Simarks™ Deployment Manager SDM™

White Paper

Simarks Software - cybersecurity

Table of contents

Introduction 3
Features 3
Application Management – Self-Service *4*
Unattended deployment – Traditional system *5*
Command Line *6*
Running Applications *7*
Management of dependencies *8*
Administrative tasks portal *8*
Inventory *9*
Scripting *9*
Environments *9*
Repositories *10*
Advantages 11
Integration with Active Directory *11*
Centralized management and integration with SIEM *11*
Requirements 12

Simarks™ SDM™

Legal Notice

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

www.simarks.com

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™) 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.

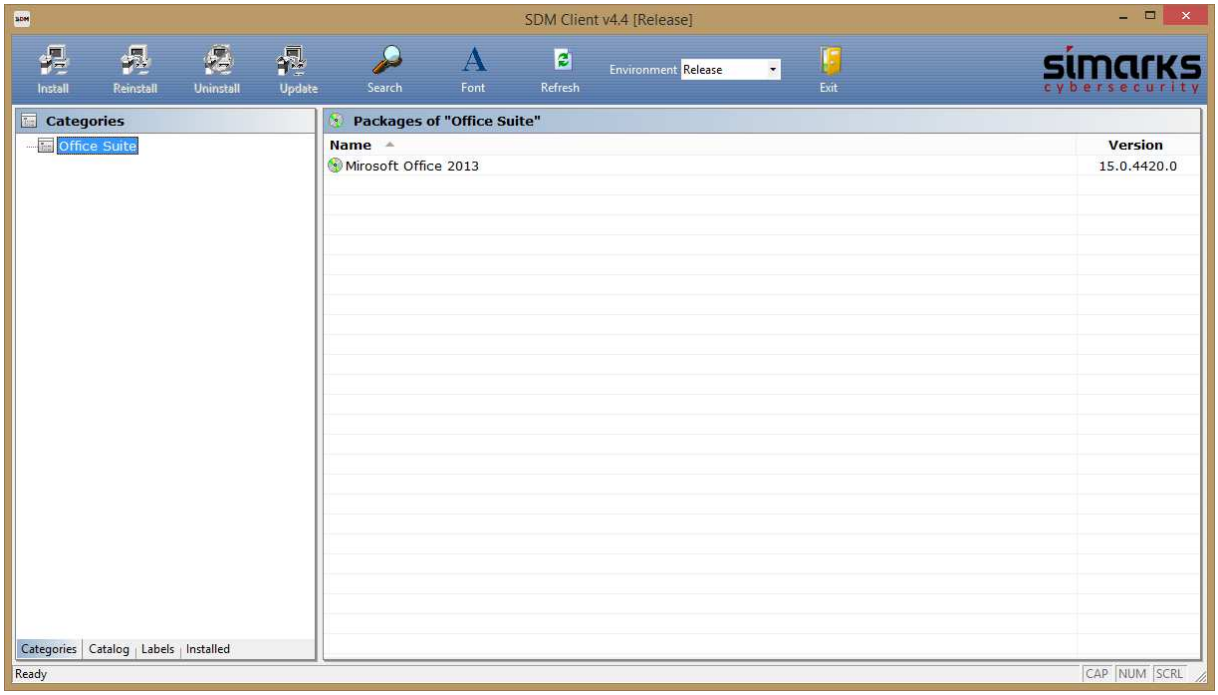
Features

The main functionalities of SDM are:

- ✓ 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.
- ✓ 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.



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.

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.

