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 8-1
- AD SSO Configuration Step Summary, page 8-5
- Add Active Directory SSO Auth Server, page 8-6
- Configure Traffic Policies for Unauthenticated Role, page 8-7
- Configure AD SSO on the CAS, page 8-11
- Configuring a CAS User on the AD Server for AD SSO, page 8-14
- Configure AD SSO in a Windows 7 Client Environment, page 8-34
- Configure Active Directory for FIPS 140-2 Compliant AD SSO, page 8-36
- Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos), page 8-40
- Confirm Active AD SSO Service, page 8-41
- Enable GPO Updates, page 8-41
- Enabling a Login Script (Optional), page 8-43
- Add LDAP Lookup Server for Active Directory SSO (Optional), page 8-46
- Troubleshooting, page 8-48

Overview

You can configure Cisco NAC Appliance to automatically authenticate 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 authentication and posture assessment without ever having to log in via the Agent.
Overview

Note
Users logging into Cisco NAC Appliance via AD SSO must be running Windows Vista or Windows 7 and have the latest Cisco NAC Agent (version 4.7.1.15 or 4.8.0.32) installed on their client machine in order to remain FIPS 140-2 compliant. Windows XP clients performing AD SSO do not conform to FIPS 140-2 compliance requirements.

Note
AD SSO is supported in cross-forest configurations with two-way trust established between the forests.

Note
The Cisco NAC Web Agent does not support AD SSO functions.

Cisco NAC Appliance Agent/AD Server Compatibility for AD SSO


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 2000/2003/2008 server Active Directory. After the user authentication is validated, authorization (role-mapping) is then performed as a separate lookup in Active Directory using LDAP.

You can also use the CAMs Auth Test function to test AD SSO authentication in Cisco NAC Appliance. For details, see the “Auth Test” section of the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3).

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 Cisco NAC Appliance to automatically authenticate users already authenticated to a backend Kerberos Domain Controller (Active Directory server). Figure 8-1 on page 8-3 shows the general process for Kerberos ticket exchange.

Note
AD SSO fails in Cisco NAC Appliance when the CAS and Cisco NAC Agent attempt to exchange Kerberos tickets with the AD domain that are larger than 16kB.
When the Clean Access Server is configured for AD SSO, it essentially replaces the “Network Services” component shown in Figure 8-1. The general sequence is as follows:

- Windows User and the CAS both have an account on the Active Directory server.
- User 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 user.
  - The NAC Agent on the client machine asks the Windows user for a Kerberos Service Ticket (ST) from AD, so that the NAC Agent can communicate with the CAS.
  - The client requests a Service Ticket from the AD.
  - The AD sends the new ST to the client and the client provides this ST to the NAC Agent.
  - The NAC Agent presents this ST to the CAS as part of the authentication process to establish communication with the CAS.
- The CAS sends back packets and mutually authenticates the client as part of the ADSSO process.
- The CAS uses this information to sign the client onto Cisco NAC Appliance and hence SSO authentication takes place.
- For additional user role mapping (for authentication and posture assessment), an LDAP lookup server with attribute mapping can be configured.

**Note**

Starting from Cisco NAC Appliance Release 4.5(1), the default timeout setting that monitors responses from the CAS changed to 60 seconds, which could impact AD SSO behavior if the response takes longer to come back to the Cisco NAC Appliance system. (For example, if the complete AD SSO process takes 2 minutes, once the 60 second timeout has elapsed, the CAM times out assuming that no response is forthcoming from the CAS that is communicating with the AD domain and automatically moves to the next CAS. If you then examine the CAS following the full 2-minute AD SSO process, you see that the service is actually working.) To help ensure reliable AD SSO behavior, Cisco also recommends verifying that your network DNS servers are functioning and accessible along with your Active Directory servers.
CAS Communication with AD Server

Figure 8-2 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 8-2, 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 Configuring a CAS User on the AD Server for AD SSO, page 8-14) only needs to be executed on the cca-eng-test.cca-eng-domain.cisco.com server.

**Figure 8-2 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:

- You must use Windows Server 2008 Enterprise SP1 (32-bit) with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or Windows 7 with Cisco NAC Agent version 4.7.1.15 or 4.8.0.32 installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO.

- 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 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 appropriate version of ktpass.exe installed. (To determine the correct version of KTPass to support your Cisco NAC Appliance/AD SSO deployment, see Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later.)

- 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.

