Microsoft | Solution Accelerators

Security Compliance Manager (SCM)

Michael Tan | Microsoft Solution Accelerators

September 28, 2010

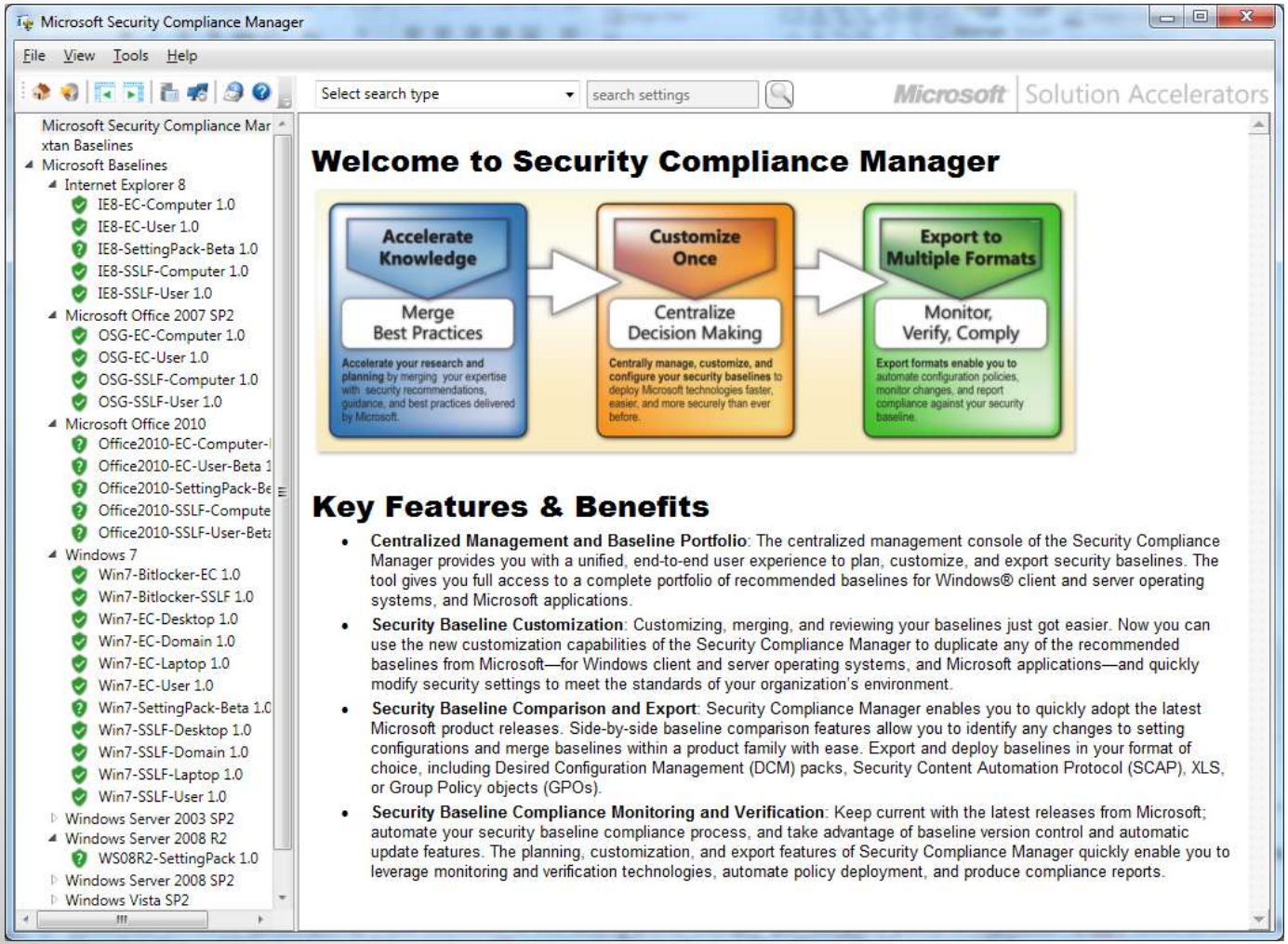
Agenda

