Report Number: C4-018R-01

Guide to Windows 2000 Kerberos Settings

Architectures and Applications Division
of the
Systems and Network Attack Center (SNAC)

Author:
Dave Opitz

Updated: April 12, 2001
Version 1.0 Draft

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

410-854-6015
securew2k@dewnet.ncsc.mil

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 April 12, 2000. See Microsoft's web page http://www.microsoft.com/ for the latest changes or modifications to the Windows 2000 operating system.

This Page Intentionally Left Blank

Trademark Information

This Page Intentionally Left Blank

Table of Contents

Table of Figures

Table of Tables

This Page Intentionally Left Blank

Introduction

Getting the Most from this Guide

The following list contains suggestions to successfully use Kerberos in Windows 2000:

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. Omitting or deleting steps 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 before implementing any of the recommendations in this guide.
  - Ensure that the latest Windows 2000 service pack and hotfixes have been installed. For further information on critical Windows 2000 updates, see the Windows Update for Windows 2000 web page http://www.microsoft.com/windows2000/downloads/default.asp.
- Follow the security settings that are appropriate for your environment.

About the Guide to Windows 2000 Kerberos Settings

This document consists of the following chapters:

Chapter 1, "Windows 2000 Kerberos Settings," contains general guidance on Kerberos, Kerberos settings in Group Policy, and Kerberos in User and Computer properties.

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

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

This Page Intentionally Left Blank

Chapter 1

Windows 2000 Kerberos Settings

Kerberos version V is the default Windows 2000 authentication mechanism. It is used for logon, domain trusts, and authentication for individual services. Kerberos is an Internet standard, described in the IETF RFC 1510 (see http://www.ietf.org/rfc/rfc1510.txt), and has been widely analyzed. The protocol is considered to be cryptographically sound, which is one of the reasons why Microsoft chose to use it.

Finding More Information

Microsoft has written many documents on Kerberos, however the paper titled ***"Authentication for Administrative Authority",*** published on July 28, 2000, seems to be particularly comprehensive. This paper was used extensively as a reference while writing this guide, and can be downloaded from http://www.microsoft.com/technet/security/authent.asp. The following topics are covered in the paper:

- Kerberos protocol overview
- Role of Kerberos
- How Kerberos fits into the logon scheme
- Kerberos management
- Interoperability with other Kerberos versions
- Trust configuration
- Planning for various environment sizes

For more details of the Kerberos protocol, Microsoft has also written a detailed white paper on the Kerberos protocol titled ***"Windows 2000 Kerberos Authentication."*** It was was published on July 9, 1999 and can be downloaded from http://www.microsoft.com/WINDOWS2000/library/howitworks/security/kerberos.asp.

There are also several other valuable Kerberos papers available from Microsoft. On the Microsoft technet web site, there is a link in the **IT Solutions** area, under the **Security** section, for **Best Security Practices for Enterprise Security**.

Kerberos Settings in Group Policy

The Microsoft ***"Best Security Practices for Enterprise Security"*** document contains a section titled "*How to Configure Kerberos in Windows 2000*" and begins with the following sentences.

"The primary thing to remember about configuring Kerberos is that the default is good. Only about a half dozen items can be changed in Kerberos on Windows 2000. Unless there is some specific reason to change one of the parameters, you should leave the parameters alone."

NSA agrees with this assessment. Before changing any of the Kerberos settings, the user should have a thorough understanding of the protocol, and a good reason why a setting should be changed. The ***"Best Security Practices for Enterprise Security"*** document does provide some possible reasons why a user might want/need to change the parameter(s).

The parameters settings can be found in the Group Policy MMC snap-in tool.

✍ Select **Computer Configuration** ? **Windows Settings** ? **Security Settings** ? **Account Policies** ? **Kerberos Policy**

A window should appear that looks similar to **Figure 1**. A domain administrator must make any changes to the Kerberos settings. Once changes are configured on one domain controller, the settings will replicate to all the other domain controllers along with the normal Active Directory replication.

