

# Configuration Active Directory SSO for NAC Guest Server

Document ID: 109602

---

## Introduction

### Prerequisites

- Requirements
- Components Used
- Conventions

### Configure

- Network Diagram
- Configurations

### Verify

- Verify ADSSO User Group Mapping

### Troubleshoot

### NetPro Discussion Forums – Featured Conversations

### Related Information

---

## Introduction

The Active Directory Single Sign-On (AD SSO) feature uses Kerberos between the web browser of the client and the Cisco NAC Guest Server in order to automatically authenticate a guest against an Active Directory Domain Controller.

**Note:** For the purpose of this document, the NTP and DNS servers are also on the DC, but this is possibly not the case in your environment.

## Prerequisites

### Requirements

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

- DNS must be configured and work on the Cisco NAC Guest Server.
- DNS must be configured and work on the Domain Controller.
- The DNS entries for the Cisco NAC Guest Server must be defined:
  - ◆ A record
  - ◆ PTR record
- The DNS entries for the Domain Controller must be defined:
  - ◆ A record
  - ◆ PTR record
- Cisco NAC Guest Server time settings must be synchronized with the Active Directory Domain.

## Components Used

The information in this document is based on these software and hardware versions:

- NAC Guest Server 2.0
- Microsoft Windows XP with Internet Explorer 6.0
- Windows Server 2003

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 the Cisco Technical Tips Conventions for more information on document conventions.