- 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



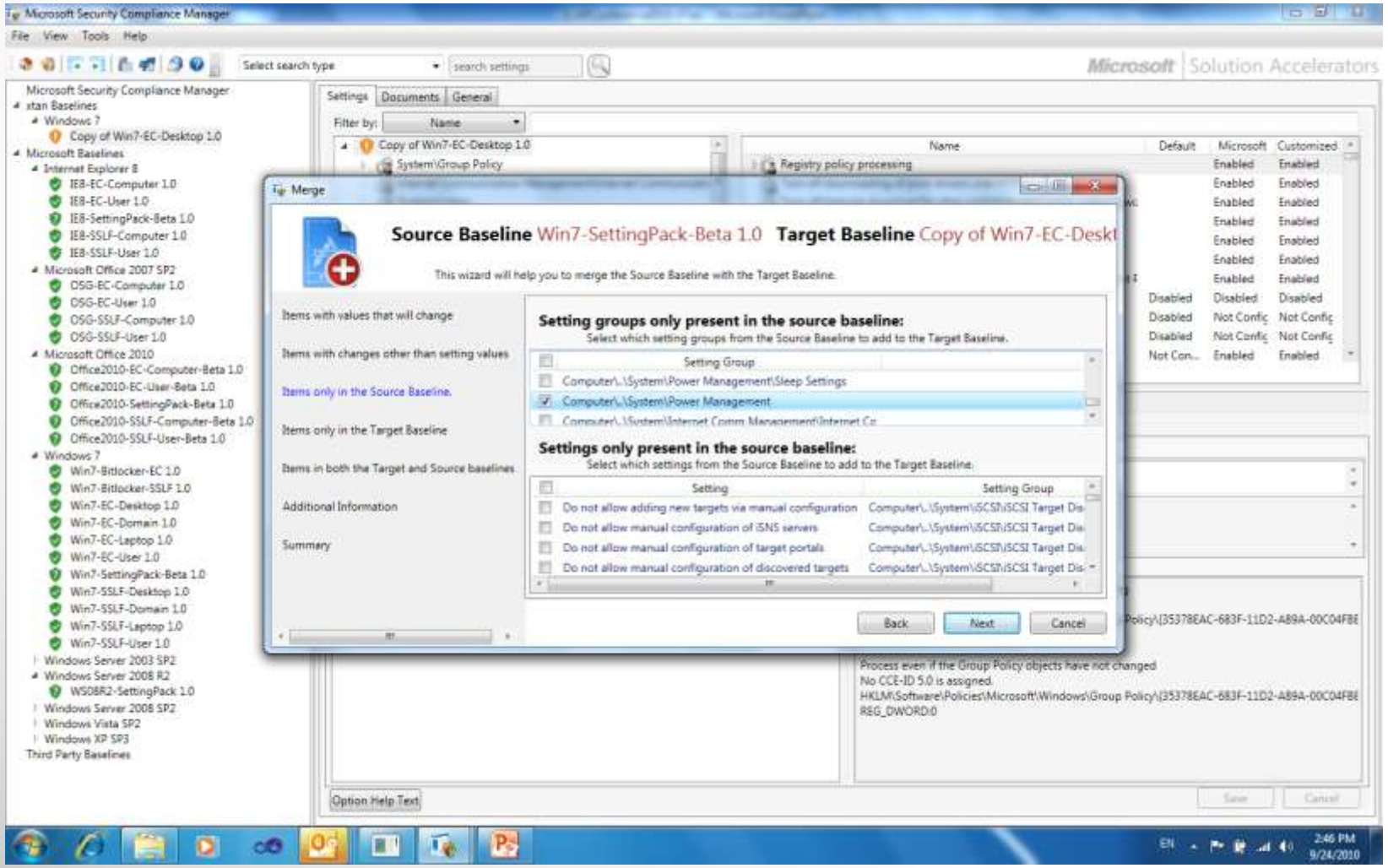
Security Baseline Portfolio

- **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*

