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
• 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

March 22, 2007

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 Karen Evans, Administrator, E-Government and Information Technology at (202)354-1181 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

Content

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
## Security Content Automation Protocol (SCAP)

**Standardizing How We Communicate**

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE</td>
<td>Common Vulnerability Enumeration</td>
</tr>
<tr>
<td>CCE</td>
<td>Common Configuration Enumeration</td>
</tr>
<tr>
<td>CPE</td>
<td>Common Platform Enumeration</td>
</tr>
<tr>
<td>XCCDF</td>
<td>eXtensible Checklist Configuration Description Format</td>
</tr>
<tr>
<td>OVAL</td>
<td>Open Vulnerability and Assessment Language</td>
</tr>
<tr>
<td>CVSS</td>
<td>Common Vulnerability Scoring System</td>
</tr>
</tbody>
</table>

### Standards and Organizations

- **CVE**: Common Vulnerability Enumeration
- **CCE**: Common Configuration Enumeration
- **CPE**: Common Platform Enumeration
- **XCCDF**: eXtensible Checklist Configuration Description Format
- **OVAL**: Open Vulnerability and Assessment Language
- **CVSS**: Common Vulnerability Scoring System

- MITRE
- NIST
- Cisco, Qualys, Symantec, Carnegie Mellon University
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

<table>
<thead>
<tr>
<th>Checklist</th>
<th>XCCDF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>CPE</td>
</tr>
<tr>
<td>Misconfiguration</td>
<td>CCE</td>
</tr>
<tr>
<td>General Impact</td>
<td>CVSS</td>
</tr>
<tr>
<td>Software Flaw</td>
<td>CVE</td>
</tr>
<tr>
<td>General Impact</td>
<td>CVSS</td>
</tr>
</tbody>
</table>

Test Procedures: OVAL

Patches: OVAL

Specific Impact CVSS Results

COTS/GOTS Tools
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_ 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>

Keyed on SP800-53 Security Controls

Traceability to Mandates

Traceability to Guidelines

Rationale for security configuration
Federal Risk Management Framework

**Starting Point**
- FIPS 199 / SP 800-60
- FIPS 200 / SP 800-53

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

**Select Security Controls**
- Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

**Supplement Security Controls**
- Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

**Document Security Controls**
- Document in the security plan the security requirements for the information system and the security controls planned or in place

**Implement Security Controls**
- Implement security controls, apply security configuration settings

**Assess Security Controls**
- Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

**Authorize Information System**
- Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

**Monitor Security Controls**
- Continuously track changes to the information system that may affect security controls and reassess control effectiveness

**Select Security Controls**
- SP 800-53 / SP 800-30

**Supplement Security Controls**
- SP 800-53 / SP 800-30

**Document Security Controls**
- SP 800-18

**Implement Security Controls**
- SP 800-70

**Assess Security Controls**
- SP 800-53A

**Authorize Information System**
- SP 800-37

**Monitor Security Controls**
- SP 800-37 / SP 800-53A

**Categorize Information System**
- FIPS 199 / SP 800-60

**Select Security Controls**
- FIPS 200 / SP 800-53

**Document Security Controls**
- FIPS 199 / SP 800-60

**Implement Security Controls**
- FIPS 200 / SP 800-53
### 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></td>
<td><strong>Total Controls</strong></td>
<td><strong>163</strong></td>
<td><strong>100%</strong></td>
<td></td>
</tr>
</tbody>
</table>
Integrating IT and IT Security Through SCAP

Vulnerability Management
- CVE
- CVSS

Asset Management
- CPE

Configuration Management
- CCE

Compliance Management
- XCCDF
- OVAL

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System
The objective is to achieve \textit{visibility} into prospective business/mission partners information security programs \textit{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>Agency</th>
<th>Logo</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHS</td>
<td><img src="image1" alt="DHS Logo" /></td>
</tr>
<tr>
<td>OMB</td>
<td><img src="image2" alt="OMB Logo" /></td>
</tr>
<tr>
<td>NSA</td>
<td><img src="image3" alt="NSA Logo" /></td>
</tr>
<tr>
<td>IC</td>
<td><img src="image4" alt="IC Logo" /></td>
</tr>
<tr>
<td>OSD</td>
<td><img src="image5" alt="OSD Logo" /></td>
</tr>
<tr>
<td>DISA</td>
<td><img src="image6" alt="DISA Logo" /></td>
</tr>
<tr>
<td>DOJ</td>
<td><img src="image7" alt="DOJ Logo" /></td>
</tr>
<tr>
<td>EPA</td>
<td><img src="image8" alt="EPA Logo" /></td>
</tr>
<tr>
<td>Army</td>
<td><img src="image9" alt="Army Logo" /></td>
</tr>
<tr>
<td>NIST</td>
<td><img src="image10" alt="NIST Logo" /></td>
</tr>
<tr>
<td>DOS</td>
<td><img src="image11" alt="DOS Logo" /></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
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.”