  Note
  In OOB deployments, ICMP (ping) is used to find the “closest AD server” by the workstation, and must work to all AD servers referenced in sites and services for the Authentication VLAN(s), or all AD servers in the domain if sites and services has not been set up.

- 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 the ktpass.exe Command, page 8-22 for details.
Client systems must already have the Agent installed. Refer to the “Distributing the Agent” chapter of the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3) for additional information on Agent distribution and installation.

Configuration Step Summary

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Add Active Directory SSO Auth Server, page 8-6.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>On the CAM, add a new auth server of type Active Directory SSO and specify a default role for users.</td>
</tr>
<tr>
<td></td>
<td>Open ports on the CAS to allow client authentication traffic to pass through the CAS to/from the Active Directory server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure AD SSO on the CAS, page 8-11.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configuring a CAS User on the AD Server for AD SSO, page 8-14.</td>
</tr>
<tr>
<td></td>
<td>Add a CAS account on the Windows 2000/2003/2008 AD server with which the CAS will communicate, and configure encryption parameters to support the Linux operating system of the CAS.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Enable Agent-Based Windows Single Sign-On with Active Directory (Kerberos), page 8-40.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Confirm Active AD SSO Service, page 8-41.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Enable GPO Updates, page 8-41.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Enabling a Login Script (Optional), page 8-43.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Add LDAP Lookup Server for Active Directory SSO (Optional), page 8-46.</td>
</tr>
<tr>
<td></td>
<td>Optionally configure LDAP lookup servers to map users to multiple roles after authentication.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Refer to Troubleshooting, page 8-48 if necessary.</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Go to User Management &gt; Auth Servers &gt; New.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>From the Authentication Type dropdown menu, choose Active Directory SSO.</td>
</tr>
</tbody>
</table>
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 8-1). 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 Agent.
Configure Traffic Policies for Unauthenticated Role

As Figure 8-2 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 Configuration Guide, Release 4.8(3)*.

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.

**TCP/UDP Ports Supporting AD SSO Implementation**

The following list is an initial comprehensive list of ports to open when implementing AD SSO in your Cisco NAC Appliance network. You may be required to open other ports to support AD services not included in this list.

<table>
<thead>
<tr>
<th>Table 8-1</th>
<th>Recommended Ports to Support AD SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td><strong>Protocol</strong></td>
</tr>
<tr>
<td><strong>Recommended TCP Ports</strong></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
</tr>
<tr>
<td><strong>Recommended UDP Ports</strong></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
</tr>
</tbody>
</table>
**Table 8-1**  
*Recommended Ports to Support AD SSO (continued)*

<table>
<thead>
<tr>
<th>Action</th>
<th>Protocol</th>
<th>Untrusted</th>
<th>Trusted</th>
<th>Purpose/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recommended TCP Ports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
<td><em>:</em></td>
<td>IP address DC Port 88</td>
<td>Kerberos</td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
<td><em>:</em></td>
<td>IP address DC Port 389</td>
<td>LDAP</td>
</tr>
<tr>
<td>Allow</td>
<td>UDP</td>
<td><em>:</em></td>
<td>IP address DC Port 636</td>
<td>LDAP with SSL</td>
</tr>
<tr>
<td><strong>Other Ports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>ICMP request</td>
<td><em>:</em></td>
<td>IP address DC</td>
<td>Ping</td>
</tr>
<tr>
<td>Allow</td>
<td>IP fragments</td>
<td><em>:</em></td>
<td>IP address DC</td>
<td>IP packet fragments</td>
</tr>
</tbody>
</table>

1. When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

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.

When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

If you experience slow performance during Windows login, you can open the following ports in addition to the ports listed in Table 8-1.

**Table 8-2**  
*Additional Ports to Support AD SSO*

<table>
<thead>
<tr>
<th>Action</th>
<th>Protocol</th>
<th>Untrusted</th>
<th>Trusted</th>
<th>Purpose/Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TCP Ports</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
<td><em>:</em></td>
<td>IP address DC Port 1024 - 65535</td>
<td>RPC</td>
</tr>
<tr>
<td>Allow</td>
<td>TCP</td>
<td><em>:</em></td>
<td>IP address DC Port 49152 - 65535</td>
<td>RPC</td>
</tr>
</tbody>
</table>

---

**Add Policy for AD Server**

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.
Configure Traffic Policies for Unauthenticated Role

Step 2 With the direction dropdown set for Untrusted -> Trusted, click the **Add Policy** link. The Add Policy form appears (Figure 8-4).

