Configuración de LDAP en el dispositivo virtual Intersight

Contenido

Introducción

Este documento describe el proceso para configurar la autenticación LDAP en un dispositivo virtual privado (PVA) Intersight.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Protocolo ligero de acceso a directorios (LDAP).
- Dispositivo virtual privado Intersight.
- Servidor de nombre de dominio (DNS).

Componentes Utilizados

- Dispositivo virtual privado Intersight.
- Microsoft Active Directory.
- Servidor DNS.

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

LDAP es un protocolo utilizado para acceder a los recursos desde un directorio a través de la red. Estos directorios almacenan información sobre usuarios, organizaciones y recursos. LDAP proporciona una forma estándar de acceder y administrar esa información que se puede utilizar para los procesos de autenticación y autorización.

Este documento muestra el proceso de configuración para agregar la autenticación remota a través de LDAP a un PVA de Intersight.

Configurar

Configuración de los parámetros básicos de LDAP

1. Vaya a System > Settings > AUTHENTICATION > LDAP/AD.
2. Haga clic en Configure LDAP.
3. Introduzca la información necesaria. Tenga en cuenta las siguientes recomendaciones:
    1. El nombre se establece arbitrariamente y no afecta a la configuración.
    2. Para BaseDN y BindDN, copie y pegue los valores correspondientes de la configuración de Active Directory (AD).
    3. El valor predeterminado para Atributo de grupo es miembro.

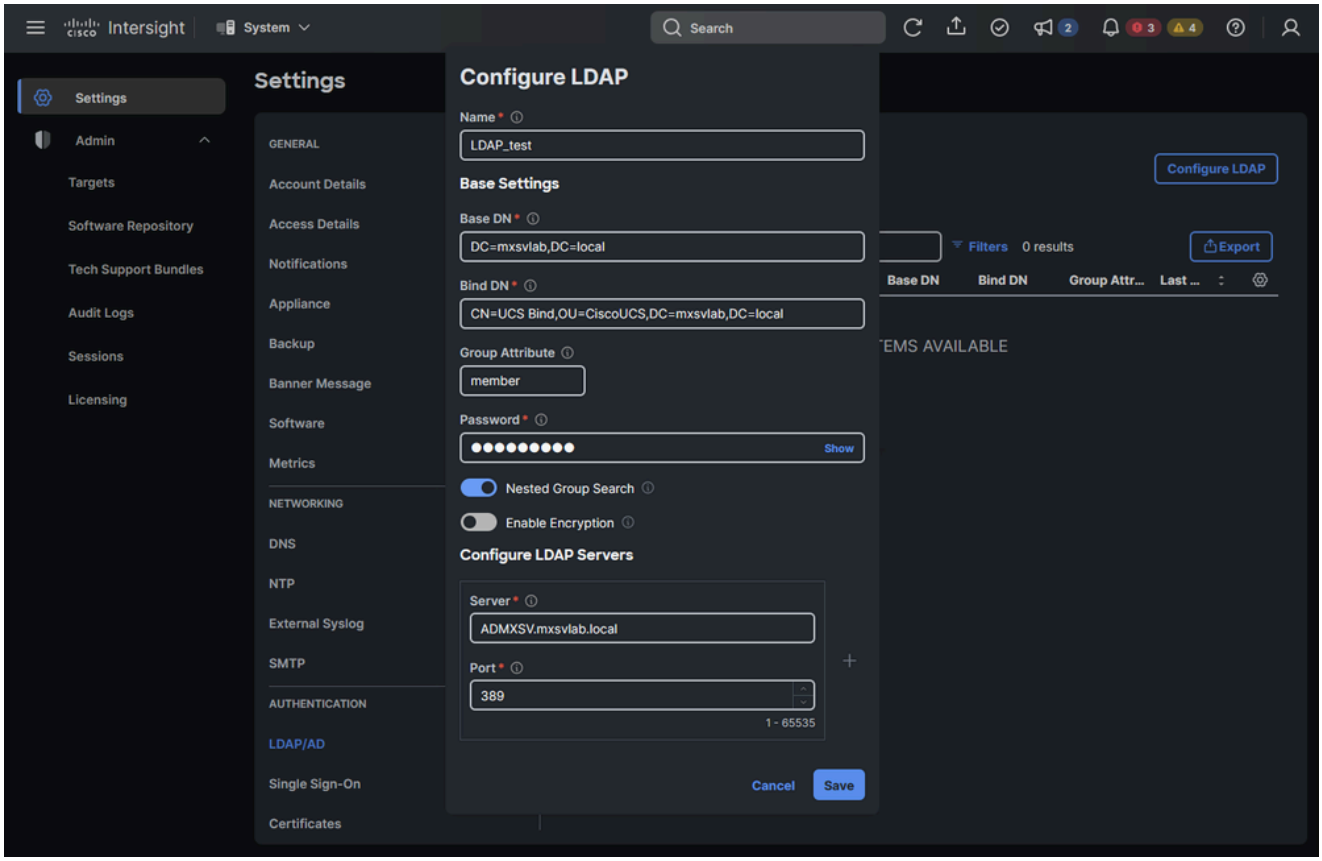
    > Nota: En otras herramientas de administración de UCS, como UCSM o CIMC, el atributo Group se establece en memberOf. En Intersight se recomienda dejarlo como miembro.

    4. Introduzca la contraseña para este proveedor LDAP.
    5. Habilite la opción Búsqueda de grupos anidados si desea permitir una búsqueda recursiva en su AD para todos los grupos desde la raíz y sus grupos contenidos.
    6. Deje Enable Encryption deshabilitado para una configuración LDAP normal. Si se necesita un LDAP seguro, actívelo y asegúrese de revisar la sección Configuración de LDAP seguro (LDAP seguro) para los pasos complementarios que debe configurar.

4. Agregue la configuración para un servidor LDAP:
    1. En Servidor introduzca la IP o el nombre de host del servidor LDAP.

