

**Microsoft** | Solution Accelerators

# Security Compliance Manager (SCM)

Michael Tan | Microsoft Solution Accelerators

September 28, 2010

## Agenda

- SCM overview + Demo
- Baseline portfolio and upcoming releases
- Setting packs + Demo
- SCAP content authoring in SCM + Demo
- IT GRC Process Management Pack
- SCM and IT GRC now together
- Baseline enhancement considerations
- SCM enhancement considerations
- Q/A

## Security Compliance Manager Overview

- **Centralized baseline knowledge management**
  - Classified data, hierarchical grouping
  - Improved data presentation
  - Version control, content updating, logging
  - Baseline comparison
  - Search (real-time filtering and global search)
- **Baseline customization**
  - Duplicate
  - Merge
- **Export in multiple formats to enable automation**
  - Baseline deployment
  - Compliance check

# Demo – SCM Basic

The screenshot shows the Microsoft Security Compliance Manager application window. The title bar reads "Microsoft Security Compliance Manager". The menu bar includes "File", "View", "Tools", and "Help". Below the menu bar is a search bar with the text "Select search type" and "search settings". The main content area displays a "Welcome to Security Compliance Manager" message with a diagram illustrating the workflow: "Accelerate Knowledge" (Merge Best Practices) leads to "Customize Once" (Centralize Decision Making), which leads to "Export to Multiple Formats" (Monitor, Verify, Comply). Each step includes a brief description of its benefits.

**Accelerate Knowledge**  
Merge Best Practices  
Accelerate your research and planning by merging your expertise with security recommendations, guidance, and best practices delivered by Microsoft.

**Customize Once**  
Centralize Decision Making  
Centrally manage, customize, and configure your security baselines to deploy Microsoft technologies faster, easier, and more securely than ever before.

**Export to Multiple Formats**  
Monitor, Verify, Comply  
Export formats enable you to automate configuration policies, monitor changes, and report compliance against your security baseline.

**Key Features & Benefits**

- **Centralized Management and Baseline Portfolio:** The centralized management console of the Security Compliance Manager provides you with a unified, end-to-end user experience to plan, customize, and export security baselines. The tool gives you full access to a complete portfolio of recommended baselines for Windows® client and server operating systems, and Microsoft applications.
- **Security Baseline Customization:** Customizing, merging, and reviewing your baselines just got easier. Now you can use the new customization capabilities of the Security Compliance Manager to duplicate any of the recommended baselines from Microsoft—for Windows client and server operating systems, and Microsoft applications—and quickly modify security settings to meet the standards of your organization's environment.
- **Security Baseline Comparison and Export:** Security Compliance Manager enables you to quickly adopt the latest Microsoft product releases. Side-by-side baseline comparison features allow you to identify any changes to setting configurations and merge baselines within a product family with ease. Export and deploy baselines in your format of choice, including Desired Configuration Management (DCM) packs, Security Content Automation Protocol (SCAP), XLS, or Group Policy objects (GPOs).
- **Security Baseline Compliance Monitoring and Verification:** Keep current with the latest releases from Microsoft; automate your security baseline compliance process, and take advantage of baseline version control and automatic update features. The planning, customization, and export features of Security Compliance Manager quickly enable you to leverage monitoring and verification technologies, automate policy deployment, and produce compliance reports.

## Security Baseline Portfolio

- **Baselines available today:**
  - Windows® XP\*, Windows Vista®\*, Windows® 7, BitLocker® Drive Encryption\*
  - Windows Server® 2003\*, Windows Server® 2008
  - Microsoft® 2007 Office\*
  - Windows® Internet Explorer® 8
- **Public beta baselines available:**
  - Windows Server 2008 R2 and setting pack
  - Microsoft Office 2010 and setting pack
  - Windows 7 setting pack
  - Internet Explorer 8 setting pack
- **Coming baselines:**
  - Microsoft Exchange Server 2007
  - SQL Server® 2008 R2
- **Future baselines:**
  - SQL Server 2008 R2 remaining roles
  - Microsoft SharePoint® 2010
  - Microsoft Exchange Server 2010
  - Sustained engineering on existing baselines\*



## Setting Packs

- **What is a setting pack?**
  - Strictly from ADMX
  - Setting definition only
  - CCE ID
  - No threat countermeasure and impact data
  - No rules defined
- **Why do we need setting packs?**
  - Setting library provision
  - “Add” (merge) new settings into customized baselines for extensibility

# Demo – Add Settings From a Setting Pack

The screenshot shows the Microsoft Security Compliance Manager interface with a 'Merge' wizard dialog box open. The dialog compares two baselines: 'Source Baseline Win7-SettingPack-Beta 1.0' and 'Target Baseline Copy of Win7-EC-Desk'. The wizard lists items that will change, items only in the source baseline, items only in the target baseline, and items in both. It also provides additional information and a summary of the merge process.

