

The Simarks logo is displayed in a bold, black, sans-serif font. A small red triangle is positioned above the letter 'i'. The logo is centered horizontally and overlaid on a background of a grey, textured wall with a grid of rectangular panels.

simarks

Simarks™ Deployment Manager SDM™

White Paper

Simarks Software - cybersecurity

Índice

Introducción	3
Funcionalidades	3
<i>Gestión de aplicaciones – Autoservicio</i>	4
<i>Despliegue desatendido – Sistema tradicional</i>	5
<i>Línea de Comandos</i>	6
<i>Aplicaciones en ejecución</i>	7
<i>Gestión de dependencias</i>	8
<i>Portal de tareas administrativas</i>	8
<i>Inventarios</i>	9
<i>Scripting</i>	9
<i>Entornos</i>	9
<i>Repositorios</i>	10
Ventajas	11
<i>Integración con Directorio Activo</i>	11
<i>Gestión centralizada e integración con SIEM</i>	11
Requerimientos	12

Simarks™ SDM™

Aviso Legal

Copyright ©2018 Simarks™ Software. Todos los derechos reservados.

Este documento contiene información que está protegida por las leyes de copyright. Ninguna de sus partes puede ser fotocopiada, reproducida o traducida a otro idioma sin el previo consentimiento expreso y por escrito de Simarks Software.

Todos los nombres de marcas y nombres de producto utilizados en este documento son marcas registradas o nombres comerciales pertenecientes a sus respectivos propietarios. Simarks Software no mantiene ningún acuerdo de asociación o de cualquier otro tipo con ninguno de los vendedores o productos mencionados en este documento.

Garantías

ESTE DOCUMENTO SE PROPORCIONA "TAL COMO ESTÁ" Y SE EXCLUYEN TODAS LAS CONDICIONES, REPRESENTACIONES Y GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS CUALQUIER GARANTÍA IMPLÍCITA DE COMERCIABILIDAD, ADECUACIÓN A UN FIN DETERMINADO O NO INFRACCIÓN, EXCEPTO EN LA MEDIDA EN QUE TALES DECLARACIONES DE RESPONSABILIDAD PUDIERAN SER LEGALMENTE INVÁLIDAS. SIMARKS NO SERÁ RESPONSABLE POR LOS DAÑOS INCIDENTALES O CONSECUENTES EN RELACIÓN CON EL USO DE ESTE DOCUMENTO. LA INFORMACIÓN CONTENIDA EN ESTE DOCUMENTO ESTÁ SUJETA A CAMBIOS SIN PREVIO AVISO.

Simarks Software S.L.
C/ Copenhagen 12 – Edificio Titan
28232 Las Rozas de Madrid - Spain.



www.simarks.com

Introducción

La gestión de aplicaciones sigue siendo uno de los problemas sin resolver de forma eficaz en organizaciones a partir de un número de puestos de trabajo. La elección entre seguridad y productividad lleva a decisiones estratégicas que no proporcionan una solución adecuada de forma conjunta, ya que cuanto más seguro es un sistema menos productivo es. Normalmente, son necesarios permisos de administrador para realizar la instalación de aplicaciones o cualquier modificación en la configuración del sistema, y los sistemas operativos carecen de la flexibilidad necesaria para no penalizar ni la seguridad ni la productividad.

Asimismo, la gestión de aplicaciones forma parte activa de la seguridad integral de una organización ya que es uno de los principales motivos por los que se otorgan permisos de administrador a los usuarios finales.

Simarks Deployment Manager (SDM™) está basado en la tecnología patentada de gestión de privilegios a nivel de proceso de Simarks, y ofrece una solución con un enfoque completamente diferente e innovador.

No solo está especializada en la gestión de aplicaciones en el momento de la instalación, desinstalación, actualización, etc., sino que además gestiona los permisos que la aplicación necesite en el momento de la ejecución. Todo ello sin necesidad de otorgar permisos adicionales al usuario final.

Con SDM es posible construir un “Portal Corporativo de Aplicaciones” donde es el usuario final quien consume las aplicaciones a las que tiene autorización sin necesidad de otorgarle permisos elevados. Esta aproximación permite la implementación completa del “Principio de Menor Privilegio” sin afectar a la productividad.

