# Configuração do diretório ativo única Sinal-para no server do convidado NAC

## Índice



## Introdução

O diretório ativo único Sinal-(AD SSO) no Kerberos dos usos da característica entre o navegador da Web do cliente e o Cisco NAC Guest Server a fim autenticar automaticamente um convidado contra um controlador de domínio do diretório ativo.

**Nota:** Com a finalidade deste documento, o NTP e os servidores DNS estão igualmente no DC, mas este não é possivelmente o caso em seu ambiente.

## Pré-requisitos

### Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- O DNS deve ser configurado e trabalho no Cisco NAC Guest Server.
- O DNS deve ser configurado e trabalho no controlador de domínio.
- As entradas de DNS para o Cisco NAC Guest Server devem ser definidas:Um registroRegistro *PTR*
- As entradas de DNS para o controlador de domínio devem ser definidas:Um registroRegistro *PTR*
- As configurações de tempo do Cisco NAC Guest Server devem ser sincronizadas com o domínio do diretório ativo.

## Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Server 2.0 do convidado NAC
- Microsoft Windows XP com internet explorer 6.0
- Windows Server 2003

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

## Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

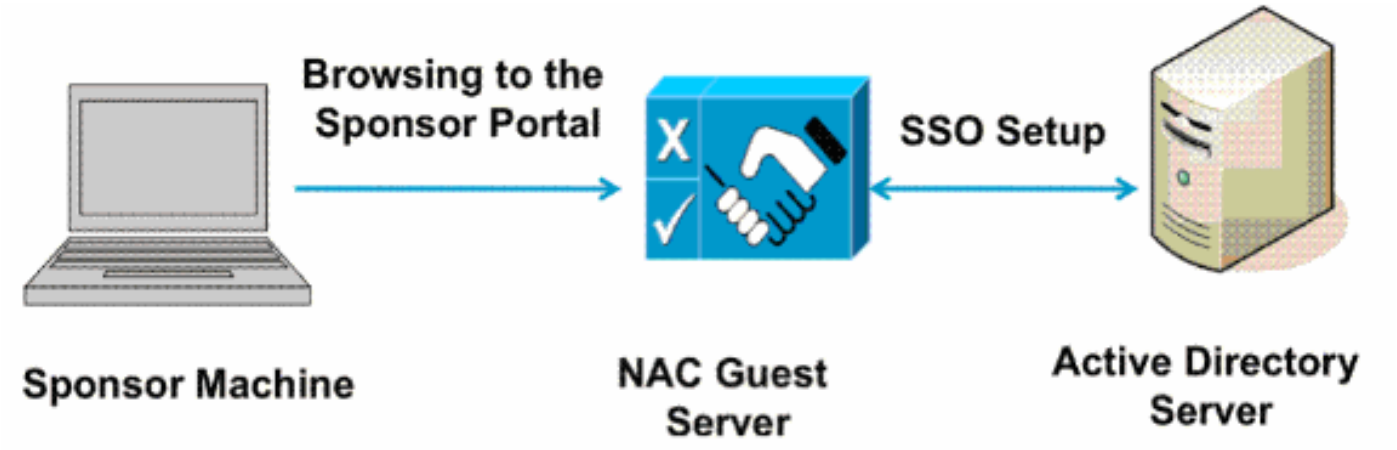
# Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

