

Configuración del Active Directory solo Muestra-en para el servidor del invitado del NAC

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Verifique la asignación del grupo de usuarios ADSSO](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

El Active Directory solo Muestra-en (AD SSO) el Kerberos de las aplicaciones de la característica entre el buscador Web del cliente y el Cisco NAC Guest Server para autenticar automáticamente a un invitado contra un regulador del dominio de Active Directory.

Nota: Con el fin de este documento, el NTP y los servidores DNS están también en DC, pero éste no es posiblemente el caso en su entorno.

[prerrequisitos](#)

[Requisitos](#)

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El DNS se debe configurar y trabajo sobre el Cisco NAC Guest Server.
- El DNS se debe configurar y trabajo sobre el controlador de dominio.
- Las entradas DNS para el Cisco NAC Guest Server deben ser definidas:Un expedienteExpediente *PTR*
- Las entradas DNS para el controlador de dominio deben ser definidas:Un expedienteExpediente *PTR*
- Las configuraciones horarias del Cisco NAC Guest Server se deben sincronizar con el dominio de Active Directory.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Servidor 2.0 del invitado del NAC
- Microsoft Windows XP con el Internet Explorer 6.0
- Servidor Windows 2003

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte [Convenciones de Consejos Técnicos de Cisco](#) para obtener más información sobre las convenciones sobre documentos.

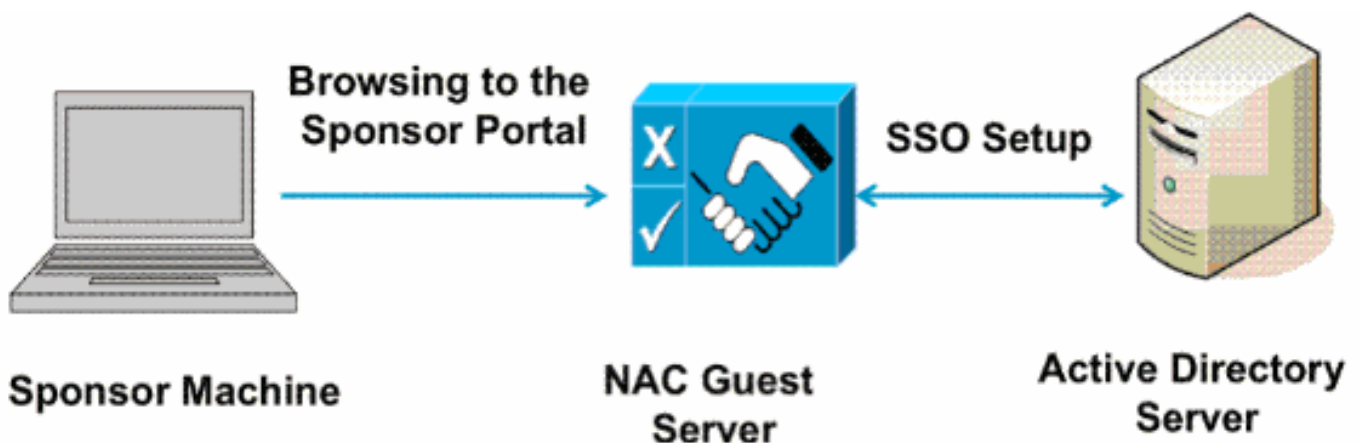
Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Utilice la herramienta [Command Lookup Tool](#) ([clientes registrados solamente](#)) para obtener más información sobre los comandos utilizados en esta sección.

Diagrama de la red

En este documento, se utiliza esta configuración de red:



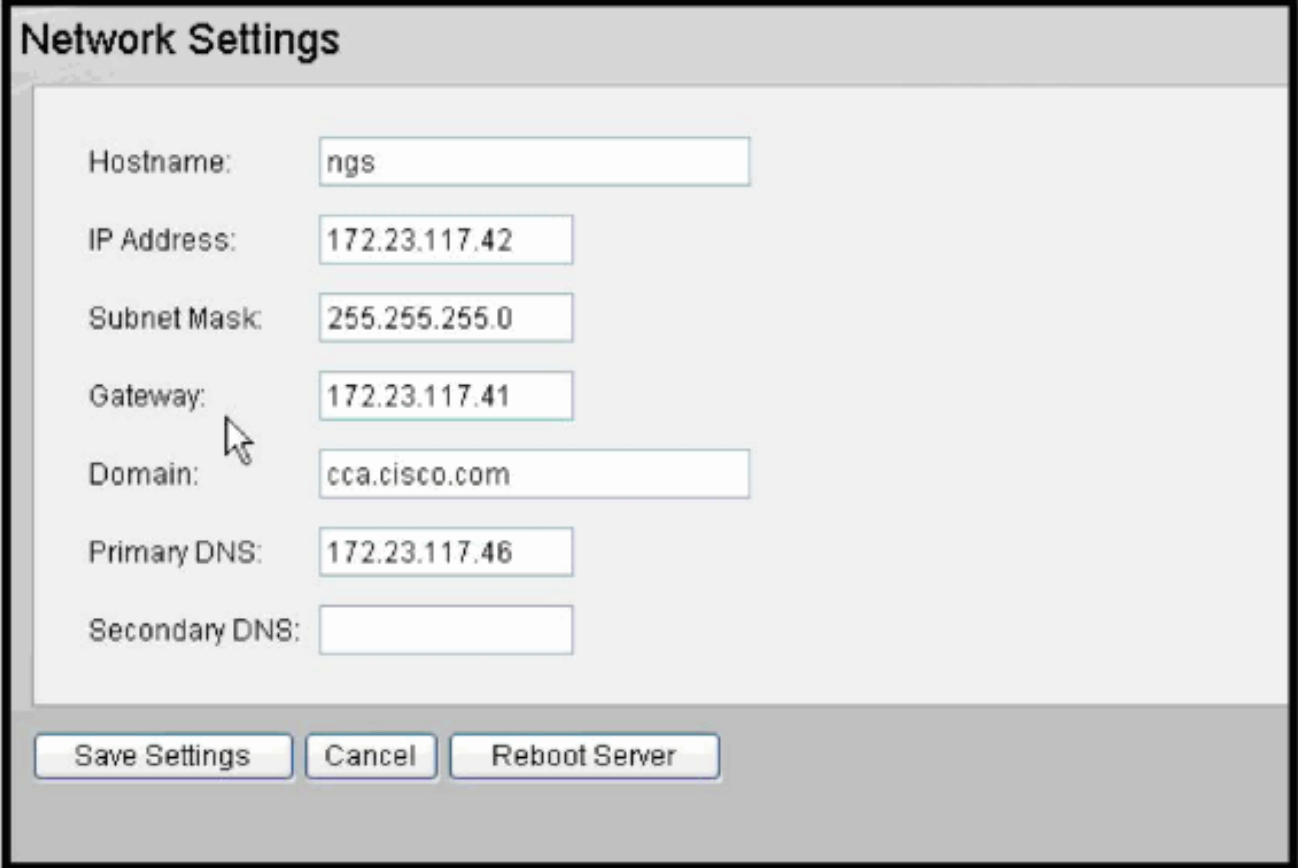
Configuraciones

Este documento utiliza estos IP Addresses:

- Controlador de dominio — 172.23.117.46 (w2k3-server.cca.cisco.com)
- Servidor del invitado del NAC — 172.23.117.42 (ngs.cca.cisco.com)
- Máquina del patrocinador — 172.23.117.45

Complete estos pasos:

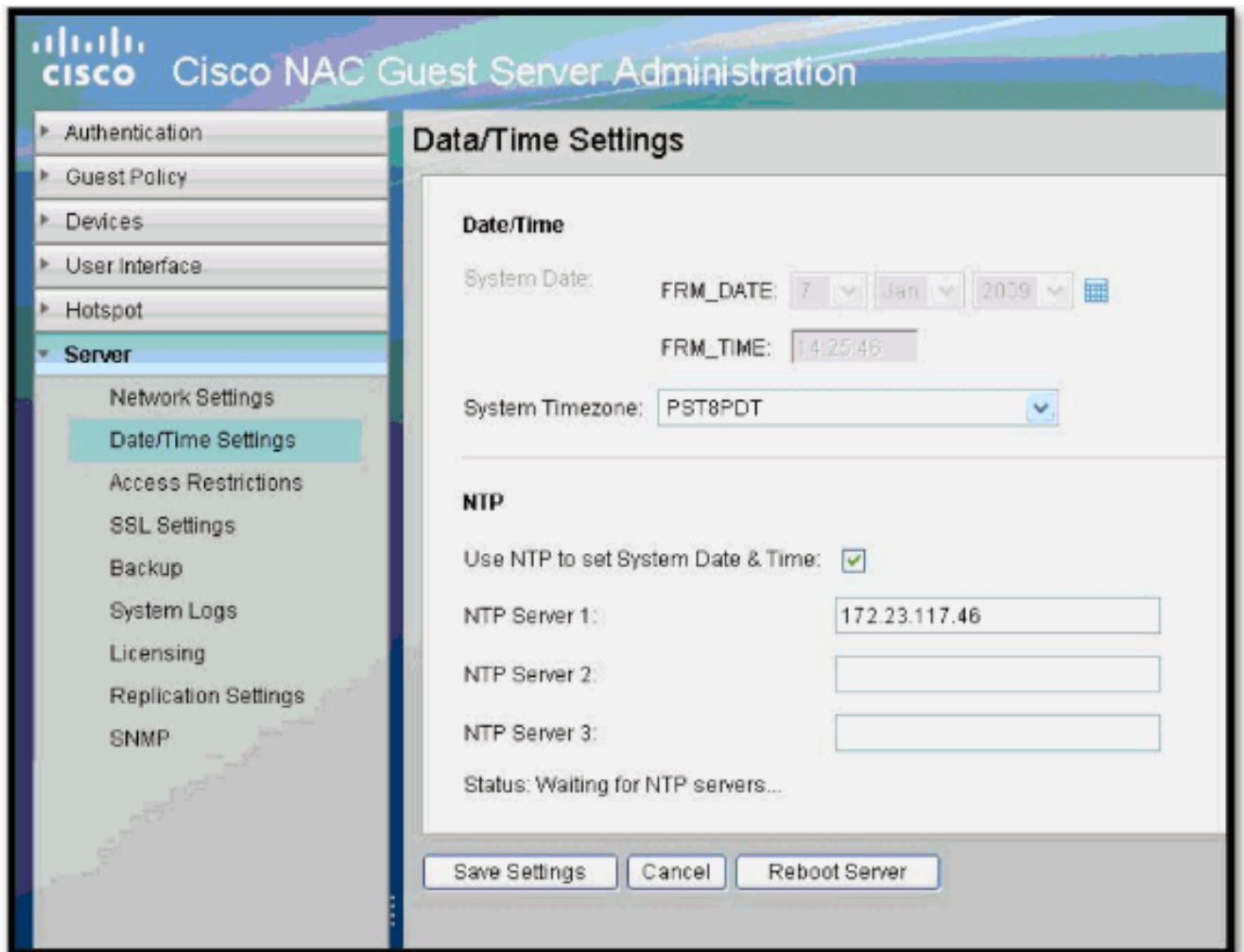
1. Acceda la interfaz NG Admin. Del navegador, vaya a <http://172.23.117.42/admin>