“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

Product Vendor

Federal Agency

NVLAP Test Effort

SCAP Compliant Products

FDCC Virtual Machine Image

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

1. What is the Federal Desktop Core Configuration (FDCC)?
   The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration for all desktops, workstations, and servers running Microsoft operating systems. The FDCC is an operating system software configuration that is designed to provide a standard baseline for the secure operation of federal systems. The FDCC is developed by the National Institute of Standards and Technology (NIST) and is based on the NIST Special Publication 800-53, Security and Privacy Controls for Information Technology Systems.

2. What operating system software configuration is used with the FDCC?
   The FDCC is a software configuration that is used with all desktops, workstations, and servers running Microsoft operating systems. The FDCC is designed to provide a standard baseline for the secure operation of federal systems. The FDCC is based on the NIST Special Publication 800-53, Security and Privacy Controls for Information Technology Systems.

3. Where can I obtain a copy of the FDCC?
   The FDCC is available for download from the National Institute of Standards and Technology (NIST) website. The FDCC is available for download in PDF format and can be found on the NIST website under the publications section.

4. Why was the FDCC developed?
   The FDCC was developed to provide a standard baseline for the secure operation of federal systems. The FDCC is designed to provide a secure and consistent operating environment for federal systems.

5. How was the FDCC developed?
   The FDCC was developed by the National Institute of Standards and Technology (NIST) and is based on the NIST Special Publication 800-53, Security and Privacy Controls for Information Technology Systems.

6. Is Microsoft Defender included in the FDCC?
   Yes, Microsoft Defender is included in the FDCC.

7. Can I use the VHD files for testing?
   Yes, VHD files can be used for testing.

8. What are the benefits of using VHD files for testing?
   The benefits of using VHD files for testing include the ability to create a consistent and reproducible testing environment.

9. What are the disadvantages of using VHD files for testing?
   The disadvantages of using VHD files for testing include the time and resources required to create and maintain VHD files.

10. What is SCAP?
    SCAP (Security Content Automation Protocol) is an XML-based standard for describing and automating security content. SCAP is used to provide a standard format for security content, which can be used to automate the process of securing systems.

11. How is SCAP used in the FDCC?
    SCAP is used in the FDCC to automate the process of applying security configurations to systems.

12. What are the benefits of using SCAP in the FDCC?
    The benefits of using SCAP in the FDCC include the ability to automate the process of applying security configurations to systems, which can save time and reduce errors.

13. What is the purpose of the FDCC?
    The purpose of the FDCC is to provide a standard baseline for the secure operation of federal systems. The FDCC is designed to provide a secure and consistent operating environment for federal systems.

14. How is the FDCC implemented?
    The FDCC is implemented by configuring the operating system software to meet the requirements of the FDCC. The FDCC is implemented by following the steps outlined in the FDCC documentation.

15. Who is responsible for implementing the FDCC?
    The responsibility for implementing the FDCC falls on the federal agency that is responsible for operating the system.

16. How do I test the FDCC?
    Testing the FDCC involves verifying that the system meets the requirements of the FDCC. This can be done using automated tools or manual testing.

17. What is the purpose of the FDCC Agency Testing?
    The purpose of the FDCC Agency Testing is to verify that the system meets the requirements of the FDCC. Agency Testing involves testing the system using automated tools or manual testing.

18. What is the purpose of the FDCC Laboratory Testing?
    The purpose of the FDCC Laboratory Testing is to verify that the system meets the requirements of the FDCC. Laboratory Testing involves testing the system using automated tools or manual testing.

19. What is the purpose of the FDCC SCAP testing?
    The purpose of the FDCC SCAP testing is to verify that the system meets the requirements of the FDCC. SCAP testing involves testing the system using automated tools or manual testing.

20. What is the purpose of the FDCC deployment?
    The purpose of the FDCC deployment is to provide a consistent and secure operating environment for federal systems. The FDCC deployment involves configuring the operating system software to meet the requirements of the FDCC.

