

# Módulos de seguridad de Alcatel-Lucent Enterprise

## Server Security Module (SSM), Media Security Module (MSM)



Los módulos de seguridad de Alcatel-Lucent Enterprise proporcionan continuidad de las actividades empresariales y protección de la información para las comunicaciones empresariales de voz sobre IP ofreciendo protección de la integridad del software y los protocolos

y también comunicaciones cifradas. La arquitectura de seguridad se basa en tecnología de Thales®, un proveedor líder en el mercado de la seguridad.

Los módulos de seguridad son dispositivos montados en rack que protegen las comunicaciones empresariales basadas en IP frente a ataques de denegación de servicios y de robo de información. Un módulo de seguridad del servidor (Server Security Module, SSM) protege las comunicaciones empresariales entre los servidores de comunicaciones de Alcatel-Lucent Enterprise y teléfonos IP, Media Gateways IP y enlaces SIP. Los módulos de seguridad de medios (Media Security Module, MSM) protegen las comunicaciones con servidores de aplicaciones que gestionan flujos de medios IP como la grabación, la mensajería o servidores de conferencias.

Funciones	Ventajas
Descarga protegida de archivos binarios y de configuración en teléfonos IP y Media Gateways IP Señalización de control de llamada y cifrado de medios	Protección de la información: prevención de ataques maliciosos, ataques de suplantación en teléfonos IP y escuchas no autorizadas de las comunicaciones.  Cumplimiento: garantice que su empresa cumple con las normas de dirección y privacidad internas y externas.
Autenticación mutua de todos los equipos e integridad de la señalización de control de llamada (que garantiza que no se han modificado los mensajes)	Continuidad de las actividades empresariales: proteja sus comunicaciones empresariales contra ataques de denegación de servicio.
Integración perfecta con OmniPCX® Enterprise Communication Server	Operaciones rentables: implante procesos de seguridad de alto nivel sin entorpecer la administración del sistema.
Repercusión nula sobre las opciones de Calidad de servicio (QoS) y la configuración de la red	Simplicidad: no afecta a la infraestructura de la red
Compatibilidad con redundancia geográfica	Continuidad empresarial: proporcione comunicaciones empresariales seguras en caso de fallos de red, del servidor o del Data Center

Como integrador de sistemas de valor añadido y proveedor de equipos y servicios, Thales es una de las empresas líderes de Europa en el mercado de la seguridad. Los equipos de seguridad de Thales colaboran con administraciones estatales, autoridades locales y clientes de empresas para desarrollar y desplegar soluciones resistentes integradas para proteger a los ciudadanos, datos confidenciales e infraestructuras críticas.



Gracias a sus potentes capacidades criptográficas, Thales es uno de los líderes mundiales en productos y soluciones de ciberseguridad para infraestructuras estatales y militares críticas y redes de satélites, así como empresas industriales y financieras. Con presencia en toda la cadena de seguridad, Thales ofrece una completa gama de servicios y soluciones, desde la consultoría de seguridad, la detección de intrusiones y el diseño de arquitecturas hasta la certificación de sistemas, el desarrollo y la gestión de productos y servicios durante todo su ciclo de vida, y también la supervisión de la seguridad con centros de operaciones de seguridad en Francia y el Reino Unido.

## Especificaciones técnicas

### Especificaciones físicas

#### Dimensiones

- Dispositivos de 482 mm (19 pulgadas) con factor de forma 1U montados en rack
  - Anchura: 371 mm (14,6 pulgadas)
  - Profundidad: 215 mm (8,5 pulgadas)
  - Altura: 43,6 mm (1,7 pulgadas)
- Peso: 2,5 kg (5,5 libras) (accesorios incluidos)

#### Fuente de alimentación

- Tensión de entrada de 110/220 V CA
  - 50/60 Hz
  - 40 W

#### Entorno operativo

- De -5 °C a +45 °C
- Humedad relativa del 5% al 95%

#### Entorno de almacenamiento

- De -25 °C a +55 °C
- Humedad relativa del 5% al 95%

#### MTBF

- Ground fijo a 25 °C: 88.000 horas

#### Interfaces de red

- Consola: Puerto 1 RJ-45 (RS232C)
- Puertos de red:
  - Sin cifrado: 4 puertos conmutados RJ-45 Gigabit Ethernet
  - Con cifrado: 1 puerto RJ-45 Gigabit Ethernet

### Seguridad

#### Cifrado

- AES-CBC 128 bits, AES-CM 128 bits
- Señalización:
  - Teléfonos IP, Alcatel-Lucent Media Gateways OmniPCX Enterprise y Passive Communication Server (PCS), servidores de aplicaciones: modo de transporte IPSEC
  - Enlaces públicos SIP: TLS

- Voz: SRTP

- IPV4 e IPV6

#### Autenticación mutua y control de integridad

- AES-XCBC (128 bits), HMAC-SHA1 (160 bits)
- Certificaciones X.509 (RSA 2048 bits)

#### Administración

- Actualización de software protegida centralizada:
  - SSM
  - MSM
  - Teléfonos IP
  - Media Gateways
- Centro de personalización de claves

#### Calidad de servicio (QoS)

- Preserva las etiquetas 802.1p/q
- Gestiona etiquetas de QoS de capa 3

### Protección mediante SSM

- Servidores de comunicaciones (CS):
  - OmniPCX Enterprise CS versión 11.1 y posteriores
  - Redundancia de servidores OmniPCX Enterprise CS
  - Redes OmniPCX Enterprise CS ABC
  - Alcatel-Lucent OpenTouch® Business Edition 2.1 y posteriores
- Media Gateways:
  - Seguridad incorporada
  - Tarjetas GD3, GA3, INTIP3
- Teléfonos IP:
  - Seguridad incorporada
  - Alcatel-Lucent 8018, 8028, 8038, 8068, 8028S, 8058S, 8068S, 8078S Premium DeskPhones
  - Teléfonos Alcatel-Lucent 4028, 4038, 4068 IP Touch®

### Protección mediante MSM

- OmniPCX Enterprise PCS
- Media Gateways: tarjetas existentes sin seguridad integrada
- Servidores de aplicaciones:
  - OpenTouch Multimedia Services
  - OpenTouch Message Center
  - Alcatel-Lucent 4645 Voice Messaging Services
  - OmniPCX RECORD Suite
  - Grabadoras externas que utilizan el protocolo IP DR-Link

### Normativa

- Marca CE
- Marca ETL
- FCC parte 15 B
- ICES 003
- ROHS

### Prestaciones de la plataforma

	SSM	MSM
Teléfonos IP por SSM (máx.)	15 000	-
Media Gateways por SSM (máx.)	240	-
Comunicaciones cifradas simultáneas por MSM al proteger PCS o servidores de aplicaciones (máx.)	-	400
Tramos de grabación cifrados simultáneos por MSM al proteger grabadoras IP DR-Link (máx.)	-	800