

# Verifique el LDAP sobre el certificado SSL/TLS (LDAPS) y CA usando Ldp.exe

## Contenido

[Introducción](#)

[Cómo verificar](#)

[Antes de que usted comience](#)

[Pasos de verificación](#)

[Resultado de la prueba](#)

[Documentos relacionados](#)

## Introducción

Cuando usted crea un objeto de la autenticación en un centro de administración de FireSIGHT para el Active Directory LDAP sobre SSL/TLS (LDAPS), puede a veces ser necesario probar el CERT CA y la conexión SSL/TLS, y verifica si el objeto de la autenticación falla en la prueba. Este documento explica cómo funcionar con la prueba usando Microsoft Ldp.exe.

## Cómo verificar

### Antes de que usted comience

Ábrase una sesión a una computadora local de Microsoft Windows con una cuenta de usuario que tenga privilegio administrativo local de realizar los pasos en este documento.

Nota: Si usted no tiene actualmente `ldp.exe` disponible en su sistema, usted debe primero descargar las **herramientas de WindowsSupport**. **Esto** está disponible en el sitio Web de Microsoft. Una vez que usted descarga y instala las **herramientas de WindowsSupport**,  **siga los pasos abajo**.

Realice esta prueba en un ordenador de las ventanas Locales que no ha sido un miembro de un dominio, pues confiaría en la raíz o la empresa CA si se unió a un dominio. Si una computadora local está no más en un dominio, el certificado CA de la raíz o de la empresa se debe quitar del almacén de los **Trusted Root Certification Authority de la computadora local** antes de realizar esta prueba.

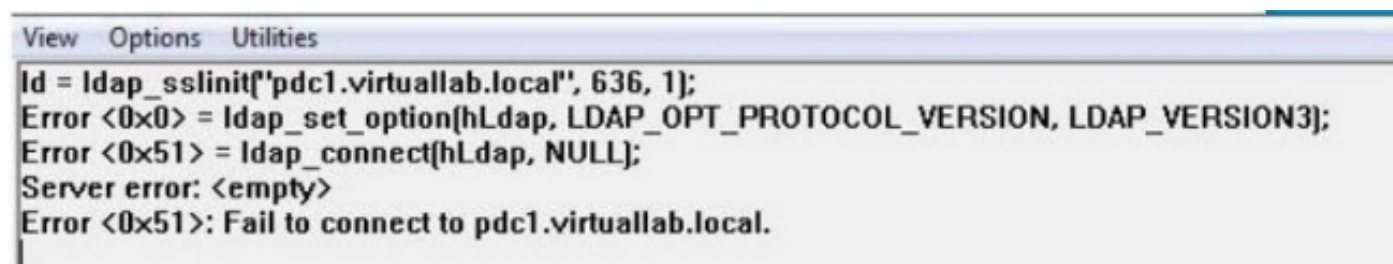
## Pasos de verificación

**Paso 1:** Comience la aplicación `ldp.exe`. Vaya al Startmenu y haga clic el funcionamiento. Pulse `ldp.exe` and `go1pean` e1 botón OK.

**Paso 2:** Conecte con el regulador del dominio que usa el regulador FQDN del dominio. Para conectar, vaya a la **conexión > conectan** y ingresan el FQDN del regulador del dominio. Después seleccione el **SSL**, especifique el puerto **636** como se muestra abajo y haga clic la **AUTORIZACIÓN**.

