Configurar LDAP no Dispositivo virtual Intersight

Contents

Introdução

Este documento descreve o processo para configurar a autenticação LDAP em um Intersight Private Virtual Appliance (PVA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Lightweight Diretory Access Protocol (LDAP)
- Dispositivo virtual privado da Intersight.
- Servidor DNS (Domain Name Server).

Componentes Utilizados

- Dispositivo virtual privado da Intersight.
- Microsoft Ative Diretory.
- Servidor DNS.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O LDAP é um protocolo usado para acessar recursos de um diretório na rede. Esses diretórios armazenam informações sobre usuários, organizações e recursos. O LDAP fornece uma maneira padrão de acessar e gerenciar essas informações que podem ser usadas para processos de autenticação e autorização.

Este documento mostra o processo de configuração para adicionar a autenticação remota através do LDAP a um PVA da Intersight.

Configurar

Configuração das configurações básicas de LDAP

1. Navegue até System > Settings > AUTHENTICATION > LDAP/AD.
2. Clique em Configure LDAP.
3. Insira as informações necessárias. Considere as próximas recomendações:
    1. O Nome é definido arbitrariamente e não afeta a configuração.
    2. Para BaseDN e BindDN, copie e cole os valores correspondentes da sua configuração do Ative Diretory (AD).
    3. O valor padrão para Atributo do Grupo é membro.

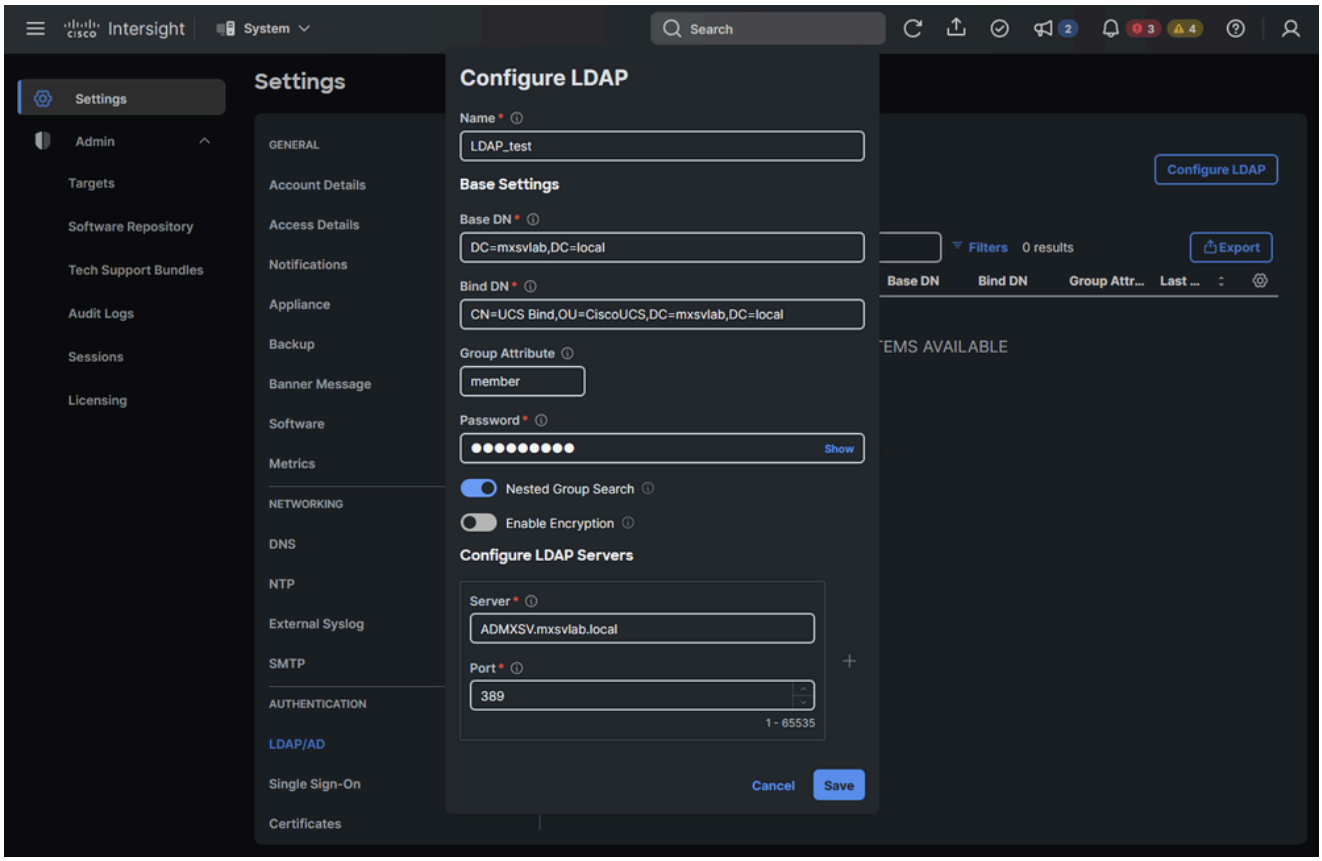
    > Note: Em outras ferramentas de gerenciamento do UCS, como UCSM ou CIMC, o atributo Grupo é definido como memberOf. Na Intersight, é recomendável deixá-lo como membro.

    4. Digite a senha para este provedor LDAP.
    5. Ative a opção Pesquisa de grupo aninhado se quiser permitir uma pesquisa recursiva em seu AD para todos os grupos da raiz e seus grupos contidos.
    6. Deixe Enable Encryption desabilitado para uma configuração LDAP regular. Se o LDAP seguro for necessário, habilite-o e certifique-se de revisar a seção Configuração de LDAP (LDAP seguro) para as etapas complementares que você precisa configurar.
4. Adicione a configuração para um servidor LDAP:
    1. Em Servidor, introduza o IP ou o nome de host do servidor LDAP.

⚠ Caution: Se o nome de host for usado, verifique se o DNS consegue mapear esse nome de host corretamente.

