

NT4 Domain Controller Security Standard

NT4 Domain Controller Security Standard

Published 16 May 2009

Copyright © 2001, 2002, 2003, 2009 Frank O'Dwyer

This document specifies technical security policy for implementations of Microsoft Windows NT4.0, and applies to domain controller implementations of NT4.0.

This standard contains 22 baseline controls, and 0 above baseline controls, for a total of 22 controls.

Important

All of these Security Standards and Security Policies are copyrighted. THEY ARE NOT IN THE PUBLIC DOMAIN. They are however distributed under a liberal open-source license, see Publishing these Security Standards and Policies.

Table of Contents

1. Introduction	1
1.1. Objectives	1
1.2. Scope	1
1.3. Not In Scope	1
1.4. Giving Feedback	1
1.5. Publishing these Security Standards and Policies	1
1.6. Related Documents	2
1.6.1. Generic Security Standards	2
1.6.2. Operating System Security Standards	3
1.6.3. Database Security Standards	3
1.7. Definitions	3
2. User Configuration	4
2.1. User Administration	4
2.1.1. User passwords must be set to be changed following reset or after the creation of a new account	4
2.1.2. A Home Directory should be specified for each user.	4
2.1.3. Each user account must have the full name and description fields completed with the details of the account owner name and phone number	5
2.1.4. All users should have a logon script	6
2.2. Default Accounts	6
2.2.1. Ensure that the Guest account is disabled	6
2.3. Privileges	7
2.3.1. The advanced user right to lock pages in memory must be held by no one.	7
2.3.2. The advanced user right to log on as a batch job must be held by no one.	7
2.3.3. The user right to take ownership of files and directories must be held by administrators only	8
2.3.4. The user right to manage auditing and security log must only be available to administrators and the security group	8
2.3.5. The user right to backup files and directories must only be held by Backup Operators	9
2.3.6. The advanced user right to increase quotas must be held by administrators only	10
2.3.7. The user right to restore files and directories must be held by administrators and backup operators only.	10
2.3.8. The user right, access this computer from the network, should be available to everyone	11
2.4. Authentication/Password Configuration	11
2.4.1. User accounts must not be set such that the user cannot change their password	12
2.4.2. User accounts must not be set such that the password never expires	12
3. Network Security Configuration	14
3.1. Network Interface Considerations	14
3.1.1. Remote Access Server must be enabled only if required	14
4. Configuration	15
4.1. Files and File Permissions	15
4.1.1. File and directory permissions must be restricted on the basis of least privilege	15
4.2. Administration	15
4.2.1. Check password filter configuration	15
4.2.2. Replication must be implemented only at the administrator level	16
5. Auditing and Monitoring	17
5.1. Events to be alerted in real-time	17
5.1.1. User accounts should be locked out after 3 consecutive login failures	17

5.1.2. The reset count for logon failures should be set to 7200 minutes 17
5.1.3. The lockout duration should be set to forever 18
6. Checklist 20

Chapter 1. Introduction

1.1. Objectives

The objectives of this document are:

- To specify a baseline configuration for implementations of <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0 domain controller.
- To provide guidance to administrators, developers and security personnel in securely implementing <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0 domain controller.

1.2. Scope

Controls specified in this document apply to domain controller implementations of NT4.0.

All of the organisation's NT4.0 domain controller systems will be subject to the policies specified within this security standard. The policies will be applied to new and existing installations.

1.3. Not In Scope

Compliance with this standard will not provide “in depth” security architecture or intelligent security design guidance to projects. As a consequence, for high impact or safety-critical business applications, additional guidance will still need to be sought from your Information Security team consultancy function.

This is a specific standard for NT4.0 domain controllers. Controls specific to workstation, server, and generic controls common to all are not specified in this document and are the subject of separate standards.

Compliance with this standard does not negate the need for an overall security review of a proposed application. Contact the Information Security team if you are in doubt.

1.4. Giving Feedback

Your feedback to improve this document is welcome. Please let me know of your experiences in applying the controls and guidance in this standard. Are the controls effective, easy to implement, too onerous, clear, unclear, something missing? Does an exceptional case need to be covered? Let me know. Please send your comments to frankodwyer AT netscape.net. Your comments will be used to produce better free security standards for the IT community.

I also request that you give feedback where you think the controls and guidance is correct. This will let us gauge whether or not specific controls are controversial or broadly acceptable to the community, and will help us to resolve cases where we have conflicting feedback on particular content.

1.5. Publishing these Security Standards and Policies

This document may be reproduced and distributed in whole or in part, free of charge, subject to the fol-

following conditions:

- All copyright and trademark notices, and this permission notice must be preserved complete on all complete or partial copies.
- Any translation or derivative work of this document must be approved by Frank O'Dwyer in writing before distribution.
- If you distribute this guide in part, instructions for obtaining the complete version of this manual must be included, and a means for obtaining a complete version provided.
- Small portions may be reproduced as illustrations for reviews or quotes in other works without this permission notice if proper citation is given.
- Neither Frank O'Dwyer's name nor the names of any contributors may be used to endorse or promote products derived from this document without specific prior written permission.