**Setting groups only present in the source baseline:**

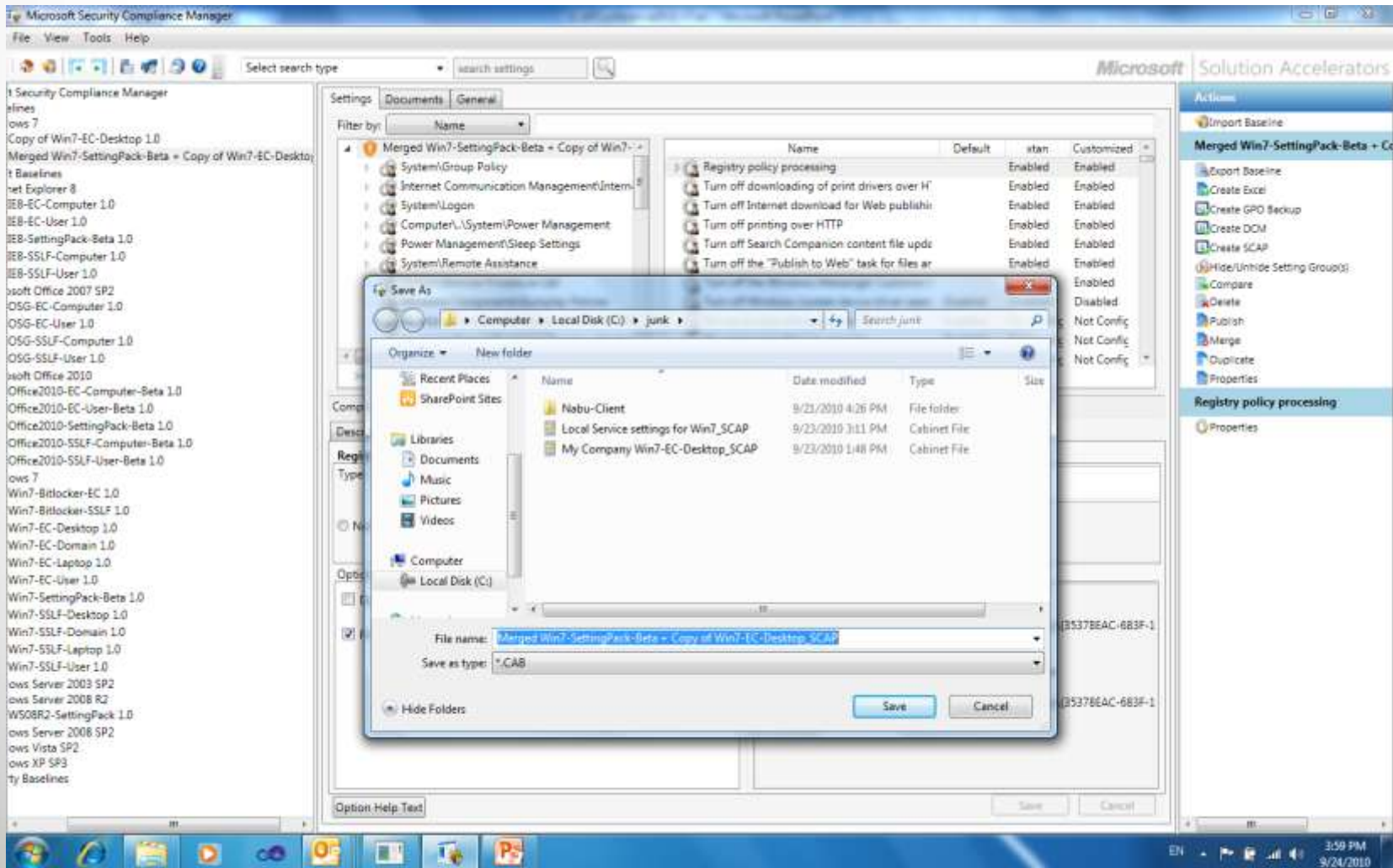
- Setting Group
- Computer\...\System\Power Management\Sleep Settings
- Computer\...\System\Power Management
- Computer\...\System\Internet Comm Management\Internet Co...

**Settings only present in the source baseline:**

Setting	Setting Group
<input type="checkbox"/> Do not allow adding new targets via manual configuration	Computer\...\System\SCSI\SCSI Target Dis...
<input type="checkbox"/> Do not allow manual configuration of iSNS servers	Computer\...\System\SCSI\SCSI Target Dis...
<input type="checkbox"/> Do not allow manual configuration of target portals	Computer\...\System\SCSI\SCSI Target Dis...
<input type="checkbox"/> Do not allow manual configuration of discovered targets	Computer\...\System\SCSI\SCSI Target Dis...

