

The Symantec Approach to Software Asset Management



Symantec has a unified approach to software asset management consisting of 5 key phases: discover, record, reconcile, deliver and enforce. This solution brief discusses each of these phases to provide a better understanding of how to tackle the complexities associated with managing the various aspects of the software lifecycle.

It is worth noting that true and effective software management also requires software and OS deployment as well as patch management to properly manage and protect endpoints and these are significant strengths of Symantec endpoint management solutions. However, for the purposes of this paper, we will focus primarily on the processes to strategically manage and track the financial, physical, licensing and contractual aspects of software throughout its life cycle.

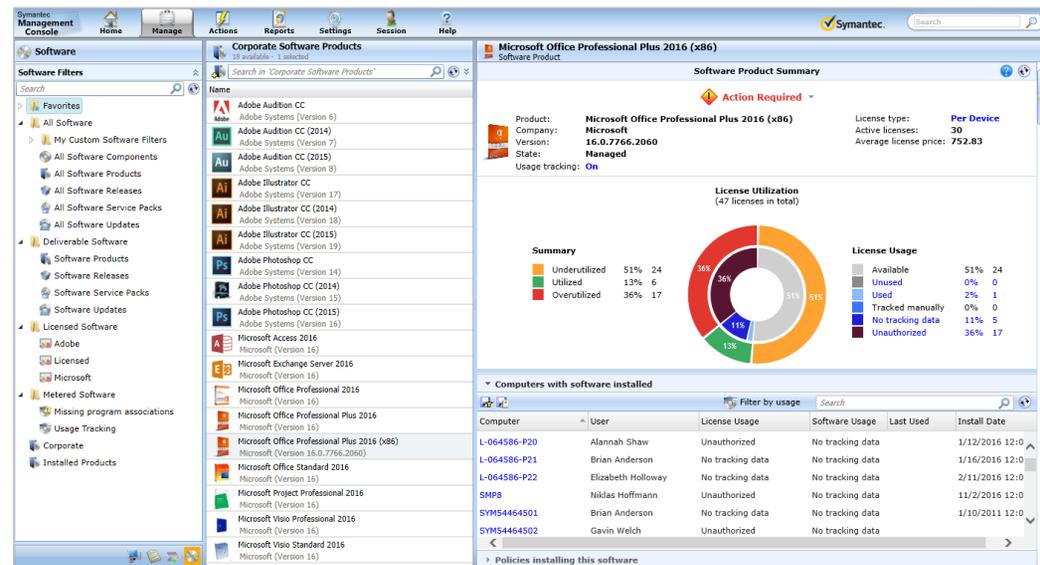
Discover

The foundation to any software asset management program and the first step to protecting your endpoints is uncovering what is currently installed in the environment and maintaining that information for up-to-date intelligence.

A critical but sometimes overlooked part of proper software management is to ensure that discovery also includes the endpoints used by roaming and remote users who may not regularly connect to the corporate network. These machines can become blind spots leading to a variety of issues that extend far beyond inventory tracking such as missing patches, outdated software and non-compliance. Choosing a solution that provides broad discovery and inventory capabilities across all endpoints regardless of their location is crucial in today's world where users work from home, on the road, and everywhere in between.

In summary, the discover phase consists of regularly and automatically identifying what is in the environment both inside and outside the perimeter setting the stage for ongoing administration by collecting information such as:

- Software
- Hardware
- Network resources
- User resources
- Custom inventory



“The underpinning of the Symantec approach to software asset management is its software catalog which is part of the Configuration Management Database (CMDB).”