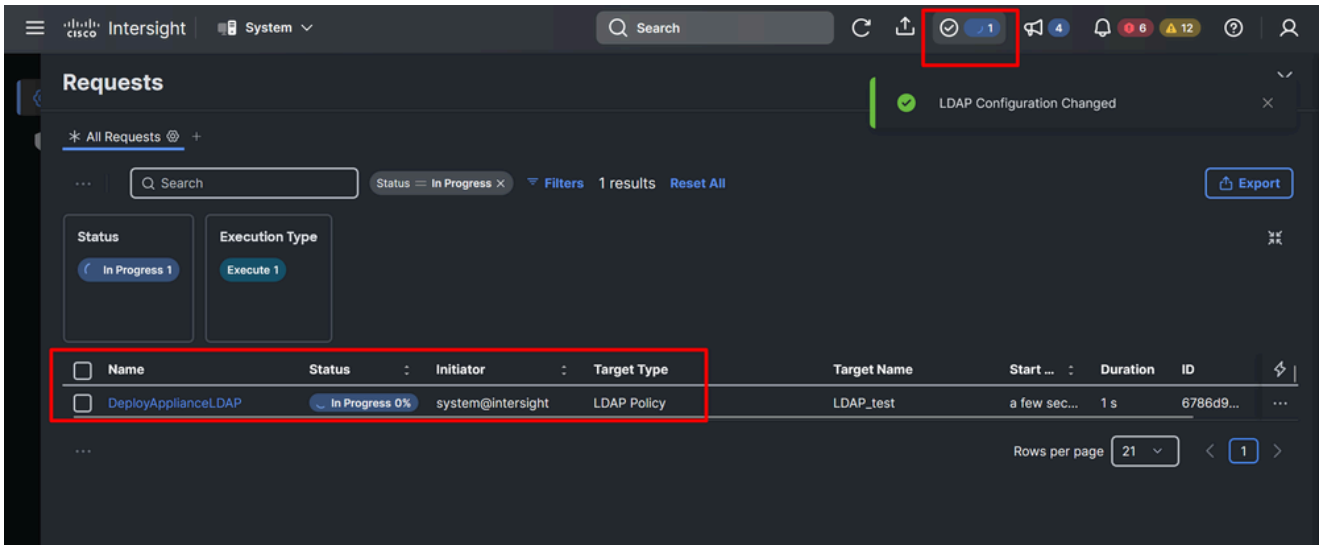
2. A porta padrão e recomendada para LDAP é 389 .

5. Click Save.



Exemplo de configuração para configurações LDAP básicas

6. Monitore o fluxo de trabalho DeployApplianceLDAP a partir de Requests na barra superior.



Solicitação de Implantação

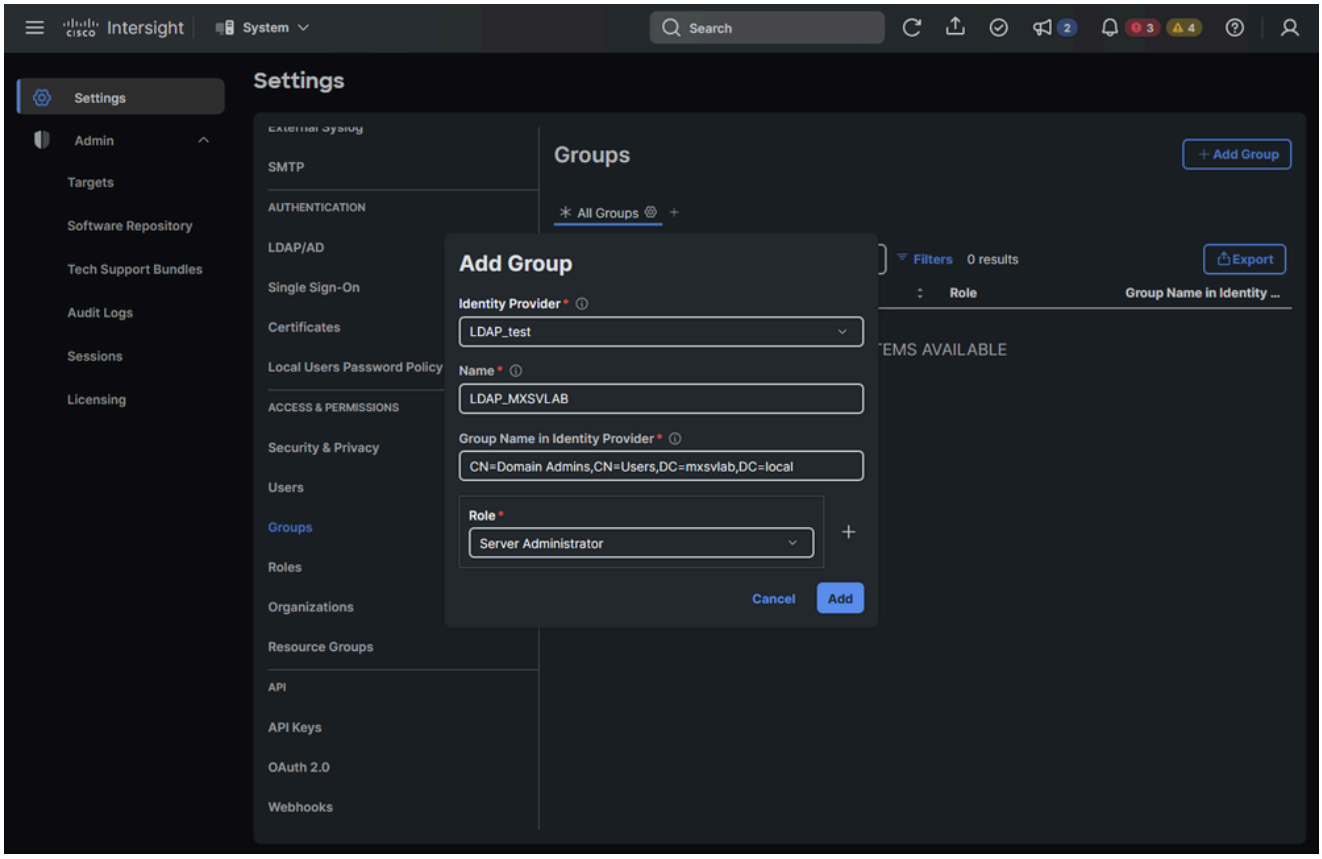
Configurar usuários e grupos

Quando o fluxo de trabalho DeployApplianceLDAP estiver concluído, você poderá configurar Grupos ou Usuários individuais.

Se você decidir usar Grupos, a autorização será fornecida a todos os usuários que pertencem a esse Grupo. Se você usar Usuários individuais, será necessário adicionar cada usuário com sua própria função de autorização.

Configurar grupos

1. Navegue até Sistema > Configurações > ACESSO e PERMISSÃO > Grupos.
2. Clique em Add Group.
3. Selecione o Provedor de identidade. É o nome que você define na seção Configurar configurações básicas de LDAP.
4. Defina um nome para o grupo.
5. Insira o valor para Nome do grupo no Provedor de identidade. Ele precisa corresponder às configurações do grupo no servidor LDAP.
6. Selecione a Função, dependendo do nível de acesso que você deseja fornecer aos usuários neste grupo. Consulte Funções e Privilégios na Intersight.