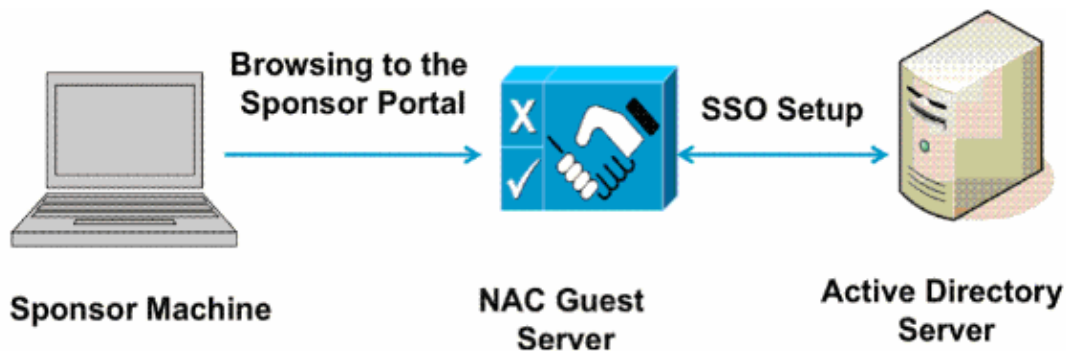
## Configure

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

**Note:** Use the Command Lookup Tool ( registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



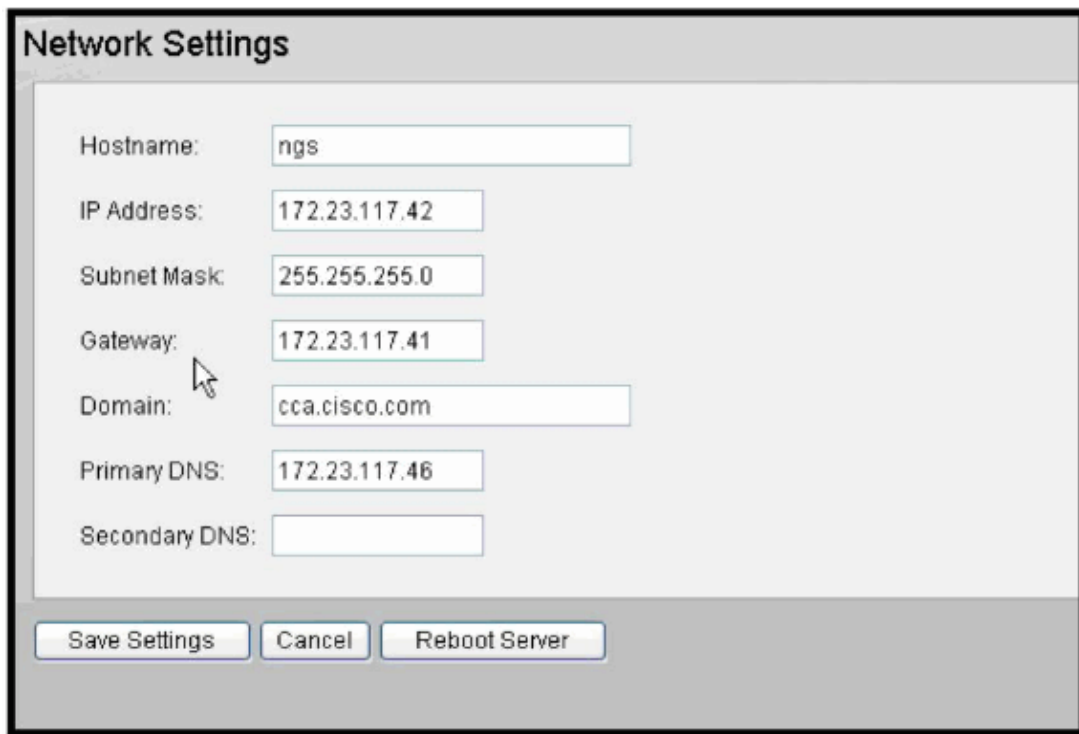
## Configurations

This document uses these IP addresses:

- Domain Controller;72.23.117.46 (w2k3-server.cca.cisco.com)
- NAC Guest Server;72.23.117.42 (ngs.cca.cisco.com)
- Sponsor Machine;72.23.117.45

Complete these steps:

1. Access the NGS Admin Interface. From the browser, go to **http://172.23.117.42/admin**



The screenshot shows a 'Network Settings' dialog box with the following fields and values:

Field	Value
Hostname:	ngs
IP Address:	172.23.117.42
Subnet Mask:	255.255.255.0
Gateway:	172.23.117.41
Domain:	cca.cisco.com
Primary DNS:	172.23.117.46
Secondary DNS:	

At the bottom of the dialog box, there are three buttons: 'Save Settings', 'Cancel', and 'Reboot Server'. A mouse cursor is visible over the 'Domain' field.

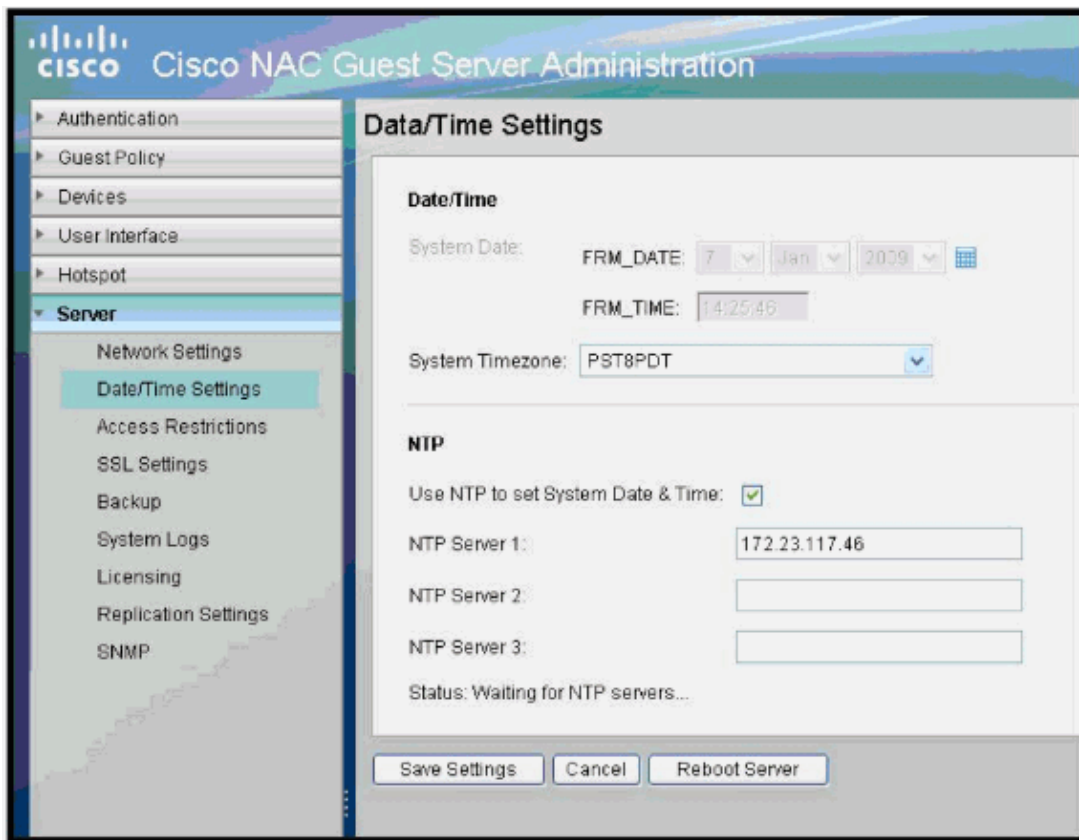
## 2. NGS Network Configuration

Choose **Server > Network Settings**.