**Nota:** Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



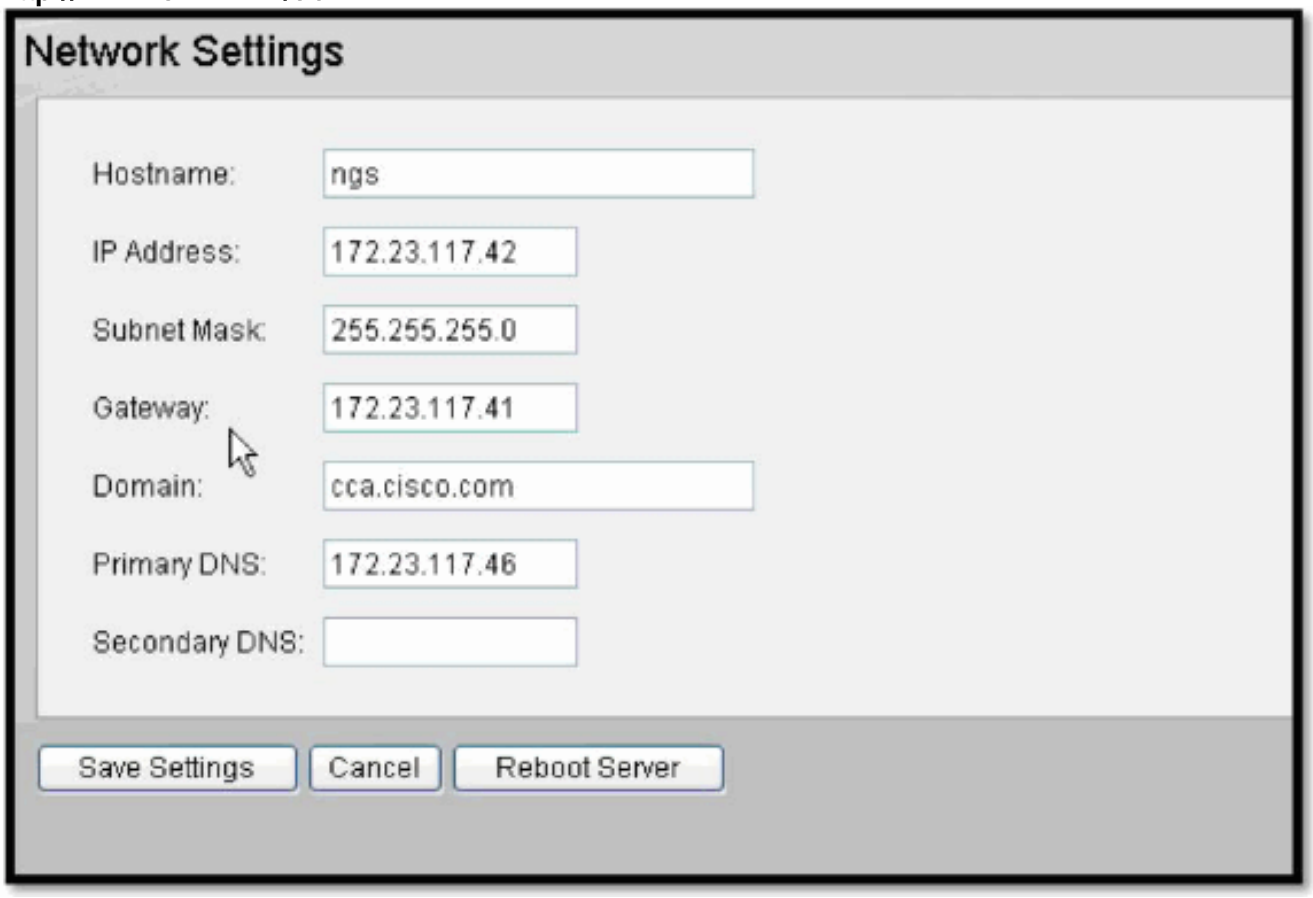

## Configurações

Este documento usa estes endereços IP de Um ou Mais Servidores Cisco ICM NT:

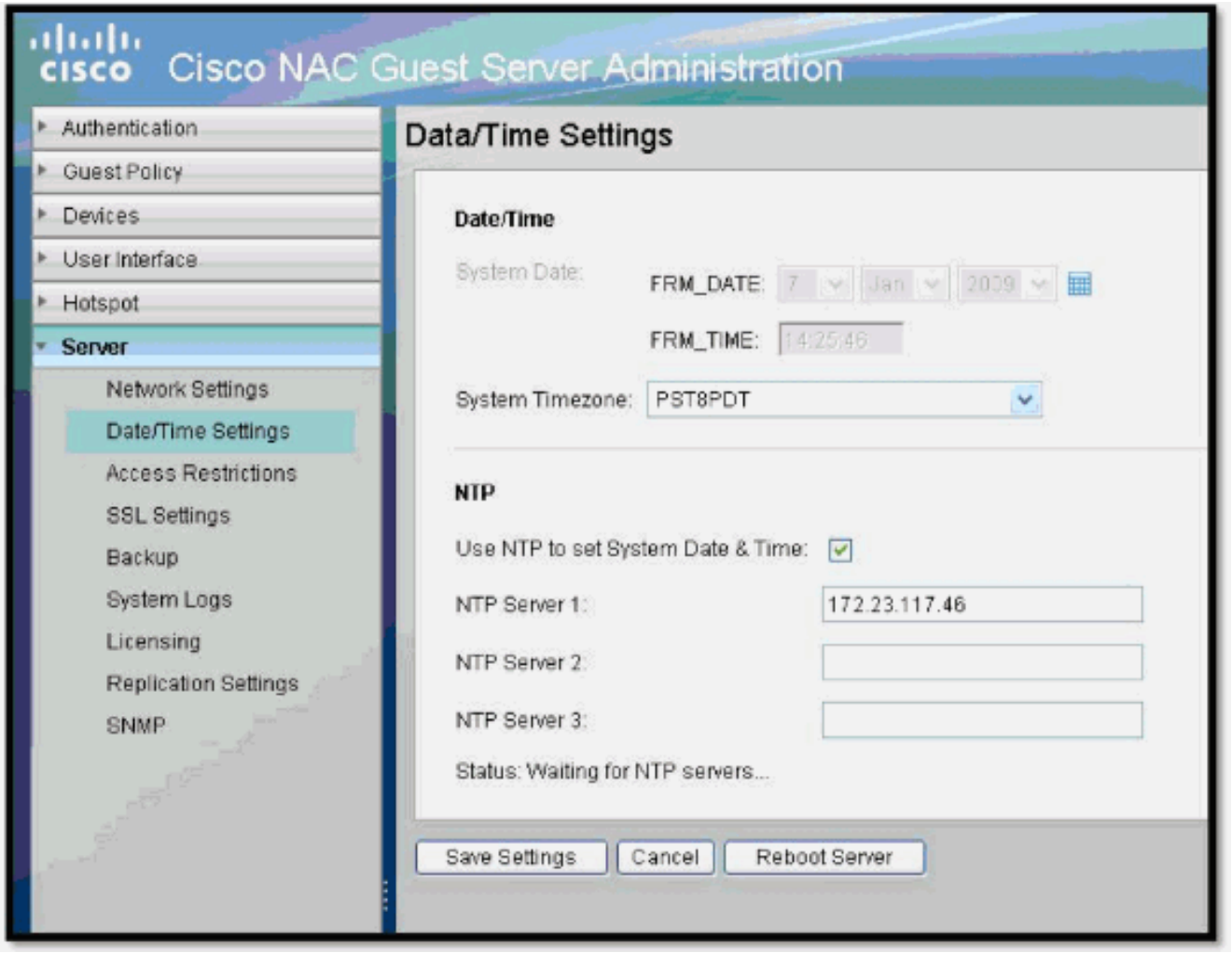
- Controlador de domínio — 172.23.117.46 (w2k3-server.cca.cisco.com)
- Server do convidado NAC — 172.23.117.42 (ngs.cca.cisco.com)
- Máquina do patrocinador — 172.23.117.45

Conclua estes passos:

1. Alcance a relação NG Admin. Do navegador, vá a **http://172.23.117.42/admin**



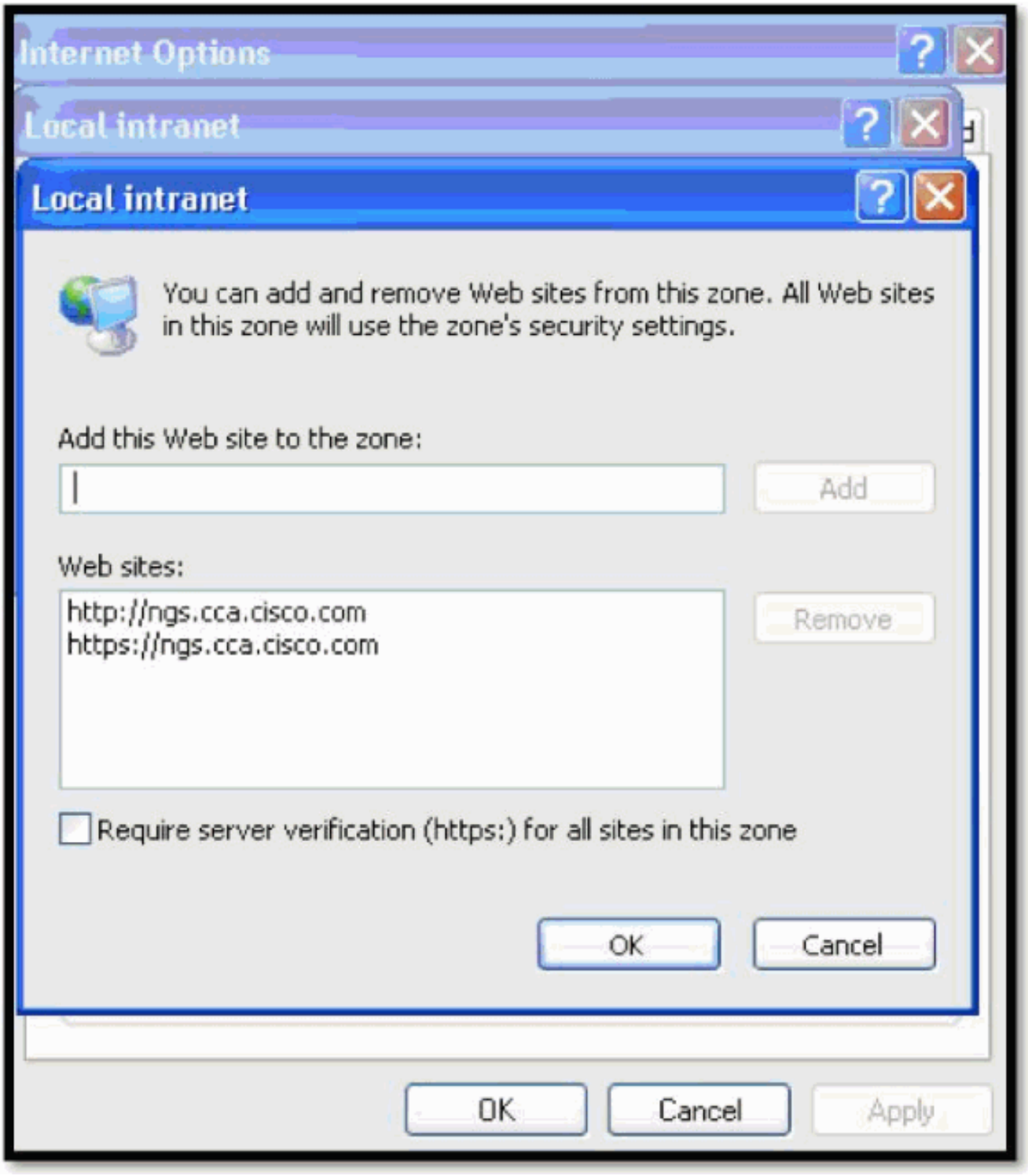

2. **Configuração de rede NG**Escolha o **server > as configurações de rede**.Hostname — ngsDomínio — cca.cisco.comDN principais — 172.23.117.46
3. **Instalação NTPNo server > na data/hora**, configurar o servidor de NTP a IP **172.23.117.46** DC.