Exemplo de configuração para um grupo

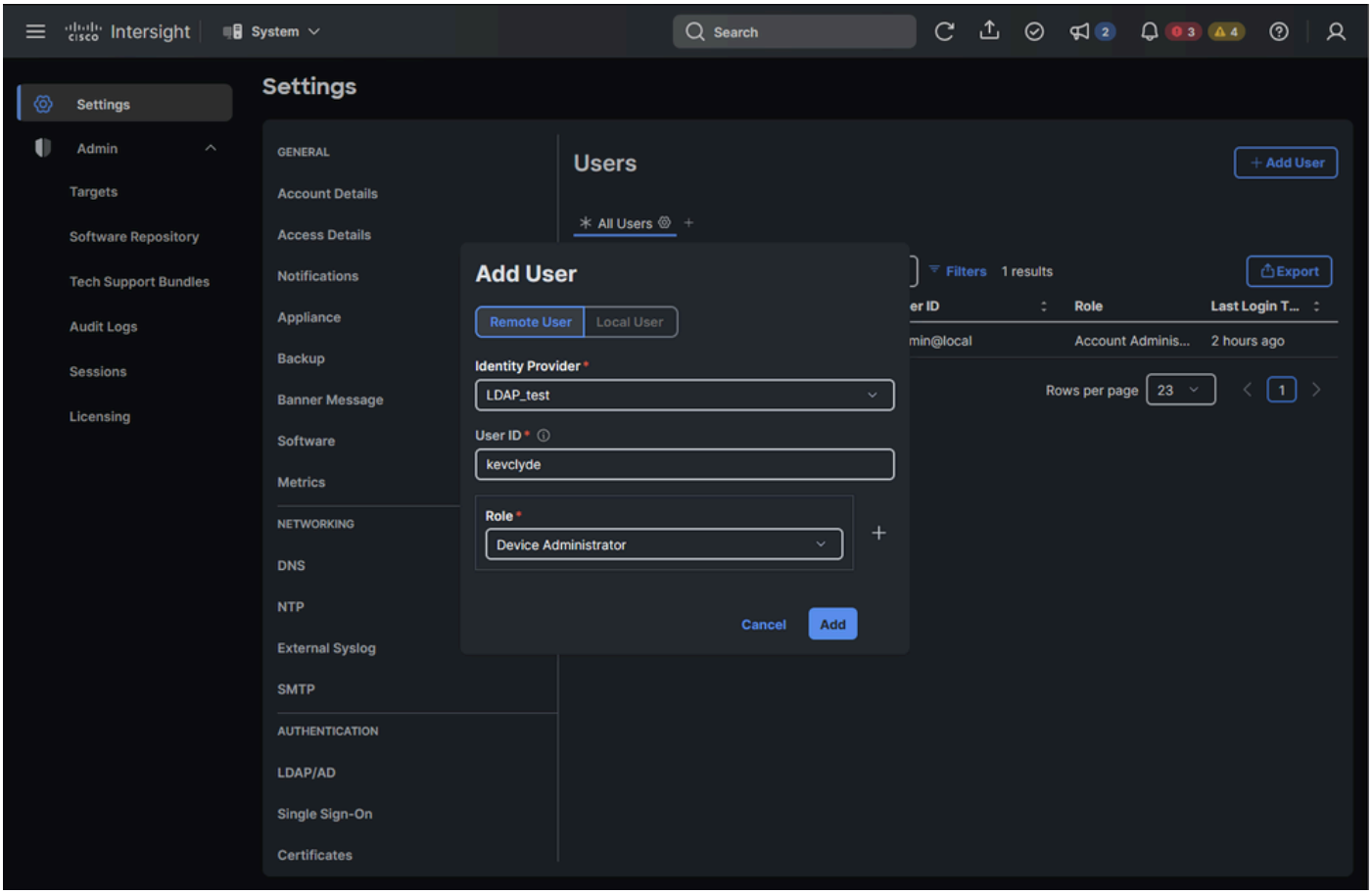
Configurar usuários

Se preferir configurar usuários individuais em vez de Grupos, siga estas instruções:

1. Navegue até Sistema > Configurações > ACESSO e PERMISSÃO > Usuários.
2. Clique em Add User.
3. Selecione Remote User.
4. Selecione o Provedor de identidade. É o nome que você define na seção Configurar configurações básicas de LDAP.
5. Defina uma ID de usuário.

> Tip: Para usar o nome de usuário como método de login, copie no campo ID de usuário o valor configurado como sAMAccountName em seu servidor LDAP.
> Se quiser usar o e-mail, certifique-se de definir o e-mail do usuário no atributo mail no servidor LDAP.

6. Selecione a Função dependendo do nível de acesso que você deseja fornecer ao usuário. Consulte Funções e Privilégios na Intersight.



