

Federal Desktop Core Configuration Windows Vista Baseline For the Federal Agencies



August 2007
fdcc@nist.gov

National Institute of Standards & Technology
Information Technology Laboratory
Computer Security Division

Outline

- Federal Desktop Core Configuration (FDCC)
- OMB memoranda
- In support of the OMB mandate
 - *NIST technical resources*
 - *Windows Vista FDCC baseline*

OMB Deep Dive Working Group

Acknowledgement

- ◎ DHS
- ◎ DISA
- ◎ NSA
- ◎ NIST
- ◎ Microsoft
- ◎ OMB
- ◎ USAF
- ◎ Vendors

Federal Desktop Core Configuration

FDCC

- ◉ Common core Microsoft Windows configuration driven by OMB
- ◉ Based on the DISA, NSA, NIST, USAF, and Microsoft existing guidelines for securing Windows XP and Vista
- ◉ Leverage USAF Standard Configuration Desktop initiative
 - Deployed and tested across half a million Windows XP systems
- ◉ Include security and other settings
 - Internet Explorer 7

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

OMB Memoranda

OMB Memo M-07-11

Implementation of Commonly Accepted Security Configurations for Windows Operating Systems



DEPUTY DIRECTOR
FOR MANAGEMENT

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 Karen Evans, Administrator, E-Government and Information Technology at (202)395-1181 or at fisma@omb.eop.gov.

OMB Memo M-07-11

Implementation of Commonly Accepted Security Configurations for
Windows Operating Systems

- ⦿ “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 desktops for **Windows XP™**. “
- ⦿ “Agencies with these operating systems and/or plans to upgrade to these operating systems must **adopt these standard security configurations by February 1, 2008.**”

OMB Memo M-07-18

Ensuring New Acquisitions Include Common Security Configurations



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

June 1, 2007

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS
CHIEF ACQUISITION OFFICERS]

FROM: Karen S. Evans *Karen S. Evans*
Administrator
Office of E-Government and Information Technology

Paul A. Denett *Paul A. Denett*
Administrator for Federal Procurement Policy

SUBJECT: Ensuring New Acquisitions Include Common Security 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."

This memorandum provides recommended language for your agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. Your agency may determine other specifications and/or language is necessary:

- a) 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). For the Windows XP settings, see: http://csrc.nist.gov/itsec/guidance_WinXP.html, and for the Windows Vista settings, see: http://csrc.nist.gov/itsec/guidance_vista.html.
- b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
- c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges."

2

A number of concurrent activities will further assist your agency's adoption of common security configurations. 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.

Additionally, Part 39 of the Federal Acquisition Regulation (FAR), which requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, will be revised to incorporate requirements for using common security configurations, as appropriate.

More information on how to access the virtual machine and progress to update the FAR will be forthcoming. The Chief Information Officers Council will facilitate the exchange of best practices and lessons learned, and NIST maintains responses to frequently asked questions at: http://csrc.nist.gov/itsec/guidance_WinXP.html#FAQ and http://csrc.nist.gov/itsec/guidance_vista.html#FAQ. Questions concerning agency adoption of the Windows XP and VISTA configurations can be sent to fisma@omb.eop.gov. If you have any questions about this memorandum, please contact Daniel Costello at 202-395-7857.

OMB Memo M-07-18

Ensuring New Acquisitions Include Common Security Configurations

- “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. “

OMB Memo for 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://nvd.nist.gov/scap.cfm>.

OMB Announcement

OMB Announces Establishment of New Website to Assist Agency Implementation of Secure Configurations



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

FOR IMMEDIATE RELEASE
July 31, 2007
Contact: OMB Communications, 202-395-7254

OMB ANNOUNCES ESTABLISHMENT OF NEW WEBSITE TO ASSIST AGENCY IMPLEMENTATION OF SECURE CONFIGURATIONS

WASHINGTON -- The Office of Management and Budget (OMB) announced today the establishment of a Web site to assist departments and agencies with the implementation of secure configurations to improve the security of their information technology investments.

The new Web site established today hosts "virtual machine images" - tools for the agencies to simulate what will happen when they transition from their current operating environment to the secure Windows XP and VISTA operating systems using these new configurations. Additionally, these images will allow agencies to see what happens to their current applications when operating with the secure operating systems of Windows XP and VISTA. Earlier this year, OMB requested agencies using or planning on upgrading to Windows XP and VISTA to adopt common security configurations. Doing so will improve IT security while reducing operating costs, for example, by managing risk when using file sharing technology. As part of this effort, OMB informed agencies that a new resource -- virtual machine images -- would be established to assist agency planning efforts.

The images contain pre-configured security settings for agencies to use when testing and evaluating their applications to ensure they function effectively and securely when they migrate to these new operating systems. The images were established through a collaborative effort with Microsoft and the National Institute of Standards and Technology (NIST), the Department of Defense, and the Department of Homeland Security.

"This resource facilitates agencies' efforts to implement common security configurations which will boost government's information security, improve system performance, and decrease operating costs," said Karen Evans, Administrator of OMB's Office of E-Government and Information Technology. "We encourage new collaborative efforts, such as this one, with both public and private sector partners to support agency adoption of the Microsoft XP and VISTA configurations."

In addition, NIST's National Checklist Program is working with a number of information technology providers on standardizing security settings for a wide variety of products and environments. NIST maintains over 120 common security configuration guides used by agencies.

Resources

- ◎ OMB Memoranda

<http://www.whitehouse.gov/omb/memoranda/>

- ◎ NIST FAQs about Implementation of Commonly Accepted Security Configurations for Windows Operating Systems Memo

http://checklists.nist.gov/faq-common_security_configurations.html

In Support of the OMB Mandate

Vista Federal Desktop Core Configuration

FDCC Technical Resources

- ◉ NIST FDCC home page
<http://csrc.nist.gov/fdcc>
- ◉ Frequently asked questions
- ◉ Draft security settings documentation for Windows XP and Vista
- ◉ Microsoft Virtual PC virtual hard disks (VHDs)
- ◉ Draft Group policy objects
- ◉ Draft security content automation protocol (SCAP) content

http://csrc.nist.gov/fdcc

Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC

NIST
National Institute of
Standards and Technology

Focus Areas **Publications** **Site Map** **Search**

FDCC

- ◆ [Home](#)
- ◆ [Disclaimer](#)
- ◆ [Contact](#)

NIST Resources

- ◆ [NIST Security Configuration Checklist for IT Products](#)
- ◆ [Security Content Automation Protocol](#)
- ◆ [Guidance for Securing Microsoft Windows Vista](#)
- ◆ [Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist](#)
- ◆ [Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist](#)
- ◆ [NIST Systems Administration Guidance for Windows 2000 Professional](#)
- ◆ [FISMA Implementation Project](#)

Federal Desktop Core Configuration FDCC

- ◆ [In support of the OMB Memoranda](#)
- ◆ [NIST Frequently Asked Questions - FAQs - 2007-07-31](#)
- ◆ [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 an addition to the [Managing Security Risks Using Common Configurations FAQ](#).