- a. Hostname ngs
- b. Domain cca.cisco.com
- c. Primary DNS; 172.23.117.46

## 3. NTP Setup

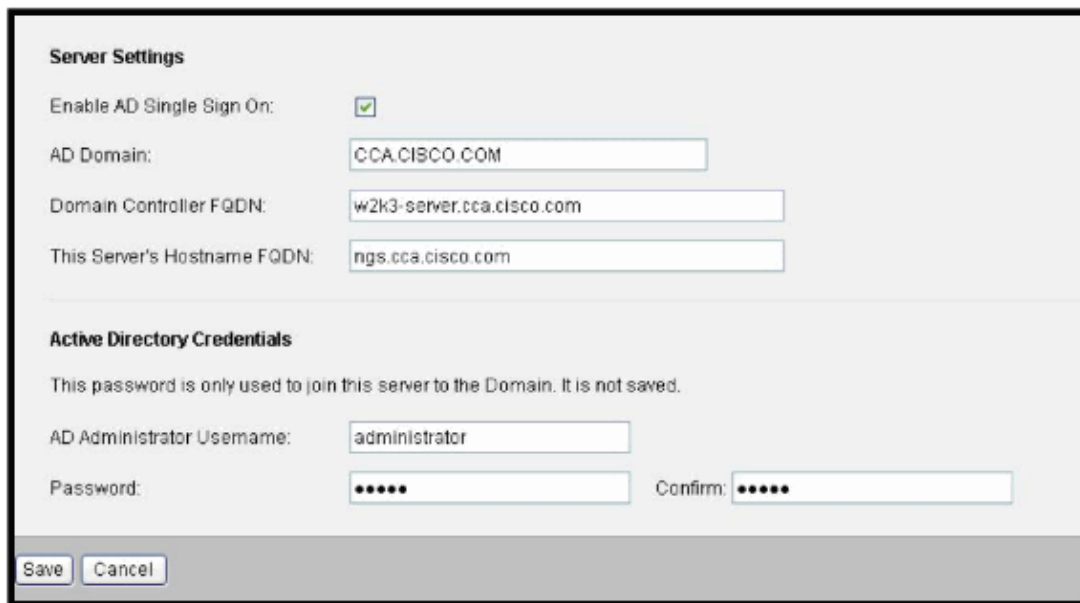
In **Server > Date/Time**, configure the NTP server to DC IP **172.23.117.46**.



#### 4. AD SSO Setup

Before you configure the SSO section, make sure the A and PTR record exist for the domain controller and NAC guest server.

In the AuthServer > Auth SSO section, configure this:



If the configuration is successful, you should see a success message.

### AD Single Sign On

 Your configuration allows non-SSL connections to this server. It is recommended that you disable this if you use AD Single Sign On.