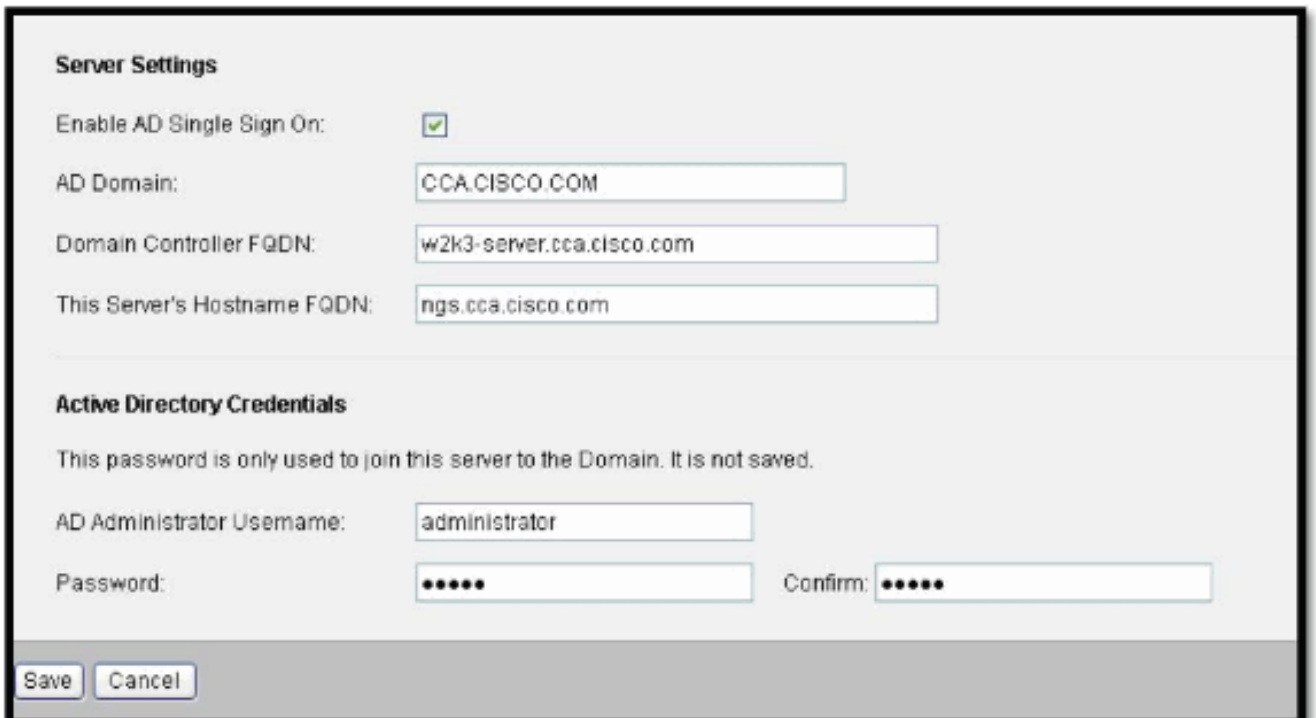
Network Settings

Hostname:	<input type="text" value="ngs"/>
IP Address:	<input type="text" value="172.23.117.42"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Gateway:	<input type="text" value="172.23.117.41"/>
Domain:	<input type="text" value="cca.cisco.com"/>
Primary DNS:	<input type="text" value="172.23.117.46"/>
Secondary DNS:	<input type="text"/>

2. **Configuración de red NGE** Elija las **configuraciones de red del server**>.Nombre de host — ngsDominio — cca.cisco.comDN primarios — 172.23.117.46
3. **Configuración NTP** En la **fecha/la hora del server**>, configure al servidor NTP a IP **172.23.117.46** de DC.



4. **Configuración AD SSO** Antes de que usted configure la sección SSO, asegurese los expedientes A y PTR existir para el servidor del controlador de dominio y del invitado del NAC. En la sección de AuthServer > del auth SSO, configure esto:



Si la configuración es acertada, usted debe ver un Mensaje de éxito.

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. **Valide la característica SSO** De la máquina del usuario, registre en el dominio. En este ejemplo, esta máquina es parte del dominio cca. Solamente soportan al Internet Explorer para la característica SSO. Usted necesita asegurarse que el servidor del invitado del NAC sea Local Intranet (Intranet local) de la parte de y el auto-login está girado. **Nota:** Utilice el FQDN para el servidor del invitado para probar el SSO del navegador. Por ejemplo, la dirección IP no trabaja. Verifique las configuraciones del buscador Web:

Internet Options

Local intranet

Local intranet



You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.

Add this Web site to the zone:

Add

Web sites:

http://ngs.cca.cisco.com
https://ngs.cca.cisco.com

Remove

Require server verification (https:) for all sites in this zone

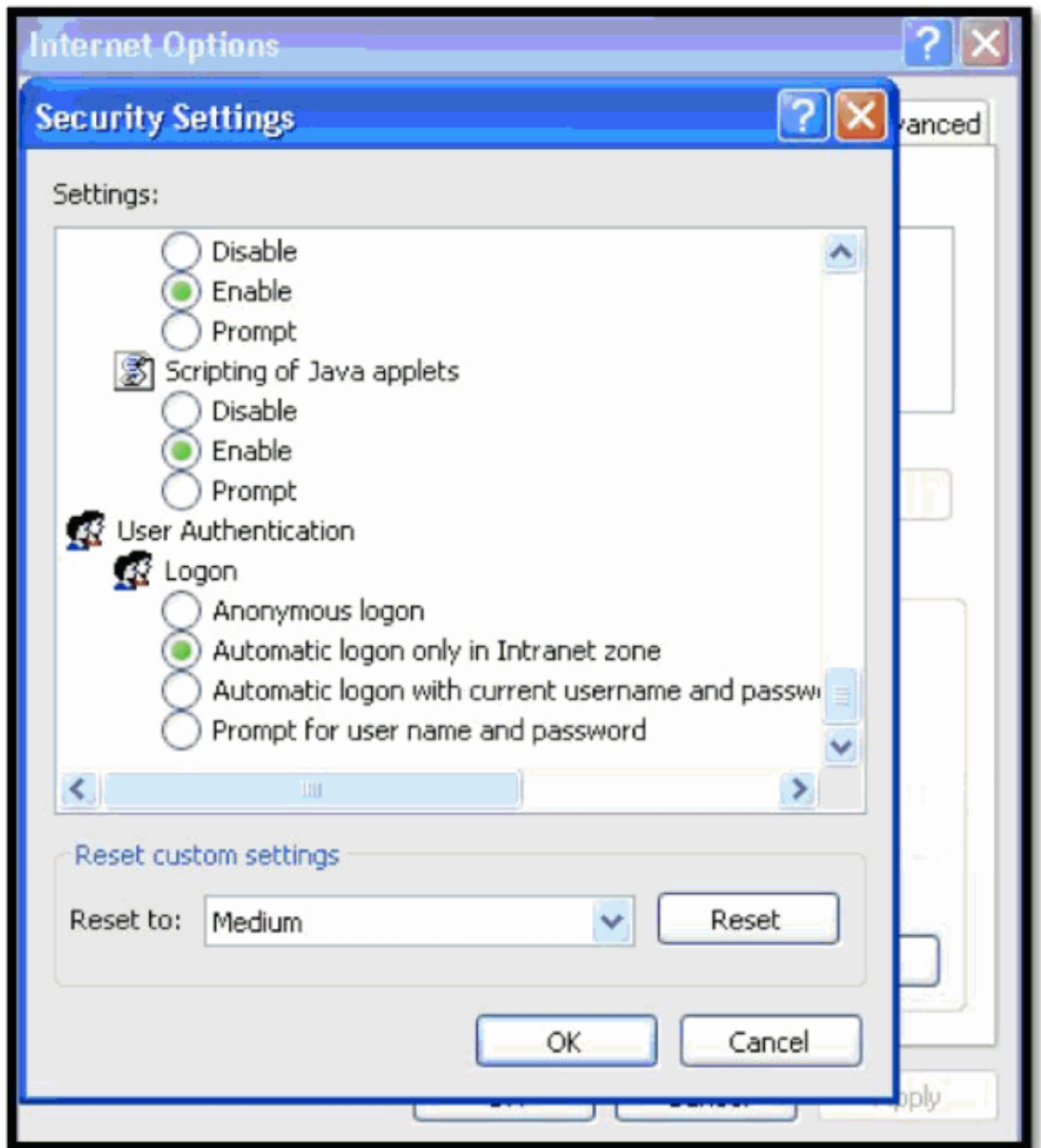
OK

Cancel

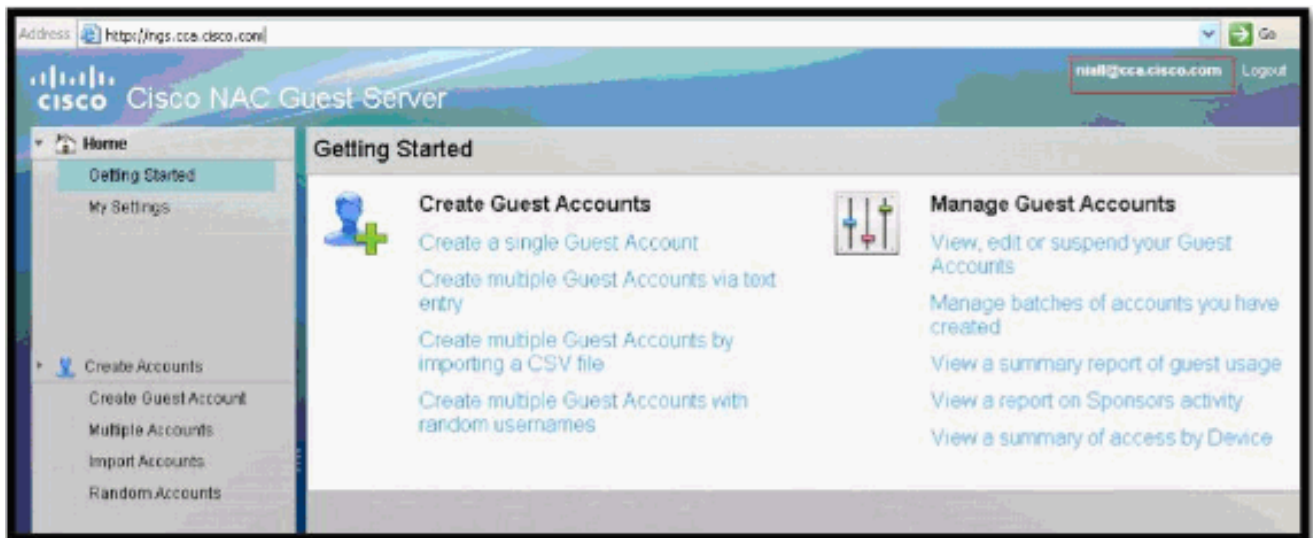
OK

Cancel

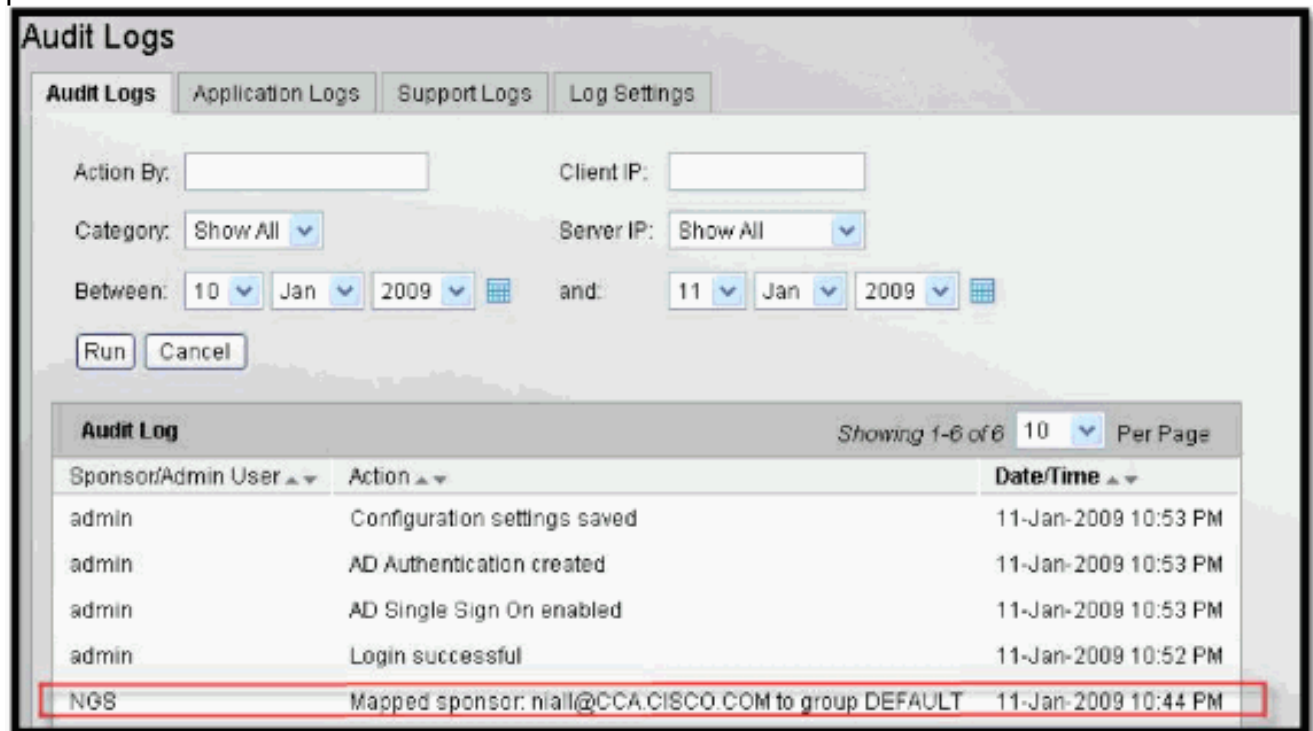
Apply



Del buscador Web, vaya a <http://ngs.cca.cisco.com>. Usted debe ser abierto una sesión automáticamente a los ngs con las credenciales del dominio. **Nota:** El link <http://ngs.cca.cisco.com> trabajará solamente si usted ha configurado el NAC en el modo admin con los credenciales de usuario.



Conforme a los registros de auditoría del servidor del invitado del NAC, usted puede ver al usuario Niall registrado en el grupo predeterminado:



6. **Asignación del grupo de usuarios con AD SSO (opcional)** En esta sección usted aprenderá asociar al usuario SSO a un grupo específico con excepción del grupo predeterminado. Para asociar al grupo de usuarios con ADSSO, usted necesita configurar al servidor Active Directory como servidor de autenticación y después asociar al grupo AD con el grupo de usuarios del patrocinador. Elija los **NG (las autenticaciones de http://172.23.117.42/admin) > patrocinan > los servidores Active Directory**. Agregue un nuevo controlador de dominio.

