



CHAPTER 10

Configuring Active Directory Single Sign-On (AD SSO)

This chapter describes how to configure Active Directory (AD) Single Sign-On (SSO) for the Cisco NAC Appliance.

Topics include:

- [Overview, page 10-1](#)
- [AD SSO Configuration Step Summary, page 10-4](#)
- [Add Active Directory SSO Auth Server, page 10-6](#)
- [Configure Traffic Policies for Unauthenticated Role, page 10-7](#)
- [Configure AD SSO on the CAS, page 10-9](#)
- [Configure the AD Server and Run KTPass Command, page 10-12](#)
- [Enable Agent-Based Windows Single Sign-On with Active Directory \(Kerberos\), page 10-23](#)
- [Confirm AD SSO Service Is Started, page 10-24](#)
- [Enable GPO Updates, page 10-25](#)
- [Enabling a Login Script \(Optional\), page 10-27](#)
- [Add LDAP Lookup Server for Active Directory SSO \(Optional\), page 10-30](#)
- [Troubleshooting, page 10-32](#)

Overview

You can configure Cisco NAC Appliance to automatically authenticate Clean Access Agent users who are already logged into a Windows domain. AD SSO allows users logging into AD on their Windows systems to automatically go through posture assessment/Clean Access certification without ever having to login through the Agent. Cisco NAC Appliance supports Windows Single Sign-On (SSO) on Windows Vista/XP/2000 client machines and AD on Windows 2000/2003 servers, as shown in [Table 10-1 on page 10-2](#).

Table 10-1 Windows Active Directory SSO Support

Active Directory (AD) Servers	Client Machines ¹
<ul style="list-style-type: none"> Windows 2000 Server SP4 Windows 2003 Enterprise SP1 Windows 2003 Enterprise R2 Windows 2003 Standard SP1² 	<ul style="list-style-type: none"> Windows 2000 SP4 Windows XP (Home/ Pro) SP1, SP2 and later Windows Vista

- AD SSO requires the Clean Access Agent to be installed on client systems (for example, you cannot use a Linux kerberos client for AD SSO with CCA.)
- Windows 2003 without SP1 is not supported.

**Note**

You can configure AD SSO for all deployment types (L2/L3, in-band/out-of-band). For OOB, client ports are put on the Auth VLAN first prior to Windows domain authentication.

With AD SSO, Cisco NAC Appliance *authenticates* the user with Kerberos, but *authorizes* the user with LDAP. Cisco NAC Appliance leverages the cached credentials/Kerberos ticket from the client machine login and uses it to validate the user authentication with the backend Windows 2000/2003 server Active Directory. After the user authentication is validated, authorization (role-mapping) is then performed as a separate lookup in Active Directory using LDAP.

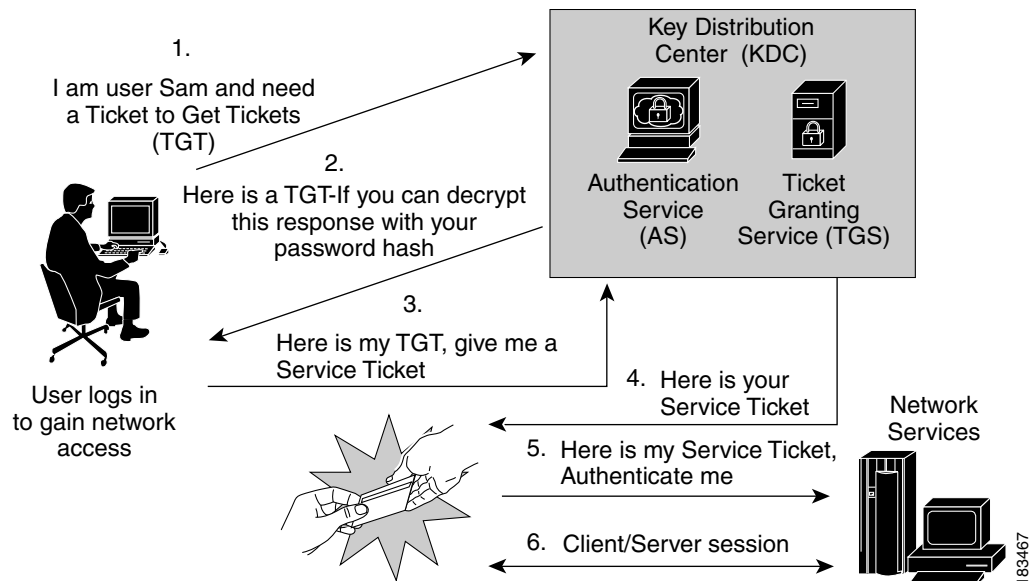
**Note**

The LDAP user account must have privileges sufficient to provide a “Search DN/ Password” that can be used to look up any attribute.

Windows SSO Process (Kerberos Ticket Exchange)

Windows SSO is the ability for CCA to automatically authenticate users already authenticated to a backend Kerberos Domain Controller (Active Directory server). [Figure 10-1 on page 10-3](#) shows the general process for Kerberos ticket exchange.

Figure 10-1 General Process for Kerberos Ticket Exchange



When the Clean Access Server is configured for AD SSO, it essentially replaces the “Network Services” component shown in Figure 10-1. The general sequence is as follows:

- Client and the CAS both have an account on the Active Directory server.
- Client logs onto Windows AD (or uses cached credentials).
- Credentials are sent to the AD. The AD authenticates and gives a Ticket Granting Ticket (TGT) to the client.
 - The Clean Access Agent on the client asks the client for a Service Ticket (ST) with the CAS username to communicate with the CAS.
 - The client requests a Service Ticket from the AD.
 - The AD gives the ST to the client, the client give this ST to the Agent.
 - The Agent is now able to communicate with the CAS.
- The CAS sends back packets and mutually authenticates the client.
- The CAS uses this information to sign the client onto Clean Access and hence SSO authentication takes place.
- For additional user role mapping (for Clean Access certification/posture assessment), an LDAP lookup server with attribute mapping can be configured.

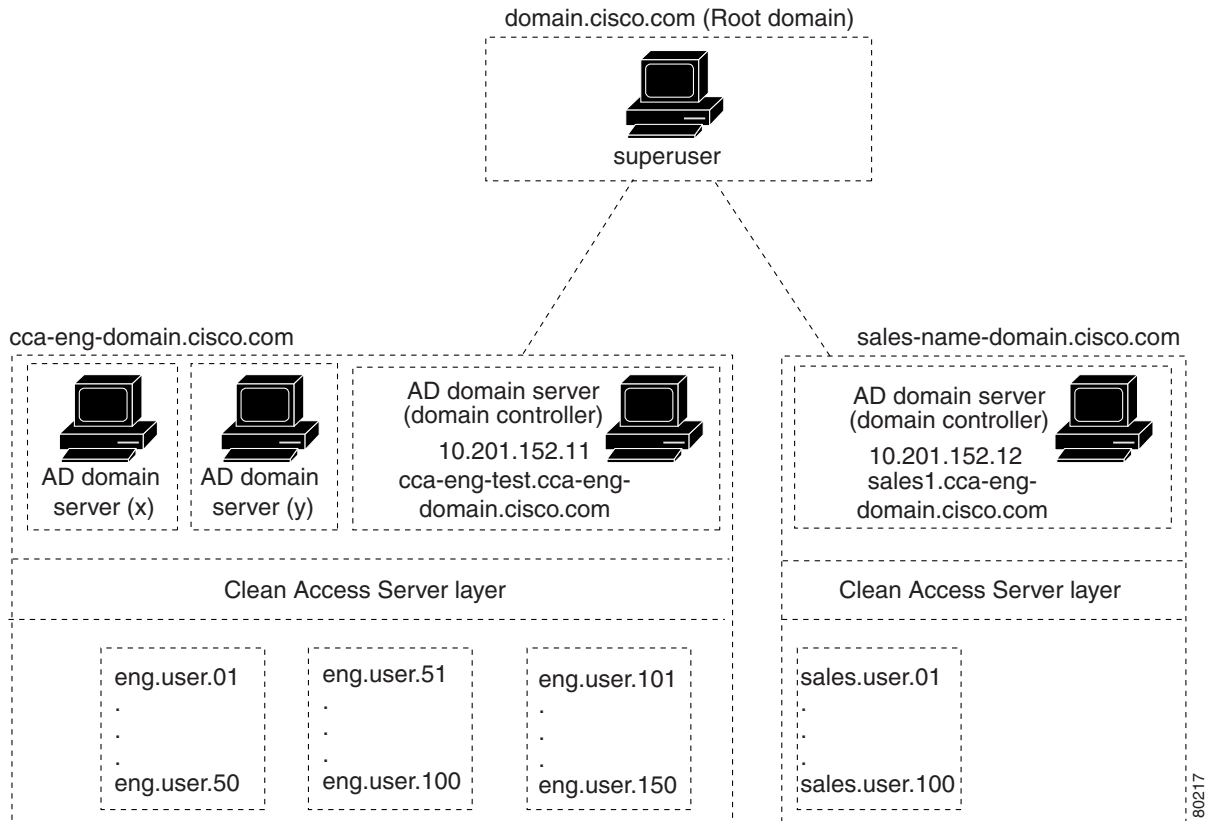
CAS Communication with AD Server

Figure 10-2 illustrates the general setup for Clean Access Server communication with the AD server for Active Directory SSO.

The CAS reads user login traffic only to the AD servers under the root domain. As shown in Figure 10-2, the sales domain (sales-name-domain.cisco.com) and the engineering domain (cca-eng-name.domain.cisco.com) are configured under different Clean Access Servers. Taking the cca-eng domain as an example, the CAS user only needs to be created and configured on the cca-eng-test.cca-eng-domain.cisco.com AD server.