**Figure 8-4 Configure Traffic Policy for CAS to AD Server**

<table>
<thead>
<tr>
<th>Priority</th>
<th>Action</th>
<th>Protocol</th>
<th>Untrusted (IP/Mask:Port)</th>
<th>Trusted (IP/Mask:Port)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Allow</td>
<td>TCP 6</td>
<td>* / * / *</td>
<td>10.201.152.12 / 255.255.255.255 / 88,135,1025,1026</td>
<td>88-knebros.135-rpc,389-kdp,1025-rpc,1026-rpc</td>
</tr>
</tbody>
</table>

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 / 88,135,1025,1026,3268

**Note** When using LDAP to connect to the AD server, Cisco recommends using TCP/UDP port 3268 (the default Microsoft Global Catalog port) instead of the default port 389. This allows for a more efficient search of all directory partitions in both single and multi domain environments.

Step 5 Type an optional **Description**.

Step 6 Click **Add Policy**.
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.

**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 Configuring a CAS User on the AD Server for AD SSO, page 8-14. You can configure the other fields of this page and click Update, as described below.

**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).
Chapter 8 Configuring Active Directory Single Sign-On (AD SSO)

Configure AD SSO on the CAS

**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 8-7**).

*Figure 8-6 AD SSO—Single Active Directory Server*
b. If you select the Domain (All Active Directory Servers) option, the Active Directory Server (FQDN) field disappears (Figure 8-8). 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 the ktpass.exe Command, page 8-22.

**Figure 8-8 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 8-7). The “Active Directory Domain” is equivalent to “Kerberos Realm”. For example:

CCA-ENG-DOMAIN.CISCO.COM
Configuring a CAS User on the AD Server for AD SSO

You can choose to set up AD SSO with or without running KTPass. In either case you must create the CAS user and then set up encryption according to the following sections:

- Create the CAS User, page 8-14
- Specify encryption using one of the following:
  - Install and Run KTPass, page 8-18
  - Configure AD SSO Without KTPass, page 8-26

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.
Step 4 Right-click the Users folder. In the menu that appears, select New > User (Figure 8-9).

Step 5 In the first New Object - User dialog (Figure 8-10), 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 8-10  Configure the CAS User**

![Diagram of Active Directory Users and Computers with a New Object - User window open. The window shows fields for first name, last name, full name, user logon name, and password.]

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

**Step 7** In the second **New Object - User** dialog (Figure 8-11), 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 8-11   Configure Password for CAS User

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

Figure 8-12   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 8-13).

Figure 8-13  CAS User is Added

Install and Run KTPass

This section addresses the following two topics:
- Install the Correct Version of ktpass.exe to Support Your AD SSO Deployment, page 8-18
- Run the ktpass.exe Command, page 8-22

Install the Correct Version of ktpass.exe to Support Your AD SSO Deployment

The ktpass.exe tool is available as part of the Windows 2000/2003/2008 Server support tools on the Microsoft support site: http://support.microsoft.com/. The KTPass executable is not installed by default in Windows Server 2000/2003. Therefore, if you are configuring in a Windows Server 2000/2003 environment, you must retrieve the executable from the Microsoft Support site prior to installation. To determine the correct version of ktpass.exe to support your Cisco NAC Appliance/AD SSO deployment, see Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later.
To ensure successful KTPass operation, obtain and install the correct version of \texttt{ktpass.exe} according to the AD SSO support table in \textit{Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later}.

You \textit{must} use Windows Server 2008 with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or Windows 7 with an appropriate version of the Cisco NAC Agent installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO.

Cisco has tested the following versions of Windows AD Server and KTPass for the purposes of enabling AD SSO for Windows 7 client authentication.

\begin{table}[h]
\centering
\caption{Windows AD Server and KTPass Version Compatibility for Windows 7 Clients}
\begin{tabular}{|l|l|}
\hline
\textbf{Windows AD Server Version} & \textbf{KTPass Version} \\
\hline
Windows 2008 Server SP2 \textsuperscript{1,2} & 6.0.6002.18005 \\
Windows 2008 Server R2 \textsuperscript{2} & 6.1.7600.16385 \\
Windows 2008 Server Enterprise SP1\textsuperscript{1} & 6.0.6001.18000 \\
Windows 2003 Server & 5.2.3790.1830 \\
\hline
\end{tabular}
\end{table}

1. Window Server 2008 SP2 servers need to perform a Windows Update before running KTPass. Make sure Windows Hotfix KB951191 is installed. Without this Windows Update, the AD SSO service in the CAS might not start. This applies to the KTPass version to be used for Windows 2008 SP2 – 6.0.6002.18005 and for Windows 2008 R2 enterprise it is 6.1.7600.16385.