Federal Desktop Core Configuration

1. What is the Federal Desktop Core Configuration (FDCC)?

The Federal Desktop Core Configuration (FDCC) is an OMB-mandated security configuration. The FDCC operating system software is the Federal Desktop Core Configuration (FDCC) 2007 memorandum for a corresponding memorandum Chief Information Officer.

2. What operating systems are supported?

Currently, FDCC settings are supported for Windows XP (Service Pack 2) and Microsoft

3. Where can I obtain systems other than Windows XP?

In general, NIST suggests using the Windows Security (SP) guide if one exists. If not available, Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist. Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist. Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist.

4. How was the FDCC developed?

The Windows Vista Federal Desktop Core Configuration Security Guides for Windows Vista Security Guide for Windows Vista, NSA, and NIST. The DISA, NSA, and NIST Windows XP Federal Desktop Core Configuration Security-Limited Functionality DoD customization of Internet Explorer 7.0.

FDCC Laboratory Testing

1. What was the objective of the recent NIST test effort?

In support of OMB and Federal Desktop Core Configuration (FDCC), DISA, Microsoft, and third-party laboratory testing to verify against the written FDCC policy.

2. What version of Microsoft Internet Explorer 7.0 was tested?

Microsoft Internet Explorer 7.0 was tested. While settings for other browsers are not available, Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist. Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist.

3. What if I use a browser other than Internet Explorer 7.0?

While settings for other browsers are not available, Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist. Federal Desktop Core Configuration (checklists.nist.gov) to the Defense Information Systems Agency (DISA) guide that could be used if it does not exist.

4. Were any Microsoft Office applications tested?

Microsoft Office is not installed in GPOs. The Microsoft Office represented in the FDCC document before laboratory testing. Microsoft Office testing after publication of the FDCC document.

5. To comply with the FDCC, what settings should be configured in Microsoft Windows Firewall?

No. The FDCC baseline recommends the Microsoft Windows Firewall system installation. However, the firewall software instead of the Microsoft Windows Firewall system installation.

1. What are Virtual PCs (VPC), and what is the difference between a VPC and a Virtual Hard Disk (VHD)?

Virtual PC (VPC) is a Microsoft product that allows users to run a virtual instance of an operating system. A Virtual Hard Disk (VHD) can utilize the USB ports) in the same way that the VHD appears as a physical hard disk.

2. Why are VHDs being used for testing?

VHDs are very useful for testing because they can be installed on a single operating system, and they can be used for testing purposes of ensuring that the system is not malfunctioned with a single physical hard disk.

3. When will VHDs be published?

According to Microsoft, VHDs will be published at <http://csr.nist.gov/fdcca>.

4. What can be done to ensure compliance with the FDCC?

The FDCC technical policy documentation contains content files.

5. Can I use the VHDs for testing?

FDCC Agency Testing

1. What is SCAP?

NIST recently established a suite of interoperable and automatable security standards known as the Security Content Automation Protocol (SCAP). By virtue of using XML-based standards, SCAP content is machine-readable. Specific host SCAP references are available at <http://nvd.nist.gov>.

2. How are the SCAP tests run?

As part of the testing process, both VHDs and physical systems were able to run the SCAP tests. The settings were pre-determined for testing to determine if new settings were needed.

3. What settings are being tested?

There are a small number of settings at this time. These settings are being tested.

4. Where can I obtain the SCAP content?

FDCC SCAP content is available at <http://nvd.nist.gov>.

Security Content Automation Protocol

FDCC Deployment

1. What are some settings that will impact system functionality that I should test before I deploy the OMB mandated FDCC baseline in an operational environment?

There are a number of settings that will impact system functionality and agencies should test thoroughly before they are deployed in an operational environment.

- Running the system as a standard user - some applications may not work properly because they require administrative access to the operating system and application directories and registry keys.
- Minimum 12 characters password and change every 60 days - this may impact system usability and interoperability with some enterprise single sign-on password management systems.
- Wireless service - the wireless service is disabled and this will prevent the use of Wi-Fi network interfaces that depend on the built-in wireless service.
- FIPS 140-2 setting - impacts browser interoperability with Web sites that do not support the FIPS 140-2 approved algorithms. This can usually be

Settings

Impact System Functionality

- 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

http://csrc.nist.gov/fdcc/download_fdcc.html

Information Technology Laboratory - Computer Security Division
Computer Security Resource Center - CSRC

NIST
National Institute of Standards and Technology

Focus Areas Publications Site Map Search

FDCC

- [Home](#)
- [Disclaimer](#)
- [Contact](#)

NIST Resources

- [NIST Security Configuration Checklist for IT Products](#)
- [Security Content Automation Protocol](#)
- [Guidance for Securing Microsoft Windows Vista](#)
- [Guidance for Securing Microsoft Windows XP Home Edition: A NIST Security Configuration Checklist](#)
- [Guidance for Securing Microsoft Windows XP Systems for IT Professionals: A NIST Security Configuration Checklist](#)
- [NIST Systems Administration Guidance for Windows 2000 Professional](#)
- [FISMA Implementation Project](#)
- [National Vulnerability Database](#)

Federal Desktop Core Configuration FDCC

- DOWNLOAD PAGE -

WARNING NOTICE

Do not attempt to implement any of the settings without first testing them in a non-operational environment. These recommendations should be applied only on Windows XP Professional SP2 and Vista systems and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003. The security policy has been tested on Windows XP Professional SP2 and Vista systems with a Windows 2003 server and will not work on Windows 9X/ME, Windows NT, Windows 2000 or Windows Server 2003.

The draft download packages contain recommended security settings; they are not meant to replace well-structured policy or sound judgment. Furthermore, these recommendations do not address site-specific configuration issues. Care must be taken when implementing these settings to address local operational and policy concerns.

These recommendations were developed at the National Institute of Standards and Technology, which collaborated with DHS, DISA, NSA, USAF, and Microsoft to produce the Windows XP and Vista FDCC baseline. Pursuant to title 17 Section 105 of the States Code, these recommendations are not subject to copyright protection and are in the public domain. NIST assumes no responsibility whatsoever for their use by other parties, and makes no guarantees, expressed or implied, about their quality, reliability, or any other characteristic. We would appreciate acknowledgement if the recommendations are used.

