

NAC: Configure el LDAP sobre el SSL en el Access Manager limpio (el CAM)

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Configurar](#)

[Pasos para configurar el LDAP sobre el SSL en el CAM](#)

[Verificación](#)

[Troubleshooting](#)

[Información Relacionada](#)

[Introducción](#)

Este documento describe cómo configurar el Lightweight Directory Access Protocol (LDAP) sobre el SSL en el Access Manager limpio (CAM).

[prerrequisitos](#)

[Requisitos](#)

Esta configuración es aplicable a la versión 3.5 y posterior CAM.

[Componentes Utilizados](#)

La información en este documento se basa en la versión 4.1 limpia del Access Manager.

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.

Note: Use la [Command Lookup Tool \(clientes registrados solamente\)](#) para obtener más información sobre los comandos usados en esta sección.

Pasos para configurar el LDAP sobre el SSL en el CAM

Complete estos pasos:

1. Obtenga el certificado raíz del CA untrusted que ha publicado el certificado al controlador de dominio y colóquelo en su escritorio. Elija el **administrador > el certificado CAM > SSL**, y entonces hojee y cargue certificado raíz CA como **confianza CA no estándar**.

The screenshot shows the 'Administration > Clean Access Manager' interface. At the top, there are navigation tabs: 'Network & Failover', 'System Time', 'SSL Certificate', 'System Upgrade', 'Licensing', and 'Support Logs'. Below the tabs, there is a 'Choose an action:' dropdown menu set to 'Import Certificate'. Underneath, the 'Certificate File:' field contains 'C:\Documents and Settings\Adminir' with a 'Browse...' button next to it. The 'File Type' dropdown is set to '^Trust Non-Standard CA', and there is an 'Upload' button. Below this, the 'Uploaded Certificate List:' section shows three entries: 'Private Key' with a 'View' button; 'CA-Signed Certificate' with 'View' and 'Details' buttons; and 'Root/Intermediate CA' with 'View', 'Details', and 'Delete' buttons. At the bottom of the list is a 'Verify and Install Uploaded Certificates' button. A small note at the bottom left states: '(+ "Trust Non-Standard CA" is for SSL communication between the Clean Access Manager and some authentication servers, e.g. LDAP Server.)'

El tecleo **verifica** y instala certificado raíz CA.

2. Configure al servidor LDAP en el CAM. Elija **User Management (Administración de usuario) > los servidores de autenticación** y elija **nuevo**. Elija el **LDAP** como el tipo de autenticación. Elija **ldaps://ip.address:636** como el servidor URL. Elija el **SSL** como el tipo de la Seguridad. ¡Elija la **manija (siga)!** como la remisión. Esta opción se fija para el entorno del dominio de la división, por ejemplo, la raíz y los Dominios hijo. Requieren al usuario y la contraseña del privilegio Admin atar con éxito el CAM (cliente del Idap) al servidor LDAP.