Record

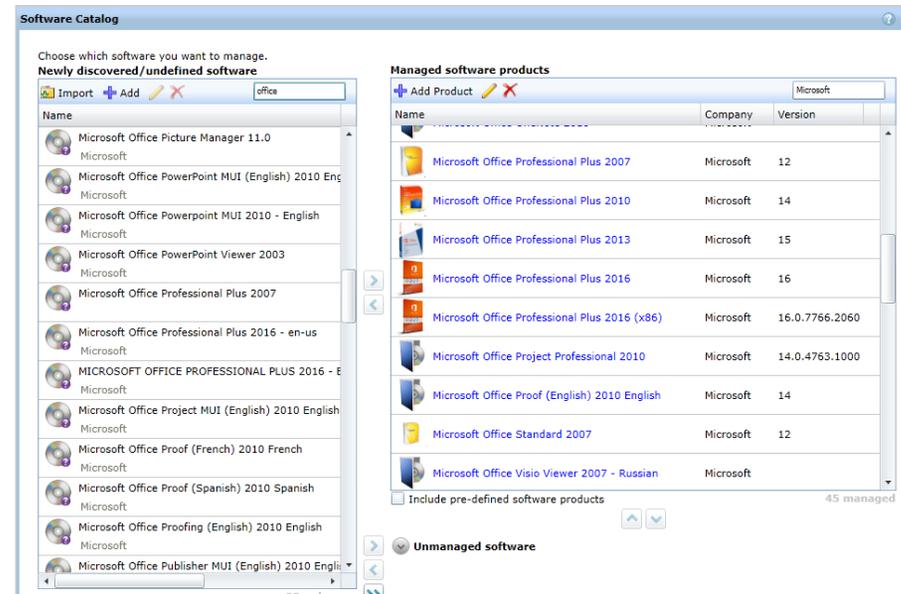
The underpinning of the Symantec approach to software asset management is its software catalog which is part of the Configuration Management Database (CMDB) and contains the meta data that enables organizations to effectively manage both supported and unsupported software. Among details found in the catalog are software detection rules, detailed information about the key executable files that are part of the software, and definitions that describe the relationship between various pieces of software. Additional details in the software catalog can be captured and customized as needed.

Following discovery and inventory, the record phase of software asset management involves the automated or manual entry of software license and purchase details and associating it with a software title such as license type, quantity, and expiration dates. License models can also

be recorded such as per seat, per user, per CPU, per core, etc. You can directly input license information, tracking definitions, purchase information and entitlements, and you may also utilize the included data connector to integrate with your procurement or other license management systems.

Recording this data establishes a baseline of what software installations are deployed in your environment as well as other parameters like the asset owner of the endpoint and software usage metering and tracking. These details are stored in the CMDB and include information such as:

- Detection rules
- Software packages
- License contracts
- License purchases
- All other CI's
- Data from third-party sources



“With the license, purchase and software inventory data, you can determine your compliance by comparing what was purchased to what is deployed.”

Reconcile

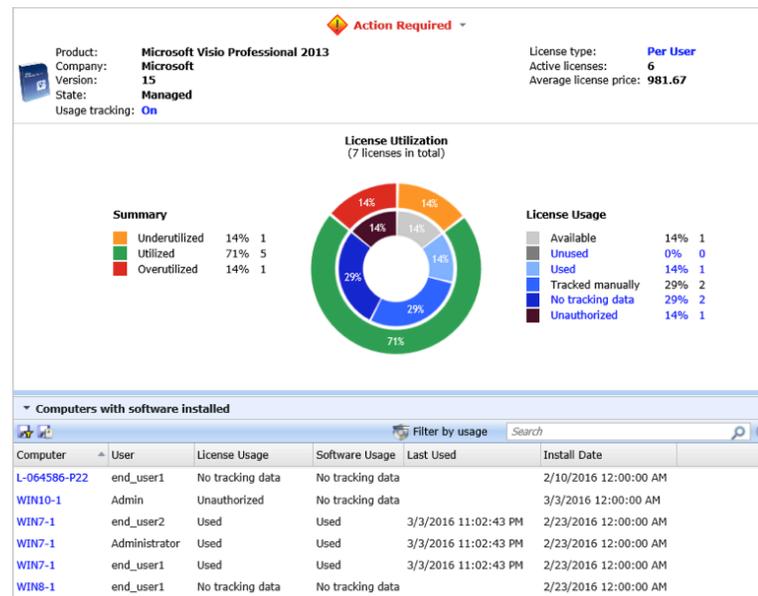
The next phase is to reconcile the software installed against software entitlements. The first step of the reconciliation process is to determine which software titles need to be metered and tracked for licensing. Consider that free titles such as Adobe Acrobat, Google Chrome, Mozilla Firefox, etc. do not need to be metered because there aren't licensing restrictions and therefore, no potential ROI savings or audit consequences. However, you will still want to manage, patch, and update these software titles just like other software titles that are metered.