Additional Information: Process even if the Group Policy objects have not changed. No CCE-ID 5.0 is assigned. HKLM\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBE... REG\_DWORD:0

# Demo – Authoring SCAP Content From SCM

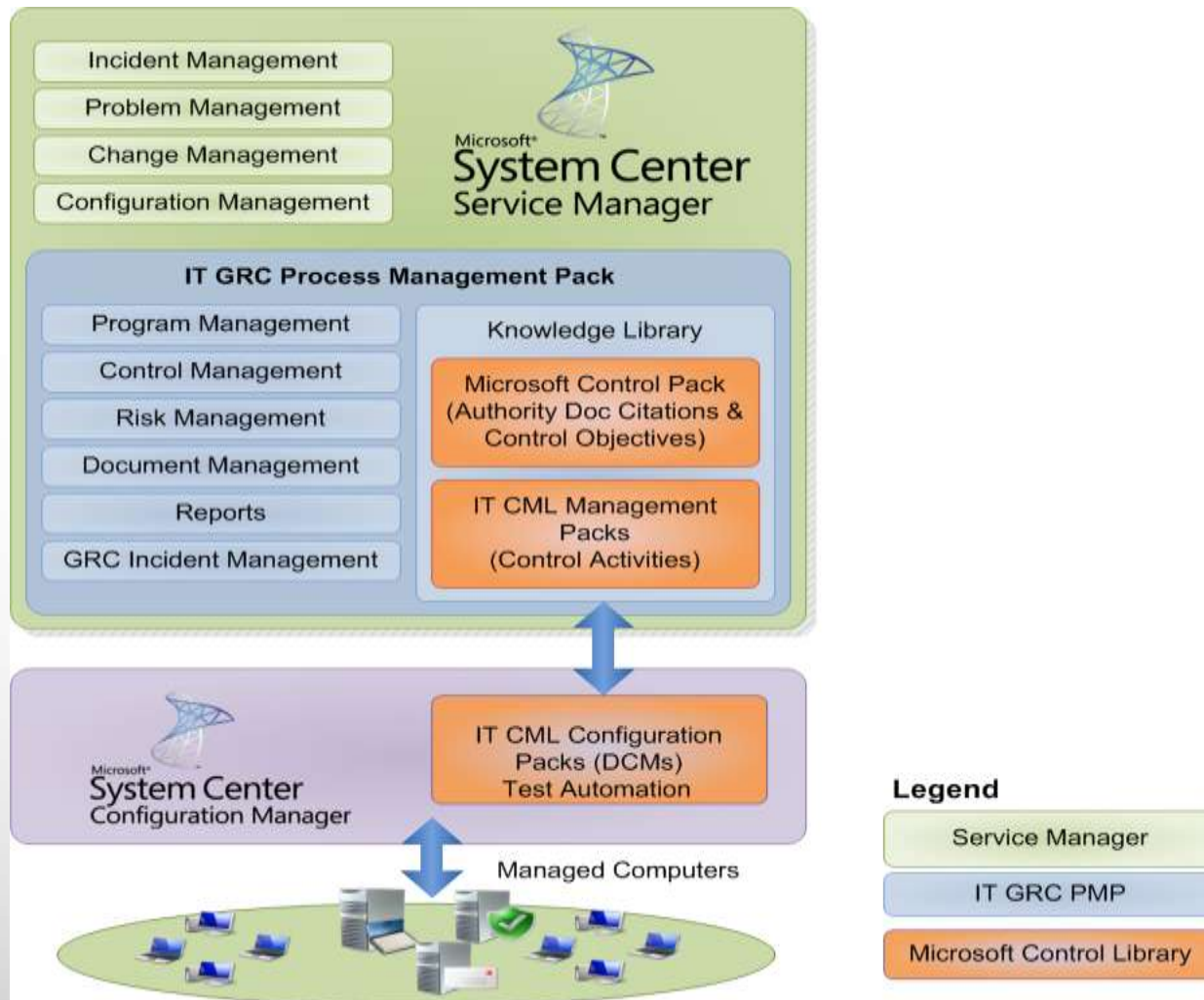




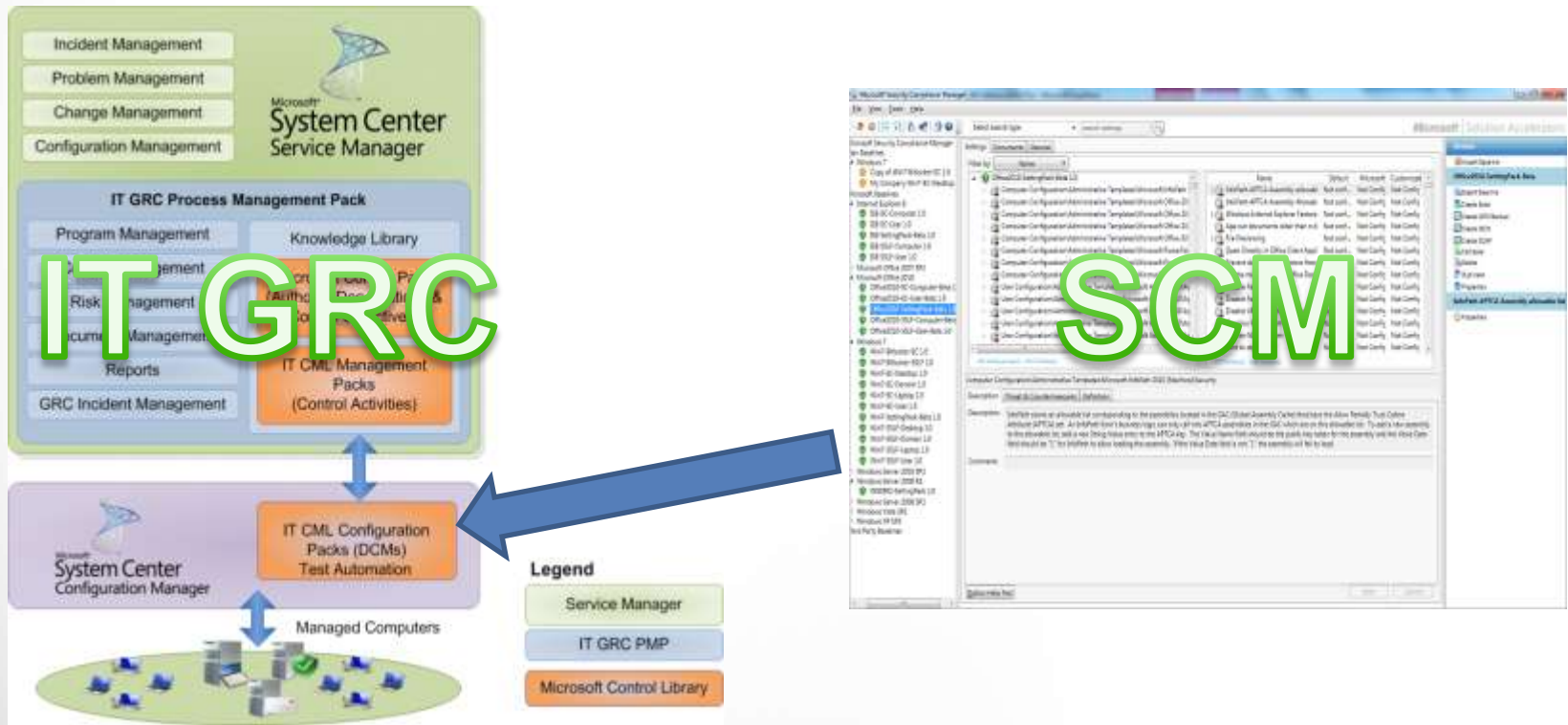
## Available Setting Packs in Beta

<b>Microsoft Product</b>	<b>Setting Groups</b>	<b>Settings/Options</b>
<b>Windows Server 2008 R2</b>	168	1478
<b>Windows 7</b>	168	1478
<b>Office 2010</b>	306	3898
<b>Internet Explorer</b>	90	2566

# IT GRC Process Management Pack Overview



# SCM and IT GRC Now Together



## Baseline Enhancement Considerations

- Single baseline (no EC/SSLF)
- Baseline severity definition
- Windows PowerShell™
- More setting data types



## SCM Enhancement Considerations

- GPO import
- Installation, taking advantage of existing SQL server instance
- Customization enhancement, baseline severity definitions and rules
- Performance enhancement

## Resources

- **SCM v1.1:** <http://technet.microsoft.com/en-us/library/cc677002.aspx>
- **IT GRC Process Management Pack:** <http://www.microsoft.com/grc> (<https://connect.microsoft.com/site446/content/content.aspx?ContentID=17903>)
- **Beta baselines:** <https://connect.microsoft.com/content/content.aspx?ContentID=17624&SiteID=715>
- **SCCM Extensions for SCAP:** <http://technet.microsoft.com/en-us/library/cc677271.aspx>
- **Feedback:** send email to [michael.tan@microsoft.com](mailto:michael.tan@microsoft.com) or [secwish@microsoft.com](mailto:secwish@microsoft.com)

# Q/A