

NAC Appliance (CCA): Configure and Troubleshoot the Active Directory Windows Single Sign On (SSO)

Document ID: 97251

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure Windows SSO

- Set up the AD SSO Provider
- Run KTPass on the DC
- SSO Configuration on the CAS
- SSO Service Started
- Open Ports to the DC
- Client Sees Agent Performing SSO
- SSO Completed
- SSO User Seen on the Online User List

Troubleshoot Windows SSO

- Could not Start the SSO Service. Please check the configuration.
- Problem : Client Authentication does not Work
- SSO Service is Started, but Client does not Perform SSO
- Kerbtray
- CAS Logs Cannot Start SSO Service
- Known Issues

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes how to configure and troubleshoot the Cisco Network Admission Control (NAC) Appliance, formerly known as Cisco Clean Access (CCA), using Microsoft® Windows Active Directory (AD) Single Sign On (SSO).

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- Make sure the DC runs Win2K SP4/Win2K3 (Standard or Enterprise) SP1 or Win 2K3 R2. Win 2K3 without SP1 is not supported.
- Make sure Windows SSO is supported in an AD environment only. Windows NT environment is not supported. Clean Access Agent is a must.
- Set up the Clean Access Server (CAS) account as shown in the Cisco NAC Appliance – Clean Access Server Installation and Configuration Guide, Release 4.1(2).

Components Used

The information in this document is based on the NAC Appliance software version 4.x or later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure Windows SSO

In this section, you are presented with the information to configure the features described in this document.

Set up the AD SSO Provider

Authentication Type	Active Directory SSO	Provider Name	ADSSO
Default Role	Unauthenticated Role	LDAP Lookup Server	NONE
Description	Single Sign on Provider		

- You cannot perform an authentication test to an AD SSO provider or a VPN SSO.
- The LDAP lookup server is needed only if the users want to do mapping rules for the AD SSO, so that after AD SSO, the users will be placed in roles based on AD attributes. This is not needed to get the basic SSO working (without role mapping).

Run KTPass on the DC

KTPass is a tool available as a part of Windows 2K/2K3 support tools. Refer to Cisco NAC Appliance – Clean Access Server Installation and Configuration Guide, Release 4.1(2) for more information.

When you run KTPass, it is important to note that the computer name that always falls between the / and the @ matches the name of the DC as it would appear under Control Panel >> System >> Computer Name >> Full Computer Name on the DC.

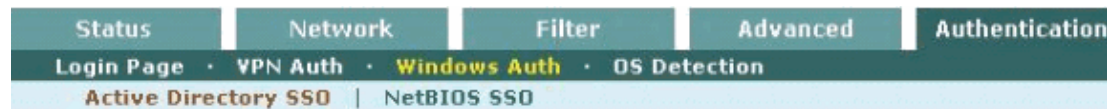
Also, make sure that the realm name that appears after @ highlighted is always in upper case letters.

```
C:\Program Files\Support Tools>ktpass -princ
    prem-vm-2003.win2k3.local@WIN2K3.LOCAL -mapuser ccsso
    -pass Cisco123 -out c:\test.keytab -ptype KRB5_NT_PRINCIPAL +DesOnly
Using legacy password setting method
Successfully mapped ccsso/prem-vm-2003.win2k3.local to ccsso. //confirms ccsso acct is
Key created.
Output keytab to c:\test.keytab
Keytab version: 0x502
keysize 80 ccsso/prem-vm-2003.win2k3.local@WIN2K3.LOCAL ptype 1
    (KRB5_NT_PRINCIPAL) vno 3 etype 0x17 (RC4-HMAC) keylength 16
    (0xf2e787d376cbf6d6dd3600132e9c215d)
Account ccsso has been set for DES-only encryption.
```

SSO Configuration on the CAS

Choose **CCA Servers >> Manage >> Authentication >> Windows Auth >> Active Directory SSO** in order to get into the AD window.