Download Packages

Please read the [Download FAQ](#)

Documentation	GPOs	VHD Files	SCAP Content
<p>2007-07-31 FDCC Documentation Release 1.0 - Draft [xls, 100K]</p> <p>SHA-1 Digest: 2CB88444394B73E69EF41175897809A1232588A0</p> <p>SHA-256 Digest: D6ECF963F4D2FA4AB92BA79D1527768DDF5ACCC875872496DE4C4C23E283CD17</p>	<p>2007-07-31 FDCC GPO Release 1.0 -Draft [zip, ~3 MB]</p> <p>SHA-1 Digest: B46C514BFABD312FA9C1AC149AFA04D2D15215FC</p> <p>SHA-256 Digest: 682B097721E068170AD7CE883BC70045803FE6A00A8C97A60A194C13CEFCDA5C</p>	<p>2007-07-31 Windows XP FDCC VHD Release 1.0 (Click to download) - Draft [zip, ~1.8GB]</p> <p>Note: Internet Explorer 6 and 7 have a download limitation of 2 GB and 4 GB respectively. Other browsers do not appear to have this limitation.</p> <p>SHA-1 Digest: E50E4F3B40920D595FA0481B3AF7E72C76203249</p> <p>SHA-256 Digest: 1F20C16989CF30B5187EA95CD07BA629CF18F0F41D89E87B8EC8DB9CD768858E</p> <p>Windows Vista FDCC VHD Release 1.0 (Click to download) -Draft [zip, ~4.5GB]</p> <p>Note: Internet Explorer 6 and 7 have a download</p>	<p>2007-07-31 FDCC SCAP Content</p> <p>Windows XP SP2</p> <p>Windows XP Firewall</p> <p>Internet Explorer 7.0</p> <p>Windows Vista</p> <p>Windows Vista Firewall</p> <p>The preceding files are intended for use with "SCAP FDCC scanning capable" tools.</p>

FDCC Security Settings

FDCC-Settings-v1-0-0.xls [Compatibility Mode] - Microsoft Excel

	A	B	C	D	E	F
	Policy Path	Policy Setting Name	FDCC Windows Vista	FDCC Windows XP	CCE Reference	Comment
1	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Enforce password history	24 passwords remembered	24 passwords remembered	CCE-60	
2	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Maximum password age	60 days	60 days	CCE-871	
3	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Minimum password age	1 day	1 day	CCE-324	
4	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Minimum password length	12 characters	12 characters	CCE-100	
5	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Password must meet complexity requirement	Enabled	Enabled	CCE-633	
6	Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy	Store passwords using reversible encryption for all users in the domain	Disabled	Disabled	CCE-479	
7	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	Account lockout duration	15 minutes	15 minutes	CCE-754	
8	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	Account lockout threshold	5 invalid logon attempts	5 invalid logon attempts	CCE-658	
9	Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy	Reset lockout counter after	15 minutes	15 minutes	CCE-733	
10	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy	Enforce user logon restrictions	Enabled	Enabled	CCE-227	
11	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy	Maximum lifetime for service ticket	600 minutes	600 minutes	CCE-6	
12	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy	Maximum lifetime for user ticket	10 hours	10 hours	CCE-37	
13	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy	Maximum lifetime for user ticket renewal	7 days	7 days	CCE-33	
14	Computer Configuration\Windows Settings\Security Settings\Account Policies\Kerberos Policy					

Ready Count: 6 100%

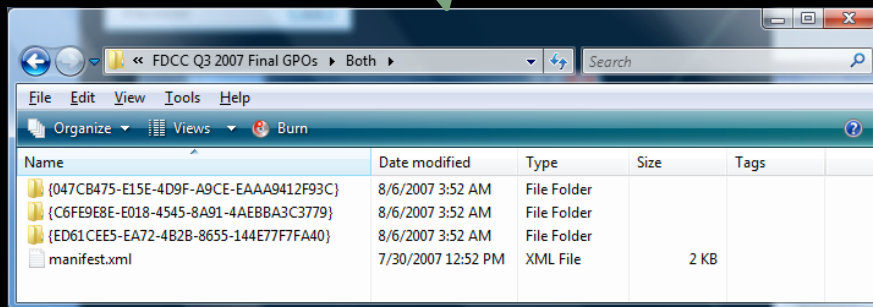
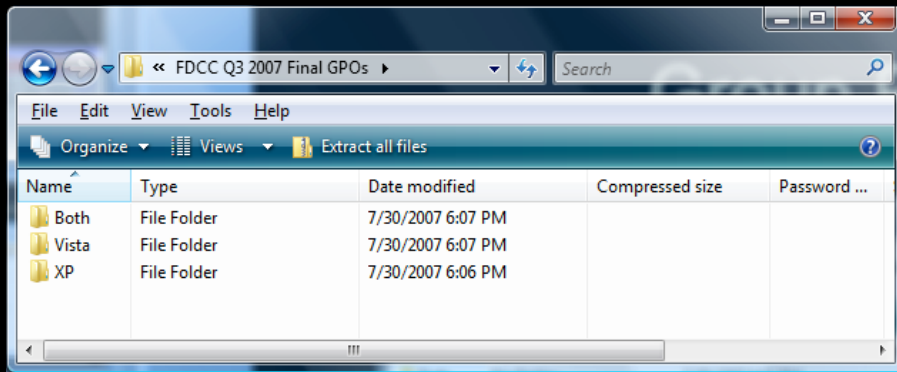
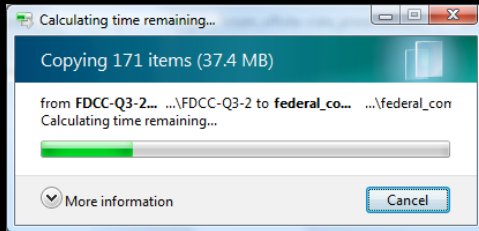
FDCC Other Settings

FDCC-Settings-v1-0-0.xls [Compatibility Mode] - Microsoft Excel

	A	B	C	D	E	F
	Policy Path	Policy Setting Name	FDCC Windows Vista	FDCC Windows XP	CCE Reference	Comment
1	Computer Configuration\Administrative Templates\Network\Link-Layer Topology Discovery	Turn on Mapper I/O (LLTDIO) driver	Disabled	(Not Applicable)	CCE-947	
2	Computer Configuration\Administrative Templates\Network\Link-Layer Topology Discovery	Turn on Responder (RSPNDR) driver	Disabled	(Not Applicable)	CCE-1134	
3	Computer Configuration\Administrative Templates\Network\Microsoft Peer-to-Peer Networking Services	Turn Off Microsoft Peer-to-Peer Networking Services	Enabled	Enabled	CCE-86	
4	Computer Configuration\Administrative Templates\Network\Network Connections	Prohibit installation and configuration of Network Bridge on your DNS domain network	Enabled	Enabled	CCE-896	
5	Computer Configuration\Administrative Templates\Network\Network Connections	Prohibit use of Internet Connection Firewall on your DNS domain network	Enabled	Enabled		
6	Computer Configuration\Administrative Templates\Network\Network Connections	Prohibit use of Internet Connection Sharing on your DNS domain network	Enabled	Enabled	CCE-672	
7	Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow file and printer sharing exception	(Not Applicable)	Disabled	CCE-555	
8	Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow ICMP exceptions	(Not Applicable)	Enabled: Allow inbound echo requests	CCE-277	
9	Computer Configuration\Administrative Templates\Network\Network Connections\Windows Firewall\Domain Profile	Windows Firewall: Allow local port exceptions	(Not Applicable)	Disabled	CCE-370	
10						

