Automating software deployment

How to transform desktops, servers, and mobile devices into self-managing devices with ManageSoft®.
Table of contents

A best practice approach to software and hardware management ........................................3
  Business requirements for enterprise configuration management ..........................3
  A unique end-to-end solution ............................................................................4

Understanding your existing IT assets ..............................................................................5
  Base-line asset discovery ..................................................................................5
  Zero-touch software and hardware inventory ......................................................6
  Automatically adopting devices for centralized management ................................7
  Web-based status reporting ................................................................................7

Managing software entitlements ......................................................................................8
  Grouping users and computers ..........................................................................8
  Packaging software for distribution ....................................................................9
  Best-practice release management processes based on ITIL and MOF ..............11
  Defining policies to specify the desired state for users and computers ..........12
  Using existing fileservers, web servers, and file shares for distribution ............14

 Automatically installing software on managed devices ......................................................16
  Checking centrally-defined policies to determine the 'desired state' ...............16
  Comparing the current state with the desired state described in policy .............17
  Downloading any differences required to achieve the desired state ..........17
  Automatic installation, updates, and repairs ......................................................19
  Central reporting to track installation progress ..................................................20

Managing the ongoing configuration management lifecycle ........................................21
  Reducing support costs with automatic self-healing ...........................................21
  Improving help desk responsiveness: remote control and diagnostics .................21
  Managing distributed data centers ....................................................................22
  Automating system builds and rebuilds ............................................................22
  Improving IT decision-making with IT business intelligence ...............................23
  Managing software licenses ............................................................................24
  Tracking hardware assets ................................................................................25
  Automating security patch management ............................................................27

Increasing reliability and reducing costs with self-managing devices ............................28
  Policy-based approach enables set-and-forget management ............................28
  Client-centric architecture provides faster implementation, increased reliability, and cost-effective scalability ..........................................................29
  A unique end-to-end enterprise configuration management solution .............31
  Find out more ................................................................................................32
A best practice approach to software and hardware management

Business requirements for enterprise configuration management

Manual processes for installing and updating software, and tracking hardware assets, are unacceptably slow and expensive in a rapidly changing business environment.

- Central IT administrators in large organizations need to be able to automatically deploy, update, and manage software for entire groups of users and computers — regardless of the location and operating system of the managed devices.

- To reduce support costs, the modern enterprise needs software installations to automatically self-heal when something goes wrong.

- For enterprise-scale deployment to Windows, Linux, and UNIX devices, bandwidth-friendly deployment is required for remote desktops and servers, and for mobile laptops on the road.

- To negotiate effectively with software vendors, IT managers need up-to-the-minute information on installed software licenses and intelligent software usage analysis.

- To avoid costly non-compliance litigation, enterprises need early notification of potential license breaches, and the ability to recapture unused licenses and reallocate available licenses across multiple business units.

- To manage hardware acquisition planning, and avoid costly late-fees for missing leased laptops, central IT administrators need accurate reporting on the status and location of hardware assets throughout the enterprise.

- To improve IT support, help desk professionals need up-to-the-minute diagnostics reports with click of a button access to information on currently installed software and hardware. To enable faster problem resolution, help desk professionals also need the ability to click through from diagnostics reports to integrated remote control tools.

- To prevent crippling virus attacks, organizations need to automate security patch management.

- To improve IT decision-making, CIOs and IT managers need rapid answers to complex IT questions with out-of-the-box analysis for common IT questions, and easy ad-hoc analysis for rapid answers on the fly.

ManageSoft provides a comprehensive configuration management solution to solve these challenges by transforming desktops, servers, and mobile devices into self-managing devices.
A unique end-to-end solution

ManageSoft is an enterprise solution to comprehensively address these business requirements. The unique ManageSoft smart agent architecture delivers the breadth of functionality, scalability and reliability of a best-of-breed configuration management tool, while also providing the quick implementation times, low infrastructure costs, and low ongoing administration costs that have traditionally been associated with point solutions that can only address one or two configuration management challenges. This integrated approach combines policy-based management with a client-centric architecture to provide the fastest and most reliable way to automatically deploy, update, and manage software and hardware assets throughout an organization.

Figure 1: ManageSoft integrated configuration management solutions
Understanding your existing IT assets

Obtaining an accurate inventory of existing IT devices throughout an organization can be time consuming and prohibitively expensive. Yet to manage an organization’s valuable investment in IT assets IT administrators need to know what software and hardware assets the organization owns, where those assets are, and how they are configured. ManageSoft provides a comprehensive automated solution to enable central IT administrators to rapidly compile an accurate initial inventory of devices in use throughout the organization, and an automated process to adopt devices for ongoing centralized management:

- Base-line asset discovery
- Zero-touch software and hardware inventory
- Automatic adoption of devices for centralized management
- Web-based status reporting

The very first step in implementing a centralized software management solution is to build an accurate baseline of the existing live environment.

Asset discovery is a key differentiator of the ManageSoft solution. ManageSoft provides out-of-the-box integration with best-of-breed asset discovery tools including HP OpenView Network Node Manager, Fluke Networks LAN MapShot, and Fluke Networks Network Inspector, and can also import existing data from a Microsoft Excel spreadsheet. This identifies all computers logged on to the network at the time of the initial discovery process, and automatically detects any other computers when they next log in to the corporate network. This cumulative process ensures that even mobile laptop users that only log on intermittently are detected at the first opportunity.

Asset discovery (sometimes referred to as ‘network discovery’) provides an accurate picture of what IT assets are already out in the live environment. This gives an accurate baseline benchmark to use for inventory gathering, planning, and monitoring progress in implementing a centralized software management solution. For many large organizations currently struggling to keep track of fixed and mobile IT assets, this step alone is a significant achievement and a major benefit of the ManageSoft solution.
Zero-touch software and hardware inventory

Having used asset discovery to find out which devices are in use in the organization’s live environment, it is then crucial to find out accurate hardware and software inventory details for those devices — what is installed where, and how it is configured. This is critically important to the success of enterprise software management as accurate inventory data is required to understand what software and hardware assets are already in use, what operating systems are currently in place, and which hardware and software requires upgrading or replacement. Initial assessment of these considerations based on accurate inventory data is vital to avoid potential disruptions later in the software management lifecycle. ManageSoft addresses this important step with a transparent innovative ‘zero-touch’ inventory gathering process for Windows, Linux, and UNIX systems throughout the enterprise.

Unlike other solutions that require a preliminary rollout of scanning software onto every target computer (which can be a major exercise in itself), questionnaires, hands-on probing (which involves travel for IT support personnel, and requires mobile laptops to be returned from the field to central IT support teams), or other inefficient task-intensive methods, ManageSoft initially can use smart agents hosted on servers to detect and automate the capture of relevant hardware and software configuration management information from devices throughout the organization — processor/speed, RAM, disk space, operating system, IP address, MAC address, peripherals, software installed, and much more. This information is critical to understanding the scope of a new centralized software management project, including compatibility issues, upgrade requirements, new purchasing requirements, and associated time and budget impacts.

