Report Number: C4-019R-01

Guide to Securing Microsoft Windows 2000® Schema

Operating Systems Division
of the
Systems and Network Attack Center (SNAC)

Author:
David Rice

Updated: March 6, 2001
Version 1.0

National Security Agency
9800 Savage Rd. Suite 6704
Ft. Meade, MD 20755-6704

W2KGuides@nsa.gov

This Page Intentionally Left Blank

Warnings

- **Do not attempt to implement any of the settings in this guide without first testing in a non-operational environment.**
- This document is only a guide containing recommended security settings. It is not meant to replace well-structured policy or sound judgment. Furthermore this guide does not address site-specific configuration issues. Care must be taken when implementing this guide to address local operational and policy concerns.
- The security changes described in this document only apply to Microsoft Windows 2000 systems and should not be applied to any other Windows 2000 versions or operating systems.
- SOFTWARE IS PROVIDED "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN NO EVENT SHALL THE CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
- This document is current as of March 6, 2001. See Microsoft's web page for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Acknowledgements

The author would like to acknowledge the authors of the Microsoft Windows 2000 Server Resource Kit, and Inside Windows 2000 Server.

Trademark Information

Table of Contents

This Page Intentionally Left Blank

Introduction

The purpose of this guide is to inform the reader about the available security settings for the Windows 2000 Schema. In all but the most specific instances, the system administrator should have little or no involvement with the Schema or have a need to load the Microsoft Management Console Schema snap-in. Any effort to modify the Schema should be heavily weighed and well thought out before being implemented, as schema modifications **cannot** be reversed. Inconsistencies in the Schema can cause significant problems that will impair or disable Active Directory.

WARNING: Any effort to modify the Schema should be heavily weighed and well though out before being implemented, as schema modifications cannot be reversed. Inconsistencies in the Schema can cause significant problems that will impair or disable Active Directory. And yes, this is important enough to state twice at the beginning of the document.

This guide provides information pertaining to the default security settings protecting the Schema, but does not contain step-by-step instructions usually found in the Security Configuration Guide Series. The Schema is guarded by a number of different mechanisms that should not be altered or changed in any way. Because most organizations will be able to use the Schema "as-is," only those organizations wishing to alter the schema should be concerned. In short, do not touch the Schema unless you must absolutely do so.

The ***Guide to Securing Microsoft Windows 2000 Schema*** presents information on security of the Schema in a network environment.

NOTE: This guide does not address security issues for the Microsoft Windows 2000 operating system that are not specifically related to the Schema and its implementation.

This document is intended for Windows 2000 network administrators, but should be read by anyone involved or interested in Windows 2000 or network security.

Getting the Most from this Guide

The following list contains suggestions to successfully secure the Windows 2000 Schema according to this guide:

WARNING: This list does not address site-specific issues and every setting in this book should be tested on a non-operational network.

- Read the guide in its entirety. Subsequent chapters build on information and settings discussed in prior chapters. Omitting or deleting concepts can potentially lead to an unstable system and/or network that will require reconfiguration and reinstallation of software.
- Perform pre-configuration recommendations:
  - Perform a complete backup of your system if this is not a new installation.

About the Guide to Securing Microsoft Windows 2000 Schema

This document consists of the following chapters:

Chapter 1, "Windows 2000 Schema Overview," provides a description and overview of the Schema, as well as discusses its importance.

Chapter 2, "Modifying Windows 2000 Schema," contains information about modifying the Schema, but does not give step-by-step instructions.

Appendix A, "Further Information," contains a list of the hyperlinks used throughout this guide and a list of the resources cited.

Appendix B, "References," contains a list of resources cited.

Chapter

1

Windows 2000 Schema Overview

Windows 2000 Active Directory is an object-oriented database composed of individual instances of various object classes. The Schema is the *blueprint* for Active Directory, containing the definition for the universe of objects that can be stored in the directory. The Schema dictates what kinds of objects can exist in the database as well as what attributes those objects may posses. In addition to defining objects and attributes, the schema also dictates the *rules* that govern both the structure and the content of the directory.

