Simarks™ Deployment Manager

Technical Feature List

SDM

Simarks Deployment Manager ™ Overview

Simarks Deployment Manager™ provides an innovative approach to the software deployment dilemma on Microsoft environments. This new approach combines Privileges Management technology with software deployment and advance security. By combining these two technologies into one solution, the benefits are clear.

- Software Deployment becomes an incredible easy task as the "setup process" is elevated with administrator rights by the SDM™ privileges management patented technology, no matter the permissions of the user who launches the application has.

- True user-centered IT. Users deploy corporate authorized applications by themselves with no IT intervention.

- Reduce IT cost and time by 5x, as compared with traditional Software Deployment solutions.

- All applications, software components, patches, hot fixes, service packs are supported as SDM™ using the original media.

- Remove automatically non-compliance and non-authorized software from the endpoints.

- Adding Advanced Security to Software Deployment becomes the safest and easiest way to deploy software.

- Add Privilege Management security for your applications at runtime.

- Add SIEM capabilities.

- SDM™ seamless integrates with Microsoft as it only requires Active Directory.

- SDM™ easy management throughout MMC snap-in console.

- Unbeatable ROI. Servers-count-to-node is as low as 0 as no additional servers or CMDBs are required.

- Avoid inadequate use of the corporate endpoints.

- Remove the risk of Privileged Access Points, cost and misusage on the company's endpoints.

Simarks™ SDM™ Feature List

Software Deployment		
Feature	**Description**	**Use Case / Remarks**
Automatic Deployment	Automatic deployments related tasks like install, update, uninstall and repair.	Company can manage common automatic software distribution tasks. Deploy applications, update them, apply service packs or patches, etc.
On Demand	The end user is who performs the application installation with no IT intervention.	Companies authorizes their users to install only previously pre-authorized applications from the company's catalog.
Automatic Removal	Remove non-desired or non-authorized software from endpoints automatically.	Company authorizes users to have installed only pre-authorized Internet Explorer browser, so remove any other browser like Firefox or Chrome.
Microsoft apps patching	Microsoft update patching support.	IT demands full control over Microsoft's endpoints products updates.
Third-party apps patching.	Third-Party application patching support.	IT must patch every single application that company make use of.
Emergency deployments	Deploy packages urgently to desired group of machines.	IT must deploy and execute a virus vaccine urgently in certain desktops.
Dependencies	Set which packages must be installed before the application.	Automatic deployment of runtimes like Java VM or .Net Framework prior to the application.
Updates	Automatic and on-demand update support.	Some updates must be performed when the end-user dictates and some others must be done automatically.
Service Packs	Automatic deployment of Service Packs.	Deploy Office 2013 SP1 automatically to those machines that have it already installed.
Hot Fixes	Deploy hot fixes.	Company needs to deploy a hot fix.
Filters	Filters available to decide what user/machine have access to every corporate application.	Machine Model, Machine Brand, Organization Unit, Site, Subnet, computer, Group, User, Role, and Corporate OUs. SDM™ allows IT administrator to do filtering for both, inclusion and exclusions. This way IT can deploy MS Office to all member of the financial department except two given users.
Command Return Code Mapping	SDM™ uniforms return codes to HRESULT type.	An application requires the user to perform an action depending on the code returned by a command.
Admin Tasks	To execute commands instead of installing, with admin privileges.	A user needs to change security settings from its desktops. With SDM™ this can be easily achieve without granting administrator credentials.
Incompatibles processes	At installation time gives control for process that make an action (install, uninstall, etc.) unavailable.	Microsoft Office needs to be updated without Outlook in execution.
Sub-Packages	Create as many sub-packages as needed. Every sub-package implements its own SDM™ Filters.	To deploy Microsoft Office SP1 update on-demand for a group of users and at the same time automatically for others.
Per user or per machine basic distributions.	SDM™ allows performing applications distributions based on users or machines.	Distribute an application that only can be executed by the user who perform the installation or, as opposite, deploy an application that any logged user can use.
User-Machine pair distribution.	Define deploy filters by User-Machine pair.	Grant USER01 permission to install SQL admin tools on WSSQL001 machine only up to March, 1 at 00:00:00.

Environments

Feature	Description	Use Case / Remarks
Number	SDM™ supports as many environments as needed within the same AD instance with a minimum of three: Release, Pre-Release and Test.	Dev, staging and release environments live all together on a single SDM™ instance. Company wants to create a specific environment for ATMs, POS, LOB, test, dev, pre-production.
Dev., staging and production	SDM™ installs three environments by default one of each type.	A package is first tested on the Test Environment, then is promoted to Pre-Release to final validation and finally promote up to Release environment for general usage.
AD Integration	Microsoft Active Directory Integration.	SDM™ is fully integrated with Active Directory. No additional components are required. Two IT engineers can manage up to 25,000 endpoints' software deployment with SDM.
Automatic Promotion	SDM™ allows promoting packages up and down between environments.	For MS Office, it runs the required tests before deploying. Once done IT staff promotes the package up to the release environment. This can be done is two single steps.
Copy Package	SDM™ allows copying package's configuration between environments.	When a package has any issues and it already on production stage, IT can copy the package back to the Test environment, fix the problem and move it back to upper environments with the new changes and fixes.
Per site distributed repository	SDM™ allows distributed repositories and site affinity feature.	Software deployment is performed from the nearest repository. This is done taking advantage of Active Directory sites feature.

System Requirements

Feature	Description	Use Case / Remarks
Server-to-node count	Number of other elements needed to support any given number of desktops.	SDM™ server-to-node-count is as low as 0 as no additional components are required.
Time to deploy	Time to deploy SDM™	Same-day deployment, as no additional components are required. SDM™ is deployed only into one Domain controller SDM™ light client components.
Scalability	Product scalability	SDM™ supports as many desktops as Microsoft AD computers supports.
Footprint	Product footprint	15MB for the SDM™ client's component. MMC snap-in console. SDM™ is added to the "Program Data" container of Active Directory.
Supportability	Windows Operating System version and editions supported by SDM™.	Client components (32 and 64 bits): - From Windows XP to Windows 10. Server components (32 and 64 bits): - Windows Server 2003 and Windows Server 2003 R2 - Windows Server 2008 and Windows Server 2008 R2 - Windows Server 2012 and Windows Server 2012 R2

Client Health - Monitoring

Feature	Description	Use Case / Remarks
Periodic maintenance task	Run IT periodic maintenance tasks.	IT must run a desktop defrag or a registry clean, on all desktops every Sunday morning.
3rd party integration	Run IT tasks from 3rd party vendors.	IT must execute a desktop backup with a 3rd party backup tool.

Login Script

Feature	Description	Use Case / Remarks
Login script	SDM™ can use logon scripts to assign tasks that will be performed when a user logs on.	IT must execute some tasks when the user logs in, like updating AV signatures, connecting to share folder or connect to a printer.
Scripting Language	SDM™ offers a scripting language specially designed to software deployment.	IT can easily create scripts to perform any action for software distribution.

Compliance and Setting Management

Feature	Description	Use Case / Remarks
Admin Roles	SDM™ has different levels of administration through a unique console	SDM™ Administrators have full access to SDM™. SDM™ Test Administrators can manage Test Environments only. Application management can be delegated to specific group of users.
Audit & History logs	SDM™ tracks any change or action.	SDM™ tracks a log record for history, auditing and compliance purposes.
Configurable automatic deployment thresholds.	SDM™ Automatic Distribution System (SADS) makes use of different time intervals to avoid collisions and minimize network traffic.	IT must deploy software in automatic way to thousands of users at the same time, SDM™ uses and internal algorithm guided by time thresholds to avoid collision and allow the completion of the deployment.

Privilege Management at Execution time

Feature	Description	Use Case / Remarks
Privilege management	SDM™ assign correct security context to applications after installation.	At installation time, SDM™ administrator decides which privileges an application needs to work properly. At execution time SDM™ will assign the correct credentials to the application.
Run as administrator	Privilege Management	IT can decide if an application needs to run as administrator.
Execute child processes without privileges	Privilege Management	An application that run with administrator credentials executes a new process. When this option is enabled child processes will no inherit administrator credentials.
Run in Restricted mode	Privileges Management	An employee require to run its desktop with administrator credentials. This can lead to a security breach (Privileged Access Point). SDM™ can assign restricted privileges to applications accessing to the

		Internet like email clients, browsers, office, etc. to mitigate the risk.
Apply to any user on client machine	Privilege Management	Apply the privilege configuration to any user on client machine.
Activate options only once	Privilege Management	Apply the privilege configuration only once.
Add process to local groups	Privilege Management	Instead of making the user member of a local group, SDM™ administrator can assign only the application to that local group.

Reporting

Feature	Description	Use Case / Remarks
Applications deployed per OS or per system	This report allow knowing the exactly list of applications in a system, OS or in an environment that have been deployed.	When an OS migration is taking place, this report allows knowing how many applications have been already migrated a how many there are left.
Custom Reports	Build a report based on the package fields.	SDM™ administrator can use any package field to elaborate a report based on the value of that fields.

Inventory

Feature	Description	Use Case / Remarks
Hardware Inventory	SDM™ Hardware inventory	Collect hardware information from corporate desktop: *Bios, Cache, Chassis, Cooling, Devices, Memory, Operating System, Ports, Power Supply and System Settings.*
Software Inventory	SDM™ Software Inventory	Collect SDM™ and Windows Installer software information from corporate desktops.
Avoid WMI	Microsoft Windows Management Instrumentation	Some tools leverage WMI service to run software deployment tasks and for collecting software & hardware (inventory) information from desktops. Although Microsoft has improved the reliability of WMI, some customers prefer to disable this service. SDM™ doesn't make use of WMI.

Repositories

Feature	Description	Use Case / Remarks
Distributed Repositories	SDM™ is particularly focus to large companies; medium and small companies can also benefits from the powerful features and capabilities that SDM™ provides. SDM™ can easily handle thousands of endpoints geographically spread.	Companies' distribution points should be physically near to the clients to avoid network latency problems and low WAN speed connections on every location. This can cause delays on the application deployment or making it impossible. SDM™ makes use of Active Directory sites to increase the bandwidth and make the software deployment faster and reliable.
Global applications	This shared folder contains all applications intended for the wide organization.	Manage and get easily access to company wide applications.
Headquarters Application	A shared folder that contains the applications intended only for singular locations.	Manage and get easily access to headquarters applications.
Administration	Shared folder for administration tools.	Manage and get IT staff easily access to administration

Applications		applications.
Repository affinity	Define the nearest repository.	IT can define the nearest repository for each user.
Third-party file replication tool support.	Distributed repositories need to be in synchronized in order to avoid application distribution problems.	Microsoft DFS can be used in order to have all distributed repositories synchronized
Cloud	Software repositories can be in the Cloud.	SDM™ can deploy applications stored in the cloud so users not connected to enterprise network can still deploy authorized applications.

Corporate Applications Catalog		
Feature	**Description**	**Use Case / Remarks**
Applications Support	Applications that can be included in the Corporate Application Catalog.	Any application from any vendor or corporate made can be included on the corporate application catalog. Users can deploy any application to theirs desktop.
Actions support	Actions that can be included in the Corporate Application Catalog.	When users need to perform some actions, like change power setting, add printer, change system settings, etc., that actions require administrator credentials. IT can add these actions to the corporate application catalog, and then user can easily preform this task without granting him administrator credentials.
True Self-Service	IT Consumerization: Organizations of all sizes can take benefits from self-service software deployment as a natural process. Search, find, select, deploy.	Users are the ones who deploy corporate authorized applications without any IT intervention. The user just select the application on SDM™ client module, right click and then install.
Labeling	Each product inside SDM™ can be labeled with custom labels to make searches easier.	Shape the corporate applications catalog is as easily as adding labels. IT add the labels "Financial Apps", "Office Tools", "Microsoft Apps" to shape the catalog. Then SDM™ mark which labels a package belongs to. The end user can then search the catalog for these labels..
Search	Search applications by name.	User can search the corporate applications catalog by application name.
Read-Only view	Users have read only access to the entire catalog.	Even if the user has not permission to install a specific application he/she can search the corporate application catalog and find which applications he/she needs to request authorization for based on filters defined by SDM™ administrator.

About Simarks™ Software

Simarks™ Software is a Cybersecurity Software company focused on striking down zero-day attacks, advanced threats, cyber threats or any form of malware that make use of the granted privileges to get unrestricted access to the systems.

Simarks Software is the only vendor who deploys software in the safest way by using our privileges management patented technology combined with our Software Deployment capabilities for Microsoft Environments.

Simarks™ Deployment Manager SDM™ benefits

- Deploy software in the best, safer and easier way.
- True on-demand for any corporate application.
- Add advanced security to your software deployment.
- Works ONE Deploy MANY!
- Takes away all the complexity.
- Traditional automatic and unattended deployment supported.
- Wide variety of filters.
- No additional elements needed.
- Deploy applications from network repositories o from the Cloud.

Contact us today and learn how you can benefit from Simarks™ Deployment Manager SDM™.

simarks cybersecurity

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