ManageSoft obtains this inventory data when devices connect to networked servers. In rare instances where a device identified through earlier asset discovery isn’t accessible during inventory gathering, an e-mail alert can be sent with a click-through link to trigger the inventory gathering process for that computer.

ManageSoft also overcomes one of the significant drawbacks of other zero-touch inventory tools: reliance on Microsoft Windows Management Interface (WMI). ManageSoft can use but does not require WMI on target Windows computers, which means that inventory can also be gathered from computers running unmodified older operating systems, including Windows 9x and Windows NT 4.0 which do not have WMI installed by default.

WMI provides a common interface for tools to query information about hardware and software on a Windows computer. It is a very detailed and effective inventory tool, and where it is installed on a computer, ManageSoft makes full use of the available WMI inventory data. However, the problem with relying solely on WMI for many enterprise configuration management projects is that WMI is not installed by default on legacy Windows platforms, and of course WMI is not available on Linux and other UNIX systems. WMI is only installed by default on Windows 2000 and later Windows operating systems. WMI can be installed on legacy Windows platforms but to use WMI to gather inventory on legacy platforms would require WMI to be rolled out prior to the inventory gathering, which would be a significant project in itself, and would require administrator rights and a reboot of the system.

ManageSoft provides a solution that enables key hardware and software information to be gathered initially from each Windows, Linux, and UNIX device without requiring installation of an agent on the device, without requiring WMI to be installed on Windows devices (but leveraging WMI if it is available), and without requiring elevated privileges on the device. This unique zero-touch approach provides increased accuracy and significantly reduces the time required to rapidly gather an initial hardware and software inventory for all computers to be brought under central IT management. (Of course once computers are later adopted for centralized management, ManageSoft is then able to provide client-side inventory tracking with ManageSoft smart agents on each managed device automatically uploading inventory data for centralized analysis and reporting).
Automatically adopting devices for centralized management

The unique ManageSoft smart-agent architecture avoids the drawbacks of expensive server-centric solutions, by transforming each computer into an intelligent self-managing device. ManageSoft does this by placing intelligence on the managed device itself through the use of client-side ManageSoft smart agents. Unlike time-consuming server-centric software management products, which typically require a lot of new hardware and can take many months to implement, the ManageSoft client-centric architecture provides an extremely fast, low infrastructure implementation with a unique automatic adoption process. Using a process similar to the zero-touch inventory process, ManageSoft automatically detects all devices throughout the organization, and can remotely install ManageSoft smart agents to adopt these devices for ongoing central management with ManageSoft. This enables remote desktops, servers, and mobile devices to be brought under central management very rapidly, without requiring a costly rollout of a proprietary server infrastructure, and without expensive travel and onsite support visits.

Web-based status reporting

Accurate and timely progress reporting is critical to the efficient management of any large-scale IT project. ManageSoft provides detailed web-based progress reporting to enable IT administrators to track the inventory gathering progress and progressive rollout of the ManageSoft agent, against the baseline obtained through asset discovery. (For example, if asset discovery revealed 10,000 desktops, laptops, and servers in the live environment, but the latest ManageSoft report only includes installation of ManageSoft smart agents on 8,000 devices, the adoption process is only 80% complete.) ManageSoft web-based reporting is accessible through a customizable executive dashboard. The executive dashboard provides up-to-the-minute graphical summary reports with click-through access to drill down to increasing levels of detail. The executive dashboard is built on Microsoft .NET technology and can be undocked from the ManageSoft console and floated on each project manager’s desktop for minute-by-minute monitoring. This level of progress reporting is critically important for large-scale software management implementations, and a huge time-saver for IT professionals.

Figure 2: Web-based progress reporting
Managing software entitlements

The initial discovery and adoption phase provided the information and initial installation of ManageSoft smart agents required as a foundation for centralized management of desktops, servers, and mobile devices throughout the organization. The next phase involves assessing the current state of all existing hardware and software assets adopted for centralized management, and defining the new desired state:

- Grouping computers and users
- Packaging software for distribution
- Defining policies to specify the desired state for users and computers
- Making software packages available for download by managed devices

Grouping users and computers

A highly accurate directory service is vital for efficient IT service support and IT service delivery. This is particularly true for software deployment targeting, and for meaningful management reporting. To be useful, the mass of discovery and inventory data collected in inventory and adoption phase needs to be organized into meaningful groups for management purposes. ManageSoft provides a powerful way to use a single directory service to manage Windows, Linux, and UNIX devices throughout an organization.

Microsoft Windows 2000, Windows XP, and Windows Server 2003 provide a range of enterprise management technologies to enable cost-effective management of Microsoft Windows-based desktops, laptops, and server applications. Key among these technologies is Active Directory. Active Directory enables organizations to manage and share information centrally on network resources and users while acting as the central authority for network security. Using Active Directory, users and computers can be grouped into Organizational Units (OU’s), sites, domains, security groups, and Group Policy Objects. Active Directory has rapidly become the industry standard for corporate directory services.

ManageSoft is the only software management solution to provide native use of Active Directory — without additional costly adapters or cumbersome synchronization of policy information with a proprietary directory service. Unlike traditional software deployment products that store policy information in proprietary databases, ManageSoft targets software deployment through the site, domain, and organization unit (SDOU) structure, security groups, and group policy extensions that are native to Active Directory. ManageSoft does this without extending the Active Directory schema, which means that IT professionals can leverage existing Active Directory Group Policy knowledge and skills. ManageSoft also provides a unique solution that enables Active Directory to be used to manage legacy Windows platforms, and to manage non-Windows platforms including Linux and other UNIX systems.

The first step though, is to populate Active Directory. Some organizations already have a functioning directory service before commencing implementation of a software management solution. However if you do not, ManageSoft can automatically populate Active Directory, using the discovery and inventory data obtained in the initial inventory phase. This facilitates enterprises migrating to Active Directory for the first time, because it dramatically reduces the time, project risk, and cost of new Active Directory implementations. ManageSoft can also provide solutions to migrate to Active Directory from other directory services such as Novell.
While Active Directory is a key feature of the Windows 2000, Windows XP, and Windows Server 2003 platforms used by many corporations, initial implementation of a centralized software management solution requires a decision as to the appropriate level of Active Directory implementation for the organization. Some organizations choose to install Windows 2000 or XP on desktops and laptops throughout the organization without ever taking advantage of the powerful directory service that Active Directory provides. ManageSoft accommodates individual organizational preferences by providing three distinct models of Active Directory use for centralized software management:

- **Deploy Active Directory now** — Roll out the entire Active Directory infrastructure first, and use that foundation to manage Windows devices throughout the organization. Unlike other products that link to Active Directory only for server-side storage, ManageSoft client-side smart agents on Windows devices can apply software policies directly from Active Directory domain controllers. There is no need for duplicate policy servers (and, importantly, no Active Directory schema changes). At the same time, ManageSoft provides enhancements such as scheduling, inventory, license management, and powerful reporting, extended reach to remote offices and mobile devices on the road, and also provides XML policy distribution for UNIX devices unable to access Active Directory domain controllers directly.