Ready Count: 6 100%

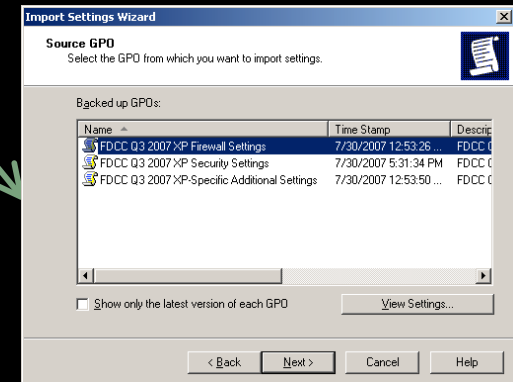
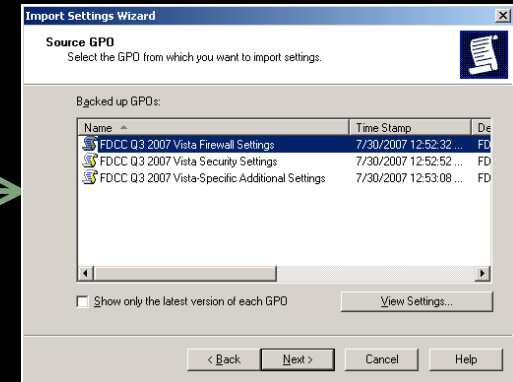
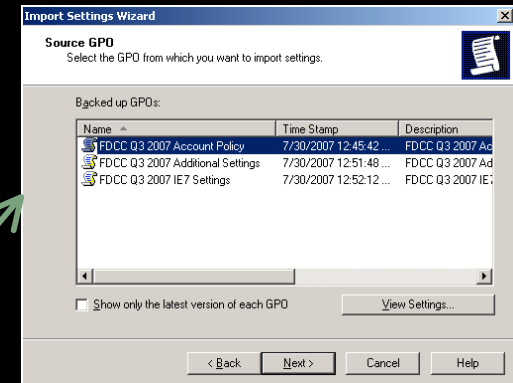
Group Policy Objects (GPOs)



Both

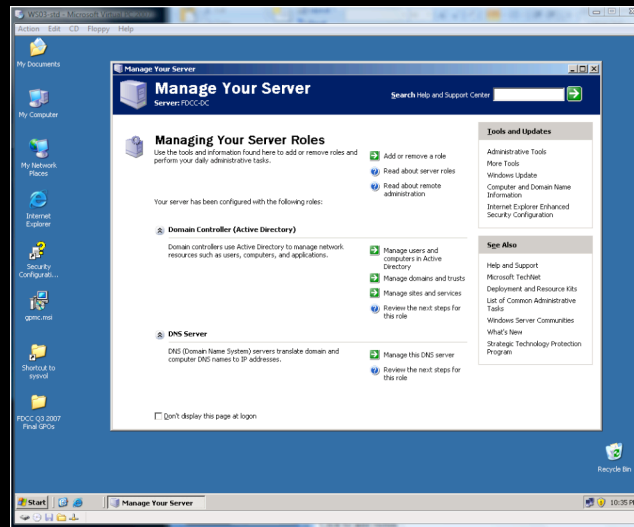
Vista

XP



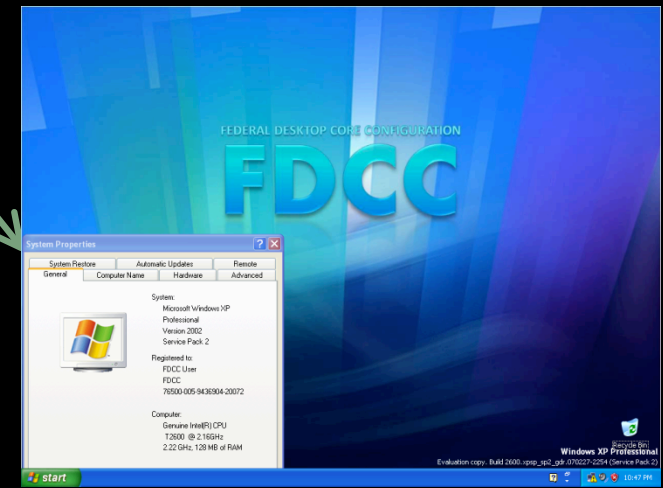
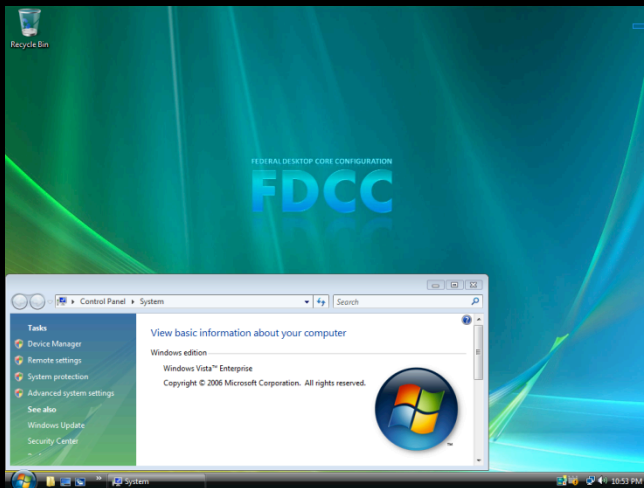
GPOs Test Environment