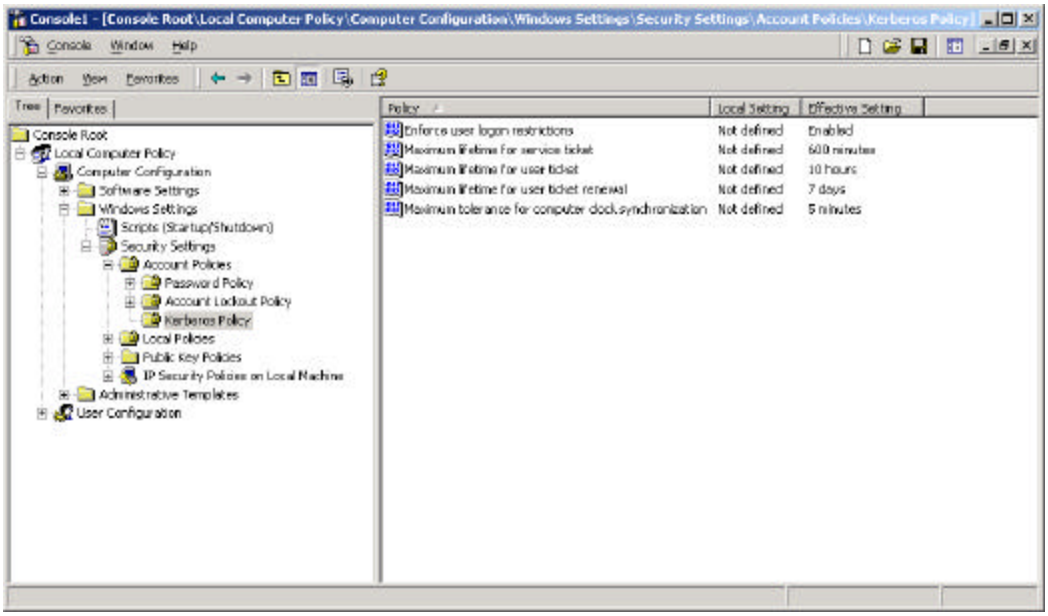

Figure 1 – Parameters in Group Policy MMC Snap-in Tool

There are five parameters that can be set. **Table 1** lists the default settings and the recommended settings. For the last four settings in Table 1, the default values, or anything approximately close to those values, are adequate.

Policy	Recommended Settings
Enforce user login restrictions Forces the Key Distribution Center (KDC) to check if a user requesting a service ticket has either the "Log on locally" (for local machine service access) or "Access this computer from the network" user right on the machine running the requested service. If the user does not have the appropriate user right, a service ticket will not be issued. This prevents a disabled account from obtaining new service tickets. The TGT will expire in 10 hours (if the default for the user ticket lifetime is used), but this user logon restriction eliminates that small window of opportunity. Enabling this option provides increased security, but may slow network access to servers.	Enabled
Maximum lifetime for service ticket Determines the number of minutes a Kerberos service ticket is valid. Values must be between 10 minutes and the setting for "Maximum lifetime for user ticket."	600 minutes
Maximum lifetime for user ticket Determines the number of hours a Kerberos ticket-granting ticket (TGT) is valid. Upon expiration of the TGT, a new one must be obtained or the old one renewed.	10 hours
Maximum lifetime for user ticket renewal Sets the maximum number of days that a user's TGT can be renewed.	7 days
Maximum tolerance for computer clock synchronization Sets the maximum number of minutes by which the KDC and client machine's clocks can differ. Kerberos makes use of time stamps to determine authenticity of requests and aid in preventing replay attacks. Therefore, it is important that KDC and client clocks remain synchronized as closely as possible.	5 minutes

Table 1 – Recommended Kerberos Settings

Kerberos in User and Computer Properties

There are a few other Kerberos options available. From the **Active Directory Users and Computers** window, select a user (probably in the **Users** folder), and click **Properties**. A window appears with numerous tabs, as shown in **Figure 2**.

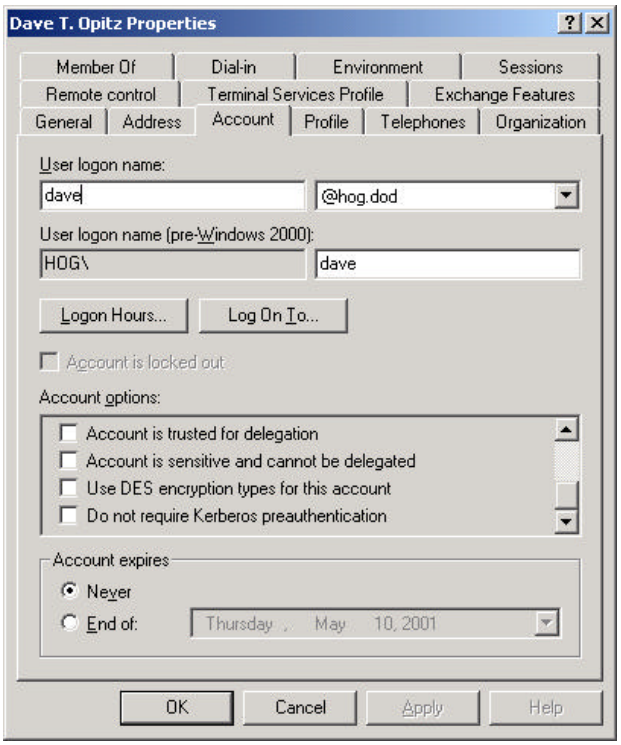

Figure 2 – Property Tabs

Click on the **Account** tab. The default settings for account options are shown in **Table 2.** By default, these account options settings are all turned off.