 Configuration Created

#### Server Settings

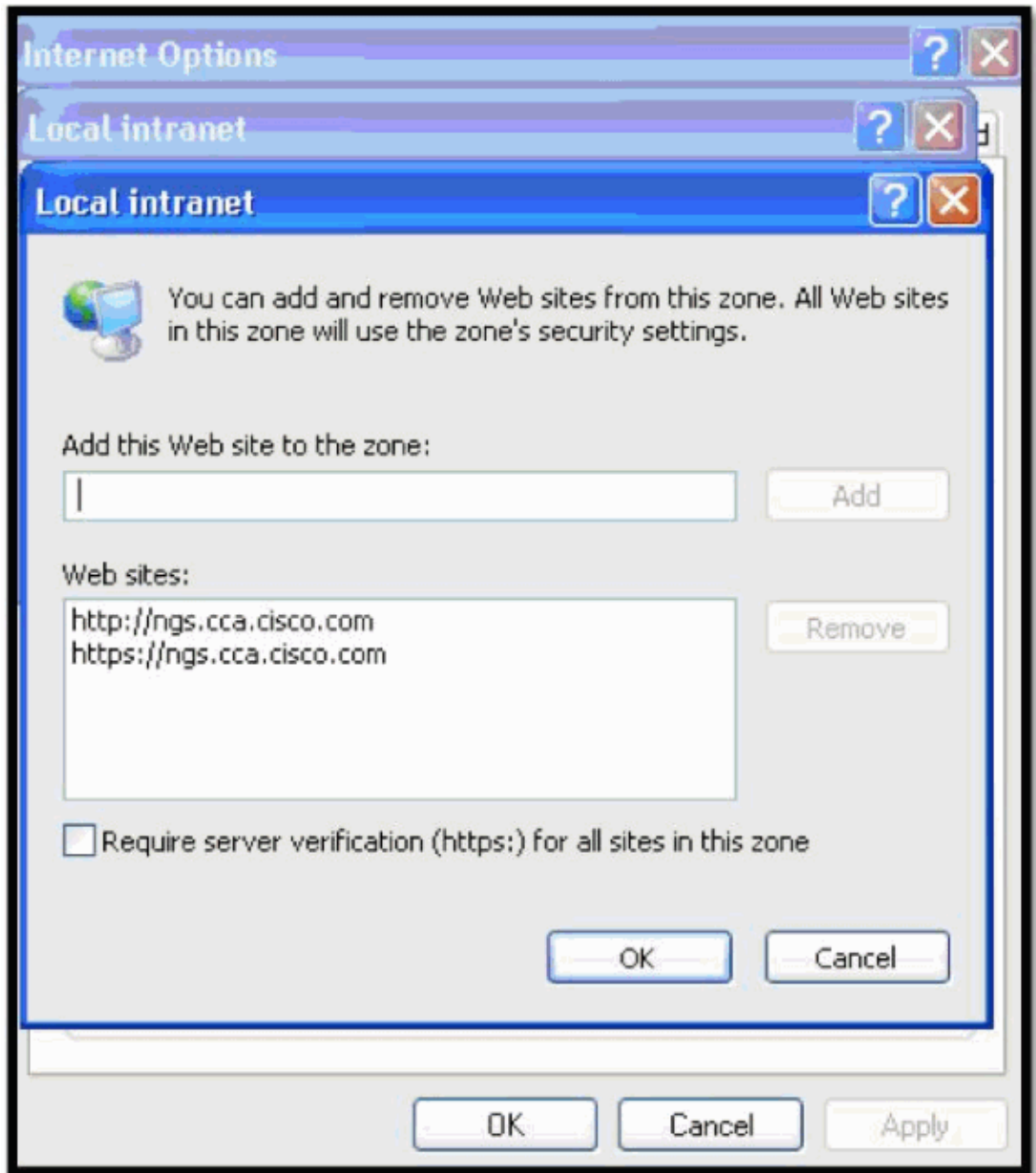
Enable AD Single Sign On:	<input checked="" type="checkbox"/>
AD Domain:	<input type="text" value="CCA.CISCO.COM"/>
Domain Controller FQDN:	<input type="text" value="w2k3-server.cca.cisco.com"/>
This Server's Hostname FQDN:	<input type="text" value="ngs.cca.cisco.com"/>

