Cloud Integration Option Pack

Cree y controle las claves criptográficas en su HSM FIPS 140-2, y exporte posteriormente de forma segura a la nube

PRINCIPALES CARACTERÍSTICAS

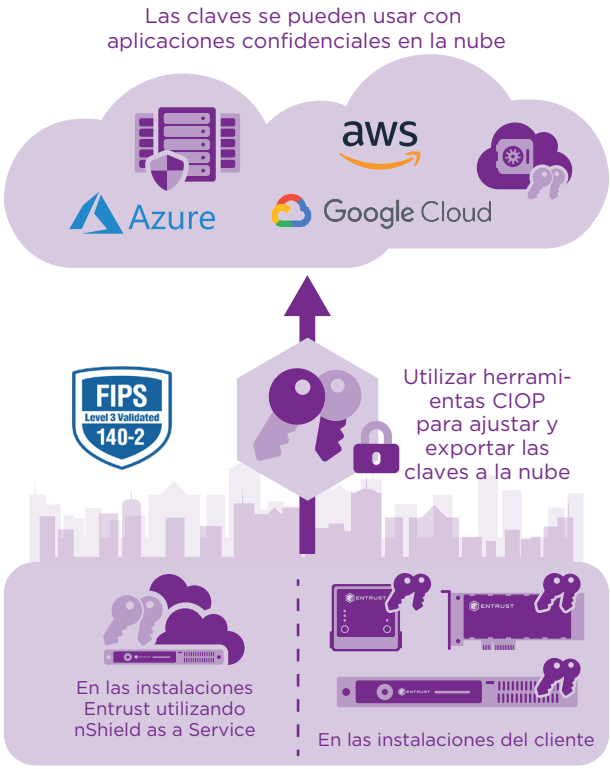
A los usuarios de servicios de la nube pública, les brinda la capacidad de generar claves criptográficas en sus propios entornos y mantener el control de esas claves, al tiempo que las pone a disposición, según sea necesario, para su uso en la nube de su elección.

- Control de sus claves criptográficas que apoyan una estrategia de nube múltiple o híbrida
- Asegura la generación de claves utilizando una fuente sólida entrópica
- Protección de claves a largo plazo utilizando un HSM con certificado FIPS
- Compatible con Amazon Web Services, Google Compute Engine, Microsoft Azure

Protege sus claves en la nube con los niveles de seguridad más alta

Protege su marca y sus datos

Validados por los estándares de seguridad más altos, como FIPS 140-2 y Common Criteria, los HSM nShield de Entrust están preparados para proteger sus datos incluso en las situaciones de seguridad más complicadas y desafiantes, tanto en las instalaciones o en la nube.



Las claves de encriptación son generadas en un HSM nShield, cifradas y exportadas de forma segura a la nube

APRENDA MÁS EN ENTRUST.COM/HSM

Cloud Integration Option Pack

Proveedores de servicio de la nube compatibles

El Cloud Integration Option Pack ofrece las herramientas que le permite crear sus claves criptográficas usando un HSM nShield y después adaptarlas y exportarlas de forma segura a los siguientes proveedores de servicio de la nube:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (usando el mecanismo BYOK de Azure)

Para los clientes que buscan un nivel de seguridad más alto, Microsoft ofrece nCipher BYOK. El método nCipher BYOK proporciona garantías adicionales de que los permisos de claves creados en el momento de generación se conservan durante la transferencia a Microsoft Azure Key Vault. Además, Microsoft utiliza nCipher Security World para restringir el uso de claves a una región específica de Azure. Este método no necesita la compra de CIOP. Véase **Importar claves protegidas de HSM a Key Vault (nCipher)** para más información.

Control de claves en entornos de nube híbrida y múltiples nubes

Cloud Integration Option Pack proporciona a los clientes el control y la seguridad que necesitan cuando se implemente una estrategia de nube híbrida, un proveedor de servicio de nube único o una estrategia de nubes múltiples. Al llevar sus claves criptográficas al proveedor de servicios en la nube, evita las dificultades asociadas con el bloqueo del proveedor, lo que puede dificultar la migración de un proveedor de servicios en la nube a otro.

Configuraciones soportadas

- Requiere nShield Security World Software v12.60 y firmware v12.60 o posterior para Azure BYOK
- Requiere nShield Security World Software v12.40 software para AWS y buscador informático de Google
- Se ha comprobado la compatibilidad de esta versión con una serie de plataformas incluidas:
  - Microsoft Windows Server 2019 x64 y 2016 x64
  - Microsoft Windows 10 x64 y 7 x64
  - Red Hat Enterprise Linux 7 x64 y AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 y 11 x64
  - Oracle Enterprise Linux 7.6 x64 y 6.10 x64
- Compatibilidad HSM
  - Compatibles con todos los modelos nShield actuales

Más información

Para saber más sobre los HSM nShield de Entrust visite **entrust.com/HSM**. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Más información
entrust.com/HSM

Contacte con nosotros:
HSMinfo@entrust.com