2. If the AD system is based on an upgrade from Windows Server 2003, you must raise the domain functionality to Windows Server 2008 level for Cisco NAC appliance to perform SSO on Windows 7 clients. Without this you will not be able to automatically login to the Cisco NAC Appliance network.


To install the \texttt{ktpass.exe} tool, follow these steps:

\begin{itemize}
\item \textbf{Step 1} Open a web browser and navigate to \url{http://support.microsoft.com/}.
\item \textbf{Step 2} Locate the Windows Server 2000/2003/2008 Support Tools section(s) of the Microsoft web site.
\end{itemize}
Step 3 Click the Download button.

Step 4 Do one of the following:


- Click Run to begin installing the Windows Server 2000/2003/2008 Support Tools on your local machine.
When you launch the Self-Extractor or click Run, Windows automatically launches the Windows Support Tools Setup Wizard.

**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 8-16.)

**Step 6**

Execute the `ktpass.exe` command according to the directions in the next section, Run the ktpass.exe Command.
Chapter 8  Configuring Active Directory Single Sign-On (AD SSO)

Chapter 8      Configuring Active Directory Single Sign-On (AD SSO)

Configuring a CAS User on the AD Server for AD SSO

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

Run the ktpass.exe Command

This section is designed to execute the KTPass executable for non-Windows 7 client machines to perform SSO. If you are setting up an environment for Windows 7 client machines, see Configure AD SSO in a Windows 7 Client Environment, page 8-34.

When a CAS is configured to interact with a single AD server, you also need to 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.

See Support Information for Cisco NAC Appliance Agents, Release 4.5 and Later for a list of the Windows server versions supported.

Note
When running ktpass.exe, it is very important to observe the following case sensitivity:

- 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. (See Figure 8-19.)
- 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 on a non-Windows 7 client machine:

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 -princ <CAS_username>/\<AD_DomainServer>\,\<AD_Domain>@\<AD_DOMAIN> -mapuser <CAS_username> -pass <CAS_password> -out c:\<CAS_username>.keytab -ptype KR5_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 8-11.

For example (see also Figure 8-17):
Chapter 8  Configuring Active Directory Single Sign-On (AD SSO)

Configuring a CAS User on the AD Server for AD SSO

If your Active Directory domain consists of multiple servers

While adding new servers to an already existing multi-server domain, it is not required to run the ktpass command again. This includes adding a 2008 server to an existing multi-server domain running in a 2003 domain functional level.

- ktpass -princ <CAS_username>/@<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 8-11.

For example (see also Figure 8-17):

C:\Program Files\Support Tools> ktpass -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

The output of the command should be as follows (see also Figure 8-18):

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 (0xbc5120bcfeda01f8)

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), 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.
Chapter 8  Configuring Active Directory Single Sign-On (AD SSO)

Configuring a CAS User on the AD Server for AD SSO

Figure 8-17  Execute ktpass.exe Command

![Command Prompt](image)

Figure 8-18  ktpass.exe Command Output

![Command Prompt](image)

Table 8-4 provides further parameter details.
### Table 8-4  ktpass.exe Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| -princ    | Service principal name (SPN) identifier  
The entire SPN string, itself, is constructed as follows:  
\(<\text{CAS\_username}>/\{<\text{AD\_DomainServer}>\mid<\text{AD\_Domain}>\}@<\text{AD\_DOMAIN}>\) |
| <CAS\_username> | UserName |
| <AD\_DomainServer> | FQDN machine name for a single AD server. This parameter must exactly match (including the case) the name 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 domain 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 8-19 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.

Configure AD SSO Without KTPass

The following procedure guides you through the process necessary to configure an AD SSO user account for both Windows Server 2003 and Windows Server 2008 Active Directory entities operating at their respective full functional levels without having to run KTPass. (This method does not support a Server 2008 AD operating at a 2003 domain functional level.)

Note

AD SSO user accounts configured to connect with Server 2008 AD entities are not FIPS 140-2 compliant.

The following steps apply for DES only encryption type.

Step 1 Open the Properties dialog for an Active Directory account you created using Create the CAS User, page 8-14.