THIS DOCUMENT IS PROVIDED BY FRANK O'DWYER AND CONTRIBUTORS "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 DISCLAIMED. IN NO EVENT SHALL FRANK O'DWYER OR 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.

I would like to be informed of any plans to publish or distribute these documents, just so I know how they're being used and where they are becoming available. If you are publishing or distributing or planning to publish or distribute any of these documents, please send mail to frankodwyer AT netscape.net

1.6. Related Documents

This document should be read and applied in conjunction with the technology specific security standards that are available from the frankodwyer.com web site. Please note that some of the documents below are currently under development and as such may not as yet be available. Check back frequently for updates to this document and those documents listed below.

1.6.1. Generic Security Standards

Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

Data Protection European Union Security Standard

<http://www.frankodwyer.com/standards/index.html#generic>

Application Service Provider Security Standards

<http://www.frankodwyer.com/standards/index.html#generic>

1.6.2. Operating System Security Standards

Generic Unix Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Generic Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Workstation Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Server Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

Windows NT4.0 Domain Security Standards

<http://www.frankodwyer.com/standards/index.html#os>

1.6.3. Database Security Standards

Oracle Security Standards

<http://www.frankodwyer.com/standards/index.html#db>

1.7. Definitions

An “Information Asset” equates to any computerised information system or component thereof and thus includes an application, off the shelf software, hardware, media, data item, data item repository and associated communications networks. The specification of the Information Asset in question will usually be given so that this document is unambiguous.

Chapter 2. User Configuration

2.1. User Administration

2.1.1. User passwords must be set to be changed following reset or after the creation of a new account

ID	Version	Level	Enforcement
NT4D-UC-2	1.0	baseline	mandatory

2.1.1.1. Standard

User passwords must be set to be changed following reset or after the creation of a new account

2.1.1.2. Detailed Steps

- Select change password at next logon for the account in question

2.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Account passwords may be compromised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.2. A Home Directory should be specified for each user.

ID	Version	Level	Enforcement
NT4D-UC-7	1.0	baseline	recommended

2.1.2.1. Standard

A Home Directory should be specified for each user.

2.1.2.2. Detailed Steps

- Ensure that the home directory is specified for each account unless it is to be defined in a login script

2.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.3. Each user account must have the full name and description fields completed with the details of the account owner name and phone number

ID	Version	Level	Enforcement
NT4D-UC-6	1.0	baseline	mandatory

2.1.3.1. Standard

Each user account must have the full name and description fields completed with the details of the account owner name, location and phone number

2.1.3.2. Detailed Steps

- Complete the full name and description for each user account

2.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- This information aids rapid investigation of anomalies
- This information aids resolution of access validation/audits
- A failure to be able to successfully audit access may result in unauthorised accounts going unnoticed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.1.4. All users should have a logon script

ID	Version	Level	Enforcement
NT4D-UC-1	1.0	baseline	recommended

2.1.4.1. Standard

All users should have a logon script

2.1.4.2. Detailed Steps

- For each user define a logon script that pertains to the group they are in or the type of user they are.

2.1.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Environment variables and restrictions may be bypassed
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.2. Default Accounts

2.2.1. Ensure that the Guest account is disabled

ID	Version	Level	Enforcement
NT4D-UC-5	1.0	baseline	recommended

2.2.1.1. Standard

Ensure that the Guest account is disabled

2.2.1.2. Detailed Steps

- Ensure that the Guest account is disabled

2.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- The Guest account can be used to gain access to information assets
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.3. Privileges

2.3.1. The advanced user right to lock pages in memory must be held by no one.

ID	Version	Level	Enforcement
NT4D-PRIV-7	1.0	baseline	mandatory

2.3.1.1. Standard

The advanced user right to lock pages in memory must be held by no one.

2.3.1.2. Detailed Steps

- Ensure that no one holds this right

2.3.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and services may be subject to a loss of availability

2.3.2. The advanced user right to log on as a batch job must be held by no one.

ID	Version	Level	Enforcement
NT4D-PRIV-8	1.0	baseline	mandatory

2.3.2.1. Standard

The advanced user right to log on as a batch job must be held by no one.

