Auditoria e registro

# Auditoria e registro

Este tópico descreve os diferentes mecanismos de auditoria e registro que você pode executar no Archer.

Nesta página

* [Descrição do registro](#Descri%C3%A7%C3%A3odoregistro)
* [Relatório de Eventos de Segurança](#Relat%C3%B3riodeEventosdeSeguran%C3%A7a)
* [Archer logs de erros](#Archerlogsdeerros)
* [Permissões do diretório de log](#Permiss%C3%B5esdodiret%C3%B3riodelog)
* [Logs de eventos do Windows](#LogsdeeventosdoWindows)

## Descrição do registro

A tabela a seguir descreve os registros relacionados à segurança fornecidos pelo Archer.

| Componente | Local |
| --- | --- |
| Relatório sobre eventos de segurança | O banco de dados da instância |
| Registros de erros do Archer | Sistema de arquivos no diretório de registro configurado |
| Registros de eventos do Windows | Visualizador de eventos |

## Relatório de Eventos de Segurança

O relatório de eventos de segurança contém uma lista de todos os eventos relacionados à segurança que ocorreram no Archer. O Archer recomenda que os administradores definam e apliquem uma política de retenção para os registros de erro do Archer, bem como os registros de eventos do Windows, de acordo com sua política corporativa de TI e práticas recomendadas de segurança. Esse relatório inclui os seguintes eventos de segurança:

* Função de acesso criada
* Função de acesso excluída
* Função de acesso modificada
* Status da conta modificado
* Administrador de configuração adicionado
* Administrador de configuração excluído
* Administrador de conteúdo adicionado
* Administrador de conteúdo excluído
* Log-in de usuário com falha
* Exclusão total do conteúdo do aplicativo
* Permissão de relatório global concedida
* Permissão de relatório global removida
* Exclusão de configuração LDAP iniciada
* Exclusão de configuração LDAP concluída
* Número máximo de tentativas de log-in excedido
* Sincronização de Acesso off-line solicitada - Download
* Sincronização de Acesso off-line solicitada - Upload
* Senha alterada pelo Administrador
* Senha alterada pelo Usuário
* Redefinir senha solicitada
* Função atribuída ao usuário
* Função removida do usuário
* Eventos de segurança iniciados
* Eventos de segurança interrompidos
* Atribuição de parâmetro de segurança modificada
* Parâmetro de segurança criado
* Parâmetro de segurança excluído
* Parâmetro de segurança modificado
* Administrador de configuração de subformulário adicionado
* Administrador de configuração de subformulário excluído
* Conta de usuário adicionada
* Conta de usuário excluída
* Conta de usuário modificada
* Usuário adicionado ao grupo
* Nome completo de usuário modificado
* Log-in de usuário
* Nome de log-in de usuário modificado
* Log-out de usuário
* Usuário removido do grupo

## Archer logs de erros

Você pode configurar o local do registro de erro do Archer no Painel de controle do Archer, tanto no nível da instância quanto da instalação. O local padrão do registro na instância é C:\ArcherFiles\logging.

O Archerrecomenda que você configure a definição no nível da instalação e deixe o local no nível de instância como padrão, com base na configuração de instalação.

Para obter mais informações, consulte "Configurações de registro" e "Verificar as propriedades de registro" na Ajuda do Painel de controle do [Archer.](https://help.archerirm.cloud/archer_suite_help/en-us/Content/PortalHome/platform_home.htm)

## Permissões do diretório de log

O Archer recomenda que você restrinja as permissões na pasta de arquivos de registros para as mesmas permissões de leitura, gravação e modificação da conta em que os processos do IIS e os serviços instalados do Archer estão sendo executados.

## Logs de eventos do Windows

Os serviços do Archer e registros do aplicativo da Web registram os seguintes itens nos registros de eventos do Windows:

* Início do serviço (aplicativo e registros do sistema)
* Interrupção do serviço (aplicativo e registros do sistema)
* Erro de tempo de execução do .NET