- **Deploy Active Directory later** — Implement Active Directory more slowly, at a pace to suit the business. Since ManageSoft smart agents do not require Active Directory infrastructure on local domain controllers, or distribution servers, or managed devices, this model provides a safe way to test and refine Active Directory design, without ‘resetting’ the entire enterprise. In this model a central single-server Active Directory installation is used to define groups and manage entitlements through policy. ManageSoft then distributes policies through the use of bandwidth-friendly lightweight XML files to provide immediate cross-platform management for Windows, Linux, and UNIX devices. If and when the organization later decides to roll out Active Directory to desktops, laptops, and servers, ManageSoft smart agents on managed devices simply switch over to access policies directly from Active Directory domain controllers — providing a seamless transition.

- **No Active Directory implementation** — Centrally manage Windows, Linux, and UNIX devices throughout the organization without ever deploying Active Directory. In this model, ManageSoft provides a solution where central smart agents utilize a single-server installation of Active Directory, together with XML policy distribution to managed devices, without ever requiring Active Directory to be implemented enterprise-wide. It is a powerful policy-based management solution for organizations that choose not to rollout Active Directory.

This unique combination of client-side and server-side policy merging means that users on multiple platforms, inside and outside the corporate firewall, can be managed with a single deployment policy and management interface.

**Packaging software for distribution**

Every existing application to be retained on managed devices, and every new application to be deployed needs to be tested on each of the operating systems in use throughout the organization. To ensure the success of a new centralized software management system, you need to be confident that every application, whatever the source, will function as intended on the operating systems currently used by managed devices throughout the organization.
Having decided on the required applications to be managed, you then need to package the applications in a format suitable for automated distribution and installation. Application packaging can be complex and expensive in many organizations, so it is very important to be able to reuse existing packages where appropriate. ManageSoft provides wizards for “receiving” existing software packages into a central software library along with relevant data such as licensing data and terms, price, and more. This lays the foundation for improved license tracking and management in the future. ManageSoft also provides powerful, flexible, and straight-forward application packaging facilities for new software packages.

ManageSoft provides wizards for “receiving” existing software packages.

ManageSoft smart agents and wizards make preparing packages fast, and reliable. ManageSoft supports Windows packaging formats including MSI (Windows Installer) packages and third-party Windows packages from InstallShield, Wise, and others, and provides a powerful and flexible native package format for non-standard installations. Facilities including a snapshot wizard, a plain-text package format, and scripting, make difficult installations simple and fast. ManageSoft also supports non-Windows packaging formats including RPM packages, and SD-UX.

- **Windows Installer (MSI) packaging** — Many commercial applications use the Windows Installer (MSI) format for installations. ManageSoft fully supports MSI installations on all Win32 platforms. Using any standard packaging tool such as Wise for Windows Installer or InstallShield for Windows Installer, you can customize the installation process while simultaneously adhering to Windows Installer guidelines. This ensures that the application installs according to the MSI standard definition while enabling you to tailor the application installation to specific needs. Unlike competitive solutions, the ManageSoft packaging process does not modify the MSI package, thereby preserving its attributes. ManageSoft also enables multiple MST transforms to be attached to a single MSI package to enable installation customizations (for example, to change the spelling checker language in Microsoft Office). This dramatically reduces package storage requirements, and reduces bandwidth consumption during package downloads.
- Packaging non-Windows Installer applications — ManageSoft also supports third-party installers and off-the-shelf or custom applications that are not in Windows Installer (MSI) format. Through the use of a snapshot wizard, ManageSoft provides a simple graphical tool that allows you to package any application without cumbersome installation scripts.

- ManageSoft state-based packaging — ManageSoft also offers its own state-based packaging format. Unlike traditional software management solutions that store packages in binary, proprietary databases, ManageSoft describes the content of an application using the lightweight XML-based Open Software Description (OSD) standard, which enables ManageSoft to easily and intelligently determine optimal updates. Using the OSD file, ManageSoft can control the application installation properties based on each individual end-point. The administrator can also configure smart agents on managed devices to perform silent, semi-silent, interactive, or scripted installations. ManageSoft also provides the ability to check for optional pre-installation and post-installation conditions before, during, and after installation. It’s also easy to modify packages you’ve created because there is no need to use a complex, object-oriented programming language. ManageSoft enables you to revise and customize software and content at any point in the publisher-to-subscriber deployment process. As a result, IT administrators can customize standard published software offerings without having to unpack and repack.

- RPM and SD-UX packaging — ManageSoft fully supports RPM and SD-UX packages for Linux and other UNIX platforms. ManageSoft wizards enable easy import of RPM and SD-UX packages. ManageSoft also enables central administrators to save time with intelligent native package management. RPM and SD-UX packages typically depend on multiple other packages. To accommodate this ManageSoft provides automatic dependency management to simplify packaging and deployment.

- Cross-platform packaging — ManageSoft enables you to create a single package that can be installed across multiple Windows, Linux, and UNIX platforms. This simplifies the packaging process, reduces packaging cost, reduces storage requirements, and conserves bandwidth during distribution.

Best-practice release management processes based on ITIL and MOF

Effective process management, with predictable and measurable outcomes, is critical to IT and business success. The vendor-independent IT Infrastructure Library (ITIL) best-practice guidelines provide a framework for managing information technology to optimize service levels and support business objectives. ITIL is recognized as the world standard for IT service support and service delivery (www.itil.co.uk). The Microsoft Operations Framework (MOF) applies ITIL guidelines in the context of Microsoft technologies (www.microsoft.com/mof). Release management is a key aspect of ITIL/MOF service support.

ManageSoft embodies industry best-practice packaging and release management processes, as documented in the vendor-independent IT Infrastructure Library (ITIL) and the Microsoft Operations Framework (MOF). In keeping with ITIL recommendations, ManageSoft stores software packages in a central Definitive Software Library in the organization’s central ManageSoft software warehouse. This Definitive Software Library is an inviolable archive of every version of every application distributed in the enterprise using ManageSoft.

Regardless of which software management tool that an organization selects, without documented, reliable, and repeatable IT processes in place the organization faces a far greater risk of failure. ManageSoft is unique in embedding ITIL/MOF best practice release management processes in online documentation and templates. ManageSoft provides out-of-the-box online best practice guidelines and detailed work instructions on how to manage the release of software and other configuration changes within the organization. These guidelines are also available as templates that allow an organization to customize the process if required to suit specific business processes.
The next step is to specify which groups of users and/or computers should receive what software applications, and when.

Defining policies to specify the desired state for users and computers

Once software applications have been packaged and tested, the next step is to specify which groups of users and/or computers should receive what software applications, and when. While it is possible deploy software to individual users, one of the strengths of ManageSoft lies in its ability to work at the policy level. This provides an opportunity to move to a ‘role-based’ or ‘user-centric’ model of IT operations management. By definition, a role-based approach replaces traditional one-size-fits-all standard operating environments, and instead focuses on delivering what specific groups of users need to perform their particular job-role, and delivering it when they need it.