2.3.2.2. Detailed Steps

- Ensure that no one holds this right

2.3.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and services may be subject to a loss of availability

2.3.3. The user right to take ownership of files and directories must be held by administrators only

ID	Version	Level	Enforcement
NT4D-PRIV-4	1.0	baseline	mandatory

2.3.3.1. Standard

The user right to take ownership of files and directories must be held by administrators only

2.3.3.2. Detailed Steps

- Ensure that the administrators group holds this right
- Ensure that only administrator staff are members of the administrators group

2.3.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be subject to unauthorised disclosure
- Business information may be subject to a loss of availability
- Business information may be subject to alteration

2.3.4. The user right to manage auditing and security log must only be available to administrators and the security group

ID	Version	Level	Enforcement
NT4D-PRIV-3	1.0	baseline	mandatory

2.3.4.1. Standard

The user right to manage auditing and security log must only be available to administrators and the security group

2.3.4.2. Detailed Steps

- Ensure that the administrators group holds this right
- Ensure that the security users group holds this right
- Ensure that only administrators are members of the administrators group
- Ensure that only security users are members of the security group

2.3.4.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Sensitive audit trail data may be lost
- Sensitive audit trail data may be disclosed
- Business information may be subject to unauthorised disclosure
- Business information may be subject to a loss of availability
- Business information may be subject to alteration

2.3.5. The user right to backup files and directories must only be held by Backup Operators

ID	Version	Level	Enforcement
NT4D-PRIV-2	1.0	baseline	mandatory

2.3.5.1. Standard

The user right to backup files and directories must only be held by Backup Operators

2.3.5.2. Detailed Steps

- Ensure that only operators are in the backup operators group
- Ensure that the backup operators group hold the backup files and directories user right

2.3.5.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be subject to unauthorised disclosure
- Business information may be subject to a loss of availability

2.3.6. The advanced user right to increase quotas must be held by administrators only

ID	Version	Level	Enforcement
NT4D-PRIV-6	1.0	baseline	mandatory

2.3.6.1. Standard

The advanced user right to increase quotas must be held by administrators only

2.3.6.2. Detailed Steps

- Ensure that the administrators group holds this right
- Ensure that only administrator staff are members of the administrators group

2.3.6.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and services may be subject to a loss of availability

2.3.7. The user right to restore files and directories must be held by administrators and backup operators only.

ID	Version	Level	Enforcement
NT4D-PRIV-5	1.0	baseline	mandatory

2.3.7.1. Standard

The user right to restore files and directories must be held by administrators and backup operators only.

2.3.7.2. Detailed Steps

- Ensure that the administrators and backup operators group holds this right
- Ensure that only administrator staff are members of the administrators group
- Ensure that only backup operators are members of the backup operators group

2.3.7.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be subject to unauthorised disclosure
- Business information may be subject to a loss of availability
- Business information may be subject to alteration

2.3.8. The user right, access this computer from the network, should be available to everyone

ID	Version	Level	Enforcement
NT4D-PRIV-1	1.0	baseline	recommended

2.3.8.1. Standard

The user right, access this computer from network should be available to everyone

2.3.8.2. Detailed Steps

- Ensure that the everyone group holds the user access right, access this computer from the network.

2.3.8.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information and applications may be unavailable.

2.4. Authentication/Password Configuration

2.4.1. User accounts must not be set such that the user cannot change their password

ID	Version	Level	Enforcement
NT4D-UC-3	1.0	baseline	recommended

2.4.1.1. Standard

User accounts must not be set such that the user cannot change their password

2.4.1.2. Detailed Steps

- Select change password at next logon for the account in question

2.4.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Account passwords may be compromised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

2.4.2. User accounts must not be set such that the password never expires

ID	Version	Level	Enforcement
NT4D-UC-4	1.0	baseline	mandatory

2.4.2.1. Standard

User accounts must not be set such that the password never expires

2.4.2.2. Detailed Steps

- For each account ensure that the password never expires flag is not set.

2.4.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Passwords that do not change are at greater risk of compromise
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 3. Network Security Configuration

3.1. Network Interface Considerations

3.1.1. Remote Access Server must be enabled only if required

ID	Version	Level	Enforcement
NT4D-NETW-1	1.0	baseline	mandatory

3.1.1.1. Standard

Remote Access Server must be enabled only if required

3.1.1.2. Detailed Steps

- Disable remote access server if it is not required

3.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Remote access server allows users potentially to gain unauthorised remote access
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 4. Configuration

4.1. Files and File Permissions

4.1.1. File and directory permissions must be restricted on the basis of least privilege

ID	Version	Level	Enforcement
NT4D-ACCESS-1	1.0	baseline	mandatory

4.1.1.1. Standard

File and directory permissions must be restricted on the basis of least privilege

4.1.1.2. Detailed Steps

- Ensure that the access permitted for each file and directory permits the minimum access permissions

4.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.2. Administration

4.2.1. Check password filter configuration

ID	Version	Level	Enforcement
NT4D-ADM-2	1.0	baseline	mandatory

4.2.1.1. Standard

The Notification Packages registry key must contain only authorised password filter or password synchronisation packages.