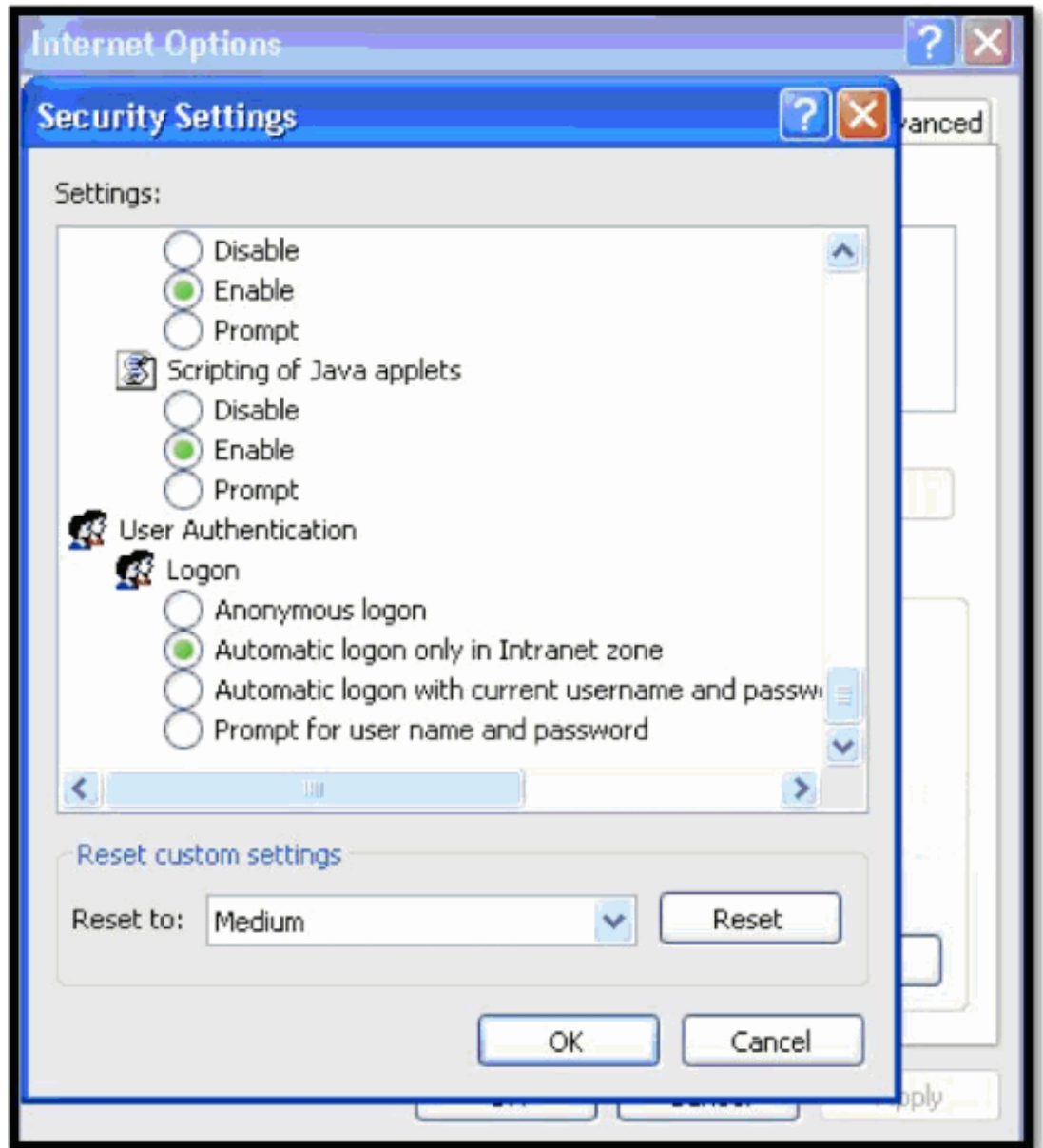
## 5. Validate the SSO feature

From the user machine, log into the domain. In this example, this machine is part of the cca domain. Only Internet Explorer is supported for SSO feature. You need to make sure that the NAC Guest Server is part of local intranet and auto-login is turned **on**.

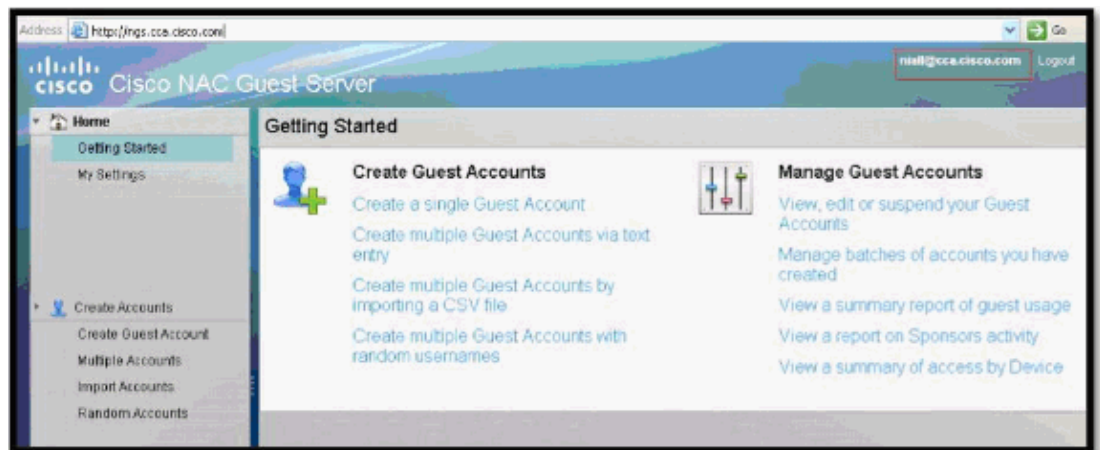
**Note:** Use the FQDN for the guest server in order to test SSO from the browser. For example, the IP address does not work.

