Effective Desktop Management under the Federal Desktop Core Configuration (FDCC) Standard

A ScriptLogic Product Positioning Paper

Effective Desktop Management Under FDCC

The Federal Desktop Core Configuration (FDCC) standards have created a unique set of challenges for federal agency IT departments. While the current focus has been on scanning and reporting compliance rates, future efforts will be centered on successfully improving compliance through effective policy and exception management. Native tools provide some of the capabilities, but to really effectively manage the desktop in an FDCC environment; more granular management options are needed. This paper is intended to introduce some of those challenges and provide some options for resolving them.

FDCC – An Overview

The Federal Desktop Core Configuration (FDCC) standards represent a set of policies designed to provide a secure operating environment for desktop and notebook computers running in federal agencies. The standards represent user security, network security and browser security policies, and are primarily focused on the Windows XP and Windows Vista operating systems. Reference policies are provided for the base operating systems, the Windows Firewall and Internet Explorer 7, however the FDCC guidelines allow for the use of other desktop firewall and web browser applications.

The FDCC standard arose from a Department of Defense (DoD) customization of the Microsoft Security Guides for Windows Vista and Internet Explorer 7. The Windows XP guidelines arose from the US Air Force modifications of the Specialized Security-Limited Functionality (SSLF) guidelines published by the National Institute of Standards and Technology (NIST). The FDCC was originally called for in a memo from Office of Management and Budget (OMB) on March 22, 2007. (OMB Memo M-07-11)

All agencies were directed by OMB to implement FDCC and report their status by February 1, 2008. Compliance is determined by scanning with an SCAP (Security Content Automation Protocol) compliant tool, and reports were to be provided in a format mandated by NIST.

Resources for Implementation

The National Institute of Standards and Technology provides a set of resources to aid implementation of FDCC. Reference images for both Microsoft Windows XP and Windows Vista are supplied as virtual hard drives (VHD). These VHDs contain the operating system configured for 100% compliance, and provide a test platform for applications and network settings in the agency. These virtual hard drives can be used for 120 days from download before the operating system license expires, but new images are uploaded quarterly.

The most common resource for implementing FDCC is the Active Directory Group Policy collection provided by NIST. This collection of policies includes Active Directory management templates

and policy files that can be imported into Active Directory and applied to the machines in the domain. This collection represents the policies needed for 100% compliance, and covers the operating system, the Windows Firewall and Internet Explorer 7.

With the availability of these Group Policy files, Active Directory has become the preferred method of initial implementation of FDCC in most agencies, but using Active Directory is not required.

Challenges of FDCC in Active Use

Many of the challenges of implementing a comprehensive policy like FDCC are minimized through standard IT best practices:

- Have a minimum number of standard images
- Actively apply all security updates
- Do not run end-user accounts as administrators
- Close unneeded ports and network connections

But FDCC is much more restrictive than these best practices. Many agencies are finding problems with networks and applications when applying 100% of FDCC policies. A recent article in *Federal Computer Week* reported on a presentation to agency IT employees regarding FDCC compliance.

> *"One audience member said their agency had a choice: Implement the FDCC and take down their entire network serving 180,000 users, or tell their secretary that they will get a red score from OMB on this year-long mandate.*

> *"FDCC crashes our system," said the audience member, who did not identify their agency. "OMB's initial assumption is wrong that you can apply the FDCC without breaking your system."*

> *Another audience member from the U.S. Patent and Trademark Office said they will not be FDCC compliant because they have a problem with a number of the settings.*

Many common applications were not designed with FDCC guidelines in mind, so they do not follow the best practices necessary to comply. They often require, or expect users to be running as privileged users. They expect ports to be open, or to be able to accept incoming connections. Web applications often require Java, or other active content that is blocked by the FDCC Internet Explorer 7 guidelines.

These problems affect many commercial applications, even for those as innocuous as office suites. Internally developed applications can create compliance issues as well. While it will take years for all commercial applications to become 100% FDCC compliant, many of them are critical to the daily functioning of federal agencies. Some internally developed applications will require intense investment to become compliant, but are used for mission critical purposes every day.

SCRIPTLOGIC

The short-term solution is to create an exception to the policies for those applications to operate properly. FDCC does provide a mechanism for reporting exceptions to the Office of Management and Budget, but does not provide a clear means of managing those exceptions.

Managing Exceptions to FDCC Policies

Using Active Directory Group Policy to manage exceptions to FDCC requirements creates challenges due to the machine based nature of Group Policy.

A Single Set of Policies for the Domain

Policy management can be simplified by using a single set of group policies for all desktop and laptop machines in the domain. Under this approach, any exceptions are applied to all machines, regardless of whether the application or network access requirements underlying the exception apply to each machine.