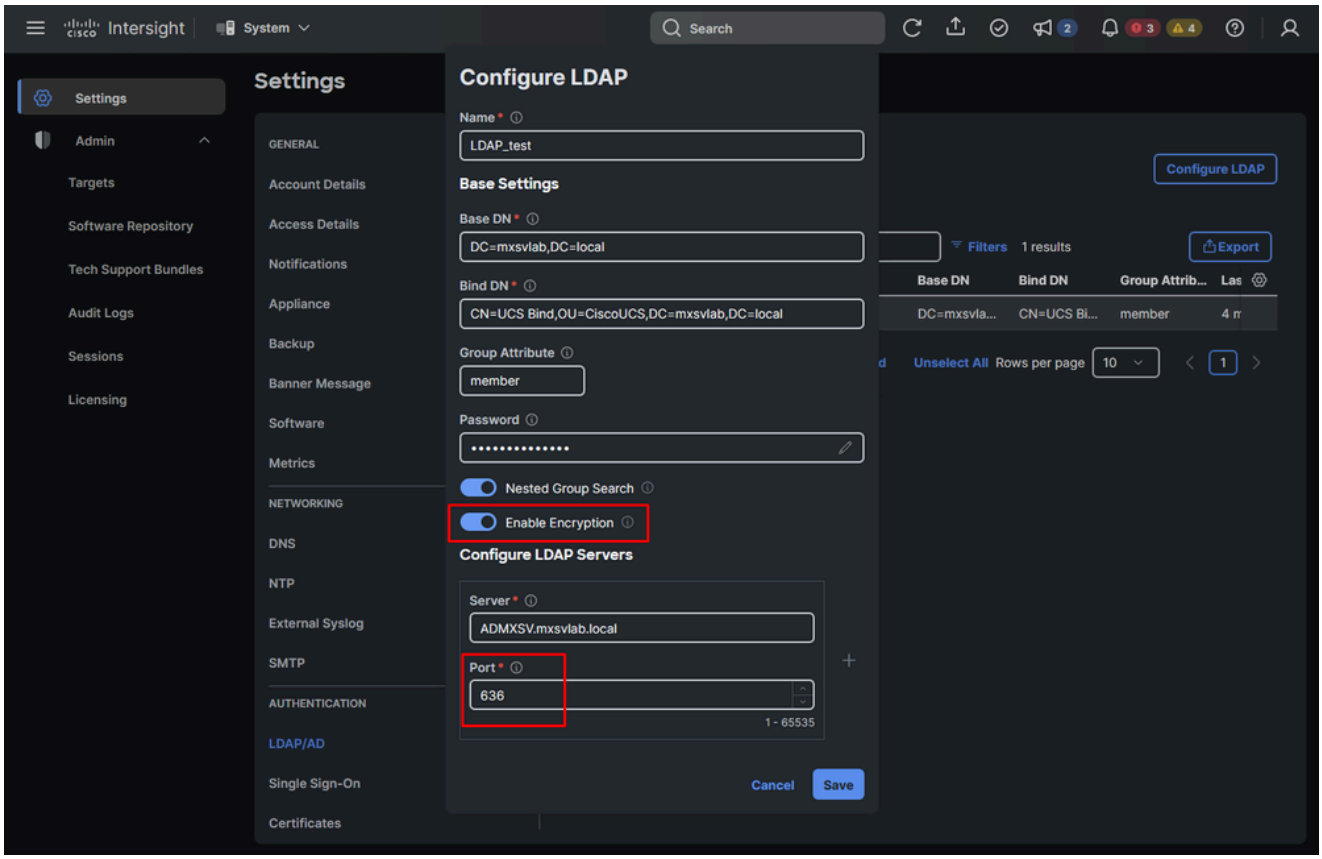
Exemplo de configuração para um usuário

Configuração de LDAPS (LDAP seguro)

Se desejar que sua comunicação LDAP seja protegida com criptografia, você precisa ter um certificado assinado por sua CA. Certifique-se de aplicar essas alterações à configuração:

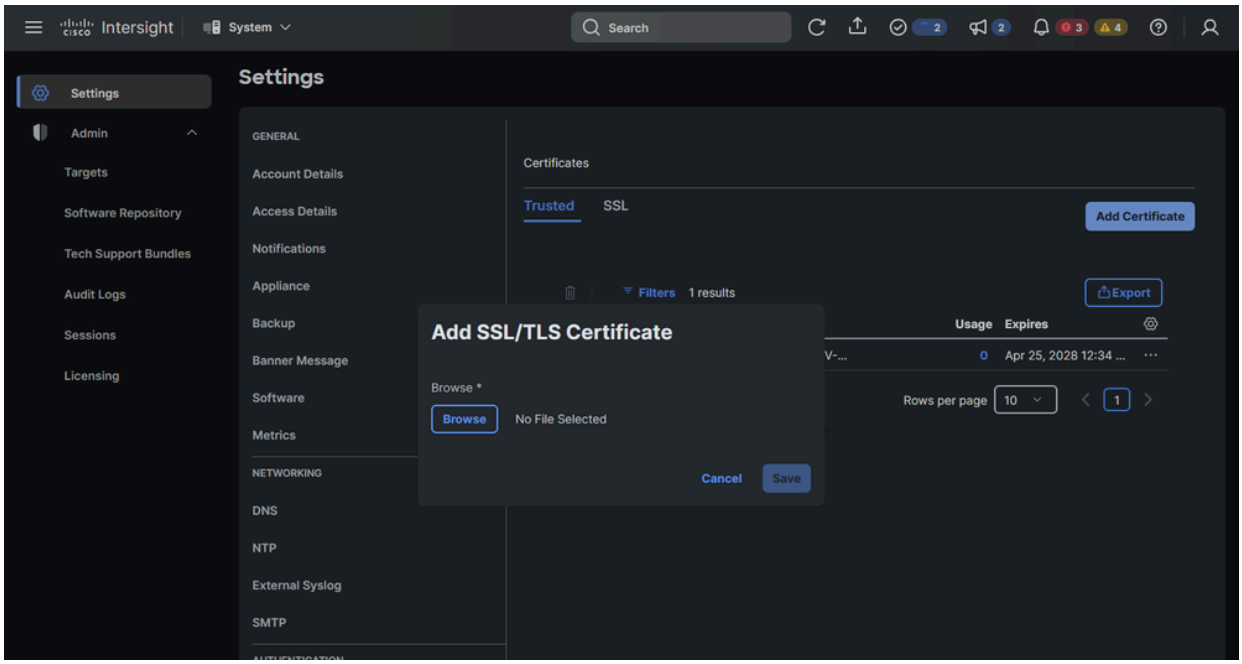
1. Conclua as etapas de Configuration of LDAP Basic Settings, mas certifique-se de mover o controle deslizante Enable Encryption para a direita (Etapa 3.g).
2. Certifique-se de que a porta usada seja 636 ou 3269 que são as portas que suportam

LDAPS (seguro). Todas as outras portas suportam LDAP sobre TLS.