Users under `cca-eng-domain.cisco.com` can log into any AD server in the domain. In addition, the `KTPass` command (described in [Configure the AD Server and Run KTPass Command, page 10-12](#)) only needs to be executed on the `cca-eng-test.cca-eng-domain.cisco.com` server.

Figure 10-2 Configuring the CAS User Account on the AD Server



AD SSO Configuration Step Summary

Administrators should start with a good understanding of their network layout with respect to their AD servers prior to configuring Active Directory SSO.

Configuration Prerequisites

To configure Active Directory SSO, you will need to have the following:

- The number of AD servers (domain controllers) to be configured. Typically, the CAS will correspond to one AD server, but you can also associate the CAS with an entire AD domain.
- The Windows 2000 or Windows 2003 server installation CD for the AD server. This is needed to install support tools for the `KTPass` command. The `KTPass` command is required to be run only on the AD server (domain controller) to which the CAS is logging in.
- The most current version of `ktpass.exe` (release 5.2.3790.0 or later) installed.

- The IP address of each AD server (to configure Unauthenticated role traffic policies). You will need to allow traffic on the CAS for every AD server that is in charge of that domain. For example, if users can log into multiple AD servers in the domain, you should allow traffic to all the multiple AD servers for the Unauthenticated role.
- If setting up a connection between the CAS and a single AD server, the FQDN of the Active Directory server that the CAS logs into (for CAS configuration).
- DNS server settings correctly configured on the CAS (**under Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS**) to resolve the FQDN for the AD server on the CAS.
- The date and time of the CAM, CAS, and AD server synchronized within 5 minutes of each other. The time on the AD server and the CAS must be synchronized to not more than 300 seconds clock skew (Kerberos is sensitive to time).
- The Active Directory Domain Name in Kerberos format (Windows 2000 and above). This is needed for both CAS configuration and CLI configuration of the AD server.



Note The host principal name in the KTPass command (i.e. “<AD_DomainServer>”) must exactly match the case of the “Full computer name” of the AD server (under **Control Panel > System > Computer Name | Full computer name.**) See [Run ktpass.exe Command, page 10-19](#) for details.

- Client systems must already have the Clean Access Agent installed. Refer to the “Distributing Clean Access Agent” chapter of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)* for additional information on Agent distribution and installation.

Configuration Step Summary

-
- Step 1** [Add Active Directory SSO Auth Server, page 10-6.](#)
On the CAM, add a new auth server of type Active Directory SSO and specify a default role for users.
- Step 2** [Configure Traffic Policies for Unauthenticated Role, page 10-7.](#)
Open ports on the CAS to allow client authentication traffic to pass through the CAS to/from the Active Directory server.
- Step 3** [Configure AD SSO on the CAS, page 10-9.](#)
From the CAS management pages, configure the Active Directory server settings, CAS user account settings, and auth server settings for the CAS corresponding to the domain of the users.
- Step 4** [Configure the AD Server and Run KTPass Command, page 10-12.](#)
Add a CAS account on the Windows 2000/2003 AD server with which the CAS will communicate, and configure encryption parameters to support the Linux operating system of the CAS.
- Step 5** [Enable Agent-Based Windows Single Sign-On with Active Directory \(Kerberos\), page 10-23.](#)
- Step 6** [Confirm AD SSO Service Is Started, page 10-24.](#)
- Step 7** [Enable GPO Updates, page 10-25.](#)
- Step 8** [Enabling a Login Script \(Optional\), page 10-27.](#)
- Step 9** [Add LDAP Lookup Server for Active Directory SSO \(Optional\), page 10-30.](#)
Optionally configure LDAP lookup servers to map users to multiple roles after authentication.

Step 10 Refer to [Troubleshooting, page 10-32](#) if necessary.

Add Active Directory SSO Auth Server

To create an AD SSO auth server on the CAM, and map the AD server to a default role for users and a secondary LDAP lookup server (if configured), follow these steps:

Step 1 Go to **User Management > Auth Servers > New**.

Step 2 From the **Authentication Type** dropdown menu, choose **Active Directory SSO**.

Figure 10-3 Active Directory SSO

The screenshot shows the 'User Management > Auth Servers' configuration page. The 'Auth Servers' tab is active, with 'List' and 'New' sub-tabs. The form contains the following fields:

- Authentication Type:** Active Directory SSO (dropdown)
- Provider Name:** (text input)
- Default Role:** Unauthenticated Role (dropdown)
- LDAP Lookup Server:** NONE (dropdown)
- Description:** (text input)

Buttons for 'Add Server' and 'Cancel' are located at the bottom of the form.

Step 3 Choose a **Default Role** from the dropdown menu. If no additional lookup is required to map users to roles, all users performing authentication via Active Directory single sign-on will be assigned to the default role. Posture assessment/Clean Access certification should be configured for this role.

Step 4 Type a **Provider Name** that will identify the AD SSO auth server on the list of authentication providers. Do not use spaces or special characters in the name.

Step 5 You can leave the **LDAP Lookup Server** dropdown menu at the default NONE setting if you plan to assign your users to one default role, and no additional lookup is required. If you plan on mapping Windows domain SSO users to multiple roles, the CAM will need to perform a second-level lookup using the LDAP Lookup server you configure as described in [Add LDAP Lookup Server for Active Directory SSO \(Optional\), page 10-30](#). In this case, select the LDAP Lookup server you have already configured from the **LDAP Lookup Server** dropdown.

Step 6 Click **Add Server**.



Note

For AD SSO users, the **Online Users** and **Certified Devices** pages will display **ad_sso** in the **Provider** field and both the username and domain of the user (for example, **user1@domain.name.com.**) in the **User/User Name** field.

**Note**

The **Auth Test** feature cannot be used to test SSO Auth providers (e.g. AD SSO or VPN SSO).

Configure Traffic Policies for Unauthenticated Role

A user in the domain logging into his/her Windows machine sends credentials to the root domain controller to perform the first portion of Kerberos ticket exchange (as shown in [Figure 10-1](#)). Once the machine receives a Service Ticket, the Agent uses it to validate the client authentication through the CAS. Only when the CAS validates the authentication is the user allowed network access, and there is no need for a separate user login through the Clean Access Agent.

As [Figure 10-2](#) illustrates, the CAS is configured to read the login credentials of user machines as they authenticate to the Active Directory (AD) server. Ports must be opened on the CAS to allow the authentication traffic to pass through the CAS to/from the AD server. The administrator can open either TCP or UDP ports, depending on what the AD server uses.

**Note**

If AD SSO traffic may include fragmented packets, you might need to enable the **IP FRAGMENT** option according to the guidelines in the [Add IP-Based Policy](#) section of the *Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide*.

Configure traffic policies for the Unauthenticated role to allow these ports on the trusted-side IP address of the AD server. This allows the client to authenticate to the AD server and for GPO and scripts to run. Cisco recommends that you install Cisco Security Agent (CSA) on the AD server/DMZ AD server.

Required TCP Ports

If the Active Directory server is using Kerberos, the following TCP ports must be opened on the CAS for the Unauthenticated role:

- TCP 88 (Kerberos)
- TCP 135 (RPC)
- TCP 389 (LDAP) or TCP 636 (LDAP with SSL)
- TCP 445 (Microsoft-SMB; needed for change notices from DC to PC)
- TCP 1025 (RPC)–non-standard
- TCP 1026 (RPC)–non-standard

Alternative UDP Ports

If it is not known whether the Active Directory server is using Kerberos, you must open the following UDP ports:

- UDP 88 (Kerberos)
- UDP 389 (LDAP) or UDP 636 (LDAP with SSL)

**Note**

Typically, the LDAP protocol uses plain text when sending traffic on TCP/UDP port 389. If encryption is required for LDAP communications, use TCP / UDP port 636 (LDAP with SSL encryption) instead.

To Add Policies for AD Server, follow these steps:

- Step 1** Go to **User Management > User Roles > List of Roles > Policies [Unauthenticated Role]**. This brings up the **IP** traffic policy form for the Unauthenticated Role.
- Step 2** With the direction dropdown set for Untrusted ->Trusted, click the **Add Policy** link. The Add Policy form appears (Figure 10-4).

Figure 10-4 Configure Traffic Policy for CAS to AD Server

Pri.	Action	Protocol	Untrusted	Trusted	Description
1	Allow	TCP	*:*	10.201.152.12 / 255.255.255.255 : 88,135,389,1025,1026	88-kerberos,135-rpc,389-ldap,1025-rpc,1026-rpc

- Step 3** Leave the following fields at their defaults:

- **Action:** Allow
- **State:** Enabled
- **Category:** IP
- **Protocol:** TCP 6
- **Untrusted (IP/Mask:Port):** * / * / *

- Step 4** For **Trusted (IP/Mask:Port)**, enter:

- The IP address of the Active Directory server
- 255.255.255.255 as the subnet mask (for just the AD server)
- Ports (using commas to separate port numbers)

For example: 10.201.152.12 / 255.255.255.255 / 88,135,389,1025,1026

Step 5 Type an optional **Description**.

Step 6 Click **Add Policy**.



Note

When testing, Cisco recommends opening complete access to the AD server/DC first, then restricting ports as outlined above once AD SSO is working. When logging into the client PC, make sure to log into the domain using Windows domain credentials (not Local Account).

Configure AD SSO on the CAS

To configure the CAS corresponding to the domain of the users, follow these steps:

Step 1 Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

Figure 10-5 Active Directory SSO

Device Management > Clean Access Servers > 10.201.241.32

Status Network Filter Advanced Authentication Misc

Login Page · VPN Auth · Windows Auth · OS Detection

Active Directory SSO | NetBIOS SSO

Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on Single Active Directory Server Domain (All Active Directory Servers)

Active Directory Server (FQDN)

Active Directory Domain

Account Name for CAS

Account Password for CAS

Active Directory SSO Auth Server
(add one in [User Management > Auth Servers])

183662

Step 2 Do *not* click the checkbox for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)** yet. The service should only be enabled after you [Configure the AD Server and Run KTPass Command, page 10-12](#). You can configure the other fields of this page and click **Update**, as described below.