The base Schema that ships in Microsoft 2000 contains all the necessary directory definitions used by Windows 2000 and Windows 2000 components. For most organizations, the base Schema is all that will ever be needed.

Windows 2000 Schema

For any particular object to exist in Active Directory, it must first be defined. Without a definition, the object cannot and will not exist. Think of the Schema as an absolute, authoritative dictionary for Active Directory. If Active Directory does not have a definition for an object in its dictionary (the Schema), the object absolutely does not exist.

For a User **object** to exist, a User **class** in the Schema must define it. The **class** is the blueprint for the **object**. The **class** defines the **object**. The **class** dictates what attributes an **object** must/will possess. Not only would Active Directory be unable to "build" a User object without the blueprint, but it would also be unable to identify or locate the object within its database.

A class is a "named collection" of attributes. The User **class** will have attributes such as FirstName, LastName, and PhoneNumber. The User **object**, therefore, will have those attributes "filled" with the respective data for each attribute. FirstName will be filled with the data "Bob"; LastName will be filled with the data "Smith", and so on.

While Active Directory data is distributed among all domain controllers in a forest, no single domain controller stores all Active Directory data for the entire forest. However, every domain controller does hold a copy of the Schema.

One can see then, if the Schema is somehow corrupted, either innocently or otherwise, the consequences can be catastrophic. Active Directory would be unable to comprehend or locate any given object because its dictionary for interpreting those objects has changed.

Security

Because the Schema is so important to Active Directory, Windows 2000 provides several mechanisms that act as safety interlocks. All the correct conditions must be met by the safety interlocks for the Schema to be modified. Again, in almost all instances, the system administrator has no reason to deal with the Schema directly.

Schema Administrator Permissions

The administrator account is automatically made a member of the Schema Administrators group. This is a built-in group created during Active Directory installation that grants its members permission to write to the Schema. However, membership in the Schema Administrators group by itself is not enough to make changes to the Schema.

WARNING: Membership in the Schema Administrators group must be highly restricted to prevent unauthorized access to the Schema. Inconsistencies in the Schema can cause significant problems that will impair or disable Active Directory.

Schema Floating Single-Master Operations

Unlike Active Directory, which uses a multi-master replication system, the Schema uses a single-master system. This means that only one domain controller can modify the schema at any given time. The domain controller that holds the Schema Master Role is the only domain controller that can perform **Write** operations to the directory schema. By default, the first domain controller in the initial domain will retain the Schema Master Role until the master role is assigned to another domain controller.

Schema updates are replicated from the Schema Master to all other domain controllers in the forest. The Schema Master Role is a per-forest operations master role. Regardless of the number of domains contained within a forest, there is only one Schema.

Any attempt modifying the Schema on the Schema Master will deny write access requests to the schema on all other domain controllers.

