the Administrator user privileges.



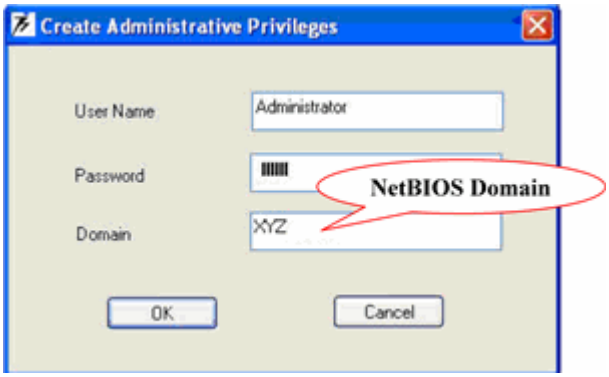
Step 6.2: Create directory SSOsetup and unzip SSCyberoamAutoSetup.zip.

Following files will be extracted:

1. SSCyberoamSetup.exe
2. SSCyberoamConfigSetup.exe
3. SSCyberoamConfig.ini
4. ElitecoreAdmin.exe
5. ElitecoreRun.exe

Step 6.3: Run ElitecoreAdmin.exe to create Admin.ini file to store the user account credentials which has installation right for all the workstations. Installation right is required to run SS Cyberoam setup and install Client on the user machine.

Specify username, password, and windows domain name from where users will log on. This will create Admin.ini file in the SSOsetup directory. If you do not know NetBIOS name, refer to Determine NetBIOS Name, FQDN and Search DN.



Admin.ini file is passed as a parameter to Elitecorerun.exe to run SS Cyberoam setup.

Step 6.4: Setup your configuration in SSCyberoamConfig.ini file using following syntax:

Domain Name=XYZ (FQDN Domain name is the domain from where users will log on)

Server=aaa.bbb.ccc.ddd (IP address of Cyberoam interface which is connected to Active Directory)

Domain Controller=ADS

Step 6.5: Copy following files to “cyberoam” directory under “NETLOGON” of domain controller:

1. SSCyberoamSetup.exe
2. SSCyberoamConfigSetup.exe
3. SSCyberoamConfig.ini
4. Admin.ini
5. ElitecoreRun.exe

Use can access NETLOGON directory using:\\adsservername\netlogon

Step 6.6: Configure logon script

Log on script is executed every time user logs on to the local computer. Each user could have an individual log on script or all users could share the same logon script.

Default location of logon script: NETLOGON directory

Go to step 7.6.1 if logon script is already created

Go to step 7.6.2 if logon script is not created

Step 6.6.1: Update logon script (If logon script is already created)

Download logon script batch file

Edit the existing logon script by using any Text Editor and add lines specified at the end of the

script.

Note:

- Replace adsservername with Active Directory domain controller's computer name.
- Do not keep any space before or after any slash (\)

If all users share the common logon script then, you need to update only the common script else you need to update all the scripts created for each user.

Step 6.6.2: Create logon script (If logon script is not already created)

a) Download logon script batch file and save as “cyberoam.bat” in the NETLOGON

Note:

- Replace adsservername with Active Directory domain controller's computer name.
- Do not keep any space before or after any slash (\)

b) Define logon script - cyberoam.bat (created in step 6.6.2) as a default logon script for all the users using following method:

Log on to Cyberoam Web Admin Console

Go to User -> Migrate Users and click "User Logon Script Updation Utility" from to download updatelogonscript.bat file

Execute this script file from the domain controller itself or any other machine which is part of the domain as follows: updatelogonscript.bat cyberoam.bat

Please note you will require administrative privilege to run the script

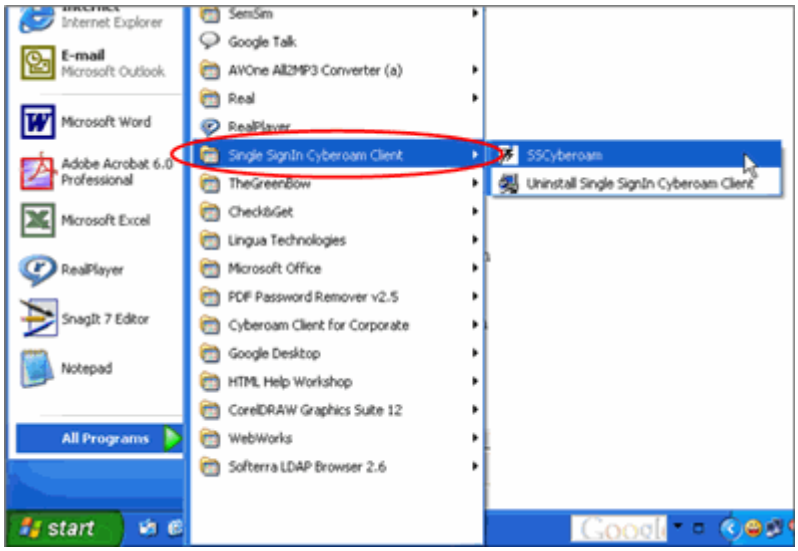
When the user logs on for the first time after the above configuration, logon script runs SSCyberoamSetup.exe and installs Cyberoam Single Sign On Client (Cyberoam SSO Client) on the user machine. Cyberoam will authenticate user based on the details specified in SSCyberoamConfig.ini and Windows username.

