Federal Desktop Core Configuration

presented by:
Stephen Quinn
National Institute of Standards and Technology
Agenda

- Federal Desktop Core Configuration History
- Security Content Automation Protocol Interlude
- SCAP and FDCC
- FDCC Web Site and Tools
- FDCC High Impact Settings and Frequently Asked Questions
OMB Deep Dive Working Group

Acknowledgements

- Office of Management and Budget
- US Air Force
- Microsoft
- National Institute of Standards and Technology
- Defense Information Systems Agency
- National Security Agency
- Department of Homeland Security
Federal Desktop Core Configuration (FDCC)

- Common core Microsoft Windows configuration driven by OMB
- Leverage USAF Standard Configuration Desktop initiative
  - Deployed and tested across half a million Windows XP systems
- Based on the DISA, NSA, NIST, USAF, and Microsoft existing guidelines for securing Windows XP and Vista
- Includes applications beyond Operating System
  - Windows XP/Vista Firewall
  - Internet Explorer 7
OMB Memo M-07-11
Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

March 22, 2007

M-07-11

MEMORANDUM FOR THE HEADS OF DEPARTMENTS AND AGENCIES

FROM: Clay Johnson
Deputy Director for Management

SUBJECT: Implementation of Commonly Accepted Security Configurations for Windows Operating Systems

To improve information security and reduce overall IT operating costs, agencies who have Windows XP™ deployed and plan to upgrade to the Vista™ operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS).

The recent release of the Vista™ operating system provides a unique opportunity for agencies to deploy secure configurations for the first time when an operating system is released. Therefore, it is critical for all Federal agencies to put in place the proper governance structure with appropriate policies to ensure a very small number of secure configurations are allowed to be used.

DOD has worked with NIST and DHS to reach a consensus agreement on secure configurations of the Vista™ operating system, and to deploy standard secure desk tops for Windows XP™. Information is more secure, overall network performance is improved, and overall operating costs are lower.

Agencies with these operating systems and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008. Agencies are requested to submit their draft implementation plans by May 1, 2007 at fisma@omb.eop.gov. With your endorsement we will work with your CIOs on this effort to improve our security for government information. If you have questions about this requirement, please contact Kiren Evans, Administrator, E-Government and Information Technology at (202) 453-1181 or at fisma@omb.eop.gov.

Corresponding OMB Memo to CIOs:
- Requires, “Implementing and automating enforcement of these configurations;”
- “NIST has established a program to develop and maintain common security configurations for many operating systems and applications, and the “Security Content Automation [Protocol]” can help your agency use common security configurations. Additionally, NIST’s revisions to Special Publication 800-70, “Security Configuration Checklist Program for IT Products,” will provide your agency additional guidance for implementing common security configurations. For additional information about NIST’s programs, please contact Stephen Quinn, at Stephen.Quinn@nist.gov.”
The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). “

Applications designed for normal end users shall run in the standard user context without elevated system administration privileges.”

“The National Institute of Standards and Technology (NIST) and the Department of Homeland Security continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers’ access to Windows XP and VISTA images. The images will be pre- configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.”
Producing an FDCC Virtual Machine Image

Implement FDCC settings on virtual machine images

Use SCAP to verify FDCC settings were implemented correctly
- Windows XP
- Windows Vista
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7.0

Reconcile any “failed” SCAP tests

Record any exceptions
**What is SCAP?**

**How**

Standardizing the format by which we communicate

**What**

Standardizing the information we communicate

**Protocol**

- CVE
- OVAL
- CVSS
- CPE
- SCAP
- XCCDF
- CCE

**Content**

- [http://nvd.nist.gov](http://nvd.nist.gov)

- 50 million hits per year
- 20 new vulnerabilities per day
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Produces XML feed for NVD content
<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>Common</td>
<td>Standard nomenclature and dictionary of security related software</td>
</tr>
<tr>
<td></td>
<td>Vulnerability</td>
<td>flaws</td>
</tr>
<tr>
<td></td>
<td>Enumeration</td>
<td></td>
</tr>
<tr>
<td>CCE</td>
<td>Common</td>
<td>Standard nomenclature and dictionary of software misconfigurations</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enumeration</td>
<td></td>
</tr>
<tr>
<td>CPE</td>
<td>Common</td>
<td>Standard nomenclature and dictionary for product naming</td>
</tr>
<tr>
<td></td>
<td>Platform</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enumeration</td>
<td></td>
</tr>
<tr>
<td>XCCDF</td>
<td>eXtensible Checklist Configuration Description Format</td>
<td>Standard XML for specifying checklists and for reporting results of checklist evaluation</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
<td>Standard XML for test procedures</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
<td>Standard for measuring the impact of vulnerabilities</td>
</tr>
</tbody>
</table>
Existing Federal Content
Standardizing What We Communicate

- In response to NIST being named in the Cyber Security R&D Act of 2002
- Encourages vendor development and maintenance of security guidance
- Currently hosts 112 separate guidance documents for over 125 IT products
- Translating this backlog of checklists into the Security Content Automating Protocol (SCAP)
- Participating organizations: DISA, NSA, NIST, Hewlett-Packard, CIS, ITAA, Oracle, Sun, Apple, Microsoft, Citadel, LJK, Secure Elements, ThreatGuard, MITRE Corporation, G2, Verisign, Verizon Federal, Kyocera, Hewlett-Packard, ConfigureSoft, McAfee, etc.

- Over 4 million hits per month
- About 20 new vulnerabilities per day
- Mis-configuration cross references to:
  - NIST SP 800-53 Security Controls (All 17 Families and 163 controls)
  - DoD IA Controls
  - DISA VMS Vulnerability IDs
  - Gold Disk VIDs
  - DISA VMS PDI IDs
  - NSA References
  - DCID
  - ISO 17799

- Reconciles software flaws from:
  - US CERT Technical Alerts
  - US CERT Vulnerability Alerts (CERTCC)
  - MITRE OVAL Software Flaw Checks
  - MITRE CVE Dictionary

- Produces XML feed for NVD content
How SCAP Works

- **Checklist XCCDF**
  - Platform CPE
  - Misconfiguration CCE
  - General Impact CVSS
  - Software Flaw CVE
  - General Impact CVSS

- **Test Procedures OVAL**
- **Patches OVAL**

- COTS/GOTS Tools

Specific Impact CVSS Results
Specific Impact CVSS Results
Traceability within SCAP Checklists

<Group id="IA-5" hidden="true">
<title>Authenticator Management</title>

<reference>ISO/IEC 17799: 11.5.2, 11.5.3</reference>
<reference>NIST 800-26: 15.1.6, 15.1.7, 15.1.9, 15.1.10, 15.1.11, 15.1.12, 15.1.13, 16.1.3, 16.2.3</reference>
<reference>GAO FISCAM: AC-3.2</reference>
<reference>DOD 8500.2: IAKM-1, IATS-1</reference>
</Group>

<Rule id="minimum-password-length" selected="false" weight="10.0">
<reference>CCE-100</reference>
<reference>DISA STIG Section 5.4.1.3</reference>
<reference>DISA Gold Disk ID 7082</reference>
<reference>PDI IAIA-12B</reference>
<reference>800-68 Section 6.1 - Table A-1.4</reference>
<reference>NSA Chapter 4 - Table 1 Row 4</reference>
<requires idref="IA-5"/>
[pointer to OVAL test procedure]
</Rule>

Rationale for security configuration

Keyed on SP800-53 Security Controls

Traceability to Mandates

Traceability to Guidelines
Federal Risk Management Framework

Starting Point
- **Categorize Information System**
  - Define criticality/sensitivity of information system according to potential impact of loss

Select Security Controls
- SP 800-37 / SP 800-53A
  - Monitor Security Controls
    - Continuously track changes to the information system that may affect security controls and reassess control effectiveness
  - Authorize Information System
    - Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation
  - Assess Security Controls
    - Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)
  - Select Information System
    - Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation
  - Implement Security Controls
    - Implement security controls; apply security configuration settings
  - Document Security Controls
    - Document in the security plan, the security requirements for the information system and the security controls planned or in place

Supplement Security Controls
- FIPS 200 / SP 800-53
  - Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

FIPS 199 / SP 800-60
- Categorize Information System
  - Define criticality/sensitivity of information system according to potential impact of loss

FIPS 800-37 / SP 800-53A
- Monitor Security Controls
  - Continuously track changes to the information system that may affect security controls and reassess control effectiveness

FIPS 800-37 / SP 800-30
- Authorize Information System
  - Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

FIPS 800-18
- Document Security Controls
  - Document in the security plan, the security requirements for the information system and the security controls planned or in place
## Controls with Automated Validation Support

<table>
<thead>
<tr>
<th>Tool Set</th>
<th>Automation</th>
<th>Control Count</th>
<th>Control Percent</th>
<th>Control Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Framework Tools</td>
<td>Full Automation</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Partial Automation</td>
<td>49</td>
<td>30%</td>
<td>PL-2 System Security Plan</td>
</tr>
<tr>
<td>Security Content Automation Protocol</td>
<td>Full Automation</td>
<td>31</td>
<td>19%</td>
<td>AC-11 Session Lock</td>
</tr>
<tr>
<td></td>
<td>Partial Automation</td>
<td>39</td>
<td>24%</td>
<td>AC-8 System Use Notification</td>
</tr>
<tr>
<td>Future Automation Techniques or No Automation</td>
<td></td>
<td>44</td>
<td>27%</td>
<td>AC-1 Access Control Policy and Procedures</td>
</tr>
<tr>
<td>Total Controls</td>
<td></td>
<td>163</td>
<td>100%</td>
<td></td>
</tr>
</tbody>
</table>
Integrating IT and IT Security Through SCAP

Vulnerability Management

SCAP

CPE

CPE

CCE

XCCDF

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System

Asset Management

Configuration Management

Compliance Management

CVE

OVAL

CVSS

Misconfiguration
The objective is to achieve *visibility* into prospective business/mission partners information security programs BEFORE critical/sensitive communications begin…establishing levels of security due diligence and trust.
Stakeholder and Contributor Landscape: Industry
Product Teams and Content Contributors

XACTA
Belarc
Shavlik
MITRE
eEye Digital Security
secure elements
ThreatGuard
nCircle
FuGEN
McAfee
Symantec
Configuresoft
The Center for Internet Security
Gideon Technologies
Tenable
SecureInfo
Lumension
redhat
Premier Data Services
NIST
## Stakeholder and Contributor Landscape: Federal Agencies

*SCAP Infrastructure, Beta Tests, Use Cases, and Early Adopters*

<table>
<thead>
<tr>
<th>DHS</th>
<th>OMB</th>
<th>DISA</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSA</td>
<td>IC</td>
<td></td>
</tr>
<tr>
<td>OSD</td>
<td>DISA</td>
<td>EPA</td>
</tr>
<tr>
<td>DOJ</td>
<td>EPA</td>
<td></td>
</tr>
<tr>
<td>Army</td>
<td>NIST</td>
<td></td>
</tr>
<tr>
<td>DOS</td>
<td>NIST</td>
<td></td>
</tr>
</tbody>
</table>
Producing an FDCC Virtual Machine Image

Implement FDCC settings on virtual machine images

Use SCAP to verify FDCC settings were implemented correctly

- Windows XP
- Windows Vista
- Windows XP Firewall
- Windows Vista Firewall
- Internet Explorer 7.0

Reconcile any “failed” SCAP tests

Record any exceptions
OMB 31 July 2007 Memo to CIOs

Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

July 31, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

FROM: Karen Evans
Administrator, Office of E-Government and Information Technology

SUBJECT: Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, “Implementation of Commonly Accepted Security Configurations for Windows Operating Systems,” which stated: “Agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008.”

As we noted in the June 1, 2007 follow-up policy memorandum M-07-18, “Ensuring New Acquisitions Include Common Security Configurations,” a virtual machine would be established “to provide agencies and information technology providers’ access to Windows XP and VISTA images.” The National Institute of Standards and Technology (NIST), Microsoft, the Department of Defense, and the Department of Homeland Security have now established a website hosting the virtual machine images, which can be found at: http://csrc.nist.gov/fdcc. The website also includes frequently asked questions and other technical information for adopting the Federal Desktop Core Configurations (FDCC).

Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST’s Security Content Automation Protocol (S-CAP) to help evaluate providers’ self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations. Related resources (e.g., group policy objects) are also provided to help facilitate agency adoption of the FDCC.

For additional information about this initiative, please call 1-800-FED-INFO. Additional information about the S-CAP can be found at: http://www.nist.gov/sccp.cfm.

“Your agency can now acquire information technology products that are self-asserted by information technology providers as compliant with the Windows XP & VISTA FDCC, and use NIST’s Security Content Automation Protocol (S-CAP) to help evaluate providers’ self-assertions. Information technology providers must use S-CAP validated tools, as they become available, to certify their products do not alter these configurations, and agencies must use these tools when monitoring use of these configurations.”
## Accomplishing FDCC with SCAP

<table>
<thead>
<tr>
<th>Operations Teams</th>
<th>Product Teams</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>●</td>
<td>●</td>
<td>Test to ensure products do not change the FDCC settings</td>
</tr>
<tr>
<td>●</td>
<td></td>
<td>Assess new implementations for FDCC compliance</td>
</tr>
<tr>
<td>●</td>
<td></td>
<td>Monitor previous implementations for FDCC compliance</td>
</tr>
<tr>
<td>●</td>
<td>●</td>
<td>Generate FDCC compliance and deviation reports</td>
</tr>
</tbody>
</table>

Quote from OMB Memo *Establishment of Windows XP and VISTA Virtual Machine and Procedures for Adopting the Federal Desktop Core Configurations*

“**Information technology providers** must use S-CAP validated tools, as they become available, to **certify their products** do not alter these configurations, and **agencies** must use these tools **when monitoring** use of these configurations. “
The Relationship Between FDCC and SCAP Product Compliance

SCAP Product

Self Asserts
SCAP Compliance

NVLAP
Test Effort

Federal Agency

Product Vendor

Self Asserts
FDCC Compliance

Federal Agency

FDCC Virtual Machine Image

SCAP Compliant Product

SCAP Compliant Product

Compliant with M-07-18? Implement Product?
Federal Desktop Core Configuration (FDCC)

- In support of the OMB Memoranda
- Download the FDCC documentation, group policy objects, Microsoft virtual hard disks, and security content automation protocol (SCAP) content - 2007-07-31

In Support of the OMB Memoranda

Under the direction of OMB and in collaboration with DHS, DISA, NSA, USAF, and Microsoft, NIST has provided the following resources to help agencies test, implement, and deploy the Microsoft Windows XP and Vista Federal Desktop Core Configuration (FDCC) baseline.

- Technical FAQs for FDCC baseline
- FDCC draft documentation, group policy objects (GPOs), Microsoft virtual hard disks (VHDs), and security content automation protocol (SCAP) content

The VHDs and GPOs should only be used for testing purposes and should not be deployed in an operational environment without extensive testing.

Comments and questions may be addressed to fdcc@nist.gov.
Frequently Asked Questions

Technical FAQs

This frequently asked questions (FAQ) document addresses subjects associated with the March 2007 OMB-mandated Federal Desktop Core Configuration (FDCC). Topics include the FDCC, laboratory testing of the FDCC, agency testing of the FDCC, use of the SCAP to evaluate computers for FDCC compliance, deploying the FDCC, and reporting deviations to the FDCC. This FAQ should be considered in addition to the Managing Security Risks Using Common Configurations FAQ.

1. What is the Federal Desktop Core Configuration (FDCC)?
The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC is an operating system software package that includes a Federal Desktop Core Configuration 2007 memorandum from a corresponding member of the Chief Information Officer Council.

2. What operating system is used? Currently, FDCC supports Windows XP (SP 2) and Microsoft Vista.

3. Where can I obtain systems other than those mandated by the Federal Desktop Core Configuration? In general, NIST suggests (SP) guide if one exists. Federal agencies that do not have a guide that can be used in their environment or do not use Federal systems should not be deployed.

4. How was the FDCC derived? Microsoft Office editions are not always included. Some systems may be included in the Federal Desktop Core Configuration. The FDCC lab is never included in the OMB-FCC or OMB-CSP.

5. What are Virtual PCs (VPC)?
Virtual PC (VPC) is a Microsoft product that allows users to run a virtual instance of an operating system (VHD) on their computer. Virtual machines can be installed on a machine with a VPC engine. They can be used with both the VPC environment and VPC-VD HDD.

6. Why are VHDs better than images?
VHDs are very useful tools. They can be installed in an operating system, and once they have been installed, they can be used with both the VPC environment and VPC-VD HDD.

7. Where are VHDs used? VHDs can be used in both the VPC environment and VPC-VD HDD.

8. Security Content Automation Protocol (SCAP)
SCAP is a framework for defining security content, automation, and compliance. It includes two main components: SCAP and the Security Content Automation Protocol (SCAP).

9. What is SCAP?
SCAP is a suite of technologies and tools for automating security content distribution and management. It includes a suite of technologies and tools for automating security content distribution and management.

10. What is SCAP?
SCAP is a suite of technologies and tools for automating security content distribution and management. It includes a suite of technologies and tools for automating security content distribution and management.

11. What is the purpose of the recent NIST test effort?
The purpose of the most recent NIST test effort was to support OMB, DISA, Microsoft, and other organizations in deploying the FDCC. The test effort was designed to verify the FDCC-compliant configuration and to determine if certain security configurations are valid.

12. Why are VHDs better than images?
VHDs are very useful tools. They can be installed in an operating system, and once they have been installed, they can be used with both the VPC environment and VPC-VD HDD.
Federal Desktop Core Configuration (FDCC)

Download Packages

Please read the Download FAQ

Documentation:
- FDCC Documentation Release 1.0 - Draft [xls, 100K]
- SHA-1 Digest: 2CB8B444394B73 E69E4F11758978 09A1232588A0
- SHA-256 Digest: D6ECEF63F4D2FA 4A8B28A79D1527 768BDF5ACCC875 97249684C4C3 E203C267

GPOs:
- FDCC GPO Release 1.0 - Draft [zip, ~3 MB]
- SHA-1 Digest: B46C5140FABD312F A331C149FA0A04D 2D15215FC
- SHA-256 Digest: 6B20B9721E068 170AD7CEB83BC7 0045803F6A00A 8C97A60A194C13 CEFCD5A5

VHD Files:
- Windows XP FDCC VHD Release 1.0 - (Click to download) - Draft [zip, ~18GB]
- SHA-1 Digest: E50G4F3E49020D 935FA0481B3AFA7 E72C75203249
- SHA-256 Digest: 1F20C16B99CF30 B5187B4A93CDB07B A623C10F0F41D 88E87B8EC8D88C D76B85BE
- Note: Windows Vista FDCC VHD Release 1.0 - (Click to download) - Draft [zip, ~45GB]
- Windows Vista SP2
- Internet Explorer 7.0
- Windows Vista SP2

SCAP Content:
- FDCC SCAP Content
- Windows XP SP2
- Internet Explorer 7.0
- Windows Vista SP2

The preceding files are intended for use with "SCAP FDCC scanning capable" tools.
# FDCC Security Settings

<table>
<thead>
<tr>
<th>Policy Path</th>
<th>Policy Setting Name</th>
<th>FDCC Windows Vista</th>
<th>FDCC Windows XP</th>
<th>CCE Reference</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Enforce password history</td>
<td>24 passwords remembered</td>
<td>25 passwords remembered</td>
<td>CCE-68</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Maximum password age</td>
<td>60 days</td>
<td>60 days</td>
<td>CCE-871</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Minimum password age</td>
<td>1 day</td>
<td>1 day</td>
<td>CCE-324</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Minimum password length</td>
<td>12 characters</td>
<td>12 characters</td>
<td>CCE-160</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Password must meet complexity requirement</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CCE-633</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy</td>
<td>Store passwords using reversible encryption for all users in the domain</td>
<td>Disabled</td>
<td>Disabled</td>
<td>CCE-479</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
<td>Account lockout duration</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>CCE-764</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
<td>Account lockout threshold</td>
<td>5 invalid logon attempts</td>
<td>5 invalid logon attempts</td>
<td>CCE-668</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
<td>Reset lockout counter after</td>
<td>15 minutes</td>
<td>15 minutes</td>
<td>CCE-733</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy</td>
<td>Enforce user logon restrictions</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CCE-227</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy</td>
<td>Maximum lifetime for service ticket</td>
<td>600 minutes</td>
<td>600 minutes</td>
<td>CCE-6</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy</td>
<td>Maximum lifetime for user ticket</td>
<td>10 hours</td>
<td>10 hours</td>
<td>CCE-37</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy</td>
<td>Maximum lifetime for user ticket renewal</td>
<td>7 days</td>
<td>7 days</td>
<td>CCE-33</td>
<td></td>
</tr>
</tbody>
</table>
# FDCC Security Settings

<table>
<thead>
<tr>
<th>Policy Path</th>
<th>Policy Setting Name</th>
<th>FDCC Windows Vista</th>
<th>FDCC Windows XP</th>
<th>CCE Reference</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer Configuration\Administrative Templates\Network\Link-Layer Topology Discovery</td>
<td>Turn on Mapper I/O (LLTDIO) driver</td>
<td>Disabled</td>
<td>(Not Applicable)</td>
<td>CDE-947</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network\Link-Layer Topology Discovery</td>
<td>Turn on Responder (RSPNDR) driver</td>
<td>Disabled</td>
<td>(Not Applicable)</td>
<td>CDE-1134</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services</td>
<td>Turn Off Microsoft Peer-to-Peer Networking Services</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CDE-86</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Prohibit installation and configuration of Network Bridge on your DNS domain network</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CDE-896</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Prohibit use of Internet Connection Firewall on your DNS domain network</td>
<td>Enabled</td>
<td>Enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Prohibit use of Internet Connection Sharing on your DNS domain network</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CDE-572</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Windows Firewall: Allow file and printer sharing exception</td>
<td>(Not Applicable)</td>
<td>Disabled</td>
<td>CDE-555</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Windows Firewall: Allow ICMP exceptions</td>
<td>(Not Applicable)</td>
<td>Enabled; Allow inbound echo requests</td>
<td>CDE-277</td>
<td></td>
</tr>
<tr>
<td>Computer Configuration\Administrative Templates\Network Network Connections</td>
<td>Windows Firewall: Allow local port exceptions</td>
<td>(Not Applicable)</td>
<td>Disabled</td>
<td>CDE-370</td>
<td></td>
</tr>
</tbody>
</table>
Group Policy Objects (GPOs)
GPOs Test Environment

Windows Server 2003
- AD/DNS -
- GPOs -

Windows Vista Client

Windows XP Client

FDCC
FDCC GPOs

Group Policy Management Console – gpmc.msc

Group Policy Object Editor – gpedit.msc
Download FAQs

1. I am having trouble downloading the VHD files with Microsoft Internet Explorer. How can I download the VHD files?
   There are known file size limitations when downloading via Internet Explorer (IE) 6 and 7. More specifically, IE 6 has a 2 GB file size limit, and IE 7 has a 4 GB file size limit. At present, no update is available for IE. However, other browsers and utilities have been used to successfully download the VHD files. Mozilla Firefox, Opera Web Browser, Curl, and GNU wget have all been confirmed as supporting download of the VHD files.

2. Does NIST intend to have HTTP mirror or FTP alternate download sites available?
   NIST is currently evaluating both HTTP mirror and FTP as additional mechanisms to download the VHD files. Additional and alternate sites will be linked to the download site as they become available.

**NTFS Disk Space Requirement:**
- Vista: 4.5 GB + 10 GB + Swap
- XP: 1.8 GB + 3.5 GB + Swap

<table>
<thead>
<tr>
<th>Name</th>
<th>Size</th>
<th>Date Modified</th>
<th>Type</th>
<th>Tags</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDCC Vista Q3 2007 Hard Disk.vhd</td>
<td>10,422,899 KB</td>
<td>7/30/2007 5:21 PM</td>
<td>Virtual Machine Hard Drive Image</td>
<td></td>
</tr>
<tr>
<td>FDCC Vista Q3 2007.vmc</td>
<td>13 KB</td>
<td>7/30/2007 5:45 PM</td>
<td>Virtual Machine Settings File</td>
<td></td>
</tr>
<tr>
<td>FDCC XP Q3 2007 Hard Disk.vhd</td>
<td>3,385,006 KB</td>
<td>7/31/2007 10:00 AM</td>
<td>Virtual Machine Hard Drive Image</td>
<td></td>
</tr>
<tr>
<td>FDCC XP Q3 2007.vmc</td>
<td>13 KB</td>
<td>7/31/2007 10:00 AM</td>
<td>Virtual Machine Settings File</td>
<td></td>
</tr>
</tbody>
</table>
Vista FDCC VPC

1. Microsoft Virtual PC 2007
2. fdcc_admin
3. P@ssw0rd123456
### SCAP Content

#### http://nvd.nist.gov/scapchecklists.cfm

<table>
<thead>
<tr>
<th>Microsoft Windows Vista</th>
<th>SCAP-WinVista.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest</th>
<th>![secure-elements-image]</th>
<th>![ThreatGuard-image]</th>
<th>Includes a Federal Desktop Core Configuration profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows XP Professional</td>
<td>SCAP-WinXPPro.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
<td>![secure-elements-image]</td>
<td>![ThreatGuard-image]</td>
<td>Includes a Federal Desktop Core Configuration profile. The FISMA compliance policies are complete. The DISA policies are substantial but still under development by Mitre.</td>
</tr>
<tr>
<td>Microsoft Windows Vista Firewall</td>
<td>SCAP-WinVistaFirewall.zip (v0.12) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
<td>![secure-elements-image]</td>
<td>![ThreatGuard-image]</td>
<td>Patches are located in the OS's zip files. Includes a Federal Desktop Core Configuration profile</td>
</tr>
<tr>
<td>Microsoft Windows XP Firewall</td>
<td>SCAP-WinXPFirewall.zip (v0.18) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
<td>![secure-elements-image]</td>
<td>![ThreatGuard-image]</td>
<td>Patches are located in the OS's zip files. Includes a Federal Desktop Core Configuration profile</td>
</tr>
<tr>
<td>Microsoft Internet Explorer Version 7.0</td>
<td>SCAP-IE7.zip (v0.35) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
<td>![secure-elements-image]</td>
<td>![ThreatGuard-image]</td>
<td>Includes a Federal Desktop Core Configuration profile</td>
</tr>
</tbody>
</table>

**File List**

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCAP-WinVista-CPE.xml</td>
<td>7/27/2007 7:17 PM</td>
<td>XML File</td>
<td>6 KB</td>
</tr>
<tr>
<td>SCAP-WinVista-OVAL-v90.xml</td>
<td>7/30/2007 9:00 AM</td>
<td>XML File</td>
<td>1,222 KB</td>
</tr>
<tr>
<td>SCAP-WinVista-Patches.xml</td>
<td>7/18/2007 12:12 PM</td>
<td>XML File</td>
<td>104 KB</td>
</tr>
<tr>
<td>SCAP-WinVista-xccdf.xml</td>
<td>7/30/2007 7:03 PM</td>
<td>XML File</td>
<td>765 KB</td>
</tr>
</tbody>
</table>
Verify and Test
More Information

NIST FDCC Questions: fdcc@nist.gov
NIST FDCC Web Site: http://fdcc.nist.gov
- FDCC SCAP Checklists
- FDCC Settings
- Virtual Machine Images
- Group Policy Objects

National Checklist Program: http://checklists.nist.gov
- SCAP Checklists
- SCAP Capable Products
- SCAP Events

NIST SCAP Mailing Lists: Scap-update@nist.gov
Scap-dev@nist.gov
Scap-content@nist.gov
Contact Information

Policy Questions
Dan Costello – OMB
Daniel_J._Costello@omb.eop.gov

ISAP NIST Project Lead
Steve Quinn
(301) 975-6967
stephen.quinn@nist.gov

NVD Project Lead
Peter Mell
(301) 975-5572
mell@nist.gov

Senior Information Security Researchers and Technical Support
Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

Murugiah Souppaya
(301) 975-4758
murugiah.souppaya@nist.gov

Matt Barrett
(301) 975-3390
matthew.barrett@nist.gov

Information and Feedback
Web: http://nvd.nist.gov/scap
Comments: scap-update@nist.gov

NIST FDCC Team Members
High Impact Settings

What 800 Pound Gorilla?

- Operate the system as a **standard user**
- Accounts: **Administrator** account status - Disabled
- **Wireless Service** - Disabled
- Maximum **password age** – 60 days
- Minimum **password length** – 12 characters
- Microsoft network client: **Digitally sign communications (always)** – Enabled
- Network security: LAN Manager authentication level - **Send NTLMv2 Response only**. Refuse LM and NTLM
- System cryptography: Use **FIPS compliant** algorithms for encryption, hashing, and signing – Enabled
- **Windows Firewall** – Enabled
- **Signed Drivers** – XP only
Common Mailing List Questions

- How does FDCC relate to FISMA compliance and SP800-53?
- How do I report compliance and exceptions? To whom do I report that information? Any special format?
- Where can I find a centralized list of FDCC compliant applications?
- Does 100% pass on SCAP-based scans mean I am 100% FDCC compliant?
- We have implemented wireless within our enterprise. Do I really need to disable wireless? What if I am using a third-party wireless client?
- Is FDCC applicable to:
  - Windows XP and Vista when used as a server?
  - logically or physical separated desktops and laptops?
  - developer or test desktops and laptops?
  - contractor computers?
  - special purpose (e.g., process control) computers?
- What about FDCC for UNIX, Macintosh, applications, etc?
Questions

National Institute of Standards & Technology
Information Technology Laboratory
Computer Security Division
Current State of Information Security
FISMA Compliance Model

30,000 FT

FISMA Legislation
High Level, Generalized, Information Security Requirements

15,000 FT

Federal Information Processing Standards
FIPS 199: Information System Security Categorization
FIPS 200: Minimum Information Security Requirements

5,000 FT

Management-level Security Controls

Technical-level Security Controls

Operational-level Security Controls

Hands On

Information System Security Configuration Settings
NIST, NSA, DISA, Vendors, Third Parties (e.g., CIS) Checklists and Implementation Guidance
Current State: Compliance and Configuration Management

Finite Set of Possible Known IT Risk Controls & Application Configuration Options

Agency Tailoring
Mgmt, Operational, Technical Risk Controls

Millions of settings to manage

Configuration Management

Supplemental
**Current State Summary - Compliance**

*A Study in Cause and Effect*

**Governance Bodies**
Recognize the need to improve security and mandate it in an increasing number of laws, directives, and policies

**Standards Bodies**
Try to keep pace with an increasing number of mandates by generating more frameworks and guidelines

**Product Teams**
Based on the increasing number of mandates, see the need for automation, many seek to enable it through proprietary methods

**Service Providers**
Based on the increasing number of mandates, see the need for automation and have responded by 1) learning a wide variety of both open and proprietary technologies and 2) implementing point solutions

**Operations Teams**
Lacking true automation, 1) have become overwhelmed by an increasing number of mandates, frameworks, and guidelines and 2) are spending a considerable amount of resources trying to keep pace
**Current State: Vulnerability Trends**

- Decreased timeline in exploit development coupled with a decreased patch development timeline (highly variable across vendors)
- Increased prevalence of zero day exploits
- Three of the SANS Top 20 Internet Security Attack Targets 2006 were categorized as “configuration weaknesses.” Many of the remaining 17 can be partially mitigated via proper configuration.
Current State: Vulnerability Management Industry

- Product functionality is becoming more hearty as vendors acknowledge connections between security operations and a wide variety of IT systems (e.g., asset management, change/configuration management).
- Some vendors understand the value of bringing together vulnerability management data across multiple vendors.
- Vendors driving differentiation through:
  - enumeration,
  - evaluation,
  - content,
  - measurement, and
  - reporting

Hinders information sharing and automation
Reduces reproducibility across vendors
Drives broad differences in prioritization and remediation
Enabling Network Centric Operations

A Wish List

Goal 1. Assured DoD mission execution in the face of cyber attack, or Goal 1. Dependability of the information and information infrastructure in the face of cyber attack

*Richard Hale, 2007 Security Automation Conference*

- Push button understanding of likely exposure to vulnerability/attack
- Push button understanding of actual vulnerability
- Ability to automatically aggregate vulnerability data from tools of varied manufacture
- Ability to implement security configurations and remediate vulnerability in a controlled yet automated way, including SSLF environments
- Ability to dynamically build trust relationships and join computer systems with mission partners
- Reduce effort and expense of documenting system vulnerability and compliance status (e.g., C&A)
- Reduce effort and expense of demonstrating compliance with various mandates
Supplemental – SCAP Platform Evaluation Tutorial
Before

After

Error Report

Problem
Air Pressure Loss

Impact
Car Will Not Start (9/10)

Diagnosis Accuracy:
All Sensors Reporting

Diagnosis:
Replace Gas Cap

Expected Cost:
$25.00
XCCDF - eXtensible Car Care Description Format

<Car>
  <Description>
    <Year> 1997 </Year>
    <Make> Ford </Make>
    <Model> Contour </Model>
  </Description>
  <Maintenance>
    <Check1> Gas Cap = On </Check1>
    <Check2> Oil Level = Full </Check2>
  </Maintenance>
</Car>

OVAL – Open Vehicle Assessment Language

<Checks>
  <Check1>
    <Location> Side of Car </Location>
    <Procedure> Turn </Procedure>
  </Check1>
  <Check2>
    <Location> Hood </Location>
    <Procedure> ... </Procedure>
  </Check2>
</Checks>

Error Report

Problem: Air Pressure Loss
Diagnosis Accuracy: All Sensors Reporting
Diagnosis: Replace Gas Cap
Expected Cost: $25.00
SCAP Content Made Simple

XCCDF - eXtensible Checklist Configuration Description Format

<Document ID> NIST SP 800-68
<Date> 04/22/06 </Date>
-Version> 1 </Version>
-Revision> 2 </Revision>
<Platform> Windows XP </>
<Check1> Password >= 8 </>
<Check2> Win XP Vuln </>
</Maintenance>
</Description>
</Car>

OVAL – Open Vulnerability Assessment Language

<Checks>
<Check1>
<Registry Check> ... <>
<Value> 8 </Value>
</Check1>
<Check2>
<File Version> ... <>
<Value> 1.0.12.4 </Value>
</Check2>
</Checks>

CPE
CCE
CVE

Standardized Checklist

Standardized Test Procedures

Standardized Measurement and Reporting

XCCDF

CVSS

NIST
Application to Automated Compliance
The Connected Path

800-53 Security Control

800-68 Security Guidance

ISAP Produced Security Guidance in XML Format

Result

API Call

COTS Tool Ingest
Application to Automated Compliance

The Connected Path

800-53 Security Control
DoD IA Control

AC-7 Unsuccessful Login Attempts

800-68 Security Guidance
DISA STIG/Checklist
NSA Guide

AC-7: Account Lockout Duration
AC-7: Account Lockout Threshold

ISAP Produced Security Guidance in XML Format

```
<registry_test id="wrt-9999"
  comment=""Account Lockout Duration Set to 5"" check=""at least 5">

  <object>
    <hive>HKEY_LOCAL_MACHINE</hive>
    <key>Software\Microsoft\Windows</key>
    <name>AccountLockoutDuration</name>
  </object>

  <data operation=""AND">
    <value operator=""greater than">5</value>
  </data>

</registry_test>
```

Result

API Call

```
lpHKey = "HKEY_LOCAL_MACHINE"
Path = "Software\Microsoft\Windows\"
Value = "5"
sKey = "AccountLockoutDuration"
Op = ">"

RegQueryValue (lpHKey, path, value, sKey, Value, Op);
If (Op == ‘>’ )
  if ((sKey < Value )
      return (1); else
    return (0);
```

COTS Tool Ingest
Supplemental – SCAP Value Reference
## SCAP Value

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standardizes <strong>how</strong> computers communicate vulnerability information –</td>
<td>■ Enables interoperability for products and services of various manufacture</td>
</tr>
<tr>
<td>the protocol</td>
<td></td>
</tr>
<tr>
<td>Standardizes <strong>what</strong> vulnerability information computers communicate –</td>
<td>■ Enables repeatability across products and services of various manufacture</td>
</tr>
<tr>
<td>the content</td>
<td>■ Reduces content-based variance in operational decisions and actions</td>
</tr>
<tr>
<td>Based on open standards</td>
<td>■ Harnesses the collective brain power of the masses for creation and evolution</td>
</tr>
<tr>
<td>Uses configuration and asset management standards</td>
<td>■ Adapts to a wide array of use cases</td>
</tr>
<tr>
<td>Applicable to many different Risk Management Frameworks – Assess, Monitor,</td>
<td>■ Mobilizes asset inventory and configuration information for use in vulnerability and compliance management</td>
</tr>
<tr>
<td>Implement</td>
<td></td>
</tr>
<tr>
<td>Detailed traceability to multiple security mandates and guidelines</td>
<td>■ Automates portions of compliance demonstration and reporting</td>
</tr>
<tr>
<td>Keyed on NIST SP 800-53 security controls</td>
<td>■ Reduces chance of misinterpretation between Inspector General/auditors and operations teams</td>
</tr>
</tbody>
</table>
Supplemental – FAQ for NIST FISMA Documents
Fundamental FISMA Questions

What are the NIST Technical Security Controls?

What are the *Specific* NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST HeCs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?
What are the NIST Technical Security Controls?

What are the *Specific* NIST recommended settings for individual technical controls?

How do I implement the recommended setting for technical controls? Can I use my COTS Product?

Am I compliant to NIST Recs & Can I use my COTS Product?

Will I be audited against the same criteria I used to secure my systems?

SP 800-18
Security Control Documentation

SP 800-30
Security Control Selection

FIPS 200 / SP 800-53

SP 800-53A / SP 800-26 / SP 800-37
Security Control Implementation

SP 800-37
Security Control Monitoring

SP 800-37
System Authorization

NIST