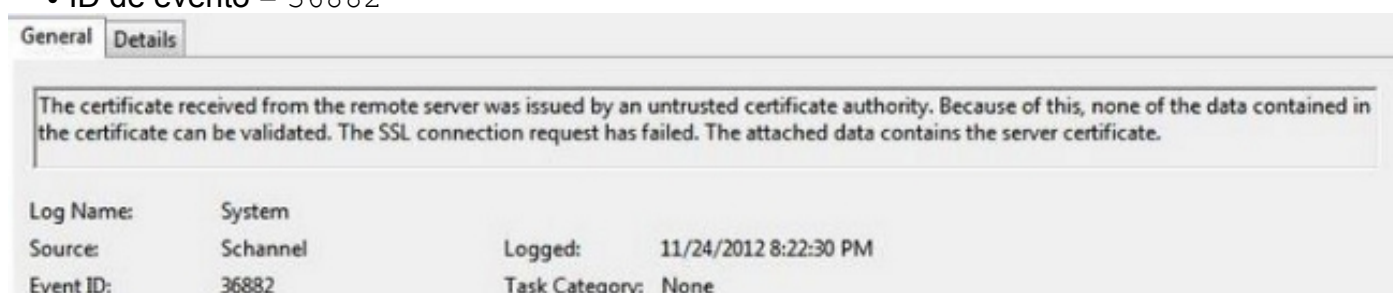


**Paso 3:** Si la raíz o la empresa CA no se confía en una computadora local, el resultado mira como abajo. El mensaje de error indica que el certificado recibido del servidor remoto fue publicado por una autoridad de certificación untrusted.



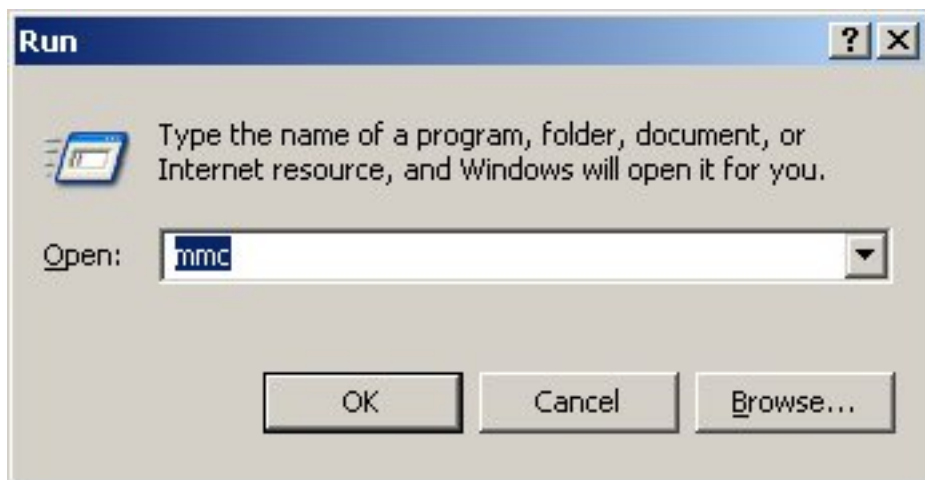
**Paso 4:** La filtración de los mensajes del evento en el ordenador de las ventanas Locales con los criterios siguientes proporciona a un resultado específico:

- Origen del evento = Schannel
- ID de evento = 36882



**Paso 5:** Importe el certificado CA al almacén de certificados del ordenador de las ventanas Locales.

i. Ejecute Microsoft Management Console (MMC). Vaya al **menú Inicio** y haga clic el **funcionamiento**. Pulse el **mmc** y golpee el **botón OK**.

