

# Simarks<sup>™</sup> Deployment Manager SDM<sup>™</sup>

## White Paper

Simarks Software - cybersecurity

## Table of contents

Introduction
Features
Application Management – Self-Service 4
Unattended deployment – Traditional system 5
Command Line
Running Applications
Management of dependencies
Administrative tasks portal
Inventory
Scripting
Environments
Repositories
Advantages
Integration with Active Directory11
Centralized management and integration with SIEM11
Requirements

## Simarks<sup>™</sup> SDM<sup>™</sup>

### Legal Notice

Copyright ©2018 Simarks<sup>™</sup> Software. All rights reserved. Simarks<sup>™</sup> Software, the Simarks<sup>™</sup> Logo, and Simarks<sup>™</sup> BestSafe<sup>™</sup> are trademarks or registered trademarks of Simarks<sup>™</sup> Software or its affiliates in the European Union – EU and other countries. Other names may be trademarks of their respective owners.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SIMARKS SOFTWARE SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Simarks<sup>™</sup> Software and its licensors, if any.

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



## Introduction

Application management continues to be an ineffectively resolved issue in organizations starting from a certain number of workstations. The choice between security and productivity leads to strategic decisions that do not provide an adequate solution together; the more secure a system is, the less productive it is. Usually, administrator permissions are required to perform application installations or any changes to system configuration, and the operating systems today lack the flexibility needed to avoid penalizing either security or productivity.

In addition, application management is an active part of an organization's security, as it is one of the main reasons for granting administrator permissions to end users.

Simarks Deployment Manager (SDM<sup>™</sup>) is based on Simarks' proprietary process-level privilege management technology and offers a completely different and innovative approach.

Not only is it specialized in the management of applications at the time of installation, uninstallation, update, etc., but also manages the permissions that the application needs at the time of execution. All this without the need to grant additional permissions to the end user.

With SDM it is possible to build a "Corporate Application Portal" where it is the end user who consumes the applications to which it has authorization without having to grant him any other elevated permissions. This approach allows the full implementation of the "Principle of Least Privilege" without affecting productivity.

### Features

The main functionalities of SDM are:

- $\checkmark$  Self-service of Applications through the Corporate Application Portal.
- ✓ Management of dependencies, updates, patches and service packs.
- ✓ Delegation of administrative tasks to the end user without the need to grant him administrator permissions.
- ✓ Different environments (test, pre-release and release) under the same Active Directory instance, fully integrated with each other.
- ✓ Distributed Software Repository based on Active Directory Sites that allows the end user to access their nearest repository.
- $\checkmark$  Execution of scheduled tasks.
- ✓ Wide range of filters.
- ✓ Urgent distribution.
- ✓ Hardware and Software Inventory.
- ✓ Reporting.

#### Application Management – Self-Service

Through the Corporate Application Portal, the user can view all the applications in the catalog, but can only install those that the administrator of the tool has authorized for him. This authorization is based on a wide range of filters, both for inclusion and exclusion, including user, group, computer, brand, model, department, subnet, site, role, OS version, 32/64 bit, etc.

Install Reinstall Categories Office Suite	Uninstall	Update	Search Search Packages of Name	Font	Refresh	Environment Release	7	Exit	Simark
			Name 🔺	of "Office Su	ıite"				
Office Suite									
			Mirosoft Offic						Version 15.0.4420.0
		12 12 12 12 12 12 12 12 12 12							
tegories Catalog   Labels	Installed								

Traditional solutions are based on the use of accounts with administrator permissions, which in most cases is different from the user who finally makes use of the applications. This entails a tedious problem that requires a laborious remediation and configuration process that must be performed after the installation and which considerably lengthens the integration time of new applications in addition to the risk of compromising the password. SDM performs the installation under the end user account, thus avoiding these problems.

Since the applications are installed by the user himself, which is who is going to use them, the applications do not require any treatment because the original media (or a dump in the software repository) is used for integrating them into the tool. For this reason, the integration in SDM of the majority of applications in the market is almost immediate.

SDM supports all versions of Windows from XP to Windows 10 (32 and 64 bit).

#### Unattended deployment – Traditional system

Although focused on self-service, SDM offers a complete and improved system of traditional and unattended distribution. Based on an advanced configuration, any application or administrative task can be run in the organization automatically.

General	Control Regi	istro Comandi	os Configura	ción Ejecución	Entorno D	ependencia
Etiquetas	Actualizacio	nes Enlaces	: Modelos	Ubicaciones	Exclusiones	Segurida
SDN X	<b>l</b> BestSafe	e Elite				
O no	o este producto hacer nada. alizar la actualiz.			lo de Actualizació	ones Automática	as debe: —
• re-	alizar la actualiza	ación automátic	amente.			
	🔲 Fecha/H	lora Activación:	20/11/20	16 🛒 13:27:	20	
Este F	e Pack: Producto tiene el este Producto n spués de instak	io está instalado	, instalar el Se	rvice Pack autor	náticamente	×[]
D si Pa	este Producto y .ck.automátican	a está instalado nente a través o	pero el Servic lel módulo de /	e Pack no, insta Actualizaciones A	lar el Service Automáticas	
		Valor Actuali	zación Periódia	ca (número de an	ranques del clie	nte): 0

It also allows the deployment of applications in a staggered way avoiding the saturation of the network, and allows an application to be deployed automatically for users who meet certain filters while other users are offered the possibility of installing that same application on demand.