Alterações de configuração para LDAP seguro

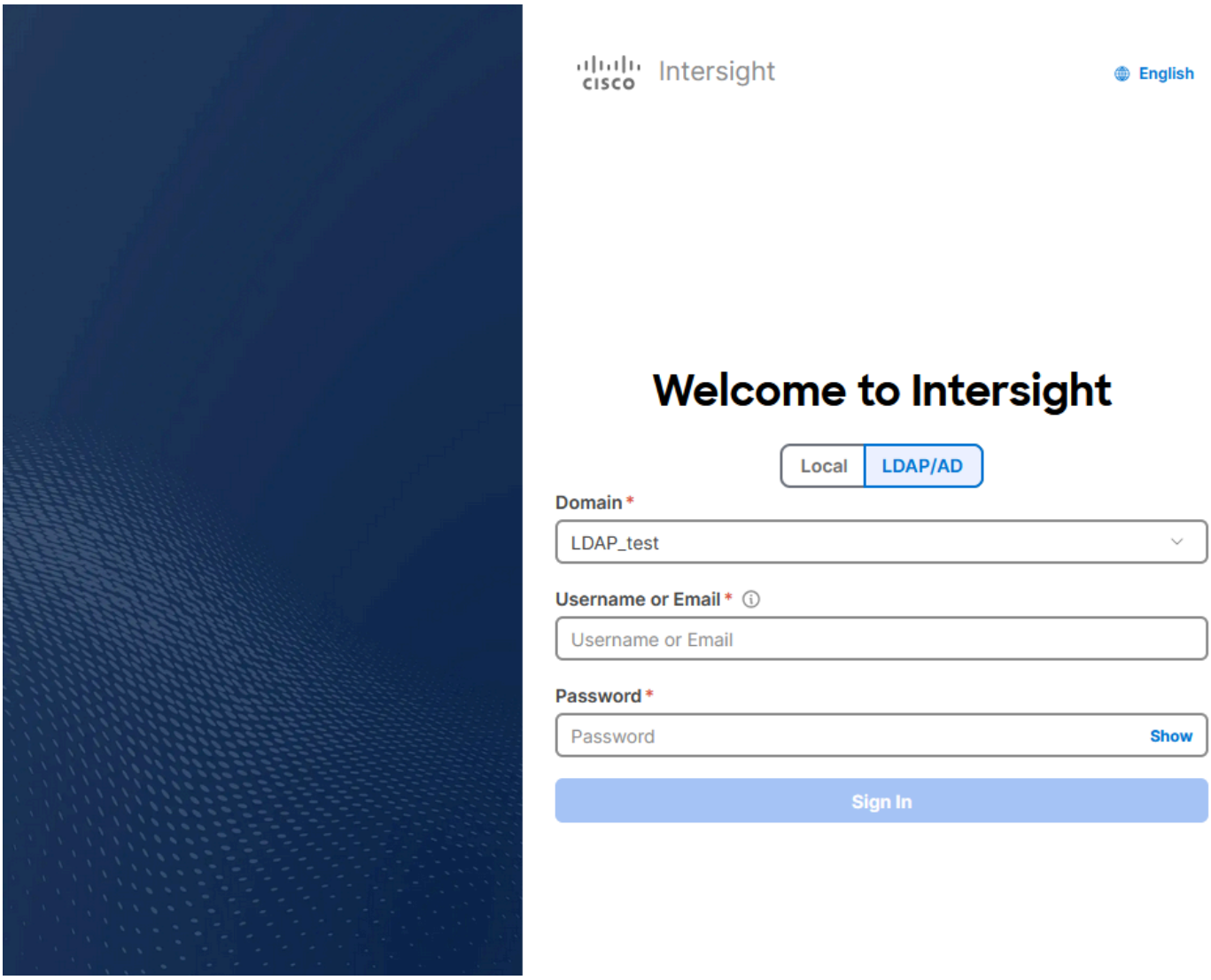
3. Salve a configuração e aguarde a conclusão do fluxo de trabalho DeployApplianceLDAP.
4. Adicione um certificado com as próximas etapas:
    1. Navegue até Sistema > Configurações > AUTENTICAÇÃO > Certificados > Confiáveis.
    2. Clique em Add Certificate (Adicionar certificado).
    3. Clique em Browse e selecione um arquivo .pem que contenha o certificado emitido por sua CA.



Configuração para adicionar um certificado

Verificar

No navegador, navegue até o URL do Dispositivo virtual Intersight. A tela agora exibe uma opção para efetuar login com credenciais LDAP:

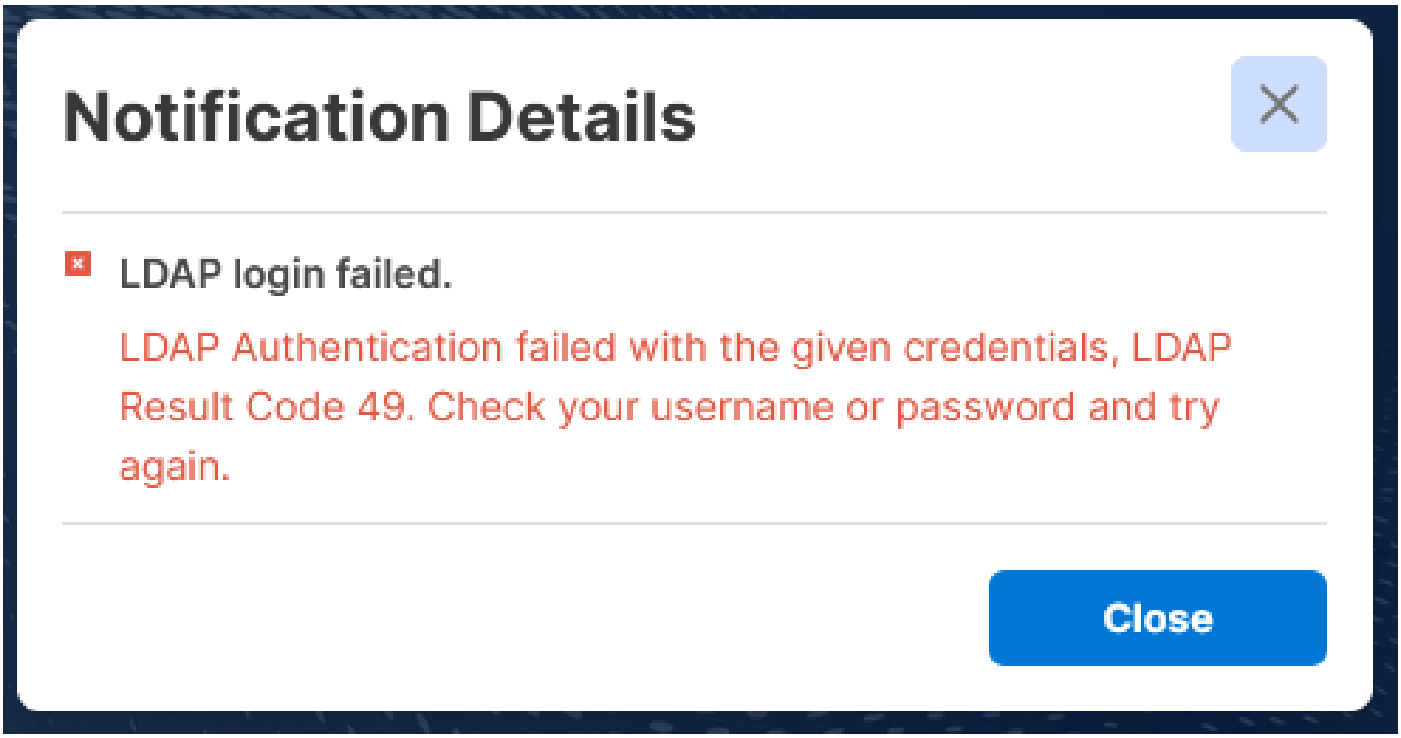


Configuração LDAP ativada na tela de login

Troubleshooting

Se o login falhar, as mensagens de erro fornecerão dicas sobre o que pode estar errado.

