Fortalecimento do host

# Fortalecimento do host

Para garantir a operação segura do Archer, os componentes subjacentes do host devem ser reforçados para que o servidor funcione corretamente e as oportunidades de vulnerabilidades sejam removidas.

O Archer recomenda reforçar o sistema host vinculado a ele para permitir apenas TLS 1.2 em todos os clientes e servidores compatíveis com o Archer.

* Verifique se os servidores SQL, web services e os clients têm os service packs mais recentes usando TLS 1.2.
* Certifique-se de que todas as atualizações de segurança sejam aplicadas antes que o reforço adicional seja executado em todos os componentes subjacentes, inclusive, mas sem limitação, sistema operacional, SQL e IIS.

Nesta página

* [Recomendações para reforço de codificação TLS/SSL](#Xb66c8b837104fa66aa531a9b0bc00917d104cbd)
* [Alterações de configuração](#X6d7b08358eea73649619610a590cc74bf98e585)
  + [Desativar o Multi-Protocol Unified Hello](#DesativaroMultiProtocolUnifiedHello)
  + [Desativar PCT 1.0](#DesativarPCT10)
  + [Desativar SSL 2.0](#DesativarSSL20)
  + [Desativar SSL 3.0](#DesativarSSL30)
  + [Desativar TLS 1.0](#DesativarTLS10)
  + [Desativar TLS 1.1](#DesativarTLS11)
  + [Ativar TLS 1.2](#AtivarTLS12)
  + [Desativar codificações não seguras](#Xe979e0c973abc7e40ccdd536952814ebadbc614)
  + [Ativar codificações não seguras](#X8f63017afd6a841a210d35e1f81341b38ef8034)
  + [Desativar algoritmos de hash não seguros](#Desativaralgoritmosdehashn%C3%A3oseguros)
  + [Ativar algoritmos de hash seguros](#Ativaralgoritmosdehashseguros)
  + [Desativar algoritmos de troca de chaves não seguros](#Xd2ce62f3135f7831f5c723f8742ccc56decd735)
  + [Ativar algoritmos de troca de chaves seguros](#Ativaralgoritmosdetrocadechavesseguros)
  + [Configurar o pedido do conjunto de codificações para Strength-Preference e Perfect-Forward Secrecy](#Xc1b6a28e4ef9b09aaa0f073250544f48ab184a7)
  + [Aplicar TLS 1.2 para .NET](#AplicarTLS12paraNET)
  + [Definir TLS 1.2 como padrão para comunicações de saída](#X9ba662074ca150e5ccca5d418ac1324a25b6243)
* [Clients compatíveis](#Clientscompat%C3%ADveis)
* [Verificando a configuração de codificação](#Xfdf779a883b49f36e5a2c0f75c59101b2b3f7d9)

## Recomendações para reforço de codificação TLS/SSL

Quando todos os componentes subjacentes forem atualizados, o reforço por criptografia TLS/SSL poderá ser aplicado. Um conjunto de codificações é um conjunto de algoritmos que ajudam a proteger uma conexão de rede usando TLS (Transport Layer Security). O reforço por codificação impede ataques de codificação conhecidos em TLS/SSL (por exemplo, Sweet32, BEAST, POODLE ou ROBOT). O reforço por codificação também garante que os dados sejam mantidos em segurança e criptografados em trânsito, de acordo com as práticas recomendadas do setor. Para garantir que a configuração da criptografia seja segura para toda a comunicação do Archer, são aplicadas as alterações abaixo nas comunicações do servidor e do client. Como tal, você deve atualizar essas configurações em todo o ambiente de maneira uniforme, caso contrário, podem ocorrer erros de comunicação.

## Alterações de configuração

**Observação:** Para as alterações de registro abaixo, muitos desses caminhos de registro não existirão por padrão. Você precisará criar os caminhos do registro.

### Desativar o Multi-Protocol Unified Hello

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\Multi-Protocol Unified Hello\Client | DisabledByDefault | DWord | 1 |

### Desativar PCT 1.0

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\PCT 1.0\Client | DisabledByDefault | DWord | 1 |

### Desativar SSL 2.0

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0\Client | DisabledByDefault | DWord | 1 |

### Desativar SSL 3.0

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client | DisabledByDefault | DWord | 1 |

**Observação:** Se você desativar o SSL 3.0, poderá bloquear alguns usuários que ainda usam o Windows XP com IE 6 ou IE 7. Sem o SSL 3.0 ativado, não há protocolo disponível para esses usuários retornarem. As certificações de compras mais seguras podem exigir que você desative o SSLv3.

### Desativar TLS 1.0

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.0\Client | DisabledByDefault | DWord | 1 |

### Desativar TLS 1.1

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Server | DisabledByDefault | DWord | 1 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.1\Client | DisabledByDefault | DWord | 1 |

### Ativar TLS 1.2

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server | DisabledByDefault | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client | DisabledByDefault | DWord | 0 |

### Desativar codificações não seguras

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\DES 56/56 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\NULL | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 128/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 40/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC2 56/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 40/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 56/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 64/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\RC4 128/128 | Ativado | DWord | 0 |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\Triple DES 168 | Ativado | DWord | 0 |

### Ativar codificações não seguras

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 128/128 | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Ciphers\AES 256/256 | Ativado | DWord | 0xffffffff |

### Desativar algoritmos de hash não seguros

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\MD5 | Ativado | DWord | 0 |

### Ativar algoritmos de hash seguros

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA256 | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA384 | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Hashes\SHA512 | Ativado | DWord | 0xffffffff |

### Desativar algoritmos de troca de chaves não seguros

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\Diffie-Hellman | Ativado | DWord | 0 |

### Ativar algoritmos de troca de chaves seguros

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\ECDH | Ativado | DWord | 0xffffffff |
| HKLM:\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\KeyExchangeAlgorithms\PKCS | Ativado | DWord | 0xffffffff |

### Configurar o pedido do conjunto de codificações para Strength-Preference e Perfect-Forward Secrecy

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002 | Funções | String | TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256, TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA, TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA |

### Aplicar TLS 1.2 para .NET

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKLM:\SOFTWARE\Microsoft.NETFramework\v2.0.50727 | SystemDefaultTlsVersions | DWord | 1 |
| HKLM:\SOFTWARE\Microsoft.NETFramework\v2.0.50727 | SchUseStrongCrypto | DWord | 1 |
| HKLM:\SOFTWARE\Microsoft.NETFramework\v4.0.30319 | SystemDefaultTlsVersions | DWord | 1 |
| HKLM:\SOFTWARE\Microsoft.NETFramework\v4.0.30319 | SchUseStrongCrypto | DWord | 1 |
| HKLM:\SOFTWARE\Wow6432Node\Microsoft.NETFramework\v2.0.50727 | SystemDefaultTlsVersions | DWord | 1 |
| HKLM:\SOFTWARE\Wow6432Node\Microsoft.NETFramework\v2.0.50727 | SchUseStrongCrypto | DWord | 1 |
| HKLM:\SOFTWARE\Wow6432Node\Microsoft.NETFramework\v4.0.30319 | SystemDefaultTlsVersions | DWord | 1 |
| HKLM:\SOFTWARE\Wow6432Node\Microsoft.NETFramework\v4.0.30319 | SchUseStrongCrypto | DWord | 1 |

### Definir TLS 1.2 como padrão para comunicações de saída

| Caminho do registro | KeyName | Tipo de propriedade | Valor |
| --- | --- | --- | --- |
| HKCU:\Software\Microsoft\Windows\CurrentVersion\Internet Settings | SecureProtocols | DWord | 2048 |
| HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings | SecureProtocols | DWord | 2048 |

## Clients compatíveis

| Client | Versão do TLS |
| --- | --- |
| Android 4.4.2 | TLS 1.2 |
| Android 5.0.0 | TLS 1.2 |
| Android 6.0 | TLS 1.2 > http/1.1 |
| Android 7.0 | TLS 1.2 > h2 |
| Android 8.0 | TLS 1.2 > h2 |
| Android 8.1 | TLS 1.2 > h2 |
| Android 9.0 | TLS 1.2 > h2 |
| BingPreview, janeiro de 2015 | TLS 1.2 |
| Chrome 49/XP SP3 | TLS 1.2 > h2 |
| Chrome 69/Windows 7 R | TLS 1.2 > h2 |
| Chrome 70/Windows 10 | TLS 1.2 > h2 |
| Chrome 80/Windows 10 R | TLS 1.2 > h2 |
| Firefox 31.3.0 ESR/Windows 7 | TLS 1.2 |
| Firefox 47/Windows 7 R | TLS 1.2 > h2 |
| Firefox 49/XP SP3 | TLS 1.2 > h2 |
| Firefox 62/Windows 7 R | TLS 1.2 > h2 |
| Firefox 73/Windows 10 R | TLS 1.2 > h2 |
| Googlebot, fevereiro de 2018 | TLS 1.2 |
| IE 11/Windows 10 R | TLS 1.2 > h2 |
| Edge 15/Windows 10 R | TLS 1.2 > h2 |
| Edge 16/Windows 10 R | TLS 1.2 > h2 |
| Edge 18/Windows 10 R | TLS 1.2 > h2 |
| Edge 13/Windows Phone 10 R | TLS 1.2 > h2 |
| Java 8u161 | TLS 1.2 |
| Java 11.0.3 | TLS 1.2 |
| Java 12.0.1 | TLS 1.2 |
| OpenSSL 1.0.1l R | TLS 1.2 |
| OpenSSL 1.0.2s R | TLS 1.2 |
| OpenSSL 1.1.0k R | TLS 1.2 |
| OpenSSL 1.1.1c R | TLS 1.2 |
| Safari 9/iOS 9 R | TLS 1.2 > h2 |
| Safari 9/OS X 10.11 R | TLS 1.2 > h2 |
| Safari 10/iOS 10 R | TLS 1.2 > h2 |
| Safari 10/OS X 10.12 R | TLS 1.2 > h2 |
| Safari 12.1.2/MacOS 10.14.6 Beta R | TLS 1.2 > h2 |
| Safari 12.1.1/iOS 12.3.1 R | TLS 1.2 > h2 |
| Apple ATS 9/iOS 9 R | TLS 1.2 > h2 |
| Yahoo Slurp, janeiro de 2015 | TLS 1.2 |
| YandexBot, janeiro de 2015 | TLS 1.2 |

**Observação:** Você pode obter segurança adicional removendo as codificações de modo CBC listadas na seção "[Configurar o pedido do conjunto de codificações para Strength-Preference e Perfect-Forward Secrecy](#Configure_cipher_suite_order)". No entanto, os clients a seguir não teriam mais suporte.

| Client | Versão do TLS | Conjunto de codificações |
| --- | --- | --- |
| IE 11/Windows 7 R | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| IE 11/Windows 8.1 R | TLS 1.2 > http/1.1 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| IE 11/Windows Phone 8.1 R | TLS 1.2 > http/1.1 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| IE 11/Windows Phone 8.1 Atualização R | TLS 1.2 > http/1.1 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| Safari 6/iOS 6.0.1 | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| Safari 7/iOS 7.1 R | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| Safari 7/OS X 10.9 R | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| Safari 8/iOS 8.4 R | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |
| Safari 8/OS X 10.10 R | TLS 1.2 | TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 |

## Verificando a configuração de codificação

Você pode usar várias ferramentas para verificar o reforço do conjunto de codificações que você configurou. O reforço do conjunto de codificações pode levar à conectividade limitada, pois os clients antigos não podem se conectar aos servidores com requisitos de segurança fortes. Algumas ferramentas fornecerão detalhes adicionais sobre essas limitações.

Para servidores públicos, é recomendável testar usando o teste da Qualys SSL Labs: [Teste de servidor SSL (desenvolvido pela Qualys SSL Labs).](https://www.ssllabs.com/ssltest/)

Para servidores privados, é recomendável testar usando TestSSL: [/bin/SSL baseado em bash/testador TLS: testssl.sh.](https://testssl.sh/)