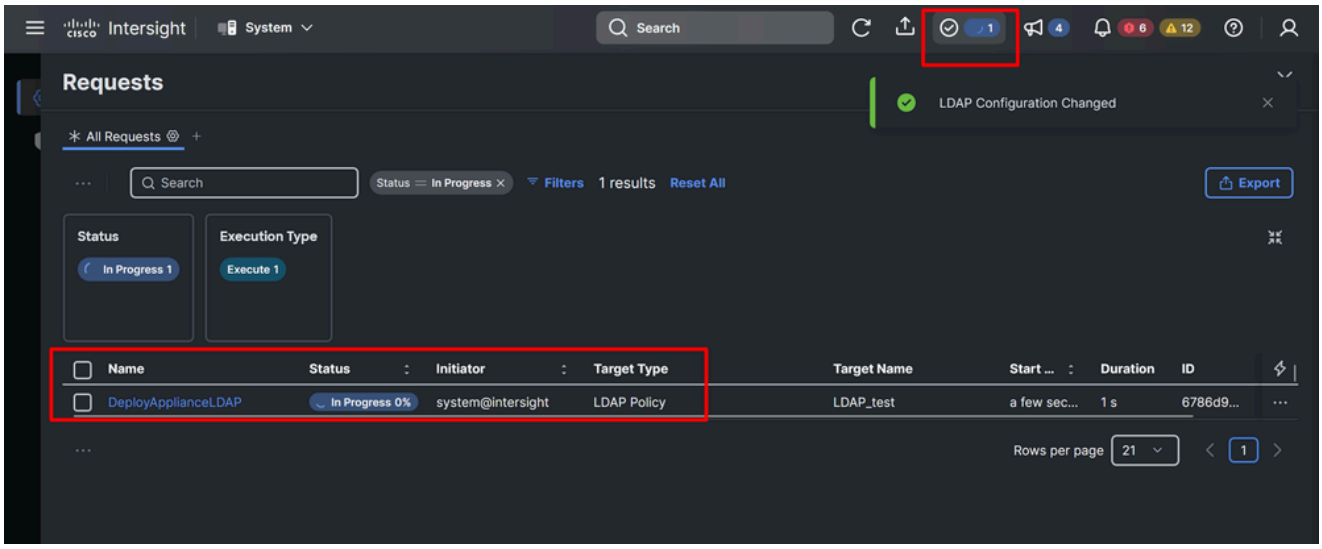
> ⚠ Precaución: Si se utiliza el nombre de host, asegúrese de que el DNS pueda asignar ese nombre de host correctamente.

    2. El puerto predeterminado y recomendado para LDAP es 389 .
5. Click Save.



Ejemplo de Configuración para los Parámetros Básicos de LDAP

6. Supervise el flujo de trabajo DeployApplianceLDAP desde Requests en la barra superior.



Solicitud de implementación

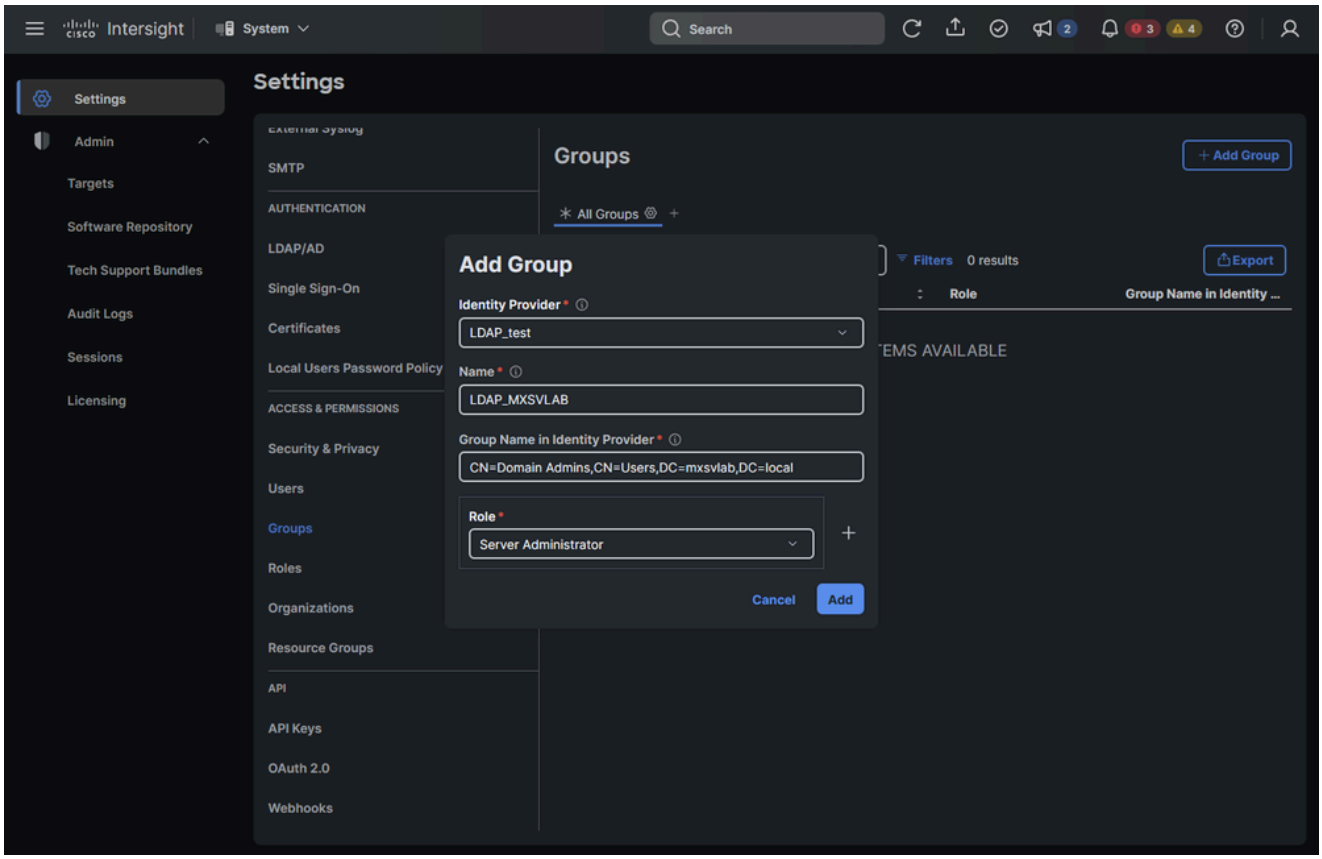
Configurar usuarios y grupos

Una vez finalizado el flujo de trabajo DeployApplianceLDAP, puede configurar Groups o Users individuales.

Si decide utilizar Grupos, la autorización se proporciona a todos los usuarios que pertenecen a ese Grupo. Si utiliza usuarios individuales, deberá agregar cada usuario con su propia función de autorización.

Configurar grupos

1. Vaya a Sistema > Configuración > ACCESO y PERMISO > Grupos.
2. Haga clic en Agregar grupo.
3. Seleccione el proveedor de identidad. Es el nombre que estableció en la sección Configure LDAP Basic Settings.
4. Establezca un nombre para el grupo.
5. Introduzca el valor de Nombre de grupo en Proveedor de identidad. Debe coincidir con las configuraciones del grupo en su servidor LDAP.
6. Seleccione el rol en función del nivel de acceso que desee proporcionar a los usuarios de este grupo. Vea Roles y Privilegios en Intersight.