Erro 1. Detalhes de Acesso Incorretos

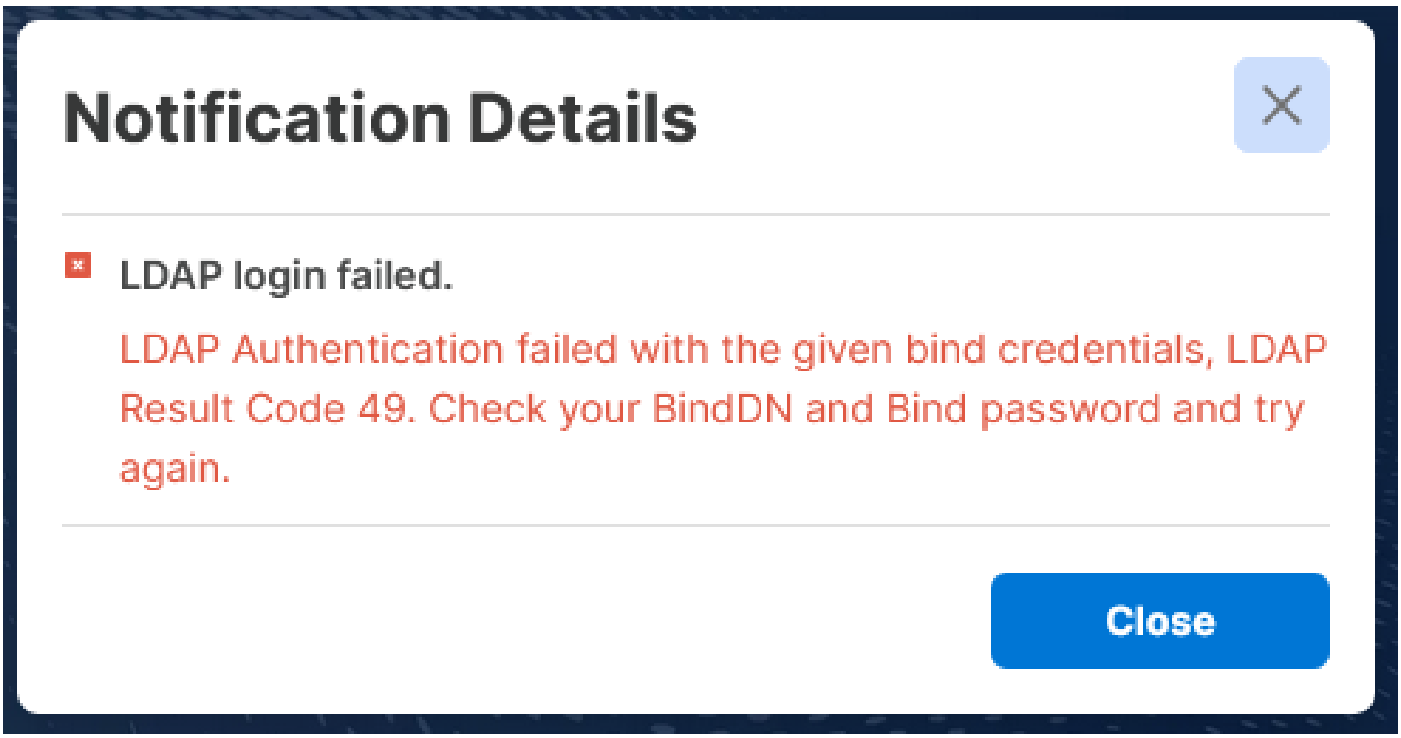


Mensagem de erro para erro de senha incorreta

Este erro significa que os dados de acesso estão incorretos.

1. Verifique se o nome de usuário e a senha estão corretos.

Erro 2. Dados de Ligação Incorretos

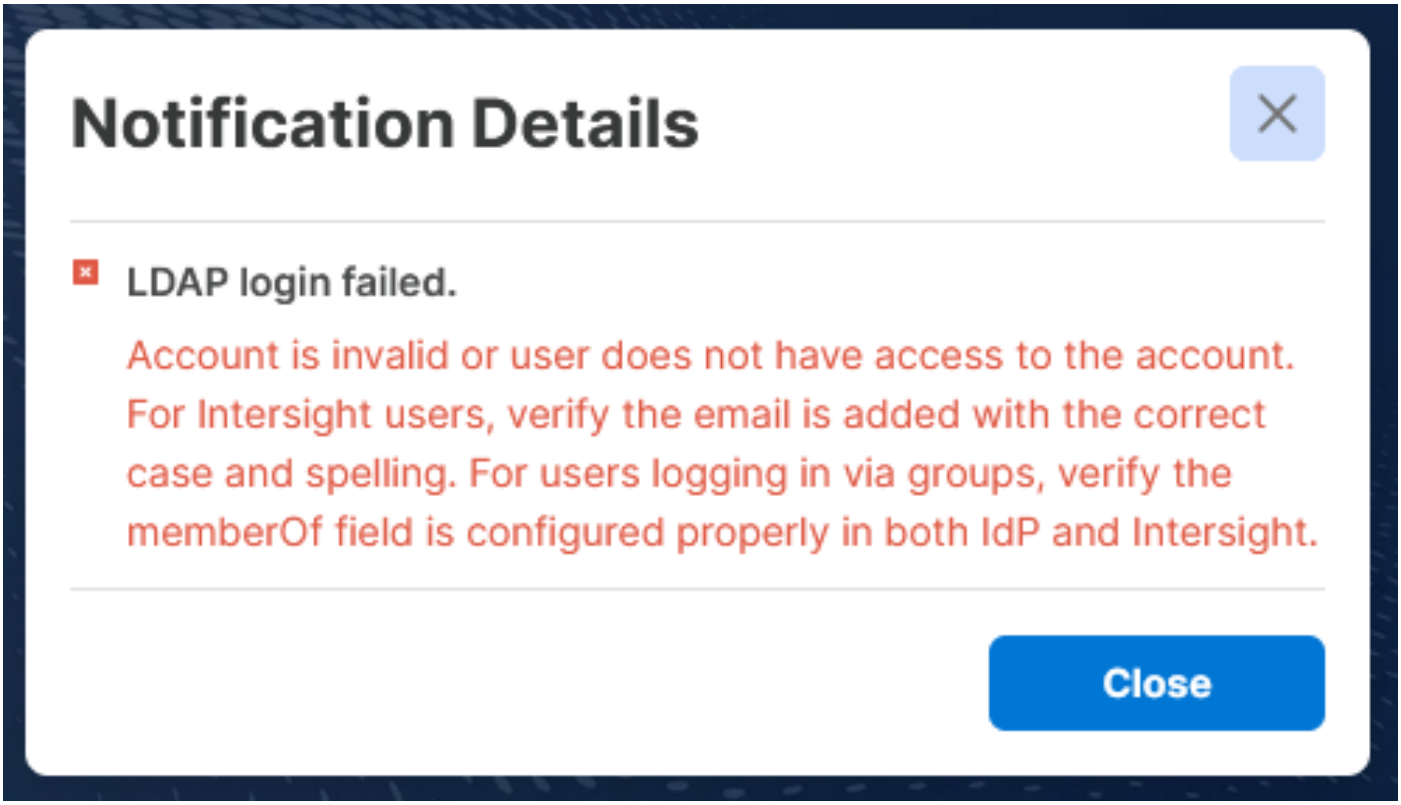


Mensagem de erro para dados de ligação incorretos

Este erro significa que os dados de ligação estão incorretos.