Windows Server 2003
- AD/DNS -
- GPOs -



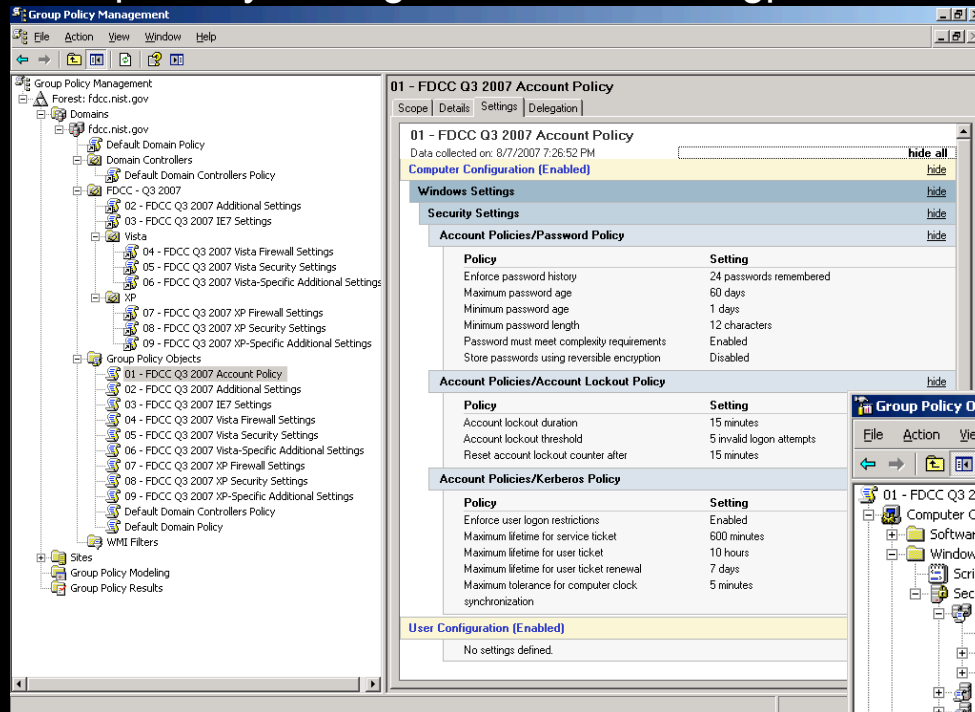
Windows Vista
Client

Windows XP
Client

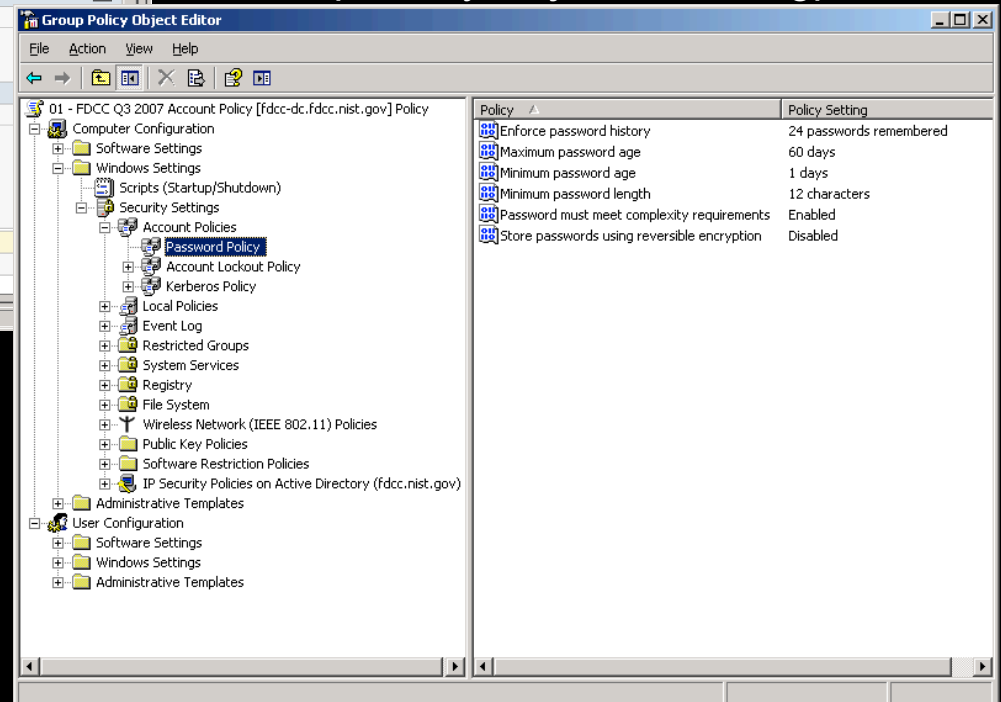


FDCC GPOs

Group Policy Management Console – gpmc.msc



Group Policy Object Editor – gpedit.msc



Download FDCC VHD Files

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

```
Command Prompt
F:\csrc-fdcc>sha256deep.exe FDCC-Uista-Q3-20070730.zip
5c7e4cb6a0db891c747dd054a7e79f69fab5ab51778213b15e56ebee625ee88
FDCC-Uista-Q3-20070730.zip
F:\csrc-fdcc>sha256deep.exe FDCC-XP-Q3-20070731.zip
1f20c16989cf30b5187ea95cd07ba629cf18f0f41d89e87b8ec8db9ed768858e
FDCC-XP-Q3-20070731.zip
F:\csrc-fdcc>_
```

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 2GB file size limit, and IE 7 has a 4GB 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.

25 Minutes and 20 Seconds remaining

Copying 3 items (9.93 GB)

From: FDCC-Vista-Q3-20070730.zip (H:\FDCC-Vista-Q3-20070730.zip)
To: My Virtual Machines (C:\...\My Virtual Machines)

Time remaining: About 25 Minutes and 20 Seconds
Items remaining: 2 (5.74 GB)
Speed: 3.81 MB/sec

[Less information](#)

My Virtual Machines > FDCC Vista Q3 2007

Name	Size	Date modified	Type	Tags
FDCC Vista Q3 2007 Hard Disk.vhd	10,422,899 KB	7/30/2007 5:21 PM	Virtual Machine H...	
FDCC Vista Q3 2007.vmc	13 KB	7/30/2007 5:45 PM	Virtual Machine S...	