ManageSoft provides unequalled reliability and control for role-based software deployment with true policy-based management. Policy-based automation avoids the costs and time delays associated with alternative labor-intensive task-based systems. With ManageSoft, IT administrators can define software policies specifying which groups of users and computers should receive what software — the ‘desired state’ for each managed device.

Since ManageSoft is content-independent, the desired state you describe in policy can include packages for any kind of software or content — including applications written in any language or composed of any type of distributed component, such as Java, C++, Microsoft Visual Basic, security patches, virus definition files, operating system configuration parameters, registry keys, icons, drivers, embedded links, data files, graphics, audio, video, web content, and interactive maps. Policies can allocate software as either mandatory (for automatic installation) or optional (to be added to a customized list for user selection).

The desired state is a fundamental design principle of the ManageSoft policy-based, client-centric architecture. This unique smart-agent architecture transforms computers into self-configuring, and self-healing devices. With ManageSoft, managed devices automatically compare their current state with the desired state described in centrally-defined software policies, and automatically download and install any differences required to achieve the desired state — without requiring human intervention. By transforming computers into self-managing devices ManageSoft significantly improves application uptime, and dramatically reduces telephone support requirements.
The desired state for each computer can be defined in one or more software deployment policies relating to groups of users and/or computers. ManageSoft automatically resolves a set of applicable policies to determine the resultant policy for a given device. Policies can target installations by business unit (Active Directory Organizational Units or Group Policy Objects), by cross-divisional user types (Active Directory Security Groups), or even by individual user or computer. These central policies give you the flexibility to assign software based on business functional groupings, including groups that cut across your organization chart, and including groups that use multiple operating systems. You can allocate software to any meaningful group of users and/or computers defined in Active Directory. Once again, it is important to note that while ManageSoft uses Active Directory centrally to target software deployment, Active Directory is not required on managed devices. Once policies have been defined centrally in Active Directory, managed devices with Active Directory installed can access policies directly from domain controllers, and other computers (including Linux/UNIX devices) can access policies through the lightweight XML policy distribution that ManageSoft enables.

In Windows 2000, XP, and Server 2003, software entitlements can be represented in Group Policy objects. ManageSoft is the only vendor solution built from the ground up on Active Directory Group Policy and related Security Groups. For corporations that have already rolled out an Active Directory infrastructure, ManageSoft uses native Active Directory Group Policy to deliver software policies — there is no need for a parallel policy server structure or Active Directory schema extensions which other solutions require for ongoing software management. In this configuration, managed devices access policies directly from Active Directory domain controllers. By contrast, for organizations that decide to delay rolling out Active Directory to desktops and laptops, and for organizations that choose to maintain a heterogeneous environment with Windows, Linux, and UNIX systems, ManageSoft can use a central single-server installation of Active Directory and distribute policies to devices as lightweight XML files.

Figure 5: Policy-based management built on Active Directory

Describe your organization
Allocate software
Deploy
Manage

Group users and computers logically within Active Directory
Use a single directory service to manage Windows, Linux, and UNIX devices. Describe business units, job-roles and other groups using native Active Directory sites, domains, and organization units (SDOU), security groups, and Group Policy extensions
Define deployment policies for each group within Active Directory
Example: ‘mandatory software’
Who: All sales laptops
What: Install/manage ‘catalog and price list’
When: Update/repair hourly when connected
Implement: Immediately
Example: ‘optional software’
Who: Marketing employees
What: Install/manage ‘graphics application X’
When: Update/repair 10pm daily
(if user has selected this optional software)
Implement: From May 10 onwards

Apply policies automatically
Apply to users and computers throughout the organization, even if Active Directory is not installed on end-user computers

Manage with web-based reporting
Use up-to-the-minute graphical reporting, built on Active Directory, to monitor deployment progress, manage software licenses, and track hardware and software assets

"Software configuration management solutions that provide policy-based automation of software management processes on desktops, laptops, and servers throughout an organization can deliver considerable IT savings that are not possible with labor-intensive task-based systems."

- Ronni Colville, Research Director, Gartner.
www.gartner.com
Using existing file servers, web servers, and file shares for distribution

To minimize network traffic and maximize service levels, managed devices need to be able to download new software and software updates from a local distribution location. For example, a user travelling from one city to another should receive software updates from a distribution location in the local office instead of having to connect back to their home office across the WAN. This means that new software packages need to be distributed in the first instance from the central software warehouse to distribution locations throughout the organization.

The client-centric ManageSoft smart-agent architecture is unique in enabling organizations to use any existing file server, web server, network share, print server, or file share as a distribution server for enterprise software configuration management. This is a fundamental difference from traditional software configuration management products. Unlike traditional server-centric products, ManageSoft places all of the intelligence on the managed device itself, with ManageSoft smart agents on each managed device automatically determining what software updates are required, and automatically downloading software updates from the nearest available software distribution location. This client-centric architecture provides dramatic scalability and cost advantages over alternative products that require a dedicated proprietary server infrastructure. Use of existing IT infrastructure also enables extremely fast initial implementation of ManageSoft. Many organizations implement ManageSoft without needing to install or maintain any new hardware in offices brought under central management.

ManageSoft automates the distribution of software packages to remote distribution locations, through an intelligent distribution hierarchy. This automated distribution of software packages is a distinct time-saver for geographically dispersed organizations that in the past have relied on CD couriers to distribute extremely large files for remote sites. ManageSoft makes automated distribution of large software packages realistic and highly reliable, with a range of industry-leading mobile and remote deployment features enabling reliable, bandwidth-friendly distribution of packages to remote sites, even over highly unreliable networks:

- **Distribution job prioritization** — ManageSoft enables distribution jobs to be prioritized when bandwidth or other resources are constrained.
- **Auto-resume after interruption** — ManageSoft provides checkpoint restart so an interrupted download never needs to be restarted from the beginning.
- **Byte-level differencing** — ManageSoft only distributes new or changed portions of a package to locations that already have an earlier version.
- **Dynamic bandwidth throttling** — The amount of bandwidth consumed during distribution can be configured to provide maximum flexibility.
- **Distribution time windows** — ManageSoft enables discrete time windows to be defined during which only a specified percentage of bandwidth is used.
- **Distribution progress reporting** — Distribution of packages, policies, and schedules to the distribution locations can be tracked centrally.

For more information about bandwidth-friendly deployment to remote sites, see the ManageSoft white paper: “Improving IT service levels for remote offices.”
ManageSoft makes automated distribution of large software packages realistic and highly reliable.

- Distribution job prioritization
- Auto-resume after interruption
- Multi-session download ("drip feed")
- Byte-level differencing
- Bandwidth throttling ("drizzle")
- Distribution time windows
- Distribution progress reporting
Automatically installing software on managed devices

With software packages now available on distribution locations, you are now ready to install software on managed devices. Instead of relying on an expensive, high-maintenance server-centric architecture to determine what software to install on each managed device, the ManageSoft client-centric architecture is unique in placing all intelligence and performing all calculations on the managed device itself. Client-side ManageSoft smart agents transform managed devices into self-managing devices that automatically adapt and self-heal in accordance with centrally defined software policies:

- Checking centrally-defined policies to determine the ‘desired state’
- Comparing the current state with the desired state — client-side intelligence
- Client-side downloads of any differences required to achieve the desired state
- Automatic installation, updates, and repairs
- Central reporting to track installation progress.

Checking centrally-defined policies to determine the ‘desired state’

ManageSoft smart agents on managed devices automatically download centrally-defined policies that describe the desired state for the user and computer. If the organization has elected to roll out Active Directory throughout the enterprise, the managed device accesses relevant policies directly through Active Directory. Alternatively, if Active Directory is not available on the managed device (which will be the case for older versions of Windows, and Linux/UNIX devices, and may also be the case for newer Windows devices in organizations that have not rolled out Active Directory), ManageSoft smart agents on managed devices simply download relevant policies from the nearest distribution location in lightweight XML files. This provides maximum flexibility for the IT organization, and immediate cross-platform management regardless of the organization’s current level of commitment to Active Directory. Whether policy is accessed directly through Active Directory, or through XML policy files, client-side ManageSoft smart agents perform this policy checking silently with no impact on the end-user.

**Figure 7: Managed devices check centrally-defined policies to determine the ‘desired state’**

Client-centric triggers for scheduled policy checks:

- Start-up
- Log-on
- Use of specific application(s)
- Network connection (‘OnConnect’)
- Delay after connection (‘OnConnect Plus’)
- ‘Immediately’ for urgent updates (including Wake-on-LAN - even across a WAN)
- Fixed times (including Wake-on-LAN)
- Random times within a time window
- Regular defined intervals
- Catch-up missed triggers at next logon
Comparing the current state with the desired state described in policy

ManageSoft smart agents on each mobile device then automatically compare the current state of the managed device, with the desired state described in relevant centrally-defined policies. This client-side intelligence is a key benefit of the ManageSoft solution. Unlike products that rely on high-overhead server-centric processing to determine what updates are required (which introduces a potential single-point-of-failure to the enterprise and is dependent on highly reliable network connections), ManageSoft smart agents provide client-side intelligence to remove any single-point-of-failure architectural characteristics, to deliver dramatically increased reliability, to enable ongoing scalability, and to significantly reduce infrastructure costs.

Figure 8: Client-side smart agents calculate differences between current state and desired state

ManageSoft excels on LAN, WAN, VPN, dial-in, satellite links, and the Internet.

Downloading any differences required to achieve the desired state

Once ManageSoft smart agents on the managed device have determined exactly what’s needed to bring the device to the desired state:

- Any 'optional' software specified in relevant policies is automatically added to a customized list available for end-user selection (user selection at any time thereafter automatically triggers the process below)

- Any missing 'mandatory' software specified in relevant policies (and any user-selected 'optional' software) is automatically downloaded from the nearest distribution location.

Unlike tools that make LAN-based assumptions and treat mobile devices and remote offices as an afterthought, ManageSoft excels on LAN, WAN, VPN, dial-in, satellite links, and the Internet. ManageSoft smart agents on the managed device use intelligent byte-level differencing to only download the differences needed to update an existing application to a new ‘desired state’. Unlike competitive technologies ManageSoft also uses byte-level differencing for ongoing self-healing. ManageSoft will never download an entire application again if the files required for an update are already available on the managed device.
ManageSoft also provides an extensive range of bandwidth and reliability capabilities.

ManageSoft also provides an extensive range of bandwidth and reliability capabilities that make ManageSoft ideal for organizations with multiple remote offices and/or large numbers of mobile workers. These unequalled mobile and remote management capabilities, which are described in more detail in other ManageSoft white papers, include:

- **Automatic detection of nearest distribution location** — Managed devices automatically download updates from the closest location, rather than over the WAN. ManageSoft uses a range of configurable algorithms to determine the closest location including IP address matching, ping results, domain matching, subnet matching, and other criteria.

- **Client-side intelligence for dynamic byte-level differential downloads** — Patented ManageSoft smart agent technology enables faster updates and minimizes network bandwidth consumption because there is no need to transfer entire applications or files just to make minor repairs and updates.

- **Client-side bandwidth management** — Smart agents use dynamic bandwidth throttling to apply centrally-defined bandwidth consumption rules based on detected network speed. End users can also modify bandwidth use through an easy-to-use user-slide-control.

- **Automatic detection of a network connection** — Unlike products that are incapable of supporting mobile users that connect from different locations at different times, ManageSoft enables mobile devices to silently check for software updates at every opportunity (for example on each new network connection).

- **Client-side server auto-failover after interruption** — If a distribution location is inaccessible or ‘times out’ during a software update, smart agents on the managed device automatically failover to the next available distribution location and resume the download from the point of interruption.

- **Client-side byte-level auto-resume after interruption** — If the connection is interrupted during a download, ManageSoft smart-agents on the managed device automatically resume the download process at the next opportunity and continue on from the point of interruption (byte-level restart) without needing to start the download again from the beginning.
- Pre-caching of install files for future installation — Deployment policies can specify pre-caching of install files to enable installation at a future specified date. If permitted, end-users can also elect to delay an installation (within centrally-defined limits).

- Total reliability even over the slowest and most unreliable networks — ManageSoft customers currently use ManageSoft to update devices with extreme network challenges including:
  - Thousands of remote offices with low-bandwidth connections
  - Deployment to Government embassies worldwide, with dramatic variations in network quality depending on the location of the embassy
  - Secure HTTPS deployment through firewalls
  - Low-speed Internet connections
  - VPN laptop dial-in links for a national sales force
  - High latency satellite links to laptops on remote ships
  - Wireless links to computers in police cars for a metropolitan police force.

**Automatic installation, updates, and repairs**

ManageSoft enables application downloads to ‘drizzle’ in the background anytime a desktop, server, or mobile devices has an available network connection. This provides background data transfers without impacting on end-user productivity. All downloads are stored in a staging area until the download is complete. As a result end users are never left with an incomplete installation; the old version of an application remains fully functional until all required files are available to install the new version. Once all of the necessary components are downloaded, ManageSoft smart agents automatically install the new or updated software on the device. The method of installation is determined by the software packaging format selected by central administrators, and other configurations specified in relevant policies.

*Figure 10: Smart agents install, update, and repair to achieve the desired state described in policy*
Central reporting to track installation progress

Unlike tools that make unrealistic LAN-based assumptions about all computers being accessible over high-bandwidth connections at all times, ManageSoft is designed to accommodate the demands of the more diverse IT environments in many large organizations. Software rollouts inevitably involve a progressive upgrading of computers because mobile users are often disconnected from the corporate network, and desktops and even servers are inevitably offline at various times due to network interruptions, hardware failure, or even end-user intervention. It is therefore critical that central IT administrators be able to track the progress of time-critical updates to know which desktops, servers, and mobile devices have completed the new installation, and which computers have yet to receive the new update. ManageSoft provides minute-by-minute progress reporting for each new rollout, with powerful summary reporting, and easy drill-down to the required level of detail.