1. Verifique o BindDN.
2. Verifique a senha de vinculação configurada nas configurações LDAP.

Erro 3. Não é possível localizar o usuário

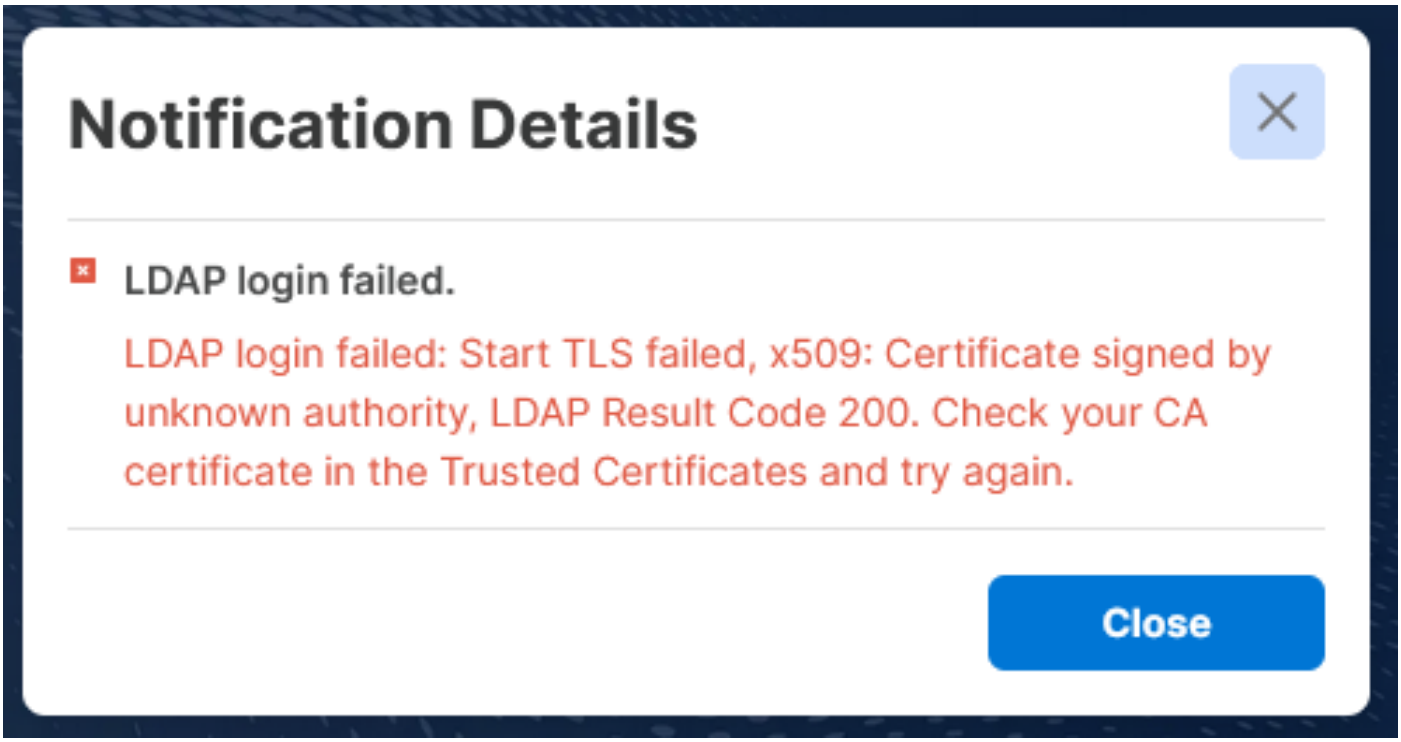


Mensagem de erro para usuário não encontrada

Isso é disparado quando a pesquisa no servidor LDAP não retorna nenhum usuário autorizado. Verifique se as próximas configurações estão corretas:

1. Verifique BaseDN. Os parâmetros usados para procurar o usuário estão incorretos.
2. Certifique-se de que o Atributo do Grupo esteja definido como membro em vez de membro de.
3. Verifique se o nome do grupo no provedor de identidade na configuração Groups está correto. Isso se aplica somente quando a autorização é fornecida via Grupos.
4. Verifique se o e-mail do usuário está definido corretamente no campo mail na configuração do AD para o usuário. Isso se aplica somente quando a autorização é fornecida a Usuários individuais.

