Microsoft | Solution Accelerators

Security Compliance Manager (SCM) v2.0

Vlad Pigin
Sr. Program Manager

Shelly Bird
Architect

November 2011

Session Objectives and Takeaways

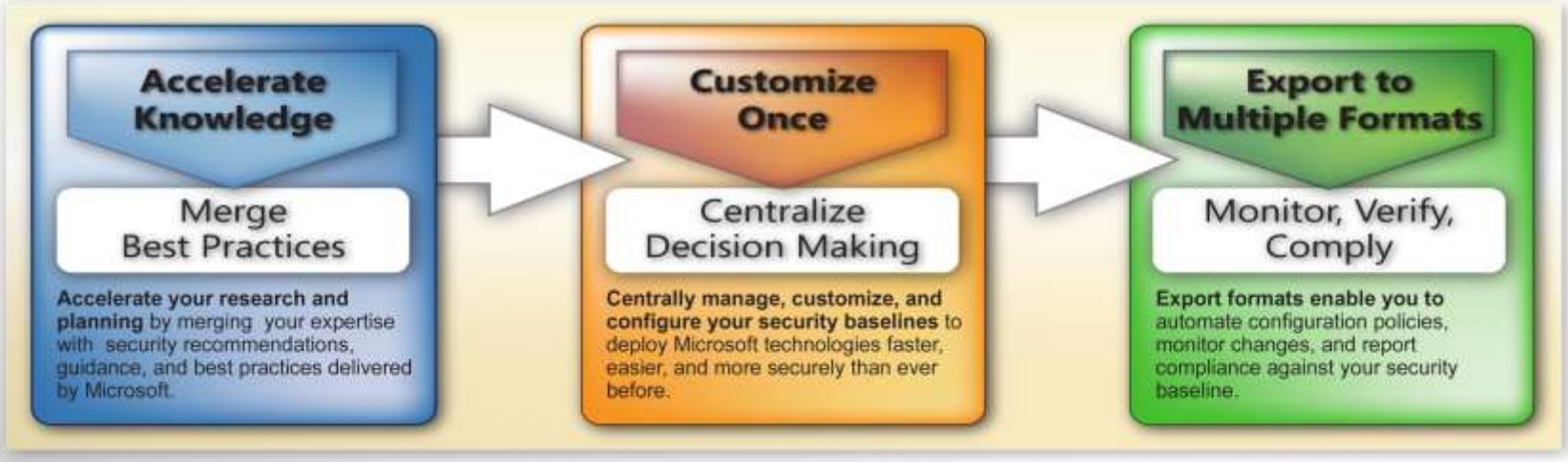
- The past, present, and future of Security Guidance and Microsoft Baselines
- Customer challenges
- SCM 2 Overview
  - Key use scenarios
  - Key features and benefits
  - Baselines we ship today
  - Installation & configuration
  - Learn
  - Customize
  - Export
  - Verify
- Field experience and examples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



