



# Managing Data Center Server Compliance

Using Microsoft® System Center

Published: June 2008

For the latest information, please see <http://www.microsoft.com/systemcenter>

---

## Contents

Executive Summary .....	i
Introduction .....	1
Managing Server Compliance in the Data Center .....	1
The Microsoft System Center Data Center Compliance Solution .....	2
Configuration Controls and Reporting .....	3
Centralized Auditing of Data Center Security .....	5
Identity and Access Management (IDA) .....	5
The Microsoft System Center Server Management Suite Enterprise .....	6
Conclusion .....	6
Resources .....	7

---

## **Executive Summary**

Data center managers are tasked with establishing and maintaining server standards to meet a growing number of external compliance requirements and internal corporate policies. With the emergence of a more centralized and virtualized approach to server and application management, data center managers seek solutions that enable them to meet server compliance standards without compromising operational efficiencies. The Microsoft System Center data center compliance solution helps data centers ensure compliance, reduce costs, improve efficiency, enhance security, and ensure data center resource availability.

## Introduction

Being able to meet internal or regulatory requirements has become a core component of the data center manager's responsibilities. The data center has evolved to meet the increasing external requirements for control of access to data center assets and the internal need to protect corporate information. However, as the number of mission-critical servers and applications in the data center grows, data center managers face the additional challenge of meeting all of these compliance requirements in a scalable and cost-effective way.

Increasing numbers of servers and applications deployed in data centers, and the emergence of the truly virtualized data center (with the potential for an ever-increasing number of servers) makes a centralized and automated server compliance process ever more important. Data center managers are now looking for integrated solutions that help them enforce compliance with their corporate policies for configuration and security, and produce compliance reports to satisfy auditors. With this combination, they can continue to meet internal and external demands without a prohibitive increase in cost or a degradation of service to the business.

This white paper explores key issues related to data center compliance and shows how the Microsoft System Center data center compliance solution can help data center managers simultaneously ensure compliance while lowering costs and improving efficiency.

## Managing Server Compliance in the Data Center

Data center environments are complex and provide many mission-critical applications across the enterprise. Thus establishing compliance with corporate policies for servers is crucial to maintaining security and avoiding downtime or data loss. Server compliance requires that all areas of the data center infrastructure comply with the organization's established standards and policies. The need to meet both internal and external compliance requirements drives these standards and policies. Table 1 lists some examples of the sources of these requirements.

<b>Internal Standards and Policies</b>	Security settings
	Data-retention rules
	Change-management policies and procedures
	Consultant-led formal and/or self-assessment audits
	Operations-management standards and policies
	Management- and/or client-mandated security rules
	Service Level Agreement (SLA) policies
<b>External Regulations</b>	Sarbanes-Oxley (SOX)
	Health Insurance Portability and Accountability Act (HIPAA)
	European Union Data Protection Directive (EUDPD)
	International Organization for Standardization (ISO)
	PCI Security Standards Council
	Federal Information Security Management Act (FISMA)
Gramm-Leach-Bliley (GLBA)	

**Table 1: Examples of Regulations and Standards for Internal and External Compliance**

Each requirement affects data centers and drives a need to establish and enforce compliance across the full environment—for both physical and virtual assets. This is no small task, given the in the thousands federal, state, and local laws and regulations currently addressing what,

how, when, and why electronic records should be created, stored, accessed, maintained, and retained over time.

For data center managers, these compliance requirements translate into the following key needs:

- Establish, deploy, and monitor server-configuration controls - including the capability to take action once an issue has been identified.
- Audit and report server security compliance status within the data center to both internal and external parties.
- Secure servers and implement an identity and access-management strategy.

Meeting these requirements might seem like an onerous task, but fully implemented and optimized server compliance can provide numerous benefits, as Figure 1 shows.