User Management > Auth Servers

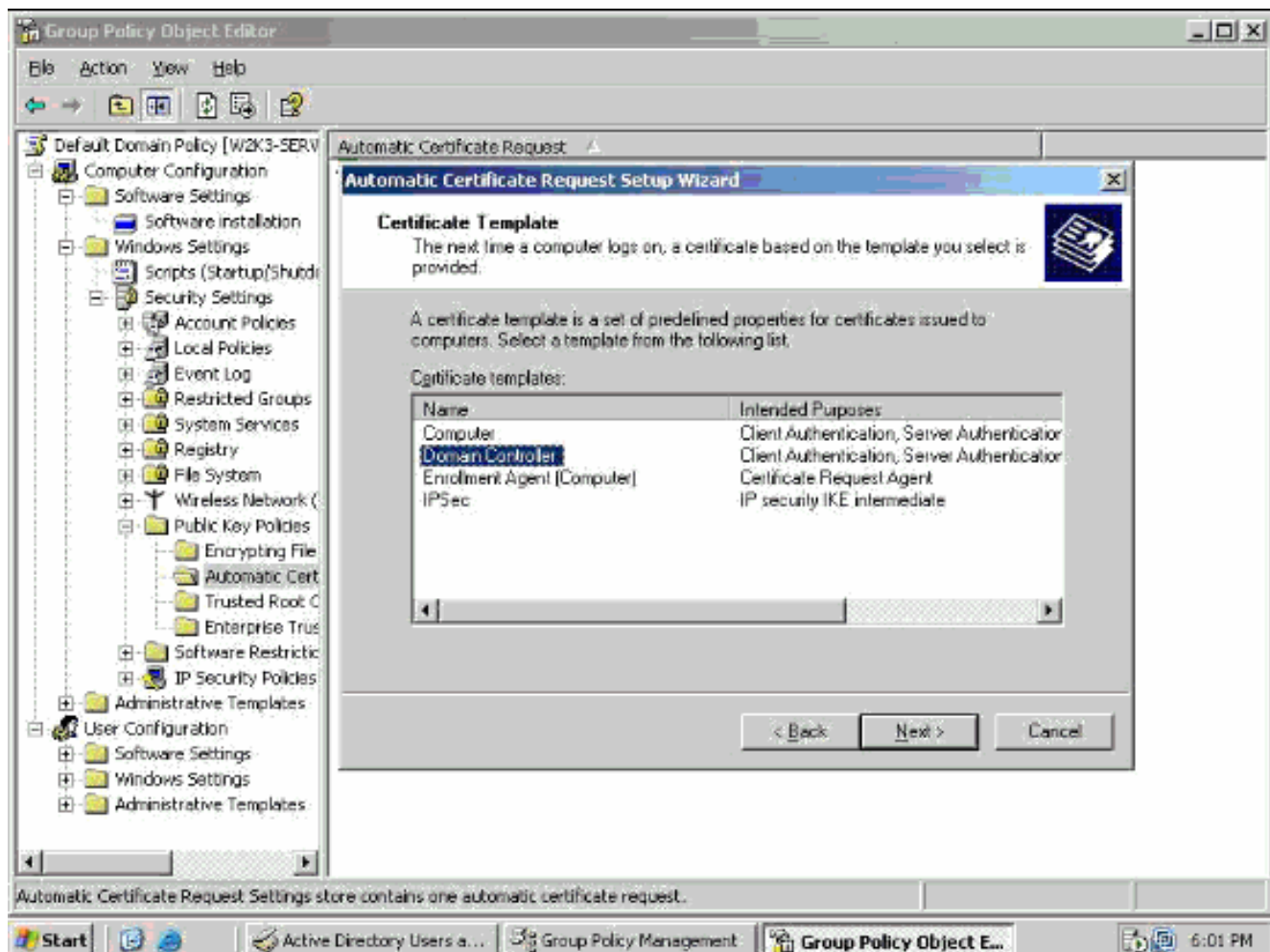
Auth Servers | Lookup Servers | Mapping Rules | Auth Test | Accounting

List · Edit

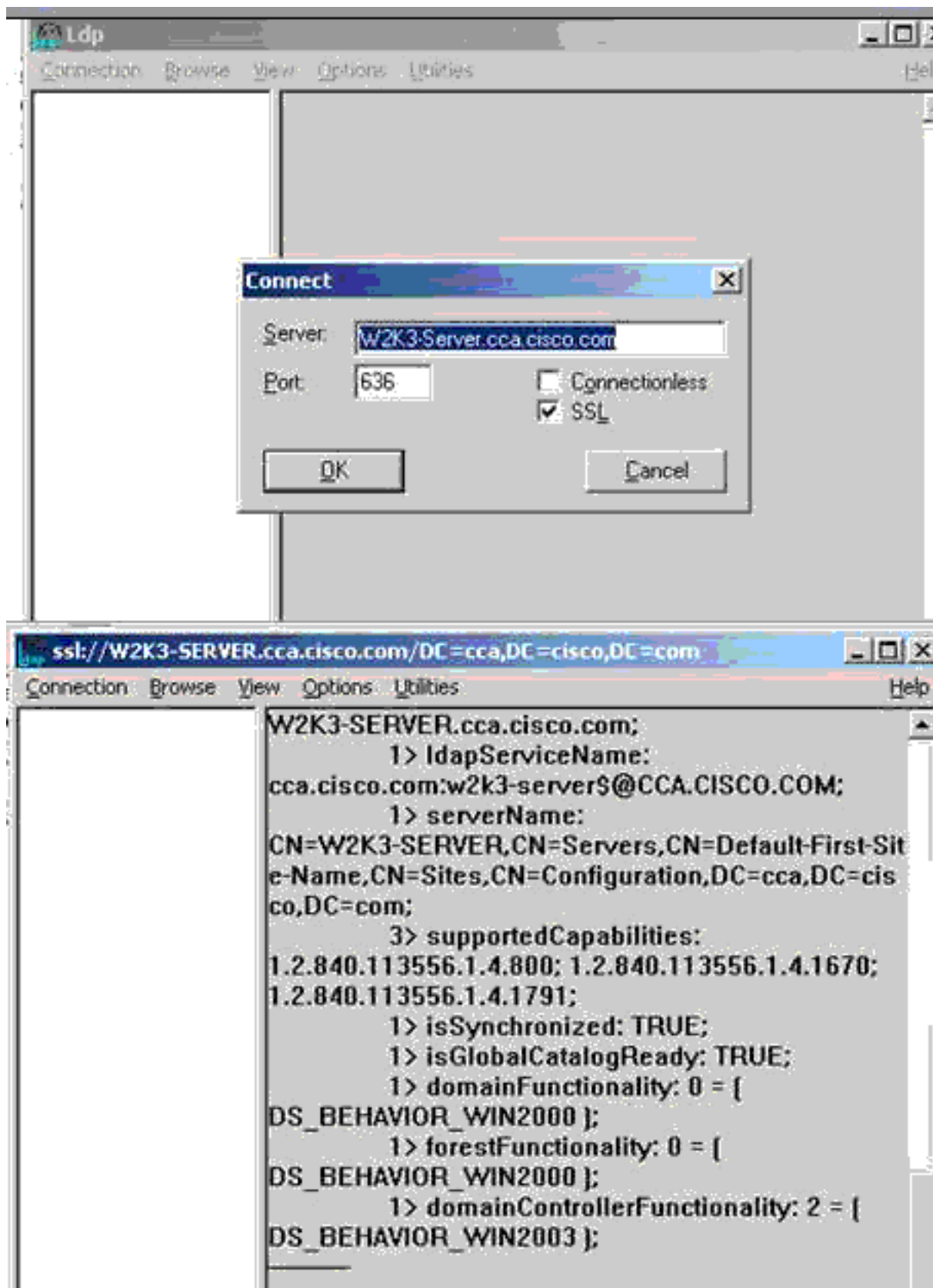
Authentication Type	LDAP	Provider Name	RootHdapS
Server URL	ldaps://192.168.137.9:63	Server version	Auto
Search(Admin) Full DN	CN=root123, CN=users,	Search(Admin) Password	●●●●●●●●
Search Base Context	DC=CCA, DC=CISCO, D	Search Filter	sAMAccountName=\$us
Referral	Handle (Follow)	DerefLink	ON
DerefAlias	Always	Security Type	SSL
Default Role	Allow All		
Description			

Update Server Cancel

- Obtenga el certificado en el controlador de dominio (DC). Cuando usted pide un certificado para DC, asegúrese de poner el CN como Nombre de dominio totalmente calificado (FQDN) del Active Directory. El certificado LDAPS está situado en el almacén del certificado personal de la computadora local. Refiérase a [cómo habilitar el LDAP sobre el SSL con las autoridades de certificación de tercera persona](#) para más información.
- Configure el controlador de dominio para el SSL. En su DC, elija el **comienzo > todos los programas > Administrative Tools > los usuarios de directorio activo y computadora**. En la ventana de los usuarios de directorio activo y computadora, haga clic con el botón derecho del ratón en su Domain Name y elija las **propiedades**. En el cuadro de diálogo Propiedades del dominio, elija la lengüeta de la **directiva del grupo**. Elija la directiva del **grupo de políticas del Default Domain** y después haga clic **editar**. Elija la **configuración de Computadora > las configuraciones de Windows**. Elija los **ajustes de seguridad** y después elija las **directivas de la clave pública**. Elija las **configuraciones automáticas del pedido de certificado**. Utilice al Asistente para agregar una directiva para los controladores de dominio como en este ejemplo:



5. Verifique el controlador de dominio para el LDAP sobre el SSL. En su DC, elija el **Start (Inicio) > Run (Ejecutar)** y teclee **ldp.exe**. Del menú de conexión, haga clic **Connect and** completan los valores para el servidor y el puerto. Esto verifica que el LDAP sobre el SSL esté configurado correctamente en



DC.

6. Elija User Management (Administración de usuario) > los servidores de autenticación > lengüeta de la prueba AUTH para verificar la configuración CAM LDAPS.

User Management > Auth Servers

Auth Servers Lookup Server Mapping Rules **Auth Test** Accounting

Provider Root-IdapS ▾

User Name child1

Password

Managed Network VLAN
(optional)

Result: Successful
Role: Unauthenticated Role

[Verificación](#)

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

[Troubleshooting](#)

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

[Información Relacionada](#)

- [Página de soporte del dispositivo NAC de Cisco](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)