# UpdateSecurityParameter

O método UpdateSecurityParameter permite modificar um parâmetro de segurança existente.

Nesta página

* [Uso](#Uso)
* [Exemplos](#Exemplos)

## Uso

**Privilégios.** Este método requer privilégios de atualização.

**Parâmetros.**

Os parâmetros do método UpdateSecurityParameter são descritos na tabela a seguir.

| Parâmetro | Tipo de dados | Valor |
| --- | --- | --- |
| sessionToken | String | sessionToken válido retornado pelo método [general.CreateUserSession](createusersession.htm) |
| securityParameterId | Número inteiro | ID interno do parâmetro de segurança retornado no elemento xcomp\_sec\_prm\_id depois da chamada a [accesscontrol.GetSecurityParameters](getsecurityparameters.htm) |
| name | String | Nome do parâmetro de segurança |
| Descrição | String | Descrição do parâmetro de segurança |
| minPasswordLength | Número inteiro | Número mínimo de caracteres necessários na senha |
| MinPasswordCharacters | Número inteiro | Número mínimo de caracteres alfabéticos necessários na senha |
| minPasswordNumerals | Número inteiro | Número mínimo de caracteres numéricos necessários na senha |
| passwordLifetime | Número inteiro | Validade da senha em dias |
| graceLogins | Número inteiro | Número máximo de log-ons permitidos após a expiração da senha |
| maxRetries | Número inteiro | Número máximo de vezes que um usuário pode tentar fazer log-on sem sucesso no sistema antes de a conta ser bloqueada |
| lockDuration | Número inteiro | Tempo pelo qual a conta de um usuário permanece bloqueada após ultrapassar número máximo de tentativas |
| lockIntervalType | Número inteiro | Tipo de duração do bloqueio (1 = horas, 2 = minutos e 3 = dias). |
| sessionTimeout | Número inteiro | Duração da inatividade. Após esse tempo, ocorre o timeout da sessão do usuário. A unidade de medida é definida no método timeoutIntervalType |
| passwordHistoryCheckDepth | Número inteiro | Número de senhas anteriores que devem ser controladas e cuja reutilização deve ser evitada. |
| expiratonNotice | Número inteiro | Número de dias para exibição de um aviso antes da expiração da senha |
| accountTimeout | Número inteiro | Número de dias após o qual o status de uma conta é alterado automaticamente para inativo.  0 = nenhum ou nunca desativar automaticamente |
| timeoutIntervalType | Número inteiro | Unidade de medida de sessionTimeout (1 = horas, 2 = minutos e 3 = dias). |
| pinTimeout | Número inteiro | Período máximo de tempo que um PIN permanece ativo antes de o PIN expirar. |
| pinTimeoutType | Número inteiro | Tipo de tempo limite do PIN (1 = horas, 2 = minutos e 3 = dias). |
| pinMaxResendAttempts | Número inteiro | Número de vezes que os usuários podem solicitar um PIN antes que o sistema os impeçam de solicitar PINs adicionais. |
| pinResendLockTimeout | Número inteiro | Período de bloqueio antes que os usuários possam solicitar um PIN após excederem o limite máximo de solicitação de PIN. |
| pinResendLockTimeoutType | Número inteiro | Tipo de tempo limite de bloqueio de reenvio de PIN (1 = horas, 2 = minutos e 3 = dias). |

**Saída.** Este método retorna um número inteiro. Se o método for bem-sucedido, o valor será 1. Se houver uma falha, a API emitirá uma exceção.

## Exemplos

Exemplo de chamada C#

iReturnCode = accesscontrol.UpdateSecurityParameter(sSessionToken, iSecParmID, “newname”, “newdescription”, 6, 2, 2, 11, 17, 7, 1, 1, 31, 7, 3, 23, 1);

Exemplo de solicitação

Veja a seguir um exemplo de solicitação e resposta SOAP 1.1. Os espaços reservados mostrados seriam substituídos por valores reais. SOAP 1.2 também é compatível.

POST /archer/ws/accesscontrol.asmx HTTP/1.1

Host: staging

Content-Type: text/xml; charset=utf-8

Content-Length: **length**

SOAPAction: "http://archer-tech.com/webservices/UpdateSecurityParameter"

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

* <soap:Body>
  + <UpdateSecurityParameter xmlns="http://archer-tech.com/webservices/">
    - <sessionToken>**string**</sessionToken>
    - <securityParameterId>**int**</securityParameterId>
    - <name>**string**</name>
    - <description>**string**</description>
    - <minPasswordLength>**int**</minPasswordLength>
    - <minPasswordCharacters>**int**</minPasswordCharacters>
    - <minPasswordNumerals>**int**</minPasswordNumerals>
    - <passwordLifetime>**int**</passwordLifetime>
    - <graceLogins>**int**</graceLogins>
    - <maxRetries>**int**</maxRetries>
    - <lockDuration>**int**</lockDuration>
    - <lockIntervalType>**int**</lockIntervalType>
    - <sessionTimeout>**int**</sessionTimeout>
    - <passwordHistoryCheckDepth>**int**</passwordHistoryCheckDepth>
    - <expirationNotice>**int**</expirationNotice>
    - <accountTimeout>**int**</accountTimeout>
    - <timeoutIntervalType>**int**</timeoutIntervalType>
    - <pinTimeout>**int**</pinTimeout>
    - <pinTimeoutType>**int**</pinTimeoutType>
    - <pinMaxResendAttempts>**int**</pinMaxResendAttempts>
    - <pinResendLockTimeout>**int**</pinResendLockTimeout>
    - <pinResendLockTimeoutType>**int**</pinResendLockTimeoutType>
  + </UpdateSecurityParameter>
* </soap:Body>

</soap:Envelope>

Exemplo de resposta

HTTP/1.1 200 OK

Content-Type: text/xml; charset=utf-8

Content-Length: **length**

<?xml version="1.0" encoding="utf-8"?>

<soap:Envelope xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">

* <soap:Body>
  + <UpdateSecurityParameterResponse xmlns="http://archer-tech.com/webservices/">
    - <UpdateSecurityParameterResult>**int**</UpdateSecurityParameterResult>
  + </UpdateSecurityParameterResponse>
* </soap:Body>

</soap:Envelope>