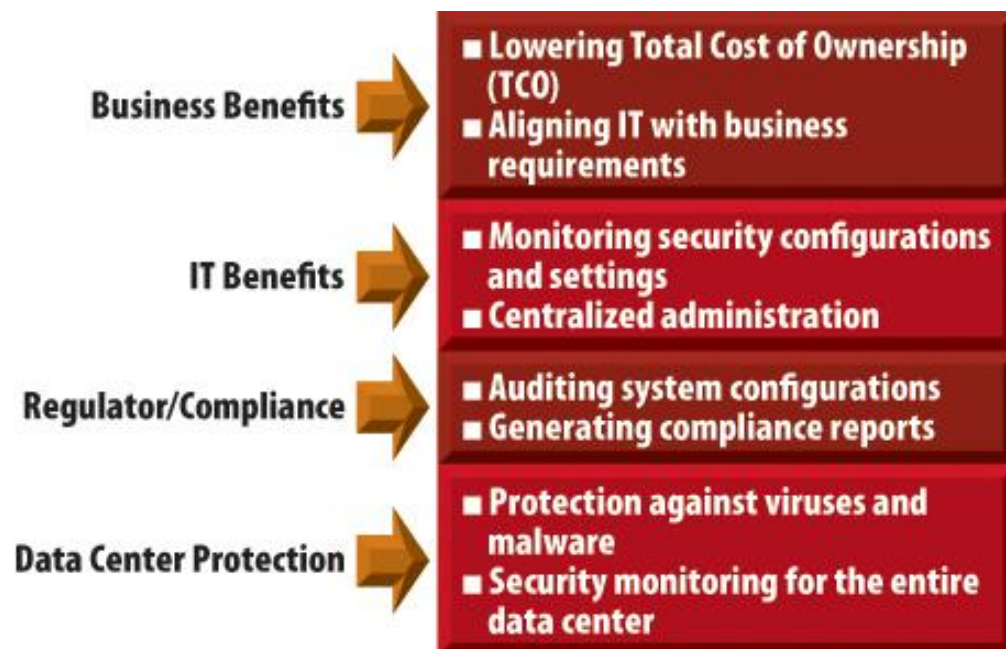


Figure 1: Key Benefits of Data Center Server Compliance

## The Microsoft System Center Data Center Compliance Solution

System Center provides a range of data center management solutions that help customers to proactively manage their environment. System Center delivers an integrated and extensible suite of solutions for configuration management, server compliance, end-to-end monitoring, and data protection and recovery that help lower costs while improving the overall operational efficiency of the data center.

The System Center data center server compliance solution simplifies and improves deployment, monitoring, and enforcement of server compliance across both physical and virtual data center environments. The solution helps data center managers create and enforce configuration controls. It also provides security and regulation auditing, flexible reporting, and

---

a centralized collection of security events that help streamline and optimize server compliance. Interoperation of security and management capabilities further enhance server compliance.

The following sections detail the capabilities and benefits of the data center server compliance solution:

### **Configuration Controls and Reporting**

- Management of server configurations to desired baselines and policies
- Packaged best practices to establish and validate server configuration
- Integrated compliance dashboards and reports
- Custom and predefined server configuration baselines

### **Centralized Security Auditing**

- Automated reporting on security policy compliance
- Security vulnerability assessment

### **Security and Identity and Access Management**

- Holistic security and access management
- Interoperability between security and management environments