1 Hour and 53 Minutes remaining

Copying 3 items (3.41 GB)

From: FDCC-XP-Q3-20070731.zip ...FDCC-XP-Q3-20070731.zip
To: My Virtual Machines (C:\...\My Virtual Machines)

Time remaining: About 1 Hour and 53 Minutes
Items remaining: 2 (3.28 GB)
Speed: 714 KB/sec

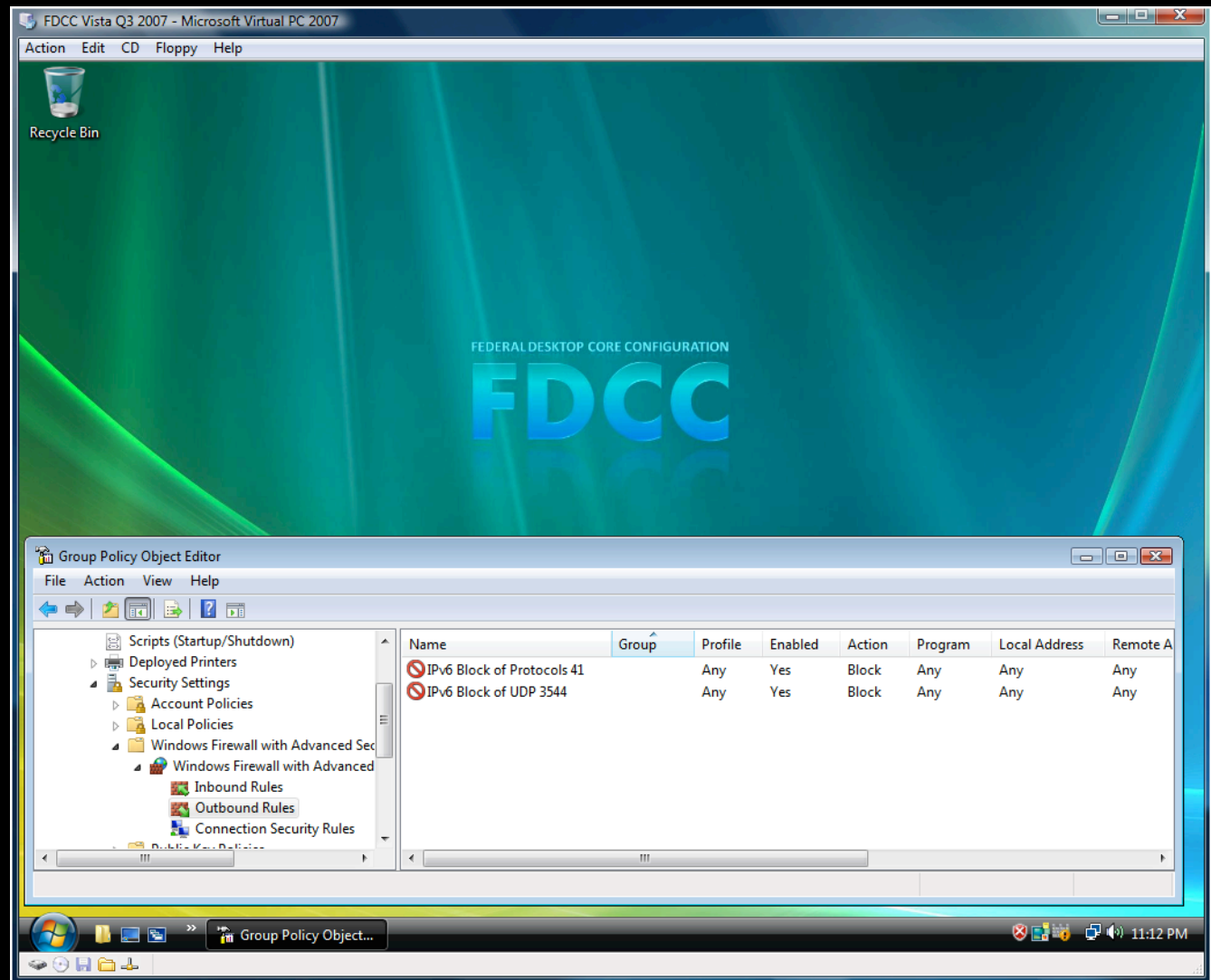
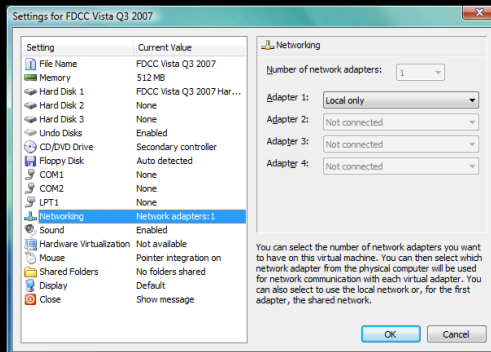
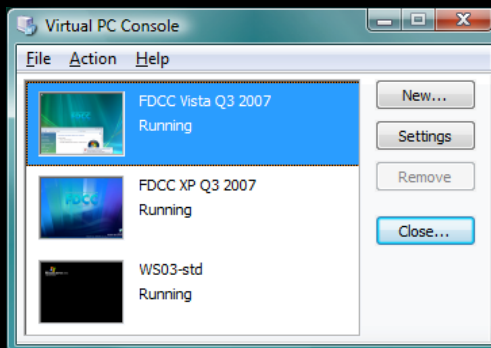
[Less information](#)

My Virtual Machines > FDCC XP Q3 2007

Name	Size	Date modified	Type	Tags
FDCC XP Q3 2007 Hard Disk.vhd	3,585,006 KB	7/31/2007 10:00 AM	Virtual Machine Hard Drive Image	
FDCC XP Q3 2007.vmc	13 KB	7/31/2007 10:00 AM	Virtual Machine Settings File	









Vista FDCC VPC

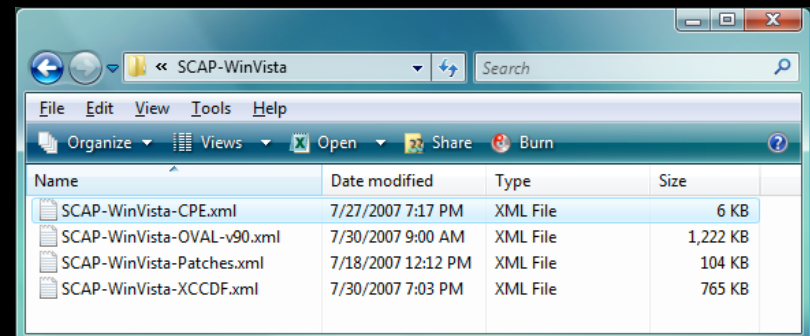
1. Microsoft Virtual PC 2007
2. fdcc_admin
3. P@ssw0rd123456



SCAP Content

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

Microsoft Windows Vista	SCAP-WinVista.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest			Includes a Federal Desktop Core Configuration profile
Microsoft Windows XP Professional	SCAP-WinXPPro.zip (v0.90) released 7/31/2007 SHA1 Digest SHA256 Digest			Includes a Federal Desktop Core Configuration profile. The FISMA compliance policies are complete. The DISA policies are substantial but still under development by Mitre.
Microsoft Windows Vista Firewall	SCAP-WinVistaFirewall.zip (v0.12) released 7/31/2007 SHA1 Digest SHA256 Digest		Patches are located in the OSs zip files.	Includes a Federal Desktop Core Configuration profile
Microsoft Windows XP Firewall	SCAP-WinXPFirewall.zip (v0.18) released 7/31/2007 SHA1 Digest SHA256 Digest		Patches are located in the OSs zip files.	Includes a Federal Desktop Core Configuration profile
Microsoft Internet Explorer Version 7.0	SCAP-IE7.zip (v0.95) released 7/31/2007 SHA1 Digest SHA256 Digest			Includes a Federal Desktop Core Configuration profile