1. Active Directory Domain = Kerberos realm name = Needs to be upper case.
2. Active Directory Server (FQDN) Make sure that the CAS can resolve this name via DNS. This field cannot be an IP address. In this example, log on to the CAS via Secure Shell (SSH) and perform `nslookup prem-vm-2003.win2k3.local` . Then, make sure it resolves successfully.
3. Make sure FQDN matches the name of the AD server (DC) exactly as it appears under Control Panel > System > Computer Name | Full computer name on the AD server machine (DC).



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

Active Directory Server (FQDN)
Active Directory Port
Active Directory Domain
Account Name for CAS
Account Password for CAS HIDDEN
Active Directory SSO Auth Server (add one in [User Management > Auth Servers])

SSO Service Started

Complete these steps:

1. Confirm that the SSO service has been started as shown under **CCA Servers>>Manage>>Status**.

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

2. Confirm that the CAS now listens on TCP 8910 (used for Windows SSO).

```
[root@cs-ccas02 ~]#netstat -a | grep 8910
tcp        0      0  *:8910                :::*
LISTEN
```

Open Ports to the DC

Complete these steps:

1. Open the appropriate ports to the DC.
2. For testing, always open complete access to the DC. Then, once SSO works, you can tie it down to specific ports.

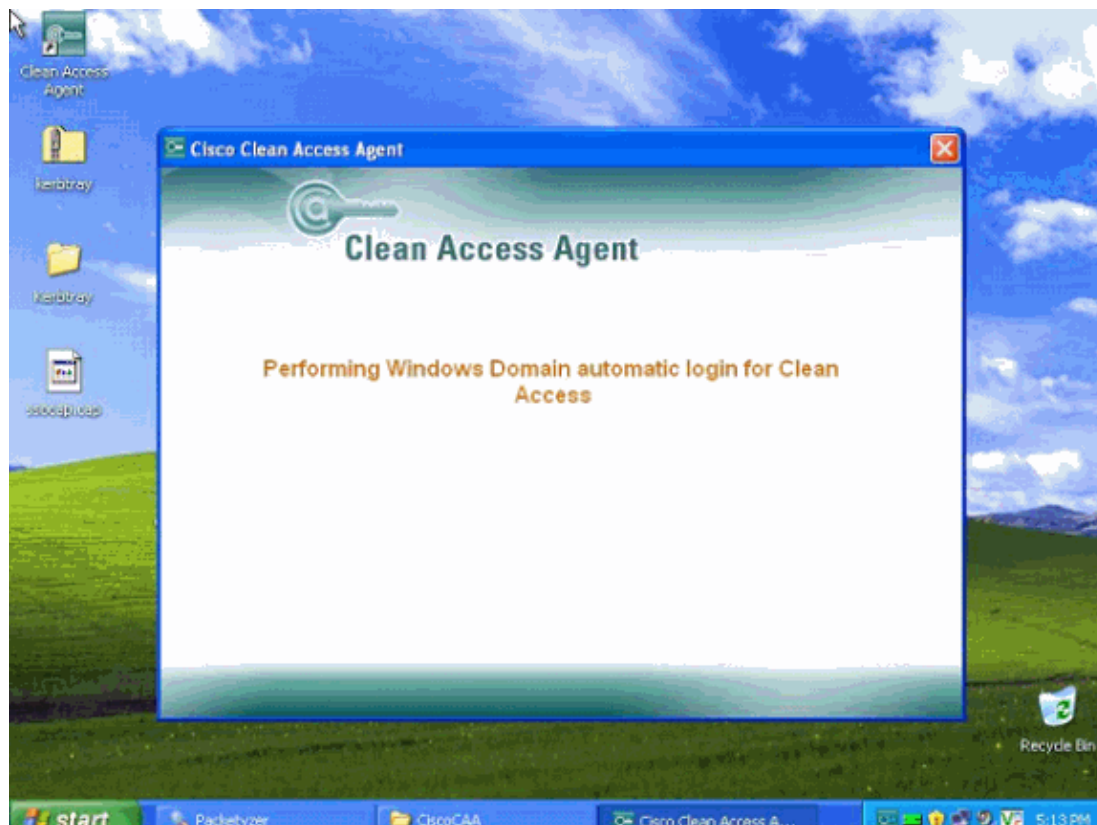
Note: Make sure the following ports are allowed in the untrusted role to Active Directory:

- ◆ **TCP:** 88, 135, 445, 389/636, 1025, 1026
- ◆ **UDP:** 88, 389

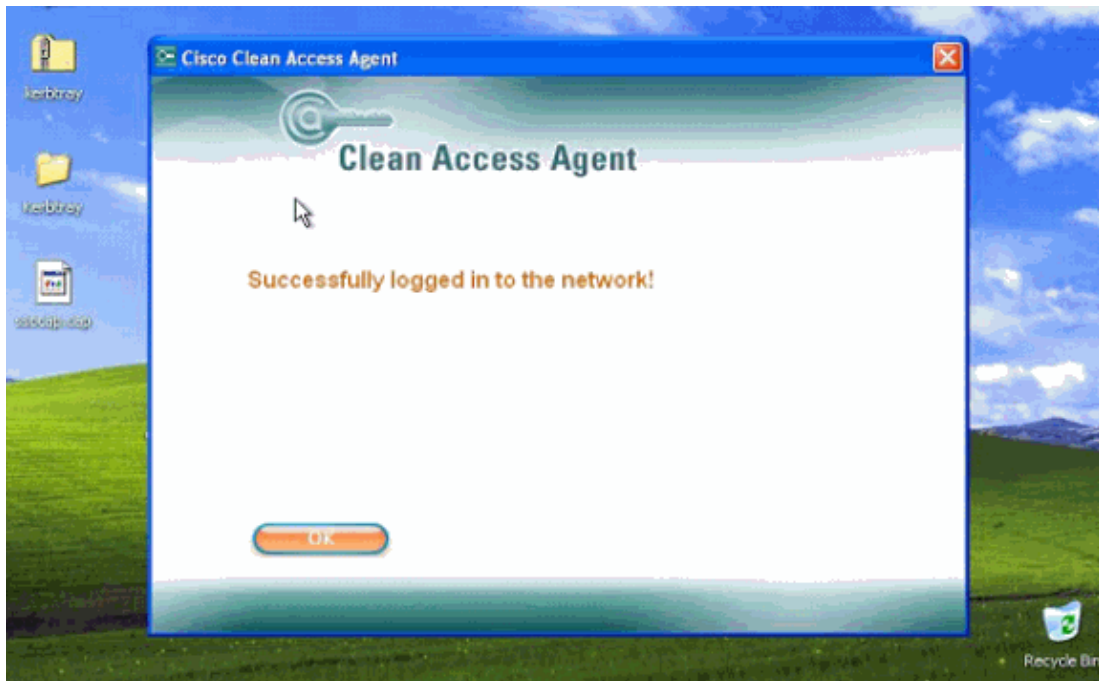
Note: *TCP PORT 445* must be open for Windows Password Reset to work correctly.

3. Ensure that the client runs CCA Agent 4.0.0.1 or later.
4. Log into the PC using the Windows Domain credentials. Make sure you are logging into the domain and not the local account.

Client Sees Agent Performing SSO



SSO Completed



SSO User Seen on the Online User List

Monitoring > Online Users

View Online Users | Display Settings

Any CCA Server | Any Provider | Any Role

View | Reset View

Search For: - Select Field - | equals |

Kick Users

Active users: 1 (Max users since last reset: 1) | Reset Max Users

Online Users 1 - 1 of 1 | First | Previous | Next | Last

User Name	User IP	User MAC	Provider	Role	
prem@WIN2K3.LOCAL	192.168.52.26	00:0C:29:91:2B:80	ADSSO	Unauthenticated Role	<input type="checkbox"/>

Troubleshoot Windows SSO

Could not Start the SSO Service. Please check the configuration.