Ejemplo de Configuración de un Grupo

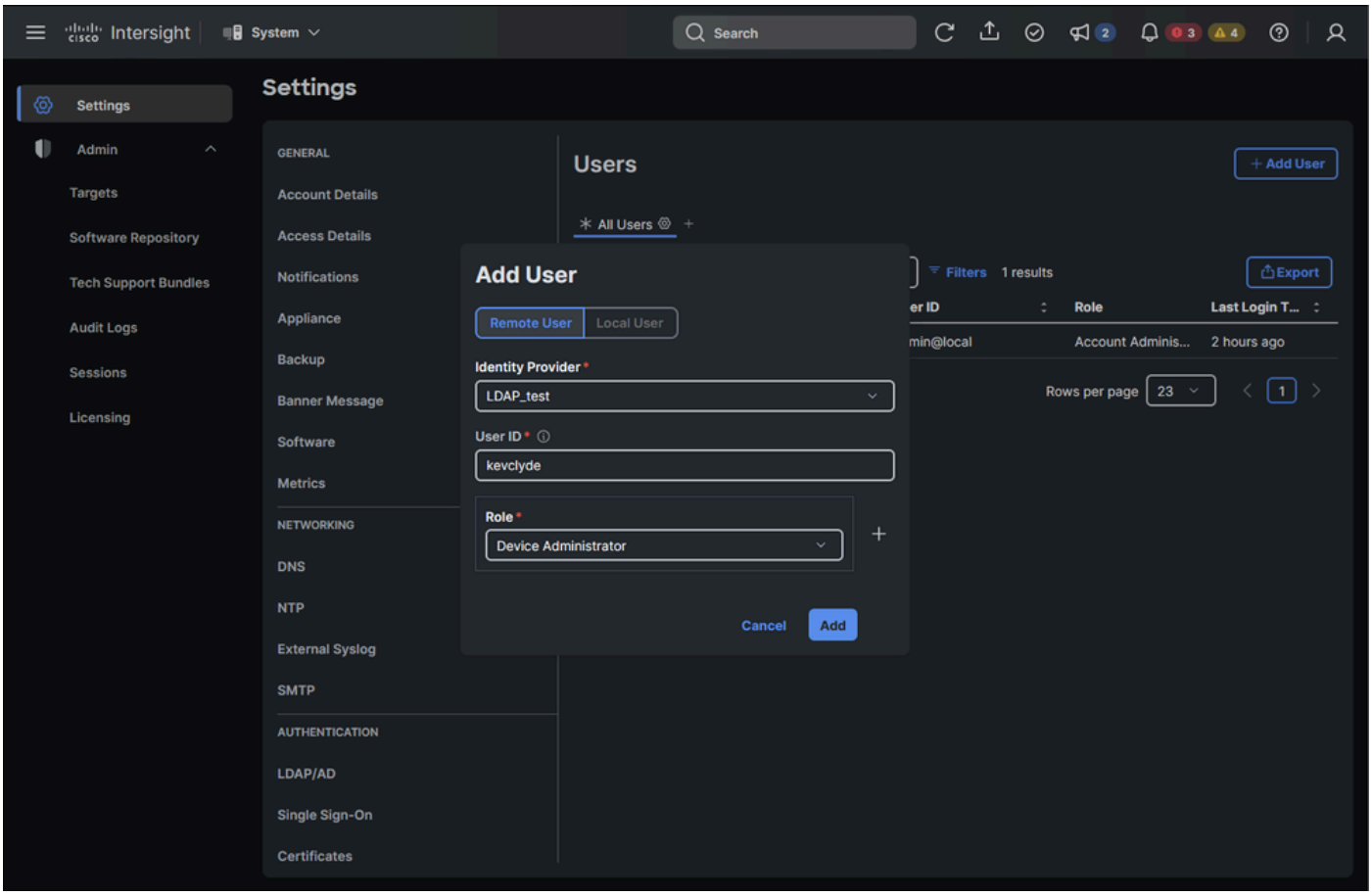
Configurar usuarios

Si prefiere configurar usuarios individuales en lugar de grupos, siga estas instrucciones:

1. Vaya a System > Settings > ACCESS & PERMISSION > Users.
2. Haga clic en Agregar usuario.
3. Seleccione Usuario remoto.
4. Seleccione el proveedor de identidad. Es el nombre que estableció en la sección Configure LDAP Basic Settings.
5. Establezca un ID de usuario.

> Consejo: Para utilizar el nombre de usuario como método de inicio de sesión, copie en el campo User ID, el valor configurado como sAMAccountName en su servidor LDAP. Si desea utilizar el correo electrónico, asegúrese de establecer el correo electrónico del usuario en el atributo mail en el servidor LDAP.

6. Seleccione el rol en función del nivel de acceso que desee proporcionar al usuario. Vea Roles y Privilegios en Intersight.