Common Platform Enumeration – CPE
 Open Vulnerability Assessment Language – OVAL
 eXtensible Configuration Checklist Description Format – XCCDF

SCAP Content

CPE

Patches

XCCDF

OVAL

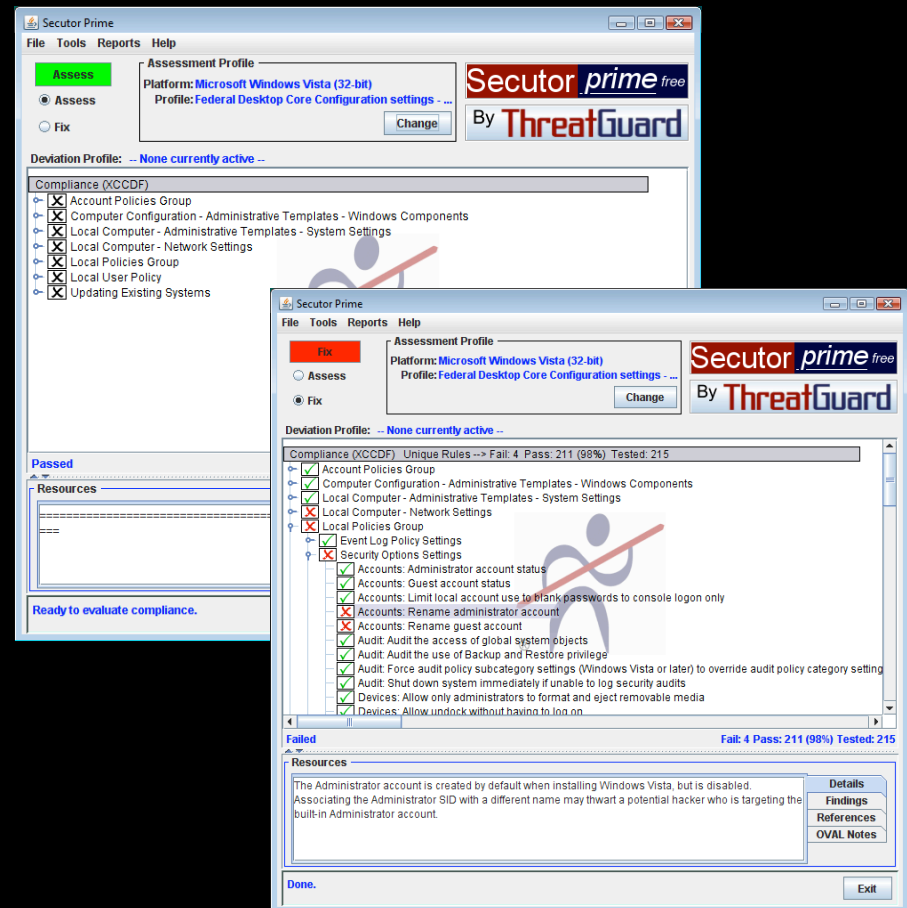
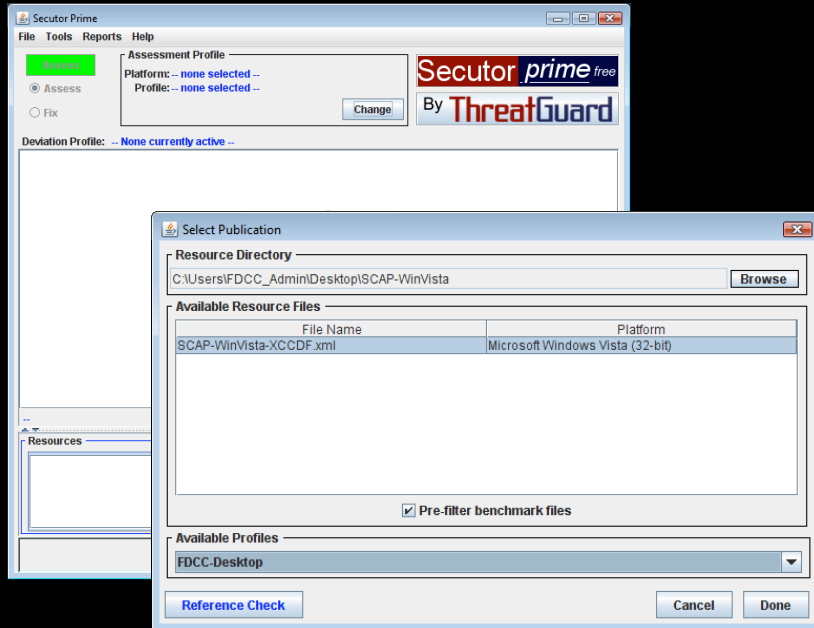
```
<?xml version="1.0" encoding="UTF-8" ?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" xmlns:unix-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix" xmlns:linux-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" xmlns:sol-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#sol" xmlns:iso-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#iso" xmlns:scap-schema="http://oval.mitre.org/XMLSchema/oval-definitions-5#scap-schema" />
<generator>
  <oval:product_name>ThreatGuard, Inc.</oval:product_name>
  <oval:schema_version>5.3</oval:schema_version>
  <oval:timestamp>2007-06-12T07:05:08</oval:timestamp>
</generator>
<definitions>
  <definition id="oval.org.mitre.oval:def:1282" version="1" class="cpe" />
  <metadata>
    <title>Microsoft Windows Vista (32-bit) is installed</title>
    <affected family="windows">
      <platform>Microsoft Windows Vista</platform>
      <affected>
        <description>The operating system installed on this computer is Microsoft Windows Vista</description>
      </affected>
      <oval_repository>
        <submitted date="2007-04-11T11:27:37" />
        <contributor organization="The MITRE Corp" />
      </oval_repository>
    </metadata>
  </definition>
  <reference source="Microsoft" ref_id="http://www.microsoft.com/technet/security/advisory/MS07-017:VulnerabilitiesInGDIControlPanel.aspx" />
  <reference source="CVE" ref_id="CVE-2006-5758" />
  <reference source="CVE" ref_id="CVE-2007-0038" />
  <reference source="CVE" ref_id="CVE-2007-1211" />
  <reference source="CVE" ref_id="CVE-2007-1212" />
  <reference source="CVE" ref_id="CVE-2007-1213" />
  <reference source="CVE" ref_id="CVE-2007-1215" />
  <reference source="Bunzian IT" ref_id="http://www.bunzian.it/2007/05/23/15-05-23-2007-05-23T15:05:23" />
  <reference source="ACCEPTED" />
  <criteria operator="AND">
    <criterion test_ref="oval.org.mitre.oval:tst:99" comment="Microsoft Windows family." />
    <criterion test_ref="oval.org.mitre.oval:tst:192" />
  </criteria>
</definitions>
</oval_definitions>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5" xmlns:oval-def="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" xmlns:unix-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix" xmlns:linux-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" xmlns:sol-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#sol" xmlns:iso-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#iso" xmlns:scap-schema="http://oval.mitre.org/XMLSchema/oval-definitions-5#scap-schema" />
<generator>
  <oval:product_name>ThreatGuard, Inc.</oval:product_name>
  <oval:schema_version>5.3</oval:schema_version>
  <oval:timestamp>2007-07-18T12:12:37</oval:timestamp>
</generator>
<definitions>
  <definition class="patch" id="oval.com.threatguard.msd07-017" version="1" class="patch" />
  <metadata>
    <title>MS07-017: Vulnerabilities in GDI Control Panel</title>
    <affected family="windows">
      <platform>Microsoft Windows Vista</platform>
      <affected>
        <description>Microsoft</description>
      </affected>
      <oval_repository>
        <reference source="Microsoft" ref_id="http://www.microsoft.com/technet/security/advisory/MS07-017:VulnerabilitiesInGDIControlPanel.aspx" />
        <reference source="CVE" ref_id="CVE-2006-5758" />
        <reference source="CVE" ref_id="CVE-2007-0038" />
        <reference source="CVE" ref_id="CVE-2007-1211" />
        <reference source="CVE" ref_id="CVE-2007-1212" />
        <reference source="CVE" ref_id="CVE-2007-1213" />
        <reference source="CVE" ref_id="CVE-2007-1215" />
        <reference source="Bunzian IT" ref_id="http://www.bunzian.it/2007/05/23/15-05-23-2007-05-23T15:05:23" />
      </oval_repository>
    </metadata>
  </definition>
  <profile id="000-53-Low" abstract="true">
    <title>000-53 Low</title>
    <description>This profile selects specific control systems in which all three security objective potential impact value of low. Each control system requires certain controls to be selected</description>
    <select idref="AC-1" selected="1" />