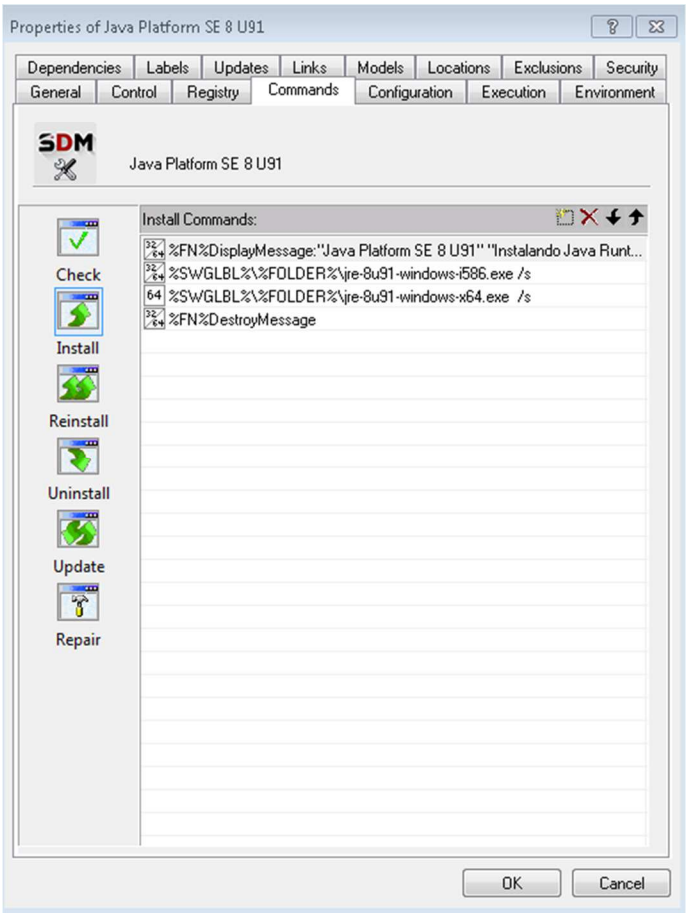
The deployment of unattended tasks and applications can be done based on a wide range of filters, both for inclusion and exclusion (user, group, computer, model, brand, department, subnet, site, role, OS version, architecture 32/64-bit, etc.), and are categorized by different types of categories:

- 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

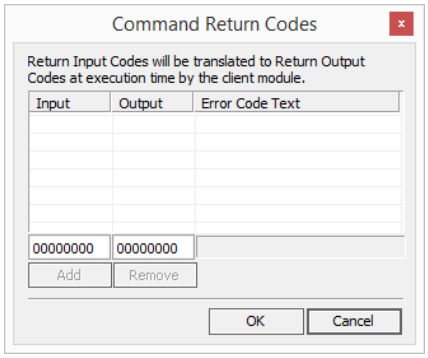
SDM offers a wide range of possibilities for configuring the processes to be executed in each phase of the software deployment including checking, installing, uninstalling, reinstalling, updating and repairing commands. In any of the options, the command lines can be configured to be executed depending 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.



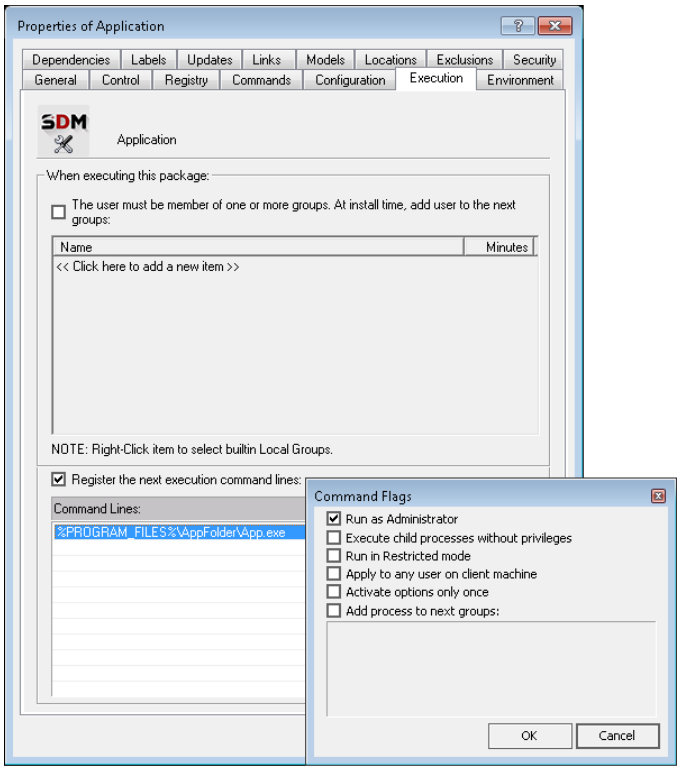
SDM uses HRESULT codes (https://msdn.microsoft.com/en-us/library/cc231198.aspx) to determine the output of each of the commands and provides a mechanism for "transforming" return codes used by the installation commands of the application.