Funcionalidades

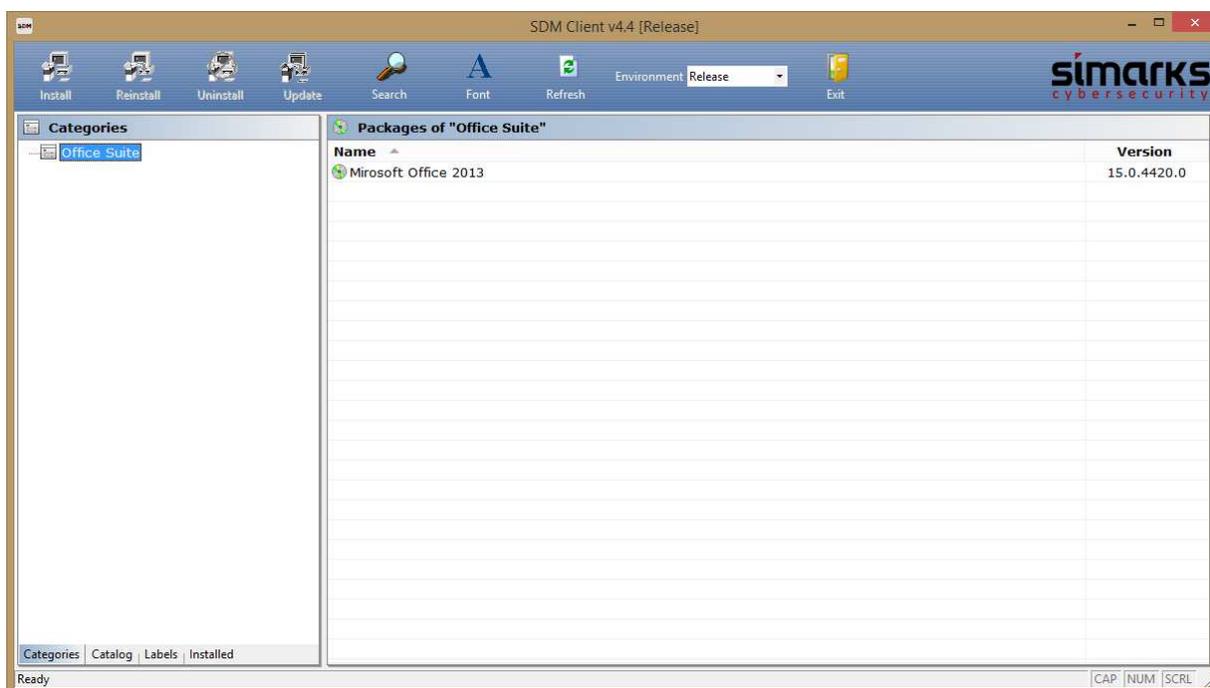
Las funcionalidades principales de SDM son:

- ✓ Autoservicio de Aplicaciones a través del Portal Corporativo de Aplicaciones.
- ✓ Gestión de Dependencias, actualizaciones, parches y *service packs*.
- ✓ Delegación de tareas administrativas en el usuario final sin necesidad de otorgarle permisos de administrador.
- ✓ Diferentes entornos (test, pre-producción y producción) bajo una misma instancia de Directorio Activo, completamente integrados entre sí.
- ✓ Repositorio de Software Distribuido en base a los *Sites* de Directorio Activo que permite al usuario final acceder a su repositorio más cercano.
- ✓ Ejecución de tareas programadas.
- ✓ Amplia gama de filtros.
- ✓ Distribución Urgente.

- ✓ Inventario de Hardware y Software.
- ✓ Informes.

Gestión de aplicaciones – Autoservicio

Mediante el Portal Corporativo de Aplicaciones el usuario puede visualizar todas las aplicaciones del catálogo, pero solamente podrá instalar aquellas que el administrador de la herramienta haya autorizado para él. Esta autorización está basada en una amplia gama de filtros, tanto de inclusión como de exclusión, incluyendo usuario, grupo, equipo, marca, modelo, departamento, subred, sitio, rol, versión del S.O., 32/64 bits, etc.



