



LA-20-07-17

Instalación de IDProtect Client - Linux

Antes de Comenzar

Para poder utilizar el Token USB/Smartcard MS-IDProtect provisto por Macroseguridad.org en una distribución Linux deberá tener instalado el middleware IDProtect Client. De no ser así, por favor instálelo y luego continúe con esta guía. Si tiene dudas o consultas por favor ingrese a nuestro portal de soporte y realice la consulta que desee <https://soporte.macroseguridad.la> .

El middleware provisto por Macroseguridad.org de MS-IDProtect incluye todos los drivers necesarios para que su sistema detecte automáticamente el dispositivo criptográfico y le permita generar on board en el Token USB sus certificados digitales. Además contiene una importante herramienta para la administración del dispositivo llamada “IDProtect Manager”. Esta herramienta le permitirá cambiar el PIN que viene por defecto por otro que usted desee, cambiar el nombre del dispositivo criptográfico para poder identificarlo con mayor facilidad, y poder exportar e importar certificados desde y hacia el dispositivo criptográfico.

Requisitos

- ☞ Sistemas Operativos:
 - ✓ Ubuntu 12.x, 13.x, 14.x, 15.x y 16.x (X86 y X64)
 - ✓ Fedora 23 , Fedora 24, Fedora 25 y Fedora 26 (X86 y X64)
 - ✓ Debian 7, Debian 8 y Debian 9 (X86 y X64)
 - ✓ Redhat 5.x, Redhat 6.x y Redhat 7.x (X86 y X64)
 - ✓ CentOS 5.x, CentOS 6.x y CentOS 7.x (X86 y X64)
 - ✓ SuSE 11, SuSE 12 y OpenSuSE (X86 y X64)
- ☞ Puerto USB habilitado.
- ☞ MS-IDProtect listo para usar.
- ☞ pcscd: se debe encontrar instalado y ejecutandose. Se recomienda establecer que pcscd se ejecute automáticamente al iniciar el sistema.



- ☞ CCID: se deben encontrar instaladas las librerías CCID.
- ☞ pcsc-lite: se deben encontrar instaladas las librerías pcsc-lite.
- ☞ openct y openct: las librerías openct y openct NO SE DEBEN ENCONTRAR INSTALADAS. Si se encuentran instaladas, por favor desinstálelas antes de realizar la instalación.
- ☞ El módulo PKCS#11 puede ser adicionado automáticamente por el instalador (DEB o RPM). Para esto se requiere que se encuentren instaladas las herramientas “*Network Security Service tools*” (Mozilla-nss-tools) y que Mozilla Firefox haya sido abierto al menos una vez antes de realizar la instalación. Mozilla Firefox se debe encontrar cerrado durante la instalación.
- ☞ Poseer permisos de root o administrador en el equipo.

Las pruebas desarrolladas en esta guía se han realizado bajo las plataformas **Ubuntu y CentOS**.

Importante: Si el dispositivo criptográfico provisto por MACROSEGURIDAD es utilizado apropiadamente y conforme su destino, en el entorno recomendado y con los PINES correctos, el mismo no bloquea en ningún caso el acceso a la información.

Si esto ocurre, no es por un defecto del producto, sino que, cumpliendo su finalidad, se produce para el resguardo de la información contenida en el dispositivo ante intentos no autorizados o erróneos (por impericia o negligencia del usuario).

Se debe tener especial cuidado y precaución en el manejo del dispositivo en el entorno recomendado, así como en el resguardo y respaldo de PINES de USUARIO y/o ADMINISTRADOR. Al adquirir el producto, el Usuario se compromete a seguir TODAS las recomendaciones técnicas provistas por MACROSEGURIDAD y ante cualquier duda, consultar al equipo de soporte técnico en <https://soporte.macroseguridad.la>



Instalación en sistemas operativos basados en Debian

1) Primero debe Instalar/actualizar librerías pc/sc y CCID necesarias para instalar el middleware IDProtect cliente desde los repositorios de su distribución:

Utilizando apt-get

```
sudo apt-get update
```

```
sudo apt-get install pcscd pcsc-tools libccid libpcsclite1
```

Utilizando aptitude

```
sudo aptitude update
```

```
sudo aptitude install pcscd pcsc-tools libccid libpcsclite1
```

2) Ahora debe instalar el middleware con la siguiente línea de comandos ("x.xx.xx-x" corresponde a la versión actual del middleware):

En sistemas operativos de 32 bits ejecute:

```
sudo dpkg -i idprotectclient_x.xx.xx-x_i386.deb
```

En sistemas operativos de 64 bits ejecute:

```
sudo dpkg -i idprotectclient_x.xx.xx-x_amd64.deb
```

```
sudo dpkg -i idprotectclientlib_x.xx.xx-x_amd64.deb
```

```
labuser@ubuntu-vm-1604: ~
labuser@ubuntu-vm-1604:~$ sudo dpkg -i idprotectclient_7.12.05-0_amd64.deb
Seleccionando el paquete idprotectclient previamente no seleccionado.
(Leyendo la base de datos ... 212135 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar idprotectclient_7.12.05-0_amd64.deb ...
Desempaquetando idprotectclient (7.12.05-0) ...
Configurando idprotectclient (7.12.05-0) ...
Procesando disparadores para desktop-file-utils (0.22-1ubuntu5.1) ...
Procesando disparadores para bamfdaemon (0.5.3-bzr0+16.04.20160824-0ubuntu1) ...
Rebuilding /usr/share/applications/bamf-2.index...
Procesando disparadores para gnome-menus (3.13.3-6ubuntu3.1) ...
Procesando disparadores para mime-support (3.59ubuntu1) ...
labuser@ubuntu-vm-1604:~$ sudo dpkg -i idprotectclientlib_7.12-0_amd64.deb
Seleccionando el paquete idprotectclientlib previamente no seleccionado.
(Leyendo la base de datos ... 212178 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar idprotectclientlib_7.12-0_amd64.deb ...
Desempaquetando idprotectclientlib (7.12-0) ...
Configurando idprotectclientlib (7.12-0) ...
labuser@ubuntu-vm-1604:~$
```



3) Al finalizar, si no se muestra ningún mensaje de error, IDProtect Client se encontrará instalado. Conecte un MS-IDProtect para e inicie IDProtect Manager para verificar que su Token USB sea correctamente reconocido.

Luego de la instalación las librería PKCS#11 se encontrarán en

☞ /usr/lib/x86-athena/libASEP11.so

☞ /usr/lib/x64-athena/libASEP11.so

Instalación en sistemas operativos basados en RedHat

1) Primero debe Instalar/actualizar librerías pc/sc y CCID necesarias para instalar el middleware IDProtect cliente desde los repositorios de su distribución:

Utilizando yum:

```
sudo yum install ccid pcsc-lite
```

Utilizando dnf

```
sudo dnf install ccid pcsc-lite
```

2) Ahora debe instalar el middleware con la siguiente línea de comandos ("x.xx.xx-x" corresponde a la versión actual del middleware):

En sistemas operativos de 32 bits ejecute:

```
sudo rpm --import GPG-KEY-athena.key
```

```
sudo rpm -i idprotectclient-x.xx.xx-x.i386.rpm
```

En sistemas operativos de 64 bits ejecute:

```
sudo rpm --import GPG-KEY-athena.key
```

```
sudo rpm -i idprotectclient-x.xx.xx-x.x86_64.rpm
```

```
sudo rpm -i idprotectclientlib-x.xx.xx-x.x86_64.rpm
```



```
labuser@centos7x64:~  
Archivo Editar Ver Buscar Terminal Ayuda  
[labuser@centos7x64 ~]$ sudo rpm --import GPG-KEY-athena.key  
[labuser@centos7x64 ~]$ sudo rpm -i idprotectclient-7.12.05-0.x86_64.rpm  
[labuser@centos7x64 ~]$ sudo rpm -i idprotectclientlib-7.12-0.x86_64.rpm  
[labuser@centos7x64 ~]$
```

3) Al finalizar, si no se muestra ningún mensaje de error, IDProtect Client se encontrará instalado. Conecte un MS-IDProtect para e inicie IDProtect Manager para verificar que su Token USB sea correctamente reconocido.

Luego de la instalación las librería PKCS#11 se encontrarán en

- ☞ /usr/lib/x86-athena/libASEP11.so
- ☞ /usr/lib/x64-athena/libASEP11.so

Para mayor información contacte al equipo de Tecnología de MacroSeguridad por el medio que usted prefiera

- ☞ Mail: soporte@macroseguridad.net
- ☞ Portal de soporte: <https://soporte.macroseguridad.la>
- ☞ Web: www.macroseguridad.net