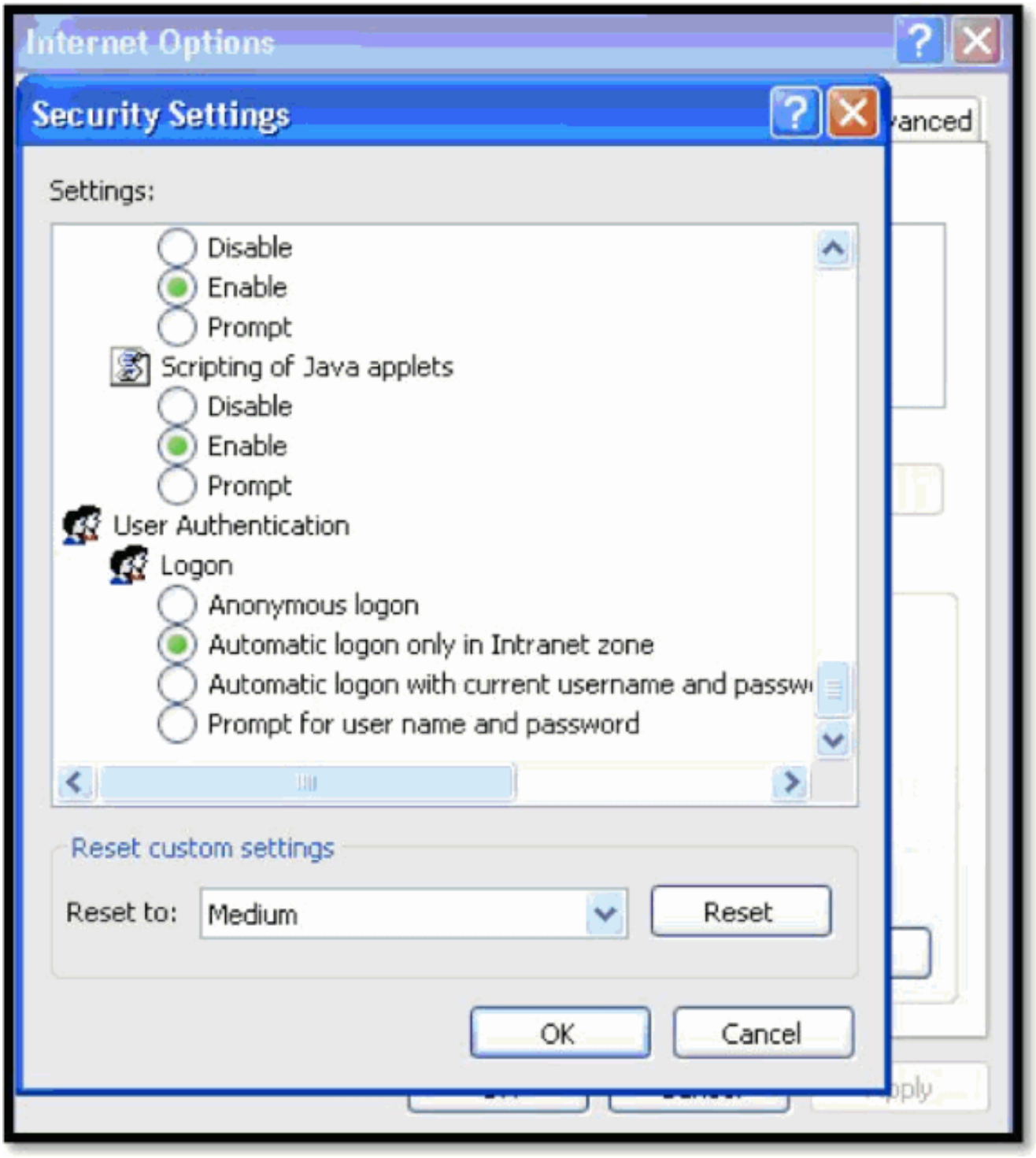



4. **Instalação AD SSO**Antes que você configure a seção SSO, certifique-se dos registros A e PTR existir para o server do controlador de domínio e do convidado NAC.Na seção de AuthServer > de AUTH SSO, configurar
isto:

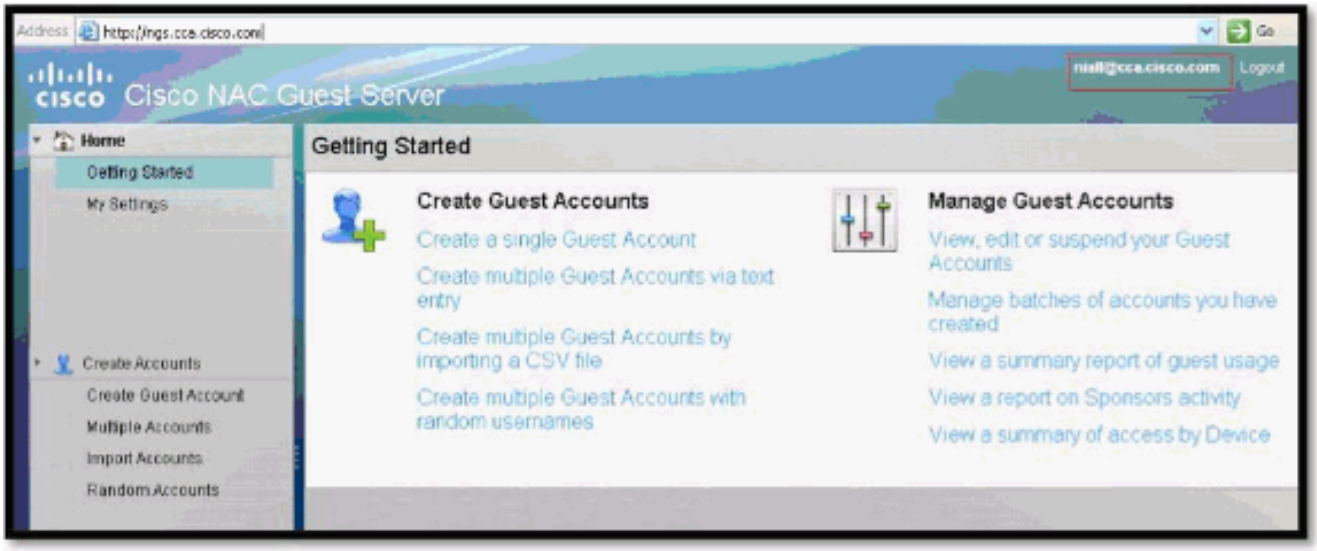

Se a configuração é bem sucedida, você deve ver um mensagem de sucesso.


5. **Valide a característica SSO**Da máquina do usuário, registre no domínio. Neste exemplo, esta máquina é parte do domínio cca. Somente o internet explorer é apoiado para a característica SSO. Você precisa de certificar-se de que o server do convidado NAC é parte de intranet local e o auto-início de uma sessão está girado **sobre**.**Nota:** Use o FQDN para o server do convidado a fim testar o SSO do navegador. Por exemplo, o endereço IP de Um ou Mais Servidores Cisco ICM NT não trabalha.Verifique os ajustes do navegador da Web:

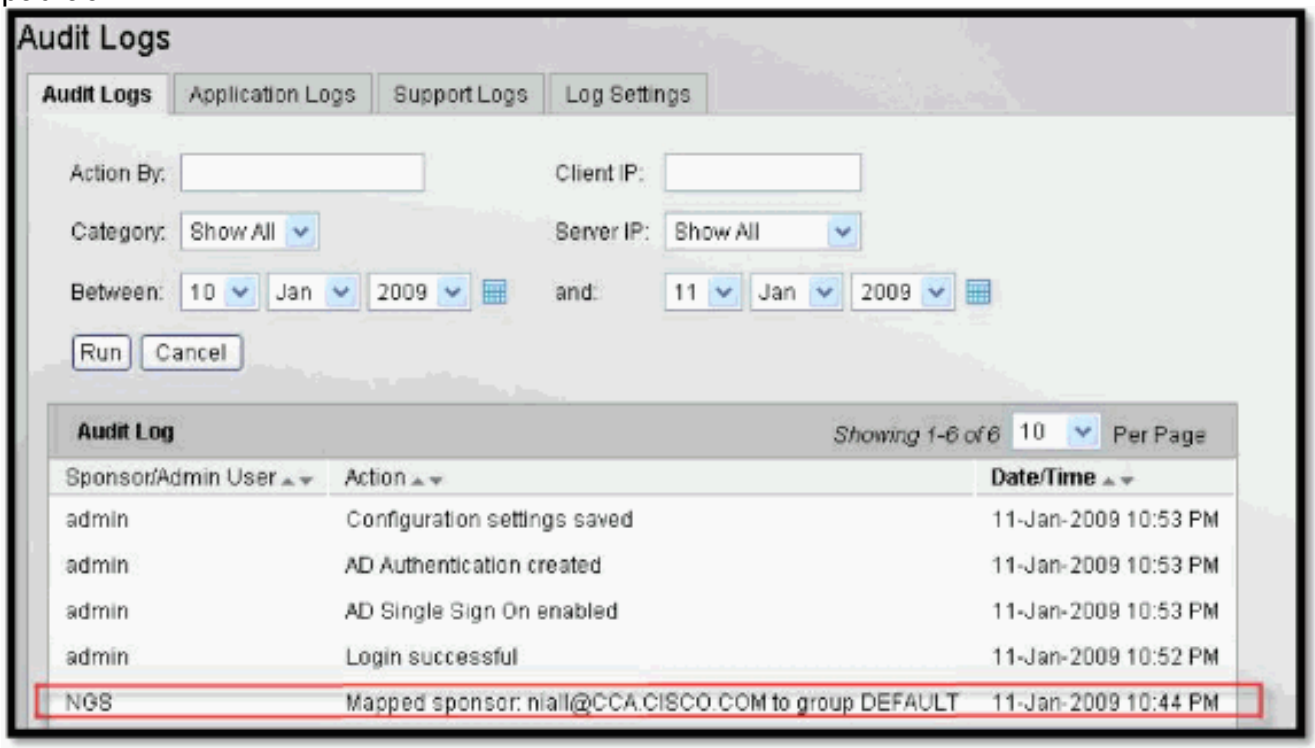

Internet Options
Local intranet
Local intranet
You can add and remove Web sites from this zone. All Web sites in this zone will use the zone's security settings.
Add this Web site to the zone:
Add
Web sites:
http://ngs.cca.cisco.com
https://ngs.cca.cisco.com
Remove
Require server verification (https:) for all sites in this zone
OK
Cancel
OK
Cancel
Apply