In a small domain, with few variations in machines and applications, a single set of policies is easy to manage, and can be highly compliant. In a large domain, with a diverse set of applications, a single set of group policies can result in a lower than needed compliance rate. The example below illustrates the problem.

Example: The agency domain includes 50,000 machines across 14 regional offices. Group policies are applied uniformly to all machines. One office requires several exceptions for an internal reporting application. Those exceptions are opened for all machines in the domain. A different regional office requires a set of firewall exceptions for field employee access. Those exceptions are applied across the domain as well. Each time a set of exceptions are applied to the domain, the compliance rate for the entire domain goes down, regardless of how many machines that need that exception.

Using Active Directory Groups to Manage Exceptions

Active Directory groups do provide a more granular way to manage exceptions to FDCC mandates. By grouping computers based on the required exception set, administrators can improve their compliance rate, at the expense of complexity. In a small organization, with a consistent set of applications, the complexity can be minimized. But in a larger agency, the number of groups can quickly become unmanageable. Each time an application is added or retired, a machine moves to a new user, or the FDCC requirements are changed, each group needs to be re-evaluated.

A New Approach: Dynamic Exception Management

The challenges that arise from using only Group Policy for exception management come from the 'all-or-nothing' approach. If a policy is assigned to a computer, that policy will be applied to the computer. There is no mechanism in Active Directory to evaluate a machine before assigning a policy.

SCRIPTLOGIC

Does this mean that Group Policy is a bad choice for managing FDCC compliance? Absolutely not! Group Policy is the ideal solution for that set of FDCC requirements that apply to all machines in the domain. For the policies that vary between computers, what is needed is a more dynamic way to evaluate conditions and then apply the appropriate exceptions. This approach, dynamic exception management, allows administrators to have high compliance rates, while still having a limited set of policies that need to be managed.

Dynamic exception management creates a 2-tiered set of policies. Tier 1 is the set of machine-based group policies that apply to all machines in the domain. Tier 2 is the set of policies that are applied to a machine conditionally, based on the exceptions needed for that computer. These conditions could be tied to applications, network settings, machine type or any other characteristic that might require an exception to the FDCC guidelines. This second tier of policies would be continuously evaluated against a computer and changed as the conditions of the computer change.

Desktop Authority and Dynamic Exception Management

ScriptLogic Desktop Authority provides the complement to Group Policy needed for dynamic exception management. Desktop Authority is a complete desktop lifecycle management solution that provides very fine-grained configuration management options. At the heart of Desktop Authority is Validation Logic, a patented system for evaluating a computer and applying a profile according to the results.

Validation Logic provides over 30 evaluation criteria, from Active Directory properties, network information, file and registry key information, machine type, operating system and more. Any configuration profile element can use validation logic to determine whether that policy should be applied. When used for dynamic exception management, Validation Logic can open exceptions based on whether an application is installed, how the user is connected to the network, or whether the user is in a specific AD group or OU. Virtually any reason an exception might be needed can be discovered through Validation Logic.
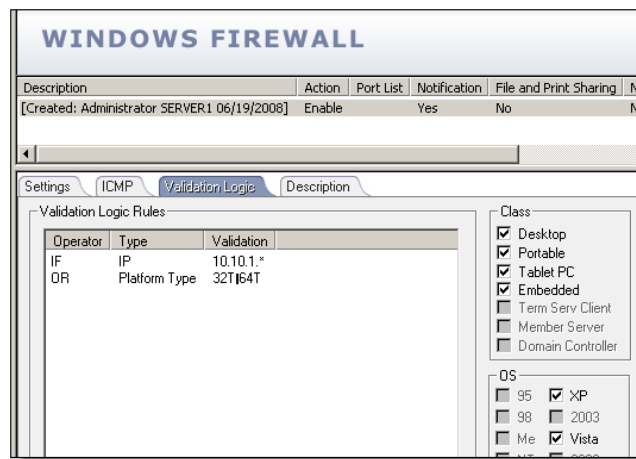
With each user logon, logoff, and at a refresh interval, Desktop Authority profiles are evaluated against each computer using Validation Logic. Only those profile elements that meet the evaluation criteria are applied. This allows a single profile to contain all exceptions, with Validation Logic providing the filtering mechanism.

Returning to our previous example, the agency with 50,000 machines over 14 offices would manage policies as follows:

- All policies that apply to every machine are applied via Group Policy
- All exceptions are defined in a single Desktop Authority profile
- When the Desktop Authority profile is applied to those machines containing the internal reporting application, the necessary exceptions would be opened
- When the profile is applied to machines with IP addresses belonging to the field employees, the firewall exceptions needed for network access would be opened

The original goal of a single set of policies for all machines is achieved, but the compliance rate is as high as using AD groups. More importantly, when the conditions on the individual computer change, Validation Logic will change the applied exceptions accordingly.


Getting Started with Desktop Authority for Exception Management

ScriptLogic offers the FDCC Import utility, which can scan through the NIST provided folder structure and import the contents of the .POL and .INF files. This imports the FDCC policies into a Desktop Authority profile. Alternatively, administrators can specify a single .POL or .INF file to import. The utility will assign default Validation Logic to each element based on operating system, so Windows XP and Vista policies will be applied accordingly.

Then, it is a simple matter of applying any remaining validation criteria to a policy that requires exceptions. Desktop Authority's robust client/server architecture will ensure that the new profile is replicated throughout the organization. As users log in to managed computers, the profile will be applied to each machine based on the profile elements.

Desktop Lifecycle Management with Desktop Authority

Desktop Authority is a complete desktop lifecycle management solution that offers benefits beyond FDCC exception management. Through the Desktop Authority product family, organizations can image new machines to meet compliance needs, package applications, deploy software, map network drives, configure Microsoft Outlook, and much more.

SCRIPTLOGIC
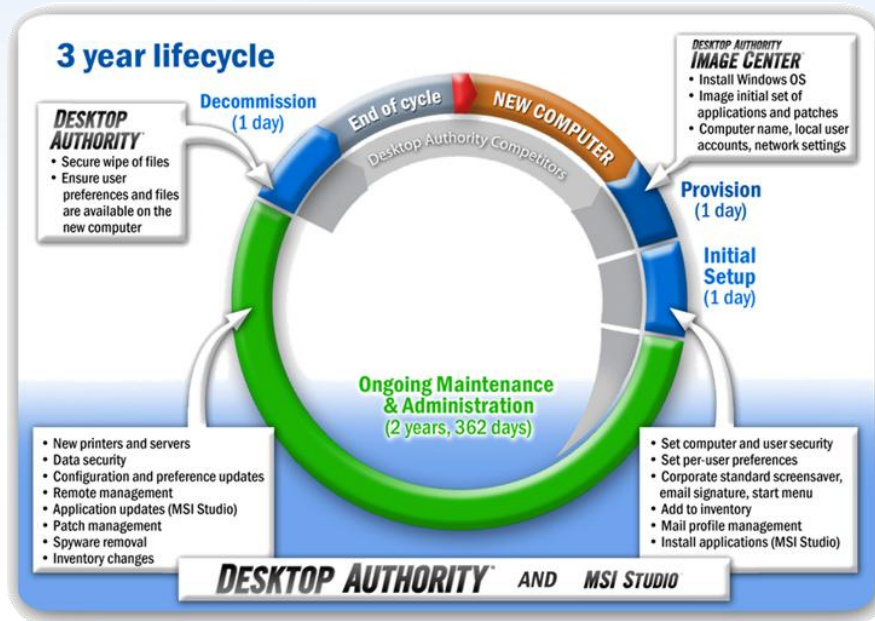
Some of the key features of Desktop Authority include:

- Application deployment
- Remote management
- Patch management and deployment
- Windows Firewall configuration
- Network drive and printer management
- Spyware detection and removal
- USB and port security
- Outlook profile management
- Service pack deployment
- Registry and permissions management

Conclusion

FDCC implementation creates several challenges for agencies, but no challenge greater than effectively managing policy exceptions. Relying only on Group Policies to manage exceptions creates a trade-off between management complexity and compliance rates. Creating an environment that is easy to manage, but still very compliant requires a two-tiered approach. Global policies can be implemented through Group Policy. Exceptions can be managed dynamically through Desktop Authority and the FDCC Import utility. Desktop Authority's patented Validation Logic can evaluate each machine and only apply the minimum number of exceptions needed.

Resources

The ScriptLogic FDCC Compliance Center:
http://www.scriptlogic.com/compliance/fdcc.asp

Desktop Authority:
http://www.scriptlogic.com/da

The FDCC Web Site:
http://fdcc.nist.gov/

References

"**OMB Stresses FDCC Compliance Means 100%**," Jason Miller, *Federal Computer Week*, January 25, 2008
http://www.fcw.com/online/news/151428-1.html

FDCC Download Page, http://nvd.nist.gov/fdcc/download_fdcc.cfm

OMB Memo M-07-11, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf

OMB Memo M-07-18, http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf

FDCC FAQs, http://nvd.nist.gov/fdcc/fdcc_faqs_20070731.cfm

SCRIPTLOGIC