Figure 11: Track software rollouts with up-to-the-minute web-based progress reporting
Managing the ongoing configuration management lifecycle

At this point ManageSoft has successfully installed all new and updated software on targeted devices throughout the organization. Unlike simple target-and-deploy tools that provide no further assistance after an initial ‘push’ distribution, ManageSoft provides ongoing client-centric intelligence and policy-based automation for self-managing devices long after the initial roll out of new software:

- Reducing support costs with automatic self-healing
- Improving help desk responsiveness: remote control and diagnostics
- Managing distributed data centers
- Automating system builds and rebuilds
- Improving IT decision-making with IT business intelligence
- Managing software licenses
- Tracking hardware assets
- Automating security patch management

Reducing support costs with automatic self-healing

Once a successful download and installation process is completed, ManageSoft smart agents on the managed device ensure that the integrity of the application is maintained automatically over time with innovative client-side self-healing features. Smart agents on each managed device automatically track the status and configuration of all managed software — right down to the individual components — and compare the current state to the desired state described in centrally-defined policies. This is significant for mobile ‘road warriors’ in the organization, and for employees in small remote offices, as these end-users often do not have access to local IT support resources. ManageSoft automatically detects any files that become corrupted, or are missing for whatever reason (including accidental or deliberate deletion by the end-user), and automatically restores the managed device to the desired state described in policy. If the required files are available on the managed device ManageSoft silently performs this repair offline. If new or replacement files are required, smart agents on the managed device automatically calculate the minimal download required (byte-level differencing), and automatically download the required bytes to perform the self-healing repair.

Improving help desk responsiveness: remote control and diagnostics

ManageSoft customers report dramatically reduced help desk loads with ManageSoft providing policy-based management and automatic client-side self-healing. While the frequency of help desk calls is dramatically reduced, there will still be some instances when end-users call the corporate IT help desk for assistance with desktops, laptops, and even with servers in small remote offices without local IT support. ManageSoft provides a comprehensive remote control and diagnostics solution which gives authorized help desk professionals touch-of-a-button access to current configuration data about the end-user’s computer including policy compliance, installed software versions, installed hardware, available memory and other vital support information. Help desk professionals can click through from any of these reports to take control of the remote computer. ManageSoft remote control enables you to see the desktop of a remote computer and control it with your local mouse and keyboard, just like you would if you were sitting in front of that computer. This reduces the need for onsite support visits, improves help desk responsiveness, and delivers faster time to resolution, which can significantly reduce enterprise IT support costs.
Managing distributed data centers

The ManageSoft client-centric architecture provides rapid server provisioning across any network, with automatic server discovery, inventory, deployment, configuration, remote control, OS provisioning, and security patch management. ManageSoft provides secure, bandwidth-friendly server provisioning for LAN, WAN, VPN, dial-in, satellite links, and the Internet. This enables central IT administrators to manage remote file servers, print servers, application servers, domain controllers, database servers, web servers, and Intel-based blade servers from HP, Dell, and IBM. Using the same policy-based management interface used to manage desktops, mobile devices, and servers significantly reduces management complexity and infrastructure costs.

Automating system builds and rebuilds

ManageSoft provides set-and-forget policy-based reliability for mobile computers, with automatic self-healing if a software installation is corrupted for whatever reason. However, there are occasions when IT administrators want to quickly and reliably rebuild a system and restore it to its previous state. For organizations that need to automatically rebuild Windows desktops, and mobile devices, ManageSoft for Windows Deployment is an ideal extension to the ManageSoft software management solution:

- **Automated system builds for new computers** — Building a new laptop or desktop PC for a new user simply involves adding the user and computer to the relevant organizational unit and/or security group in Active Directory. ManageSoft for Windows Deployment then automatically determines, downloads, installs, and configures the required operating system and job-role-specific software appropriate to the particular end-user and computer.

- **Automated operating system migration** — Unlike processes that wipe everything during an OS migration, ManageSoft automatically saves and restores user data and settings to that end-users can start working productively again immediately after migration to a new Windows operating system.

- **Automated system rebuilds** — Unlike other solutions, ManageSoft provides far more than a simple rebuild back to the state when the last operating system image was created. With ManageSoft for Windows Deployment you can automatically rebuild a desktop or laptop system back to the current desired state described in policy, including service packs, new applications and configuration changes. This is only possible with a policy-based management system. Smart agents on the managed device itself determine what’s required to rebuild to the desired state described in current policies.
Intelligent partial system rebuilds — ManageSoft for Windows Deployment also enables intelligent partial rebuilds when a computer is moved from one organizational group to another. For example, if a mobile laptop is moved from Marketing to Sales, ManageSoft smart agents on the laptop will automatically reconfigure the device to achieve the desired state described in policies applying to the Sales group. Without needing to build the computer again from scratch, ManageSoft for Windows Deployment will automatically remove any Marketing applications that are no longer required (freeing up licenses to be used elsewhere in the organization), and will automatically download and install any additional Sales applications specified in centrally-defined policies. This capability is also particularly useful in educational settings when, for example, computers routinely need to be moved between a maths laboratory and other computer laboratories in the school or University.

These capabilities are discussed in more detail in the ManageSoft white paper: "Automating deployment of Microsoft Windows 2000, Windows XP, or Windows Server 2003".

Improving IT decision-making with IT business intelligence

This unique ManageSoft smart-agent architecture provides a wealth of management data on the status and location of software and hardware assets throughout the organization. Centralized monitoring and control is further enhanced with a .NET-powered customizable executive dashboard providing minute-by-minute graphical reporting on software and hardware assets located anywhere in the world. It’s a powerful reporting solution for IT administrators, enabling easy monitoring of key performance indicators for daily IT tasks and processes. Organizations can extend this powerful reporting even further with the addition of ManageSoft IT Business Intelligence.

The optional addition of ManageSoft IT Business Intelligence dramatically extends ManageSoft reporting capabilities with Online Analytical Processing (OLAP) to enable CIOs and IT Managers to slice-and-dice this information in conjunction with data from other IT systems to provide business insight and to improve IT decision-making. Unlike the ManageSoft reporting module, which shows a “just in time” snapshot of deployment projects and of hardware and software assets based on very detailed and technical data, ManageSoft IT Business Intelligence presents strategic information through visualizations of trends and highlights changes over time with powerful data aggregation, automated analysis, and easy flexible queries for ad-hoc analysis. This provides a quick and easy way to get the answers needed to make complex IT business decisions by providing touch-of-a-button answers to common questions with automated analysis of software and hardware assets, and easy management interrogation of IT data for rapid ‘answers-on-the-fly’.