Erro 4. Certificado incorreto

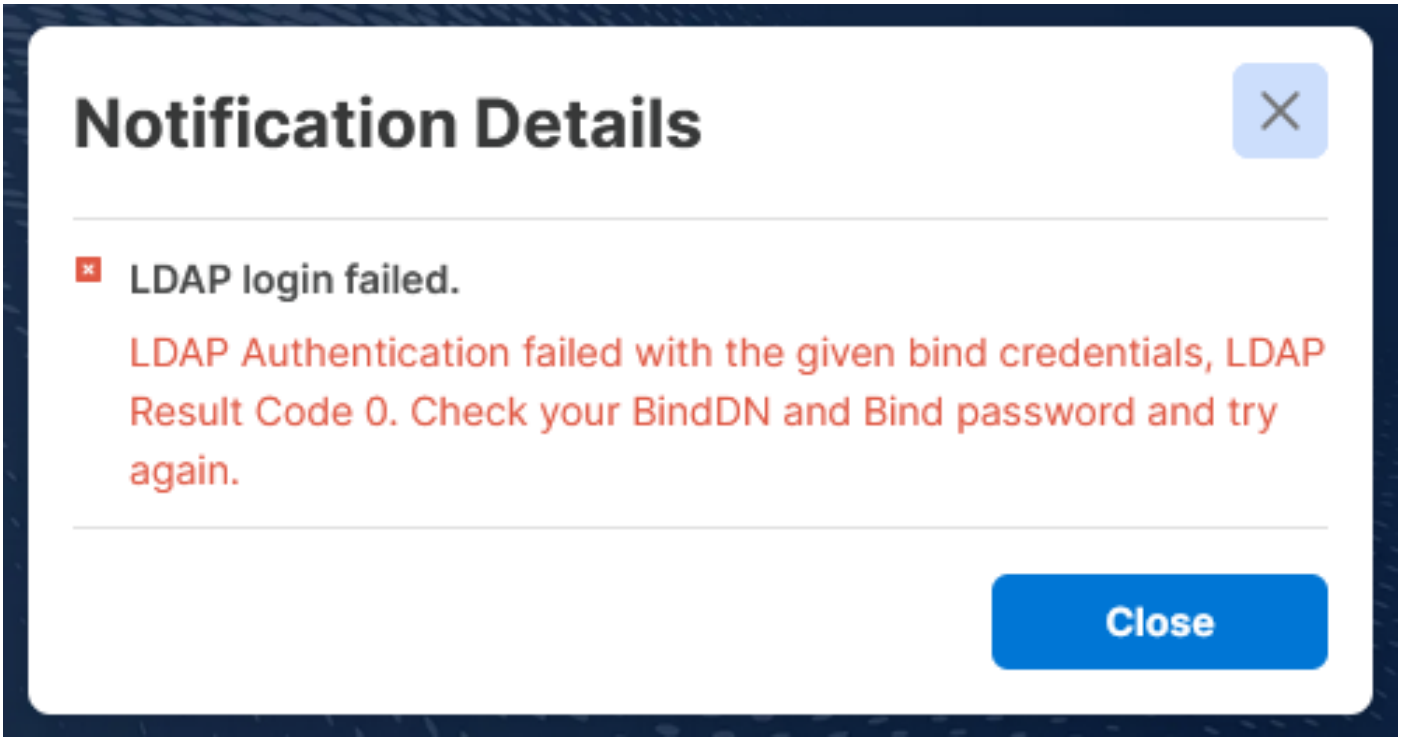


Mensagem de erro para certificado incorreto

Se o LDAP criptografado estiver habilitado:

1. Verifique se o certificado está configurado e se ele inclui o certificado completo correto.

Erro 5. Habilitar criptografia é usada com uma porta segura

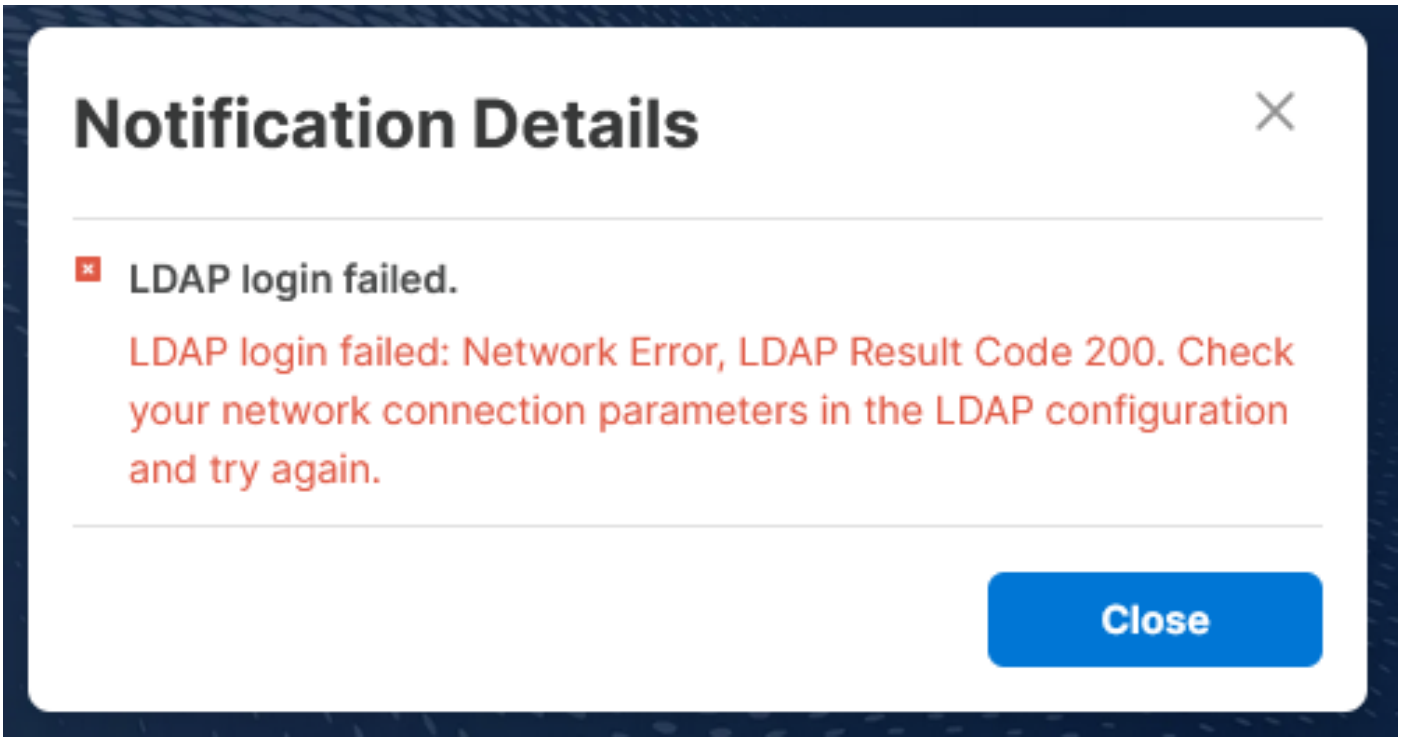


A mensagem de erro para Habilitar criptografia está desabilitada

Este erro aparece quando Enable Encryption não está habilitado, mas uma porta para LDAP seguro está configurada.

1. Certifique-se de usar a porta 389 se a criptografia não estiver habilitada.

Erro 6. Parâmetros De Conexão Incorretos



Mensagem de erro para porta incorreta

Esse erro significa que não foi possível estabelecer uma conexão bem-sucedida com o servidor LDAP. Verifique:

1. O servidor DNS deve resolver o nome de host do servidor LDAP para o IP correto.
2. O aplicativo Intersight consegue acessar o servidor LDAP.
3. Verifique se a porta 389 é usada para LDAP não criptografado, 636 ou 3269 para LDAP seguro (LDAPS) e qualquer outra para TLS (habilite a criptografia e configure um certificado).

Informações Relacionadas

- Integração do Cisco Intersight Virtual Appliance com LDAP (vídeo)
- Definir configurações LDAP no aplicativo Intersight
- Atribuições e Privilégios em Intersight
- Exemplo de configuração para LDAP em UCSM

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.