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



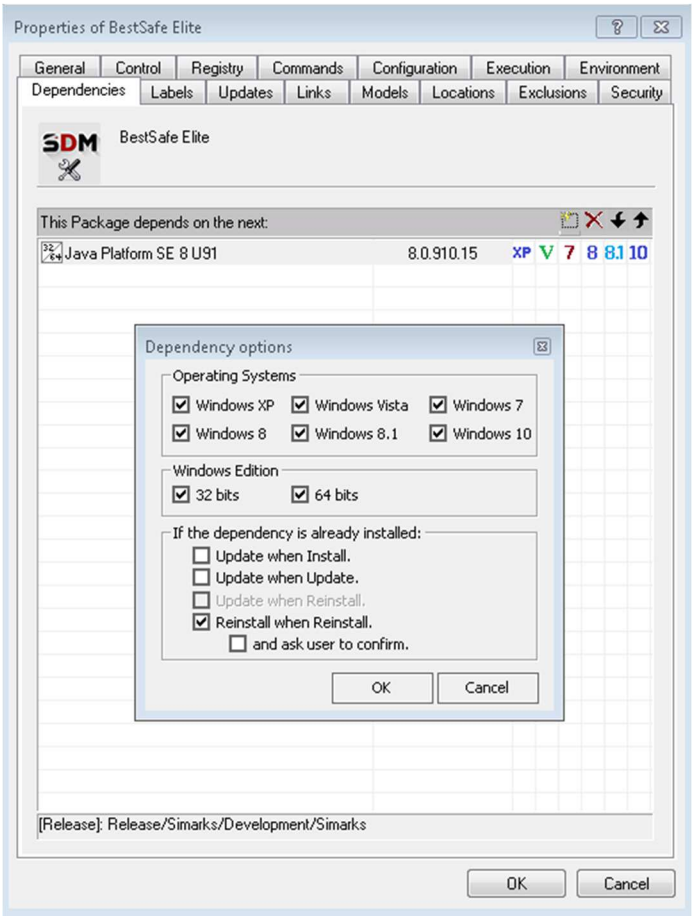
Running Applications

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.



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.



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.

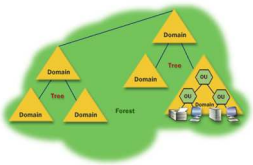
In turn, the repository of the Production environment can be replicated in the different geographic locations of the organization. SDM makes extensive use of Active Directory site topology to, among other things, provide the end-user to access the repository closest to his location.

Advantages

Simarks Deployment Manager (SDM ™) 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

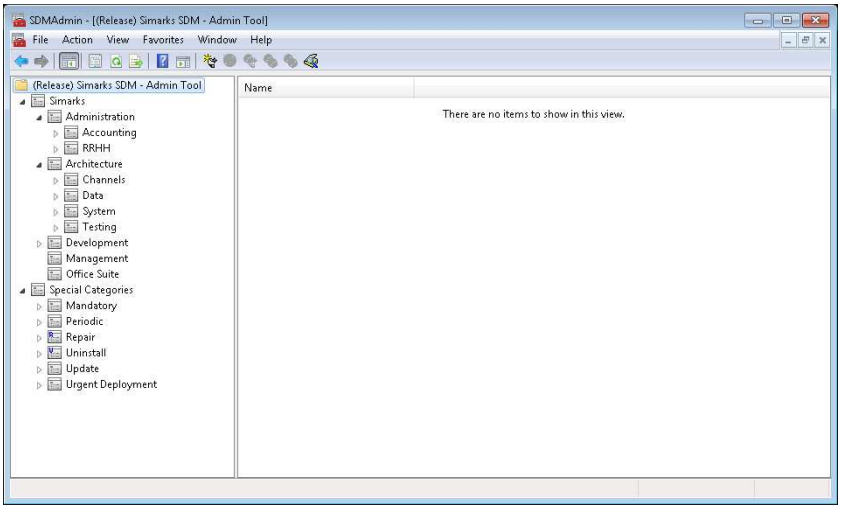


SDM is not only integrated with Active Directory in the part that feeds the filters with objects of the own directory of the organization (user, group, computer, subnet, site), but also persists all its data in the Active Directory itself, taking advantage of it Replication characteristics.

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.



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 ™) 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™ 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™ is part of the BestSafe Suite that includes the Simarks™ BestSafe™ 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
info@simarks.com