Figure 13: ManageSoft IT Business Intelligence
Managing software licenses

The ManageSoft client-centric, policy-based architecture used for the initial deployment provides ongoing real-time license management, software metering and usage tracking. IT administrators can use ManageSoft to record software license details including license name, description, expiration date, pricing model, publisher, reseller, and associated software releases. Easy allocation, and reallocation, of existing licenses across multiple business units enables efficient use of existing licenses and enables accurate charge-back of license costs to individual business units and automatic license breach alerts also enable administrators to avoid costly license breaches. The addition of ManageSoft IT Business Intelligence extends these capabilities to provide detailed trend analysis over time, and integrates with asset management and finance systems to provide:

- **Software inventory analysis** — ManageSoft IT Business Intelligence provides detailed analysis of software inventory changes over time. This analysis can be filtered at the touch of a button for users, computers, business units, and domains. Software inventory analysis highlights increasing installation/de-installation of individual software products, enabling CIOs to take pre-emptive action if inappropriate software is identified, and to monitor emerging trends in new software use.

- **Software usage analysis** — ManageSoft IT Business Intelligence provides out-of-the-box analysis of software usage indicators for installed software by business unit, domain, users, or computers. It enables rapid analysis of individual usage profiles, the identification of unused and under-used software assets, and analysis of inappropriate individual usage patterns for applications like MSN Messenger.

![Software usage analysis with ManageSoft IT Business Intelligence](image)

- **Software license management** — ManageSoft IT Business Intelligence turns the table to put enterprise CIOs in control of license true-ups and not the software vendor. Automated analysis and detailed reporting for license usage and compliance enables CIOs and IT Managers to negotiate effectively with software license vendors and recapture and reallocate unused software licenses across multiple business units. License analysis highlights the volume and cost of existing licenses, and compares this with actual installation and usage. This powerful analysis with touch-of-a-button graphical reporting reveals potential license savings, hidden software assets (unused and forgotten "rusting software"), and enables CIOs to proactively avoid the costs and business risk associated with license breaches.

These capabilities are discussed in more detail in the ManageSoft white paper: "Improving IT decision-making with IT business intelligence".

---

**ManageSoft IT Business Intelligence turns the table to put enterprise CIOs in control of license true-ups and not the software vendor.**

---

**Figure 14: Software usage analysis with ManageSoft IT Business Intelligence**

- Analyze software usage metrics for any software product opened during a defined period.
- Highlight inappropriate software use. Identify unused and underused software. Interrogate usage data to compare active usage against total application run time.
- Filter analysis by software application, domain, organizational unit, computers, or specific users.
Figure 15: Powerful software license analysis and graphical reporting

Negotiate software license agreements based on detailed analysis of existing licenses, current installations, and number of installations actually being used.

Point and click to save graphical analysis for use in license negotiations.

Manage licenses across multiple organizational units. Reclaim and reallocate unused licenses to reduce costs.

These capabilities are discussed in more detail in the ManageSoft white paper: "Improving IT decision-making with IT business intelligence".

Tracking hardware assets

Obtaining an accurate inventory of IT assets in geographically dispersed organizations can be time consuming and prohibitively expensive. Keeping that inventory up to date over time is even more difficult in many organizations. Yet to manage your organization’s valuable investment in IT assets you need to know what software and hardware you own, where those assets are, and how they are configured — including mobile and remote devices. The ManageSoft client-centric architecture used to deploy software, also provides ongoing up-to-the-minute IT asset tracking. Smart-agents on each managed device upload inventory data including processor, disk space, available memory, operating system, and a variety of other information to a central SQL database for real-time central reporting on the status and location of hardware assets throughout the organization. Inventory data is uploaded in lightweight XML files, which are also compressed to further reduce network traffic. ManageSoft also enables a combination of full inventory reports, incremental inventory reporting (inventory changes since the last incremental inventory report), and differential inventory reporting (inventory changes since the last full inventory report) to further minimize network traffic. Up-to-the-minute inventory data is accessible centrally at any time through powerful graphical reporting in the ManageSoft executive dashboard.

The addition of ManageSoft IT Business Intelligence extends these capabilities to provide detailed trend analysis over time, and integrates with asset management and finance systems to provide powerful analysis of hardware changes over time for any type of specified hardware item. Identification and location of hardware additions and losses streamlines acquisition management, lease management, and IT budgeting.
ManageSoft IT Business Intelligence also provides a simple yet extremely powerful out-of-the-box analysis that many CIO’s have long sought because it offers the potential for significant IT savings. ManageSoft IT Business Intelligence highlights at-a-glance all computers that are “overdue” (haven’t reported any data within a defined period of time). This might indicate that an overdue computer is a mobile sales laptop “on-the-road” that only connects intermittently to the corporate network. However, the computer could also be absent because of network problems that need to be addressed, or because the laptop has been lost or stolen—something that should be addressed before the organization incurs unnecessary replacement costs or penalty fees for late return of leased computers.

These capabilities are discussed in more detail in the ManageSoft white paper: "Improving IT decision-making with IT business intelligence".
Automating security patch management

ManageSoft Security Patch Management enables IT administrators to use the same management infrastructure used for software deployment, to also eliminate known security vulnerabilities quickly and reliably by automating the patch management process. ManageSoft Security Patch Management extends the ManageSoft administration interface to provide powerful security patch management capabilities, and uses the ManageSoft smart-agent architecture to provide rapid and reliable distribution of security patches across any network, including low-bandwidth and unreliable connections. Automatic installation and policy-based self-healing ensure that managed devices are always protected against crippling virus attacks. It’s the quickest and most reliable way to deploy security patches to desktops, servers, and mobile devices.

Figure 18: Automated security patch management to eliminate known software vulnerabilities

See at a glance the status and severity of existing security patches. Rapidly accept, rollout, and/or rollback new patches. Access extensive out-of-the-box security reports.

Up-to-the-minute graphical enterprise security compliance reporting in an executive dashboard. Click through to report details for progressive drill-down through organizational unit security summaries to individual computers.

These capabilities are discussed in more detail in the ManageSoft white paper: “Automating security patch management”. 
Increasing reliability and reducing costs with self-managing devices

ManageSoft is an end-to-end cross-platform configuration management solution that transforms desktops, servers, and mobile devices into self-managing devices. The ManageSoft smart-agent architecture provides unique advantages that make ManageSoft the fastest and most reliable way to deploy, update, and manage software and hardware IT assets:

- Policy-based approach enables set-and-forget management
- Client-centric architecture provides faster implementation, greater reliability, and cost-effective scalability
- A unique end-to-end enterprise configuration management solution.

Policy-based approach enables set-and-forget management

Unlike labor-intensive task-based products that require manual targeting of software deployments, and repeated manual intervention to successfully complete installations missed in the initial distribution, the ManageSoft smart-agent architecture provides the set-and-forget reliability of policy-based software management. This policy-based approach enables central IT administrators to define the desired state for computers throughout the enterprise and/or specific groups within the enterprise. Once this desired state is defined in policy, managed devices throughout the enterprise automatically comply with centrally defined security policies, without requiring manual intervention of any kind.

