

Você está aqui: [Configuração e manutenção](#) > [Gerenciando usuários, grupos e funções](#) > Configurando uma instância para Logon único

Configurando uma instância para Logon único

O Logon único (SSO) reduz a sobrecarga administrativa relacionada a contas de usuário. Com a autenticação SSO habilitada, é possível recuperar informações do perfil de usuário de um servidor de diretórios LDAP no momento da criação da conta. Essa etapa opcional automatiza a configuração de dados básicos do perfil de usuário. Configure o SSL (Secure Sockets Layer) para SSO ou como um método independente. Configure a autenticação SSO para Windows integrado ou para Windows integrado e SSL. A configuração da autenticação exige modificar o arquivo web.config.

Nesta página

- [Mecanismos de autenticação compatíveis](#)
- [Propriedades do Logon único](#)
- [Opções de autenticação](#)
- [Procedimento de configuração](#)
 - [Tarefa 1: Ativar autenticação para o Logon único](#)
 - [Tarefa 2: Configurar Single Sign-on](#)
 - [Nomes de declaração para a opção Federação](#)
 - [Tarefa 3: Configurar a autenticação para logon único](#)
- [Configurar o modo SAML Single Sign-on](#)
- [Configurar a conexão do provedor de identidade e as configurações de provisionamento de usuários](#)
 - [Mapeamento de atributo compatível com o Archer para SAML](#)

Mecanismos de autenticação compatíveis

Archer aceita 2 mecanismos básicos de autenticação: Esquema de log-in nome de usuário/senha (padrão) Configuração SSO, que facilita o login do usuário em ambientes de computação corporativa e é compatível com os produtos de autenticação Web mais conhecidos.

O Painel de controle do Archer fornece controles para habilitar o SSO e selecionar um método de SSO. Ao configurar o SSO, você configura a integração LDAP da página Gerenciar configuração de dados LDAP no recurso Controle de acesso.

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

Propriedades do Logon único

A seguinte tabela descreve as propriedades de SSO.

Opção	Descrição
Modo Logon único	<p>Especifica o método de login do usuário. Por padrão, o método está Desativado. Quando você ativa esta opção, o sistema garante acesso ao usuário se ele existir no Archer. Se o usuário não existir, uma consulta LDAP recuperará as informações do perfil do usuário e criará uma conta.</p> <p>As outras opções são: Cabeçalho HTTP. Este método exige um parâmetro de cabeçalho HTTP que identifica o usuário que está tentando acessar o aplicativo. Parâmetro de solicitação. Este método exige um formulário de solicitação ou um parâmetro de string de consulta que identifica o usuário que está tentando acessar o aplicativo. O Windows integrado utiliza a "Autenticação do Windows integrado" incorporada ao IIS (Internet Information Services) que usa as credenciais do usuário via NTLM/Active Directory.Federação. Este método permite que o Archer processe declarações federadas do Windows a partir dos Serviços de Federação do Active Directory (ADFS). Use a Federação para processar declarações geradas diretamente do ADFS. Você também pode configurar o ADFS como provedor de serviços para um provedor de identidade (IDP) SAML 2.0 e converter as asserções SAML 2.0 em declarações federadas.SAML. Este método permite que você configure um provedor compatível com SAML 2.0 para funcionar com o Archer e autenticar com base em asserções SAML de IDPs. Use o ADFS como o provedor de serviços para a opção Federação.</p>
	Especifica o nome de usuário de quem está fazendo login no Archer. Esta opção será obrigatória quando você tiver

Opção	Descrição
Parâmetro do nome de usuário	selecionado o método Parâmetro de solicitação ou Cabeçalho HTTP como Modo Logon único.
Parâmetro do domínio	Especifica o domínio ao qual o usuário pode se conectar. Esta opção é obrigatória quando os métodos Parâmetro de solicitação ou Cabeçalho HTTP estão especificados como Modo Logon único.
Permitir desvio manual	<p>Ativa o login manual. Os usuários podem se conectar ao sistema manualmente adicionando o parâmetro manuallogin com o valor true para string de consulta transmitida a default.aspx. Por exemplo, https://mycompany.archerirm.us/default.aspx?manuallogin=true.</p> <p>Este parâmetro é aplicável às instalações Archer SaaS e às instalações no local do Archer.</p> <p>Quando este parâmetro está na string de consulta, os usuários veem a caixa de diálogo Log-in em vez de transmitir as credenciais de usuário ao aplicativo. Esta opção beneficia um administrador do sistema que faz login com a conta de usuário do Administrador do sistema em vez de fazer com que o SSO envie as credenciais da conta de usuário pessoal.</p>

