

NT4 Server Security Standard

NT4 Server 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 12 baseline controls, and 0 above baseline controls, for a total of 12 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. Privileges	4
2.1.1. The advanced user right to increase quotas must be held by administrators only	4
2.1.2. The advanced user right to lock pages in memory must be held by no one.	4
2.1.3. The user right to backup files and directories must only be held by Backup Operators	5
2.1.4. The advanced user right to log on as a batch job must be held by no one.	5
3. Network Security Configuration	7
3.1. Network Interface Considerations	7
3.1.1. Remote Access Server must be enabled only if required	7
4. Configuration	8
4.1. Files and File Permissions	8
4.1.1. File and directory permissions must be restricted on the basis of least privilege	8
4.2. Administration	8
4.2.1. Replication must be implemented only at the administrator level	8
5. Auditing and Monitoring	10
5.1. Events to be audited	10
5.1.1. Auditing should be enabled for RAS for failed authentication and authentication timeout	10
5.1.2. Failed attempts to delete documents in a print queue should be audited	10
5.1.3. Failed attempts to take ownership of documents should be audited	11
5.1.4. Failed attempts to change permissions on a print queue should be audited	11
6. Other	13
6.1. RAS should be set up to encrypt logon information by any remote client before sending across the network	13
6.1.1. Standard	13
6.1.2. Detailed Steps	13
6.1.3. Risks Addressed	13
7. Checklist	14

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 server.
- To provide guidance to administrators, developers and security personnel in securely implementing <trademark>Microsoft</trademark> <trademark>Windows</trademark> NT4.0 server.

1.2. Scope

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

All of the organisation's NT4.0 server 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 servers. Controls specific to workstation, domain controller, 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, an item of off the shelf software, hardware, media, a data item, a 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, except where a control relates to any “Information Asset”.

The use of “must” or “will” indicates what the author considers to be a mandatory control.

However, whether the controls listed here are mandatory for your organisation is entirely at your organisation's discretion and thus they should be interpreted as representing the strongest recommendation of the author.

The use of “should” or “recommended” or “ought” indicates that the author believe that the controls in question are worthwhile and should be implemented unless such an implementation is impossible, onerous or impractical. Again, the implementation of controls so recommended in this document is entirely at your organisation's discretion.

Chapter 2. User Configuration

2.1. Privileges

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

ID	Version	Level	Enforcement
NT4S-PRIV-6	1.0	baseline	mandatory

2.1.1.1. Standard

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

2.1.1.2. Detailed Steps

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

2.1.1.3. 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

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

ID	Version	Level	Enforcement
NT4S-PRIV-7	1.0	baseline	mandatory

2.1.2.1. Standard

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

2.1.2.2. Detailed Steps

- Ensure that no one holds this right

2.1.2.3. 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

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

ID	Version	Level	Enforcement
NT4S-PRIV-2	1.0	baseline	mandatory

2.1.3.1. Standard

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

2.1.3.2. 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

2.1.3.3. 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

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

ID	Version	Level	Enforcement
NT4S-PRIV-8	1.0	baseline	mandatory

2.1.4.1. Standard

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

2.1.4.2. Detailed Steps

- Ensure that no one holds this right

2.1.4.3. 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

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
NT4S-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
NT4S-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. Replication must be implemented only at the administrator level

ID	Version	Level	Enforcement
NT4S-ADMIN-1	1.0	baseline	mandatory

4.2.1.1. Standard

Replication must be implemented only at the administrator level

4.2.1.2. Detailed Steps

4.2.1.3. 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.

Chapter 5. Auditing and Monitoring

5.1. Events to be audited

5.1.1. Auditing should be enabled for RAS for failed authentication and authentication timeout

ID	Version	Level	Enforcement
NT4S-AUDIT-4	1.0	baseline	recommended

5.1.1.1. Standard

Auditing should be enabled for RAS for failed authentication and authentication timeout

5.1.1.2. Detailed Steps

- Set up auditing to audit for failed authentication and authentication timeout

5.1.1.3. Risks Addressed

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

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

5.1.2. Failed attempts to delete documents in a print queue should be audited

ID	Version	Level	Enforcement
NT4S-AUDIT-1	1.0	baseline	recommended

5.1.2.1. Standard

Failed attempts to delete documents in a print queue should be audited

5.1.2.2. Detailed Steps

- Set up auditing to audit for failed attempts to delete documents in a print queue

5.1.2.3. Risks Addressed

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

- Business information and applications may be unavailable.

5.1.3. Failed attempts to take ownership of documents should be audited

ID	Version	Level	Enforcement
NT4S-AUDIT-3	1.0	baseline	recommended

5.1.3.1. Standard

Failed attempts to take ownership of documents should be audited

5.1.3.2. Detailed Steps

- Set up auditing to audit for failed attempts to take ownership of documents in a print queue

5.1.3.3. Risks Addressed

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

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

5.1.4. Failed attempts to change permissions on a print queue should be audited

ID	Version	Level	Enforcement
copy of NT4S-AUDIT-2	1.0	baseline	recommended

5.1.4.1. Standard

Failed attempts to change permissions on a print queue should be audited

5.1.4.2. Detailed Steps

- Set up auditing to audit for failed attempts to delete documents in a print queue

5.1.4.3. Risks Addressed

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

- Business information and applications may be unavailable.

Chapter 6. Other

6.1. RAS should be set up to encrypt logon information by any remote client before sending across the network

ID	Version	Level	Enforcement
NT4S-NETW-2	1.0	baseline	recommended

6.1.1. Standard

RAS should be set up to encrypt logon information by any remote client before sending across the network

6.1.2. Detailed Steps

- RAS should be configured to encrypt logon information by any remote client before sending across the network

6.1.3. Risks Addressed

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

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

Chapter 7. Checklist

<i>User Configuration</i>		
<i>Privileges</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4S-PRIV-6	Is the advanced user right to increase quotas must be held by administrators only	
NT4S-PRIV-7	Is the advanced user right to lock pages in memory held by no one?	
NT4S-PRIV-2	Is the user right to backup files and directories only held by Backup Operators?	
NT4S-PRIV-8	Is the advanced user right to log on as a batch job held by any user?	
<i>Network Security Configuration</i>		
<i>Network Interface Considerations</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4S-NETW-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>
NT4S-ACCESS-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>
NT4S-ADMIN-1	Is replication implemented only at the administrator level?	
<i>Auditing and Monitoring</i>		
<i>Events to be audited</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4S-AUDIT-4	Is auditing enabled for RAS for failed authentication and authentication timeout?	
NT4S-AUDIT-1	Are failed attempts to delete documents in a print queue audited?	

Checklist

NT4S-AUDI T-3	Are failed attempts to take ownership of documents audited?	
copy of NT4S-AUDI T-2	Are failed attempts to change permissions on a print queue audited?	
<i>Other</i>		
<i>Control ID</i>	<i>Checklist Question</i>	<i>Your Answer</i>
NT4S-NET W-2	Is RAS set up to encrypt logon information by any remote client before sending across the network?	