Note:

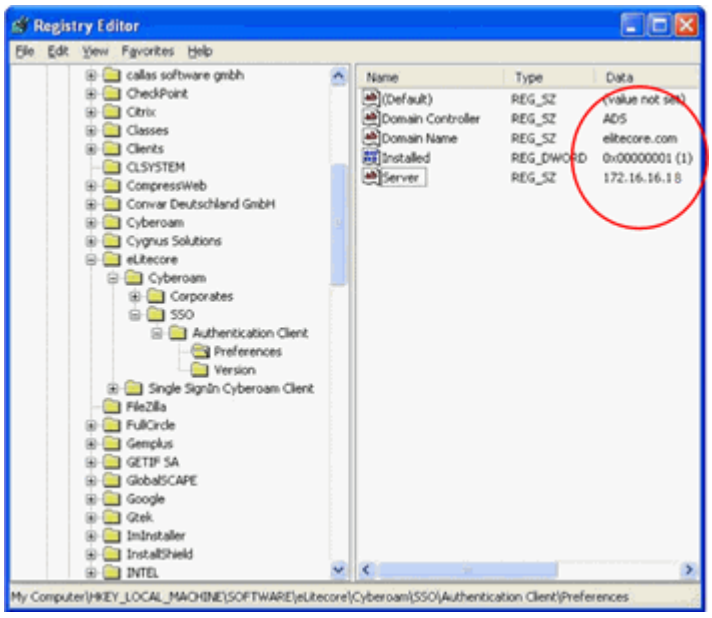
On every log on attempt, SSCyberoamSetup.exe is executed which installs Cyberoam SSO Client if Client is not available on user machine.

Step 6.7: Check whether Cyberoam SSO Client is installed and configured properly from any of the local machine.

a) Check for “Single SignIn Cyberoam Client” folder from Start Programs. If client is installed properly, Single SignIn Cyberoam Client folder will be created.



b) Check SSO version and server IP address from HKEY_LOCAL_MACHINE/SOFTWARE/eLitecore/Cyberoam of the registry of the local machine.

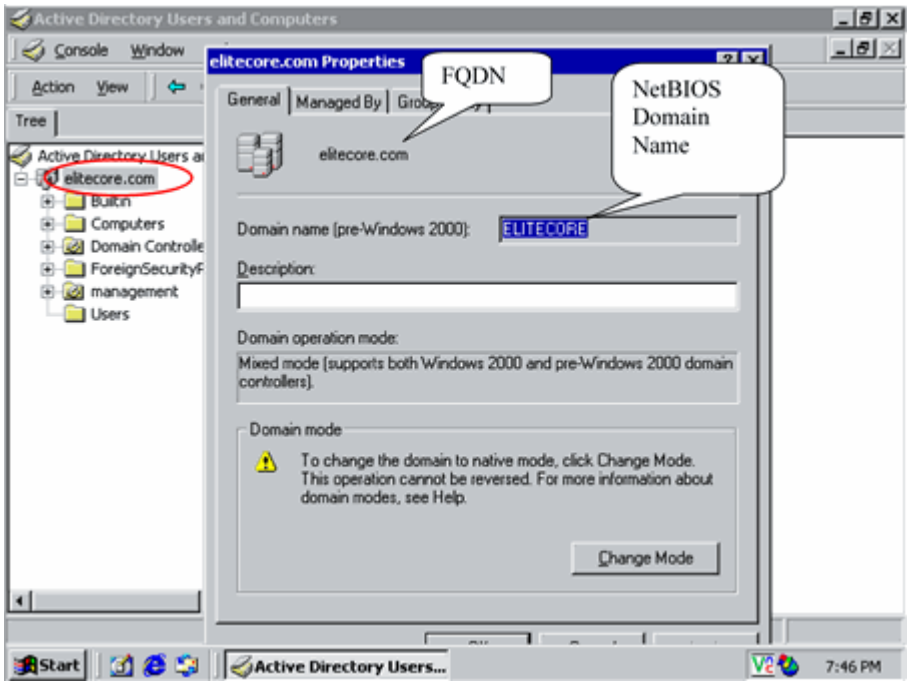


Step 7: This completes the implementation of single sign on authentication with Active Directory integration.

Determine NetBIOS Name, FQDN and Search DN

On the ADS server:

- Go to Start>Programs > Administrative Tools > Active Directory Users and Computers
- Right Click the required domain and go to Properties tab
- Search DN will be based on the FQDN. In the given example FQDN is elitecore.com and Search DN will be DC=elitecore, DC=com



Document Version: 5.0-29/08/2008