Step 2 To require DES encryption for the new CAS user account, click on the Account tab, enable (check) the Use DES encryption types for this account (Server 2003) or Use Kerberos DES encryption types for this account (Server 2008) option under Account options, and click OK. (See Figure 8-20 and Figure 8-21.)

Note

To set up a Windows 7 client machine for DES encryption, refer to Manually Enable DES on Individual Windows 7 Client Machines.
Figure 8-20    Server 2003 Example—Account Properties

![Server 2003 Example—Account Properties](image)

- User logon name: `ccasso_des_NoKT` @ `cca.cisco.com`
- User logon name [pre-Windows 2000]: `CCAR007\ccasso_des_NoKT`
- Logon Hours
- Log On To
- Account options:
  - Smart card is required for interactive logon
  - Account is sensitive and cannot be delegated
  - Use DES encryption types for this account
  - Do not require Kerberos preauthentication
- Account expires:
  - Never
  - End of: `Saturday, June 12, 2010`
Step 3  Open a DOS prompt on the AD server and enter `ldp.exe` (Figure 8-22 background). An additional Ldp application window opens.

Note  If you do not have a local copy of the `ldp.exe` file, you can locate it under Support Tools in the Microsoft Windows Server Resource Kit.

Step 4  In the Ldp window, connect to the Active Directory domain controller using the Connection > Connect command and entering the domain controller’s IP address or domain name (Figure 8-22 and Figure 8-23). For example, in the Connect dialog, enter `10.201.150.11` or `child.2k8.com`. 

**Figure 8-21 Server 2008 Example—Account Properties**
Figure 8-22  Ldp Application Connection > Connect—Server 2003 Example

Figure 8-23  Ldp Application Connection > Connect—Server 2008 Example

Step 5  After you are connected to the domain controller, use the **Connection > Bind** command to bind to the AD domain as an administrator (Figure 8-24 and Figure 8-25). (You can specify the same ID that you used to create the user account).
Step 6  Display a list of known domain suffixes using the View > Tree command and expanding the pull-down menu that appears (Figure 8-26).

Step 7  Choose DC=cca,DC=cisco,DC=com and click OK.
Step 8  Expand the DC=cca,DC=cisco,DC=com tree and double-click on CN=Users,DC=cca,DC=cisco,DC=com (Figure 8-27).

Step 9  Locate the user account you created in Step 1, right-click on the account entry, and click Modify (Figure 8-28). The account Modify dialog box opens.
Step 10  Specify **userPrincipalName** in the **Attribute** field and enter a `<username>/<FQDN>@<REALM>` value. For example, enter `ccasso_des_NoKT/dcroot.cca.cisco.com@CCA.CISCO.COM` (Figure 8-29).

**Note**  If there are multiple servers in the Active Directory domain, the value must be `<username>/<AD_domain>@<AD_DOMAIN>` (e.g., `casuser_des_NoKT/qa-test1.cca.cisco.com@QA-TEST1.CCA.CISCO.COM`).

Step 11  Complete the change by choosing the **Replace** operation and clicking **Enter**.
Step 12  Specify **servicePrincipalName** in the attribute field and enter `<username>/<FQDN>`. For example, enter `ccasso_des_NoKT/dcroot.cca.cisco.com` value (Figure 8-30).

Step 13  Complete the addition by choosing the **Add** operation and clicking **Enter**.
Step 14 Verify that there are two lines representing your changes in the Entry List display and click **Run**.

Step 15 Once complete, the bottom of the **Ldp** application window should display “Modified `<userDN>`” without errors.

`Modified
"CN=ccasso_des_NoKT,CN=Users,DC=cca,DC-cisco,DC=com"`.

Step 16 To confirm, double-click on the user account name on the left side of the application window and verify that your changes are present in the user account entry.

---

**Configure AD SSO in a Windows 7 Client Environment**

Administrators who configured AD SSO prior to Release 4.7(1) can provide only limited support for Windows 7 clients after upgrade. An unmodified Windows 7 client machine with the Cisco NAC Agent installed still prompts the user with a manual login dialog because Microsoft has disabled DES encryption on Windows 7 client machines by default.