Opções de autenticação

- SSO para Windows integrado apenas
- SSO para Windows integrado com SSL
- SSL apenas

Procedimento de configuração

Tarefa 1: Ativar autenticação para o Logon único

1. Vá para o Gerenciador de IIS (Internet Information Services, serviços de informações da internet).

2. Habilite a autenticação para os seguintes modos SSO para a conexão da área de trabalho atual do servidor:
 - Para cabeçalho HTTP, habilite a Autenticação anônima.
 - Para o parâmetro de solicitação, habilite a Autenticação anônima.
 - Para a opção integrada com o Windows, habilite a Autenticação do Windows. Para obter mais informações, consulte [Autenticação do Windows](#) na Ajuda do Archer Platform.
 - Para a federação, habilite a autenticação anônima.
 - Para SAML, habilite a Autenticação anônima.

Observação: o Archer exige que somente 1 tipo de autenticação seja habilitado por vez.

3. No Painel de controle do Archer, especifique e depois habilite a instância para a qual você está configurando o SSO.

Tarefa 2: Configurar Single Sign-on

Observação: Você deve ter direitos de administrador do sistema no servidor que está executando o aplicativo da Web Archer.

1. Clique na guia Logon único da instância que você deseja configurar.
 - a. Abra o Archer Control Panel.
 - b. Na lista Gerenciamento de instâncias, clique duas vezes na Instância.
2. No campo Modo Logon único, selecione uma das seguintes opções:
 - Cabeçalho HTTP
 - Parâmetro de solicitação
 - Integrado com o Windows
 - Federação
 - SAML
3. Execute um destes procedimentos:
 - Se tiver selecionado Parâmetro de solicitação ou Cabeçalho HTTP, vá para a próxima etapa.
 - Se tiver selecionado o método Windows Integrated, siga para a etapa 6.
 - Se tiver selecionado Federação, vá para a etapa 7.
 - Se você selecionou SAML, vá para [Configurando o modo Logon único para SAML](#).
4. No campo Parâmetro de nome do usuário, digite o nome do logon do usuário.
5. No campo Parâmetro de domínio, digite o domínio no qual o usuário pode fazer login.
6. Execute um destes procedimentos:
 - Para habilitar o login manual, clique em Permitir desvio manual e vá para a etapa 14.

- Para forçar o SSO independentemente do usuário, vá para a etapa 14.
- 7. Configure as seguintes opções na seção Logon único:
 - a. Selecione Substituir metadados de Federação para ignorar esses metadados no nível das instalações, o que permite que as instâncias utilizem outro provedor de serviços do ADFS.

Observação: qualquer alteração no nome da entidade ou em qualquer certificado no ADFS exige que os metadados sejam importados novamente para o Archer.

- b. Se você selecionou Substituir metadados de Federação, clique em Selecionar para ir para outro arquivo .xml de metadados e, em seguida, selecione o arquivo.

Observação: para obter instruções sobre como obter federationmetadata.xml, consulte a documentação do provedor de serviços. Por exemplo, no ADFS, a URL para obter o arquivo .xml será exibido como `https://{server}/FederationMetadata/2007-06/FederationMetadata.xml`, em que *server* é o nome do seu provedor de serviços.

- c. No campo Identificador de parte dependente, informe esse identificador, fornecido no ADFS para essa instância.
 - d. No campo Parâmetro de realm inicial, digite o nome que você criou para identificar seu realm. Esse nome é o identificador usado na URL intuitiva. A sintaxe para essa string é:

`https://{servername}/../Default.aspx?
<HomeRealmIdentifier>=<IdpRealmName>`

Por exemplo, para ignorar o prompt do provedor de identidade, você pode passar o realm interno como um parâmetro:


`https://{servername}/../Default.aspx?Realm=ADFS-IDP`

- 8. Configure as seguintes opções na seção Provedores de identidade:
 - a. No campo Cabeçalho da página de decisão, digite o texto a ser exibido como cabeçalho na parte superior da página de decisão.
 - b. No campo Rótulo suspenso, digite o texto que deseja exibir na página de decisão como o rótulo do menu suspenso que lista todos os provedores de identidade.
 - c. No campo Provedor de identidade, selecione um IDP existente. Preencha os 3 campos a seguir para adicionar um IDP. Na tabela Federação no final deste procedimento, consulte nomes de declaração compatíveis com o Archer:
 - No campo Realm, digite o nome do realm para o novo provedor de identidade.