4.2.1.2. Detailed Steps

- Check the contents of the registry key \System\CurrentControlSet\Control\Lsa\Notification Packages.
- This key should name only authorised password filters and password synchronisation packages. It should not reference the FPNWCLNT package (see Knowledge Base Q99885). PASSFILT is an acceptable entry under this key.

4.2.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Passwords may be intercepted during password change.
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

4.2.2. Replication must be implemented only at the administrator level

ID	Version	Level	Enforcement
NT4D-ADMIN-1	1.0	baseline	mandatory

4.2.2.1. Standard

Replication must be implemented only at the administrator level

4.2.2.2. Detailed Steps

4.2.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 5. Auditing and Monitoring

5.1. Events to be alerted in real-time

5.1.1. User accounts should be locked out after 3 consecutive login failures

ID	Version	Level	Enforcement
NT4D-AUDIT-1	1.0	baseline	recommended

5.1.1.1. Standard

User accounts should be locked out after 3 consecutive login failures

5.1.1.2. Detailed Steps

- Define in the domain policy that accounts be locked out after 3 login failures

5.1.1.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Given enough attempts any account password may be guessed
- Unauthorised access may result from allowing a liberal number of logon attempts
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.1.2. The reset count for logon failures should be set to 7200 minutes

ID	Version	Level	Enforcement
NT4D-AUDIT-2	1.0	baseline	recommended

5.1.2.1. Standard

The reset count for logon failures should be set to 7200 minutes

5.1.2.2. Detailed Steps

- Define in the domain policy for reset count for logon failures be 7200 minutes

5.1.2.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Slowing down the number of guesses that can be attempted will hinder a breakin attempt.
- A short reset time effectively increases the number of attempts before lockout
- This may result in an account being compromised
- Business information may be accidentally or maliciously altered.
- Business information may be disclosed.
- Business information and applications may be unavailable.

5.1.3. The lockout duration should be set to forever

ID	Version	Level	Enforcement
NT4D-AUDIT-3	1.0	baseline	recommended

5.1.3.1. Standard

The lockout duration should be set to forever

5.1.3.2. Detailed Steps

- Define in the domain policy lockout duration to be forever

5.1.3.3. Risks Addressed

Where this control is not applied, the following residual risks exist:

- Setting lockout duration to anything other than forever allows password guessing attempts to be resumed against the account after the lockout period expires
- Given enough time and enough attempts account passwords will be guessed
- Accounts may be compromised
- Business information may be accidentally or maliciously altered.

- Business information may be disclosed.
- Business information and applications may be unavailable.

Chapter 6. Checklist

<i>User Configuration</i>		
<i>User Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-UC-2	Are user passwords set to be changed following reset or after the creation of a new account?	
NT4D-UC-7	Is a home directory specified for each user?	
NT4D-UC-6	Does each user account have the full name and description fields completed with the details of the account owner name, location and phone number?	
NT4D-UC-1	Do all users have a logon script defined?	
<i>Default Accounts</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-UC-5	Is the Guest account is disabled?	
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-PRIV-7	Is the advanced user right to lock pages in memory held by no one?	
NT4D-PRIV-8	Is the advanced user right to log on as a batch job held by any user?	
NT4D-PRIV-4	Is the user right to take ownership of files and directories held by administrators only?	
NT4D-PRIV-3	Is the user right to manage auditing and security log only available to administrators and the security group?	
NT4D-PRIV-2	Is the user right to backup files and directories only held by Backup Operators?	
NT4D-PRIV-6	Is the advanced user right to increase quotas must be held by administrators only?	
NT4D-PRIV-5	Is the user right to restore files and directories held by administrators and backup operators only?	
NT4D-PRIV-1	Is the user right, access this computer from network, available to everyone?	
<i>Authentication/Password Configuration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-UC-3	Are user accounts set such that the user can change their password?	
NT4D-UC-4	Is it ensured that user accounts are not set such that their password never expires?	

Checklist

<i>Network Security Configuration</i>		
<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-NET W-1	If Remote Access Server is enabled is it required?	
<i>Configuration</i>		
<i>Files and File Permissions</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-ACCE SS-1	Are file and directory permissions restricted on the basis of least privilege?	
<i>Administration</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-ADM- 2	Has the Notification Packages registry key been checked for Unauthorised/unexpected values in the Notification Packages registry key?	
NT4D-ADMIN- 1	Is replication implemented only at the administrator level?	
<i>Auditing and Monitoring</i>		
<i>Events to be alerted in real-time</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4D-AUDIT- 1	Are user accounts locked out after 3 consecutive login failures?	
NT4D-AUDIT- 2	Is the reset count for logon failures set to 7200 minutes?	
NT4D-AUDIT- 3	Is the lockout duration set to forever?	