# Autenticação

Nesta página

* [SessionContext](#SessionContext)
* [Login](#Login)
  + [Solicitação](#Solicita%C3%A7%C3%A3o)
  + [Cabeçalho da solicitação](#Cabe%C3%A7alhodasolicita%C3%A7%C3%A3o)
  + [Corpo da solicitação](#Corpodasolicita%C3%A7%C3%A3o)
* [Log-out](#Logout)
  + [Solicitação](#Solicita%C3%A7%C3%A3o1)
  + [Cabeçalho da solicitação](#Cabe%C3%A7alhodasolicita%C3%A7%C3%A3o1)
  + [Corpo da solicitação](#Corpodasolicita%C3%A7%C3%A3o1)

## SessionContext

É possível obter um SessionContext passando credenciais válidas ao método de log-in da controladora de segurança. Este SessionContext contém uma string chamada SessionToken que aparece em todas as solicitações subsequentes em um cabeçalho de autenticação personalizado.

**Exemplo:**

Authorization: Archer session-id="D45BB616F3F564B12199F8198522042D"

**Observação:** Informe o ID de token da sessão de seu log-in. Nesta documentação, o id da sessão do Archer é representado como "ID de token do log-in".

Visto que SessionContext é obtido por meio do AuthenticationManager, cada chamada precisa estar em conformidade com as restrições normais de seus parâmetros de segurança associados no Archer. Cada solicitação da API precisa conter um cabeçalho de autenticação válido usando o esquema de autenticação do Archer.

**Importante:** Se o logon único estiver habilitado, selecione Permitir desvio manual no Archer Control Panel para que a API RESTful gere o token de sessão. No entanto, a API de serviços da Web gera tokens de sessão, mesmo que a opção Permitir desvio manual não esteja selecionada. O token gerado pela API de serviços da Web pode ser usado para fazer chamadas de API RESTful. Consulte "Configurando uma instância para single sign-on" na Ajuda do Painel de controle do [Archer](https://help.archerirm.cloud/archer_suite_help/en-us/Content/PortalHome/platform_home.htm).

O segmento Autenticação é acessado por meio da controladora de segurança e inclui os seguintes serviços:

**Importante:** A URL base para chamadas API RESTful mudou na versão 6.5 de /RSAArcher/api/ para /RSAArcher/platformapi/. Se você atualizou de uma versão anterior à 6.5, atualize todas as suas chamadas de API RESTful imediatamente.

## Login

O log-in cria uma sessão do Archer usando as credenciais especificadas na instância especificada. A solicitação de API retorna uma representação serializada de um objeto SessionContext.

### Solicitação

POST http://Archer/platformapi/core/security/login

### Cabeçalho da solicitação

Accept: application/json,text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Content-Type: application/json

### Corpo da solicitação

* {
* "InstanceName":"v5.0",
* "Username":"sysadmin",
* "UserDomain":"",
* "Password":"Archer123"
* }

Exemplo de resposta

* {
* “SessionToken”:” C204E18D0ED58E288533F39C455A36E8”
* }

## Log-out

Este método chama um serviço que encerra a sessão especificada. Se a sessão em questão já foi encerrada ou é inválida, o método ainda retorna verdadeiro. O usuário associado à sessão no cabeçalho de autorização precisa ter as permissões necessárias para encerrar a sessão de outro usuário.

Normalmente, o ID de token da sessão é o mesmo para log-in e log-out, supondo que seja o mesmo usuário. Se um usuário tiver permissões para fazer log-out de outros usuários, o ID de token de sessão de log-out será o do usuário que está sendo desconectado.

### Solicitação

POST http://Archer/platformapi/core/security/logout

### Cabeçalho da solicitação

Accept: application/json,text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8

Authorization: Archer session-id="session token ID from login"

Content-Type: application/json

### Corpo da solicitação

* {
* "Value":"session token ID to logout"
* }