- a. Verify the web browser settings:





b. From web browser, go to <http://ngs.cca.cisco.com> . You should be automatically logged in to the ngs with the domain credentials:



Under the NAC Guest Server Audit Logs, you can see the user Niall logged into the default group:

**Audit Logs**

Audit Logs Application Logs Support Logs Log Settings

Action By:  Client IP:

Category: Show All  Server IP: Show All

Between: 10  Jan  2009  and: 11  Jan  2009

Audit Log		
Sponsor/Admin User <input type="button" value="v"/>	Action <input type="button" value="v"/>	Date/Time <input type="button" value="v"/>
admin	Configuration settings saved	11-Jan-2009 10:53 PM
admin	AD Authentication created	11-Jan-2009 10:53 PM
admin	AD Single Sign On enabled	11-Jan-2009 10:53 PM
admin	Login successful	11-Jan-2009 10:52 PM
NGS	Mapped sponsor: niall@CCA.CISCO.COM to group DEFAULT	11-Jan-2009 10:44 PM

Showing 1-6 of 8  10  Per Page

## 6. User Group Mapping with AD SSO (Optional)

*In this section you will learn to map the SSO user to a specific group other than the default group.*

To map the user group with ADSSO, you need to configure the Active Directory Server as Auth Server and then map the AD group with Sponsor User Group.

- Choose **NGS (<http://172.23.117.42/admin>) Authentications > Sponsors > Active Directory Servers**. Add a new domain controller.

**Active Directory Servers**

Active Directory Details

Server Name: NGS.CCA.CISCO.COM

User Account Suffix: @CCA.CISCO.COM

Domain Controller: w2k3-server.cca.cisco.com

Base DN: dc=cca,dc=cisco,dc=com

Username: Administrator

Password:  Confirm:

If you don't wish to change the password please keep the entry empty

Status:

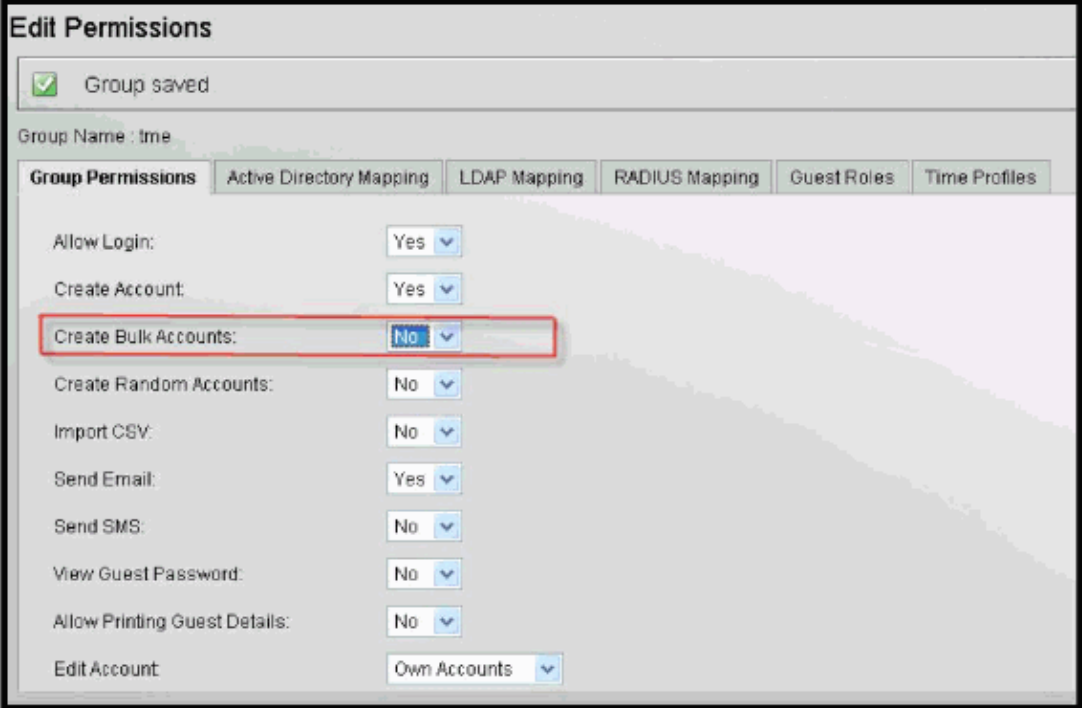
To test the Active Directory connection, enter the details into the form and then click the 'Test Connection' button.

**Active Directory connection successful**

The test connection option has been introduced in NGS 2.0 for ease of troubleshooting. It tells you whether you have configured the DC correctly.