## **Configuration Controls and Reporting**

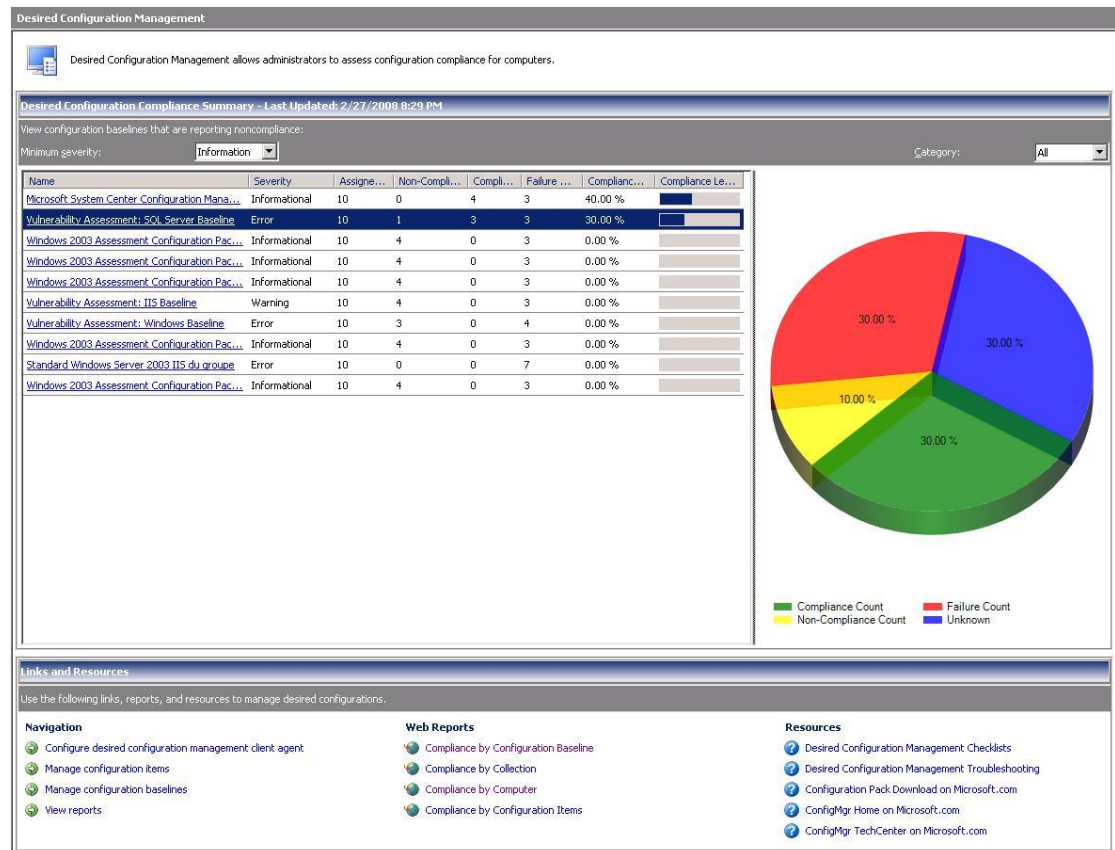
As the number of servers deployed in data centers grows, the risk of compliance and security problems increases, especially if existing processes for ensuring compliance cannot scale to accommodate the additional servers and complexity. Often, multiple administrators are given permission to change settings or install updates, which further increases the risk that server configuration can “drift” from what corporate policies demand. This configuration drift also increases the risk that applications and other data center resources will be unavailable to the business.

The System Center data center compliance solution is designed to help data center managers deal with these configuration compliance issues. A key capability this solution offers is to create and then help enforce configuration controls. This is achieved through the ability to create, deploy, and monitor server-configuration baselines. (This is in part delivered through Desired Configuration Management, a powerful set of capabilities that help monitor server configuration compliance throughout the data center) These baselines can be deployed to new servers during the build process, or they can be compared against existing, production server images to determine whether additional software and security updates must be applied to achieve compliance. Custom baselines can also help data center managers streamline many compliance and security tasks.

Configuration Packs deliver the detailed knowledge and prescriptive guidance for desired configuration management. These packs contain configuration items (such as settings for the OS, users, applications, security, or access) that help data center managers validate a desired server configuration in terms of the policies or controls they have developed in response to specific requirements. Regulation-specific Configuration Packs help data center managers establish and validate desired server configurations for the regulations that impact their organization. For example, Configuration Packs from Microsoft and third-party vendors contain suggested system configurations that map best practices and standards for complying with regulations such as FISMA, HIPAA, Sarbanes-Oxley, or GLBA. When the solution detects that settings are out of compliance, the system generates alerts and makes data available for reporting.