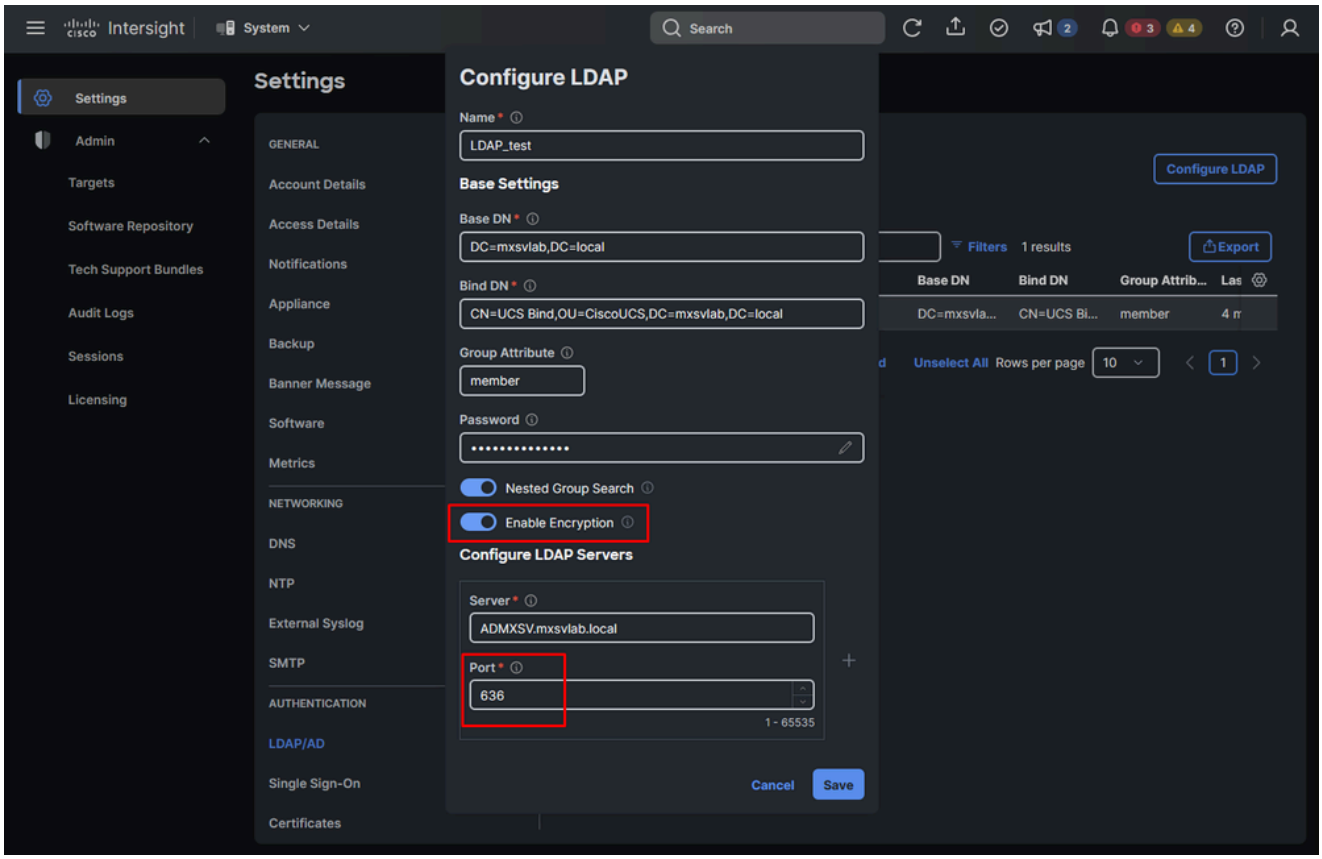


Ejemplo de configuración para un usuario

Configuración de LDAP seguro (LDAP seguro)

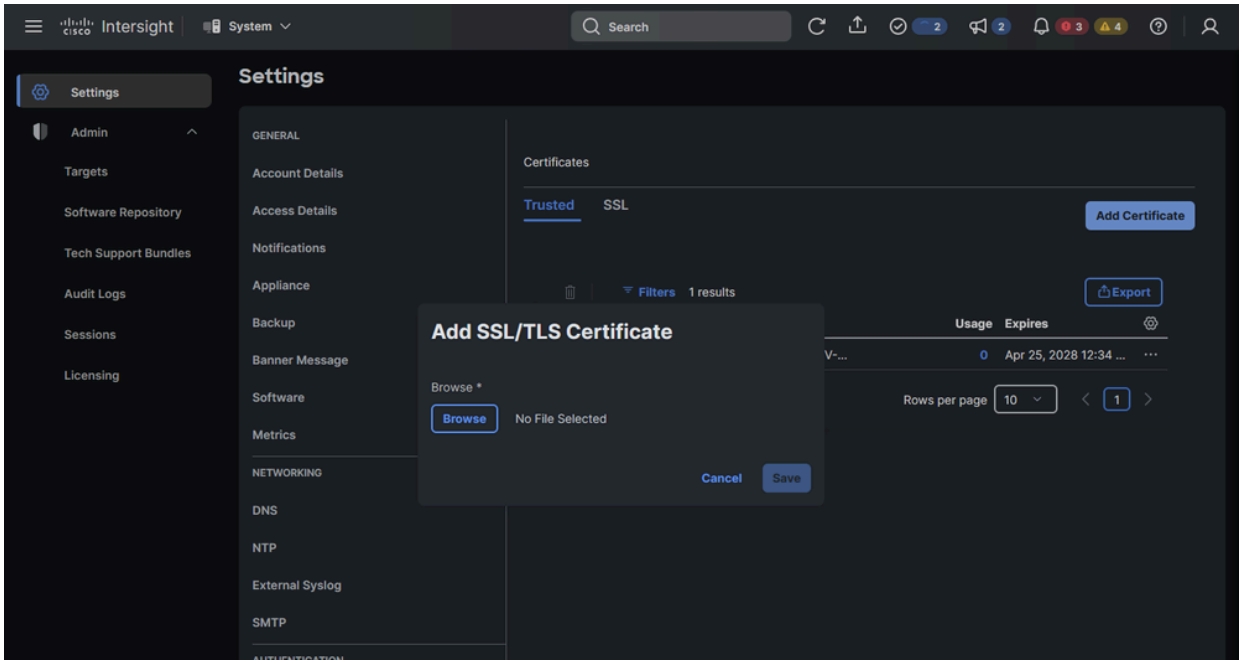
Si desea que la comunicación LDAP esté protegida con cifrado, debe tener un certificado firmado por la CA. Asegúrese de aplicar estos cambios a la configuración:

1. Complete los pasos de Configuración de los parámetros básicos de LDAP pero asegúrese de mover el control deslizante Habilitar cifrado hacia la derecha (Paso 3.g).
2. Asegúrese de que el puerto utilizado sea 636 o 3269, que son los puertos que admiten LDAPS (seguro). Todos los demás puertos admiten LDAP sobre TLS.