To enable Windows 7 client machines to authenticate via AD SSO in your Cisco NAC Appliance network, you can do one of the following:

**Option 1 (Recommended)**

Allow AD SSO for Windows 7 by enabling additional algorithms on the Microsoft Active Directory servers (see **Enable Additional Algorithms on Existing AD Servers**).
Option 2 (Recommended Only for Small Client Group Testing)

Enable the DES algorithm on the Windows 7 client machines so that they can communicate via the CASs existing AD SSO DES service account configuration (see Manually Enable DES on Individual Windows 7 Client Machines). You can also enable all the encryption types to start the authentication via AD SSO.

Enable Additional Algorithms on Existing AD Servers

**Step 1**
Create a new AD SSO service account according to the guidelines in Add Active Directory SSO Auth Server, page 8-6. Cisco recommends that the current AD SSO account remain unchanged to allow you to quickly switch between the original DES encryption system and the this multi-algorithm option.

**Step 2**
Run KTPass to allow multiple algorithms for this new service account (see Table 8-3).

- For Windows 2008 Server at full functional level:

  ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL -crypto All

- For Windows 2008 Server at 2003 Server functional level:

  ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL

**Note**
Before performing the following step, Cisco strongly recommends making a backup copy of the CAS’s /perfigo/access/tomcat/conf/krb.txt file.

After running the ktpass command above, manually modify two files on the CAS as follows:

- In the CAS CLI, navigate to /perfigo/access/tomcat/conf/krb.txt and add the following lines:

  ```
  [libdefaults]
  kdc_timeout = 20000
  default_tkt_enctypes = RC4-HMAC
  default_tgs_enctypes = RC4-HMAC
  permitted_enctypes = RC4-HMAC
  ```

- Navigate to /perfigo/access/bin/starttomcat.

  Search for CATALINA_OPTS.

  Add -DKRB_OVERRIDE=true to the value of CATALINA_OPTS.

  For example:

  ```
  Old value: CATALINA_OPTS="-server ...
  New Value: CATALINA_OPTS="-server ... -DKRB_OVERRIDE=true"
  ```

  **Note**
  If you are applying this change to an existing HA pair, you must perform the above update on both the HA-Primary and HA-Secondary CAS just as you would upgrade a pair of HA-enabled CASs. For more information, see the Release Notes for Cisco NAC Appliance, Version 4.8(3).

- Restart the CAS by entering the service perfigo stop and service perfigo start commands.

- For Windows 2003 Server at full functional level:

  ktpass -princ newadsso/[adserver.]domain.com@DOMAIN.COM -mapuser newadsso -pass PasswordText -out c:\newadsso.keytab -ptype KRB5_NT_PRINCIPAL
Configure Active Directory for FIPS 140-2 Compliant AD SSO

This section describes how to configure your Windows Server 2008 environment to communicate with a FIPS 140-2 compliant Cisco NAC Appliance deployment. This section covers the following topics:

- Prerequisites
- Configuring Your Windows Environment for FIPS 140-2 Compliance

Prerequisites

- You must use Windows Server 2008 with KTPass version 6.0.6001.18000, and client machines must be running Windows Vista or Windows 7 with Cisco NAC Agent version 4.7.1.15 or 4.8.0.32 installed, to ensure you are able to maintain FIPS 140-2 compliance and support AD SSO. (It is assumed that the user has already configured an Active Directory domain on this system.)
- The Clean Access Manager and Clean Access Server should be configured in FIPS mode and must be running Cisco NAC Appliance Release 4.7(0) or later.
Configuring Your Windows Environment for FIPS 140-2 Compliance

To set up your Windows environment for FIPS 140-2 compliant AD SSO with the Cisco NAC Appliance system:

**Step 1**  
If the AD system is based on an upgrade from Windows Server 2003, you must raise the domain functionality to Windows Server 2008 level for Cisco NAC appliance to operate in FIPS mode, as shown in Figure 8-31. Without this you will not be able connect to the Cisco NAC Appliance network.

![Update the Domain Functional Level](image)

**Figure 8-31  Update the Domain Functional Level**

**Configure the User Profile**

**Step 2**  
Create the user in Windows. The example in this procedure uses the name “fipsy.”
Configure Active Directory for FIPS 140-2 Compliant AD SSO

Figure 8-32  Create a New User

Step 3  Ensure you click the **Password never expires** option and leave the other user options unchecked (especially, ensure that you *do not* require the password to be changed on first login).

Figure 8-33  New User Settings
Step 4  Open the user Properties and update the username to include the domain, as shown in Figure 8-34.

![User Properties](image)

**Figure 8-34  User Properties**

Step 5  Specify Account Options as shown in Figure 8-35.