System Center not only enables data center managers to automate the process of deploying these baselines, but also provides detailed auditing and reporting information. As Figure 3 shows, the integrated dashboards and reports make monitoring and managing server compliance a simpler and more scalable process. Data center managers can quickly identify

configuration problems that might cause compliance issues (or that might affect application availability or performance). Data center managers can correct problems by deploying software updates or scripts, or by making other necessary changes to bring the offending entity into compliance. Again, using System Center, they can automate any required update.



**Figure 2: Desired Configuration Management Helps Administrators Assess Configuration Compliance**

Specific reports also let data center managers drill down to specific servers or issues, for more targeted troubleshooting and remediation. These reports include information such as:

- Summary of compliance for a configuration item, by computer
- Summary of noncompliance for a configuration item, by validation criteria
- Noncompliance details for a configuration item on a particular computer
- Summary of compliance, by configuration baseline
- Compliance history for a configuration item on a particular computer

With this drill-down feature, data center managers can quickly understand any compliance issues and see details about which elements of the configuration baseline cause a particular computer to be out of compliance. The solution also includes guidance and tools that help data center managers more easily discover and fix system vulnerabilities and identify systems that are out of compliance.

The reporting available in the solution also extends to asset usage information (often called asset intelligence), providing in-depth information about which hardware and software assets are deployed in the data center. With this knowledge, data center managers can proactively track and manage compliance with current licensing agreements.

The solution's reporting capabilities include security vulnerability assessments that are available via specific packaged best practices. This specificity is designed to reduce risks of

---

compromised system security or stability associated with incorrectly configured or installed software. This packaged knowledge and best practices help data center managers address data center configuration issues or operational weaknesses and take corrective action. The solution includes vulnerability assessment reporting for common software configuration errors and carries out the following types of assessments:

- Detecting unnecessary services
- Determining whether strong passwords are enforced
- Detecting enabled but unsecured guest accounts
- Checking permissions on shared folders

## **Centralized Auditing of Data Center Security**

As discussed earlier, an increase in the number of servers, whether physical or virtual, increases the effort data center managers must make to ensure compliance. This increase is further compounded by the centralization of sensitive or mission-critical information and applications within the data center. Many corporate policies or external regulations produce specific security-auditing requirements that, when applied to all the servers in a data center, can produce very large data requirements.

The System Center server compliance solution is designed to automatically gather the information on the security-related events that are critical to an organization's compliance efforts. For example, information regarding password policies, authentication rules, and account status is captured from across the data center environment; this comprehensive information both enables the production of reports for internal security committees or external agencies, and lets data center managers easily detect server modifications that can result in noncompliance. These audit capabilities automate the collection and archiving of Windows Security Event Logs across the data in near real-time, ensuring that data center managers have the most up-to-date information available to them.

Examples of server security events that data center managers can monitor include:

- Modifications to application or OS permissions
- Changes to group membership
- Changes to user permissions
- Password policy changes
- User account lockouts
- Changes to inventory or asset-related details

To support compliance requirements, System Center separates the audit database from the operations and data-warehouse databases. This approach meets data-separation requirements and also improves performance. Reporting is based on Microsoft SQL Server® Reporting Services, which enables easy customization or modification.

The centralized security-audit capabilities bring together all the key server security log information, so data center managers can understand the security status of their data centers without additional management overhead. The solution also provides the appropriate level of reporting to meet the needs of internal and external compliance requirements.

## **Identity and Access (IDA) Management**

Configuration management and security event reporting are key to meeting the compliance needs in the data center. However, the actual security of applications and data within that environment remains essential when data center managers consider their compliance efforts. With the increasing complexity and scope of the data center environment, Identity and Access (IDA) management is becoming ever more important. As a combination of processes,

---

technologies, and policies that manage digital identities and specify how they are used to access resources, IDA requires a holistic approach that encompasses both the security and management disciplines. Microsoft offers a holistic approach to IDA management, which includes the ability to aggregate user identities from across the enterprise into a single view and ensure that compliance is enhanced through auditable access rights processes.

For data center security, System Center and Microsoft Forefront's™ security capabilities work together to provide protection for information and controlled access to data center resources. These capabilities bring together System Center's deployment, reporting, and remediation functionality with the Forefront security solutions. The value of an organization's investment in Microsoft technology is increased by combining Forefront with System Center, as each solution builds and expands the capabilities of the Windows® platform and applications.

Being able to integrate security alerts with the overall management environment ensures that data center managers have a consolidated view of their data centers. Additionally, the integration with System Center delivers the global deployment of Forefront security updates to servers and users. Forefront management packs for server products such as Microsoft Exchange Server 2007 and Office SharePoint Server 2007 work with System Center to protect and monitor data center systems 24/7.

This combination of capabilities secures servers in the data center and provides identity and access management, which in turn results in less overhead associated with managing identities and improved data center security.

## **The Microsoft System Center Server Management Suite Enterprise**

Businesses are optimizing their existing data center infrastructure by transitioning to a Dynamic IT infrastructure. With a comprehensive set of solutions for managing the physical and logical IT environment, the Microsoft System Center Server Management Suite Enterprise (SMSE) license is an ideal solution for IT organizations that want to optimize their changing data centers.

The SMSE provides an integrated combination of the System Center data center management solution core components. The SMSE provides an easy, cost-effective way to acquire the System Center data center management solutions for complete server management of departmental or enterprise server environments

## **Conclusion**

The System Center data center server compliance solution provides capabilities that help data center managers meet server compliance standards. Server configuration controls implemented through desired configuration management help data center managers create, deploy, and monitor server configuration baselines throughout the data center. Regulation-specific Configuration Packs assist data center managers in establishing and validating desired configurations for servers.

System Center simplifies server compliance monitoring and management through dashboards and reports. The solution also includes prescriptive guidance and tools that help data center managers more easily discover and fix system vulnerabilities and identify systems that are out of compliance. Powerful reporting capabilities provide near real-time server configuration and compliance knowledge, along with asset and license intelligence.

System Center also provides high-level reporting on security events with drill-down capabilities that enable data center managers to view details of data captured from across the data center. By centralizing security audit capabilities, data center managers can gain a better

---

overview of the data center security status and ensure that they are meeting both internal and external compliance requirements.

Security with IDA management is an integral component of data center compliance management. Controlled access to data center servers and applications is a key element of server compliance. With their consolidated views, integrated security alerts, and edge protection, System Center and Microsoft Forefront give data center managers capabilities to control access and protect the data center from intrusion, spyware, viruses, and malware.

With the System Center data center server compliance solution, data center managers benefit from streamlined server compliance, reduced cost, improved productivity, and ultimately a greater return on IT investments.

## **Resources**

Microsoft System Center

<http://www.microsoft.com/systemcenter>

System Center Management Pack Catalog

<http://www.microsoft.com/technet/prodtechnol/scp/catalog.aspx>

Solution Accelerators

<http://technet.microsoft.com/en-us/solutionaccelerators/default.aspx>

System Center Data Center Solutions

<http://www.microsoft.com/systemcenter/en/us/dynamic-data-centers.aspx>

System Center Server Management Suites – How to Buy

<http://www.microsoft.com/systemcenter/en/us/management-suites.aspx>

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2008 Microsoft Corporation. All rights reserved.

Microsoft, the Microsoft logo, People Ready, Forefront, SharePoint, SQL Server, and Windows and are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.