- É possível criar um link para o site a seguir para mostrar como configurar o provedor de declaração e a terceira parte confiável no ADFS:

[https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides\(v=ws.10\).aspx](https://technet.microsoft.com/en-us/library/adfs2-step-by-step-guides(v=ws.10).aspx)

- No campo Identificador, informe o identificador do provedor de requisição apropriado que é fornecido no ADFS de um provedor de identidade específico. Para obter uma lista completa das declarações compatíveis com o Archer, consulte a [tabela Nomes de declaração para a opção Federação](#) abaixo.
- No campo Nome de exibição, digite o nome de exibição do novo identificador, que mostrará a lista suspensa da página de decisão.

d. Para adicionar mais provedores, clique em  e preencha os mesmos 3 campos para cada provedor.

9. (Opcional) No campo Em erro de login, digite a URL da página que você criou. O usuário será redirecionado aqui se houver falha de login.
10. (Opcional) No campo Em usuário não encontrado, digite a URL da página que você criou. O usuário será redirecionado aqui se não for possível encontrar o nome de usuário no Archer.
11. (Opcional) No campo Em falha de provisionamento, digite a URL da página que você criou. O usuário será redirecionado aqui se houver falha de provisionamento. Por exemplo, se você excedeu o número máximo de usuários para sua instância.
12. Selecione as Configurações de provisionamento do IDP selecionado, conforme apropriado.
13. Digite o nome, sobrenome e função de usuário padrão que o Archer usa se nenhum nome e função são especificados no momento do provisionamento. Você poderá editar esses valores mais tarde para o novo usuário.
14. Na barra de ferramentas, clique em Salvar.

Nomes de declaração para a opção Federação

Observação: o ADFS espera que as requisições estejam em formato URL, por exemplo <http://schemas.xmlsoap.org/claims/Group>.

A tabela a seguir contém informações de mapeamento de declarações. Os itens marcados obrigatórios.

ArcherNome do campo	Nome/namespace da requisição compo
Informações de identidade do usuário	
Nome de usuário*	UPN*
Domínio	UserDomain
Nome	FirstName
Sobrenome	Sobrenome
Segundo nome	MiddleName
Título	Título
Detalhes de contato	
Endereço de e-mail	EmailAddress
Telefone	PhoneNumber
Nome da empresa	CompanyName
Endereço	FullAddress

ArcherNome do campo	Nome/namespaces da requisição compo
	Rua
	Cidade
	Estado
	CEP
Localização	
Fuso horário	TimeZoneId
Manutenção da conta	
ID do parâmetro de segurança	SecurityParameterId
Grupos/funções de controle de acesso	
Grupo	Grupo
Função	Função

Tarefa 3: Configurar a autenticação para logon único

1. Habilite a sincronização LDAP no IIS.

2. Especifique e ative a instância para a qual você está configurando o SSO.
3. Configure o SSO para a instância.
4. Modifique o arquivo web.config para seu método de autenticação.

Configurar o modo SAML Single Sign-on


1. Permita desvio manual.
 - Habilitado permite ignorar o modo SSO e fazer login usando credenciais do Archer.
 - Desabilitado permite usar apenas SSO por meio de provedores de identidade (IDPs) configurados.
2. Forneça o ID da entidade da instância (obrigatório).
 - O identificador para essa instância atua como um provedor de serviços SAML ao emitir solicitações de autenticação.
 - Os IDs de entidade devem ser exclusivos em instâncias do Archer que usam o mesmo IDP e limitados a 1024 caracteres no formato de URL.
3. Forneça uma impressão digital do certificado. (Atualmente não é compatível no Archer SaaS)
 - Um certificado x.509 é necessário para permitir a assinatura de solicitações SAML e a criptografia de asserções SAML. O Archer assina solicitações quando o IDP exige. O IDP usa o mesmo certificado ao criptografar asserções.
 - Forneça uma impressão digital para o certificado x.509 no Repositório de certificados de máquina local com Windows.
 - A identidade do pool de aplicativos IIS executado pelo Archer exige permissão de leitura de chave privada.
 - Se você usar vários servidores da Web, importe o mesmo certificado para todos os Repositórios de certificados de máquina local.
4. Os metadados do provedor de serviços exportam o XML desses metadados do Archer para uso ao configurar o Archer como um client com o IDP. Os metadados incluem:
 - ID da entidade da instância
 - URL de redirecionamento para o serviço do consumidor de asserção do Archer
 - Preferência no ID de nome necessário
 - Chave pública de assinatura e certificado de criptografia (atualmente não é compatível no Archer SaaS)
 - Preferência para asserções assinadas do IDP

Importante: Salve todas as alterações pendentes antes de gerar metadados. Gere novamente os metadados depois de revisar o ID da entidade da instância ou o URL base.

Importante: gere novamente os metadados depois de revisar o ID da entidade da instância, o URL base ou a impressão digital do certificado.