![Specify Account Options](image)

**Figure 8-35  Specify Account Options**

Step 6  Ensure you have Administrator privileges on the client machine and open a CMD prompt. Verify whether or not KTPass is available by entering `ktpass` at the CMD prompt. If KTPass is not available, navigate to the `\Windows\System32\` directory and try again.

**Note**  KTPass is available on Windows 2008 Server by default.

Step 7  Run the KTPass command as follows:

```
ktpass -princ fipsy/nac-ad-1.nacdevteam.local@NACDEVTEAM.LOCAL -mapuser fipsy -pass Pass1234 -out c:\fipsy.keytab -ptype KRB5_NT_PRINCIPAL -crypto AES128-SHA1
```

Step 8  Configure the Clean Access Server for AD SSO, as described in **Configure AD SSO on the CAS**, page 8-11.
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 8-36  Active Directory SSO*

**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 8-11 for further details on Active Directory SSO page fields.
Confirm Active AD SSO Service

Once you have performed all the configuration outlined in AD SSO Configuration Step Summary, page 8-5, make sure the AD SSO service starts on the Clean Access Server.

Go to Device Management > CCA Servers > Manage [CAS_IP] > Status (see Figure 8-37).

**Figure 8-37  AD SSO Service Is Started**

![Device Management > Clean Access Servers > 10.201.3.30](image)

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

**Note**
You can also confirm that the CAS trusted interface (eth0) 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 Cisco NAC Appliance (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 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 8-43.

**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 7/Vista/XP machines.

To enable GPO update, follow these steps:

**Step 1**
Go to Device Management > Clean Access > General Setup > Agent Login.
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 XP 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 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 8-5 lists the options for handling network-based scripts.

<table>
<thead>
<tr>
<th>Deployment</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Band</td>
<td>Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.</td>
</tr>
<tr>
<td>Out-of-Band without IP change</td>
<td>Open access to the AD server port in the Temporary or Unauthenticated user role and introduce a delay in the body of the script.</td>
</tr>
<tr>
<td>Out-of-Band with IP change</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 8-44.

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 8-45.
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 successful Cisco NAC Appliance login.
- 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**
```batch
: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 8-6 lists the script statements and meanings.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>:CHECK</td>
<td>Begin the script.</td>
</tr>
<tr>
<td>@echo off</td>
<td>Only display the command output.</td>
</tr>
<tr>
<td>echo Please wait...</td>
<td>Show the words “Please wait...” to the end user.</td>
</tr>
<tr>
<td>ping -n 1 -l 1 192.168.88.128</td>
<td>Use the ping utility to check if the IP address 192.168.88.128 is reachable:</td>
</tr>
<tr>
<td></td>
<td>-n—do not look up a hostname.</td>
</tr>
<tr>
<td></td>
<td>1—send one packet.</td>
</tr>
<tr>
<td></td>
<td>-l—use the ODBC driver or library.</td>
</tr>
<tr>
<td></td>
<td>1—wait one second.</td>
</tr>
<tr>
<td>if errorlevel 1 goto CHECK</td>
<td>If the ping utility did not reach 192.168.88.128 successfully, then start again from :CHECK.</td>
</tr>
</tbody>
</table>
Enabling a Login Script (Optional)

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.

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

Table 8-7 lists the script statements and the meaning of each line.

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 8-44. 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.

<table>
<thead>
<tr>
<th>Statement</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>@echo off</td>
<td>Only display the command output.</td>
</tr>
<tr>
<td>echo Please wait...</td>
<td>Show the words “Please wait...” to the end user.</td>
</tr>
<tr>
<td>copy \192.168.88.228\notlogon\actual.bat</td>
<td>Copy the script “actual.bat” from the “notlogon” folder on the AD server at IP address 192.168.88.228.</td>
</tr>
<tr>
<td>actual.bat</td>
<td>Launch the script named “actual.bat”.</td>
</tr>
</tbody>
</table>
Example

```
:CHECK
@echo off
echo Please wait...
ping -n 1 -l 1 192.168.88.128
if errorlevel 1 goto CHECK
@echo on
netuse \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 8-6. You can configure your LDAP Lookup server to use one of the following two authentication mechanisms:

- **SIMPLE**—The CAM and LDAP server pass user ID and password information between themselves without encrypting the data.

- **GSSAPI**—(Generic Security Services Application Programming Interface) Provides an option to encrypt user ID and password information passed between the CAM and the specified LDAP server to help ensure privacy.