Read-Only Schema Access

Finally, all domain controllers are configured by default during Active Directory installation to permit read-only access to the Schema. This means that in order to write to the Schema, the administrator must create a new DWORD registry entry called *Schema Update Allowed* under the following key:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
```

A value of 1 will enable write-access to the Schema. A value of 0 will disable write-access to the Schema. This additional entry need only be created on the domain controller that holds the Schema Master Role.

WARNING: It is imperative the *Schema Update Allowed* value is set back to 0 (disable write-access) after any changes have been made to the Schema. Failure to do so may leave the Schema vulnerable.

Consistency Checks

Any modifications to the Schema must also pass a number of consistency checks. While these are not necessarily security related, they maintain the stability of the Schema by checking a number of different parameters for class and attribute creation. Seven different consistency checks are conducted on new class definitions and six different consistency checks are conducted on new attribute definitions. A complete enumeration of the consistency checks has been elided for brevity.

Chapter

2

Modifying Windows 2000 Schema

Modifying the Schema is an event of great consequence, and for that reason this guide **purposefully** avoids making recommendations as to altering the Schema. Once the safety interlocks introduced in the previous chapter have been set to allow Schema modification, changes to the Schema are entirely and solely the responsibility of the Chief Information Officer or accountable IT Manager.

This guide can only serve to make organizations aware of the implications of Schema modification. **Please consult the Microsoft Windows 2000 Server Resource Kit documentation for appropriate step-by-step guidance in altering the contents of the Schema.**

Schema Modification Issues

Modifying the Schema is subject to the same vigilance as modifying a Windows NT/2000 system registry, except on a much larger scale. Just as improper registry modifications can adversely affect a single system, improper Schema modifications can have a devastating effect on the entire network. Again, once the safety interlocks are set to permit Schema modification, the issue is no longer of security, i.e. access control, but stability.

Schema Hegemony

A forest is a collection of one or more Windows 2000 Active Directory trees, organized as peers and connected by two-way, transitive trust relationships. Multiple domains constitute multiple trees. If trust relationships exist between the domains, that collection of trees is a forest.

Conceptually, it is easier to comprehend multiple trees constituting a forest because the reader can draw on examples from the physical world. By definition, a forest in the real world is considered to consist of a collection of trees. A pine **forest** consists of pine **trees**.

Where some confusion may arise however, is that in Windows 2000 architecture, a single domain may also constitute a tree of one domain. Even though there is only one tree, that tree exists in a forest. It is a forest with a single tree.

Regardless of the number of trees in a forest, and irrespective of the number of domains within a tree, the forest consists of **one and only one** Schema.

Currently, Windows 2000 provides no mechanism for Tree Root trusts or Domain Trusts between **existing** Windows 2000 domains. For organizations creating a brand new peer domain this is not an issue. The new domain controllers are simply promoted and instructed to join an already existing forest.

However, when one organization with a functioning Windows 2000 domain wishes to incorporate another organization that already has a functioning Windows 2000 domain,

the two cannot join together to form a forest. One organization would be forced to demote **every** Windows 2000 domain controller in the domain and then rebuild the domain from scratch with the appropriate trust relationship.

Though this task may seem extremely daunting, especially for very large organizations, it ensures that all domain controllers within the forest posses a consistent Schema. Otherwise, innumerable attempts would be made on the part of the system administrator to reconcile two, possibly incompatible Schemas.

The reader can see then why modification of the Schema can have such profound repercussions. If the two organizations mentioned above have made extensive changes to the Users class in their respective Schemas, one organization is bound to lose some fidelity when transferring to the new domain.

This is not to say an organization **must** completely avoid changing the Schema, though that has been overriding recommendation in this document. Sometimes, operational necessity dictates that changes must be made. In some cases, 3rd Party applications will make valid changes to the Schema. It is recommended that you modify the Schema only **when it is absolutely necessary** and that changes are well planned and well thought out before implementation. Confirm when and how 3rd Party applications alter the Schema.

WARNING: Valid changes to the Active Directory Schema may occur when loading 3rd Party applications. This is to be expected as Microsoft made great efforts to enable Independent Software Vendors access to the power of Active Directory. However, Administrators should be aware when and how 3rd Party applications make changes to the Schema. It is imperative the *Schema Update Allowed* value located in the registry is set back to 0 (disable write-access) after any changes have been made to the Schema. Correctly written 3rd Party applications should already do this for you, but it is always wise to double-check.

If an organization decides to alter the Schema, and the above recommendation is dutifully considered, other issues arise particularly in reference to replication, concurrency control, and handling invalid object instances. Though these issues are not critical to the survival of the Schema, they can cause some very insidious troubleshooting issues. Please consult the Microsoft Windows 2000 Server Resource Kit Distributed Systems Guide for specific considerations.

Appendix

A

Further Information

Microsoft's web site, http://www.microsoft.com/

This Page Intentionally Left Blank

Appendix

B

References

Apsley, et al, Microsoft Windows 2000 Server Deployment Planning Guide, Microsoft Press, 2000.

Boswell, William, Inside Windows 2000 Server, New Riders, 2000.

Iseminger, David, Active Directory Services for Microsoft Windows 2000 Technical Reference, Microsoft Press, 2000.

Lundman, et al, Microsoft Windows 2000 Server Distributed Systems Guide, Microsoft Press, 2000.

Microsoft's web site, http://www.microsoft.com/

Russel, Charlie and Sharon Crawford, Microsoft Windows 2000 Server Administrator's Companion, Microsoft Press, 2000.