Las soluciones tradicionales se basan en la utilización de cuentas con permisos de administrador que, en la mayoría de los casos, es diferente del usuario que finalmente hace uso de las aplicaciones. Esto conlleva un tedioso problema que requiere de un laborioso proceso de remediación y configuración que debe realizarse después de la instalación y que alarga considerablemente el plazo de integración de nuevas aplicaciones además del riesgo por compromiso de la contraseña. SDM realiza la instalación bajo la cuenta del usuario final, evitando así estos problemas.

Ya que las aplicaciones las instala el propio usuario, que es quién las va a usar, las aplicaciones no requieren de tratamiento porque se utiliza el medio original (o un volcado en el repositorio de software) para la integración en la herramienta. Por ello, la integración en SDM de la mayoría de aplicaciones del mercado es prácticamente inmediata.

SDM soporta todas las versiones de Windows desde XP a Windows 10 (32 y 64 bits).

Despliegue desatendido – Sistema tradicional

Aunque enfocado al autoservicio, SDM ofrece un sistema completo y mejorado de distribución tradicional y desatendida. En base a una avanzada configuración, cualquier aplicación o tarea administrativa se puede ejecutar en la organización de forma automática.



Además posibilita el despliegue de aplicaciones de forma escalonada evitando la saturación de la red, y permite que una misma aplicación pueda ser desplegada de forma automática para usuarios que cumplan determinados filtros mientras que a otros se les ofrece la posibilidad de instalar la misma aplicación bajo demanda.

El despliegue de tareas y aplicaciones desatendidas se puede realizar en base a una amplia gama de filtros, tanto de inclusión como exclusión (usuario, grupo, equipo, modelo, marca, departamento, subred, sitio, role, versión del S.O., arquitectura de 32/64 bits, etc.), y se clasifican mediante diferentes tipos de categorías:

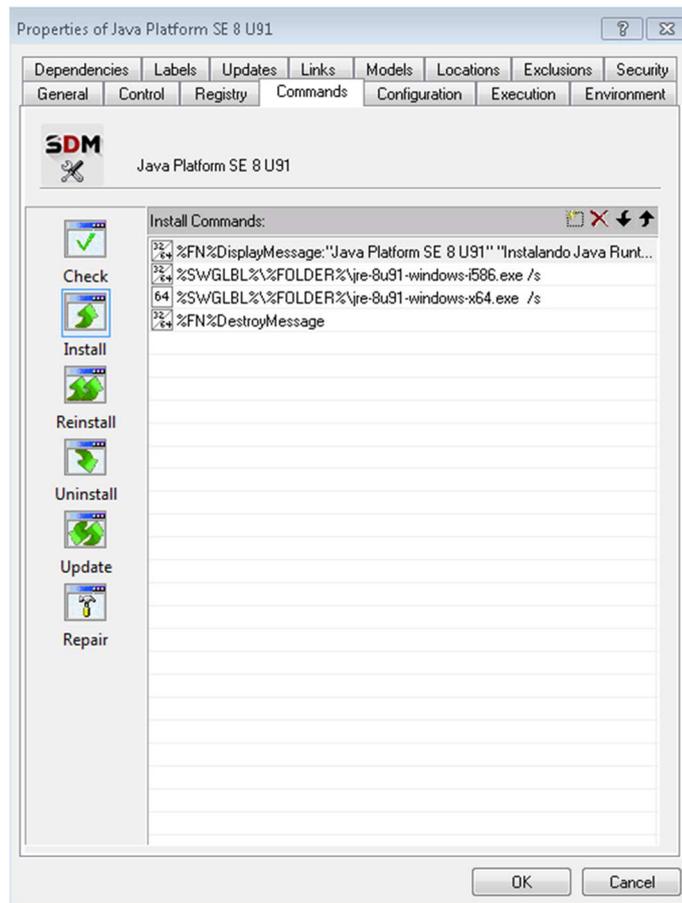
- **Obligatorias** – Instalación automática de aplicaciones obligatorias basada en los filtros.
- **Desinstalación** – Desinstalación automática de aplicaciones, independientemente de si han sido instaladas a través de SDM o no.
- **Actualización** – Actualización automática de productos ya instalados, con gestión de parches y *Service Packs*.
- **Periódicas** – Ejecución periódica y automática de tareas administrativas.