The deployment of unattended tasks and applications can be done based on a wide range of filters, both for inclusion and exclusion (user, group, computer, model, brand, department, subnet, site, role, OS version, architecture 32/64-bit, etc.), and are categorized by different types of categories:

- Mandatory Automatic installation of mandatory applications based on filters.
- Uninstallation Automatic uninstallation of applications, regardless of whether they have been installed through SDM or not.
- Update Automatic update of products, patch management and service packs included.
- Periodicals Periodic and automatic execution of administrative tasks.
- **Repair** Execution of commands to solve incidents by executing tasks, or for applications that are already installed and need to be repaired.
- Emergency Possibility to execute specific commands within minutes in case of emergency.

#### Command Line

SDM offers a wide range of possibilities for configuring the processes to be executed in each phase of the software deployment including checking, installing, uninstalling, reinstalling, updating and repairing commands. In any of the options, the command lines can be configured to be executed depending on the architecture of the endpoint; 32 bit, 64 bit, or both. Also the applications can be configured to be executed each of them in any of the Windows versions.

SDM has predefined functions that can be included in command lines, for example, to show a message to the user informing the progress of the installation, which is extremely useful when the application is installed silently.

roperties of Java	a Platform SE 8 U91	8 23
Dependencies	Labels Updates Links Models Locations	
General Co	ntrol Registry Commands Configuration E	execution Environment
SDM X	Java Platform SE 8 U91	
	Install Commands:	<b>□×</b> ++
$\checkmark$	👫 %FN%DisplayMessage:"Java Platform SE 8 U91"	"Instalando Java Runt
Check	% SWGLBL% \%FOLDER% \jre-8u91-windows-i586	
	64 %SWGLBL%\%FOLDER%\jre-8u91-windows-x64.	exe /s
Install	200 % NAD ESUDYMESSAGE	
<u></u>		
Reinstall		
$\mathbf{N}$		
Uninstall		
<b>S</b>		
Update		
7		
Repair		
Nepan		
	-	
		OK Cancel

SDM uses HRESULT codes (<u>https://msdn.microsoft.com/en-us/library/cc231198.aspx</u>) to determine the output of each of the commands and provides a mechanism for "transforming" return codes used by the installation commands of the application.

This way, the treatment of all return codes of all applications is made homogeneous.

	t Codes will be	d Return Codes  translated to Return Output the client module.
Input	Output	Error Code Text
		7
00000000	00000000	
Add	Remove	
		OK Cancel

#### Running Applications

Applications that require special privileges at runtime can be configured at the time of installation so that they always run with the correct permissions without having to grant those permissions to the user. File spoofing is avoided by digital signature and internal file name checking.

Properties of Application	
Dependencies         Labels         Updates         Links         Models         Locations         Exclusions         Security           General         Control         Registry         Commands         Configuration         Execution         Environment	
Application	
When executing this package: The user must be member of one or more groups. At install time, add user to the next groups:	
Name Minutes Minutes	
NOTE: Right-Click item to select builtin Local Groups.	
Register the next execution command lines:	(
Command Lines: PRDGRAM_FILES%VAppFolderVApp exe  Run in Restricted mode Apply to any user on client machine Activate options only once Add process to next groups:	
ок	Cancel

#### Management of dependencies

SDM manages dependencies between applications making sure to first install those necessary software packages for the correct operation of an application, such as Java runtimes or .Net Framework.

General	Control	Registry	Comman		guration	Exec	ution		Envir	onmen
Dependen	cies Lat	oels Upda	ates Link	s Models	Loca	tions	Exclu	sion	s S	Securit
SDM X	BestSaf	e Elite								
This Pack	age deper	ids on the ne	ext:					凹	×	F 🕈
32/Java	Platform SE	8 U91			8.0.910.1	5 X	PV	7	88	1 10
	_							_		
	Dep	endency o	ptions				8			
	— г	Operating S	ystems —					-		
		Window:	s XP 🗹 V	/indows Vista	₩ 🗹	indows 7	,			
-		Window:	s 8 🔽 V	/indows 8.1	V W	indows 1	0			
		Windows Ed	lition				_			
		✓ 32 bits	6	4 bits						
		If the dener	odency is all	ready installe	d		_			
			te when In:							
			te when Up					-		
			te when Re tall when R							
		_		er to confirm						
							5			
	_			ОК		Cancel				
[Release]	Release/9	oimarks/Dev	elopment/S	imarks						- I

#### Administrative tasks portal

The main element of SDM is the process. Any software package is configured as a succession of commands to execute to perform the installation, uninstallation, update, etc. This feature allows you to add an element whose command is the execution of an administrative task, such as changing network settings, installing a printer driver, setting the clock time, running a System Restore, etc.

SDM allows certain administrative tasks to be delegated to end users without the need to grant them administrator permissions.