5. Configure as seguintes opções na seção Provedores de identidade:
 - a. No campo Cabeçalho da página de decisão, digite o texto a ser exibido como cabeçalho na parte superior da página de decisão.
 - b. No campo Rótulo suspenso, digite o texto que deseja exibir na página de decisão como o rótulo do menu suspenso que lista todos os provedores de identidade.

Configurar a conexão do provedor de identidade e as configurações de provisionamento de usuários

1. Preencha os seguintes campos para adicionar um IDP ou selecione um IDP existente na lista para editar. Se você estiver adicionando um segundo IDP ou vários, clique no ícone  e, em seguida, preencha os seguintes itens (obrigatórios):
 - a. No campo Nome de exibição, digite o nome de exibição do novo identificador. O identificador é exibido na lista suspensa na página de decisão de Logon único. O nome de exibição é mostrado quando o URL da instância é fornecido sem o parâmetro IDP.
 - b. No campo Realm, digite o nome do realm para o novo provedor de identidade. O valor do campo Realm, o URL da instância e o nome do parâmetro IDP podem ser usados para ignorar a página de decisão de Logon único.

Exemplo:

- URL da instância: <https://archer.domain.com>
- Realm: CorpIDP

Acessar <https://archer.domain.com/default.aspx?IDP=CorpIDP> ignora a página de decisão e redireciona você imediatamente para CorpIDP para autenticação.

2. Importe metadados SAML do provedor de identidade (obrigatório).
 - a. Clique em Importar e vá para o arquivo .xml de metadados.
 - b. Clique em OK para concluir a importação.

O campo Metadados do IDP mostra o valor de EntityID contido no descritor de entidade dos metadados.

Observação: se a opção Asserções criptografadas necessárias estiver habilitada, o Archer não aceitará asserções não criptografadas do IDP. É preciso especificar uma impressão digital de certificado válida para exigir asserções criptografadas.

3. Selecione as Configurações de provisionamento apropriadas do IDP selecionado (Opcional):
 - Habilite o Provisionamento de usuários. Se não existir uma conta, será criada uma nova conta com base no nome de usuário.
 - Habilite a Atualização de usuário. Informações de perfil, como nome, sobrenome, endereço e endereço de e-mail, são atualizadas sempre que um usuário é autenticado com sucesso por meio do SSO.
 - Habilite a Atualização de grupo. A associação de grupo é atualizada em cada SSO.
 - Habilite a Atualização de função. A atribuição de função é atualizada em cada SSO.
4. Digite o nome, sobrenome e função de usuário padrão (obrigatório). O Archer usa esses padrões se nenhum nome e função são especificados no momento do provisionamento. Você poderá editar esses valores mais tarde para o novo usuário.
5. Clique em Salvar para salvar todas as definições de configuração na guia Single Sign-on.

Observação: qualquer alteração na seção SSO ou IDP não será salva enquanto esta etapa não for concluída.

Mapeamento de atributo compatível com o Archer para SAML

A tabela a seguir contém informações de Mapeamento de atributo compatível com o Archer para SAML. Os itens marcados com um asterisco (*) são obrigatórios.

ArcherNome do campo	Mapeamento de atributo compatível com o Archer
Informações de identidade do usuário	
Nome de usuário*	NameID*

ArcherNome do campo	Mapeamento de atributo compatível com o Archer
Domínio de usuário	UserDomain
Nome	FirstName
Sobrenome	Sobrenome
Segundo nome	MiddleName
Título	Título
Detalhes de contato	
Endereço	FullAddress
	Rua
	Cidade
	Estado
	CEP
Empresa	Empresa

ArcherNome do campo	Mapeamento de atributo compatível com o Archer
Endereço de e-mail padrão	EmailAddress
Telefone 1	PhoneNumber
Localização	
Fuso horário	TimeZoneId
Manutenção da conta	
Parâmetro de segurança	SecurityParameterId
Grupos/Funções de acesso	
Grupos	<p>Grupo/Grupos</p> <p>Use Grupo para atributo de valor único. Use Grupos para atributos de diversos valores.</p>
Funções	<p>Função/Funções</p> <p>Use a função para o atributo de valor único. Use funções para atributos de vários valores.</p>

Observação: para atualizar o endereço do usuário, use 1 das seguintes opções:

- Atributo FullAddress. O campo Endereço no Perfil de usuário é atualizado com os valores fornecidos neste atributo.
- Atributo Rua, cidade, estado, código postal. O campo Endereço é atualizado com os valores de rua, cidade, estado e código postal.

Observação: Consulte Valores de ID de fuso horário compatíveis para obter uma lista de todos os valores de ID de fuso horário compatíveis com o Archer.