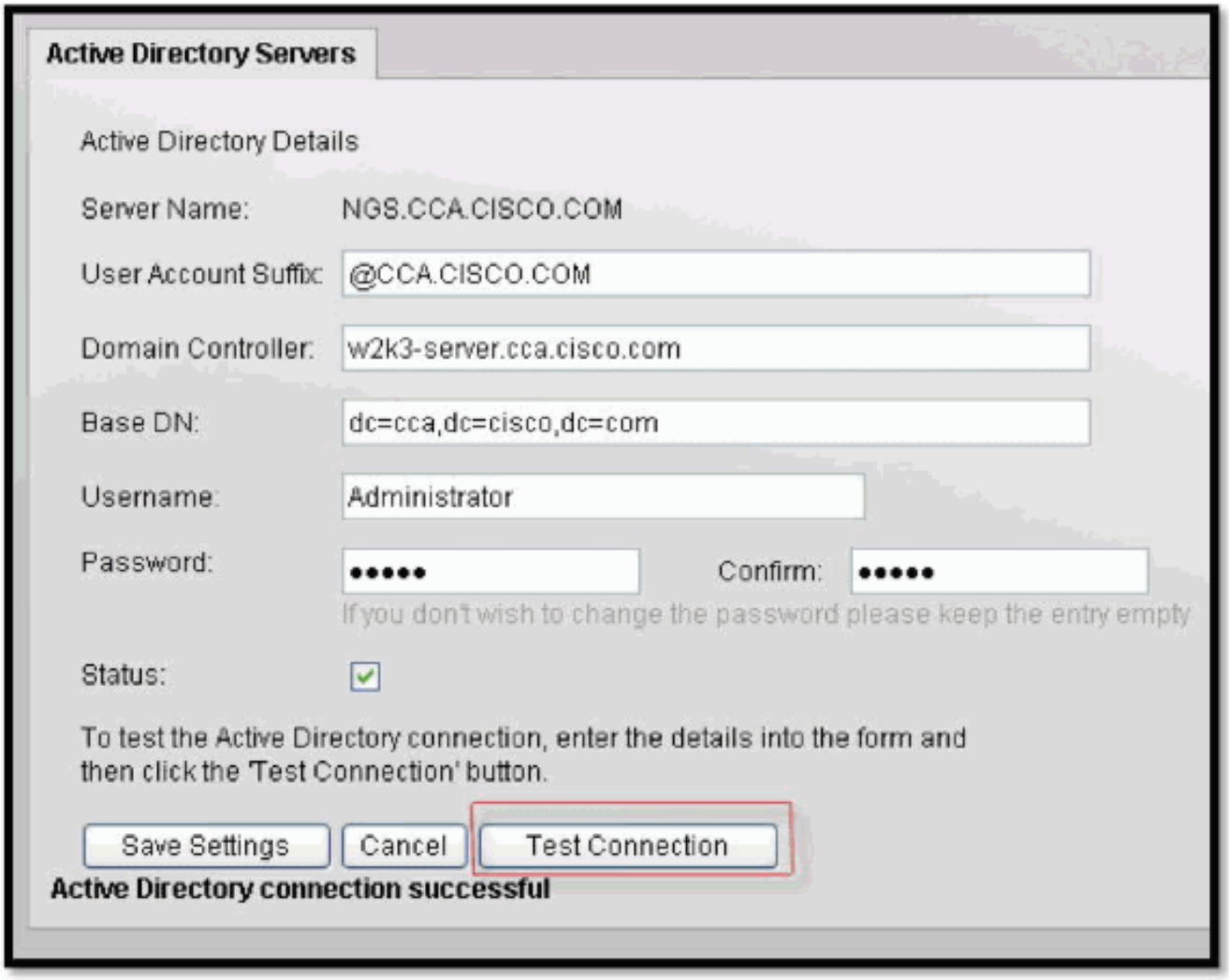

Do navegador da Web, vá a **http://ngs.cca.cisco.com**. Você deve automaticamente ser entrado aos ngs com as credenciais do domínio.**Nota:** O link **http://ngs.cca.cisco.com** trabalhará somente se você configurou o NAC no modo admin com as credenciais do usuário.



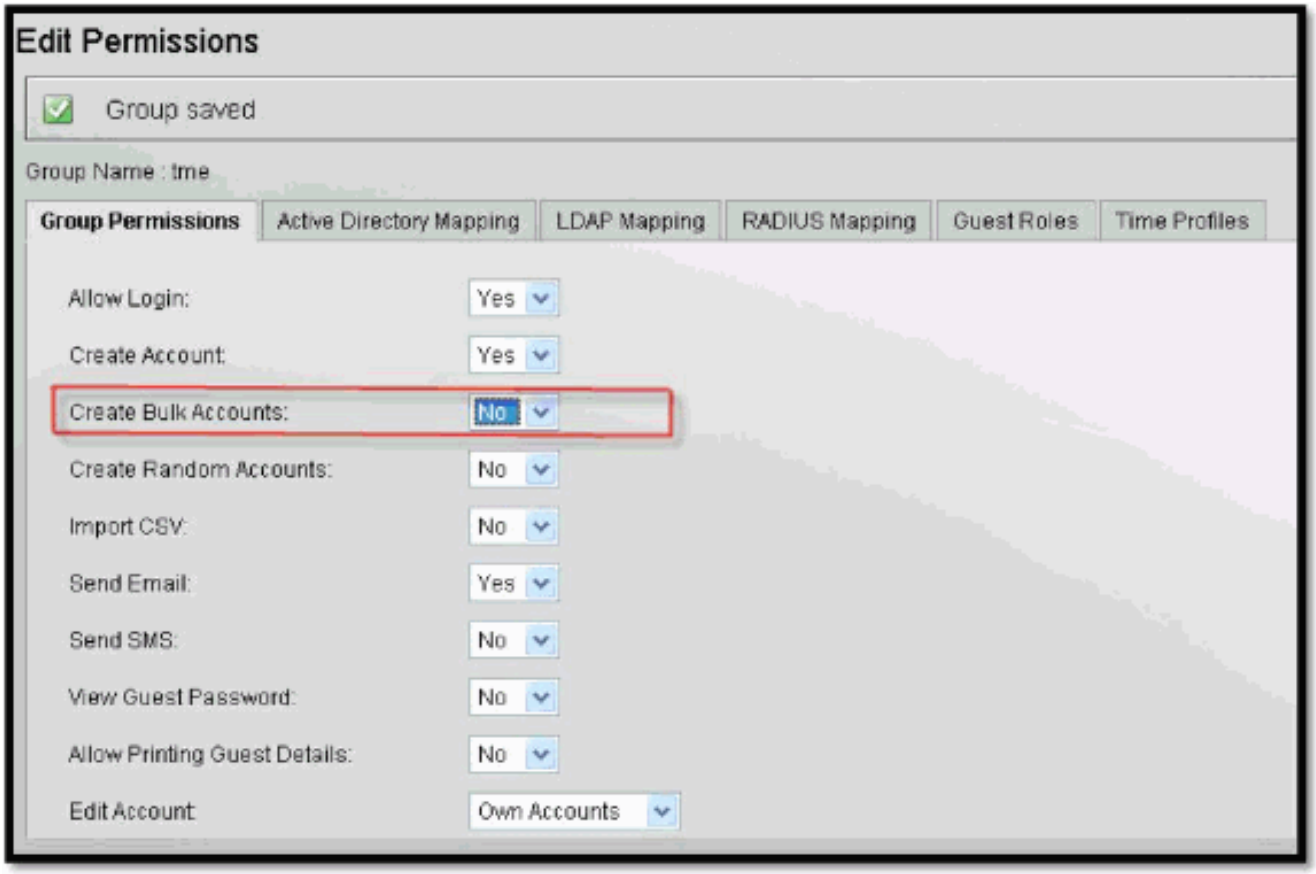

Sob os log de auditoria do server do convidado NAC, você pode ver o usuário Niall registrado no grupo
padrão:



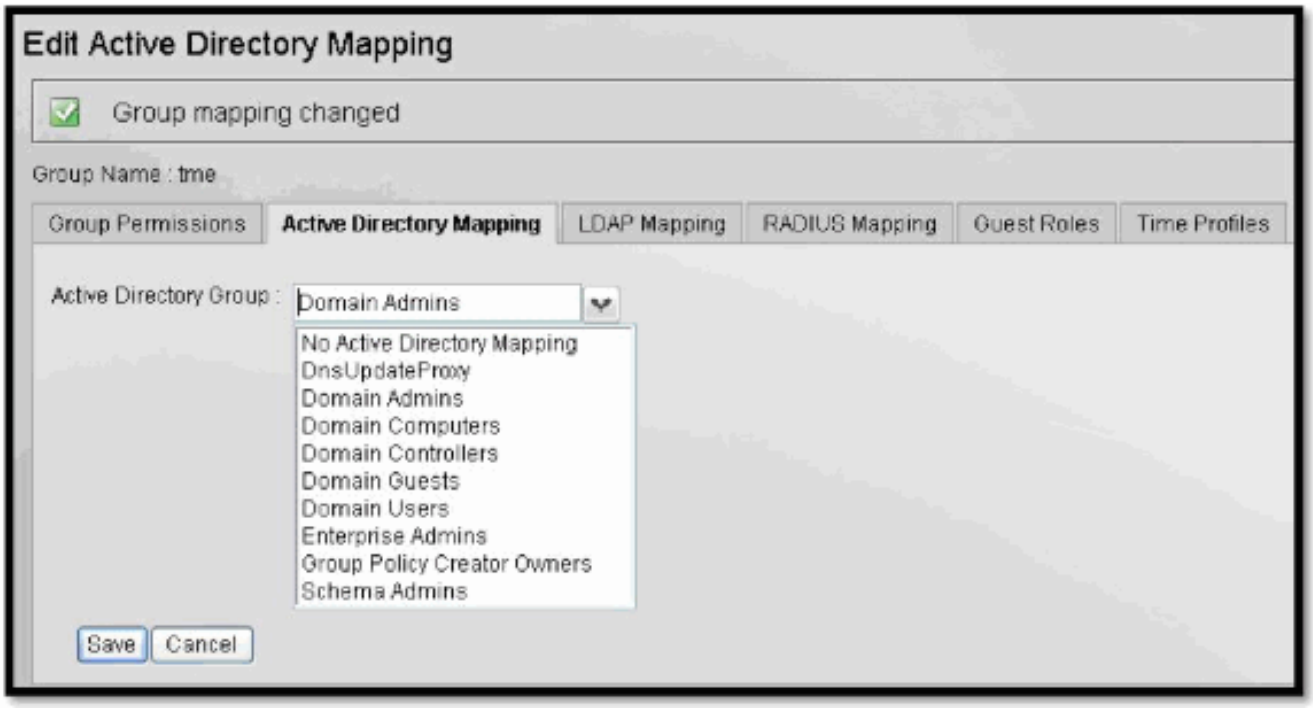

6. **Mapeamento do grupo de usuário com o AD SSO (opcional)***Nesta seção você aprenderá traçar o usuário SSO a um grupo específico a não ser o grupo padrão.*Para traçar o grupo de usuário com ADSSO, você precisa de configurar o servidor ative directory como o servidor de autenticação e de traçar então o grupo AD com grupo de usuário do patrocinador.Escolha **NG (as autenticações de http://172.23.117.42/admin) > patrocinam > servidores ative directory**. Adicionar um controlador de domínio
novo.




A opção de conexão de teste foi introduzida em NG 2.0 para a facilidade do Troubleshooting. Diz-lhe se você configurou o DC corretamente.**Configurar o grupo de usuário**Adicionar um nome do grupo do novo usuário **— tme**. Neste exemplo, você escolhe **NENHUM** a fim aumentar criação de conta. Esta maneira você sabe imediatamente se o usuário esteve colocado ao grupo do tme *ou ao* grupo padrão.




No mapeamento do diretório ativo, o usuário de teste Niall é já parte de domínio Admins.




## Verificar

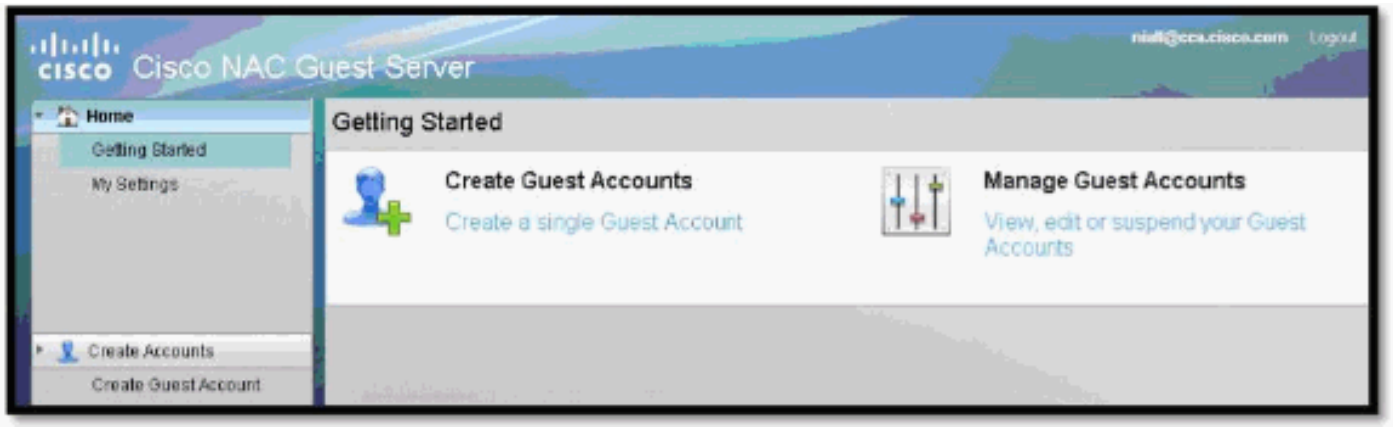
Use esta seção para confirmar se a sua configuração funciona corretamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