## b. Configure the User Group

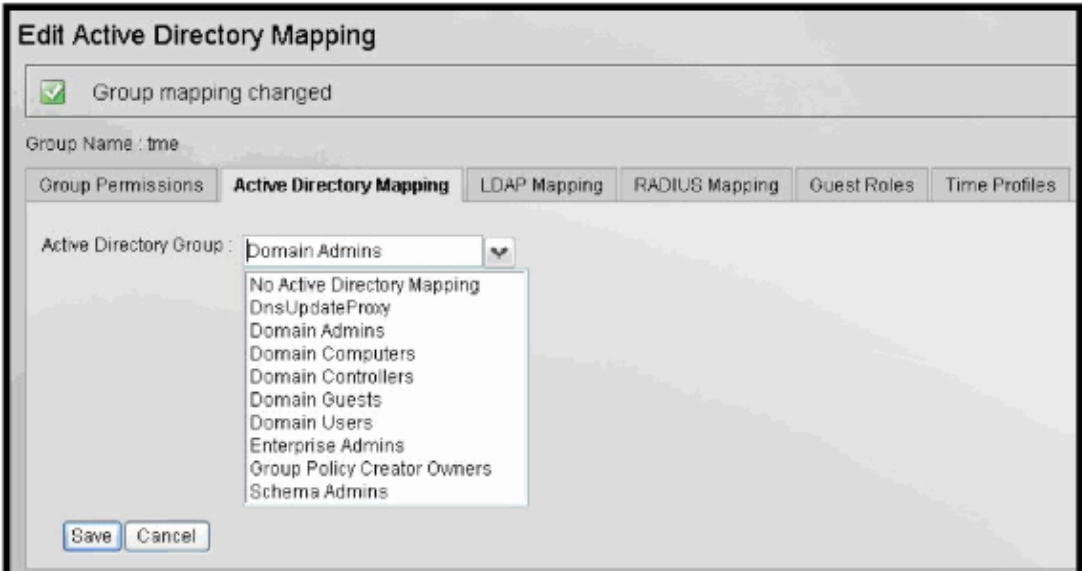
Add a new user group name **tme**. In this example, you choose **NO** in order to bulk account creation. This way you know immediately whether the user has been placed to the tme group or the default group.



The screenshot shows the 'Edit Permissions' interface for a group named 'tme'. At the top, there is a green checkmark and the text 'Group saved'. Below this, the group name 'tme' is displayed. A series of tabs are visible: 'Group Permissions' (selected), 'Active Directory Mapping', 'LDAP Mapping', 'RADIUS Mapping', 'Guest Roles', and 'Time Profiles'. The 'Group Permissions' section contains several settings, each with a dropdown menu:

- Allow Login: Yes
- Create Account: Yes
- Create Bulk Accounts: No (highlighted with a red box)
- Create Random Accounts: No
- Import CSV: No
- Send Email: Yes
- Send SMS: No
- View Guest Password: No
- Allow Printing Guest Details: No
- Edit Account: Own Accounts

In Active Directory Mapping, the test user niall is already part of Domain Admins.



The screenshot shows the 'Edit Active Directory Mapping' interface for a group named 'tme'. At the top, there is a green checkmark and the text 'Group mapping changed'. Below this, the group name 'tme' is displayed. A series of tabs are visible: 'Group Permissions', 'Active Directory Mapping' (selected), 'LDAP Mapping', 'RADIUS Mapping', 'Guest Roles', and 'Time Profiles'. The 'Active Directory Mapping' section contains a dropdown menu for 'Active Directory Group' with the following options:

- Domain Admins (selected)
- No Active Directory Mapping
- DnsUpdateProxy
- Domain Admins
- Domain Computers
- Domain Controllers
- Domain Guests
- Domain Users
- Enterprise Admins
- Group Policy Creator Owners
- Schema Admins

At the bottom of the page, there are 'Save' and 'Cancel' buttons.