Note

Until you perform the configuration on the AD server, the following message will appear:
Error: Could not start the SSO service. Please check the configuration.

Step 3 For **Account for CAS on**, specify whether the CAS account resides on a **Single Active Directory Server** or multiple servers within a **Domain (All Active Directory Servers)**.



Note Make sure the CAS can resolve the name you type in the **Active Directory Server (FQDN)** field via DNS. A DNS server must be correctly configured on the CAS (under **Device Management > CCA Servers > Manage [CAS_IP] > Network > DNS**) so that the CAS can resolve the FQDN for the AD server.

- a. If you specify that the CAS account resides on a **Single Active Directory Server**, enter the fully qualified domain name of the AD server in the **Active Directory Server (FQDN)** field (for **example**, `cca-eng-test.cca-eng-domain.cisco.com`). This field cannot be an IP address, and must exactly match CASE-BY-CASE the name of the AD server it appears under **Control Panel > System > Computer Name | Full computer name** on the AD server (see [Figure 10-7](#)).

Figure 10-6 AD SSO—Single Active Directory Server

Device Management > Clean Access Servers > 10.201.241.32

Status Network Filter Advanced Authentication Misc

Login Page · VPN Auth · Windows Auth · OS Detection

Active Directory SSO | NetBIOS SSO

Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on Single Active Directory Server Domain (All Active Directory Servers)

Active Directory Server (FQDN)

Active Directory Domain

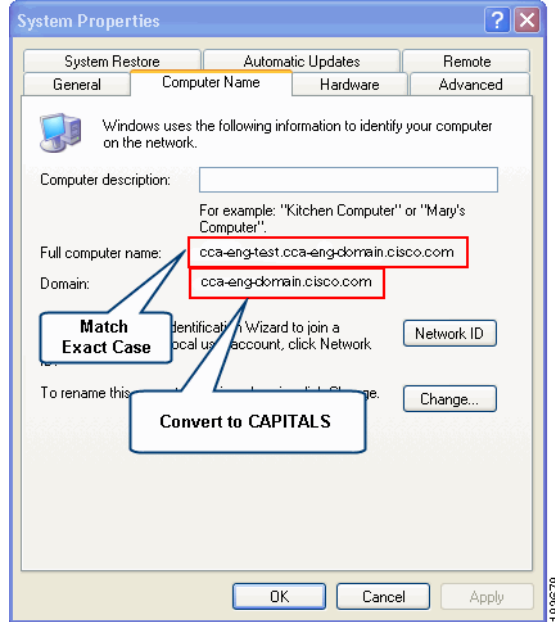
Account Name for CAS

Account Password for CAS

Active Directory SSO Auth Server (add one in [User Management > Auth Servers])

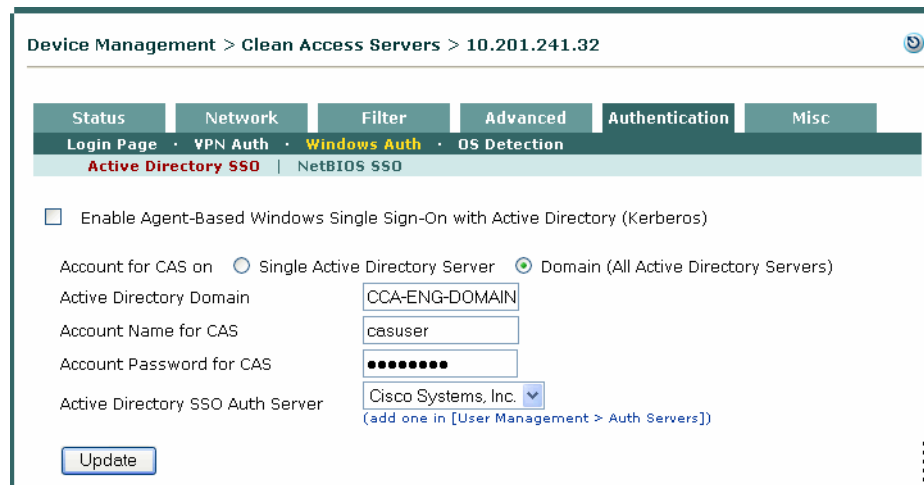
183681

Figure 10-7 Control Panel > System > Computer Name | Full computer name



- b. If you select the **Domain (All Active Directory Servers)** option, the **Active Directory Server (FQDN)** field disappears (Figure 10-8). DNS automatically resolves the Active Directory domain specified to the primary domain controller (DC) and, if the primary DC becomes inaccessible, the secondary DC. In this case, you specify only the domain and not the full FQDN of the AD server. Note also that the KTPass command syntax also changes based on whether you specify the **Single Active Directory Server** or **Domain (All Active Directory Servers)** option. For details, see [Run ktpass.exe Command, page 10-19](#).

Figure 10-8 AD SSO—Domain (All Active Directory Servers)



- Step 4** For **Active Directory Domain**, type the name of the domain for the KDC/Active Directory server in **UPPER CASE** (see Figure 10-7). The “Active Directory Domain” is equivalent to “Kerberos Realm”. For example:

CCA-ENG-DOMAIN.CISCO.COM

Step 5 For **Account Name for CAS**, type the name of the Clean Access Server user you have created on the AD server, for example: `casuser`.
The CAS user account allows the CAS to log into the AD server.

Step 6 For **Account Password for CAS**, type the password for the CAS user on the AD server.

**Note**

The password is case sensitive. From the CAS side, there is no limitation on the number of characters, and standard characters are allowed. Since this password is based of the mapping created using the KTPass command, observe any limitations from the Windows server side (e.g. password policies).

Step 7 From the **Active Directory SSO Auth Server** dropdown, choose the Active Directory SSO Server you configured on the CAM. This field maps the auth provider created on the CAM to the CAS (along with the Default Role, and secondary LDAP Lookup server, if configured).

Step 8 Click **Update**.

**Note**

If the Active Directory server is not reachable from the CAS at the time of CAS startup, AD SSO service is not started. If this occurs, the administrator must go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO** and click the **Update** button to restart the AD SSO service.

Configure the AD Server and Run KTPass Command

Both the GUI and CLI interfaces are used to configure the Active Directory server:

- [Create the CAS User, page 10-12](#)
- [Install Support Tools, page 10-16](#)
- [Run ktpass.exe Command, page 10-19](#)

Create the CAS User

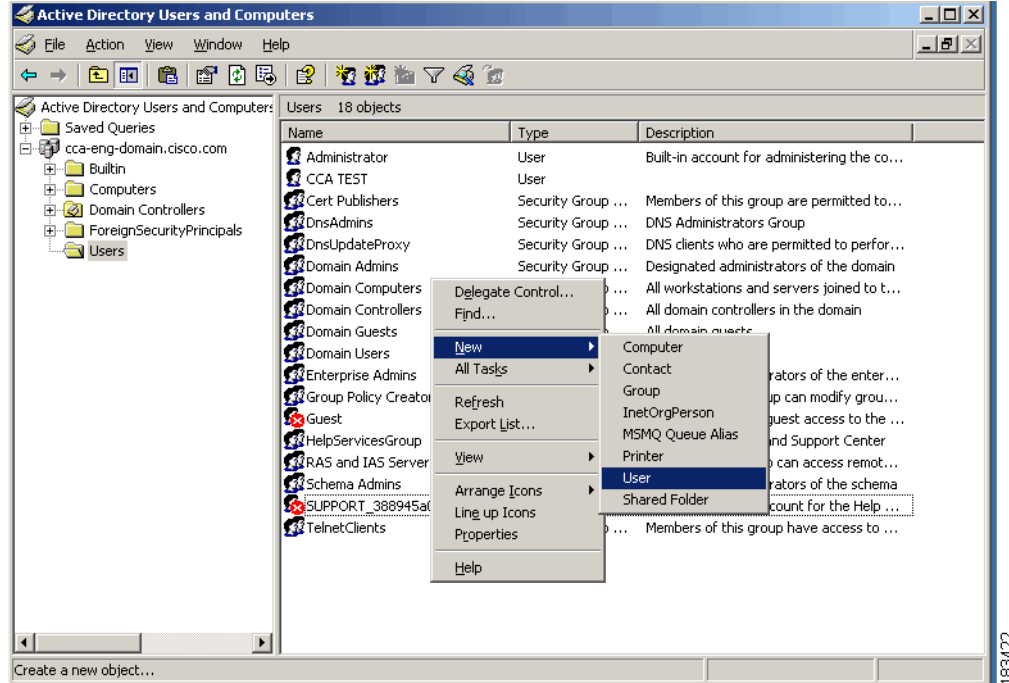
To create a CAS user, follow these steps:

Step 1 Login as the administrator on the Active Directory server machine.

Step 2 Open the Active Directory Management console from **All Programs > Admin Tools > Active Directory Users and Computers**.

Step 3 From the left-hand pane of the **Active Directory Users and Computers** window, navigate to the domain for which you want to configure the CAS, for example, `cca-eng-domain.cisco.com`.