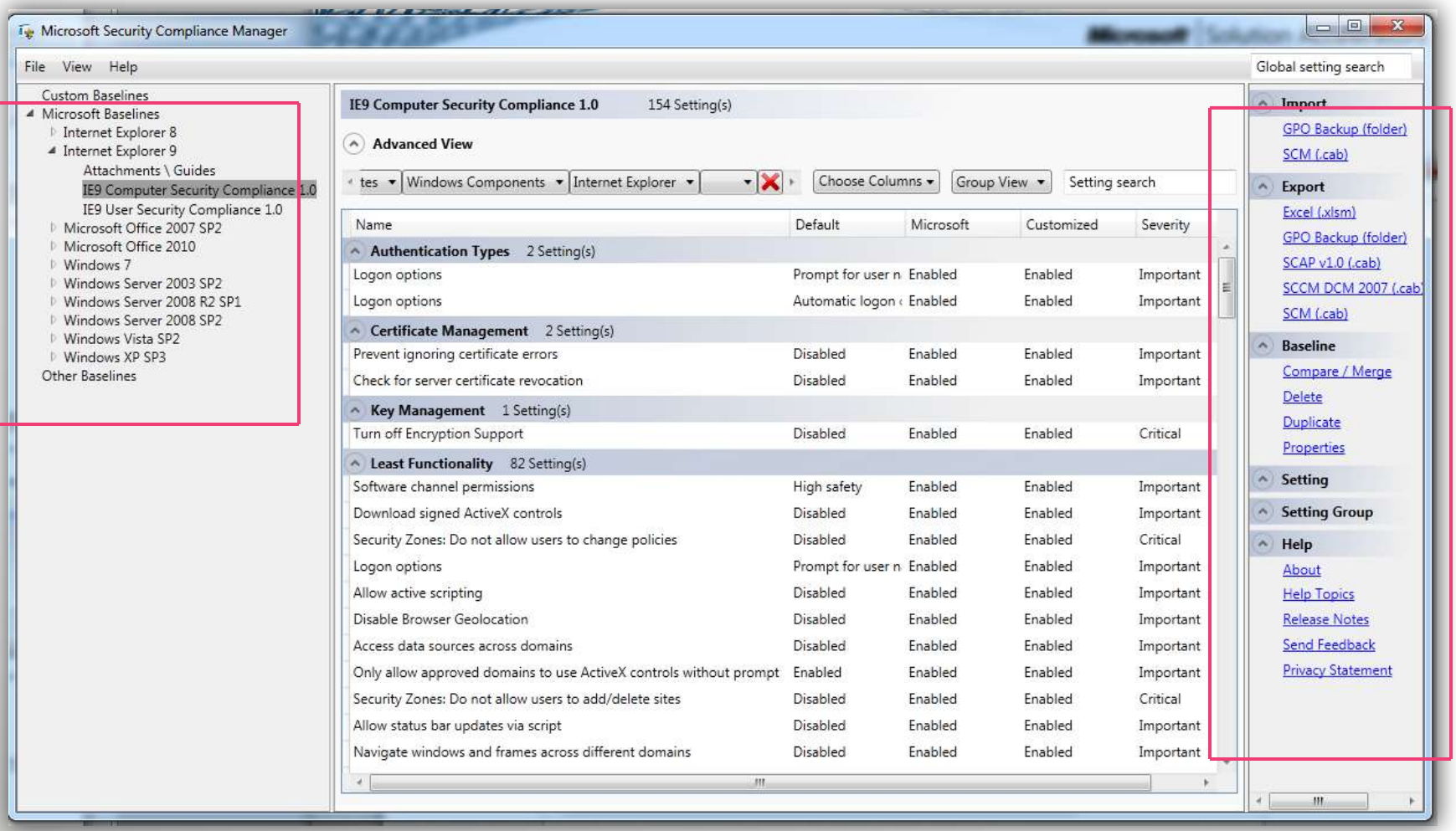
SCM v2 Use Scenarios

- 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

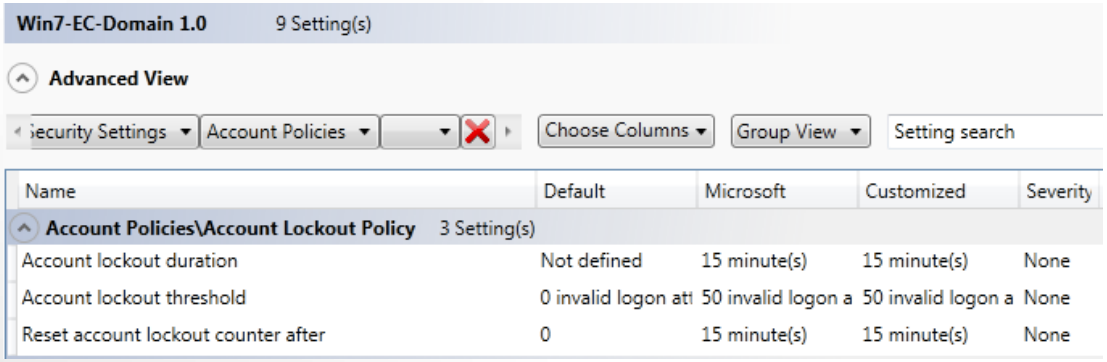
- **Server Operating Systems:**
  - Windows Server 2008 R2 SP1
  - Windows Server 2008 SP2
  - Windows Server 2003 SP2
- **Client Operating Systems:**
  - Windows 7
  - Windows Vista SP2
  - Windows XP SP3
- **Applications:**
  - Office 2010
  - Office 2007 SP2
  - Internet Explorer 9
  - Internet Explorer 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

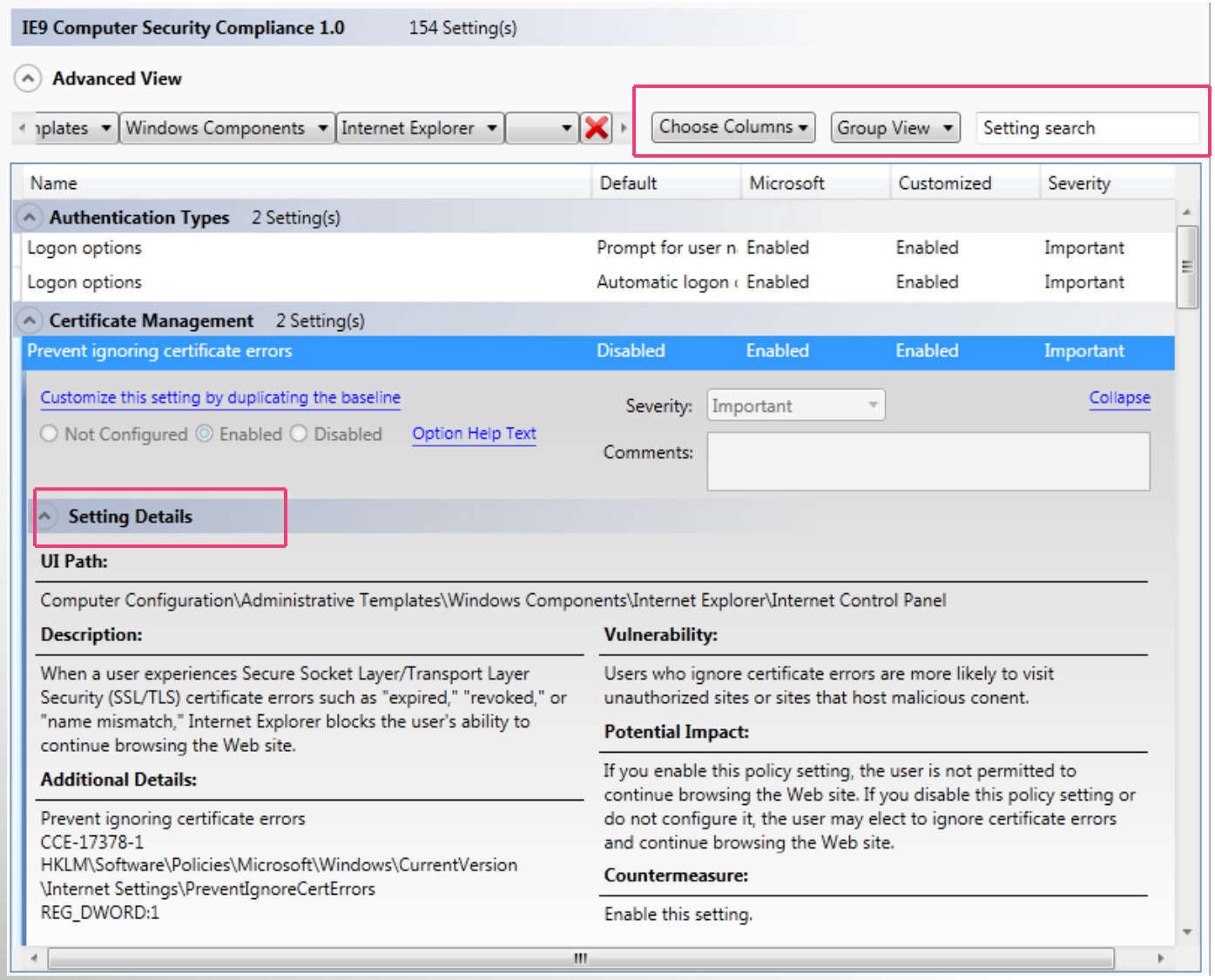


SCM Overview

- 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

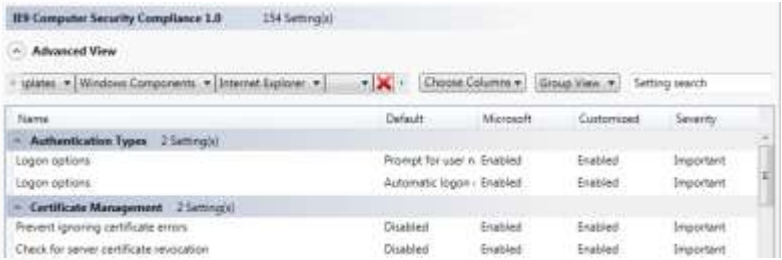


Settings details view



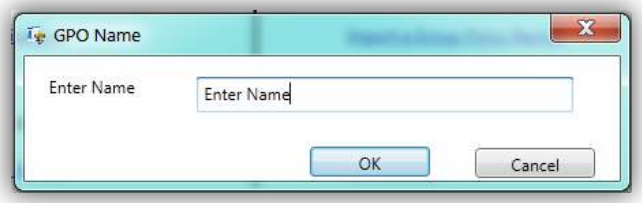
Editing Baselines in Library

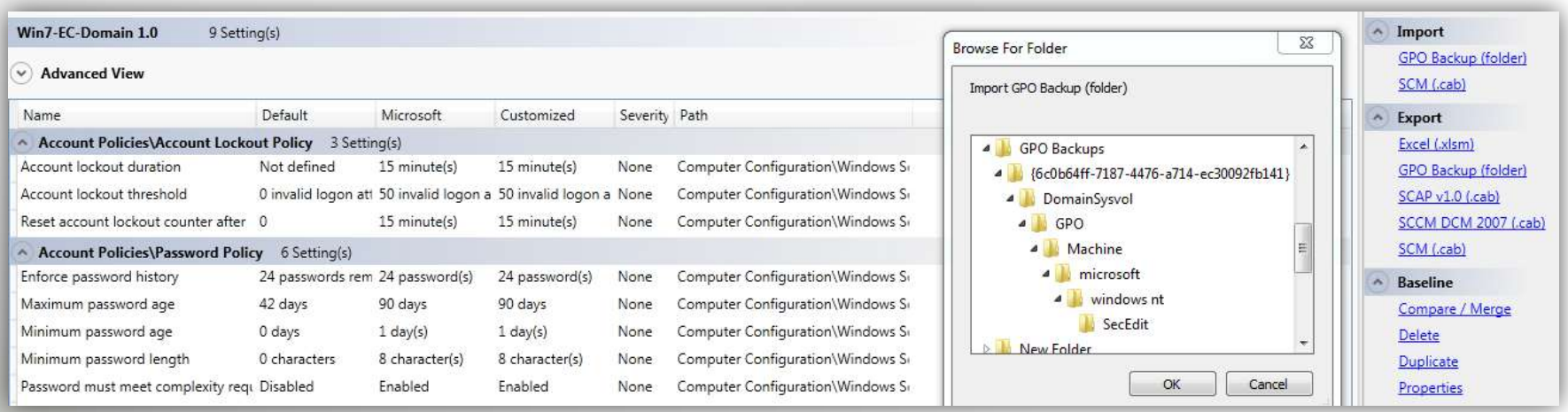
- Baseline Library lives in left pane
- Baselines downloaded from Download Center are Read-Only
- Duplicate Read-Only baselines to create editable Baselines
- More Actions exposed when editable Baseline highlighted
- Search for Baselines or Settings using keywords



Importing security baselines / GPO's

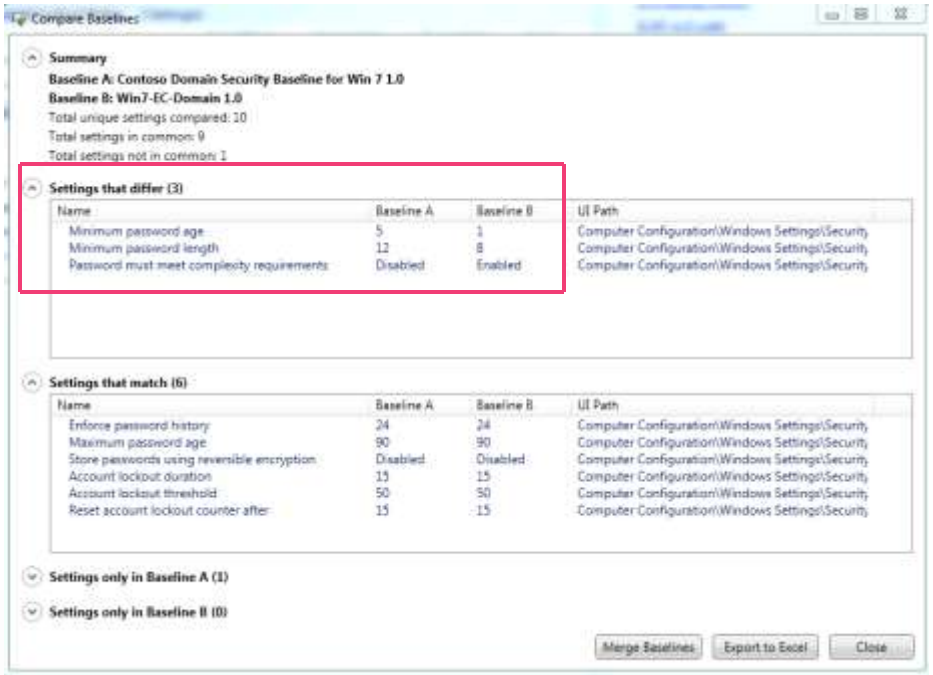
- Knowledge lives in the AD, not in SCM Baselines
- Create baselines from your production GPOs
  - Import GPO Backups created using GPMC
- Import Third Party Baselines in .cab format
- GPO Backups created using LocalGPO
  - Snapshot your "golden master" configuration from a reference computer
  - Create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

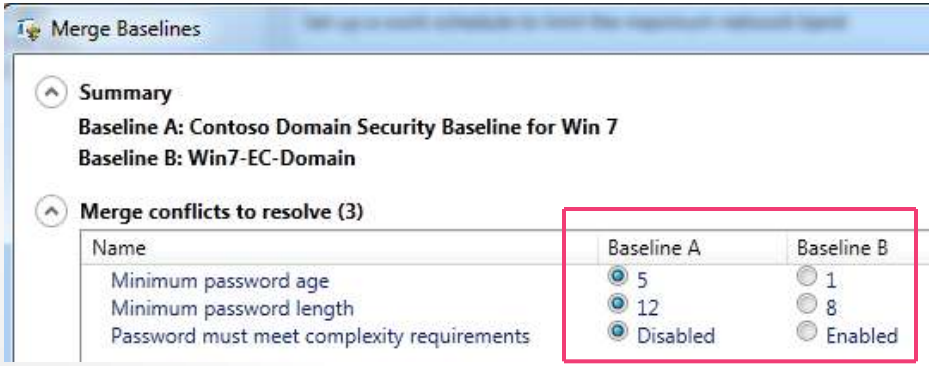




Compare & Merge baselines

- 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?





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

Export Local Policy to GPO Backup

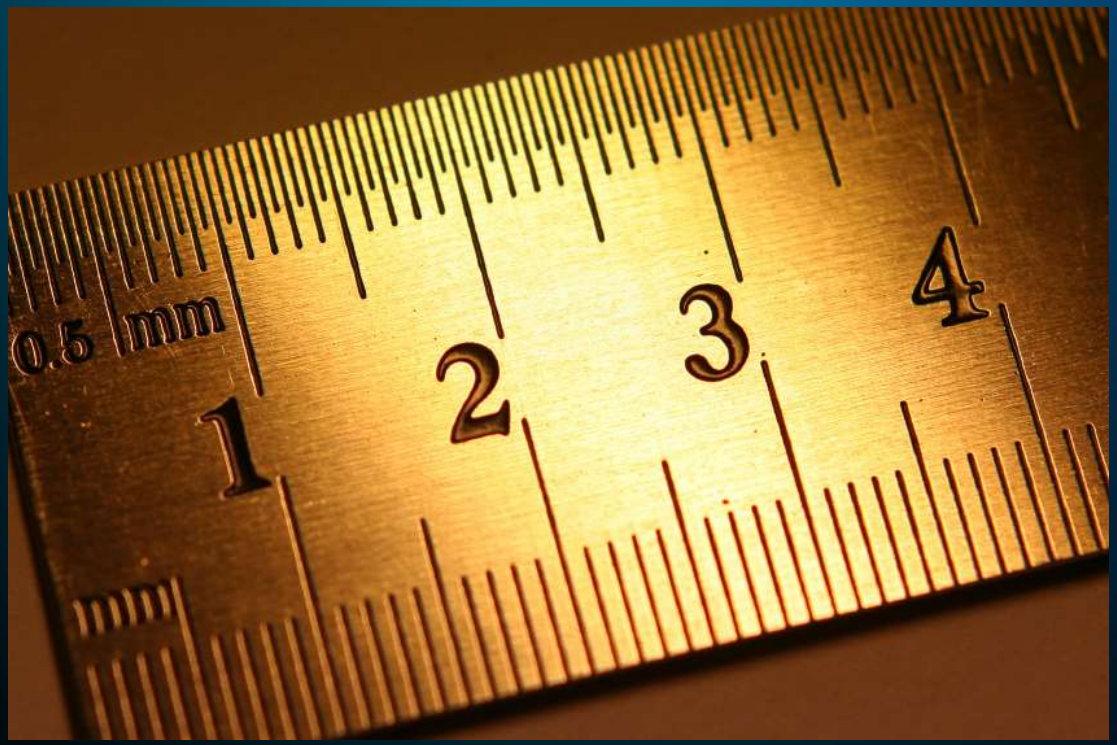
- Exported baselines/GPOs can be imported to non-domain joined computers
- Exported GPO Backups can be imported into SCM v2 beta
- Share Baselines/GPOs between Local and Domain policies

Microsoft | Solution Accelerators

Lessons Learned
Using SCM to Meet the USGCB Mandate

Windows 7 Focus

Stick to the Standard



Istockphoto.com/rtortoit@hotmail.com

Don’t pull in old settings

Istockphoto.com/rtortoit@hotmail.com

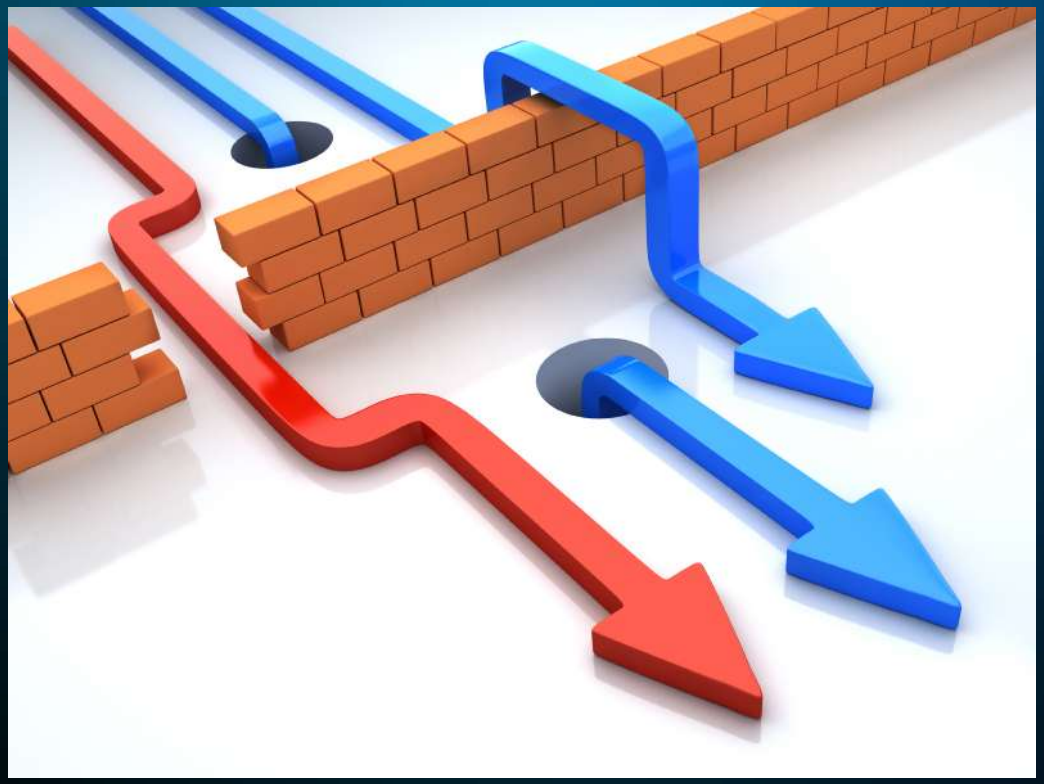
Contain the new systems

Add a WMI Filter

Study impact statements

Istockphoto.com/rtortoit@hotmail.com

Veer when absolutely necessary



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

Microsoft | Solution Accelerators

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**

Microsoft | Solution Accelerators

Questions?