Modo de conformidade com FIPS

O FIPS (Federal Information Processing Standard) é um padrão do governo dos Estados Unidos e do Canadá que se destina a garantir a comunicação segura de dados entre sistemas compatíveis. O FIPS 140-2 especifica os Requisitos de Segurança para Módulos Criptográficos, inclusive os algoritmos de criptografia aprovados e algoritmos de hash, além dos métodos para geração e gerenciamento de chaves de criptografia. Para se qualificar na conformidade com FIPS, o Archer deve ser configurado e operado de acordo com os requisitos FIPS 140-2, utilizando componentes e algoritmos certificados FIPS em todas as instâncias necessárias.

Nesta página

- Versão da plataforma compatível com FIPS
  - Requisitos operacionais de conformidade FIPS
- Certificados FIPS
  - Configurar FIPS para Windows
- Configuração FIPS do SQL Server
  - Configurar o navegador para conformidade com FIPS
- Configuração de LDAP para o modo FIPS
- Certificação FIPS da plataforma
  - Padrão SHA (Secure Hash Algorithm) (FIPS 180-4)
  - Algoritmo AES (Advanced Encryption Standard, padrão de criptografia avançada) (FIPS 197)

Versão da plataforma compatível com FIPS

Requisitos operacionais de conformidade FIPS

Você pode configurar a conformidade com FIPS em qualquer sistema Windows compatível com o Archer.

Observação: este requisito se aplica a todos os componentes do Archer.

Você deve configurar os navegadores da Web para a operação FIPS.

Certificados FIPS

Módulos criptográficos certificados FIPS 140-2 passaram por testes e verificação de um laboratório de avaliação aprovado pelo governo. Você pode obter os certificados FIPS necessários no site do NIST (National Institute of Standards and Technology, Instituto Nacional de Padrões e Tecnologia) em:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Para obter uma lista dos certificados aplicáveis ao Archer, consulte Certificação FIPS de plataforma.

Configurar FIPS para Windows

Use a ferramenta Política de segurança local para realizar a configuração FIPS para Microsoft Windows.

Procedimento

1. Faça o log-on no Windows como administrador do sistema Windows.
2. Clique em Iniciar > Painel de Controle.
3. Na janela Painel de Controle, clique em Ferramentas administrativas.
4. Na janela Ferramentas administrativas, clique em Política de segurança local.
5. Na janela Política de segurança local, no painel de navegação, clique em Políticas locais > Opções de segurança.
6. No painel Política, clique duas vezes em Criptografia do sistema: Usar algoritmos compatíveis com FIPS para criptografia, hash e assinatura.
7. Na guia Configuração de segurança local, clique em Habilitado.
8. Clique em Aplicar.
9. Clique em OK.
10. Feche a janela Política de segurança local.

Configuração FIPS do SQL Server

Todas as versões do SQL Server compatíveis com o Archer podem ser configuradas para fins de conformidade com FIPS. Para obter instruções sobre como configurar o FIPS no SQL Server, consulte a documentação do Microsoft SQL Server.

Observação: SQL Server 2017, SQL Server 2017 no Linux (Ubuntu) ou SQL Server 2019 deve estar instalado em um servidor Windows Server

2016 ou 2019. O servidor do Windows deve ser habilitado para FIPS antes de iniciar o SQL Server.

Para a segurança do diálogo entre os serviços, a criptografia utiliza a instância certificada FIPS do AES se o modo FIPS estiver habilitado. Se o modo FIPS estiver desativado, a criptografia usará RC4. Quando um ponto periférico Agente de serviços é configurado no modo FIPS, o administrador deve especificar AES para o Agente de serviços. Se o endpoint é configurado como RC4, o SQL Server gera um erro, e a camada de transporte não inicia.

Mensagens em 2 registros verificam se o SQL Server está sendo executado no modo FIPS:

- Quando o serviço do SQL Server detecta que o modo FIPS está habilitado na inicialização, ele registra esta mensagem no registro de erros do SQL Server:

  O transporte do Service Broker está sendo executado no modo de conformidade FIPS.

- Esta mensagem é registrada no registro de eventos do Windows:

  O transporte do Database Mirroring está sendo executado no modo de conformidade FIPS.

Configurar o navegador para conformidade com FIPS

Além da habilitação do FIPS no sistema host, você deve configurar qualquer navegador da Web usado para se conectar ao Archer para conformidade com FIPS. Para obter mais informações, consulte Configurar FIPS para Windows

Ao usar as versões compatíveis do Microsoft Internet Explorer com a plataforma em modo FIPS, habilite no navegador o TLS 1.2 ou superior. Para obter mais informações, consulte Ambientes qualificados e compatíveis.

1. Abra o Internet Explorer.
2. Clique em Ferramentas e depois em Opções da Internet.
3. Na guia Ferramentas avançadas:
   a. Verifique se as opções Usar TLS 1.0 e Usar TLS 1.1 estão desmarcadas.
   b. Selecione Usar TLS 1.2.
4. Observe que as opções Usar SSL 2.0 e Usar SSL 3.0 são desmarcadas.

Configuração de LDAP para o modo FIPS

Observação: O Archer supõe que o Microsoft Active Directory seja usado como servidor LDAP. Para outros tipos de servidores LDAP, consulte a documentação específica do produto.

As conexões com o Active Directory a partir do Archer podem ser criptografadas ou não criptografadas. Se você pretende criptografar as conexões, deverá configurar o Active Directory com um certificado de servidor. Você pode conseguir isso com um certificado de servidor no Windows Server, que instala o certificado de servidor usando o registro automático no Active Directory.

Para configurar o Active Directory no modo FIPS, o servidor Windows que hospeda o Active Directory deve ser habilitado para FIPS.

Certificação FIPS da plataforma

As tabelas a seguir apresentam os certificados FIPS dos componentes criptográficos que o Archer usa.

Padrão SHA (Secure Hash Algorithm) (FIPS 180-4)

Algoritmo	Sistema operacional	Número do certificado
SHS	Windows Server 2016	#3347
	Windows Server 2019	#C211

Algoritmo AES (Advanced Encryption Standard, padrão de criptografia avançada) (FIPS 197)

Algoritmo	Sistema operacional	Número do certificado
AES	Windows Server 2016	#4064

Algoritmo	Sistema operacional	Número do certificado
	Windows Server 2019	#C211