## Verify

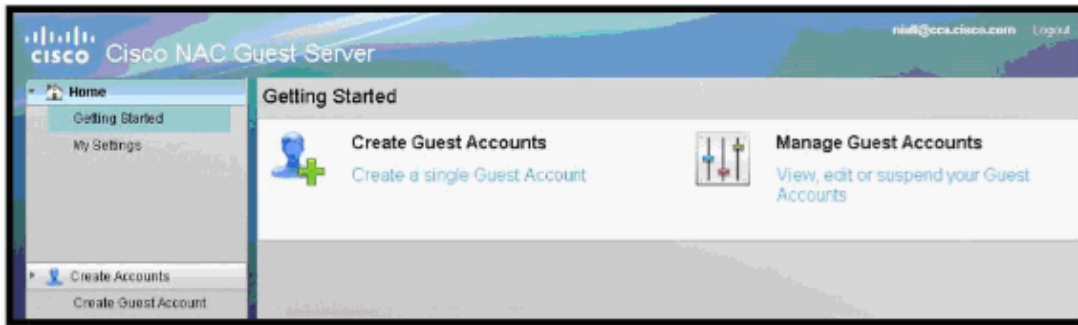
Use this section to confirm that your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

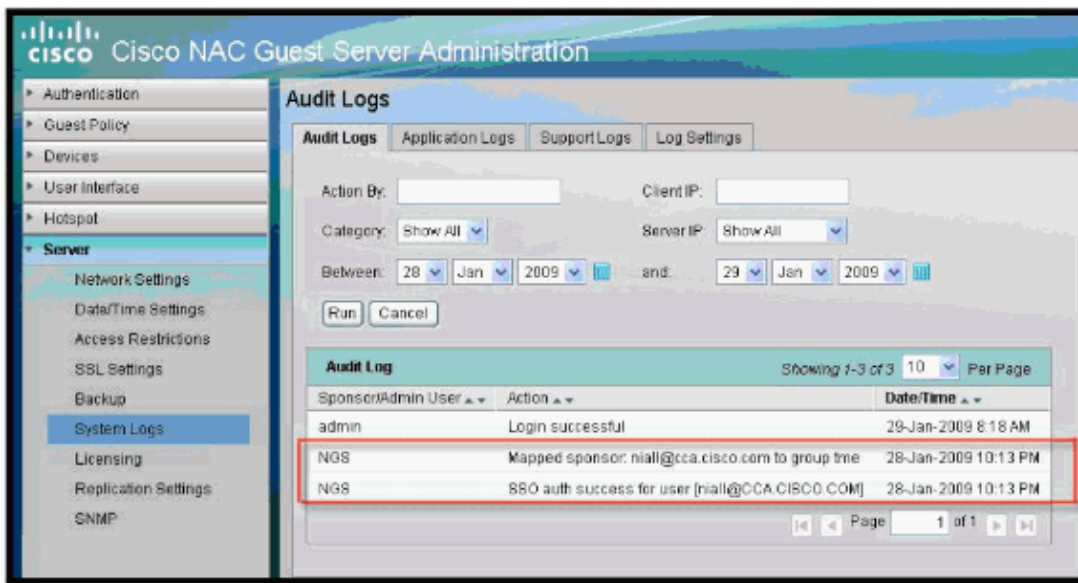
## Verify ADSSO User Group Mapping

In order to access the Sponsor machine, open a new browser and go to <http://ngs.cca.cisco.com>.

Niall should be placed in tme group with no access to bulk account creation.



If you look at the audit logs, you can verify that the Sponsor is placed into the correct Role.



## Troubleshoot

This section provides information you can use to troubleshoot your configuration.

These are error messages in the logs. Kerberos errors results in one of these errors:

- Domain format incorrect / Domain Controller must be a FQDN, not an IP address

The domain has not been entered in a correct format (should be of the form CCA.CISCO.COM).

- Hostname must be a FQDN, not an IP address

The hostname of the NAC Guest server cannot be an IP address it must be a Fully-Qualified Domain Name e.g. nac.cca.cisco.com.

- Cannot determine IP address for Domain Controller

There is a DNS configuration issue.

- Cannot get DNS A record for Domain Controller

There is a DNS configuration issue.

- Cannot get DNS A record for hostname

There is a DNS configuration issue.

- Cannot get DNS PTR record for Domain Controller IP address

There is a DNS configuration issue.

- Cannot get DNS PTR record for hostname IP address

There is a DNS configuration issue.

- Failed to create computer account for this server on the Domain Controller. See application log for details

. View the application log to see the full details of the error.

- Invalid username/password

The administrator username/password is incorrect.

- Invalid Domain or cannot resolve network address for DC

There is a DNS problem on the AD server.

- Domain Controller time does not match this server's time

Ensure the server times match, it is recommended you use NTP to synchronise server times.

- The DC cannot determine the hostname for the Guest server by reverse lookup. There may be an issue with your DNS configuration.

There is a DNS configuration issue on your AD server.

## 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

- [Technical Support & Documentation – Cisco Systems](#)
-