Cambios de configuración para LDAP seguro

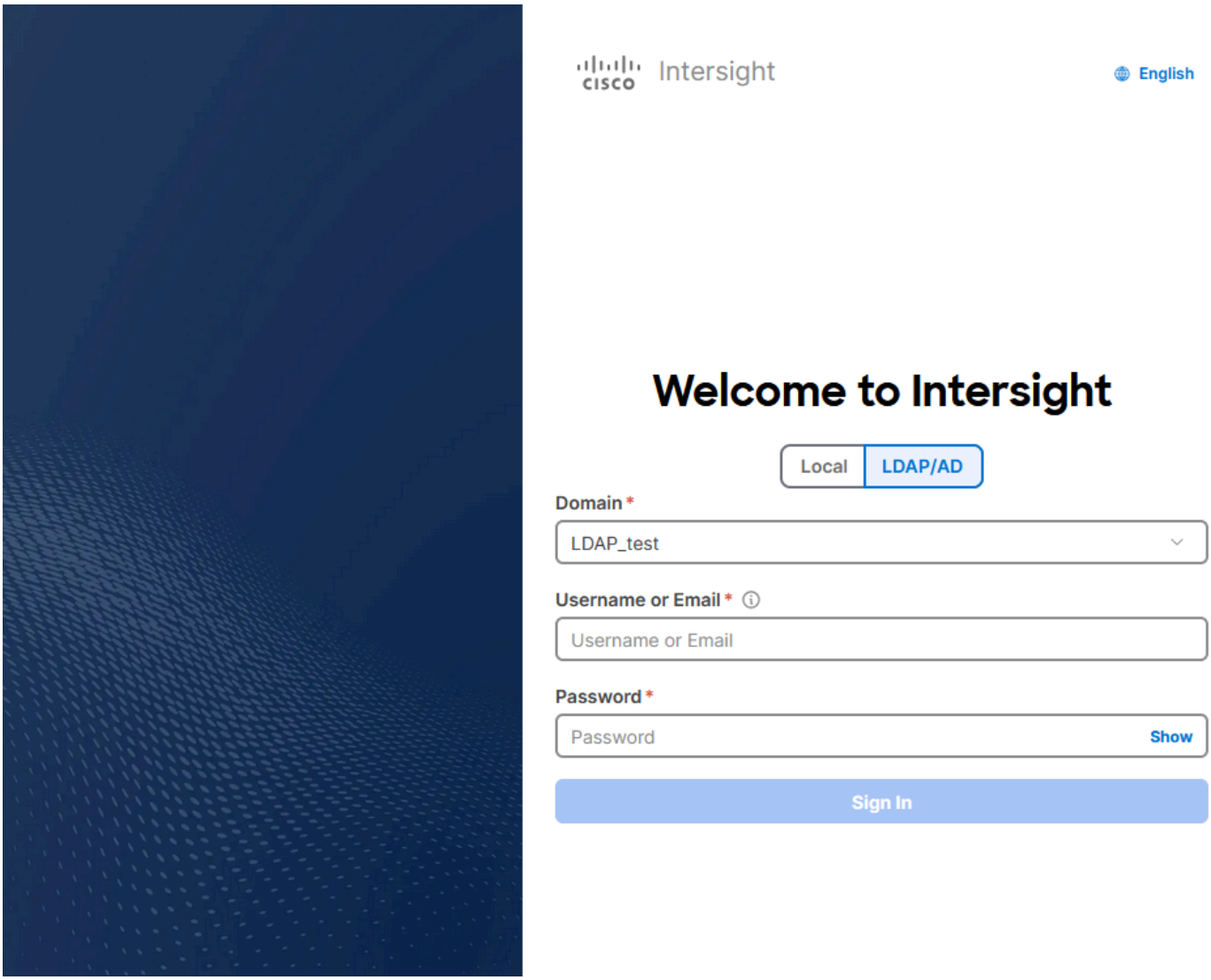
3. Guarde la configuración y espere a que el flujo de trabajo DeployApplianceLDAP finalice.
4. Agregue un certificado con los siguientes pasos:
    1. Vaya a Sistema > Configuración > AUTENTICACIÓN > Certificados > De confianza.
    2. Haga clic en Agregar certificado.
    3. Haga clic en Browse y seleccione un archivo .pem que contenga el certificado emitido por su CA.



Configuración para agregar un certificado

Verificación

En su navegador, navegue hasta la URL de su dispositivo virtual Intersight. La pantalla ahora muestra una opción para iniciar sesión con credenciales LDAP:

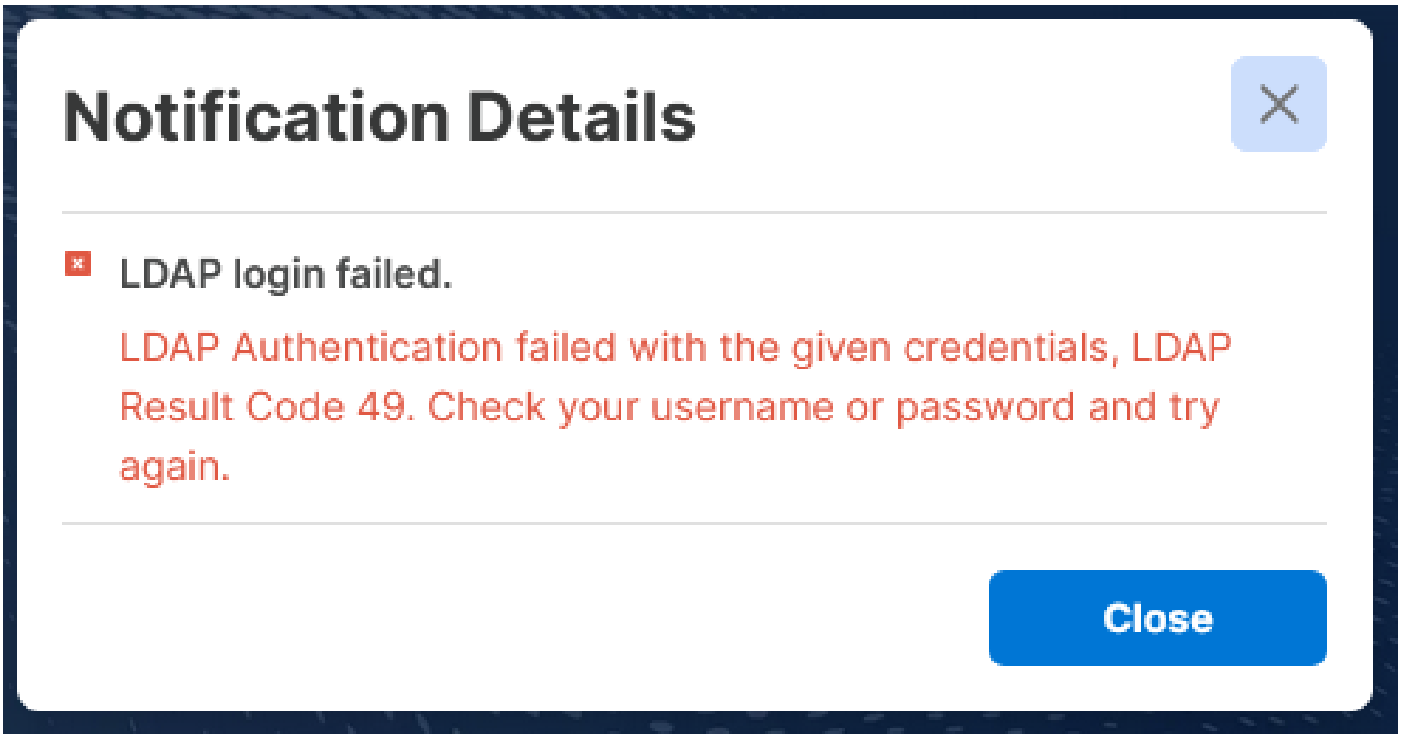


Configuración LDAP habilitada desde la pantalla de inicio de sesión

Troubleshoot

Si el login falla, los mensajes de error proporcionan pistas sobre lo que podría estar mal.