Error : Could not start the SSO service. Please check the configuration.

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

Active Directory Server (FQDN) | prem-vm-2003.win2k3.local

Active Directory Port | 88

Active Directory Domain | WIN2K3.LOCAL

Account Name for CAS | ccasso

Account Password for CAS |

Active Directory SSO Auth Server | ADSSO

(add one in [User Management > Auth Servers])

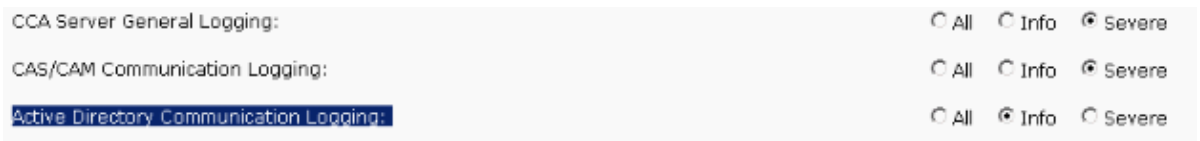
Complete these steps:

1. Check to make sure KTPass runs correctly. It is important to check the fields as mentioned in slide X. If KTPass was run incorrectly, delete the account and create a new account on AD and run KTPass again.
2. Make sure time on the CAS is synchronized with the DC.

This step can be performed by pointing them both to the same time server. In lab setups, point the CAS to the DC itself for time (DC runs Windows time). Kerberos is sensitive to clock and the skew cannot be greater than 5 minutes (300 secs).

Note: When you try to start the AD SSO service of the CAS, an issue might occur with the time synchronization, NTP. If NTP is configured, and clocks are not synchronized, services will not work. Once fixed the services should work.

3. Make sure the Active Directory Domain is in upper case (Realm) and the CAS can resolve FQDN in DNS. For lab setups, you can point to a DC that runs DNS (AD requires at least one DNS server).
4. Log into CAS directly as `https://<CAS-IP-address>/admin`. Then, click **Support Logs** and change the logging level for the Active Directory Communication Logging to **Info**.



5. Re-create the problem and download the support logs.

Problem : Client Authentication does not Work

AD SSO service is started, but client authentication does not work.

Solution

UDP ports were not open in the unauthenticated role. After you add these ports to the traffic policies, authentication should work.

SSO Service is Started, but Client does not Perform SSO

This is usually due to some communication issue between the DC/client PC or between the client PC and the CAS.

These are a few things to make sure of:

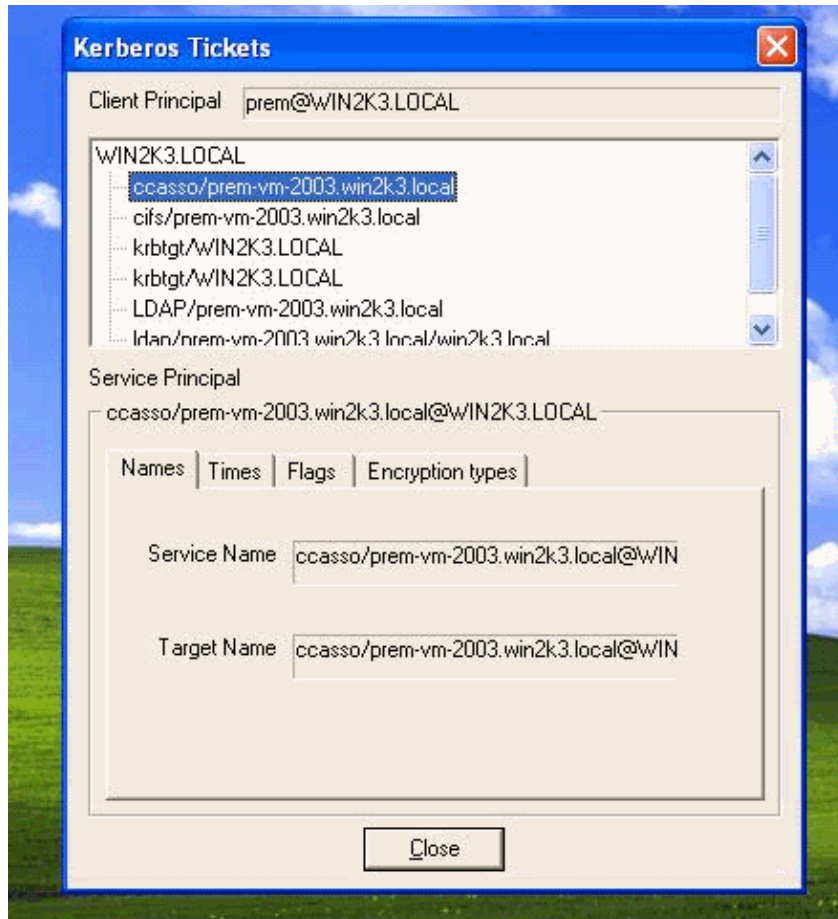
- Client has Kerberos keys.
- Ports are open to the DC so the client can connect, receive agent logs, and receive logs on the CAS.
- Time or clock on the client PC is synchronized with the DC.
- Confirm CAS is listening on port 8910. A sniffer trace on the client PC will also help.
- CCA Agent is 4.0.0.1 or later.
- User is actually logged in using the domain account and not using the local account.

Kerbtray

Kerbtray can be used to confirm that the client has obtained the Kerberos Tickets (TGT and ST). The concern is for the Service Ticket (ST), which is for the CAS account that you created on the DC.

Kerbtray is a free tool available from Microsoft Support tools. It can also be used to purge the Kerberos Tickets on a client machine.

A green Kerbray Icon on the system tray indicates that client has active Kerberos Tickets. However, you need to verify that the ticket is correct (valid) for the CAS account.



CAS Logs Cannot Start SSO Service

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

AD SSO Service does not start on CAS is a CAS-DC communication issue:

1. **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

This means the clock is not synchronized between the CAS and the domain controller.

2. 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.

This means the username is incorrect. Note the wrong username ccass , error code 6 and the last warning.

3. 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 password is incorrect or realm is invalid (not in upper case?). Bad FQDN? KTPass runs incorrectly? Note the Error 24 and the last warning.

Note: Make sure that the KTPass version is 5.2.3790.0. Unless there is a bad version of KTPass that even if the script is run properly, the SSO service will not start.

Client CAS Communication Issue:

```
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))
```

This error is seen when the client PC time is not synchronized with the DC.

Note: The difference between this error and the one where the CAS time is not synchronized with the DC.

Known Issues

- Cisco bug ID CSCse64395 (registered customers only) 4.0 Agent does not resolve DNS for Windows SSO.

This issue is resolved in CCA Agent 4.0.0.1.

- Cisco bug ID CSCse46141 (registered customers only) SSO fails in case CAS cannot reach the AD server during startup.

The workaround is to go to **CCA Servers > Manage [CAS_IP] Authentication > Windows Auth > Active Directory SSO** and click **Update** in order to restart the AD SSO service.

- Perform a service perfigo restart on the CAS. There is a caching issue when the old credentials are cached on the CAS and it does not use the new one until Tomcat is restarted.
- You cannot limit single user log in for SSO. This is the normal behavior for SSO because it is a kerberos protocol, and there is no option to limit single user log in a kerberos protocol.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco NAC Appliance \(Clean Access\) Support Page](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Dec 01, 2008

Document ID: 97251