#### Inventory

Knowing the existing hardware and software in an organization is essential and SDM offers the possibility to enable the configuration of inventories, both hardware and software, in a separate way. The inventory information is integrated into the SDM reporting tool. Any information related to the products can be used as an evaluation criteria on report generation in a simple way and with the possibility of exporting the obtained reports to csv and xls files.

#### Scripting

SDM offers a proprietary scripting language that has been designed with the aim of providing common functionalities in the management of applications, including functions designed so that the process of installing an application is done without the intervention of the user and in a silent manner.



In most cases, the installation process requires the user to provide a set of parameters to continue with the installation. However, the IT personnel in charge of managing applications often want to provide these parameters with custom values and do not want the end user to have to intervene in it in any way, since there are parameters (such as the number of the product license) that you want to hide.

Along with the ability to debug the scripts, the SDM scripting language provides a set of functions to interact with windows, files, Windows registry, among others, in a simple and extremely fast way that make it the best tool for the deployment of any application, however complex, and in SDM in a record time.

However, since SDM is command-based, it allows you to use any scripting language, such as Powershell, Visual Basic Script, or any other scripting language on the market.

#### Environments

SDM offers three fully interconnected environments on the same Active Directory instance:

- ✓ Test. Aimed at performing tests prior to the release of applications. Both test administrators and SDM global administrators have access to this environment.
- ✓ Pre-Production. Provides a functional validation environment for applications by the responsible user. Only global SDM administrators have access.
- ✓ Production. Default environment for end users.

The movement of products from one environment to another is done through a wizard that guarantees that the configuration and testing performed in an environment will work exactly the same way in the target environment without needing to make any changes, except for the configuration of authorization filters.

#### Repositories

SDM supports any shared resource to store the binary files of the applications. The only requirement is that it be accessible through a UNC (Universal Name Convention) name.

The next "Major Release" of SDM will offer the ability to use cloud repositories that will be accessible through an URL.

Each SDM environment requires its own software repository. The applications contained in each of the repositories can be deployed using one of the different shared resources and depending on the following types:



- ✓ Global applications. Aimed at all users of the organization.
- ✓ Headquarters Applications. Aimed at back-office users and central buildings.
- ✓ Administration Applications. Software packages for performing administrative tasks.

In turn, the repository of the Production environment can be replicated in the different geographic locations of the organization. SDM makes extensive use of Active Directory site topology to, among other things, provide the end-user to access the repository closest to his location.

## Advantages

Simarks Deployment Manager (SDM  $^{\text{M}}$ ) combines traditional application distribution with privilege management which gives end users the ability to manage the applications they need on their workforce, but without compromising the organization's security, since it is not necessary to grant them administrator privileges.

At the same time, SDM provides IT staff with the right tool to decide which applications or tasks they want to delegate to end users while maintaining control over the organization's teams, significantly reducing resources and cost for IT management.

#### Integration with Active Directory



SDM is not only integrated with Active Directory in the part that feeds the filters with objects of the own directory of the organization (user, group, computer, subnet, site), but also persists all its data in the Active Directory itself, taking advantage of it Replication characteristics.

This provides scalability, high availability, and fault tolerance at no additional cost as it grows at the same time as Active Directory.

#### Centralized management and integration with SIEM

The management tool is based on a Microsoft Management Console (MMC) that modifies its data in the Active Directory. Thanks to its bandwidth topology, it is always managed on the closest domain controller, and thanks to object replication, this configuration will be available across the entire domain.

File Action View Favorites Wind			- 8
🔶 🗔 🖸 🙆 🗟 関 🏘			
Release)     Smarks     SMA - Admin Tool       Smarks     Accounting       >     Channels       >     Spectar       >     Spectar       >     Office Suite       >     Management       >     Management <td< th=""><th>Name</th><th>There are no items to show in this view,</th><th></th></td<>	Name	There are no items to show in this view,	

#### Simarks<sup>™</sup> Deployment Manager SDM<sup>™</sup> - White Paper

It is easy to keep track of the whole tool, including the agents, thanks to its meticulous integration with any SIEM system. Through logs, reports on the use of applications and processes that can help control licenses, unauthorized software, etc.

Finally, it has a tool designed to prepare the reports that are desired based on any parameters that can be placed in SDM, in addition to the information collected by agents (such as hardware and software inventory).

### Requirements

Simarks Deployment Manager (SDM  $^{\text{m}}$ ) does not require additional hardware or software. It is only necessary to provide the tool with the necessary software repositories to host the binary files that make up the applications.

#### Simarks Software

Simarks<sup>™</sup> Software is a Spanish company specialized in the development of software for cybersecurity and focused on ZeroDay-type threat protection, advanced threats and security breaches of any kind, especially those that make use of administrator privileges.

SDM<sup>™</sup> is part of the BestSafe Suite that includes the Simarks<sup>™</sup> BestSafe<sup>™</sup> product, a user-level and application-level Privilege Management solution that allows you to grant elevated privileges per application (or process) regardless of privileges granted to the user who is running the application.

Simarks Software is the only company that, thanks to its patented security context control technology, offers the most comprehensive application and privilege management solution on the market.



#### Headquarters

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