Error 1. Detalles de acceso erróneos

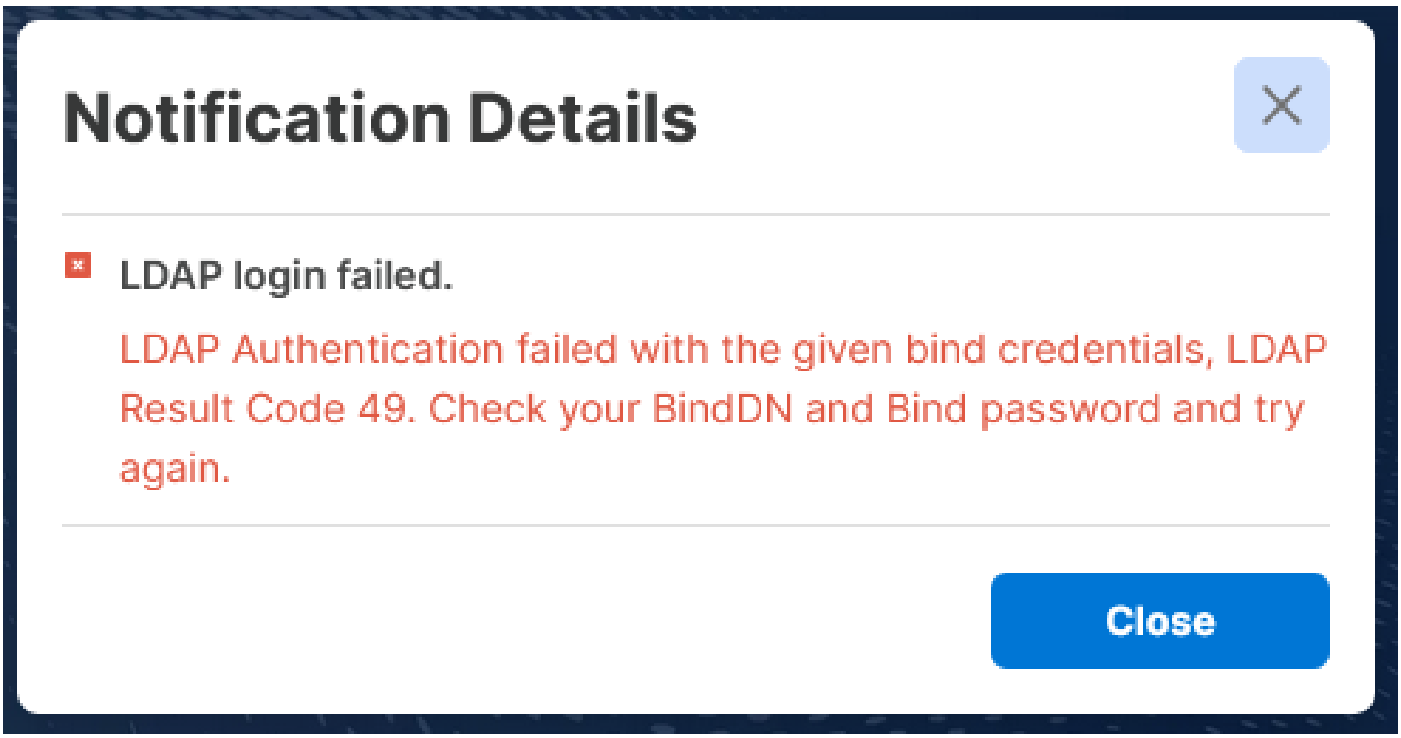


Mensaje de error para error de contraseña incorrecta

Este error significa que los datos de acceso son incorrectos.

1. Verifique que el nombre de usuario y la contraseña sean correctos.

Error 2. Datos de enlace erróneos

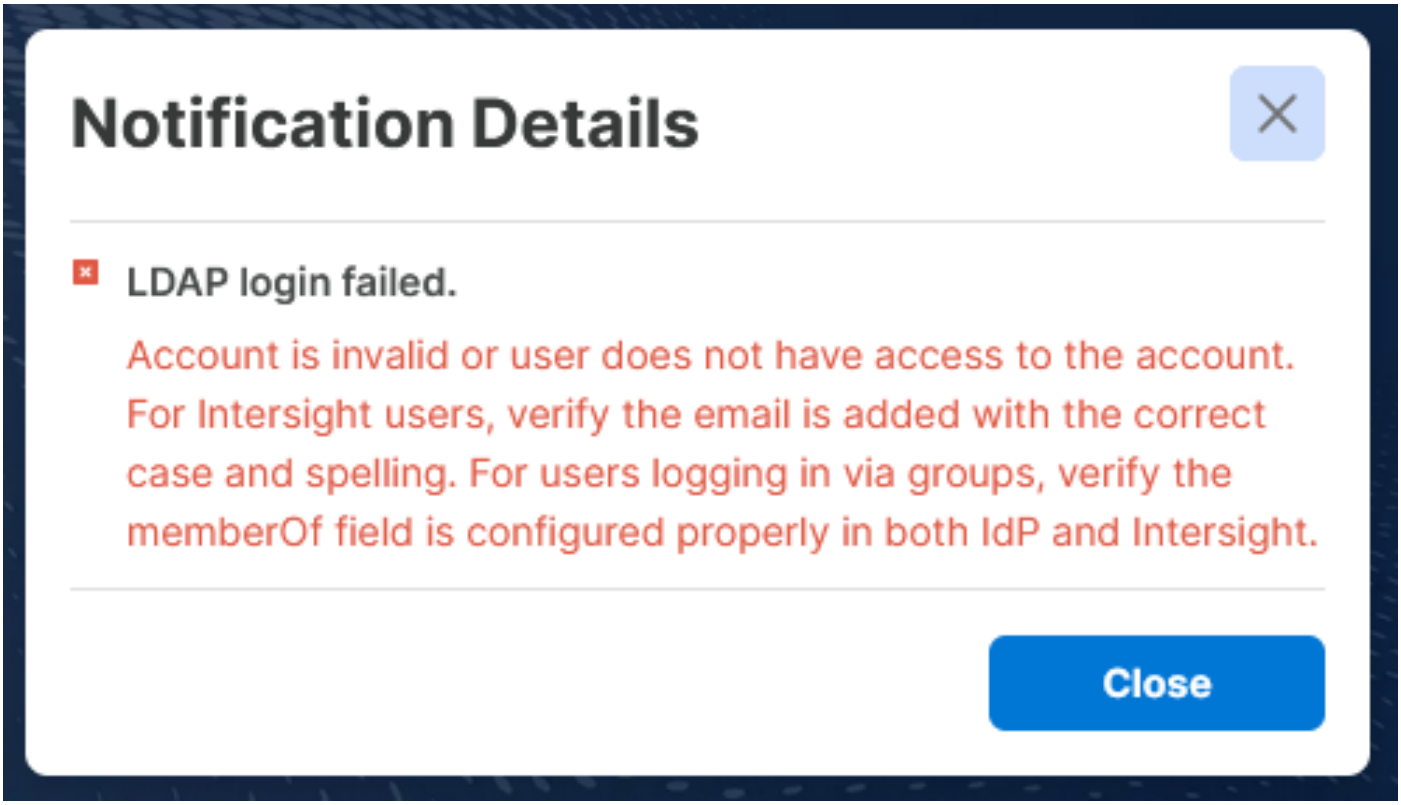


Mensaje de error para datos de enlace erróneos

Este error significa que los datos de enlace son incorrectos.