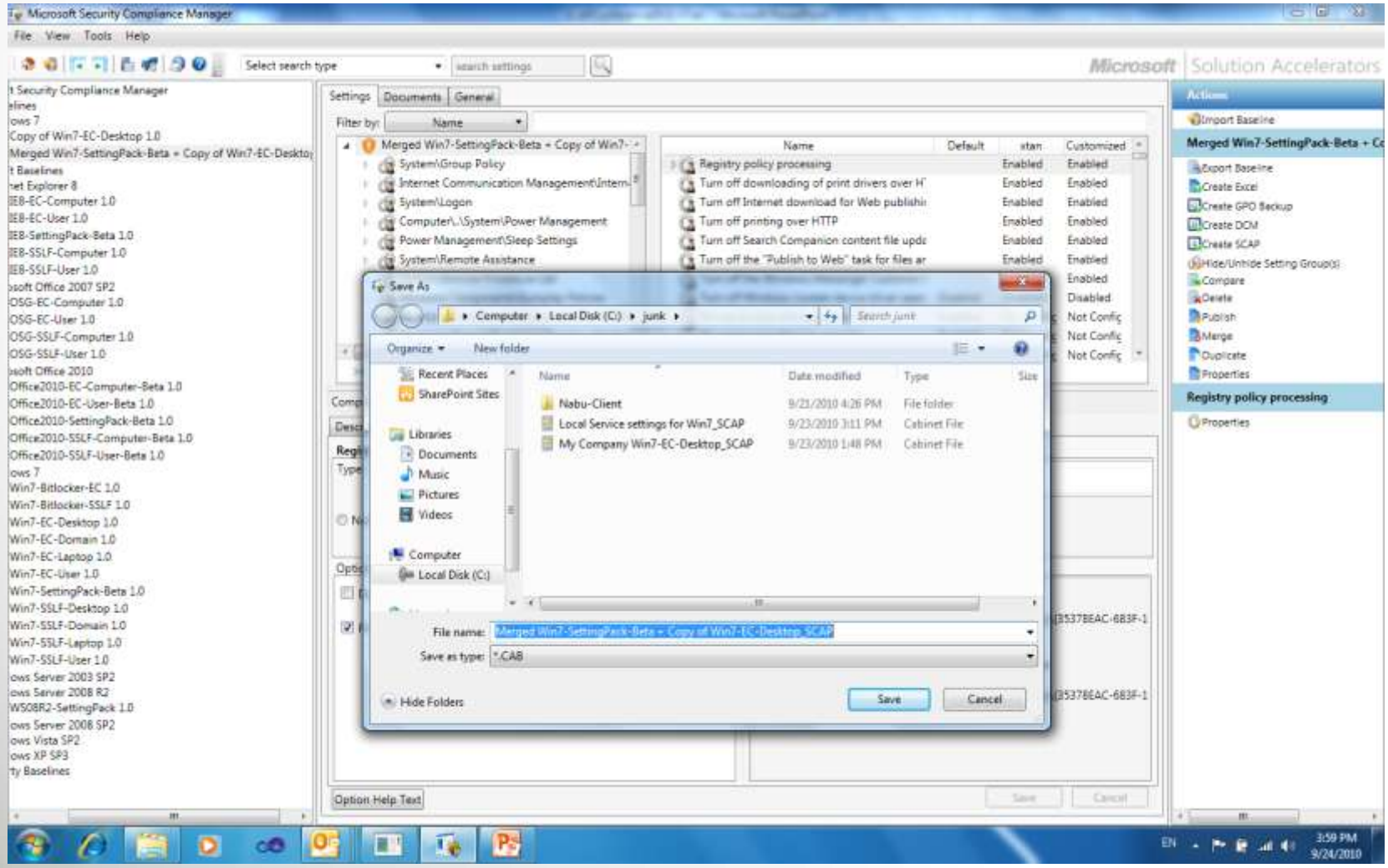
Setting Packs

- **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



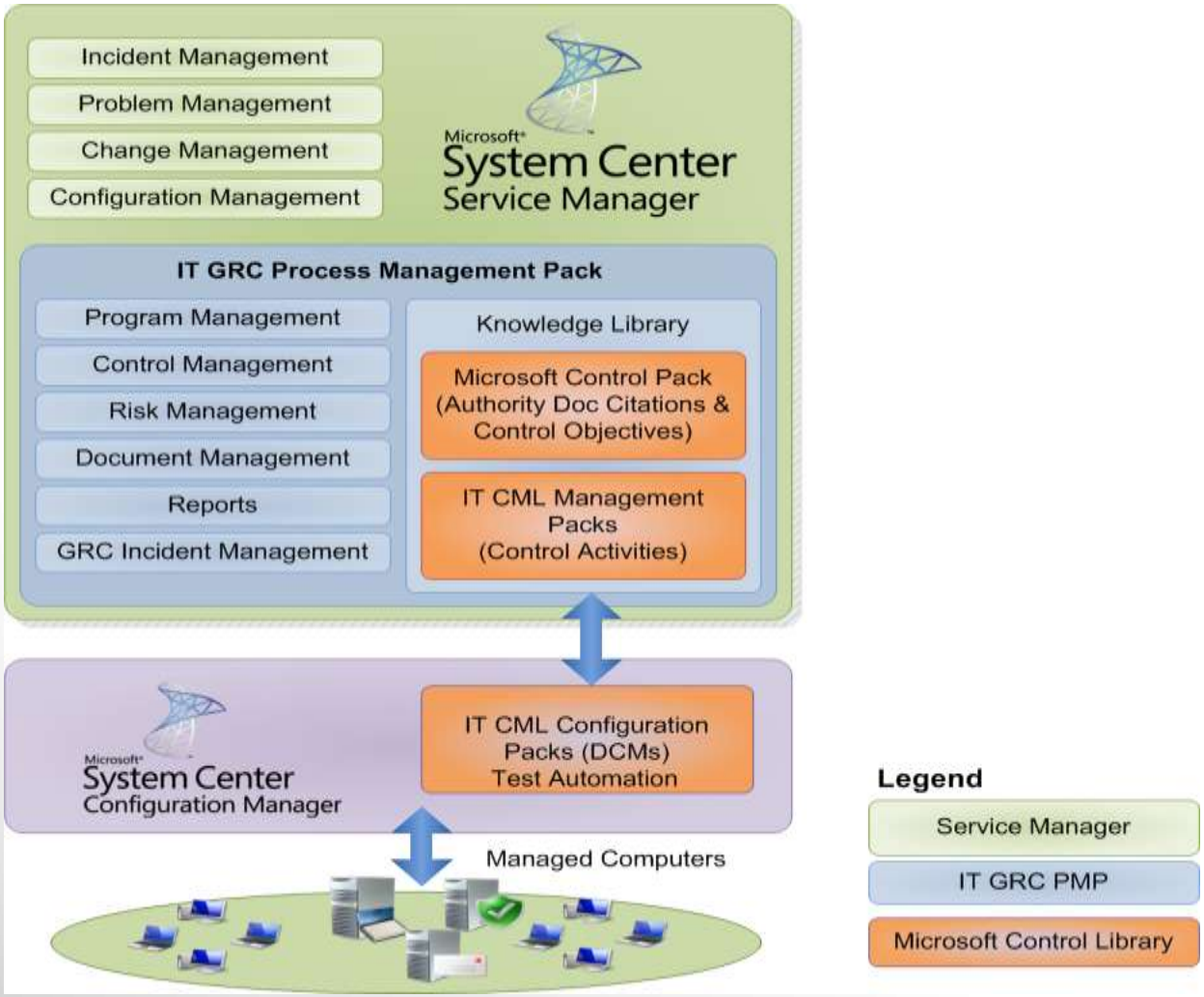
Demo – Authoring SCAP Content From SCM



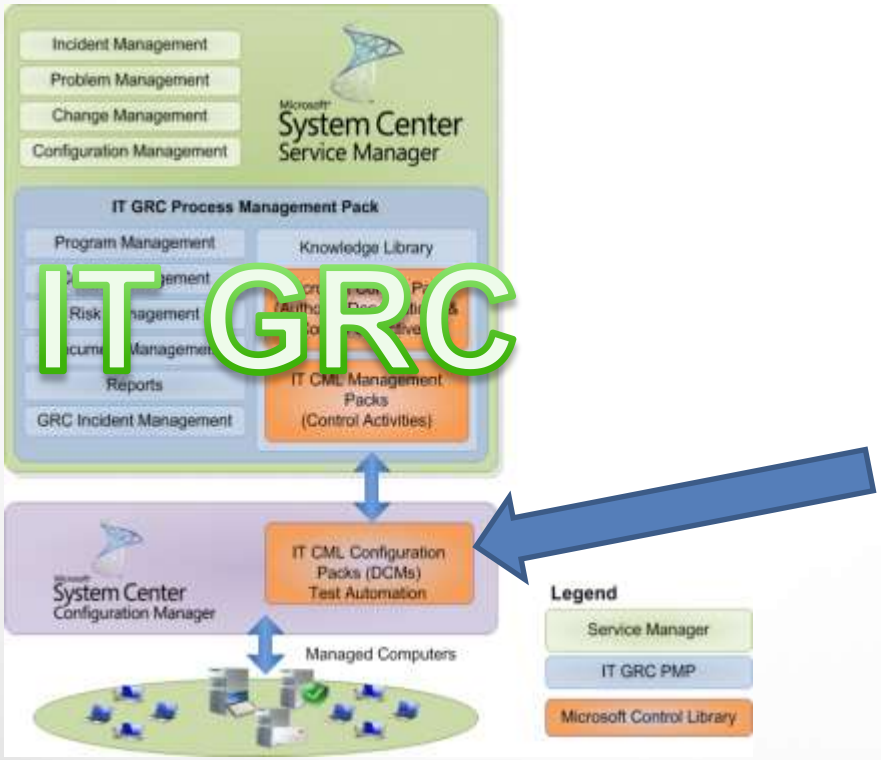
Available Setting Packs in Beta

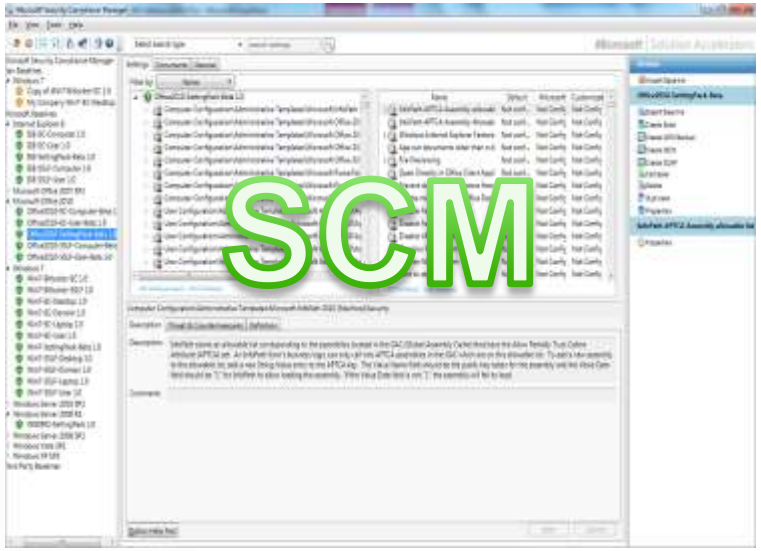
Microsoft Product	Setting Groups	Settings/Options
Windows Server 2008 R2	168	1478
Windows 7	168	1478
Office 2010	306	3898
Internet Explorer	90	2566

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 or secwish@microsoft.com

Q/A