Figure 19: Policy-based management with ManageSoft provides set-and-forget reliability

Policy-based patch management

- Centrally-defined policies specify who gets what software and when — ‘Desired state’
- Managed devices automatically compare their current state with the desired state described in relevant policies
- All calculations are performed automatically on the managed device
This policy-based approach provides distinct advantages, including:

- **Policy-based management provides increased reliability** — With ManageSoft, if a managed device is disconnected or unavailable when a security update is released, the managed device will automatically detect, download, and install the update at the next connection to the network.

- **Policy-based management ensures increased compliance** — If a computer is rebuilt, or a new computer is joined to the domain for the first time, ManageSoft automatically applies relevant policies, with the managed device automatically downloading and installing any necessary updates required to achieve the desired state described in policy (without the traditional delay of waiting for an initial client inventory report).

- **Policy-based management reduces administration costs** — ManageSoft enables IT administrators to define software deployment policies for an entire group of users/computers, and define it just once. There is no need for the administrator to continually generate target lists of devices to target future deployments. Central IT administrators can simply define a deployment policy and then forget it — ManageSoft provides intelligent automation from then on.

---

### Client-centric architecture provides faster implementation, increased reliability, and cost-effective scalability

ManageSoft is the only client-centric software management solution. All other software deployment and configuration management products use a server-centric architecture. With server-centric products, all data processing and intelligence resides on dedicated management servers that are responsible for all communication with client devices.

**Figure 20: Alternative server-centric products are less reliable and very expensive to scale**

Alternative server-centric products

- Unlike ManageSoft, all calculations are performed on dedicated servers
- Server-centric products create ‘single-point-of-failure’
- Server-centric products require expensive, high-maintenance servers
- Server-centric products are very expensive to scale-up

Server-centric products present distinct disadvantages for enterprise-scale configuration management, including:

- **Server-centric architectures are highly inefficient** — Some software management products claim to provide policy-based management but are still limited by a server-centric architecture. In this server-centric model the policy for each managed device is calculated on the server, and only then are instructions passed to the client for local execution. Since this approach requires intensive server-side processing for many PC clients, the servers required for this architecture must be high-resource, dedicated machines with fast CPUs, ample RAM, and 24x7 IT support to ensure maximum server availability.

- **Server-centric approaches create a single-point-of-failure** — Server-centric products tend to be vulnerable to a single-point-of-failure because each managed device receives instructions from a single server.

---
Server-centric products are bandwidth inefficient — A server-centric architecture requires dedicated management servers to query each client to determine the desired configuration for that device. This creates additional network traffic and is extremely bandwidth inefficient. Server-centric products also typically upload inventory and event information directly back to the root administration server rather than back through a distribution hierarchy, which further compounds the bandwidth impact of the server-centric architecture.

Server-centric products are expensive to implement and expensive to scale up — A server-centric architecture requires dedicated servers, which generates significant overhead costs for companies stemming from the purchase and administration of dozens or hundreds of dedicated servers. For example, if an enterprise has 200 sites around the world, server-centric products would typically require a dedicated server at each site. For a typical $15,000 server deployed at 200 sites this would represent an initial investment of $3 million for hardware alone. The costs multiply when recurring maintenance and administration expenses are considered as part of the total cost of server ownership. In addition, server-centric architectures can support far fewer clients from a single server because they are gated by the processing and memory capacity of the server machine. This means that future scalability requires the addition of even more dedicated servers.

Server-centric architectures create implementation complexities — Server-centric products require extensive additional server infrastructure deployments. This inevitably involves complex, costly, and lengthy implementation periods, which can be highly embarrassing for IT managers attempting to respond rapidly to line-of-business pressures for increased IT security after a damaging virus attack. ManageSoft is the only solution that eliminates server-centric limitations by employing a client-centric architecture. Unlike server-centric products, the ManageSoft client-centric smart-agent architecture performs all processing at the point where it is most efficient: on the client PC itself.

Figure 21: ManageSoft client-centric architecture performs all calculations on the managed device

ManageSoft client-centric architecture
- All calculations are performed on the managed device
- Client-centric approaches avoids the “single point of failure” inherent in server-centric approaches
- Any existing webserver, fileserver, or fileshare can be used as a distribution server: rapid implementation, ongoing scalability
By avoiding the need for dozens or hundreds of dedicated management servers commonly required by server-centric products, the ManageSoft client-centric approach reduces implementation costs significantly and provides a range of distinct advantages:

- **Client-centric processing is more efficient and very flexible** — The ManageSoft client-centric processing model uses a local smart-agent on the managed device to examine and analyze the current state of the computer, and perform policy calculations on the local computer. This local client-side processing consumes negligible resources (This is in sharp contrast with server-centric models where these calculations are aggregated on a server that must calculate policies for hundreds of client computers).

- **Client-centric management provides in-built fault tolerance** — With ManageSoft, if a distribution server is unavailable, the client can automatically failover to an alternate server and continue the download from the point of interruption. ManageSoft can use any existing web server, filesystem, file share, or even an existing Novell server as a distribution server.

- **Client-centric management is bandwidth-friendly** — ManageSoft provides automatic detection of the nearest available distribution server, which means there is no need to traverse the WAN to reach other servers or get instructions. ManageSoft also provides byte-level differencing and configurable bandwidth throttling for highly efficient use of available network bandwidth.

- **Client-centric architecture provides ongoing scalability** — The ManageSoft client-centric architectures create a scalable solution that does not require a dedicated server infrastructure.

- **Client-centric architecture provides cost-efficient implementation** — With ManageSoft smart agents the client performing the policy calculations locally on each managed device, there is no need to implement a fleet of dedicated servers. In some enterprises, the minimum required server for a client-centric system is a simple file share from which to download packages. This could be an existing file/print server, an FTP server, Web server, or even an existing Novell file/print server — all of which would require no additional installed software. Since the ManageSoft client-centric architecture requires only the sharing of files, a single server can support a far larger number of clients.

- **Client-centric management delivers low ongoing administration costs** — Since there’s no need to deploy additional dedicated servers, infrastructure administration costs do not increase because there are no additional servers to manage.

- **Client-centric architecture enables the fastest implementation** — A client-centric model is faster to implement because of the absence of server infrastructure and overhead, and can be implemented extremely rapidly.

**A unique end-to-end enterprise configuration management solution**

The unique ManageSoft smart agent architecture delivers the breadth of functionality, scalability and reliability of a best-of-breed configuration management tool, while also providing the quick implementation times, low infrastructure costs, and low ongoing administration costs that have traditionally been associated with point solutions (that subsequently fall down in the areas of scalability and breadth of functionality). This integrated approach combines policy-based management with a client-centric architecture to provide the fastest and most reliable way to automatically deploy, update, and manage software and hardware assets throughout an organization.
Find out more

Find out how ManageSoft can help you to automatically deploy, update, and manage software and hardware IT assets.

- Telephone your nearest ManageSoft office to discuss your requirements or request a product demonstration
- Visit www.managesoft.com for additional resources or to register for a seminar
- Request an in-house proof-of-concept to see how ManageSoft can meet your particular requirements.