After you determine which software to actively meter, define what information needs to be tracked such as version, dependencies and what updates are required. This helps to ensure the currently supported version always gets distributed and that any updates to that software are applied as part of the initial software delivery job. It also

helps to ensure that all the dependencies and pre-requisites required to use a particular application get distributed along with that software.

With the license, purchase and software inventory data, you can determine your compliance by comparing what was purchased to what is deployed. For software that has been over deployed, you may have to pay for additional licenses to meet your usage or uninstall them (also known as harvesting) to meet your license agreement. You can also use the results of your analysis to determine unauthorized installations to help take corrective actions as needed. The reconcile phase of software asset management will help you:

- Understand effective license position (how current software installation and usage compares with license agreements)
- Predict future costs and savings
- Track unauthorized installations



“You can also provide on-demand software delivery through the end user self-service app store providing users with additional flexibility to quickly obtain new applications as they are needed.”

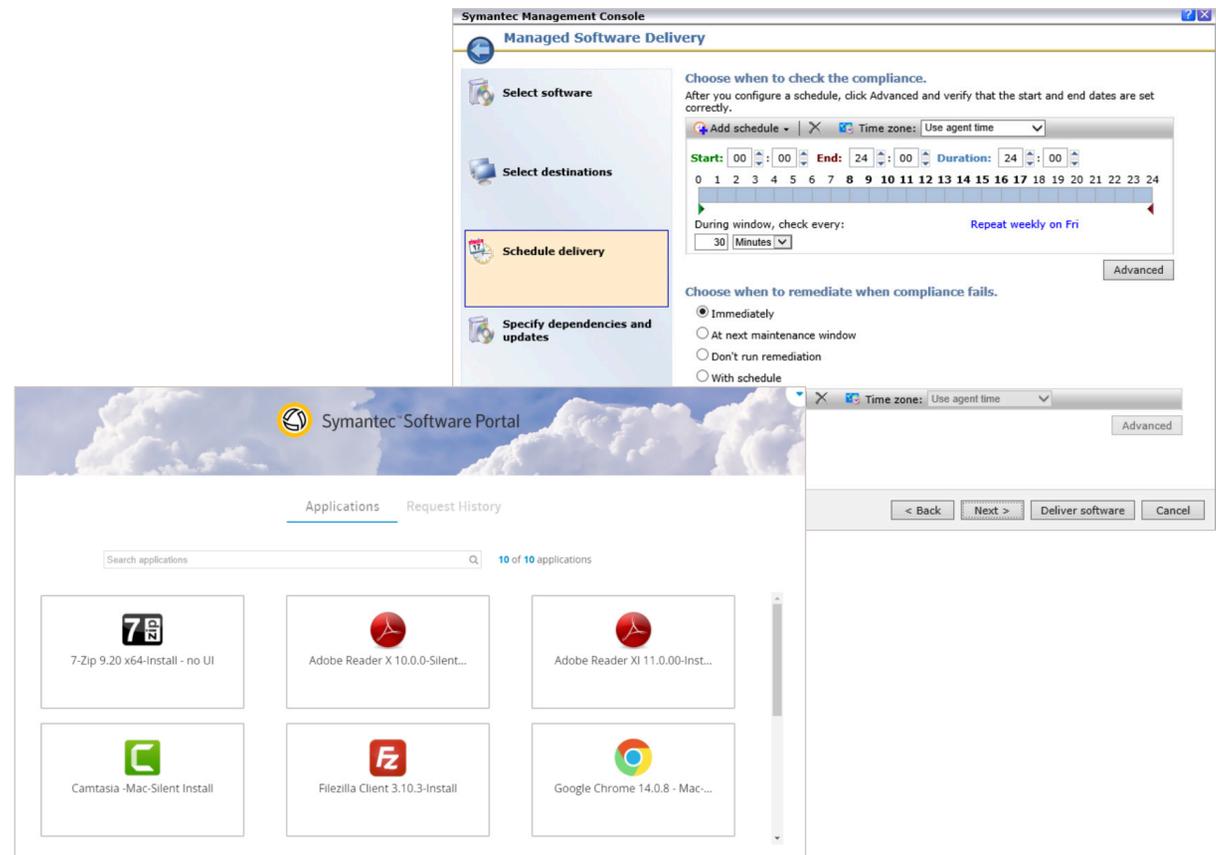
Deliver

The next phase of software asset management is the intelligent deployment of software based on the software attributes gathered in the previous phases. You can deliver and install software safely and accurately on managed client computers through the creation of tasks and policies to respond to software delivery needs from the elementary to complex.

- Traditional & policy based delivery
- Fully automated

You can also provide on-demand software delivery through the end user self-service app store providing users with additional flexibility to quickly obtain new applications as they are needed. The Symantec software portal has been recently updated and includes several new features:

- Customizable
- Browser agnostic
- Applications delivered based on user role and operating system



“Identify overutilized or unauthorized software through built-in reports and queries that will use that data to target these installations and perform uninstallation actions to remediate costly discrepancies for license true ups.”

Enforce

The final phase of software asset management is enforce and is focused on achieving software compliance and uncovering savings opportunities. Symantec integrates software metering and tracking to enable organizations to monitor the usage of software and meter the usage or control the availability of software on an on-going basis. This process also provides the ability to expose underutilized software that is installed (and perhaps licensed), but is not being used and reclaim those licenses for cost savings and better distribution.

Remediation of software license discrepancies is achieved through the identification and notification of license status, removal of overutilized or unauthorized software, the consolidation or sharing of underutilized instances, and through the control of access or execution of the application. These actions are achieved through three features that work together to manage software license discrepancies:

- **Automation Policies** - System-defined, or administrator-defined, sets of rules that govern the execution of automated actions such as running a license compliance report using the parameters that were obtained from the policy, sending an email alert to the software administrator, and executing a command or running a task on managed computers.
- **Software Harvesting** – Identify overutilized or unauthorized software through built-in reports and queries that will use that data to target these installations and perform uninstallation actions to remediate costly discrepancies for license true ups.

- **Application Metering** – Some software license terms are not just based on installation or hardware specifications, some require true control over the application itself. By combining the identification and grouping of license discrepancies with the application control features in Application Metering, you can notify or deny the use of any application to maintain compliance.

An important part of the enforce phase is the ability to report and share software management data, trends, and compliance status. Symantec software asset management includes several predefined web reports to make extracting software asset information quick and easy. You can also use the built-in reporting tools to customize reports and create new queries. You can run, share, and edit the reports based on your organization's needs.

The enforce phase of Symantec software asset management provides these benefits:

- Policy based remediation
- Consistent software profiles
- Uncover cost savings
- Prepare for audits
- Promote compliance
- Works across all endpoints both in and outside the perimeter (remote and roaming users)

Conclusion

The Symantec approach to software management is based on 5 key phases: discover, record, reconcile, deliver and enforce. Taking this approach to software management allows organizations to gain and maintain an accurate picture of all their software assets both inside and outside the perimeter, track and compare software usage against license agreements, and efficiently deploy, manage and reclaim software to uncover savings and promote compliance.

To learn more about Symantec software asset management, contact your sales representative or visit <http://go.symantec.com/manage>.

About Symantec

Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on [Facebook](#), [Twitter](#), and [LinkedIn](#).



350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com