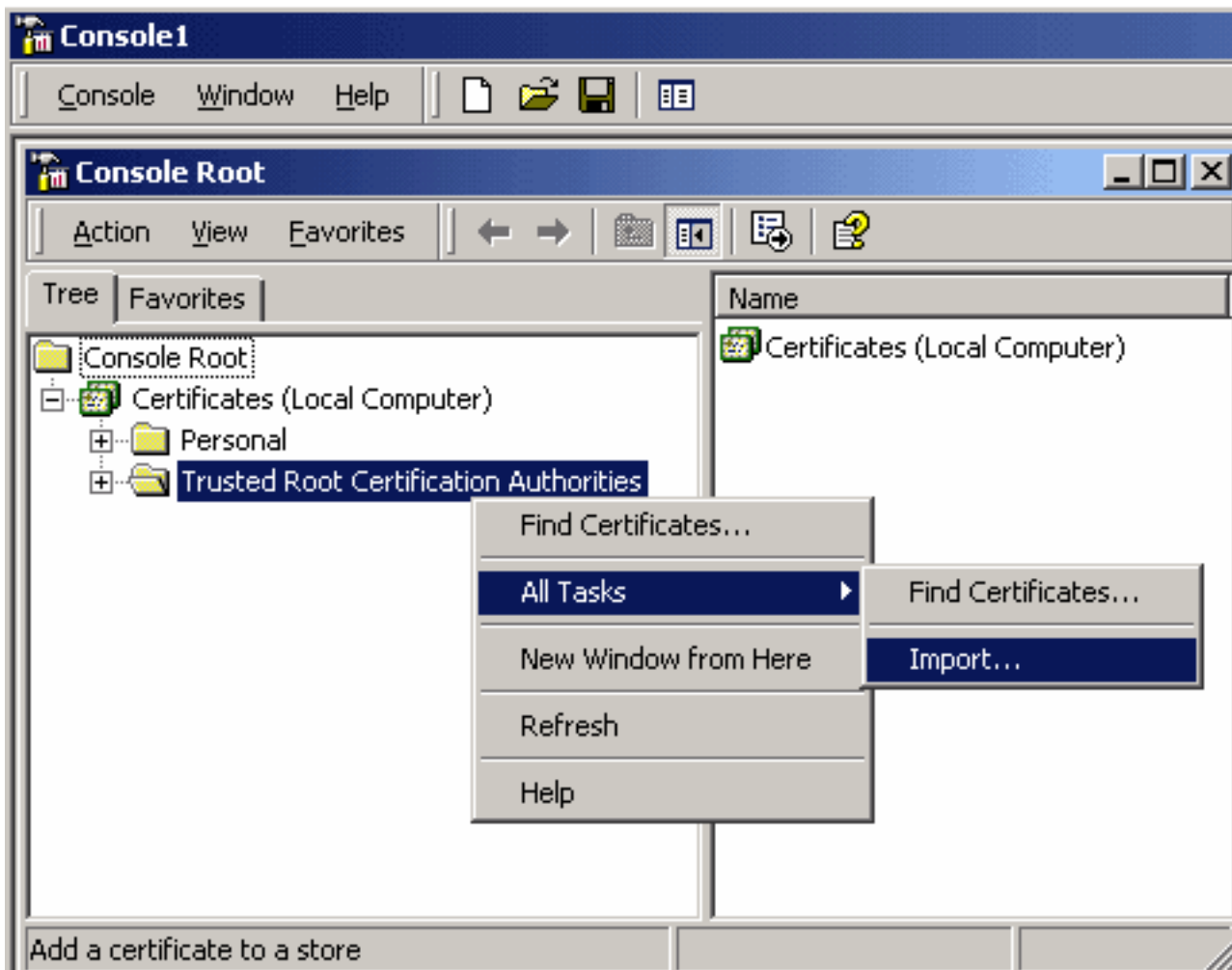


ii. Agregue el certificado de la computadora local broche-en. Navegue a las opciones siguientes en el **menú de archivo**:

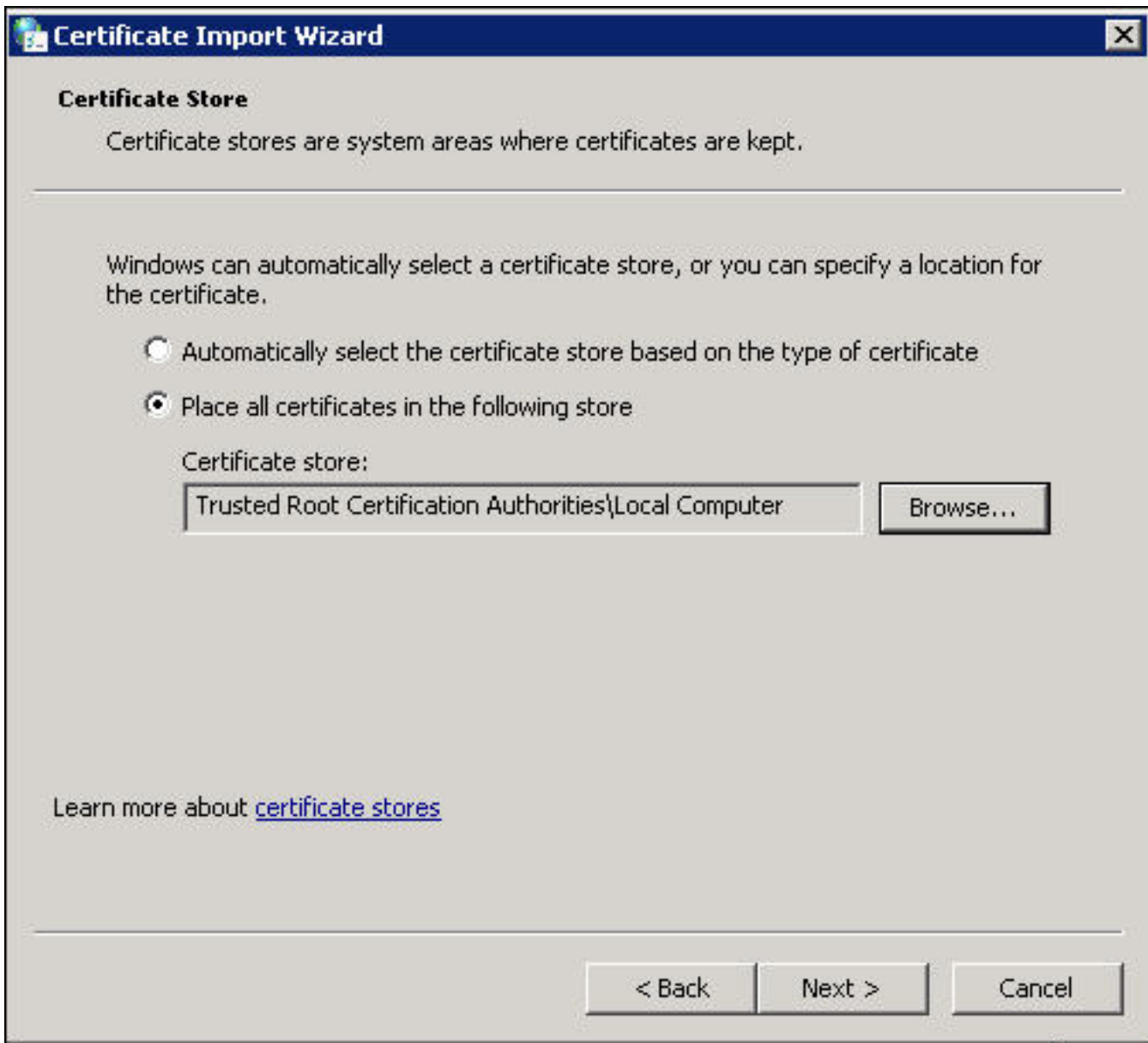
**Agregue/telecontrol Broche-en > los Certificados > agregan > eligen la "cuenta del ordenador" > computadora local: (el ordenador que esta consola está funcionando con encendido) > final > ACEPTABLE.**

iii. Importe el certificado CA.

**La Raíz de la consola > certifica (computadora local) > los Trusted Root Certification Authority > los Certificados > clic derecho > todas las tareas > importación.**



- Haga clic **después** y hojee al archivo de certificado codificado Base64 del certificado X.509 (\*.cer, \*.crt) CA. Entonces seleccione el fichero.
- Haga clic **abierto > después** y el lugar selecto **todos los Certificados** en el almacén siguiente: **Trusted Root Certification Authority**.
- Tecleo **después > final** para importar el fichero.



iv. Confirme que el CA está enumerado con la otra Raíz confiable CAs.

**Paso 6:** Siga el paso 1 y 2 para conectar con el servidor LDAP del ANUNCIO sobre el SSL. Si el certificado CA está correcto, las primeras 10 líneas en el panel derecho de `ldp.exe` deben estar como abajo:

```
ld = ldap_sslinit("pdc1.virtuallab.local", 636, 1);
Error <0x0> = ldap_set_option(hLdap, LDAP_OPT_PROTOCOL_VERSION, LDAP_VERSION3);
Error <0x0> = ldap_connect(hLdap, NULL);
Error <0x0> = ldap_get_option(hLdap,LDAP_OPT_SSL,(void*)&lv);
Host supports SSL, SSL cipher strength = 128 bits
Established connection to pdc1.virtuallab.local.
Retrieving base DSA information...
Result <0>: [null]
Matched DN's:
Getting 1 entries:
>> Dn:
```

**Resultado de la prueba**

Si un certificado y una conexión LDAP pasan esta prueba, usted puede configurar con éxito el objeto de la autenticación para el LDAP sobre el SSL/TLS. Sin embargo, si el fall de la prueba debido a la configuración de servidor LDAP o al problema del certificado, resuelve por favor el problema en el servidor del ANUNCIO o descarga el certificado CA correcto antes de que usted configure el objeto de la autenticación en el centro de administración de FireSIGHT.

## Documentos relacionados

- [Identifique los atributos de objeto del Active Directory LDAP para la configuración del objeto de la autenticación](#)
- [Configuración del objeto de la autenticación LDAP en el sistema de FireSIGHT](#)