1. Verifique el BindDN.
2. Verifique la contraseña de enlace configurada en los parámetros de LDAP.

Error 3. No se encuentra el usuario

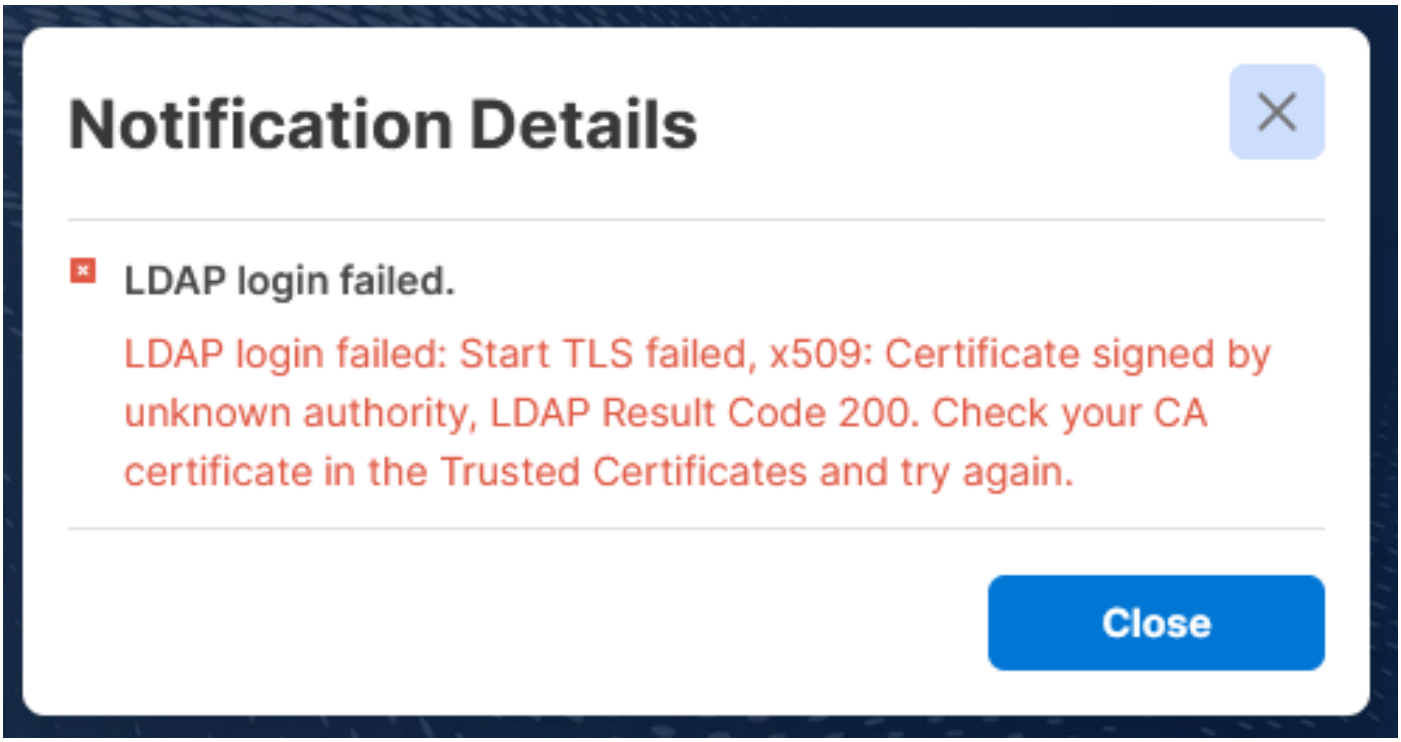


Mensaje de error para el usuario no encontrado

Se activa cuando la búsqueda en el servidor LDAP no devuelve ningún usuario autorizado. Compruebe que los siguientes parámetros son correctos:

1. Marque BaseDN. Los parámetros utilizados para buscar al usuario son incorrectos.
2. Asegúrese de que el atributo de grupo está establecido en member en lugar de memberOf.
3. Verifique que el Nombre de grupo en el Proveedor de identidad en la configuración de Grupos sea correcto. Esto solo se aplica cuando la autorización se proporciona a través de Grupos.
4. Verifique que el correo electrónico del usuario esté configurado correctamente en el campo mail en la configuración de AD para el usuario. Esto solo se aplica cuando se proporciona autorización a usuarios individuales.