- Reparación – Ejecución de comandos con el fin de resolver incidencias ejecutando tareas, o como aplicaciones que ya están instaladas y necesitan ser reparadas.
- Emergencia – Posibilidad de ejecutar comandos específicos en cuestión de minutos en caso de emergencia.

Línea de Comandos

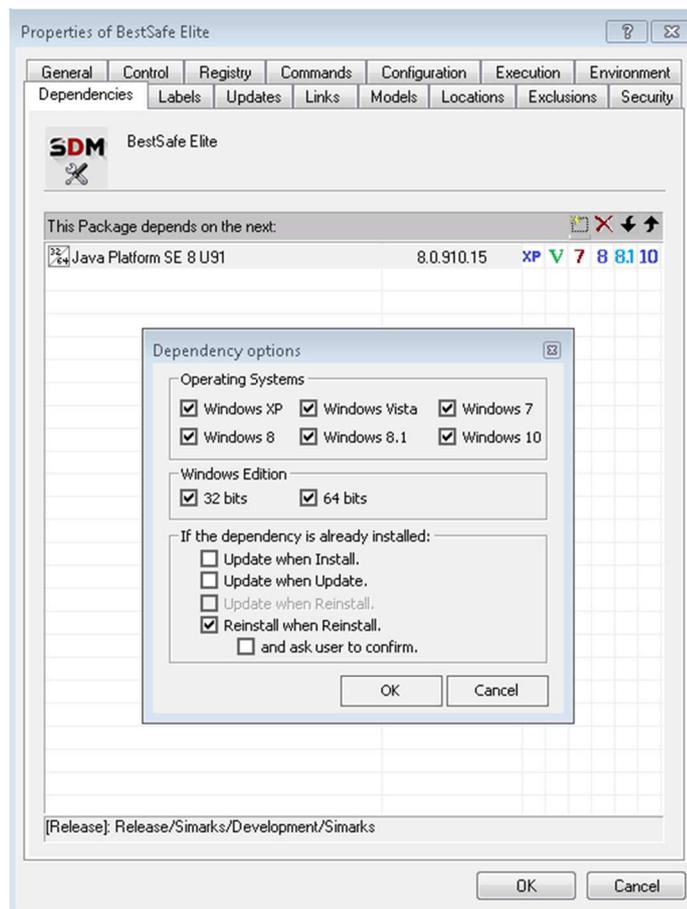
SDM ofrece un gran abanico de posibilidades para la configuración de los procesos a ejecutar en cada fase del despliegue de software incluyendo comandos de comprobación, instalación, desinstalación, reinstalación, actualización y reparación. En cualquiera de las opciones, las líneas de comando se pueden configurar para ser ejecutadas dependiendo de la arquitectura del *endpoint*, 32 bits, 64 bits, o ambas. Igualmente las aplicaciones pueden ser configuradas para ser ejecutadas cada una de ellas en cualquiera de las versiones de Windows.

SDM dispone de funciones predefinidas que se pueden incluir en las líneas de comandos que permite, por ejemplo, presentar una mensaje al usuario informando del progreso de la instalación, lo que es sumamente útil cuando las aplicación se instala de forma silenciosa.



Gestión de dependencias

SDM gestiona las dependencias entre aplicaciones asegurándose de instalar previamente aquellos paquetes de software necesarios para el correcto funcionamiento de una aplicación, como por ejemplo *runtime*s de Java o .Net Framework.



Portal de tareas administrativas

El elemento principal de SDM es el proceso. Cualquier paquete de software se configura como una sucesión de comandos a ejecutar para realizar la instalación, desinstalación, actualización, etc. Esta característica permite que pueda añadirse un elemento cuyo comando sea la **ejecución de una tarea administrativa**, como por ejemplo cambiar la configuración de red, instalar un driver de impresora, ajustar la hora del reloj, ejecutar una restauración del sistema, etc.

SDM permite la delegación de determinadas tareas administrativas en los usuarios finales sin necesidad de otorgarle permisos de administrador.