Account Options	Default Value
Smart Card is required for interactive logon Requires a user to use a smart card for successful logon. See the **Other Guidance** section for more information on smart cards.	Disabled
Account is trusted for delegation Provides a service running under a user account (as many, but not all, services do) the ability to forward Kerberos tickets. There are many services where this is needed, but this should only be turned on for accounts that run those services. An example service requiring delegation is when a user connects to a web server and retrieves his mail from an Exchange server.	Disabled
Account is sensitive and cannot be delegated Enabling this option means that a user cannot have his/her credentials forwarded. While selecting this option is a more secure setting, the administrator needs to be aware that enabling this option could break several useful services. It should be selected for administration accounts - although the domain administrator has the ability to reset it if needed.	Disabled
Use DES encryption for this account Allows for the use of 56-bit DES encryption instead of the much more secure 128-bit RC4 used in Microsoft Kerberos. This option was included to interoperate with an older Unix-based Kerberos implementations. Due to the susceptibility of DES to cryptographic exhaustion attack, the use of DES is not recommended. This does lead to a security weakness if the administrator is attempting to interoperate with a Unix based Kerberos, since DES is the only encryption that will work in this configuration. Until Microsoft decides to include 3DES as a Kerberos encryption option, there will be no secure way to interoperate. Related to this, the administrator should ensure the high encryption pack is installed so not to result in weakened cryptography, possibly without the administrator's knowledge.	Disabled
Do not require Kerberos pre-authentication Requiring pre-authentication makes it slightly more difficult for an attacker to gather information on which to run password-guessing attacks. If pre-authentication is used (which is the default, when the option is disabled), an attacker has to sniff the logon for each user to collect data for password guessing. Without this option, the attacker could send bogus messages to the KDC, pretending to be every valid user one at a time, and collect the data sent in reply. With this, the attacker could do off-line password guessing on all of the users' passwords at once.	Disabled

Table 2 – Default Settings for Account Options

The final Kerberos option, **Trust computer for delegation** (See **Figure 3**), is also available from the **Active Directory Users and Computers** window and can be reached by performing the following steps:

- Right-click on a specific computer and select **Properties**
- Click the **General** tab and locate the checkbox for **Trust computer for delegation**

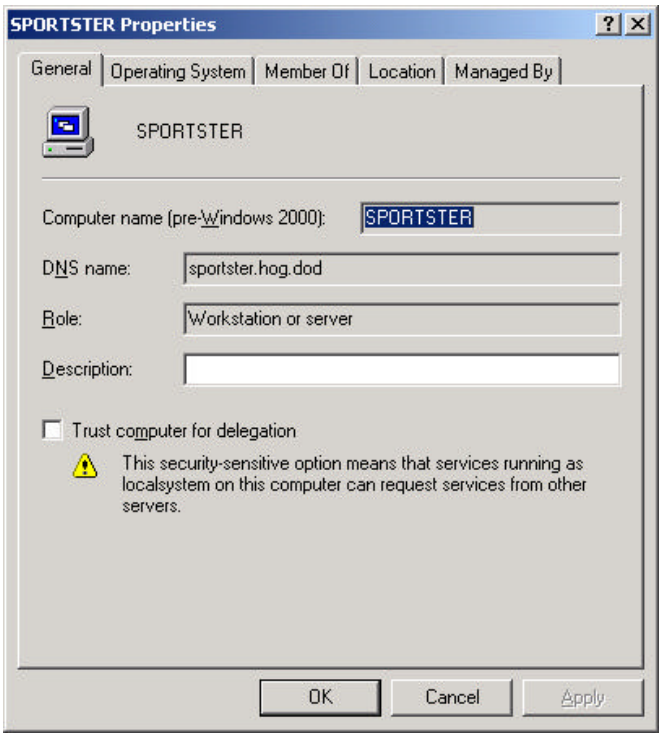

Figure 3 – Trust Computer for Delegation Option

By default, this option is unchecked. This is similar to the **Account is trusted for delegation** button, but many services run as the local administrator instead of as a user, so this is a way of controlling ticket forwarding on those services. This should be enabled only when needed.

Other Guidance

Smart Cards

There is one Kerberos related issue that the Microsoft ***"Best Security Practices for Enterprise Security"*** paper fails to discuss completely. It does mention the well-known fact that the security of Kerberos is based on the user's password. Thus, users should choose passwords that are difficult to guess, authentication failures should be logged, and multiple failures in a short time should cause a user account to be locked out. However, the paper does not talk about one countermeasure to this weakness – smart cards.

Windows 2000 can use smart cards for logon. The user's certificate and private key are stored on this smart card. When the user logs in by inserting the smart card, instead of using the password to protect the first pair of Kerberos messages, the user's public key is used to protect them. It is much more difficult to attack the key pair on a smart card than to guess a password. Adding smart card logons can be a large feature to deploy, but it does eliminate the password weakness of Kerberos.

Non-Windows 2000 Clients

Windows 2000 domain controllers can support Windows 2000, Windows NT, or Windows 9x clients. Windows 2000 clients can take advantage of the full functionality of Kerberos authentication. Windows NT or 9x clients, however, cannot, and must use the weaker NTLM authentication method. To ensure that only the stronger Kerberos authentication method is being used, upgrade non-Windows 2000 clients to Windows 2000.

Appendix

A

Further Information

http://www.Microsoft.com

http://www.ietf.org/rfc/rfc1510.txt

http://www.microsoft.com/technet/security/authent.asp

http://www.microsoft.com/WINDOWS2000/library/howitworks/security/kerberos.asp

This Page Intentionally Left Blank

Appendix

B

References

"Authentication for Administrative Authority", Microsoft white paper, July 2000.