21. What is the purpose of the FDCC documentation?
    The purpose of the FDCC documentation is to provide guidance on how to implement and test the FDCC. The FDCC documentation is used by federal agencies to implement and test the FDCC.
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\Password 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\Password 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\Password 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\Kerberos 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/Link-Layer Topology Discovery</td>
<td>Turn Off Microsoft Peer-to-Peer Networking Services</td>
<td>Enabled</td>
<td>Enabled</td>
<td>CDE-98</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-396</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-672</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/Domain Profile</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 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 downloading 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
1. Microsoft Virtual PC 2007
2. fdcc_admin
3. P@ssw0rd123456
# SCAP Content

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

<table>
<thead>
<tr>
<th>SCAP Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Windows Vista</strong></td>
<td>SCAP-WinVista.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
</tr>
<tr>
<td><strong>Microsoft Windows XP Professional</strong></td>
<td>SCAP-WinXPPro.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
</tr>
<tr>
<td><strong>Microsoft Windows Vista Firewall</strong></td>
<td>SCAP-WinVistaFirewall.zip (v0.12) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
</tr>
<tr>
<td><strong>Microsoft Windows XP Firewall</strong></td>
<td>SCAP-WinXPFirewall.zip (v0.18) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
</tr>
<tr>
<td><strong>Microsoft Internet Explorer Version 7.0</strong></td>
<td>SCAP-IET.zip (v0.95) released 7/31/2007 SHA1 Digest SHA256 Digest</td>
</tr>
</tbody>
</table>

- Includes a Federal Desktop Core Configuration profile.
- Patches are located in the OSs zip files.
- Secure elements

The NIST National Institute of Standards and Technology and MITRE ThreatGuard logos are also present.

---

[Image: A screenshot of a website with a table and logos related to SCAP content.]
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

National Vulnerability Database

- 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

Agency Guides
NSA Guides
DISA STIGS & Checklists

Enterprise
Mobile
Stand Alone
SSLF

High
Moderate
Low

SP1
SP2
SP 800-53
Title III
DCID6/3
NSA Req
DoD IA Controls
17799/27001

Windows
XP

OS or Application
Version/Role
Major Patch Level
Environment
Impact Rating or MAC/CONF

ISO
Vendor
3rd Party

FISMA
HIPAA
SOX
DCID
COMSEC '97
DoD

Supplemental
Current State Summary - Compliance
A Study in Cause and Effect

**Governing 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
Current and Near-Term Use Cases

**Configuration**
- Organization Guidelines (e.g., STIG)
- National Checklist Program

**Misconfiguration**
- National Vulnerability Database
- Information Feeds
- Vulnerability Alerts (e.g., IAVA)

**Software Flaws**
- XCCDF, CPE, CVE, CCE, OVAL, CVSS

**Decision and Change Control Process**
- Standardized Change List
  - XCCDF
- Standardized Change Procedures
  - OVAL
- Standardized Measurement and Reporting
  - XCCDF
  - CVSS

**Monitor/Assess/Evaluate**
- Risk Decision Report
  - XCCDF
  - CVSS
- Metrics Report
  - XCCDF
  - CVSS

**Implement/Remediate**
- Standardized Test Procedures
  - OVAL
- Standardized Measurement and Reporting
  - CVSS
  - XCCDF

**Organization**
- COTS / GOTS
- NIST
Current Problems
Conceptual Analogy (Continued)

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

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

OVAL – Open Vehicle Assessment Language

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

<Check1>
  <Value> 8 </Value>
</Check1>

<Check2>
  <Value> 1.0.12.4 </Value>
</Check2>

OVAL – Open Vulnerability Assessment Language

<Check1>
  <Value> 8 </Value>
</Check1>

<Check2>
  <Value> 1.0.12.4 </Value>
</Check2>

Standardized Checklist

Standardized Test Procedures

CPE
CCE
CVE

CVSS

XCCDF
security benchmark automation
Application to Automated Compliance

The Connected Path

800-53 Security Control

Result

800-68 Security Guidance

API Call

ISAP Produced Security Guidance in XML Format

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>
```

API Call

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

COTS Tool Ingest

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

Result
Supplemental – SCAP Value Reference
### SCAP Value

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

FIPS 200 / SP 800-53

Security Control Selection

SP 800-53 / FIPS 200 / SP 800-30

Security Control Refinement

SP 800-70

Security Control Implementation

SP 800-37

Security Control Monitoring

SP 800-37

System Authorization

SP 800-53A / SP 800-26 / SP 800-37

Security Control Assessment

Fundamental FISMA Documents