Figure 10-9 Create New User on AD Server

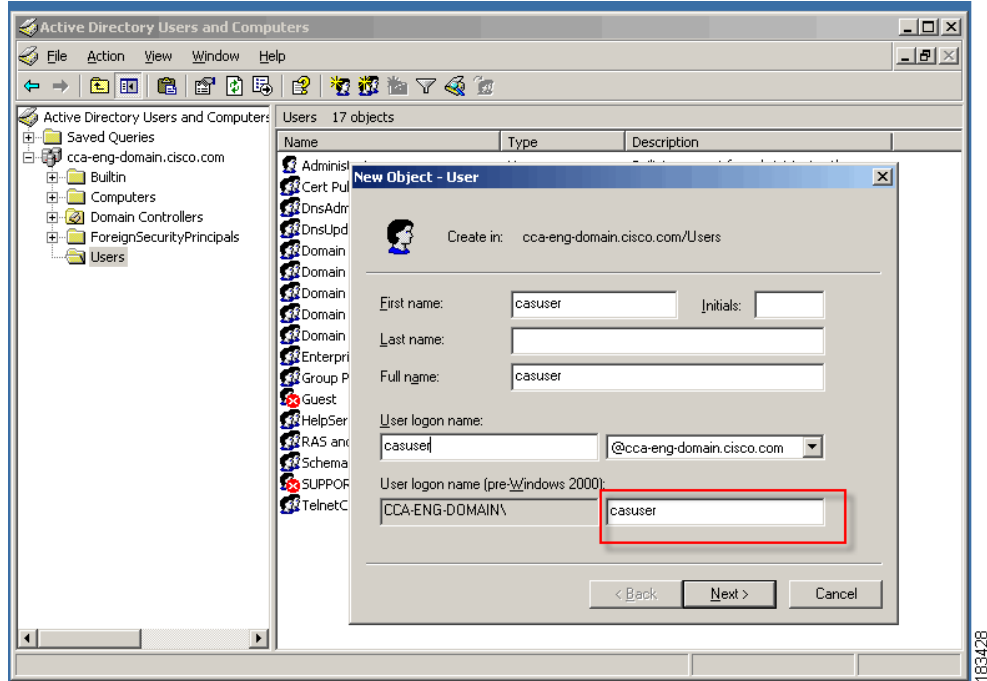


Step 4 Right-click the **Users** folder. In the menu that appears, select **New > User** (Figure 10-9).

Step 5 In the first **New Object - User** dialog (Figure 10-10), configure the fields for the Clean Access Server user as follows:

Enter the name you want the CAS to use in the **First name** field, for example: **casuser**. This automatically populates the **Full name** and **User logon name** fields. The **User logon name** must be one word. Make sure First name= Full name = User name for the user account.

Figure 10-10 Configure the CAS User

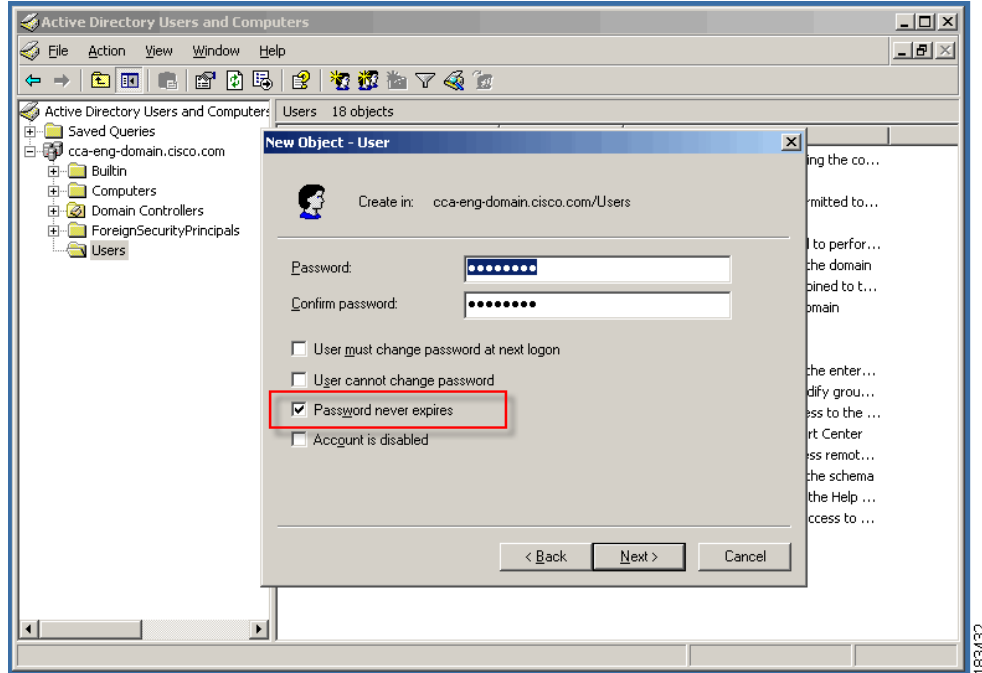


Step 6 Click **Next** to bring up the second **New Object - User** dialog.

Step 7 In the second **New Object - User** dialog (Figure 10-11), configure the following:

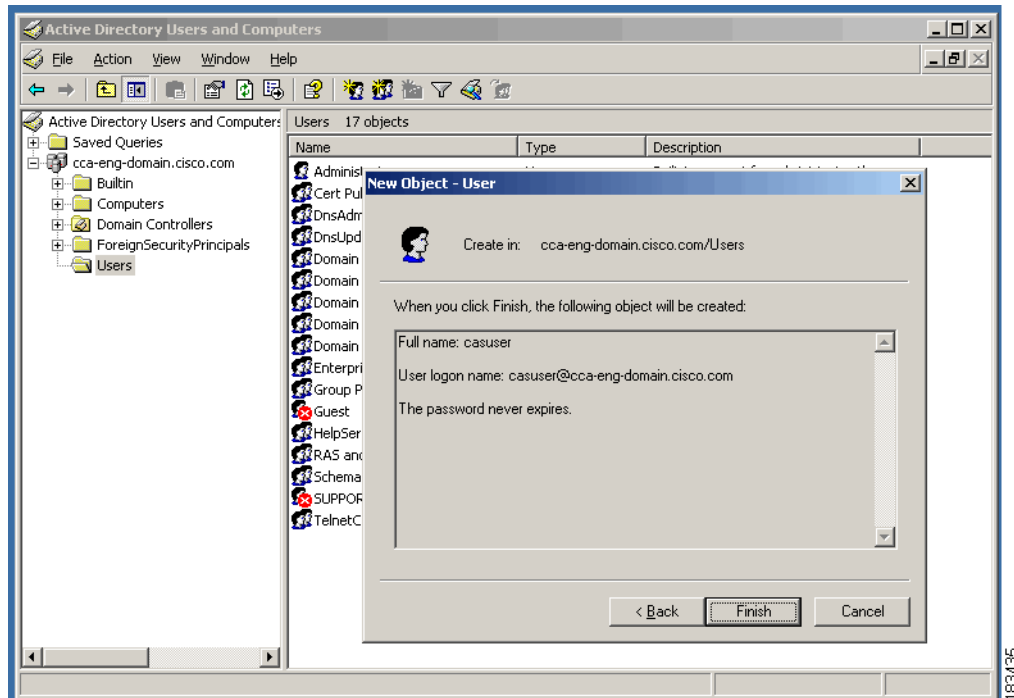
- Type and retype the password for the CAS user in the **Password** and **Confirm Password** fields.
- Make sure the **Password never expires** option is **CHECKED**.
- Make sure the **User must check password at next login** option is **UNCHECKED**.

Figure 10-11 Configure Password for CAS User



Step 8 Click **Next** to bring up the confirmation **New Object - User** dialog (Figure 10-12).

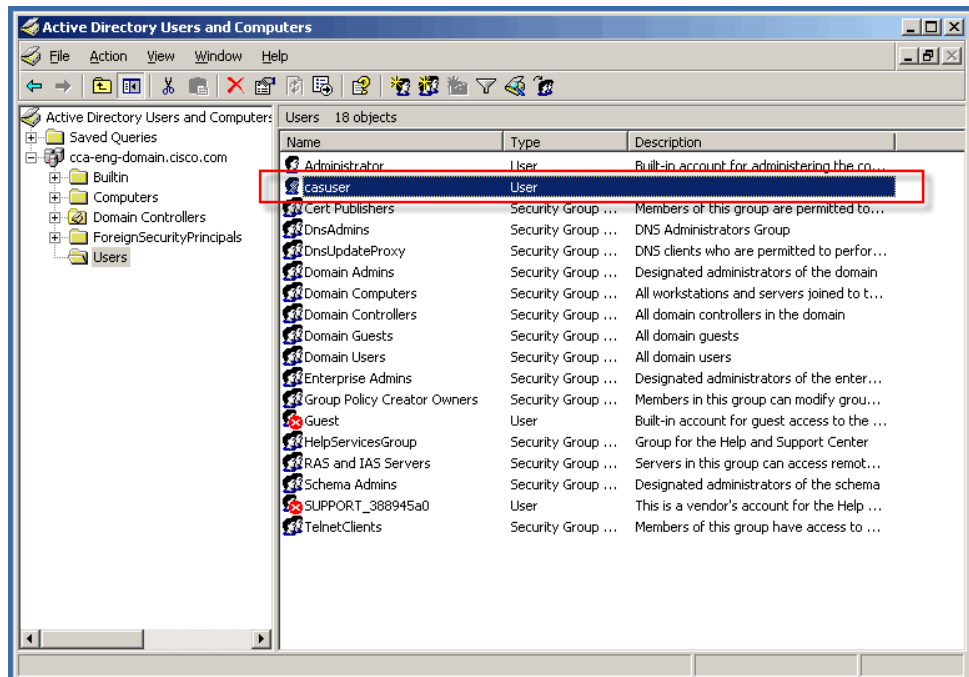
Figure 10-12 Confirm CAS User Properties



Step 9 Confirm the properties for the CAS user and click **Finish** to conclude, or click **Back** if you need to make corrections.

Step 10 The CAS user is successfully added to the AD domain (Figure 10-13).

Figure 10-13 CAS User is Added



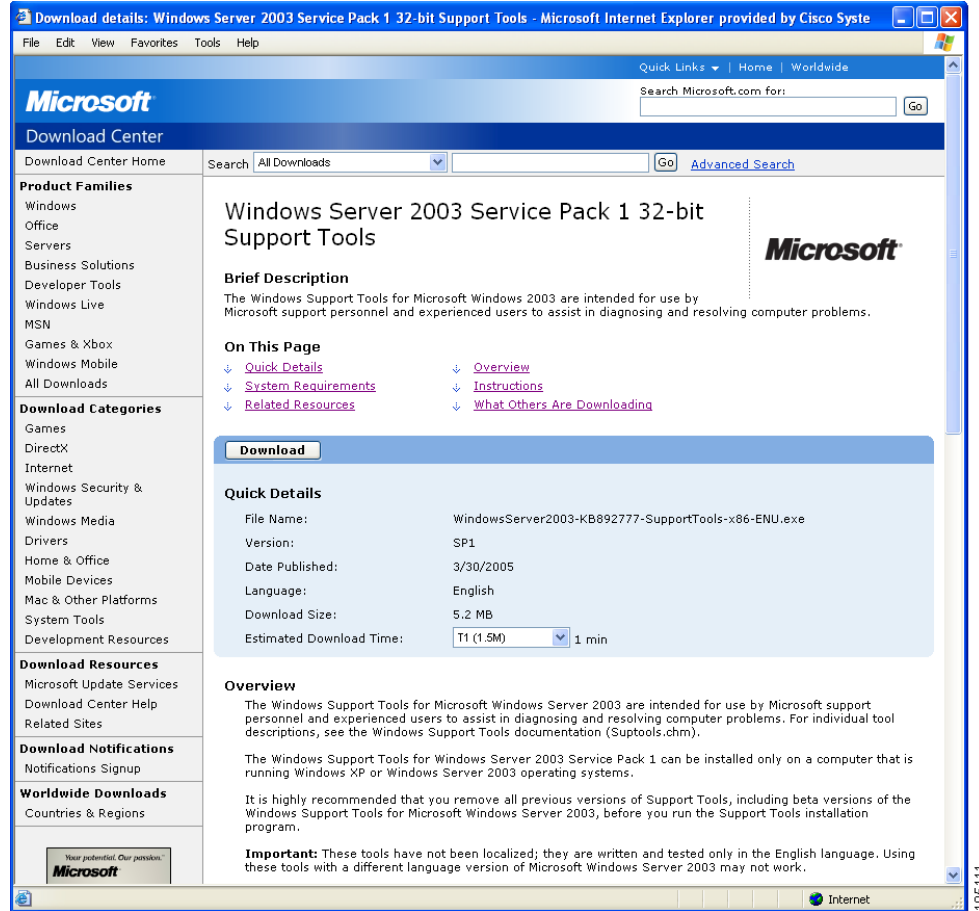
Install Support Tools

The **ktpass.exe** tool is available as part of the Windows 2000/2003 Server support tools on the Microsoft support site: <http://support.microsoft.com/>. The KTPass executable is not installed by default. Therefore, you must retrieve the executable from the Microsoft Support site prior to installation.

To install the **ktpass.exe** tool, follow these steps:

-
- Step 1** Open a web browser and navigate to <http://support.microsoft.com/>.
 - Step 2** Locate the Windows Server 2000/2003 Support Tools section(s) of the Microsoft web site.

Figure 10-14 Support Tools for Windows 2003 Server



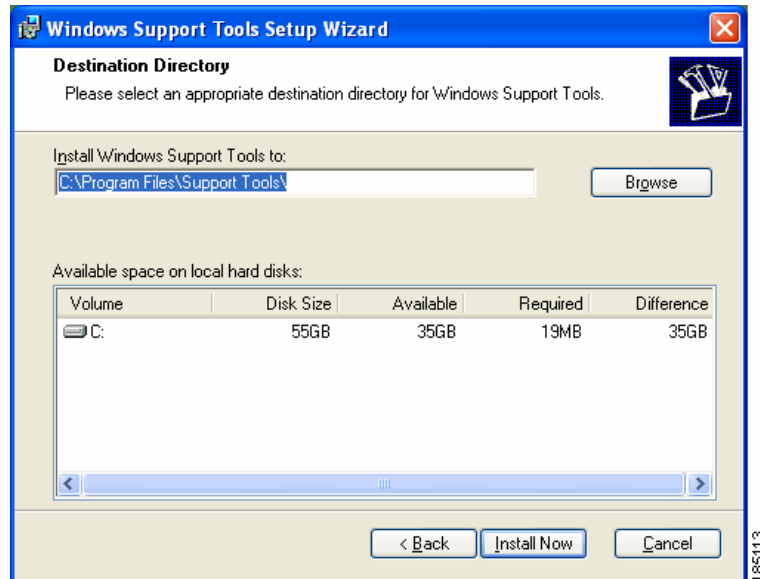
Step 3 Click the **Download** button.

Step 4 Do one of the following:

- Click **Save** to save a copy of the Windows Server 2000/2003 Support Tools Self-Extractor executable on your local machine.
- Click **Run** to begin installing the Windows Server 2000/2003 Support Tools on your local machine.

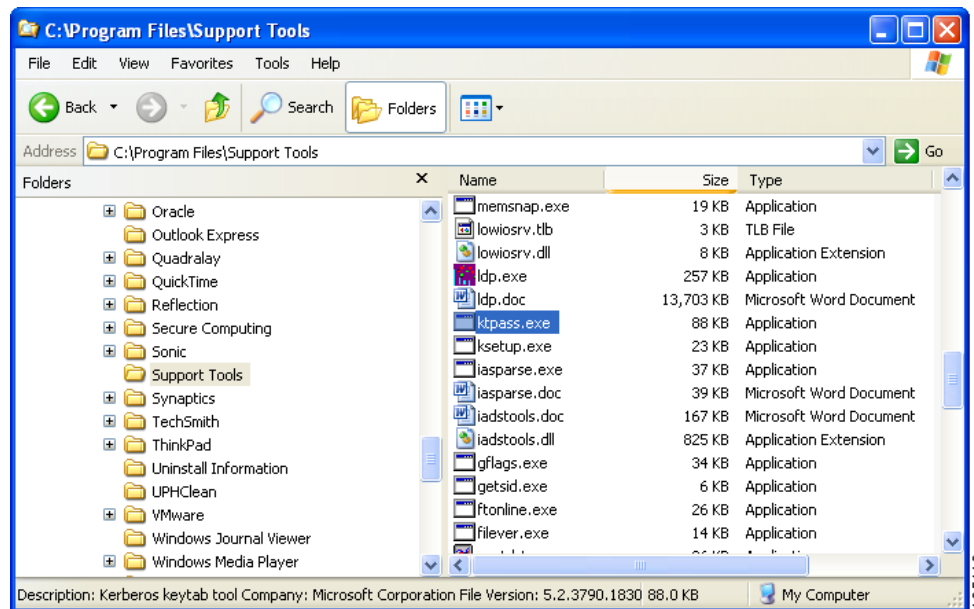
When you launch the Self-Extractor or click **Run**, Windows automatically launches the **Windows Support Tools Setup Wizard**.

Figure 10-15 Installing Windows Server 2003 Support Tools



- Step 5** Once the installation is complete, open Windows Explorer and navigate to the C:\Program Files\Support Tools directory (or another directory you may have specified in the Setup Wizard session), and verify that the **ktpass.exe** component appears in the file list. (See [Figure 10-16](#).)

Figure 10-16 Support Tools—ktpass.exe



- Step 6** Execute the **ktpass.** command according to the directions in the next section, [Run ktpass.exe Command](#).

**Note**

Do not double-click the **ktpass.exe** command in Windows Explorer; it must be run from a command prompt.

Run ktpass.exe Command

**Note**

To ensure successful KTPass operation, obtain and install the most current version of **ktpass.exe**.

Cisco recommends using release 5.2.3790.0 or later of the KTPass executable.

When a CAS is configured to interact with a single AD server, you must run the KTPass command on the AD server configured in the CAS.

If you are associating the CAS with an entire AD domain, you must run the KTPass command on any single AD server (not all AD servers) in the AD domain. The information in the KTPass command operation is then automatically propagated to the other members of the AD domain.

Linux supports DES (a widely used encryption type) but does not support the default encryption of Active Directory (e.g. RC4) which is specific to Microsoft. Because the Clean Access Server is a Linux machine, you must run the **ktpass.exe** command to ensure that the CAS user uses DES instead of the default encryption for compatibility when logging into AD.

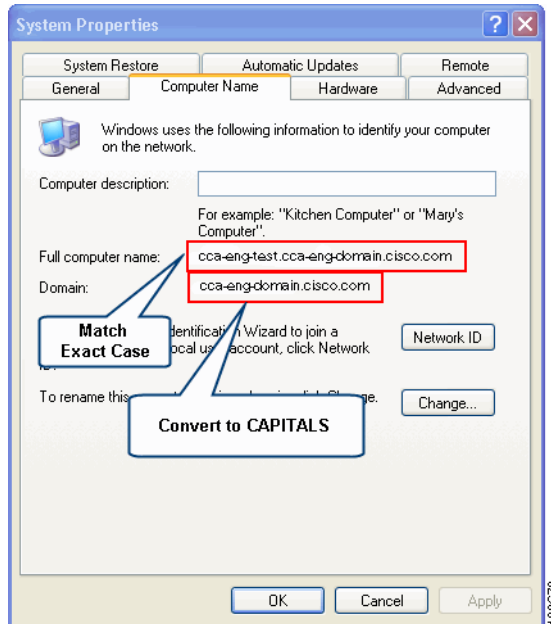
See [Table 10-1 on page 10-2, “Windows Active Directory SSO Support”](#) for a list of the Windows server versions supported.

**Note**

When running **ktpass.exe**, it is very important to observe the following case sensitivity (see [Figure 10-17](#)).

- The computer name that is entered between “/” and “@” in the command (e.g. “AD_DomainServer”) must exactly match CASE-BY-CASE the name of the AD server as it appears under **Control Panel > System > Computer Name | Full computer name** on the AD server.
- The realm name that is entered after “@” (e.g. “AD_DOMAIN”) must always be in **UPPER CASE**. You must convert the Domain name that appears under **Control Panel > System > Computer Name | Domain** on the AD server to UPPER CASE when entering it in the KTPass command.

Figure 10-17 Control Panel > System > Computer Name | Full computer name



- No warnings should appear after you execute **ktpass.exe**.
- Execution of the command must display the following output:
Account <CAS user> has been set for DES-only encryption

To run **ktpass.exe**, follow these steps:

- Step 1** Open a command prompt and cd to C:\Program Files\Support Tools\. The **ktpass.exe** command should be in the folder.
- Step 2** Enter one of the following commands:

If your Active Directory domain consists of only one server

- `ktpass.exe -princ <CAS_username>/<AD_DomainServer>@<AD_DOMAIN> -mapuser <CAS_username> -pass <CAS_password> -out c:\<CAS_username>.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly`

Use this command syntax when you specify the **Account for CAS on Single Active Directory Server** option in [Configure AD SSO on the CAS](#), page 10-9.

For example (see also [Figure 10-18](#)):

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser
casuser -pass Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
```

If your Active Directory domain consists of multiple servers

- `ktpass.exe -princ <CAS_username>/<AD_Domain>@<AD_DOMAIN> -mapuser <CAS_username> -pass <CAS_password> -out c:\<CAS_username>.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly`

Use this command syntax when you specify the **Account for CAS on Domain (All Active Directory Servers)** option in [Configure AD SSO on the CAS, page 10-9](#).

For example (see also [Figure 10-18](#)):

```
C:\Program Files\Support Tools> ktpass.exe -princ
casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass
Cisco123 -out c:\casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
```

The output of the command should be as follows (see also [Figure 10-19](#)):

```
Targeting domain controller: cca-eng-test.cca-eng-domain.cisco.com
Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser.
Key created.
Output keytab to c:\casuser.keytab:
Keytab version: 0x502
keysize 97 casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0xbc5120bcfed01f8)
Account casuser has been set for DES-only encryption.
```



Note The “**Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser**” response confirms that the **casuser** account is mapped correctly.

In the example above, the service principal name (SPN), `ktpass.exe -princ casuser/cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.COM`, is the key to ensuring that any AD server within a managed domain can appropriately resolve user credentials passed from the CAS.

Step 3 Save the exact command you ran and the output to a text file (you do not need to save the CAS user password). For troubleshooting purposes, this will facilitate TAC support.

Figure 10-18 Execute `ktpass.exe` Command

```

CA Command Prompt
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files\Support Tools"

C:\Program Files\Support Tools>
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>ktpass.exe -princ casuser/cca-eng-test.cca-eng-do
main.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass Cisco123 -out c:\
casuser.keytab -ptype KRB5_NT_PRINCIPAL +Desonly_

```

183449

Figure 10-19 ktpass.exe Command Output

```

C:\Documents and Settings\Administrator>cd "%Program Files\Support Tools"
C:\Program Files\Support Tools>
C:\Program Files\Support Tools>ktpass.exe -princ casuser/cca-eng-test.cca-eng-do
main.cisco.com@CCA-ENG-DOMAIN.CISCO.COM -mapuser casuser -pass Cisco123 -out c:\
casuser.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
Targeting domain controller: cca-eng-test.cca-eng-domain.cisco.com
Successfully mapped casuser/cca-eng-test.cca-eng-domain.cisco.com to casuser.
Key created.
Output keytab to c:\casuser.keytab:
Keytab version: 0x502
keysize 97 casuser/cca-eng-test.cca-eng-domain.cisco.com@CCA-ENG-DOMAIN.CISCO.CO
M ptype 1 (KRB5_NT_PRINCIPAL) vno 3 etype 0x3 (DES-CBC-MD5) keylength 8 (0xbc512
0bcfeda01f8)
Account casuser has been set for DES-only encryption.
C:\Program Files\Support Tools>_

```

Table 10-2 provides further parameter details.

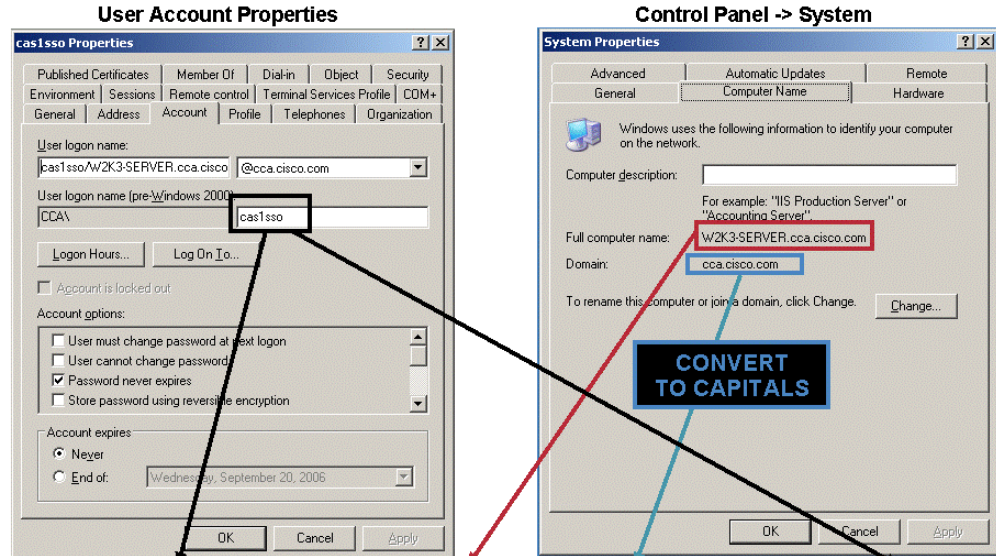
Table 10-2 ktpass.exe Parameters

Parameter	Description
-princ	Service principal name (SPN) identifier The entire SPN string, itself, is constructed as follows: <CAS_username> / [<AD_DomainServer> <AD_Domain>] @<AD_DOMAIN>
<CAS_username>	UserName
<AD_DomainServer>	FQDN machine name for a single AD server. This parameter must exactly match (including the case) the <i>name</i> of the AD server under Control Panel > System > Computer Name Full computer name .
<AD_Domain>	The name of the AD domain the CAS uses to authenticate user credentials. This parameter must exactly match (including the case) the <i>domain</i> of the AD server(s) under Control Panel > System > Domain .
<AD_DOMAIN>	Domain name (must be in UPPER CASE)
-mapuser	Maps the CAS user to the domain
-pass	CAS user password
-out	Outputs the "c:\<CAS_user_name>.keytab" key to generate a key tab (similar to a certificate) for this user
c:\<CAS_user_name>.keytab	Required parameter
-ptype	Principal type (required parameter)
KRB5_NT_PRINCIPAL	The Principal provided is of this type. By default AD servers should use this type, but some do not.
+DesOnly	Flag for DES encryption

Example KTPass Command Execution

Figure 10-20 shows how parameters are derived from the CAS user account properties and AD server computer name to run the KTPass command. Note that the values in this figure are example values only; they do not match the configuration example steps outlined in this chapter.

Figure 10-20 Example of How KTPass is Run—SAMPLE VALUES



```
ktpass -princ cas1sso/W2K3-SERVER.cca.cisco.com@CCA.CISCO.COM -mapuser cas1sso -
pass Cisco123 -out c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
```

188747

Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

After the AD server configuration is completed, perform the final step.

To enable the Agent-Based Windows single sign-on with Active Directory (AD), follow these steps:

- Step 1** Go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO**.

Figure 10-21 Active Directory SSO

Device Management > Clean Access Servers > 10.201.241.32

Status Network Filter Advanced Authentication Misc

Login Page · VPN Auth · Windows Auth · OS Detection

Active Directory SSO | NetBIOS SSO

Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)

Account for CAS on Single Active Directory Server Domain (All Active Directory Servers)

Active Directory Server (FQDN)

Active Directory Domain

Account Name for CAS

Account Password for CAS

Active Directory SSO Auth Server

Update

183679

Step 2 Click the checkbox for **Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos)**.

Step 3 Click **Update**.

**Note**

See [Configure AD SSO on the CAS, page 10-9](#) for further details on **Active Directory SSO** page fields.

Confirm AD SSO Service Is Started

Once you have performed all the configuration outlined in [AD SSO Configuration Step Summary, page 10-4](#), make sure the AD SSO service starts on the Clean Access Server.

Go to **Device Management > CCA Servers > Manage [CAS_IP] > Status** ([Figure 10-22](#)).

Figure 10-22 AD SSO Service Is Started

Device Management > Clean Access Servers > 10.201.5.30

Status Network Filter Advanced Authentication Misc

Module	Status
IP Filter	Started
DHCP Server	Started
DHCP Relay	Stopped
IPSec Server	Started
Active Directory SSO	Started
Windows NetBIOS SSO	Stopped

183721

Make sure **Active Directory SSO** is listed with a Status of **Started**.

**Note**

You can also confirm that the CAS is listening on TCP port 8910 (used for Windows SSO) via SSH command: `netstat -a | grep 8910`.

Enable GPO Updates

When a user is not yet authenticated/certified by the Cisco Clean Access (or is on the Authentication VLAN), access to the Windows Domain Controller is limited; and as a result, a complete group policy update might not finish. In addition, the next refresh for group policies occurs every 90 minutes by default. In order to accomplish a GPO update, administrators can force a group policy refresh for Agent users immediately after AD SSO login by enabling the **Refresh Windows domain group policy after login** option.

Administrators can configure the Cisco Clean Access Agent to retrigger a Group Policy Object (GPO) update after the AD SSO user login finishes. If configured in the CAM web console, the Agent calls the “gpupdate” command to re-trigger the Group Policy update after users are logged in.

Login scripts are controlled by the Domain Controller and require a login event to run. For more information about how to use login script in a Windows environment, see [Enabling a Login Script \(Optional\)](#), page 10-27.

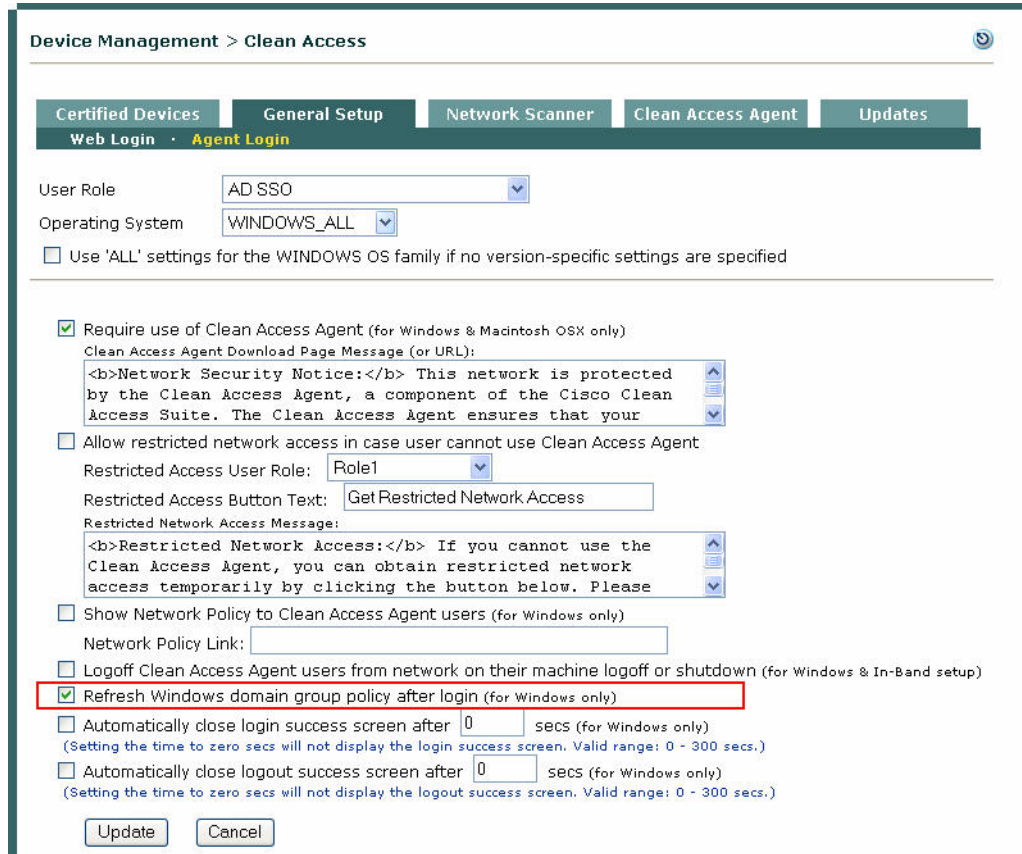
**Note**

Because Microsoft Group Policies are only available since the advent of Active Directory (Windows 2000 and later), the GPO trigger update feature is only available on Windows Vista/XP/2000 machines.

To enable GPO update, follow these steps:

Step 1 Go to **Device Management > Clean Access > General Setup > Agent Login**.

Figure 10-23 Agent Login—General Setup



- Step 2** From the **User Role** dropdown, choose the role to which to apply the GPO update.
- Step 3** From the **Operating System** dropdown, choose the OS to which to apply the GPO update (must be Windows 2000 or later).
- Step 4** Click the checkbox for **Refresh Windows domain group policy after login (for Windows)**.
- Step 5** Click **Update**.

Enabling a Login Script (Optional)



Caution

This step is optional and this section provides reference information for convenience only. Cisco Technical Assistance Center (TAC) does not support questions or troubleshooting for Microsoft login scripts. Refer to <http://support.microsoft.com> for additional support.

GPO update objects, such as login scripts, require an event to trigger them, such as login, or they fail. Running a script in a Windows environment prior to NAC login fails because users do not have access to drive mappings to the AD server or drive resources.

Network-based login scripts and local login scripts are handled differently:

- Local login scripts run locally on a client machine. If you introduce an artificial delay with a script, they work correctly.
- Network-based scripts require continuous access to a AD server for initialization. Depending on your network deployment, you can use a combination of steps to use them. Network-based scripts typically reside on the AD server in the %Sysvol%\scripts folder.

Table 10-3 lists the options for handling network-based scripts.

Table 10-3 Network-Based Login Script Options

Deployment	Option
In Band	Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.
Out-of-Band without IP change	Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.
Out-of-Band with IP change	Use a combination of scripts to copy a script that introduces delay locally, run it, and then delete it. Note A security concern exists while the script resides on the client machine because it can be viewed or copied.

In any type of deployment, you need to create an artificial delay script to run during authentication in order for local or network-based scripts to work correctly. See [Introducing a Delay to Allow Script Use, page 10-28](#).

For network-based script use in Out-of-Band deployments with IP address changes, you must also:

- Append the delete command to the end of the “delay” script.
- Use a reference script that copies the “delay” script to the client machine and then launches it.

For more information, see [Using Network-Based Scripts in Out-of-Band Mode with IP Address Changes, page 10-29](#).

Introducing a Delay to Allow Script Use

You can introduce delay by calling a persistent check action that fails until authentication finishes. For example, you can use ping, Telnet, nslookup, or another action that requires network connectivity to succeed. The following example is a .bat script, but you can use other types of scripts.

When using ping, remember:

- You can ping any IP address that is reachable after Clean Access login succeeds.
- The IP address used for the ping and the AD server do not have to be the same.



Caution

If you ping a protected device that has a real IP address, the user will be able to see the IP address while the delay script runs. You can add a statement to the script to hide the DOS window.

- You only need one IP address.
- All of your mappings can be assigned after the ping succeeds.

Example

```
:CHECK
@echo off
echo Please wait...
ping -n 1 -l 1 192.168.88.128
if errorlevel 1 goto CHECK
@echo on
netuse L:\\192.168.88.128\Scripttest
```

In the example, ping runs in the background until it succeeds. After succeeding, the loop is broken; the system maps to drive L:\ on the same node, where the network-based script resides, and then that script runs. The user sees a DOS window in the background.



Note

You can enhance the script with statements to hide or minimize the DOS window from the user.

Table 10-4 lists the script statements and meanings.

Table 10-4 Reference Script Statements and Meaning

Statement	Meaning
:CHECK	Begin the script.
@echo off	Only display the command output.
echo Please wait...	Show the words “Please wait...” to the end user.
ping -n 1 -l 1 192.168.88.128	Use the ping utility to check if the IP address 192.168.88.128 is reachable: <ul style="list-style-type: none"> -n—do not look up a hostname. 1—send one packet. -l—use the ODBC driver or library. 1—wait one second.
if errorlevel 1 goto CHECK	If the ping utility did not reach 192.168.88.128 successfully, then start again from :CHECK.

Table 10-4 Reference Script Statements and Meaning (continued)

Statement	Meaning
@echo on	Display debug messages.
netuse L:\\192.168.88.128\Scripttest	Map the file share at 192.168.88.128 to the L: drive.

Using Network-Based Scripts in Out-of-Band Mode with IP Address Changes

In Out-of-Band mode with an IP address change, you need to create and run two scripts before calling the targeted network-based script:

- A reference script to copy over and launch the local copy of the script.
- A delay script with a line added to delete the network script after it runs.



Caution

Copying a network script to a user machine that has not been granted network access is a security concern. While the script resides on the user machine, the user can copy or view the script.

Reference Script

Create a script similar to the following example. The script is named “refer.bat”, and it copies over a delay script named “actual.bat” and then launches it.

```
@echo off
echo Please wait...
copy \\192.168.88.228\notlogon\actual.bat actual.bat
actual.bat
```

Table 10-5 lists the script statements and the meaning of each line.

Table 10-5 Reference Script Statements and Meaning

Statement	Meaning
@echo off	Only display the command output.
echo Please wait...	Show the words “Please wait...” to the end user.
copy \\192.168.88.228\notlogon\actual.bat actual.bat	Copy the script “actual.bat” from the “notlogon” folder on the AD server at IP address 192.168.88.228.
actual.bat	Launch the script named “actual.bat”.

Delay Script with Delete Command

To create a script that delays script initialization, refer to the [“Introducing a Delay to Allow Script Use” section on page 10-28](#). As shown in the following example add the **del** command and the name of the script that you want to delete to the end of the delay script. The script is named “actual.bat”.



Caution

We recommend that you reduce network vulnerability by deleting the local copy of the script residing on the end user machine. The last line of the sample script performs the deletion or clean up function.

Example

```

:CHECK
@echo off
echo Please wait...
ping -n 1 -l 1 192.168.88.128
if errorlevel 1 goto CHECK
@echo on
netuse L:\\192.168/88/128/Scripttest
del actual.bat

```

Add LDAP Lookup Server for Active Directory SSO (Optional)

**Note**

The LDAP Lookup server is only needed if you want to configure mapping rules so that users are placed into user roles based on AD attributes after AD SSO authentication. For basic AD SSO without role mapping, or for testing purposes, it is not necessary to configure an LDAP Lookup Server.

If you plan on mapping Windows domain SSO users to multiple user roles, you will need to configure a secondary LDAP Lookup server so that the CAM can perform the mapping. You then specify this LDAP Lookup server for the Active Directory SSO auth provider, as described in [Add Active Directory SSO Auth Server, page 10-6](#).

To configure an LDAP Lookup server, follow these steps:

Step 1 Go to **User Management > Auth Servers > Lookup Servers**.

Figure 10-24 *Lookup Server (LDAP)*

User Management > Auth Servers

Auth Servers | **Lookup Servers** | Mapping Rules | Auth Test | Accounting

List · **New**


Server Type	LDAP Lookup	Provider Name	<input type="text"/>
Server URL	<input type="text" value="ldap://10.1.1.1:389"/>	Server version	Auto <input type="button" value="v"/>
Search(Admin) Full DN	<input type="text"/>	Search(Admin) Password	<input type="text"/>
Search Base Context	<input type="text" value="dc=cisco"/>	Search Filter	<input type="text" value="uid=\$user\$"/>
Referral	Manage (Ignore) <input type="button" value="v"/>	DerefLink	OFF <input type="button" value="v"/>
DerefAlias	Always <input type="button" value="v"/>	Security Type	None <input type="button" value="v"/>
Description	<input type="text"/>		

183845

Step 2 **Server Type** is set to **LDAP Lookup**.

**Note**

There is no **Default Role** dropdown menu on the LDAP Lookup server form because the role is already assigned to the Active Directory SSO auth server. If the LDAP lookup fails, users are mapped to the Default Role of the AD auth server.

- Step 3 Provider Name**—Type a unique name for this lookup server.
- Step 4 Server URL**—Type the URL of the LDAP lookup server, in the form:
`ldap://<directory_server_name>:<port_number>`
- If no port number is specified, 389 is assumed.
- Step 5 Server version**—The LDAP version. Leave as **Auto** (default) to have the server version automatically detected. Supported types include Version 2 and Version 3.
- Step 6 Search(Admin) Full DN (REQUIRED)**—Type the full domain name (DN) of the LDAP administrator or other LDAP user with search privileges. For example, for a domain of CCA-ENG-DOMAIN.CISCO.COM, the Search DN is:
`CN=<username>, CN=Users, DC=CCA, DC=ENG, DC=CISCO, DC=COM`
- Step 7 Search(Admin) Password (REQUIRED)**—Type the password for the LDAP administrator or other LDAP user with search privileges.
- Step 8 Search Base Context**—The Base Context (root of the LDAP tree) in which to perform the search for users, for example:
`CN=Users, DC=CCA, DC=ENG, DC=CISCO, DC=COM`
- Step 9 Search Filter**—The attribute to be authenticated. The search attribute to be matched with any user in the base of the LDAP tree. For example:
- `CN=$user$,` OR
 - `uid=$user$,` OR
 - `sAMAccountName=$user$`
- Step 10 Referral**—The default is Manage(Ignore). Sets whether referral entries are managed (in which the LDAP server returns referral entries as ordinary entries) or returned as handles (Handle(Follow)).
- Step 11 DereferLink**—The default is OFF. If ON, object aliases returned as search results are de-referenced, that is, the actual object that the alias refers to is returned as the search result, not the alias itself.
- Step 12 DereferAlias**—Options are Always (default), Never, Finding, Searching
- Step 13 Security Type**—The default is None. Sets whether the connection to the LDAP server uses SSL.
-
-  **Note** If the LDAP server uses SSL, be sure to import the certificate to the CAM from **Administration > CCA Manager > SSL Certificate | Import Certificate**.
-
- Step 14 Description**—(Optional) If desired, type a description of the LDAP Lookup server.
- Step 15** Click **Add Server**.
- Step 16** Once the lookup server is added, make sure to configure the AD SSO auth server accordingly:
- a. Go to **User Management > Auth Servers > List**.
 - b. Click the **Edit** button for the Active Directory SSO auth server you configured.
 - c. In the **Edit** form, choose the lookup server from the **LDAP Lookup Server** dropdown menu.
 - d. Click **Update Server**.

**Note**

Once the LDAP Lookup Server is configured, role mapping using mapping rules is configured the same way as for any other LDAP server. See “Map Users to Roles Using Attributes or VLAN IDs” in the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(2\)](#) for further details.

Troubleshooting

General

- Make sure the date and time of the CAM, CAS and AD server are all synchronized within 5 minutes of each other or AD SSO will not work. You will have to delete the account on AD, synchronize the times and recreate the account. If the AD server still keeps a record of the old account even though you have deleted it, you may need to create a new account with a different name.
- When setting up the CAS account on the AD server, make sure that the CAS account does not require Kerberos pre-authentication.

**Note**

Perform a `service perfigo restart` on the CAS to make sure it is not using old cached credentials.

KTPass Command

- Make sure the AD domain name (for multiple servers) or single AD server name you enter between “/” and “@” in the KTPass command (e.g. “AD_DomainServer”) exactly matches case-by-case the domain or single AD server name as it appears under **Control Panel > System > Computer Name | Full computer name**. See [Run ktpass.exe Command, page 10-19](#) for details.
- Make sure you enter the realm name after “@” (e.g. “AD_DOMAIN”) in the KTPass command in all **upper case characters**. You must convert the Domain name that appears under **Control Panel > System > Computer Name | Domain** on the AD server to UPPER CASE when entering it in the KTPass command.

Cannot Start AD SSO Service on CAS

If the AD SSO service cannot start on the CAS, this typically indicates a communication issue between the AD server and the CAS.

- If the Active Directory server is not reachable from the CAS at the time of CAS startup, AD SSO service is not started. As a workaround, the administrator must go to **Device Management > CCA Servers > Manage [CAS_IP] > Authentication > Windows Auth > Active Directory SSO** and click the **Update** button to restart the AD SSO service.
- Check that the KTPass command is run correctly. Verify the fields are correct as described in [Run ktpass.exe Command, page 10-19](#). If KTPass was run incorrectly, delete the account, create a new account on the AD server, and run KTPass again.

- Make sure the time on the CAS is synchronized with the AD server. This can be done by pointing them both to the same time server (or, in lab setups by just pointing the CAS to the AD server itself for time (AD server runs Windows time)). Kerberos is sensitive to clock timing and the clock skew cannot be greater than 5 minutes (300 seconds).
- Make sure the Active Directory Domain is in UPPERCASE (Realm) and that the CAS can resolve the FQDN in DNS. (For lab setups you can point to a AD server that runs DNS, as AD requires at least one DNS server).
- Make sure the following are correct: CAS username on the AD server, Active Directory Domain (Kerberos Realm) on the CAS (uppercase), Active Directory Server (FQDN) on the CAS.
- When creating a TAC support case, login to CAS directly at **https://<CAS_IP-address>/admin**, click on Support Logs and change the logging level for Active Directory communication logging to “INFO”. Recreate the problem and download support logs. Make sure to restart the CAS or change the log level back to the default after the support logs are downloaded. See the [Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1\(2\)](#) for further details.

AD SSO Service Starts, but Client Not Performing SSO

If AD SSO service is started on the CAS, but the client machine is not performing Windows Single Sign-On, this typically indicates a communication issue between the AD server and client PC or between the client PC and the CAS. Check that:

- The client does have Kerberos keys.
- Ports are open in the Unauthenticated role to the AD server so that the client can connect.



Note When you test, Cisco recommends first opening complete access to the AD server/DC, then restricting ports once AD SSO is working. When logging into the client PC, make sure to log into the domain using Windows domain credentials (not Local Account).

- The client PC time/clock is synchronized with the AD server.
- The CAS is listening on TCP port 8910. A sniffer trace on the client PC can help.
- The user is logged in using the Windows domain account and not the local account.



Note You must use Clean Access Agent 4.0.0.1 or later to support AD SSO.



Note The CAS/Clean Access Agent do not support the use of multiple NICs on the client PC. The client PC's Wireless NIC must be turned OFF when the Wired NIC is turned ON.

Kerbtray

Kerbtray is a free tool available from Microsoft Support Tools that can be used to confirm that the client has obtained the Kerberos Tickets (TGT and ST), and can also be used to purge Kerberos Tickets on a client machine. The ST (Service Ticket) is of concern for the CAS user account that is created on the AD Server. A green Kerbtray icon on the system tray indicates that the client has active Kerberos tickets. However the ticket needs to be verified as correct (valid) for the CAS user account.

CAS Log Files



Note

The log file of interest on the CAS is `/perfigo/logs/perfigo-redirect-log0.log.0`.

If AD SSO Service does not start on CAS, this indicates a CAS-AD server communication issue:

- Clock is not synchronized between CAS and the Domain Controller:

```
SEVERE: startServer - SSO Service authentication failed. Clock skew too great (37)
Aug 3, 2006 7:52:48 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
```

- Username is incorrect. Note the wrong username “ccass,” error code 6 and the last warning:

```
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos
database (6)
Aug 21, 2006 3:39:11 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
WARNING: GSSServer loginSubject could not be created.
```

- Password is incorrect or Realm is invalid (e.g. not uppercase, bad FQDN, or KTPass run incorrectly). Note error code 24 and last warning:

```
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
INFO: GSSServer - SPN : [ccasso/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer loginToKDC
SEVERE: startServer - SSO Service authentication failed. Pre-authentication
information was invalid (24)
Aug 21, 2006 3:40:26 PM com.perfigo.wlan.jmx.admin.GSSServer startServer
WARNING: GSSServer loginSubject could not be created.
```

The following error indicates a client-CAS communication issue, seen when the client PC’s time is not synchronized with AD server. (Note the difference between this error and the one in which the CAS time is not synchronized with the AD server.)

```
Aug 3, 2006 10:03:05 AM com.perfigo.wlan.jmx.admin.GSSHandler run
SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Clock skew
too great (37))
```