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

La opción de conexión de prueba se ha introducido en NG 2.0 para la facilidad del troubleshooting. Le dice si usted ha configurado DC correctamente. **Configure al grupo de usuarios** Agregue un nombre del grupo del usuario nuevo — **tme**. En este ejemplo, usted elige **NINGÚN** para abultar creación de una cuenta. Esta manera usted sabe inmediatamente si han colocado al usuario al grupo del tme o al grupo predeterminado.

Edit Permissions

Group saved

Group Name : tme

Allow Login:

 Create Account:

 Create Bulk Accounts:

 Create Random Accounts:

 Import CSV:

 Send Email:

 Send SMS:

 View Guest Password:

 Allow Printing Guest Details:

 Edit Account:

En la asignación del Active Directory, el usuario a prueba Niall es ya dominio Admins de la parte de.

Edit Active Directory Mapping

Group mapping changed

Group Name : tme

Active Directory Group :

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

Verificación

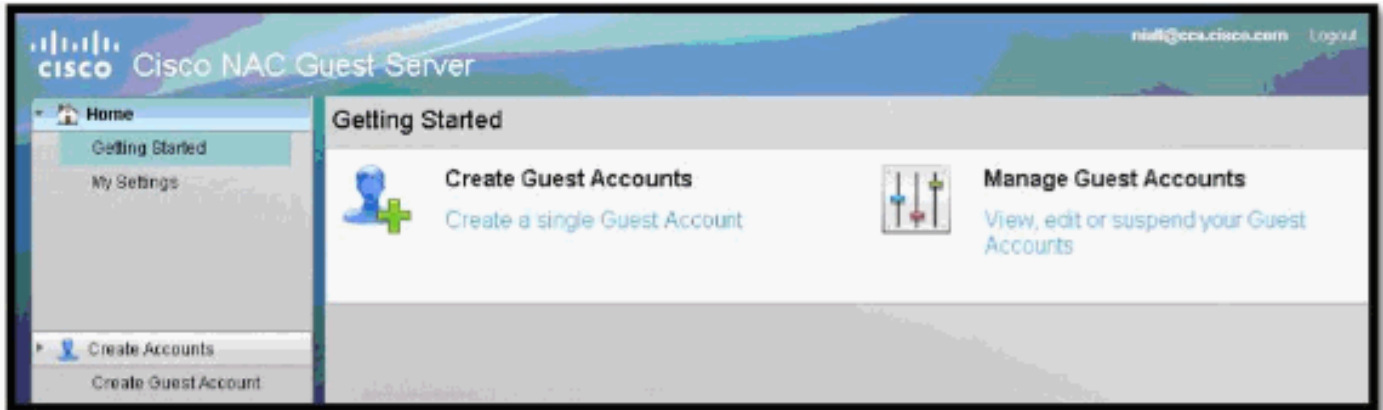
Use esta sección para confirmar que su configuración funciona correctamente.

[La herramienta Output Interpreter Tool \(clientes registrados solamente\)](#) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

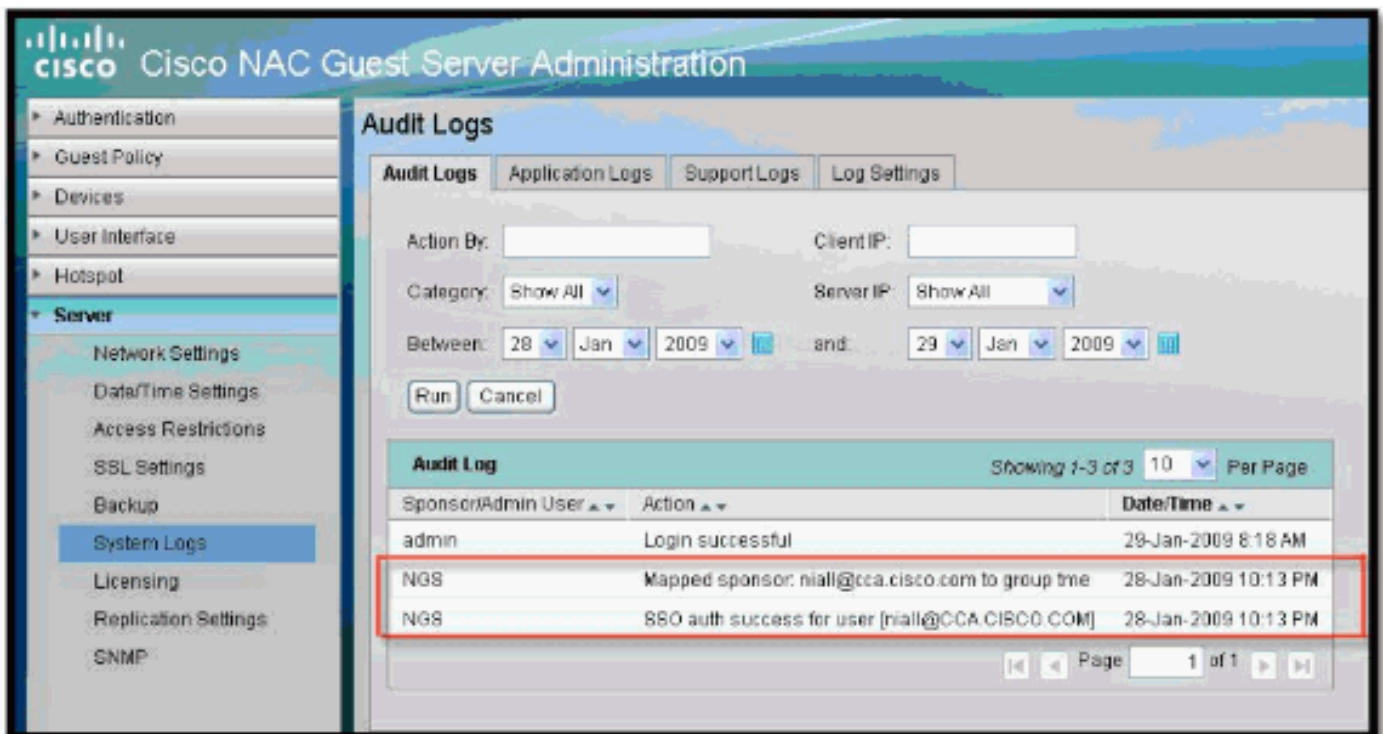
Verifique la asignación del grupo de usuarios ADSSO

Para acceder la máquina del patrocinador, abra a un nuevo navegador y vaya a <http://ngs.cca.cisco.com>.

Niall debe ser colocado en el grupo del tme sin el acceso para abultar creación de una cuenta.



Si usted mira los registros de auditoría, usted puede verificar que coloquen al patrocinador en el papel correcto.



Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Éstos son mensajes de error en los registros. Los errores del Kerberos dan lugar a uno de estos errores:

- El formato del dominio incorrecto/controlador de dominio debe ser un FQDN, no una dirección IP El dominio no se ha ingresado en un formato correcto (debe estar de la forma

CCA.CISCO.COM).

- El nombre de host debe ser un FQDN, no una dirección IP El nombre de host del servidor del invitado del NAC no puede ser una dirección IP que debe ser un nombre de dominio completamente calificado e.g. nac.cca.cisco.com.
- No puede determinar el IP Address para el controlador de dominio Hay un problema de la Configuración de DNS.
- No puede conseguir al DNS un expediente para el controlador de dominio Hay un problema de la Configuración de DNS.
- No puede conseguir el expediente DNS A para el nombre de host Hay un problema de la Configuración de DNS.
- No puede conseguir el expediente PTR DNS para la dirección IP del controlador de dominio Hay un problema de la Configuración de DNS.
- No puede conseguir el expediente PTR DNS para la dirección IP del nombre de host Hay un problema de la Configuración de DNS.
- No podido crear el ordenador explique este servidor en el controlador de dominio. Vea el log de aplicaciones para los detalles . Vea el log de aplicaciones para ver las profundidades totales del error.
- Nombre de usuario inválido/contraseña El nombre de usuario del administrador/la contraseña es incorrectos.
- El dominio inválido o no puede resolver a la dirección de red para DC Hay un Problema de DNS en el servidor AD.
- El tiempo del controlador de dominio no hace juego el tiempo de este servidor Asegure la coincidencia de las horas del servidor, él se recomienda le el uso NTP de sincronizar las horas del servidor.
- El CC no puede determinar el nombre de host para el servidor del invitado por la búsqueda inversa. Puede haber un problema con su confiugration DNS. Hay un problema de la Configuración de DNS en su servidor AD.

[Información Relacionada](#)

- [Soporte Técnico y Documentación - Cisco Systems](#)