**Note**
To ensure complete DNS capability when using GSSAPI, you must ensure that all Domain Controllers, child domains, and hosts conform to strict DNS naming conventions and that you have the ability to perform both forward- and reverse-DNS.

In Cisco NAC Appliance, you can configure one LDAP auth provider using the GSSAPI authentication method and one Kerberos auth provider, but only one of the two can be active at any time. See the “Kerberos” section in the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3)* for more information.
Configure an LDAP Lookup Server

Step 1
Go to User Management > Auth Servers > Lookup Servers. The Server Type is automatically set to LDAP Lookup.

Figure 8-39 Lookup Server (LDAP)—SIMPLE Authentication Method

The configuration page for the LDAP Lookup Server features the same fields as the LDAP Authentication Provider configuration page. For complete details on configuring SIMPLE and GSSAPI authentication methods, refer to the “LDAP” configuration section in the Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3).

Cross-Forest Group Mapping using LDAP Lookup

Step 1
Set up a bidirectional trust between two AD forests.

Step 2
Create an LDAP Lookup Server with GSSAPI in the CAM Web Console.

Step 3
In the Base/Realm Mapping field, specify the base context and realm mapping of the AD forest. For example, if the realm of the first AD forest is CCA.CISCO.COM and other AD forest is NAC.PERFIGO.COM respectively, the base/realm mapping will be as follows:

dc=cca,dc=cisco,dc=com/CCA.CISCO.COM

dc=nac,dc=perfigo,dc=com/NAC.PERFIGO.COM

Step 4
Create an ADSSO server with the LDAP Lookup server.

Note
Reverse DNS lookups should be enabled for the Domain Controllers.
You can use the **Auth Test** function to test AD SSO authentication in Cisco NAC Appliance. For details, see the “Auth Test” section of the *Cisco NAC Appliance - Clean Access Manager Configuration Guide, Release 4.8(3)*.

In the **Auth Test** tab, the realm name must be entered in addition to the username. For example, if the username is `nacuser` and the realm is `NAC.PERFIGO.COM`, then you must enter `nacuser@NAC.PERFIGO.COM`.

You can test with users available in either or both the AD forests.

## Troubleshooting

### General

- If the following error occurs, the issue is most likely with reverse DNS lookup. Reverse DNS lookups must be enabled for the Domain Controllers.

  **No valid credentials provided (Mechanism level: Server not found in Kerberos database (7)).**

- 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.

- In OOB deployments, ICMP (ping) is used to find the “closest AD server” by the workstation, and must work to all AD servers referenced in sites and services for the Authentication VLAN(s), or all AD servers in the domain if sites and services has not been set up.

- In a NAT environment, ensure that the CAM is configured with the NAT entry, for the AD SSO to work properly.

  **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 the ktpass.exe Command, page 8-22 for details.

- Make sure you enter the realm name after “@” (e.g. “ADDOMAIN”) 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 UPPERCASE 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 the ktpass.exe Command, page 8-22. 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 Configuration Guide, Release 4.8(3) 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.
- The client PC time/clock is synchronized with the AD server.
- The CAS trusted interface (eth0) 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: 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 trusted interface (eth0) 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: The CAS and Agent do not support using multiple NICs on the client machine. The client machine 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.

> **Note**

AD SSO fails in Cisco NAC Appliance when the CAS and Cisco NAC Agent attempt to exchange Kerberos tickets with the AD domain that are larger than 16kB.

CAS Log Files

The log file of interest on the CAS is `/perfigo/access/tomcat/logs/nac_server.log`.

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)`
  

- **Username is incorrect. Note the wrong username “ccass,” error code 6 and the last warning:**
  
  INFO: GSSServer - SPN : [ccass/PreM-vM-2003.win2k3public.local@WIN2K3PUBLIC.LOCAL]
  SEVERE: startServer - SSO Service authentication failed. Client not found in Kerberos database (6)`
  
  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)
  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))`
### “Integrity check on decrypted field failed” Error

If AD SSO is not working, and the CAS logs show a “SEVERE: GSS Error: Failure unspecified at GSS-API level (Mechanism level: Integrity check on decrypted field failed (31))” message, check the account name/password in the AD configuration and KTPass command.

The CAS typically returns error messages such as “Integrity check on decrypted field failed” when the password or key is incorrect. For example, this error could appear if you run KTPass on the same account existing on multiple AD servers. Executing the KTPass command again on a new account from a single AD server should resolve the issue.