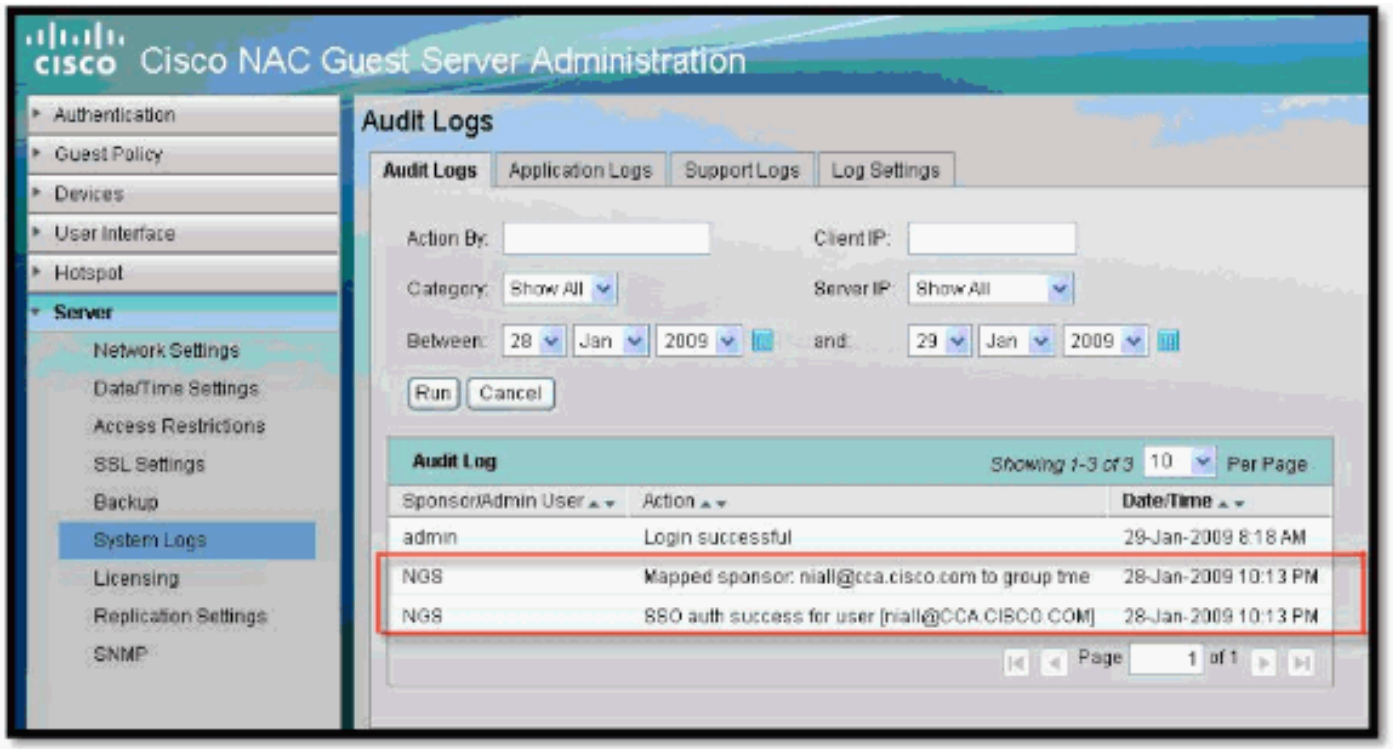
### Verifique o mapeamento do grupo de usuário ADSSO

A fim alcançar a máquina do patrocinador, abra um navegador novo e vá a http://ngs.cca.cisco.com.

Niall deve ser colocado no grupo do tme sem o acesso para aumentar criação de conta.




Se você olha os log de auditoria, você pode verificar que o patrocinador está colocado no papel correto.




## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Estes são Mensagens de Erro nos logs. Os erros do Kerberos conduzem a um destes erros:

- `O formato do domínio incorreto/controlador de domínio deve ser um FQDN, não um endereço IP de Um ou Mais Servidores Cisco ICM NT` O domínio não foi incorporado a um formato correto

(deve ser do formulário CCA.CISCO.COM).

- `O hostname deve ser um FQDN, não um endereço IP de Um ou Mais Servidores Cisco ICM NT` O hostname do server do convidado NAC não pode ser um endereço IP de Um ou Mais Servidores Cisco ICM NT que deve ser um nome de domínio totalmente qualificado por exemplo nac.cca.cisco.com.
- `Não pode determinar o endereço IP de Um ou Mais Servidores Cisco ICM NT para o controlador de domínio` Há uma edição da Configuração de DNS.
- `Não pode obter ao DNS um registro para o controlador de domínio` Há uma edição da Configuração de DNS.
- `Não pode obter o registro DNS A para o hostname` Há uma edição da Configuração de DNS.
- `Não pode obter o registro PTR DNS para o endereço IP de Um ou Mais Servidores Cisco ICM NT do controlador de domínio` Há uma edição da Configuração de DNS.
- `Não pode obter o registro PTR DNS para o endereço IP de Um ou Mais Servidores Cisco ICM NT do hostname` Há uma edição da Configuração de DNS.
- `Não criam o computador esclareça este server no controlador de domínio. Veja o log do aplicativo para detalhes` . Veja o log do aplicativo para ver os detalhes completos do erro.
- `Nome de usuário inválido/senha` O nome de usuário de administrador/senha está incorretos.
- `O domínio inválido ou não pode resolver o endereço de rede para o DC` Há um problema de DNS no server AD.
- `O tempo do controlador de domínio não combina o tempo deste server` Assegure o fósforo do tempo de servidor, ele é-o recomendado o uso NTP sincronizar o tempo de servidor.
- `O DC não pode determinar o hostname para o server do convidado pela consulta reversa. Pode haver uma edição com seu confiugration DNS.` Há uma edição da Configuração de DNS em seu server AD.

## Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems