

Você está aqui: [Configuração e manutenção](#) > [Gerenciando usuários, grupos e funções](#) > Configuração de LDAP

Configuração de LDAP

Como administrador do recurso Controle de acesso, você pode sincronizar informações entre o Archer e o servidor LDAP (Lightweight Directory Access Protocol) da respectiva organização. Com a sincronização LDAP, a administração de contas de usuário e grupos pode ser simplificada, permitindo que atualizações e alterações feitas no servidor LDAP sejam refletidas automaticamente no Archer.

Importante: A sincronização LDAP não está disponível para o Archer SaaS.

O recurso de configuração de LDAP permite que você faça o seguinte:

- Associar contas de usuário aos usuários LDAP.
- Criar contas quando há novos usuários no servidor LDAP.
- Desative contas que não podem mais ser associadas diretamente a um usuário no LDAP. Não é possível excluir as contas de usuário por meio da sincronização LDAP.
- Reativar contas quando certos critérios de usuário são localizados no servidor LDAP, por exemplo, status do emprego renovado.
- Atualizar dados de perfil de usuário para contas baseadas em modificações de LDAP.

O recurso de configuração do LDAP aceita informações de SSO (single sign-on) de vários domínios e as sincroniza com sistemas LDAP distintos, o que permite fazer o seguinte:

- Padronizar os procedimentos de log-on em ambientes de domínio heterogêneos.
- Adicionar de forma incremental novos domínios a configurações existentes de acesso de usuário.
- Sincronizar dados com várias contas de domínio.

Os grupos LDAP não podem ser associadas a um grupo já existente do Archer. O processo de sincronização replica a estrutura de grupos LDAP no Archer. Os grupos criados no Archer pelo processo de sincronização de LDAP não podem ser editados no Archer.

Configuração de LDAP com vários domínios

É recomendável que você não especifique uma configuração padrão de LDAP se sua organização empregar vários domínios e permitir nomes de usuários não exclusivos entre os domínios. Se você fizer isso, um indivíduo com um nome de usuário idêntico ao de um indivíduo no domínio padrão, provavelmente poderá obter acesso indevido ao Archer.

Por exemplo, John Smith (jsmith@apac.company.com), do domínio Ásia-Pacífico, e Jim Smith (jsmith@us.company.com), do domínio Estados Unidos, têm o mesmo nome de usuário. Se uma configuração padrão do LDAP especificar us.company como o domínio padrão e o domínio apac.company.com não for válido na instância us.company, então John Smith poderá fazer log-on na conta de Jim Smith. Quando John Smith fez logon no Archer usando SSO, o Archer tentou validá-lo no domínio padrão com o nome de usuário **jsmith**. O Archer faz a correspondência desse nome de usuário com uma conta existente (jsmith@us.company.com), mesmo que seja um indivíduo diferente.