

 | Solution Accelerators

# Security Compliance Manager (SCM) v2.0

Vlad Pigin  
Sr. Program Manager

Shelly Bird  
Architect

November 2011

# Session Objectives and Takeaways

- The past, present, and future of Security Guidance and Microsoft Baselines
- Customer challenges
- SCM 2 Overview
  - Key use scenarios
  - Key features and benefits
  - Baselines we ship today
  - Installation & configuration
  - Learn
  - Customize
  - Export
  - Verify
- Field experience and examples
- SCM related links
- Questions

## Customer Challenges

- **Lack of timely authoritative prescriptive security guidance**
  - Guidance released for different products at different times and comes from various sources
- **Inconsistent customer experience**
  - Security guidance provided by Microsoft was delivered in many different formats
  - Customers need to visit several websites, and download separate tools and documents to get guidance for all products
- **Lack of automation tools**
  - Customizing and deploying security guidance is tedious and time consuming
  - Multiple products involved – GPO to set, DCM to check, etc.
- **IT compliance is difficult to manage**
  - Determining if deployed security configurations are still in effect, and comply with an environments requirements is quite challenging

## SCM Overview

- Learn → Customize → Export → Verify
- SCM provides centralized security baseline management features, a baseline portfolio, customization capabilities, and security baseline export flexibility to accelerate your organization's ability to efficiently manage the security and compliance process for the most widely used Microsoft technologies.



## SCM v2 Use Scenarios

- Securing Windows Client
- Locking Down Windows Server Roles
- Applying Security recommendations to Microsoft Office
- Creating Public Access or Kiosk Desktops
- Internet Disconnected Environment
- Tracking decision making for security audits

## Baselines that ship inside SCM today

- **Server Operating Systems:**
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2
  - Windows Server 2003 SP2
- **Client Operating Systems:**
  - Windows 7
  - Windows Vista SP2
  - Windows XP SP3
- **Applications:**
  - Office 2010
  - Office 2007 SP2
  - Internet Explorer 9
  - Internet Explorer 8
- **MS Consulting Services:**
  - USGCB (United States Government Configuration Baseline) – <http://usgcb.nist.gov>
- Auto-update functionality in SCM alerts you of new baselines releases



# Main view breakdown & filters

The screenshot displays the Microsoft Security Compliance Manager interface. The left-hand navigation pane shows a tree view of baselines, with 'IE9 Computer Security Compliance 1.0' selected. The central pane shows the 'Advanced View' of this baseline, displaying a table of settings. The right-hand pane contains various actions such as 'Import', 'Export', 'Baseline', 'Setting', and 'Help'.

**Left-hand navigation pane (Custom Baselines):**

- Microsoft Baselines
  - Internet Explorer 8
  - Internet Explorer 9
    - Attachments \ Guides
    - IE9 Computer Security Compliance 1.0
    - IE9 User Security Compliance 1.0
  - Microsoft Office 2007 SP2
  - Microsoft Office 2010
  - Windows 7
  - Windows Server 2003 SP2
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2
  - Windows Vista SP2
  - Windows XP SP3
- Other Baselines

**Central pane (IE9 Computer Security Compliance 1.0 - 154 Setting(s)):**

**Advanced View**

tes | Windows Components | Internet Explorer | Choose Columns | Group View | Setting search

Name	Default	Microsoft	Customized	Severity
<b>Authentication Types</b> 2 Setting(s)				
Logon options	Prompt for user n	Enabled	Enabled	Important
Logon options	Automatic logon	Enabled	Enabled	Important
<b>Certificate Management</b> 2 Setting(s)				
Prevent ignoring certificate errors	Disabled	Enabled	Enabled	Important
Check for server certificate revocation	Disabled	Enabled	Enabled	Important
<b>Key Management</b> 1 Setting(s)				
Turn off Encryption Support	Disabled	Enabled	Enabled	Critical
<b>Least Functionality</b> 82 Setting(s)				
Software channel permissions	High safety	Enabled	Enabled	Important
Download signed ActiveX controls	Disabled	Enabled	Enabled	Important
Security Zones: Do not allow users to change policies	Disabled	Enabled	Enabled	Critical
Logon options	Prompt for user n	Enabled	Enabled	Important
Allow active scripting	Disabled	Enabled	Enabled	Important
Disable Browser Geolocation	Disabled	Enabled	Enabled	Important
Access data sources across domains	Disabled	Enabled	Enabled	Important
Only allow approved domains to use ActiveX controls without prompt	Enabled	Enabled	Enabled	Important
Security Zones: Do not allow users to add/delete sites	Disabled	Enabled	Enabled	Critical
Allow status bar updates via script	Disabled	Enabled	Enabled	Important
Navigate windows and frames across different domains	Disabled	Enabled	Enabled	Important

**Right-hand pane:**

- Global setting search
- Import
  - GPO Backup (folder)
  - SCM (.cab)
- Export
  - Excel (.xism)
  - GPO Backup (folder)
  - SCAP v1.0 (.cab)
  - SCCM DCM 2007 (.cab)
  - SCM (.cab)
- Baseline
  - Compare / Merge
  - Delete
  - Duplicate
  - Properties
- Setting
- Setting Group
- Help
  - About
  - Help Topics
  - Release Notes
  - Send Feedback
  - Privacy Statement

# SCM Overview

- Baselines Library in the left pane
- Settings / recommendations in middle
- Actions in right pane
- New setting grid
- Advanced view
- New Compare & Merge
- Add / Delete settings



Win7-EC-Domain 1.0 9 Setting(s)

Advanced View

< Security Settings > Account Policies > > X > Choose Columns > Group View > Setting search

Name	Default	Microsoft	Customized	Severity
Account Policies\Account Lockout Policy 3 Setting(s)				
Account lockout duration	Not defined	15 minute(s)	15 minute(s)	None
Account lockout threshold	0 invalid logon attempts	50 invalid logon attempts	50 invalid logon attempts	None
Reset account lockout counter after	0	15 minute(s)	15 minute(s)	None



# Settings details view

IE9 Computer Security Compliance 1.0 154 Setting(s)

Advanced View

Name	Default	Microsoft	Customized	Severity
<b>Authentication Types</b> 2 Setting(s)				
Logon options	Prompt for user n	Enabled	Enabled	Important
Logon options	Automatic logon	Enabled	Enabled	Important
<b>Certificate Management</b> 2 Setting(s)				
Prevent ignoring certificate errors	Disabled	Enabled	Enabled	Important

[Customize this setting by duplicating the baseline](#)
 Severity: 
[Collapse](#)

Not Configured
  Enabled
  Disabled
 [Option Help Text](#)

**Setting Details**

**UI Path:**  
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel

**Description:**  
When a user experiences Secure Socket Layer/Transport Layer Security (SSL/TLS) certificate errors such as "expired," "revoked," or "name mismatch," Internet Explorer blocks the user's ability to continue browsing the Web site.

**Vulnerability:**  
Users who ignore certificate errors are more likely to visit unauthorized sites or sites that host malicious content.

**Potential Impact:**  
If you enable this policy setting, the user is not permitted to continue browsing the Web site. If you disable this policy setting or do not configure it, the user may elect to ignore certificate errors and continue browsing the Web site.

**Additional Details:**  
Prevent ignoring certificate errors  
CCE-17378-1  
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\PreventIgnoreCertErrors  
REG\_DWORD:1

**Countermeasure:**  
Enable this setting.

## Editing Baselines in Library

- Baseline Library lives in left pane
- Baselines downloaded from Download Center are Read-Only
- Duplicate Read-Only baselines to create editable Baselines
- More Actions exposed when editable Baseline highlighted
- Search for Baselines or Settings using keywords

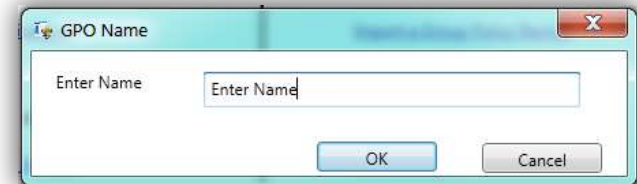


The screenshot shows the "Advanced View" of the Microsoft Security Compliance Manager settings. The table displays the following data:

Name	Default	Microsoft	Customized	Severity
<b>Authentication Types</b> (2 Setting(s))				
Logon options	Prompt for user n	Enabled	Enabled	Important
Logon options	Automatic logon	Enabled	Enabled	Important
<b>Certificate Management</b> (2 Setting(s))				
Prevent ignoring certificate errors	Disabled	Enabled	Enabled	Important
Check for server certificate revocation	Disabled	Enabled	Enabled	Important

# Importing security baselines / GPO's

- Knowledge lives in the AD, not in SCM Baselines
- Create baselines from your production GPOs
  - Import GPO Backups created using GPMC
- Import Third Party Baselines in .cab format
- GPO Backups created using LocalGPO
  - Snapshot your “golden master” configuration from a reference computer
  - Create baselines in SCM that match the configuration of your reference computers



Name	Default	Microsoft	Customized	Severity	Path
<b>Account Policies\Account Lockout Policy</b> 3 Setting(s)					
Account lockout duration	Not defined	15 minute(s)	15 minute(s)	None	Computer Configuration\Windows Si
Account lockout threshold	0 invalid logon att	50 invalid logon a	50 invalid logon a	None	Computer Configuration\Windows Si
Reset account lockout counter after	0	15 minute(s)	15 minute(s)	None	Computer Configuration\Windows Si
<b>Account Policies\Password Policy</b> 6 Setting(s)					
Enforce password history	24 passwords rem	24 password(s)	24 password(s)	None	Computer Configuration\Windows Si
Maximum password age	42 days	90 days	90 days	None	Computer Configuration\Windows Si
Minimum password age	0 days	1 day(s)	1 day(s)	None	Computer Configuration\Windows Si
Minimum password length	0 characters	8 character(s)	8 character(s)	None	Computer Configuration\Windows Si
Password must meet complexity req	Disabled	Enabled	Enabled	None	Computer Configuration\Windows Si

# Compare & Merge baselines

- SCM has the ability to compare & merge Baselines/GPOs
- Baselines/GPOs must be imported into SCM
- Highlight Baseline then select Compare/Merge in Actions pane
- Save Results in .EXCEL report
- Use comparison to compare against Microsoft baseline recommendations
  - To identify overlap
  - To learn about settings unique to Microsoft baselines
  - To review setting prescriptions specific to your baselines
- Merge wizard allows review settings with changing values; defined in both baselines, overwrite?

**Compare Baselines**

**Summary**  
 Baseline A: Contoso Domain Security Baseline for Win 7 1.0  
 Baseline B: Win7-EC-Domain 1.0  
 Total unique settings compared: 20  
 Total settings in common: 9  
 Total settings not in common: 1

**Settings that differ (3)**

Name	Baseline A	Baseline B	UI Path
Minimum password age	5	1	Computer Configuration\Windows Settings\Security
Minimum password length	12	8	Computer Configuration\Windows Settings\Security
Password must meet complexity requirements	Disabled	Enabled	Computer Configuration\Windows Settings\Security

**Settings that match (6)**

Name	Baseline A	Baseline B	UI Path
Enforce password history	24	24	Computer Configuration\Windows Settings\Security
Maximum password age	90	90	Computer Configuration\Windows Settings\Security
Store passwords using reversible encryption	Disabled	Disabled	Computer Configuration\Windows Settings\Security
Account lockout duration	15	15	Computer Configuration\Windows Settings\Security
Account lockout threshold	50	50	Computer Configuration\Windows Settings\Security
Reset account lockout counter after	15	15	Computer Configuration\Windows Settings\Security

Buttons: Merge Baselines, Export to Excel, Close

**Merge Baselines**

**Summary**  
 Baseline A: Contoso Domain Security Baseline for Win 7  
 Baseline B: Win7-EC-Domain

**Merge conflicts to resolve (3)**

Name	Baseline A	Baseline B
Minimum password age	<input checked="" type="radio"/> 5	<input type="radio"/> 1
Minimum password length	<input checked="" type="radio"/> 12	<input type="radio"/> 8
Password must meet complexity requirements	<input checked="" type="radio"/> Disabled	<input type="radio"/> Enabled



## Export baselines to desired format

- **GPO Backup (Set)**
  - Can be imported into Active Directory
  - Can be applied to standalone computers using LocalGPO
- **SCCM 2007 DCM Pack (Get)**
  - Can help verify deployed configurations
- **SCAP data stream (Get)**
  - Product agnostic scanning method (<http://scap.nist.gov>)
- **Excel (for documentation and analysis purposes)**
  - Includes all setting data visible in SCM
- **SCM .CAB format**
  - Allows for baseline sharing between SCM installations





## Apply GPO Backup to Local Policy

- LocalGPO can apply a GPO Backup to a local machine
- Lockdown DMZ computers with domain GPOs
- Apply Baseline to image before deployment

```

LocalGPO Tool

Microsoft (R) Windows Script Host Version 5.8
Copyright (C) Microsoft Corporation. All rights reserved.

LocalGPO - Configures various aspects of a computer's Local Policy

Usage: LocalGPO.exe [-Path:Path] [-GPO Backup:GPO Backup] [-Export] [-GPO Backup:Name]
LocalGPO.exe [-ConfigGPO] [-RestoreGPO] [-Restore]

Options:
-Path:Path          : Applies the contents of a GPO Backup to the local policy
                    of a Windows computer.
-Export             : Exports Local Policy to a GPO Backup.
-GPO Backup:Name    : Creates a GPO Backup that contains all components required
                    for it to apply. It is to be applied to the local security policy of a
                    computer. Specifying a name is optional.
-ConfigGPO          : Applies user settings from a GPO Backup to the specified
                    GPO on a Windows computer. Must specify Administrator,
                    Secure(Not-Administrator), or a valid account name.
-Restore            : Restores Local Policy to the default configuration.
-ConfigGPO          : Configures Security Configuration Editor (SCE) to display
                    MSE settings.
-RestoreGPO         : Restores SCE to default settings.

Examples:

script LocalGPO.exe /Path:C:\GPOBackups\GPO Backup GPO1
- Applies the contents of the GPO Backup stored in the specified
  path to the Local Policy of a Windows computer.

script LocalGPO.exe /Path:C:\GPOBackups /Export
- Exports a GPO Backup based on the Local Policy configuration
  to a folder in the specified path.

script LocalGPO.exe /Path:C:\GPOBackups /Export /GPOBackup
- Creates a GPOBackup and stores it in the specified path. GPOBackups
  can be copied to other computers, and applied by double-clicking
  GPOBackup.exe.

script LocalGPO.exe /Path:C:\GPOBackups\GPO Backup GPO2 /-ConfigGPO
- Applies the contents of the GPO Backup stored in the specified
  path to the specified Multiple Local Group Policy Object (MLGPO).

script LocalGPO.exe /Restore
- Restores the entire local policy to its default configuration.
  
```

## Export Local Policy to GPO Backup

- Exported baselines/GPOs can be imported to non-domain joined computers
- Exported GPO Backups can be imported into SCM v2 beta
- Share Baselines/GPOs between Local and Domain policies

The Microsoft logo is displayed in white, followed by a vertical line and the text "Solution Accelerators" in a white sans-serif font. The background is a dark blue gradient with a white grid pattern of curved lines in the upper left corner.

**Microsoft** | Solution Accelerators

# **Lessons Learned Using SCM to Meet the USGCB Mandate**

Windows 7 Focus

# Stick to the Standard



Istockphoto.com/rtortolt@hotmail.com

# Don't pull in old settings



istockphoto.com/rtortoit@hotmail.com

# Contain the new systems



Istockphoto.com/rtortoit@hotmail.com



# Add a WMI Filter



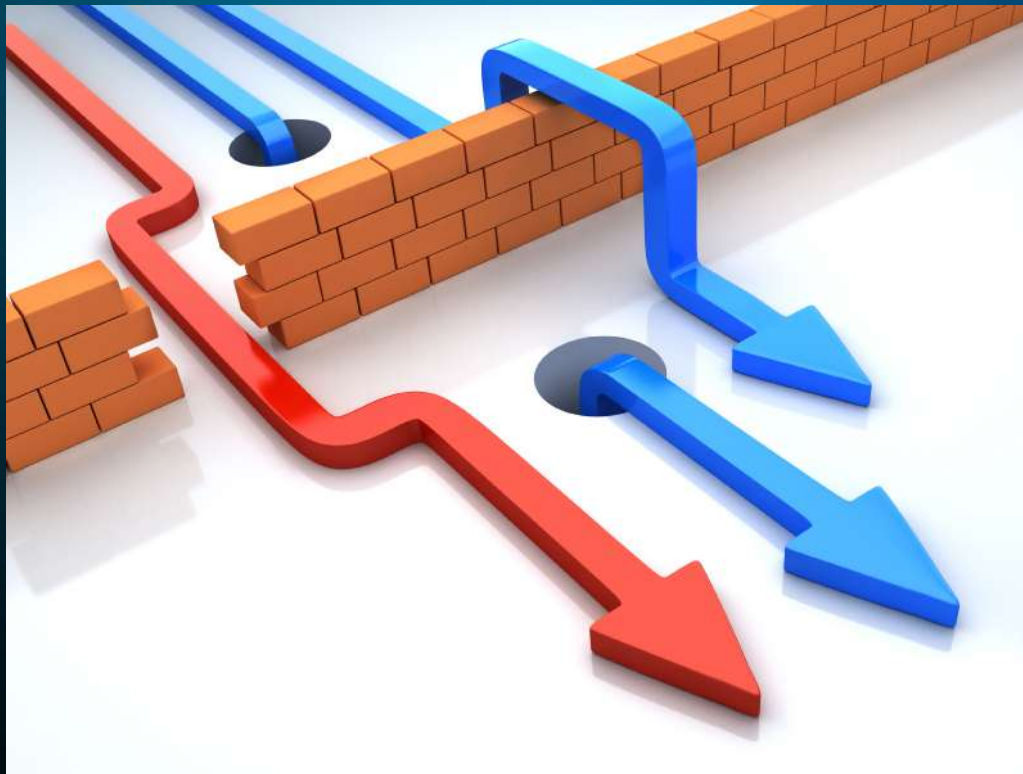
istockphoto.com/rtortol@hotmail.com

# Study impact statements



Istockphoto.com/rortolt@hotmail.com

# Veer when absolutely necessary



istockphoto.com/rtortol@hotmail.com

## Recap: Lessons Learned

1. **Stick to the standard:** US Govt Configuration Baseline
2. **Don't pull in old settings** from older operating systems
3. **Contain the new Windows 7 systems** in a carefully controlled set of OUs
4. **Add a WMI filter to Group Policy** to target Windows 7
5. **Study impact statements** in SCM and gather your own
6. **Don't be afraid to veer from the standard** when your situation calls for it; document why for auditors in SCM





## How it works in the Real World



## Real World Implementation: US Air Force



- **History:**
  - Coming from Vista / XP
  - Managed for 7 years
- **Achievement:**
  - 386,000 desktops deployed in 12 months (~575,000 targeted)
  - 253 management sites
  - Averaging over 8,000 desktops per week
- **Using:** Configuration Manager 2007 OSD, SCM LGPO, Bitlocker, Network Access Protection (NAP)

## Some History

- Largely unmanaged in 2004
- Moved 525,000 to managed Windows XP in **18** months (FDCC)
- Moved 400,000 to Vista in **15** months
- Moved 386,000 to Windows 7 in **12** months
- When self-service offered, saw a 2:1 pickup (pull versus push)
- US Air Force is an active participant in early adopter programs (Technical Adoption Program)

## Key Factors in Success

- **Hardware Council**, hardware buy each quarter
- **Inclusive planning sessions**, regular outreach
- **Strategically placed technical resources**
- **Quarterly image** (just one for all models)
- **Simple installation**, less than five steps from USB FOB or disk, or Zero Touch push of image
- **Zero Touch** Systems Center Configuration Manager Operating System Deployment

## Some Surprising Facts

- **Application compatibility:** issues with security settings were and are far less than expected
- **Controlled self-service is popular, and cheap**
- **Each deployment cycle accelerated, despite 3x larger images compared to XP**
- **Comply & Connect in monitoring mode works**
- **Going through Vista was worth it**
- **Zero Touch Systems Center Configuration Manager Operating System Deployment**

## From 1,000/week to 8,000

- From 10Mbps Ethernet to 1 Gigabit  
(cut 30-40 min per install, 10-15 min download)
- From Network data transfer to in-disk transfer  
(cut 2 hrs per install, 3 to 5 minutes per 5GB)
  - User State Migration Toolkit Hard Links
- Standardized procedures
  - Task sequences
  - Group Policy Objects
- **Practice**



Questions?