Error 4. Certificado incorrecto

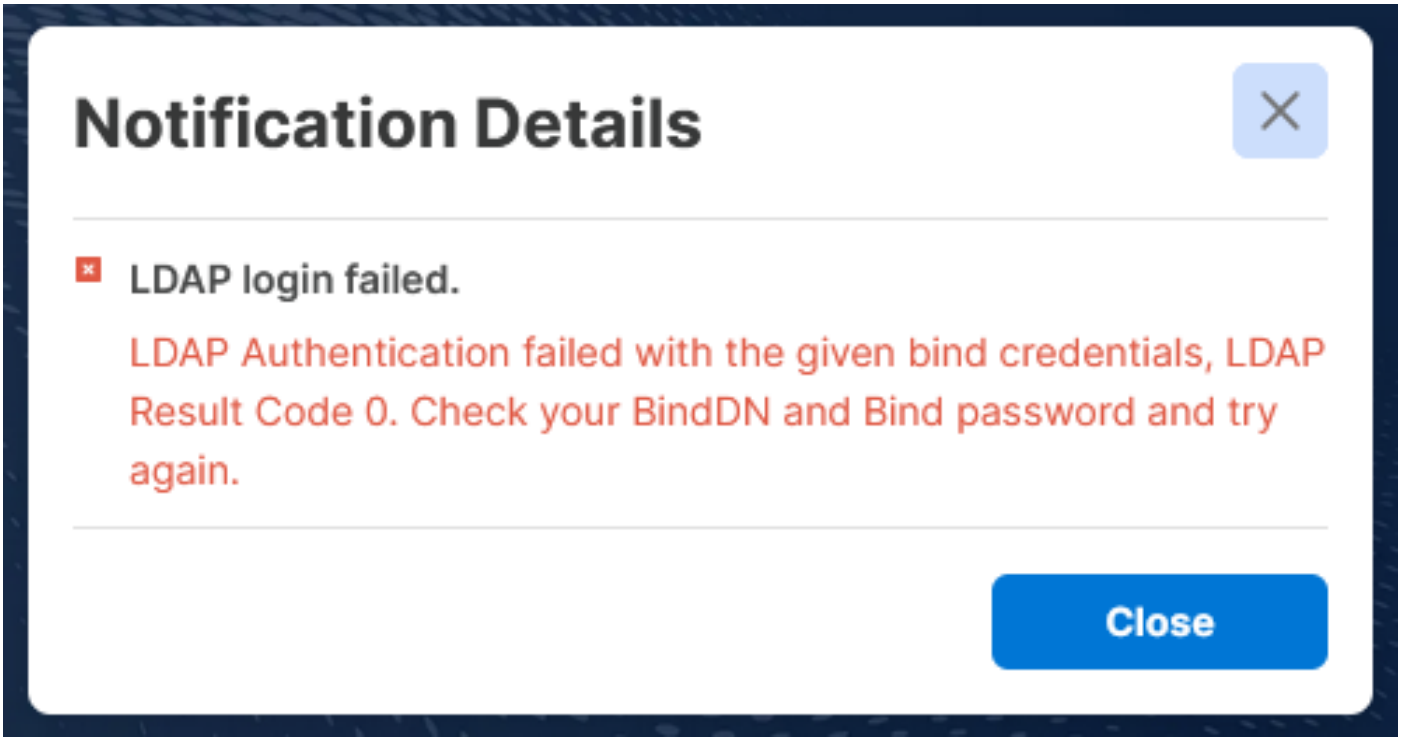


Mensaje de error para certificado incorrecto

Si LDAP cifrado está habilitado:

1. Verifique que el certificado esté configurado e incluya el certificado completo correcto.

Error 5. Habilitar cifrado se utiliza con un puerto seguro

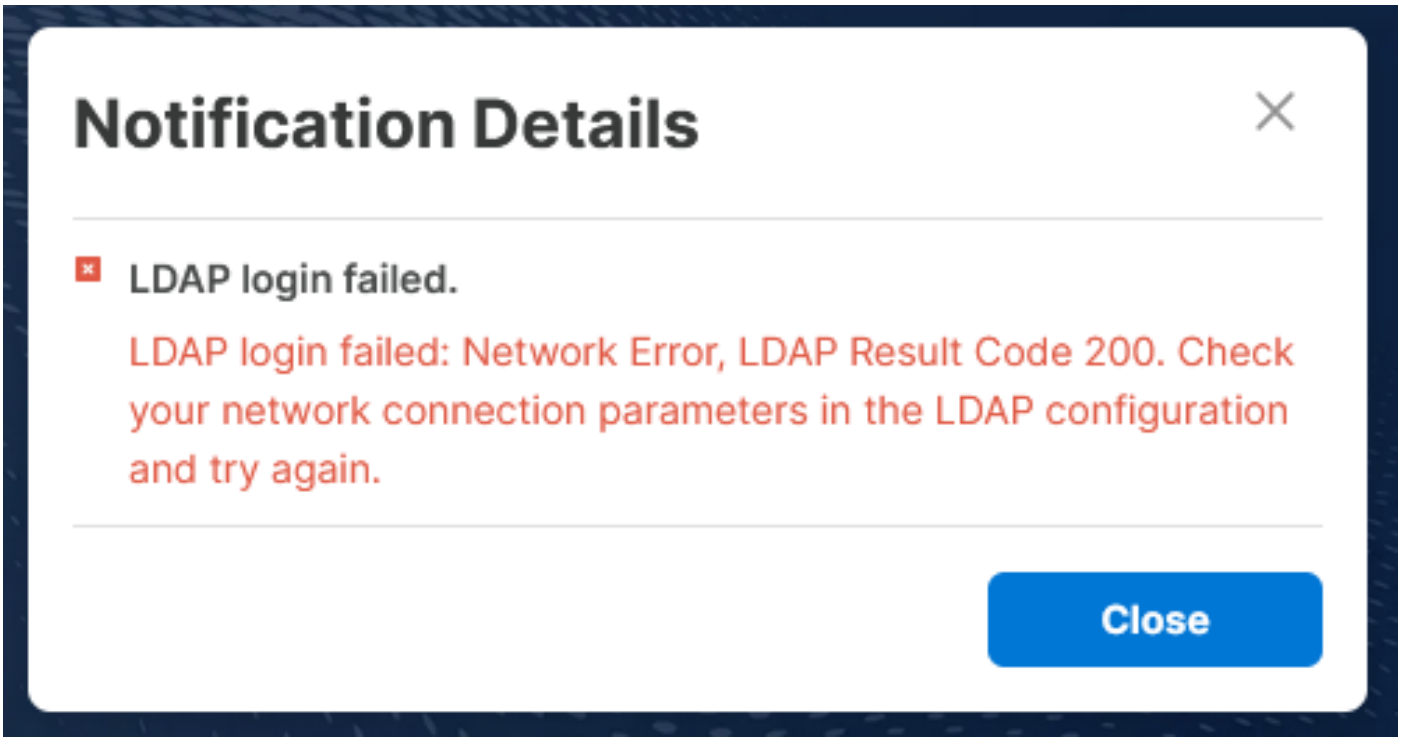


El mensaje de error para Habilitar cifrado está deshabilitado

Este error aparece cuando Enable Encryption no está habilitado pero se ha configurado un puerto para LDAP seguro.

1. Asegúrese de utilizar el puerto 389 si el cifrado no está habilitado.

Error 6. Parámetros de conexión erróneos



Mensaje de error para puerto incorrecto

Este error significa que no fue posible establecer una conexión exitosa con el servidor LDAP. Verifique lo siguiente:

1. El servidor DNS debe resolver el nombre de host del servidor LDAP con la dirección IP correcta.
2. El dispositivo Intersight puede alcanzar el servidor LDAP.
3. Asegúrese de que el puerto 389 se utilice para LDAP no cifrado, 636 o 3269 para LDAP seguro (LDAP) y cualquier otro para TLS (active el cifrado y configure un certificado).

Información Relacionada

- Integración del dispositivo virtual Cisco Intersight con LDAP (vídeo)
- Configuración de los parámetros de LDAP en el dispositivo Intersight
- Funciones y privilegios en la interacción
- Configuración de muestra para LDAP en UCSM

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).