# Acesso de usuários

O controle de acesso oferece uma estrutura para manter usuários, funções e parâmetros de segurança e atribuir privilégios de acesso nos níveis de sistema, aplicativo, registro e campos.

- Contas de usuário permitem que os usuários façam log-on no Archer.
- Grupos de usuários são um meio de agrupar usuários com base na estrutura organizacional ou localização geográfica.
- Funções de acesso são um conjunto de direitos no nível de aplicativo e de página, que um administrador pode criar e atribuir a qualquer número de usuários e grupos para controlar os privilégios de usuário (de criação, leitura, atualização e exclusão).
- Parâmetros de segurança são regras para controle do acesso do usuário ao Archer e às respectivas páginas individuais.
- Sincronização LDAP simplifica a administração de usuários e grupos, permitindo que atualizações e alterações feitas no servidor LDAP sejam refletidas automaticamente no Archer.

Nesta página



## Suporte aos usuários

É importante ter políticas bem definidas em torno dos procedimentos de Help Desk para a instalação do Archer. Os administradores de suporte devem compreender a importância da força da senha e da confidencialidade dos dados, como nomes de log-on de usuário e senhas. Criar um ambiente em que é frequentemente solicitado esse tipo de

dados confidenciais ao usuário final aumenta a oportunidade de ataques de engenharia social. Oriente os usuários finais a oferecer, e os administradores do help desk a solicitar, o mínimo de informação necessária em cada situação.

## Impedindo ataques de engenharia social

Os fraudadores frequentemente usam ataques de engenharia social para fazer com que funcionários ou indivíduos desavisados divulguem dados confidenciais que podem ser utilizados para ter acesso aos sistemas protegidos. É recomendável que você use as seguintes orientações para ajudar a reduzir a probabilidade de um ataque de engenharia social bem-sucedido:

- Se os administradores de Help Desk precisarem iniciar o contato com um usuário, eles não devem solicitar nenhuma informação do usuário. Em vez disso, os usuários devem ser instruídos a ligar novamente ao Help Desk em um número de telefone conhecido do Help Desk para garantir que o pedido original é legítimo.

- O número de telefone do Help Desk deve ser conhecido por todos os usuários.

- Os administradores de Help Desk só devem perguntar o nome de usuário dos usuários via telefone quando eles ligarem para o Help Desk. Os administradores de Help Desk nunca devem pedir as senhas de usuários.

- Os administradores do help desk devem autenticar a identidade do usuário antes de executar qualquer ação administrativa em nome desse usuário. É recomendável que você verifique a identidade do usuário usando os seguintes métodos:

    - Ligue de volta para o usuário usando um telefone da organização e um número que já esteja armazenado no sistema.

      **Importante:** Tenha cuidado ao usar telefones celulares para confirmar identidade, mesmo que sejam de propriedade da empresa, porque os números de telefones celulares são, muitas vezes, armazenados em locais vulneráveis à adulteração ou engenharia social.

    - Envie um e-mail ao usuário para um endereço de e-mail da empresa. Se possível, use e-mail criptografado.

    - Trabalhe com o gerente do funcionário para verificar a identidade do usuário.

    - Verifique a identidade pessoalmente.
    - Use várias perguntas abertas a partir dos registros do funcionário. Por exemplo: "Nomeie 1 pessoa de seu grupo." ou pergunte "Qual é o número de seu crachá?" Evite perguntas cuja resposta seja sim ou não.

## Confirmando identidades dos usuários

É fundamental que os administradores de help desk verifiquem a identidade de cada usuário final antes de realizar qualquer operação de help desk em seu nome. É recomendável que você verifique as identidades do usuário usando os seguintes métodos:

- Ligue de volta para o usuário final em um telefone pertencente à organização e em um número já armazenado no sistema.

  **Importante:** Tenha cuidado ao usar telefones celulares para confirmar a identidade, mesmo se eles pertencerem à empresa. Números de telefone celular são frequentemente armazenados em locais vulneráveis à adulteração ou engenharia social.

- Envie um e-mail ao usuário para um endereço de e-mail da empresa. Se possível, use e-mail criptografado.
- Trabalhe com o gerente do funcionário para verificar a identidade do usuário.
- Verifique a identidade pessoalmente.
- Use várias perguntas abertas a partir dos registros do funcionário. Por exemplo: "Nomeie 1 pessoa de seu grupo." ou pergunte "Qual é o número de seu crachá?" Evite perguntas cuja resposta seja sim ou não.

## Recomendações para os usuários

É recomendável que você instrua seus usuários a fazer o seguinte:

- Nunca dar suas senhas para ninguém, nem mesmo aos administradores de Help Desk.
- Mudar suas senhas com frequência.
- Esteja ciente sobre as solicitações de informações que você pode esperar dos administradores de help desk.
- Sempre fazer log-off da interface Web do Archer quando terminar.

- Sempre bloquear os desktops quando saírem de perto de seus computadores.
- Fechar o navegador regularmente e limpar os dados de cache.
- Não faça upload de nenhum arquivo para o Archer de fontes que não sejam as originais.
- Antes de fazer upload dos arquivos para o Archer, execute uma verificação de vírus local para pesquisar qualquer conteúdo mal-intencionado.
- Nunca habilite o conteúdo ativo ao abrir arquivos CSV com aplicativos de planilha como o Microsoft Excel ou o LibreOffice Calc.

**Observação:** É recomendável que você realize treinamento regular para comunicar essas orientações aos usuários.

# Permissões de entidade

O Archer aceita permissões de usuário em uma série de componentes do sistema. É recomendável que você conceda permissões apenas aos usuários que precisam acessar esses componentes. Ao conceder permissões a esses componentes, é recomendável que você não selecione o grupo Todos, porque esse grupo concede direitos a todos os usuários. Além disso, é recomendável que você analise as permissões concedidas regularmente para assegurar que o acesso correto é concedido aos usuários.

A tabela a seguir explica como as permissões de usuário são configuradas nos componentes compatíveis.

| **Componente** | **Explicação das permissões** |
|---|---|
| Áreas de trabalho, painéis de controle | Configurado na seção Acesso em uma área de trabalho ou em um painel de controle.<br><br>É recomendável configurar esses componentes para serem privados ou restringir os usuários em Global do Dashboard. |
| Relatórios globais | Configurado quando você salva um relatório. É recomendável que |

| **Componente** | **Explicação das permissões** |
| --- | --- |
| | você defina o campo Permissões como Relatório Global. |
| Permissões de registro | Configurado em um campo Permissões de registro em um aplicativo ou questionário. |
| Permissões do campo | Configurado na guia Acesso em um campo em um aplicativo ou questionário. É recomendável que você configure esses campos como privados. |
| Administradores de configuração | Os administradores de configuração têm direitos aos aspectos de configuração (por exemplo, campos, layout, eventos orientados por dados, notificações) de um aplicativo, questionário ou subformulário. Os administradores de configuração têm direitos de leitura da página de conteúdo para o aplicativo ou questionários. |
| Administradores de conteúdo | Configurados em aplicativos e questionários. Concede inerentemente direitos de CRUD sobre todo o conteúdo do aplicativo ou questionário, independentemente das permissões de registro. |
| Administradores do relatório global | Configurados no Gerador de aplicativos para os proprietários do relatório atribuídos em um |

| **Componente** | **Explicação das permissões** |
| --- | --- |
| | aplicativo ou questionário específico. |