    <select idref="AC-2" selected="1" />
    <select idref="AC-3" selected="1" />
  </profile>
</definitions>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<benchmark xmlns="http://checklists.nist.gov/xccdf/1.1" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:htm="http://www.w3.org/1999/xhtml" />
<title>SCAP: Guidance for Securing Microsoft Windows</title>
<description>This guide has been created to assist in the implementation of the SCAP (Security Content Automation Protocol) for Microsoft Windows Vista</description>
<notice id="Terms-Of-Use" xml:lang="en">This document is the property of the National Institute of Standards and Technology (NIST). It is made available for use under the terms of the NIST Copyright License (http://www.nist.gov/public_affairs/discuss/announce.htm#copyright). This benchmark applies to Microsoft Windows Vista</notice>
<reference href="http://www.microsoft.com/technet/security/guide/default.mspx" />
<dc:title>Guidance for Securing Microsoft Windows</dc:title>
<dc:creator>Sudhir Gandhe</dc:creator>
<dc:creator>Dragos Prisaca</dc:creator>
<dc:publisher>Secure Elements, Inc.</dc:publisher>
<dc:identifier>http://www.secure-elements.com/publications/SCAP-Guidance-for-Securing-Microsoft-Windows-Vista</dc:identifier>
<reference href="http://www.microsoft.com/technet/security/guide/default.mspx" />
<reference href="http://www.secure-elements.com/publications/SCAP-Guidance-for-Securing-Microsoft-Windows-Vista" />
<cpe:cpe-list>
  <cpe:cpe-item name="cpe:/microsoft:windows" />
  <cpe:cpe-item name="cpe:/microsoft:windows:vista" />
  <cpe:cpe-item name="cpe:/microsoft:windows:vista:32-bit" />
  <cpe:cpe-item name="cpe:/microsoft:windows:vista:32-bit:en" />
  <cpe:cpe-item name="cpe:/microsoft:windows:vista:32-bit:en:0.90" />
  <cpe:cpe-item name="cpe:/microsoft:windows:vista:32-bit:en:0.90:2007-07-30-draft" />
</cpe:cpe-list>
<model system="urn:xccdf:scoring:default" />
<model system="urn:xccdf:scoring:flat" />
<profile id="Low-800-53" abstract="true">
  <title>800-53 Low</title>
  <description>This profile selects specific control systems in which all three security objective potential impact value of low. Each control system requires certain controls to be selected</description>
  <select idref="AC-1" selected="1" />
  <select idref="AC-2" selected="1" />
  <select idref="AC-3" selected="1" />
</profile>
</benchmark>
```

```
<?xml version="1.0" encoding="UTF-8" ?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" xmlns:oval="http://oval.mitre.org/XMLSchema/oval-definitions-5" xmlns:ind-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#independent" xmlns:win-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows" xmlns:unix-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#unix" xmlns:linux-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#linux" xmlns:sol-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#sol" xmlns:iso-def="http://oval.mitre.org/XMLSchema/oval-definitions-5#iso" xmlns:scap-schema="http://oval.mitre.org/XMLSchema/oval-definitions-5#scap-schema" />
<generator>
  <oval:schema_version>5.3</oval:schema_version>
  <oval:timestamp>2007-07-30T09:00:10.000-05:00</oval:timestamp>
</generator>
<definitions>
  <definition id="oval.gov.nist.1:def:6001" version="1" class="compliance">
    <metadata>
      <title>Enforce Password History</title>
      <affected family="windows">
        <platform>Microsoft Windows Vista</platform>
      </affected>
      <reference source="NIST" ref_id="NIST-SP-800-53" />
      <description>The number of passwords remembered</description>
      <oval_repository>
        <submitted date="2007-04-05T13:57:10.000-05:00" />
        <contributor organization="Secure Elements, Inc.">Sudhir Gandhe</contributor>
      </oval_repository>
    </metadata>
  </definition>
  <notes>
    <note>Secure Elements - Microsoft Windows Vista Benchmark</note>
  </notes>
  <criteria operator="AND">
    <extend_definition definition_ref="oval.gov.nist.1:def:2" comment="Microsoft Windows Vista is installed" />
    <criterion test_ref="oval.gov.nist.1:tst:60011" comment="Comments need to be added" />
  </criteria>
</definitions>
<definition id="oval.gov.nist.1:def:6002" version="1" class="compliance">
  <metadata>
    <title>Maximum Password Age</title>
  </metadata>
</definition>
```

Verify and Test



Demo
&
Questions