Inventarios

Conocer el hardware y el software existente en una organización es algo indispensable y SDM ofrece la posibilidad de habilitar la configuración de inventarios, tanto de hardware como de software, de manera separada. La información de inventarios se integra en la herramienta SDM Reports. Cualquier información relativa a los productos puede ser utilizada como criterio de evaluación en la generación de informes de una forma sencilla y con la posibilidad de exportar los informes obtenidos a ficheros tipo csv y xls.

Scripting

SDM ofrece un lenguaje de scripting propietario que ha sido diseñado con el objetivo de proporcionar funcionalidades comunes en la gestión de aplicaciones, incluyendo funciones para que el proceso de instalación de una aplicación se realice sin intervención del usuario y de forma silenciosa.



En la mayoría de los casos, el proceso de instalación requiere que el usuario proporcione una serie de parámetros para continuar con la instalación. Sin embargo, el personal de IT encargado de la gestión de las aplicaciones, a menudo desea proporcionar estos parámetros con valores personalizados y no desea que el usuario final tenga que intervenir en ella de ninguna manera, puesto que hay parámetros (como el número de la licencia del producto) que desea ocultar.

Junto con las posibilidades de depuración, el lenguaje de scripting de SDM proporciona una serie de funciones para interactuar con ventanas, ficheros, el registro de Windows, entre otros, de una manera sencilla y extremadamente rápida que le convierten en la mejor herramienta para el despliegue de cualquier aplicación, por compleja que sea, y en SDM en un tiempo record.

No obstante, al estar basado en comandos, SDM permite la utilización de cualquier lenguaje de script, como Powershell, Visual Basic Script o cualquier otro lenguaje de script del mercado.

Entornos

SDM ofrece tres entornos completamente interconectados entre sí sobre la misma instancia de Directorio Activo:

- ✓ **Pruebas.** Dirigido a la realización de pruebas previas. Tienen acceso tanto los usuarios administradores de Test como los administradores globales de SDM.
- ✓ **Pre-Producción.** Proporciona un entorno de validación funcional de las aplicaciones por parte del usuario responsable. Solamente tienen acceso los administradores globales de SDM.
- ✓ **Producción.** Entorno por defecto para los usuarios finales.

El paso de productos de un entorno a otro se realiza mediante un asistente que posibilita que la configuración y pruebas realizadas en un entorno funcionará exactamente igual en el entorno de

destino si necesidad de realizar ningún cambio, a excepción de la configuración de los filtros de autorización.

Repositorios

SDM soporta cualquier recurso compartido donde almacenar los ficheros binarios de las aplicaciones. El único requisito es que sea accesible a través de un nombre UNC (*Universal Name Convention*).

La siguiente “*Major Release*” de SDM ofrecerá la posibilidad de utilizar repositorios en la nube que serán accesibles a través de una URL.

Cada entorno de SDM requiere de su propio repositorio de software. Las aplicaciones contenidas en cada uno de los repositorios pueden ser desplegadas utilizando uno de los diferentes recursos compartidos y dependiendo de los siguientes tipos:



- ✓ **Aplicaciones globales.** Dirigidas a todos los usuarios de la organización.
- ✓ **Aplicaciones para *Headquarters*.** Dirigidas a usuarios de back-office y edificios centrales.
- ✓ **Aplicaciones de Administración.** Paquetes de software para la realización de tareas administrativas.

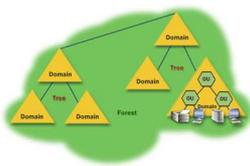
A su vez, el repositorio del entorno de Producción puede estar replicado en las diferentes ubicaciones geográficas de la organización. SDM hace un uso extensivo de la topología de *sites* de Directorio Activo para, entre otras cosas, proporcionar que el usuario final acceda al repositorio más cercano a su ubicación.

Ventajas

Simarks Deployment Manager (SDM™) combina la distribución de aplicaciones tradicional con la gestión de privilegios lo que ofrece al usuario final la posibilidad de gestionar las aplicaciones que necesita en su equipo de trabajo, pero sin comprometer la seguridad de la organización ya que no es necesario otorgarle privilegios de administrador.

Al mismo tiempo SDM proporciona al personal de TI la herramienta adecuada para decidir que aplicaciones o tareas desea delegar a los usuarios finales a la vez que mantiene el control sobre los equipos de la organización, reduciendo considerablemente los recursos y el coste destinado a la Gestión de Aplicaciones Corporativa.

Integración con Directorio Activo

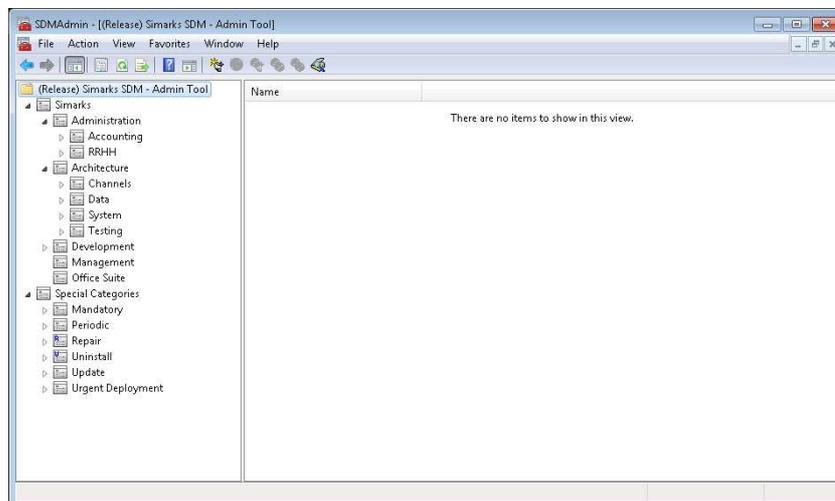


SDM no sólo está integrado con Directorio Activo en la parte que alimenta los filtros con objetos del propio directorio de la organización (usuario, grupo, equipo, subred, sitio), sino que además persiste todos sus datos en el propio Directorio Activo, aprovechando al máximo sus características de replicación.

Esto proporciona escalabilidad, alta disponibilidad y tolerancia a fallos sin ningún coste adicional, ya que ésta crece al mismo tiempo que Directorio Activo.

Gestión centralizada e integración con SIEM

La herramienta de gestión está basada en una MMC (*Microsoft Management Console*) que modifica sus datos en el Directorio Activo. Gracias a su topología de ancho de banda, se administra siempre en el controlador de dominio más cercano, y gracias a la replicación de objetos, esta configuración estará disponible a través de todo el dominio.



Resulta fácil hacer un seguimiento de toda la herramienta, incluidos los agentes, gracias a su meticulosa integración con cualquier sistema SIEM. A través de logs, informa del uso de aplicaciones y procesos que pueden ayudar a controlar licencias, el software no autorizado, etc.

Finalmente, dispone de una herramienta diseñada para elaborar los informes que se desee en base a cualquier parámetro que se pueda poner en SDM, además de la información que recogen los agentes (como inventario de hardware y de software).

Requerimientos

Simarks Deployment Manager (SDM™) no necesita de elementos adicionales ni de hardware ni de software. Únicamente es necesario dotar a la herramienta de los repositorios de software necesarios para albergar los ficheros binarios que componen las aplicaciones.

Simarks Software

Simarks™ Software es una compañía española especializada en el desarrollo de software de ciberseguridad y enfocada en la protección ante amenazas de tipo *ZeroDay*, amenazas avanzadas y brechas de seguridad de cualquier tipo, y en especial las que hacen uso de los privilegios de administrador.

SDM™ es parte de la Suite BestSafe que incluye el producto Simarks™ BestSafe™, una solución de Gestión de Privilegios, tanto a nivel de usuario como a nivel de aplicación, que permite otorgar privilegios elevados por aplicación (o proceso) independientemente de los privilegios del usuario que ejecuta la aplicación.

Simarks Software es la única compañía que, gracias a su tecnología patentada de control del contexto de seguridad, ofrece la solución integral en gestión de privilegios y aplicaciones más completa del mercado.



Oficinas Centrales

C/ Copenhagen 12
Edificio Titan – Oficina 204
28232 Las Rozas de Madrid
Madrid – Spain
+34 910 534 037
www.simarks.com
info@simarks.com