Orientação para certificados SSL

Para habilitar a criptografia de campo no Archer, é aconselhável que o certificado seja obtido de uma CA (Certificate Authority, autoridade de certificação) confiável. No entanto, você pode optar por gerar um certificado autoassinado.

É recomendável o uso de um HSM (Hardware Security Module, módulo de segurança de hardware) para a criptografia de campo, em vez de um certificado em um armazenamento local.

Nesta página

Requisitos de certificado para criptografia de campo

Os certificados devem atender aos seguintes requisitos:

- O certificado está presente na área de armazenamento da máquina local como um certificado pessoal.
- O certificado é exportável.
- O certificado não está expirado.
- O certificado tem um tamanho de chave de 2048 bits.
- O certificado tem uma chave privada.

Como proteger um certificado de criptografia de campo

O certificado que está sendo usado para criptografia deve ter acesso muito limitado. Aqui estão algumas das medidas de segurança que devem ser tomadas para proteger o certificado:

- Conceder controle total e acesso de leitura ao certificado apenas para a conta de administrador. Todas as outras contas devem ter acesso somente leitura.
- Dar ao certificado acesso somente leitura às contas a seguir:
  - Em um servidor que hospeda o aplicativo da Web do Archer, somente a conta AppPool usada pelo aplicativo da Web deve ter acesso (somente leitura) ao certificado.
  - Em um servidor que hospeda serviços do Archer, por exemplo, serviço de configuração e framework de trabalho, somente as contas usadas pelos serviços devem ter acesso (somente leitura) ao certificado.
- Revogar o acesso de todas as contas que não são necessárias.
- Fazer backup do certificado de criptografia regularmente. O backup deve ser protegido por senha e armazenado em segurança.

Para obter recomendações sobre como gerar/instalar um certificado SSL usando o IIS, consulte a Microsoft TechNet Library.

Para obter informações sobre as práticas recomendadas do setor, consulte:

- NIST SP 800-52
- PCI-DSS v3.2.1 – Maio de 2018